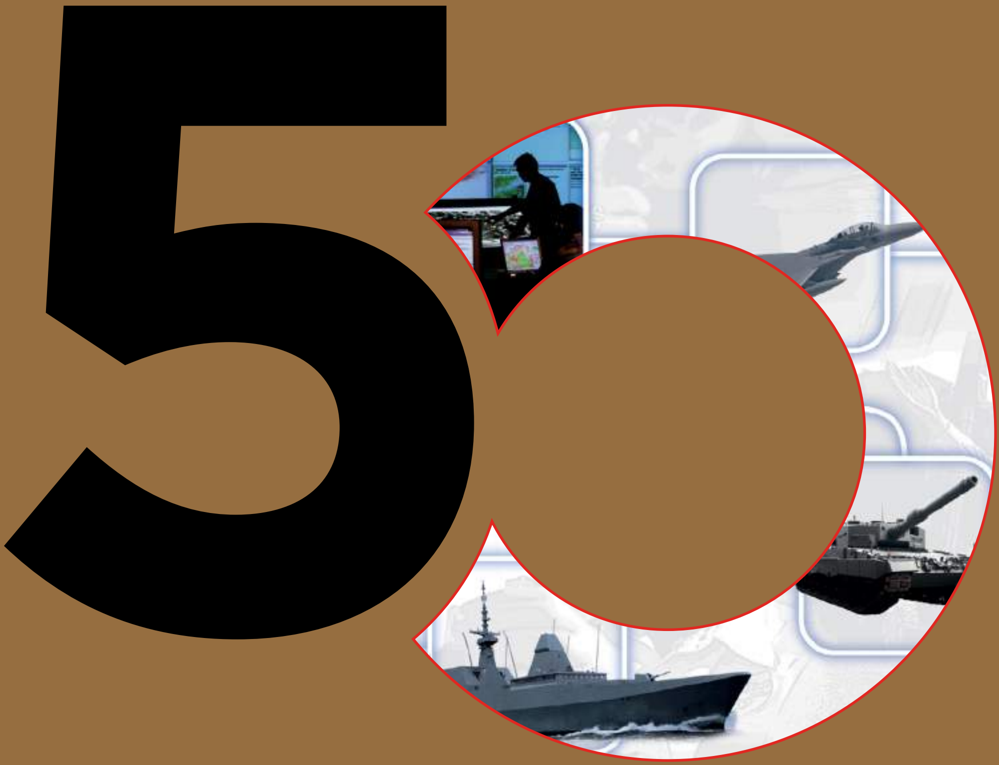
ENGINEERING SYSTEMS-OF-SYSTEMS



> *"DTC IS THE SECRET-EDGE WEAPON OF THE SAF"*
>
> DR NG ENG HEN
> MINISTER FOR DEFENCE

DEFENCE TECHNOLOGY COMMUNITY
50th ANNIVERSARY

ENGINEERING SINGAPORE'S DEFENCE — THE EARLY YEARS

DTC IS THE SECRET-EDGE WEAPON OF THE SAF

The opinions and views expressed in this work are the authors' and do not necessarily reflect the official views of the Ministry of Defence

TABLE OF CONTENTS

FOREWORD

The journey of Singapore's Defence Technology Community (DTC) parallels that of the Singapore Armed Forces (SAF) – indeed both were co-dependent and iterative processes which fed off each other's success. Pioneers in both communities recognised very early on the stark limitations of a small island with no geographical depth and limited manpower. But despite this realisation, they were undaunted and shared a common resolve to mitigate Singapore's vulnerabilities and constraints, and build a credible SAF through sheer will, commitment and the harnessing of the powers of technology. In Dr Goh Keng Swee's words, "we have to supplement the SAF's manpower with new technology, as manpower constraints will always be there. Our dependency should be more on technology than manpower. And we must develop indigenously that technological edge." As worthy and important as these ideals were, it was an arduous journey for the DTC. With poor standards of general education, let alone engineers or scientists, how could Singapore develop such capabilities?

This book series chronicles the last 50 years of that ascent that begun in 1966. The DTC has indeed come a long way from its humble beginnings and with it, a transformation of the SAF's capabilities. Today, both the SAF and the DTC are respected professional bodies and the requests from advanced economies to collaborate reflect the standards which we have achieved. Our closely-knit community of defence engineers and scientists stands at the frontier of technological progress. Indeed the DTC is the secret-edge weapon of the SAF.

As the DTC celebrates its 50th anniversary, we want to thank especially its pioneers who were committed to achieve the unthinkable and were not daunted by severe challenges along the way. Their efforts and beliefs have spawned world class agencies such as DSTA and DSO, and the family of Singapore Technologies (ST) companies.

More hearteningly, the virtuous effects extend into mainstream society too. Today the defence cluster of DSTA, DSO, MINDEF, the SAF and ST employs the largest proportion of scientists and engineers in Singapore – almost one in every 12! It is not an overstatement that these entities have been the main receptacles to maintain the science and technology capabilities in our nation, providing life-long careers in the process.

Beyond defence, the DTC has also positively impacted our society in a variety of ways: in producing mass thermal scanners to combat the 2003 SARS outbreak, in designing and building the iconic Marina Bay Floating Platform to host the National Day Parades and sports events, in breaking new ground and old mindsets when we built the underground storage for munitions, in forming the nucleus to start the MRO (maintenance, repair and overhaul) industries to service airlines in Singapore and globally.

The stories that are told in this book series should lift the spirits of Singaporeans, old and young. They celebrate what pioneers and successive generations of committed scientists and engineers have accomplished over the years. But they also give hope to our future, as they will serve as reminders during difficult times to overcome challenges and continue to keep Singapore safe and secure for many years to come.

Dr Ng Eng Hen
Minister for Defence
Singapore

MESSAGE

The Defence Technology Community (DTC) has steadily evolved over the last 50 years. We started off as a small, three-man technical department in the Logistics Division in 1966 supporting defence equipment procurement and there was much work to be done. The Army then was largely equipped with second-hand vehicles and surplus equipment left by the British. The Republic of Singapore Navy (RSN) had two boats, one steel and the other wooden. Recognising the need to overcome the immutable challenges of geography and resource constraints facing Singapore, we extended our scope to include conceptualisation, development and upgrade of defence systems. These efforts leverage the force multiplying effects of technology to meet the unique challenges and operational requirements of the Singapore Armed Forces (SAF), beyond what could be had buying off-the-shelf.

This four-book "Engineering Singapore's Defence – The Early Years" series covers the entire spectrum of the DTC's work in the land, air and sea domains to deliver cutting-edge technological capabilities to the SAF. It chronicles our 50-year journey and documents the largely unheard stories of our people – their challenges, struggles and triumphs, their resolve and ingenuity, and their persistence in overcoming the odds. These stories include:

- The upgrading of the French-made AMX-13 light tank to the AMX-13 SM1 configuration by the DTC, the Army and ST Engineering, laying the foundation for the design, engineering and production of the Bionix, Bronco and Terrex armoured fighting vehicles for the Army.
- The integration of the RSN's missile gunboats and missile corvettes which built up the DTC's confidence to move on to specify and acquire best of breed systems to integrate into new ships like the frigates. It also laid the foundations for ST Engineering's capabilities to design and build ships for the RSN and some other navies.
- The conversion of old US Navy's A-4 Skyhawk aircraft into the A-4SU Super Skyhawk for the Republic of Singapore Air Force, building up ST Engineering's capabilities to undertake further aircraft upgrades such as for the F-5E Tiger fighter aircraft, and to undertake servicing and repair of commercial aircraft.
- The system-of-systems integration efforts to evolve the island air defence system, building on legacy systems left by the British to seamlessly incorporate new weapons, sensors, and indigenously developed command and control systems to extend the range and coverage of Singapore's air defence umbrella, and the build-up of the DTC as a system-of-systems to deliver cutting-edge capabilities and systems to the SAF, and to meet the technology requirements of the nation.

While not exhaustive, these stories provide us with a glimpse of the "dare-to-do" and enterprising spirit that our DTC personnel and forerunners possess.

There is no end to change and transformation. Singapore and the SAF will continue to face many challenges in the years ahead. However, with the capabilities and expertise developed over the years in its more than 5,000-strong personnel, and its established linkages with renowned R&D partners locally and around the world, I am confident that the DTC will remain steadfast in delivering the critical technologies and innovative solutions for the SAF and the nation. May the stories in these books inspire our current and future defence engineers and scientists to continue to push boundaries and think creatively to deliver capabilities that will safeguard our sovereignty for the years to come.

Ng Chee Khern

Mr Ng Chee Khern
Permanent Secretary (Defence Development)
Ministry of Defence, Singapore

PREFACE

The engineering challenges of safeguarding Singapore's security have involved overcoming the twin constraints of size (resources, especially population) and strategic depth (geographical space). Having a modest number of high quality and high readiness defence systems that are capable of multiple roles provides a strong foundation for our defence, but how can we scale this to the level required for our needs?

Our defence engineers have applied systems thinking and engineering approaches to overcome some of these challenges. A fundamental approach is to create a System-of-Systems (SoS) by integrating individual systems together such that the SoS will have unique emergent properties not available from the constituent systems in themselves. Some of these properties include enhanced situational awareness, cooperative engagement, speed (both in decision making and execution) as well as resilience.

The desired emergent capabilities (or desired defence and security effects) of these SoS may be categorised into effecting force multiplication, creating strategic depth, enhancing sustainability and operating effectively in complex environments. These are elaborated as follows:

First, force multiplication is the ability to deploy technology-enabled flexible force structures that can mass at decisive points to achieve superior combat power. The critical enablers for force multiplication are interoperability and Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR).

Second, strategic depth in both the space and time dimensions can be created via several complementary approaches. One is to provide foresight and early warning through the exploitation and smart use of information, with C4ISR and sense-making systems as critical enablers. Another is to create virtual depth via the use of stealth, speed and fast decision cycles, with advanced platform technologies and C4ISR as critical enablers. Yet another approach is to employ resilient networks and systems, with protective technologies and system architectures as critical enablers.

Third, the achievement of sustainability over time requires efforts in multiple thrusts. One is to design adaptable and resilient systems and architectures, including the ability for legacy systems to be enhanced and integrated with new systems, enabled by systems architecting. Another is to ensure high reliability and readiness of systems, enabled by a strong engineering and logistics capability. Yet another is to have highly trained, competent and motivated personnel, enabled by organisational development and learning. Sound planning and execution with holistic and longer-term perspectives are also key, enabled by a defence capability development and management system. Finally, it is important to have a system that encourages innovation and learning, enabled by a culture where its people "dare to dream and to act upon these dreams".

Fourth, the ability to operate effectively in complex environments is enabled by sense-making and C4ISR systems and users that are accustomed to working in complex and uncertain environments and who are tech-savvy and well-schooled in complex systems thinking.

For the purpose of this book, we will introduce two notional categories of SoS – Defence SoS and Enabling SoS.

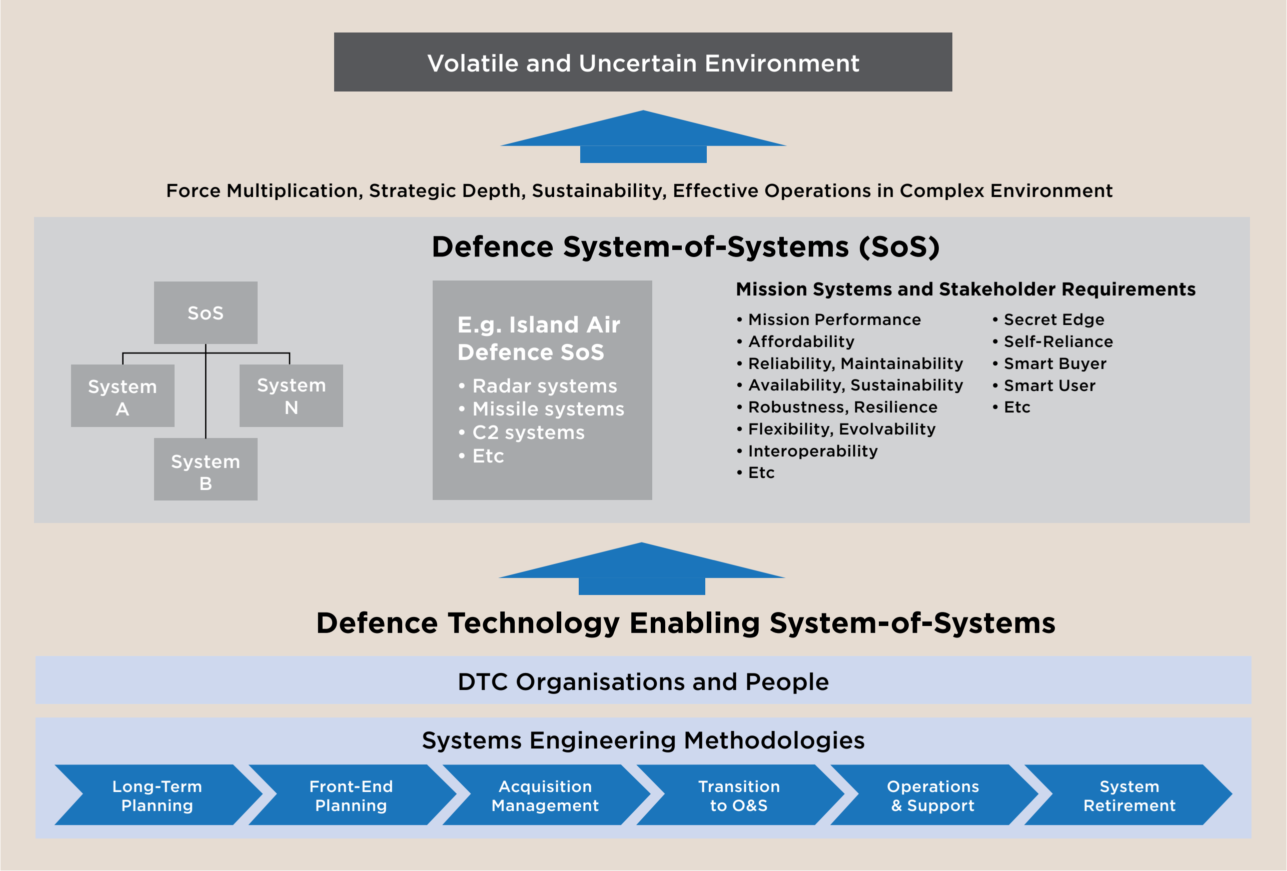
By Defence SoS, we refer to an integrated collection of individual military systems required to defend Singapore by fulfilling specific military operations such as air defence, maritime security and land battle. An example is the networked Island Air Defence (IAD) SoS that comprises a suite of individual systems such as ground-based radars, surface-to-air missile systems, aircraft and command and control (C2) systems that work cooperatively to defend the skies of Singapore. In Chapter 1 we will look at the history of how Singapore built up its IAD capability from the 1960s to the present, first by acquiring and developing systems and subsequently evolving systems into a Defence SoS in the 2000s.

By Enabling SoS, we refer to an integrated collection of systems that enables the existence of the Defence SoS, from designing it, to implementing it, to sustaining it throughout its lifetime. An example is the Defence Technology Community (DTC), comprising an interdependent ecosystem of engineering organisations and methodologies that work in concert to deliver the Singapore Armed Forces' technological systems (hardware, software). Our defence systems have been engineered and supported by the DTC over the past 50 years. This accumulated knowledge base and the experience and expertise of our defence engineers form a formidable resource pool that can be aptly termed an Enabling SoS.

The rest of the book will expound on the DTC Enabling SoS. From Chapters 2 to 8, we will examine more details of the DTC Enabling SoS. Chapter 2 – Concepts to Capabilities will share more of how concepts and requirements for Defence systems and SoS are formulated before implementation; Chapter 3 – Software Systems Design and Realisation will elaborate on software systems (C2 and Enterprise Information Technology (IT) systems) – a critical component that "glues" together different systems into a Defence SoS; Chapter 4 – Operations and Support Engineering will illuminate a critical area that is often away from the limelight, but one that enables defence systems and SoS to sustain their performance and viability. Chapter 5 – Systems Engineering Methodologies and Tools will provide more insights on the key systems engineering methodologies and tools used in the DTC, in addition to those already covered from Chapters 2 to 5; Chapter 6 – Organisation and People Development will trace how the organisations within DTC evolved over time, together with the build-up of a critical mass of engineering and scientific expertise; Chapter 7 – Beyond Defence will bring the reader beyond the defence context in areas that DTC has made significant impact with its engineering and scientific expertise; and Chapter 8 – Advancing DTC's Systems Approach through the Generations will highlight key success factors for the DTC thus far, summarising our lineage of systems engineering leaders and offering food for thought in DTC's journey ahead. Chapter 9 – Beyond DTC50, is a think piece with its focus on the decades ahead, examining the trends and constants that will shape the DTC and its contributions to the long term survival, security and success of Singapore as a nation.

Richard Lim

RADM (Ret) Richard Lim
Editor, Engineering Systems-of-Systems


Volatile and Uncertain Environment
Force Multiplication, Strategic Depth, Sustainability, Effective Operations in Complex Environment
Defence System-of-Systems (SoS)
SoS
System A
System N
System B
E.g. Island Air Defence SoS
• Radar systems
• Missile systems
• C2 systems
• Etc
Mission Systems and Stakeholder Requirements
• Mission Performance
• Affordability
• Reliability, Maintainability
• Availability, Sustainability
• Robustness, Resilience
• Flexibility, Evolvability
• Interoperability
• Etc
• Secret Edge
• Self-Reliance
• Smart Buyer
• Smart User
• Etc
Defence Technology Enabling System-of-Systems
DTC Organisations and People
Systems Engineering Methodologies
Long-Term Planning
Front-End Planning
Acquisition Management
Transition to O&S
Operations & Support
System Retirement

Relationship between Defence SoS and Enabling SoS

Chapter One

EVOLUTION AND DEVELOPMENT OF ISLAND AIR DEFENCE SYSTEM-OF-SYSTEMS

A Historical Narrative of Building Singapore's Island Air Defence Systems from the 1960s to 1990s

A Journey Fuelled by a Need and a Vision

The evolution of Singapore's Island Air Defence (IAD) system provides a useful narrative of the development of a Defence System-of-Systems (SoS). At the same time it illustrates the parallel development of some of the engineering capabilities and organisations that today form the Defence Technology Community (DTC) – the Enabling SoS for Singapore's defence.

In the early years, there was no established systems engineering body of knowledge to take reference from. The Ministry of Defence (MINDEF) Life Cycle Management (LCM) Manual only came into being many years later. This was a journey of learning through trial and error by taking calculated risks and measured steps. Two factors made this possible. First, the strong belief by senior leadership within MINDEF that we needed to build a strong indigenous systems engineering capability and their trust and support given to our young engineers and the fledgling engineering organisations that were established. Second, it was probably fortuitous that we had very limited resources to engage foreign consultants and defence contractors to meet our needs. Hence, there was no easy way out but to do many things ourselves.

Recollections of Prof Lui Pao Chuen, Er. BG (Ret) Wesley D'aranjo and Mr William Lau Yue Khei on the journey in building up Singapore's IAD systems from the 1960s to 1990s.

Five Power Defence Arrangements and Integrated Air Defence System

There was great fear that confidence in Malaysia and Singapore would dip without the air umbrella provided by the Royal Air Force (RAF). To allay this fear, the United Kingdom (UK) organised a Five Power Defence Conference with Australia, New Zealand, Malaysia and Singapore in Kuala Lumpur on 10th and 11th June 1968 to address the issue of the needs for the defence of Malaysia and Singapore.

The five countries agreed that in the event of an armed attack or such a threat, the governments concerned would immediately consult with one another to decide on measures to be taken. The Five Power Defence Arrangements would be established with a Joint Consultative Council comprising the respective Permanent Secretaries for defence of Malaysia and Singapore, and the High Commissioners of the UK, Australia and New Zealand, and with an Air Defence Council responsible for the functioning of the Integrated Air Defence System (IADS) and to provide direction for the Air Defence Commander.

IADS became operational on 1st September 1971 just before the complete withdrawal of UK troops. The headquarters of IADS (HQ IADS) was located in Royal Malaysian Air Force (RMAF) Butterworth Air Base and the Commander IADS would be a two-star Air Vice-Marshal of the Royal Australian Air Force (RAAF). The staff of the IADS would come from the five nations.

The RAAF with its fighter wing of French-made Mirage fighters would continue to operate from Butterworth, as they had since 1955 with two fighter squadrons and one bomber squadron. In 1970 the RAAF handed over Butterworth Air Base to the Malaysian Government and it became RMAF Butterworth Air Base.

One RAAF Mirage squadron would be deployed to Tengah Air Base from time to time for exercises to defend the southern sector with the Bloodhound surface-to-air missile (SAM) squadron.

Bloodhound Surface-to-Air Missiles

RAF No.65 Squadron with three sections deployed at the north-eastern end of Seletar Air Base formed part of the RAF Far East Air Force. The Bloodhound Mk2 was the most modern SAM with a range of 80km covering altitudes from 150ft to 65,000ft (around 46m to 20km). The missile, powered by ramjet engines would achieve a maximum velocity of Mach 2.7 in its flight out to intercept targets with speed of Mach 2 at a range of more than 80km. The missile would be guided to its target by a target tracking and illumination radar (TIR), the Marconi Type 97 Scorpion radar.

The Bloodhound squadron was however vulnerable as the launchers were fixed and could be attacked with low-cost mortar bombs. Operational analysis studies showed that the vulnerability would be greatly reduced if two sections of Bloodhound missiles could be deployed to other parts of the island. The best site would be on the top of Lim Chu Kang Hill, just north of the Nanyang University campus. The second best site would be at Amoy Quee Camp.

The late Mr Pang Tee Pow (left), then Permanent Secretary (Defence), accepting the handover of the Bloodhound SAM Squadron from a British Aircraft Corporation representative in 1974

Bloodhound missile section deployed at Seletar Air Base

Another view of Bloodhound missile deployment in 1974

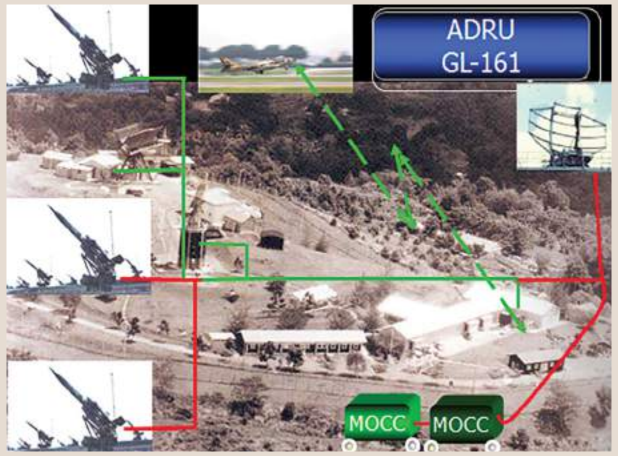
The Bloodhound missile would be accelerated by four boost rocket motors to a speed of Mach 2.5 in three seconds. The spent rocket casings would peel away and the Thor ramjet engines would continue propelling the missile to its target. The prescribed safety distance was three miles around the launcher. This safety distance and height constraint around the missile site resulted in the loss of development potential by the Housing and Development Board for Ang Mo Kio New Town.

One Bloodhound missile was fired during its service with the Republic of Singapore Air Force (RSAF). The firing took place on 24th September 1980 at UK Ministry of Defence (MOD) Aberporth in Wales in the UK. MOD Aberporth has played a significant part in the development and testing of a variety of military weapons and is still in use today. CPT Martin Baptist, a Bloodhound Engagement Controller from 170 Squadron, had the honour of firing a missile selected randomly from the RSAF's inventory of Bloodhound missiles. Soon after launch, the missile lost lock with its TIR but it was expertly re-acquired by CPT Martin Baptist who continued to complete the engagement successfully. A "hit" with a miss distance of 69ft was recorded, well within the lethality range of 180ft of the warhead. The missile fired by the RSAF was the hundredth Bloodhound missile ever to be launched.

The technical challenge in re-deploying the two sections of Bloodhound missiles from Seletar was its re-integration with the search radars and the GL-161 control centre of the Air Defence Radar Unit (ADRU) on the top of Bukit Gombak. The air defence controllers in ADRU would need to be connected in real time to the Bloodhound missile controllers at the three sites to share radar target data.

The Bloodhound missile was effectively an unmanned aircraft with two ramjet engines and electronic and electro-mechanical components that required regular servicing. The missiles from the missile site at Lim Chu Kang Hill would have to traverse half the island to get to the maintenance shops of the squadron in Seletar. Each trip was a major logistics operation as a collision of the missile carrying vehicle could cause serious damage. Because of all the care taken for each operation there were no road accidents with the Bloodhound missiles.

From RAF Gombak Radar Unit to Air Defence Radar Unit



The Island Air Defence System in the early 1980s

The radars and operations centre of the RAF air defence system for Singapore and southern Malaya were located on the top of Bukit Gombak, the second highest hill in Singapore. The civilian air traffic control centre at Paya Lebar Airport hosted the Joint Air Traffic Control Centre (JATCC). A microwave communication system connected the Gombak operations centre with JATCC, the operations centres of Tengah Air Base and Changi Air Base, and the Bloodhound squadron at Seletar. This was the most comprehensive air defence system of the RAF outside the UK.

The air defence system for northern Malaya consisted of radars and a control station located on Western Hill in Penang with two fighter squadrons based in the RAF airbase at Butterworth. Western Hill is the highest point in Penang at an elevation of 833m above sea level. A radar deployed at this site could detect targets from sea level to radar horizon. It would be very difficult for enemy attack aircraft to sneak into the defended airspace without being detected.

Given the limited height of our hills in Singapore for deploying ground-based radars, attacking aircraft flying low and hidden by terrain features could not be detected till they were 10km away. The defeat of attacking aircraft appearing at this range could only be achieved with low level SAM and anti-aircraft (AA) guns.

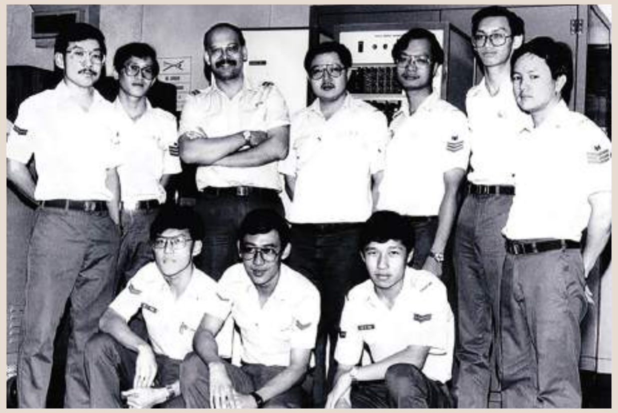
The two operations centres were connected by a modern tropospheric scatter radio link (also known as "troposcatter"). The RAF IADS was handed over to Malaysia and Singapore during the withdrawal of UK troops.

All the radars deployed on the top of Bukit Gombak were exposed and could be harassed by air and artillery attacks. The operations control centre was located inside a light building that had not been built to resist weapon effects. Space diversity would therefore be required to reduce the chances of our air operations being disrupted by enemy action. Relocating the large stationary radars was one solution studied. The conclusion of the operations research studies was that a mobile radar and mobile operations control centre would be a more robust solution. The best mobile three-dimensional (3D) radar then was the AN/TPS-43 operated by the US Air Force. The radar was manufactured by Westinghouse. The radar equipment and operational consoles were fitted inside cabins that could be towed to alternate deployment sites within a few hours.

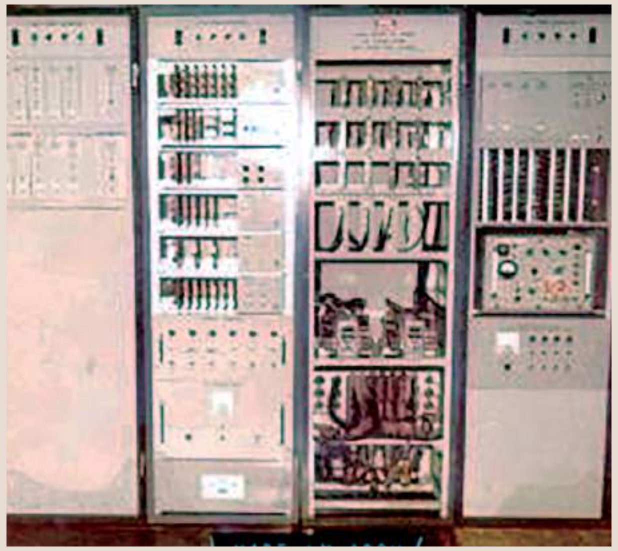
Integration with the GL-161 system in the operations centre at ADRU was a technical challenge that kept the radar engineers very busy but happy.

An Air Defence controller and his assistant at work in a pitch-dark operations room

CPT Wesley D'aranjo, an electrical and electronic engineering graduate from the University of Manchester Institute of Science and Technology, was posted from the Singapore Army (the Army) to ADRU. He learnt the intricacies of radars, radios, computers and display, and systems integration by being hands-on. He took the initiative to replace all the vacuum tube electronics with transistors and integrated circuits. This was the first major upgrade of a complex radar and control centre.



The team that re-designed, upgraded and manufactured new electronics for radars and signal processing at ADRU



A very large room of vacuum tube electronics re-designed and miniaturised into two racks

Special Projects Organisation

In 1979, the Special Projects Organisation (SPO) headed by then LTC Lui Pao Chuen as its Special Projects Director (SPD), was formed. This was part of MINDEF's efforts to develop defence technological capabilities and to undertake complex defence acquisition projects. SPO comprised five project divisions (PD): PD1 to PD5.

GL-161 Air Defence Command and Control System

Even at that time, SPD Lui understood that it was important for the then Defence Science Organisation (DSO) to build up capability to master the software of command and control systems. He called this area "real-time" software and later DSO called it "defence software". This real-time software processed data from radar sensors and converted them into useful information for the Air Force operators in the control centres.

The British left behind the GL-161 which, at that time, was their latest real-time computerised air defence command and control system. The GL-161 was capable of computing air intercepts. Radar sensors provided "raw radar" video to the GL-161 for processing and display. In those days, the Air Force operators preferred "raw radar" video because, with experience, they could perceive from the "raw radar" video information on aircraft turning (that was not available from synthetic extracted plots). Hence, they could predict what the targets would do by looking at the dynamics of the "raw radar" video. As sensors later became digital, "raw radar" video was replaced by regenerated video (1986) and later with symbols (1990s). There was a lot of debate in the Air Force then between the utility of "raw" versus "processed" video. It was expensive to handle "raw video" all the way from the radar head.

Mobile Operations Control Centre

The acquisition from Plessey of a mobile operations control centre (MOCC) was one of the solutions selected to replace the GL-161. MINDEF chose to purchase the MOCC separately from the radar sensors. This meant that we took upon ourselves the responsibility to integrate the MOCC with the radar sensors. The motivation for this was the ability to keep knowledge of some of its capabilities confidential and also to have the flexibility to "mix and match" systems to meet the operational requirements.

The plan was to use the MOCC as a launch pad for the build-up of the defence software capability in DSO. A team comprising six fresh graduates and experienced technicians from the Air Force was sent to Surrey, UK to master the inner workings of the Plessey MOCC.

There were two processing chains in the MOCC, each powered by a DEC PDP-11/34 processor. Each chain had a magnetic disk drive, which was not the most reliable for a transportable cabin. The software was written in a now defunct high-level language called RTL/2. Through RTL/2 the team learned how to design software in modules (called "bricks"). RTL/2 also had the "CODE" statement which allowed the program to jump to assembler coding to achieve critical real-time performance where needed. An important aspect of a command and control system that the team learned was how to achieve high availability through the switch-over between two processing chains.

Indigenous Systems Integration

When the MOCC team returned to Singapore, it set about integrating the MOCC with three radars in parallel, almost simultaneously:

- The existing mobile AN/TPS-43F – first operational in 1975 as the AN/TPS-43DX and then upgraded to improve radar performance and allow integration with a control centre
- The new ITT-RS320
- The Hollandse Signaalapparaten LAR2 at the Long Range Radar and Display System I air traffic control centre at Changi Airport – the LAR2 radar was commissioned in 1981

All three radars were just being brought into service or newly commissioned! The MOCC came with the source codes (except for the core operating system called MTS-3G) compiler, linker and other software tools.

The ITT-RS320 was developed for Sweden and only 17 such radars were produced – 16 for Sweden and one for Singapore. It was the most advanced "pencil beam steering" 3D radar available then and an improvement over the AN/TPS-32. The Swedes used their radars very cleverly. Each was installed on a 30m mast and protected in silos. Then, a game of "musical chairs" would be played and surveillance achieved by elevating and lowering the radars tactically. The radar would be allowed to "blink" during the time it was exposed. The mast was an ordinary mast, the type used at construction sites.

The team worked with Plessey to learn how to integrate the ITT-RS320 radar but did the integration with the other two radars independently.

One challenge the team faced was that the radar message formats were non-standard, unlike, for example, the Eurocontrol ASTERIX protocols of today. Each radar type had its own unique interface specifications. This meant that a common suite of utilities could not be developed to interpret them. Each software interface had to be separately developed and the team had to figure out where and how to insert these pieces of software into the MOCC. The radar manufacturers did not provide any tools, not even a radar simulator. The team had no choice but to work with the Interface Requirement Specifications (IRS) of each radar type and testing had to be done with live radar data.

The AN/TPS-43F radar at a deployment site

The ITT-RS320 radar

Another challenge was that the interfaces were of the synchronous type (this required tight synchronisation between signal transmission and signal reception mechanisms) which made them much more difficult to work with.

So how did this team overcome all these challenges? First, it set about building an in-house tool to decode and process the different data formats. In 1985, the team made use of an Apple IIe computer with an interface card that it fabricated to receive and decode the synchronous data coming from the radar under live test. This must have been one of the first uses of the Apple IIe for serious work! It also used a protocol analyser to view the raw data. By doing this, the team was able to verify the correctness of the IRS and eventually write the driver modules in the MOCC that were able to take in the radar data correctly to be processed by the MOCC tracker.

Other Radar Issues

Unlike the other two Air Force radars the LAR2 was not a 3D radar. As the MOCC required plot height data, a fictitious height had to be set as a default value and this caused the Air Force operators some consternation when such tracks were displayed, all with the same height.

We also had several issues with the ITT-RS320 radar. First, we learned that one should not specify and test radar range detection performance with theoretical Swerling target models that specify the radar cross-section of a given object. There were five types of Swerling target models using a distribution in the location-scale family of the "chi-squared distribution". The ITT-RS320 did not meet the range detection performance the Air Force wanted. What followed was a very difficult and protracted negotiation with the manufacturer on how the Swerling target models had been misinterpreted by us. The performance of the radar was as it was, and that we should have known better! In short, the radar manufacturer's response was "you tell me the answer you want and I will give you a calculation for it"! Thereafter, this bitter lesson taught us to use an unambiguous target – a "clean" F-5E aircraft flying head-on into the radar, as the basis for contractual specification and performance verification.

Second, we discovered that the primary radar plots were out-of-sync with the secondary surveillance radar plots. This was discovered through painstaking data analysis. This was most likely due to a design flaw that was not discovered during acceptance testing of the ITT-RS320. The secondary surveillance radar plots were received much later and therefore were not able to correlate with tracks that were initiated from the primary radar plots. MINDEF reported the problem to the manufacturer but they could not fix it. The team eventually solved the problem by modifying the MOCC tracking software to delay the tracking sector which in turn delayed the track-to-plot correlation process. This allowed more time for the secondary surveillance radar plots to come in for proper correlation.

The integration of MOCC and ITT-RS320 was a big challenge. The non-release of software by Plessey was a painful but very useful learning exercise. The lessons learned were applied to the purchase of the next generation of command and control system with the demand that the software be developed by a joint venture between Singapore Technologies

(ST) and Ericsson Microwave System called "Software Engineering of Singapore".

The lessons learned from bravely taking on the systems integration tasks for the MOCC enabled the team to increase its confidence to take on more challenging projects in the future.

Link to HQ IADS Butterworth

Around 1987, MINDEF had offered to cross-tell tracks from the MOCC to HQ IADS at Butterworth in Malaysia to facilitate exercises. The team developed and installed a PDP11/34 serial interface card in the MOCC and another external interface box to re-format the track messages and send them via a leased telephone line to Butterworth. At the Singapore end, the team also implemented a large screen display projected from a Barco projector connected to an International Business Machines Corporation (IBM) 286 AT PC that interpreted the tracks coming from the interface box.

Singapore Air Defence System, Version 1

Following the decision to purchase the Hunter fighter aircraft and Bloodhound SAM system, the Singapore Government decided expatriate officers would be employed to build up the Air Force, known then as the Singapore Air Defence Command (SADC).

In 1971 Brigadier General (BG) John Langer was seconded by the RAF to be the first Director of Air Staff, MINDEF. The Head of Air Operations was Group Captain (GC) Marie Turnbull. The Head Air Logistics was GC Basil Fox. Head Air Engineering was Mr Wong Yeok Yeok, a very experienced and respected aircraft engineer seconded from Singapore Airlines.

The SADC Order of Battle (ORBAT) would consist of:

- Two squadrons of Hawker Hunter fighter aircraft
- Two squadrons of Next Generation fighter aircraft
- Two airbases (Tengah and Changi)
- One squadron of Bloodhound SAM system
- One air defence radar unit
- One mobile 3D air defence radar
- One squadron of low level SAM system (Rapier was the prime candidate)
- One squadron of Oerlikon 35mm AA guns

The acquisition of AA guns to protect vital assets began in early 1968 with the evaluation of the Bofors 40mm AA gun from Sweden and the Oerlikon twin 35mm AA guns from Switzerland. The fire control system of the Bofors 40mm AA gun, the L4/5, was made by Hollandse Signaalapparaten. The fire control equipment for the 35mm AA guns, Superfledermaus, was made by Contraves of Switzerland.

The first study visit to Switzerland in March 1968 was conducted by COL Kirpa Ram Vij, Director SAFTI and CPT Lui Pao Chuen, then Head Technical Department, Logistics Division.

The Bofors 40mm AA gun had the advantage of being the AA gun of the allied navies during World War II. It was battle proven and remained the market leader after the war.

Operations research had shown that the claims of both manufacturers (that the Probability of Kill (P_k) exceeded 0.8) were true only for the engagement of targets flying straight and level, such as when firing at banner targets towed by an aircraft. In an attack, fighters would be "jinking", i.e. executing evasive manoeuvres with sudden changes in direction, which made it very difficult for the fire control system to predict the future position of the aircraft for the AA rounds to score a hit.

The pilot would need to aim at the target and to release the bombs. The time for this depended on the skill of the pilot. Experienced pilots would take less than two seconds and "rookies" up to six seconds. Thus the window of opportunity to shoot a fighter down would be between two to six seconds.

The P_k would therefore depend on the number of rounds the AA guns could fire in a two-second burst. The designer of the Oerlikon 35mm AA guns had figured this out and had two barrels in each gun. With a combined rate-of-fire of 1,100 rounds per minute from the two barrels it was clearly superior compared to the single barrel Bofors gun which had a rate-of-fire of 330 rounds per minute.

In 1969 a team comprising LTC M S Gill, Chief of Artillery, LTC Chew Bak Khoon, Chief Communications and Electronics Officer, CPT Henry Cheong and CPT Lui Pao Chuen visited Switzerland and Holland to verify the performance of both systems during firing exercises and the logistics support required.

CPT Lui Pao Chuen (left) and CPT Henry Cheong (second from left) in discussion with personnel from Hollandse Signaalapparaten in 1969 during the evaluation of the fire control radar for AA guns.

On completion of the evaluation the team recommended the Oerlikon 35mm AA guns and Superfledermaus fire control equipment for the Singapore Armed Forces (SAF). Twelve fire units, each comprising one unit of fire control equipment and two guns, were purchased (the guns are highly reliable and with proper maintenance they remain operational to date). The analogue computer of the Superfledermaus was replaced in the early 1980s after about 10 years of service. The tracking radar and optical sights had also seen many upgrades. The only original parts of the Superfledermaus still in service are the cabinets and mechanical components.

The maximum engagement range of 5km by the Oerlikon guns will require the target to be detected beyond this range. A search radar with a range exceeding 10km will enhance the effectiveness of the fire unit.

The radars at ADRU could not detect attackers approaching at low level. The Giraffe radar with a 12m high antenna mast, made by Ericsson Microwave Systems for the Swedish Armed Forces, was found to be the most effective radar to cover the low level gap. It could provide direction to the Superfledermaus fire control tracking radar to search and track targets.

The candidates for the low level SAM missile system and their average fire unit cost (in Singapore dollars) were:

Rapier (UK)	$8m
Blindfire Rapier (UK)	$14m
Roland II (Germany)	$21m
Crotale (France)	$21m
Indigo (Italy)	$20m

All the systems, except for Rapier, were radar guided and had an effective engagement range of 10km when there was a line-of-sight to the target beyond this range. Operations research in the UK showed that in most scenarios detection of low flying aircraft could only be achieved by 10km and therefore a maximum engagement range of 6km for the missile would be sufficient. Rapier and Blindfire Rapier had been designed to defeat attacking targets at 6km.

Rapier was selected for the SAF. Rapier had the cost advantage and being modular in design allowed a night engagement capability to be added with the DN181 "Blindfire" radar. Slightly earlier, the US Air Force had conducted a competition for the acquisition of a low level air defence SAM system for the protection of their airbases in Europe. However, Roland II was the winner of this competition.

Mr Norman Augustine, Under Secretary of the US Army, visited Singapore in the mid 1970s. A member of his delegation was BG John Dean, the project officer who had led the competition for the US Air Force low level air defence SAM system. He shared that Roland II won because it had an automatic missile loader and a magazine that allowed 12 missiles to be launched before requiring reloading. Rapier had only four rounds on fixed launcher rails. The RAF had found that in scenarios of less than 18 attacking aircraft, a target defended by six Rapier fire units was the most cost-effective system. In the most demanding scenario of the US Air Force, with 54 attacking aircraft, Roland II was superior as engagement opportunities were lost during reloading of Rapier missiles.

This information was helpful as it confirmed the cost effectiveness of Rapier, determined by our operations analysis studies.

Pioneering Integrated Air Defence System
2G Air Defence System
BLOODHOUND
I-HAWK
RAPIER
RBS-70
35MM GUNS
MALAY PENINSULA
SINGAPORE

Illustration of multi-layered Island Air Defence System

Stinger versus RBS-70

In 1974 the Army had determined an operational need for the defence of Army units in the field. Though foliage and camouflage would provide the best defence from air attacks, the movement of armoured units along roads and open ground would expose them to attacks by fighter ground attack aircraft and attack helicopters.

Mobile air defence of armoured units is very demanding. The very short range of combat required automatic detection and tracking of targets from the moving AA tank and engagement within the dead zone of 1km of SAMs. Dr Buehler, then Chairman of Oerlikon, had identified this need and used company funds to develop a turret armed with twin Oerlikon 35mm AA guns and a radar fire control mounted on a Leopard chassis. The German Army evaluated and found that this system best met their operational requirements and purchased it. This AA tank was named "Gepard".

Unlike the German Army, the US Army did not have such a stringent operational requirement. In their concept of operation a conflict would begin with air superiority missions, which the US Air Force would undertake and complete before combat on the ground began. A simple man-portable SAM, "Redeye", was issued to their armoured units for self-defence. Development of Stinger to replace Redeye began in 1967 and adopted for service in 1972.

Our Army wanted Stinger as Gepard did not meet their operational requirement. The candidates for this competition were:

- Redeye (US)
- Blowpipe (UK)
- Stinger (US)
- RBS-70 (Sweden)

Redeye was ruled out, as the missile could be defeated by fighter aircraft manoeuvre and flares.

The command line-of-sight guidance of Blowpipe required the operator to guide the missile to target with a thumb joy stick on the aiming unit clipped to the launching tube. Target acquisition was very difficult and to guide the missile required skills that would be difficult for National Servicemen (NSmen). This assessment was proven correct by the operational use of Blowpipe by UK troops in the Falklands War. There were reports that of the 100 Blowpipe missiles launched only nine scored hits against slow flying aircraft and helicopters.

The two finalists were Stinger and the Bofors RBS-70 used by the Swedish Army.

The advantage of Stinger was its "fire-and-forget" capability. However, target acquisition was a serious problem as the operator would need to find his target in his sight from verbal directions provided by the commander and other crew members of his vehicle. Fratricide was assessed to be a serious challenge as the commander and gunner would have to decide if a target was "friend or foe" mainly by visual aircraft recognition. The simple Identification Friend or Foe (IFF) equipment mounted on the sight could help to identify friendly aircraft if their IFF transponders were switched on. However, an aircraft without IFF returns could be a friendly with its IFF turned off or not serviceable. The commander with the help of his binoculars would have to make the final decision to launch the missile. The missile seeker was assessed to be vulnerable to flares dropped by attacking aircraft. The weight of the launcher and missile at 15kg was heavy for our soldiers to carry on their shoulders to search and acquire targets.

For the RBS-70, the Swedes overcame the weight problem by using a stand to support the launcher. The operator could then sit while searching and acquiring targets. The critical need of target acquisition was met and enhanced with the use of the Giraffe radar to detect targets and designate them to the fire unit. The operator would then need to search in the designated piece of sky and acquire it as soon as it appeared in his sight. Target identification would be determined initially by air defence controllers in the Giraffe radar control cabin via their own aircraft situation picture which was also connected to the regional air force operations control centre. The commander and gunner would make the final confirmation using IFF and optical recognition. The chance of fratricide of RBS-70 was greatly reduced as compared to Stinger. The missile was immune to flares as it was guided to target riding on a laser beam that the missile operator aimed at the target.

RBS-70 was clearly a superior air defence weapon system. However, one disadvantage assessed was that the operator would need to track the target to keep the laser beam on it. This required the operator to be well trained and calm when engaging a target. As operators could be expected to be excited and scared during combat, there was a need to assess the loss of intercept performance under emotional stress.

To confirm the performance of our operators locally, Bofors was requested to bring a training system to Singapore for test and evaluation from September to October 1977. The air defence of army units was the responsibility of the Army. Thus G5 Army led the test and evaluation programme. The Chief of Artillery was the Senior Specialist Staff Officer for Army air defence and 160 Battalion, the AA gun battalion, was an artillery unit then. The RSAF experts on SAM operation were from the 170 Squadron, the Bloodhound SAM unit. Air Operations Department was a key participant as flying of aircraft for the tests would be its responsibility. Technical evaluation would be done by Systems Integration Management Team and Electronic Test Centre (now known as DSO). This test and evaluation programme was a landmark with the Army working closely with the RSAF in the planning and execution of the programme. Eight Non-Commissioned Officers from the 160 Battalion and 170 Squadron were trained by a team from Bofors on the operation of the RBS-70 missile system. A series of flight trials was conducted in Changi and the final demonstration was conducted for VIPs in October 1977.

In the operational evaluation of RBS-70 in standalone configuration and using fighter aircraft as targets, the average reaction time was found to be longer as compared to the timing in the specifications. The latter could rarely be achieved even under ideal conditions. However, the test and evaluation was done without the critical Giraffe radar to enhance target acquisition. With the subsequent integration of a Giraffe radar and the Air Force air operations centres, reaction time would be shorter and this would improve the performance of RBS-70 and allow the maximum range of the missile to be exploited.

Local flight trials of RBS-70, viewed by MINDEF officials, at Changi Air Base in October 1977

RBS-70 was the obvious winner of the competition for an air defence weapon of the Army when the US disallowed the export of Stinger to Singapore. An initial purchase was made of one Giraffe radar and RBS-70 fire units and missiles for training in 1979. A team of 14 officers and 10 technicians went to Bofors to be trained on the operation and maintenance of RBS-70. In May 1980, on completion of the training programme, a live-firing exercise was conducted at the Swedish missile range RFN located at Vidsel, close to the Arctic Circle.

The RBS-70 project was the first project of the Project Management Team (PMT) formed to take care of air defence projects. The PMT was the predecessor, and later formed one of the divisions of the SPO. Today, we speak easily and confidently about missile systems, interfaces, integration, command line-of-sight guidance, radars, data links and so on. At that time, all of these were entirely new and perhaps even "Greek" to novices who had to deliver such projects. "Daring" engineering work was undertaken by ourselves, despite the fact that we were completely inexperienced and had very few teachers to learn from. The SAF constantly needed something "different". Yet, the conventional wisdom was to leave such requests for changes and modifications to the overseas manufacturers.

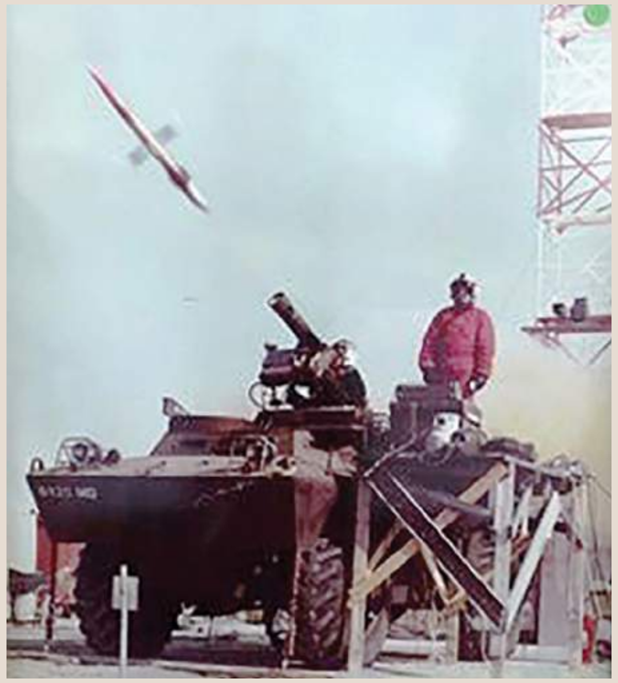
In order to keep up with armoured units, the RBS-70 system had to be installed in an armoured vehicle. The V-200 was selected for this. This meant we decided to design, develop, test locally as well as conduct live-firing in Sweden, and go into series production all on our own!

The RBS-70 system was operated by a commander and firer. The complete fire unit was designed for a "soft" ride and each major component had its own protective transit case. RBS-70 was designed for deployment on the ground; the Swedish Army had developed an optimal workflow for fire unit deployment and target engagement.

The fire unit consisted of:

- Sight
- Stand with tripod legs onto which the sight was attached
- Dedicated communications system between commander and firer
- IFF system with the antenna integrated with the transceiver
- Target data receiver (TDR)
- Missiles

The fire unit communicated with the Giraffe radar via the TDR only.



Firing of an RBS-70 missile from a V-200 vehicle

MINDEF and RSAF officials and Singapore Air Defence Artillery operators at the live-firing exercise conducted at RFN, Vidsel, circa 1980

The following were the requirements for the new system. In effect, a completely new system evolved:

- The fire unit had to be installed in the V-200 and operated in two modes – inside the vehicle for transit and administrative moves, and elevated for target engagement.
- The V-200 needed the following new mechanical parts:
  - o redesigned top deck
  - o new cupola
  - o ready-use-missile container on the new top deck
  - o easy-to-use elevating platform to which the sight and stand were installed and secured easily, and removed quickly if the fire unit needed to redeploy outside the vehicle
  - o racks for missile storage in the V-200
  - o adjustable stand for the TDR
- The fire unit communications system had to be interfaced to the combat radio system of the V-200, and CVC helmets used instead of the RBS-70 headset.
- The IFF antenna had to be split from its transceiver and placed in front of the sight; the IFF transceiver was placed low on the RBS-70 and lost line-of-sight when installed in the V-200 even in the elevated mode.
- Ensure that operational and system technical performance – safety, shock and vibration profiles, missile guidance, DC power, ergonomics, coming-into-action and engagement workflow – was not degraded by the new environment in which the system was to be installed, transported and operated.
- Conduct local trials to prove the viability of the new system design (with very limited test means and instrumentation available).
- Prepare for live-firing trials at Robotförsöksplats Norr (RFN) Vidsel, the Swedish missile test range inside the Arctic Circle.

- Take into consideration and prepare for eventual production vis-à-vis the build-up of Singapore Air Defence Artillery (SADA) battalions.

Work on the installation started towards the end of 1979. The team was well tutored by SPD Lui. It consisted of CPT Wesley D'aranjo, one electronics technician "borrowed" from ADRU and two mechanical technicians from Singapore Automotive Engineering, Mr Khoo Wai Yeow and Mr Richard Kwok (now Dr Richard Kwok). SPD Lui was kind enough to allow much time to complete the vehicle for live-firing tests in Sweden. The second prototype had to be ready well before the firing date, which had already been set for early May 1980!

The design for mounting the RBS-70 on the V-200 – the "elevating platform" – was completed by March 1980. Two prototypes were fabricated. The first prototype was used for various technical trials – vibration, shock, ergonomics and simulated firings – so as to verify the suitability of the design for operational use of the RBS-70. The first prototype was subjected to a 5,000 mile endurance test over roads, tracks and cross-country at the Sungei Gedong armour driving test track. Defects were analysed and the design iterated to eliminate the causes of the defects.

Some months later, we learned that Bofors was planning to install RBS-70 in the M113. Two engineers from Bofors came for a week to study our prototype. They wanted to learn the methods we had adopted to solve various problems, like the attenuation of vehicle vibrations, and elevating the sight from inside the vehicle to firing position. To encourage a more open exchange of views and information, we took time to study their drawings and gave them our comments. In exchange, we received their drawings which contained some useful designs. This exchange of information was of benefit to both parties. The Bofors engineers were pleasantly surprised by the amount of information on operational concepts they had gained in the exchange. They were impressed by our solutions and concluded that the mounting would be safe and acceptable for firing the RBS-70 missile.

RBS-70 was designed for deployment on the ground. The Bofors engineers cautioned that the back blast of the missile could hit the top deck of the V-200 for high elevation firings. The back blast might rock the vehicle and cause the laser guidance beam to be deflected too much for the missile in flight resulting in guidance loss and failure. To check if this would be a problem, we conducted two local simulated "high angle" firings with dummy Armburst missiles. Vehicle movements were measured and compared with the RBS-70 specifications for the allowable angular rotation rates of sight.

During the May 1980 live firing exercise in Sweden, and prior to each firing, the RBS-70 sight was used intensely for numerous practice engagements. Ten missiles were fired successfully from the V-200. Our users, the Swedish Army and Bofors were pleased with the data collected based on a working model of the RBS-70 in the V-200. These firings marked the end of the development period that lasted less than a year.

By mid 1981, six prototype RBS-70/V-200 vehicles were produced for further operational evaluation and troop trials. These were completed by September 1981 and all designs "frozen". Approval for series production was given and, in total, Singapore Automotive Engineering delivered a considerable number of production vehicles by 1983.

The RBS-70/V-200 vehicles have continued to be used for air defence, air base defence and island defence for many years.

V-200 and RBS-70 during National Day Parade

Air Defence Weapon Operators operating the RBS-70 Ground-Based Air Defence system mounted on the V-200 Armoured Fighting Vehicle during Exercise Wallaby 2016

RBS-70 versus Rapier

The selection of the Giraffe radar and RBS-70 precipitated a question as to whether air defence units built for the Army could also be used for the low level air defence of Singapore. But, this would create a gap in the defence of Singapore when the units were deployed out country. These units could enhance the coverage but could not replace the need for national low level air defence units.

The second question was if the needs for national low level air defence could be met by RBS-70. There would be economic benefits to invest in RBS-70 instead of Rapier.

Rapier had a larger coverage against manoeuvring targets equal to three times that of RBS-70. Comparison of costs would be based on one unit of Rapier versus three units of RBS-70. As national air defence would need to be operational over long periods, the extent of manning time was a critical parameter.

The Rapier system being deployed

Personnel preparing for the first Rapier live firing

Rapier could be upgraded with DN181 "Blindfire" radar for operation at night and in time of poor visibility. This was considered to be another important capability. After all the operational studies and cost benefit analysis, MINDEF accepted the case for the Air Force to acquire Rapier.

The UK Army had developed Rapier to equip the units of the "British Army On the Rhine". Maintenance would be done at three levels: the fire unit, the battery and the base level at the manufacturer of Rapier in the UK. Trouble shooting at the fire unit would locate unserviceable assemblies and these would be replaced with spares. The assemblies removed would then be sent to the battery maintenance unit for tests by an Automatic Test Equipment (ATE) and the sub-assemblies identified to be unserviceable would be sent to the manufacturer for repairs. The turnaround time was long using this maintenance support system.

As distances to the deployment sites in Singapore were short, a central supply and maintenance base using factory test equipment and technicians would be more efficient. Initially, the manufacturer objected, as this had never done before, but was persuaded by our defence engineers and eventually agreed to the technical soundness of the alternative solution.

Mr Quek Gim Pew became a defence engineer in 1981 and expressed interest to do Research and Development (R&D) at DSO. Due to the urgency of building up our air defence capabilities, he was persuaded to manage an acquisition project first. He managed the Rapier successfully and was then posted to DSO.

Improved Hawk and Super Giraffe

The case for the replacement of Bloodhound with Improved Hawk (I-Hawk) was made on operational grounds and economics. The Bloodhound missile would prevent an enemy from using medium and high altitudes to perform its mission. It could not contribute to the low level air defence of Singapore. Besides medium and high altitude air defence, the I-Hawk missile could contribute to low level air defence.

A squadron of I-Hawk was estimated to cost S$100m. The I-Hawk was also assessed to have a lower operating cost compared to the Bloodhound, and an annual savings of S$5m could be achieved. As I-Hawk was a mobile system that was not dependent on fixed on-site infrastructure, it had the flexibility to be deployed in other parts of the island beyond the existing SAM sites. This would enable the land at the Bloodhound missile sites at Seletar and Amoy Quee to be returned to the State for re-development. The lifting of height constraints to buildings in the immediate vicinity of Amoy Quee would also unlock development potential of the surrounding area. Overall, this would result in huge benefits to the nation.

The US Army deployed I-Hawk in a standard "battalion" configuration. Studies of other users worldwide revealed that the deployment area for the "battalion" configuration was large and Sweden had found a way to reduce deployment requirements and increase the mobility of the fire unit. The Swedes had developed a new radar based on the Giraffe radar, the Super Giraffe, and had integrated it with the high power illuminator of the I-Hawk and two sets of missile launchers. This was the ideal configuration for Singapore as it would be very mobile, quick to deploy and camouflage, and required a very small footprint.

The US Army Missile Command (MICOM) did not support the integration of I-Hawk with Super Giraffe. Their position was that the MICOM would only sell complete fire units. The smallest fire unit of the US Army was the Improved Assault Fire Unit (IAFU). The solution to meet the demands of MICOM and our operational requirement was the procurement of three IAFUs, the minimum order quantity, and five sets of equipment to be integrated with Super Giraffe radars, which MICOM termed the Modified Improved Assault Fire Unit (MIAFU).

I-Hawk was the most costly system acquired for SADA. The Foreign Military Sales (FMS) case for its purchase was signed in February 1980. Eight Super Giraffe radars complemented the I-Hawk system. The US Army and MICOM were very resistant to any configuration changes and dissuaded us from doing so. Their constant refrain was: "If anything goes wrong, it's your responsibility". In addition to introducing the Super Giraffes, we made several other configuration changes that resulted in better performance and used more modern equipment than those offered by the US Army. This resulted in considerable savings and significantly lower life cycle costs. Two examples are described here.

The power source for I-Hawk was the MEP-115, a venerable 60kW, 400Hz diesel generator. It was antiquated and expensive. The MEP-115 was the US Army standard diesel generator of which thousands had been produced. Hence, they were deliverable items in our FMS case. More importantly, the MEP-115 was inadequate for the planned product improvements (PIP-2) that our I-Hawk system would come with. It did not have the reserve power capacity and was not responsive enough for the PIP-2 upgrades. These upgrades demanded more power from the diesel generator, as new equipment was added to the fire unit, and the launchers were made to slew more rapidly for simultaneous and multiple target engagements. The increased surge power demand caused the generators to "trip", which in turn caused the computers in the control post to fail at the most critical phase of a target engagement. On the other hand, the US Army did not have any plans to replace the MEP-115 in the near future. Thus, we decided to design and build new diesel generators to our own specifications.

From Raytheon we learned that a small company had made a proposal to the US Army for replacement of the MEP-115, but approval for this would take years due to the staffing process of the US Army. The company was called Vallely Power and was owned by James ("Jim") Vallely – a very practical and experienced specialist in customising power generators for demanding environments. He briefed us on his proposal to the US Army.

His design utilised current state-of-the-art engines and alternators, and accurate and fast responding electronic "governors" compared to the old mechanical governors of the MEP-115. The only shortcoming, in our opinion, was that the power capacity of this new design just matched the requirements of the PIP-2 upgrade. We suggested adding a more powerful diesel engine and a much larger alternator. Jim Vallely agreed and we tested a prototype of the Singapore diesel generator, which worked very well. We used our own diesel generators for the first firing of our I-Hawk system at the White Sands missile test range in New Mexico. The firing took place on 15th September 1982 and was a success. The Singapore diesel generators are still in service with the RSAF. Only two have been replaced after more than 30 years of reliable service.

The AN/TPQ-29, the I-Hawk training simulator, was also a deliverable item in our FMS case. It was a transportable system that would be shipped together with an I-Hawk system that was deployed overseas. It used old vacuum tube technology and was powered by the 60kW, 400Hz MEP-115 diesel generator. In turn, this necessitated the use of 400Hz "mobile" air-conditioning units. Very compact, maintenance intensive, mil-spec 115VAC, 400Hz air-conditioning units were part of the system. In all, the AN/TPQ-29 was an expensive and antiquated simulator with equally expensive and antiquated power supplies and air-conditioning systems. However, it was needed for training I-Hawk SAM controllers locally.

170 Squadron operated and had much experience with its Bloodhound Engagement Controller Simulator, which was introduced in 1971 and retired in 1990. It was, likewise, designed and produced from the era of vacuum tube equipment. The main reason for its high failure rate and general unreliability was the large amount of heat generated from the vacuum tubes.

We did not need the AN/TPQ-29 to be transportable as it would serve as a static simulator in the I-Hawk unit. Normal mains power was thus used for the AN/TPQ-29. Instead of using mil-spec 115VAC, 400Hz air-conditioning units, we over-cooled the AN/TPQ-29 with commercial and inexpensive Toshiba air-conditioners. The Commanding Officer of the I-Hawk unit reported that the AN/TPQ-29 was heavily used and that its serviceability and availability was always high. The AN/TPQ-29 was delivered to Singapore towards the end of 1982 and retired from service use in 2004.

An I-HAWK MIAFU deployed in Sweden

The lesson learned from our experience with the Bloodhound simulator is that electronics equipment, especially analogue vacuum tube systems, should be cooled to as low a temperature as practically possible. So while we over-cooled the AN/TPQ-29 – the vacuum tubes were very happy, the reliability of the simulator was very high – the trainees felt they were in Siberia!

A funny situation arose during a project meeting: Mr Bo Johannsen and Mr Kent Drefeldt of Ericsson Microwave Systems joined us for a project meeting with the US Army, MICOM, Raytheon and others at MICOM in Huntsville Alabama. Mr Bo Johannsen was our Super Giraffe MIAFU project manager and Mr Kent Drefeldt was in charge of our Basic and Super Giraffe radars.

A US Army major gave the first briefing. In typical US Army style he stood erect and stiff in front of us, hands clasped behind his back and he delivered his presentation very formally and in staccato from his slides. When he came to the MIAFU, he said "…. the Singaporeans have decided to adopt both the IAFU and MIAFU; IAFU stands for "Improved Assault Fire Unit" and the US has termed the MIAFU the "Mini-Improved Assault Fire Unit".

Unlike Mr Bo Johannsen who was large and spoke loudly, Mr Kent Drefeldt was a slightly built and generally soft-spoken man. He put up his hand and said: "Excuse me, but in Sweden we call the MIAFU the "Much Improved Assault Fire Unit". The silence in the room was so thick you could have cut it with a knife!

E-2C Airborne Early Warning (AEW) Aircraft – Changing the Rules of the Game for Island Air Defence

Introduction

In the book "Up close with Lee Kuan Yew: Insights from colleagues and friends", Mr Philip Yeo recalls the following incidents that took place when he was Second Permanent Secretary of MINDEF. The following is an extract from pages 94-95:

"… in February 1979, Dr Goh Keng Swee asked me to take charge of Air Defence build-up portfolio … Sometime later, he called me to his office for our usual ten-minute catch-up. He asked me how my SADA (Singapore Air Defence Artillery) build-up was going. I replied that we needed Airborne Early Warning capabilities to complete the air defence build-up. He knew what equipment was needed and asked how many I wanted. I replied, three. He countered, "Two is enough."

The next day, I was called to attend an unscheduled Defence Committee meeting at the Istana with Prime Minister Lee. Minister for Defence Goh Chok Tong and Second Minister for Defence Yeo Ning Hong were present. Dr Goh said, "Philip says we need this [E-2C Hawkeye airborne early warning aircraft]." Mr Lee asked what the next step was. I replied that I would be going to the Pentagon. The meeting lasted less than two minutes. No memo was needed.

In Washington, I met up with John Lehman, Secretary of the US Navy. The US Department of Defense Letter of Offer and Acceptance to Singapore was US$601 million for four Hawkeye E-2Cs and a basic integrated Logistics System package. Our project staff completed the overall programme for US$340 million …"

As E-2C was considered to be a strategic system by the US, it took more than three years of staffing before the Letter of Offer and Acceptance (LOA) would be sent to Singapore.

The disruptive innovation the E-2C brought about was the breaking of the constraint of "line-of-sight" to our air defence system. The disruptive change was created when we could position the E-2C and detect adversarial fighters at a significantly further range that our ground-based radars could and consequently also intercept them at extended ranges from Singapore using our fighter aircraft. With surface radars we could detect incoming fighters flying at 150 feet to approximately 10km from their targets. Fighter interceptors and medium level SAM would be useless against such threats. Hence, our 1978 Air Defence Plan was based on Giraffe radars, 35mm anti-aircraft artillery and the RBS-70, Rapier and the I-Hawk SAM systems. With E-2C, the new air defence plan was changed to be based on fighters complemented by SAMs.

In May 1982 during the Falklands War, Dr Goh Keng Swee, then Minister for Education, observed that the Royal Navy was lucky that the bombs delivered by Argentinian A-4 Skyhawks that had struck their ships did not explode. He observed that the lack of AEW nearly caused the UK to lose the war and concluded that E-2C would be critical for the air defence of Singapore. Though the cost would be very high he stated that: "It is still cheaper than one oil refinery".

An AEW radar was not part of the consideration in the original design of Singapore's air defence system. We had never even dreamed of it. Immediately, we researched all that we could gather and learn about the E-2C from our library – there was no Internet or Wikipedia then. Once we knew and understood what operational capability and advantage the E-2C would bring to the air defence of Singapore, we thought we had "died and gone to Heaven".

Grumman Corporation, the designer and manufacturer of the E-2C system, was quick to respond. In early 1982, it set up a regional office in Singapore and relocated the vice-president of their Tokyo office, Mr Herb Moska, to Singapore.

In November 1982 a team of 11 senior staff from the RSAF, DSO and SPO was despatched to the Grumman plant in Bethpage, New York to learn about the E-2C. The course lasted for five weeks and ended just before Christmas.

A US Navy (USN) and Grumman team arrived in Singapore in January 1983 to work out the terms of reference for a logistics planning conference (LPC) that was scheduled for April 1983. US Congressional approval for the sale of E-2C to Singapore was obtained on 17th May 1983 at a ceiling price of US$601m. The LOAs for four E-2Cs and support were presented by the USN at the end of July 1983. Detailed clarifications were held with USN officials in August and September 1983 to review the scope and essential items with respect to our requirements. The LOAs were signed on 30th September 1983.

The E-2C Project 1982-1987

The vulnerability of Singapore to aerial assault was a big problem, due to the lack of strategic depth to provide sufficient warning time of threats to the entire country – "our front door is our back door!". If we were to allow enemy aircraft into our airspace, anywhere in Singapore would be bombed within seconds. An increase in our warning time is crucial if we are not to be caught by surprise. Hence, the E-2C.

The E-2C is the USN's airborne surveillance, and command and control (C2) aircraft designed and built to operate off an aircraft carrier to support a naval task force. A fleet of four E-2Cs was estimated to cost more than S$1 billion in 1982. The other US alternative then was the US Air Force Airborne Warning and Control System E-3 Sentry which was even more costly. There was also the Nimrod proposed by the British. Fortunately, we did not consider it as that project encountered many technical and insurmountable difficulties and was eventually cancelled. We would not have considered the Russian Bison.

For comparison, the most sophisticated aircraft operated by the RSAF then was the F-5; and the Mass Rapid Transit (MRT) system had just been approved at an estimated cost of S$5 billion. Compared to the MRT, a brand new concept of transportation eagerly awaited by the entire population of Singapore, the thought of spending S$1 billion for a mere four aircraft was quite daunting. As expected, the Singapore Government was engaged in a good amount of debate with opposition members questioning the need for this large expenditure. The press reported on the debate and Singaporeans got to know about the E-2C. However, the E-2C was an essential component in Singapore's defence strategy and had to be bought.

The responsibility for managing this huge programme was handed to MAJ Wesley D'aranjo who was appointed the Programme Director. MAJ Wesley D'aranjo remembers clearly the briefing he received one Saturday morning from his boss, SPD Lui: "I think you know by now that we've decided to buy the E-2C and I want you to be in-charge". (And, yes, we worked Saturdays then.) When MAJ Wesley D'aranjo reminded SPD Lui that his contract would end soon, as his scholarship bond expired in July 1983, SPD Lui said: "Please tell that to DS (Air Force)". Lim Ming Seong was the DS (Air Force) then. He listened, said "not acceptable", and the rest is history.

Intense negotiations between USN-Grumman and MINDEF preceded the signing of the LOA. As we now understood the E-2C better, having just completed an extensive logistics planning exercise on it, we wanted several software changes to better suit the RSAF's operational requirements; alternatives for support and logistics implementation; as well as better terms and industrial offsets from Grumman. The protracted delay caused the Pentagon concern as approval for the release of E-2C to Singapore was given by President Ronald Reagan himself. Mr Jim White, an Under Secretary at the Pentagon, travelled to Singapore in mid September 1983 to meet with SPD Lui and MAJ Wesley D'aranjo. After the pleasantries, he gingerly asked if the LOA would be signed as it would expire on 30th September 1983. Mr Jim White was left speechless when SPD Lui instructed MAJ Wesley D'aranjo to draft and type, on the spot, a letter confirming the purchase of the E-2C with support, which SPD Lui signed and handed to him. The LOAs were signed on 30th September 1983.

Two project teams under the direction of MAJ Wesley D'aranjo were established: one at the Grumman plant in Bethpage, New York headed by Mr Chinniah Manohara, and the other in Singapore headed by CPT John Wong. There was much travel between Singapore and New York. As a result, quite a few people developed a distaste for travel due to the distances involved and the discomfort of flying economy class in those days.

The first project meeting with USN Naval Air Systems Command (NAVAIR), the USN E-2C project management office, was held in Bethpage in December 1983. COL Lui Pao Chuen, SPD, spoke on behalf of the Republic of Singapore and voiced his concerns in the management of the programme. His introductory speech (see page 28) is worth recounting.

Managing the project involved a great amount of detailed work; this being the nature of large-scale systems integration work and logistics. Our aim was to build an infrastructure that would enable the squadron to maintain its intended operational readiness throughout the life of the aircraft. Hence, not only did the hardware and logistics need to be purchased and installed on time, the equally important tasks of training adequate numbers of operators, engineers, technical officers and technicians on a continual basis had to be planned for and implemented. When the first aircraft arrived in Singapore in 1987, the project team had prepared the logistics and operational infrastructure such that flying could begin immediately, and it did! This is a testament to the sound groundwork laid more than 30 years before – and which continues to this day by the present generation of AEW operators and maintainers. While other countries sometimes rely on foreign help even after many years, Singapore set a target to be self-reliant within two years.

As a legacy of the E-2C, the management of such large and complex projects was never the same again from the project management perspective. Our ability to integrate complex systems, thereby producing a very effective SoS, was put to the test and we succeeded.

The E-2C Programme Spawned Several "Firsts"

It was the first SAF programme estimated at a billion Singapore dollars.

It had the first full-time Government of Singapore Programme Office (GOSPO) established overseas:

- Apart from the aircraft programme, GOSPO also took responsibility for the spares management and housing / accommodation for trainees, which at one point built up to about 140 such personnel in the US. To the best knowledge of the Programme Director, MAJ Wesley D'aranjo, this had not been done before on such a scale, nor has the range and span of responsibilities been assigned to a single project office for subsequent programmes or projects.
- Much of the work done at the GOSPO was duplicated by Grumman for another FMS programme that was running concurrently. Even our requirements for aircrew flying suits, which we compiled based on the physical profile of our trainees, were accepted by the Egyptians. This was because the Egyptian pilots found that the suits issued by Grumman obviously did not fit, as the USN pilots were of much bigger build.

The E-2C squadron was the first to incorporate maintenance of hardware and software within the squadron. Much confidence was gained from this project in our own ability to maintain, repair and modify high technology equipment. This mentality is still ingrained in the SAF today.

The USN is a professional and focused organisation. Once they agree to do something, they do so without a fuss. Our first aircraft was handed over in March 1986 during a six-monthly programme review at Grumman.

A Project Management Review meeting at Grumman – inspecting the fabrication of a fuselage section

Handover of Singapore's first E-2C in January 1986 by Mr George Skurla, President of Grumman, to COL Lui Pao Chuen

COL Lui Pao Chuen delivering his speech during the handover ceremony

COL Lui Pao Chuen (left) and BG George Yeo, then Chief of Staff (Air Staff) and concurrently Director of Joint Operations and Planning Directorate, taking a commemorative photo with the E-2Cs

What Was Learned?

In dealing with the USN, we had to learn a new set of vocabulary: FMSGEL, NAVAIR, ASO, NAVILCO, ILSMT, CINCPACFLT, FCDSSA, GOSPO, NAVSUP, TLDP, COMNAVAIRPAC, NAVFAC, SPAWARSYSCEN .... The list of "NAVSpeak" is even longer.

We learned a systematic way of managing projects. This was the first time we managed a project in such an integrated way; in what is today called "Ops-Tech" integration. The skeleton crew of the squadron was formed and both operators and logistics personnel were involved in the planning of the project, including the physical requirements of the squadron. The senior squadron officers in the initial batch were the same officers managing the local office of the project, thus ensuring that they were the ones who had to live with the decisions they made. Upon returning from Grumman, most of the GOSPO staff were assigned to the squadron or took up appointments in Air Logistics Department responsible for the E-2C.

The USN initiated each E-2C FMS project with a massive LPC. During the LPC, each and every main and subsystem – hardware and software – and sometimes up to the individual component of the aircraft system was examined from the perspective of mission needs. The operational, logistical and other local support needed to fulfil the mission was derived and documented thoroughly in an implementation plan called the Technical and Logistics Development Plan. This was very logical and commendable. However, a major mismatch in expectations arose soon after the start of the LPC. NAVAIR 231, the USN E-2C project management office, had limited experience dealing with FMS customers and, understandably, assumed that what was good for the USN was applicable for others as well. Many who came for the LPC were from USN fleet squadrons or bases and were only schooled in the USN way of doing things. To make matters worse, the LPC for Japan had been "successfully" completed recently and it was taken as an additional reference. For example, the Japanese required extensive local manufacturing capability, which we did not. They also wanted a complete radar test range for testing rotodomes (the rotating antenna of the E-2C radar); and the eight Japanese E-2Cs would be deployed at more than one operating base across Japan. To the USN, it seemed obvious that Singapore's requirements had to be similar to those of the Japanese.

The Singapore team assigned for the LPC spent considerable time first learning how the USN did things, then aligning expectations and finally examining and outlining alternative cost-effective approaches to local and relevant industial support needs. The support required for the E-2C – spares, ground support equipment, a software development facility and training – was specified and decisions taken whether to buy them through the USN or directly from their manufacturers. This saved us an enormous amount of money. In all, teams from the RSAF, DSO, Singapore Aerospace, other local companies and SPO spent five weeks cooped up in a local hotel working with 40 USN, Grumman and subcontractor personnel during the LPC. The USN estimated the LPC to last 13 weeks.

The approach to logistics management learned during the LPC evolved into a value-added robust process for MINDEF, which the SAF described as the "LCM" of projects. All subsequent projects adopted this methodology and, in June 1990, it was formally accepted and documented as the MINDEF LCM Manual, which clearly defined the Integrated Logistics Support requirements for project systems. This was further codified into the Logistics Management Information System (LMIS) and implemented using the German software, Systemanalyse und Programmentwicklung (SAP) R/3, which up till today is probably the best industrial Enterprise Resource Planning logistics software tool available commercially. The LCM methodology ensures that all aspects of the system life cycle are considered in arriving at relevant and cost-effective solutions. It can be said with some degree of confidence that MINDEF and the SAF are now able to get the best value for its money when acquiring weapon systems. In 2012, the LCM Manual was replaced by the Defence Capability Management (DCM) Manual to take into account the increased sophistication of systems being acquired or developed, and the need for more Operations-Logistics coordination and integration taking a capability perspective. Correspondingly, the Enterprise Systems for Logistics replaced the LMIS, and it continues to be implemented in SAP, albeit an updated version ECC6 Enhancement Pack 4.

Interoperability

The USN, and in general the US Armed Forces, interoperate via classified datalinks. The main datalinks used by the USN then were Link 11 and Link 4/4A, the former for linking C2 centres and the latter for the E-2C to "talk" to fighter aircraft. These datalinks encapsulate decades of thought, war fighting experience and lessons learned by the USN. A "Book of Standards" defines and disciplines every protocol aspect of each datalink – terminology, convention, metrics, data packages, transmission rates, track quality, error correction schemes, "red / black" separation, encryption, change management and more.

As Singapore is neither a member of the North Atlantic Treaty Organization nor an ally of the US, the LOA included a provision for Grumman to develop a unique datalink for Singapore called Link ∑. This would cost at least US$26m but the operational requirements had to be specified by the RSAF. The requirement specifications were defined by the RSAF and DSO. An innovation and specific requirement was a novel priority scheme to ensure that the most important messages get priority of bandwidth. However, a large amount of flight testing would be required to qualify Link ∑ and there was no guarantee it would work. In addition, for Link ∑ to be interoperable with our C2 system, the interface would have to be via a Ground Entry Station (GES), and the GES would cost another US$26m.

This matter was of great concern as the SAF did not have the interoperability the USN assumed existed. We had not yet achieved interoperability within a service, let alone among the three services of the SAF.

One may be surprised at what we did next.

During the meeting with Mr Jim White, we took a chance and explained the dilemma and risk that Link ∑ posed to us. We asked if Link 11 could be released to us. We were surprised when Mr Jim White said he would staff our request through USN and the Pentagon. It was our turn to be speechless when we were granted release not only of Link 11 but also of Link 4/4A, i.e. the USN's own configuration! This removed a big worry from our minds and saved at least US$26m. Often we are afraid to ask because we are afraid of negative answers. The learning point here was to ask sincerely, or innocently, in order to get the answer you wanted. However, what could we do about the GES?

The GES proposed by the USN and Grumman was an actual "backend" of the E-2C – the three control workstations, a slightly antiquated central computer and other associated hardware. This was the standard solution proposed and implemented then. Imagine, a full airborne mil-spec "backend" of the E-2C sitting on the ground in an air-conditioned room and relaying data to and from our C2 system! This did not sit well with us. By then, we had moved away from the use of proprietary "mainframe" computers and had already introduced commercially available standard information technology (IT) processors connected by local area networks and performing distributed processing. We demurred and decided to study the matter in more detail. We discovered that several companies could provide a "backend" using standard IT hardware but very few had experience in implementing "interoperability" or working with classified US Government datalinks.

In mid 1984, we issued a request for proposal to two companies, Grumman and Rockwell-Collins, for the development of a GES to interface the E-2C to our C2 system. Both companies were asked to propose modern IT hardware and software solutions. Grumman's non-recurring development costs were very high and we continued with Rockwell-Collins.

The Rockwell-Collins group developing interoperability solutions was based in Rodgau near Frankfurt and headed by Mr Dave Adams, a retired colonel from the US Marine Corps. Mr Dave Adams was a graduate of the US Naval Postgraduate School in Monterey, and was well regarded in the US military and industry for his expertise in US and North Atlantic Treaty Organisation datalinks and C2 systems. Mr Dave Adams had strong opinions on many things but he delivered as promised.

The E-2C GES was developed and delivered by Mr Dave Adams and his team at a fraction of the price of the Grumman GES. Development of the E-2C GES took place from mid 1986 and it was commissioned in early 1989. Software staff from DSO, led by Mr William Lau, participated in the development of GES.

E-2C flying along the coastline of Long Island, USA

Fokker 50 Maritime Patrol Aircraft

Missile Corvette

Systems enabled with C2 interoperability training

This was a valuable learning experience for our work on various types of datalinks in later years.

The implementation of the E-2C GES enabled and spawned the following capabilities:

- Enhanced effectiveness to our weapon systems via improved target acquisition provided by E-2C
- Modernisation to Link 11 communications system
- Advanced standalone and embedded simulators for C2 interoperability training between the E-2C, MPA and RSN ships

In 1991, Mr Dave Adams and three of his senior system developers left Rockwell-Collins and formed their own company called Interoperability Systems International Hellas, which eventually moved to Athens, Greece and is still in existence today.

Financial Control

The GOSPO, though small, had oversight over all matters relating to our programme and they scrutinised all expenditures and verified them to be necessary before agreeing.

Understandably, the first and main preoccupation of NAVAIR 231 was the USN fleet. NAVAIR 231, who also handled our project under the FMS arrangement, was always short-handed and, as a practical approach, could spend our funds to employ subcontractors to work on various aspects of our programme. These subcontractors were called "Beltway Bandits" and they made their living by performing work outsourced from the USN. The offices of many such companies lined the "beltway" (a ring road) that surrounds the Pentagon; hence the name "Beltway Bandits". Where we could, we would not agree to the use of "Beltway Bandits" and, where possible, we did most of the work ourselves. An example was the provisioning of spares for the various systems and subsystems of the E-2C, which the USN wanted "Beltway Bandits" to do. Instead, we asked the Aviation Supply Office (ASO) in Philadelphia to generate the listing of spares with their reliability data based on USN usage data. We then worked out the provisioning list based on our experience and flying profiles.

Deciding on the quantity of spares was an intimidating challenge because of the high costs involved. Relying on the spares list given by the USN would have cost many tens of millions of dollars more. Everything seemed inflated, probably due to the relatively smaller number of E-2Cs compared to other aircraft types. So, without the benefit of operational experience on the E-2C, and relying on the reliability data provided by ASO, we had to decide which spares to buy, item by item. We could have played it safe and purchased what the USN recommended. Instead, we took a calculated risk by using a yet untested (by us) software programme on spares provisioning called Optimisation of Units as Spares (OPUS); we asked relevant questions of various knowledgeable USN personnel, and then made our own judgments. OPUS is a software provisioning tool to determine the spares holding necessary to achieve a desired operational availability. This became a standard tool for calculating and provisioning our spares in future projects. We sometimes wondered if anyone would thank us for saving tens of millions of dollars if a plane was grounded for want of a spare!

Being at Grumman enabled the team and the RSAF to learn a lot about the evolution and development of the E-2C, and the forthcoming modifications and upgrades planned. In fact, we received the latest multi-function display consoles ahead of the USN as we signed up for the modification in time for it to be incorporated into our aircraft during production. This saved a lot of money as a retrofit would have been more costly.

A line item in the LOA was for a "staging area" in New York to receive, store and dispatch to Singapore the multitude of spares and materials purchased for the E-2C squadron. As we would have to manage the logistics of the E-2C ourselves eventually, we informed the USN that we wanted to handle this task by ourselves. Singapore Aerospace (SAMCO) was approached and asked if they would take up the challenge of doing this. SAMCO established the "SAMCO Warehouse" close to Bethpage at less than half the cost estimated by the USN.

Onto Singapore

After the "roll-out" of our first two E-2Cs at Grumman, they were used for pilot and "wizzo" (weapon systems operator) training. Upon completion of the flying training, the aircraft were flown to San Diego from the Grumman plant in Bethpage, preserved for sea transportation across the Pacific Ocean and shipped to the USN naval base at Subic Bay. The sea journey took about three weeks. After off-loading at Subic Bay the E-2Cs were stripped of their preservation, made operational again and then flown to Brunei. RSAF pilots flew our E-2Cs from Brunei to a memorable welcome at Paya Lebar Air Base in March 1987.

"Draw-Down" and Renewal

The E-2Cs were decommissioned after 25 years of sterling service to Singapore and the SAF.

The "draw-down" ceremony was held on 15th October 2010 at the Air Force Museum in Paya Lebar Air Base with Chief of Air Force (CAF), MG Ng Chee Meng, as the guest-of-honour. The ceremony was dignified and comprised a formation flypast with CAF on board the E-2C. There was also a symbolic handover of the E-2C yoke to Commander Air Force Training Command, a photo taking session, a video tribute and unveiling of the E-2C "draw-down" plaque, and the presentation of mementoes.

Arrival of our first two E-2Cs at Paya Lebar Airbase in March 1987

The E-2C was replaced by the Gulfstream G550 AEW system.

We are now into the fourth decade of AEW operations in Singapore, and as we take stock of what the E-2C has gained for Singapore, MINDEF and the SAF, it can be argued that we have reaped more than enough benefits to justify its costs, if such benefits can be priced. Singapore's AEW squadron must continue to aim for and be "The best AEW squadron in the world".

G550 AEW flying alongside E-2C as part of the E-2C decommissioning event

Then-CAF MG Ng Chee Meng (centre) with founding members of the E-2C project team

COL Lui's Introductory Speech at the First E-2C Project Meeting with USN NAVAIR in December 1983

Then COL Lui Pao Chuen, SPD, spoke on behalf of the Republic of Singapore. His speech, which voiced his concerns in the management of this programme, was as follows:

Mr Chairman, Ladies and Gentlemen,

As most of you will now have discovered, Singapore is a very small country. We have no natural resources. Even the water we drink has to be imported from Malaysia.

To survive and prosper as a nation we have to work very hard and be as efficient as we can. We have learned the habit of thrift and spending within our means. We have had a surplus budget every year since we gained our independence in 1965.

We, however, do not save on defence. Each year we spend 6% of our Gross National Product on defence. It is the responsibility of our Ministry of Defence to ensure we get the maximum defence capability for this investment.

The E-2C is a very large investment when compared to the Gross National Product of Singapore. Money spent on the E-2C will have to be taken from the budget of other weapon systems. To get the most "bang for the buck", we must cut down expenditures that do not result in tangible returns. In short, we must trim project overhead costs.

Being a small and relatively young country, we are fortunate to have a small bureaucracy. We can therefore be very fast in decision making and we can complete our actions rather quickly, provided we get the facts and figures.

As we have built up a credible defence capability in a relatively short time, we have to work in a "pressure cooker" environment. We have become intolerant of waste, especially of valuable time. Please bear with us should you find us to be more "pushy" than other more established FMS countries. We pay cash, and on time.

As we have spent considerable time during the Logistics Planning Conference, being briefed and talking to each other, let us not cover subjects that have been covered there and adequately documented. We should get down to issues that will affect the project. We are ready to respond to any matters that any participant in this conference would like to raise and we will work as long as necessary to give a response before we end this conference. I hope that the issues we raised with PMA-231 will be similarly dealt with so that we can both feel satisfied that the conference is worth the effort of attending.

Thank you.

The Island Air Defence's Transformation into a System-of-Systems in the 2000s

The Third Generation SAF in the 2000s

We have seen three key categories of IAD systems that were progressively acquired and modernised from the 1960s to 1990s:

- *Sensor systems*, e.g. ITT-RS320 radar, Super Giraffe, E-2C airborne radar, etc
- *Weapon systems*, e.g. Bloodhound, I-HAWK, Rapier, RBS-70, fighter jets, etc
- *C2 systems*, e.g. GL-161, MOCC, newer in-flight C2 systems, etc

Through a journey of some 30 years, our DTC pioneers and predecessors grew in proficiency and mastery of these systems through "learning by doing". By the 1990s, we had a suite of capable sensor, C2 and weapon systems that were able to detect, sense-make and deal with a range of air defence threats.

Moving into the 2000s, DTC embarked on a journey to develop IAD into an SoS. Defence capabilities being developed were increasing in scale and complexity compared to the individual systems for sensors, weapons and C2 that DTC had managed so far. The continual advancement of communications, computing and information technologies in the new millennium was offering new opportunities for systems to be networked together and to interoperate. Concepts of Network-Centric Warfare (NCW) were being explored or pursued by countries such as the US. It was at this time that the SAF embarked on a journey to transform itself into a Third Generation capability.

"The transformation of the SAF to exploit rapidly emerging technologies and concepts is a strategic imperative for the 3G SAF. These will lead to changes in organisation, less demand for conventional platforms, more demand for less visible technologies like information systems, precision weapons, electronic warfare systems, unmanned platform technologies, and a new type of soldier who is trained to exploit these capabilities."

Minister for Defence Teo Chee Hean, March 2004 Announcement in Parliament of the Third Generation SAF

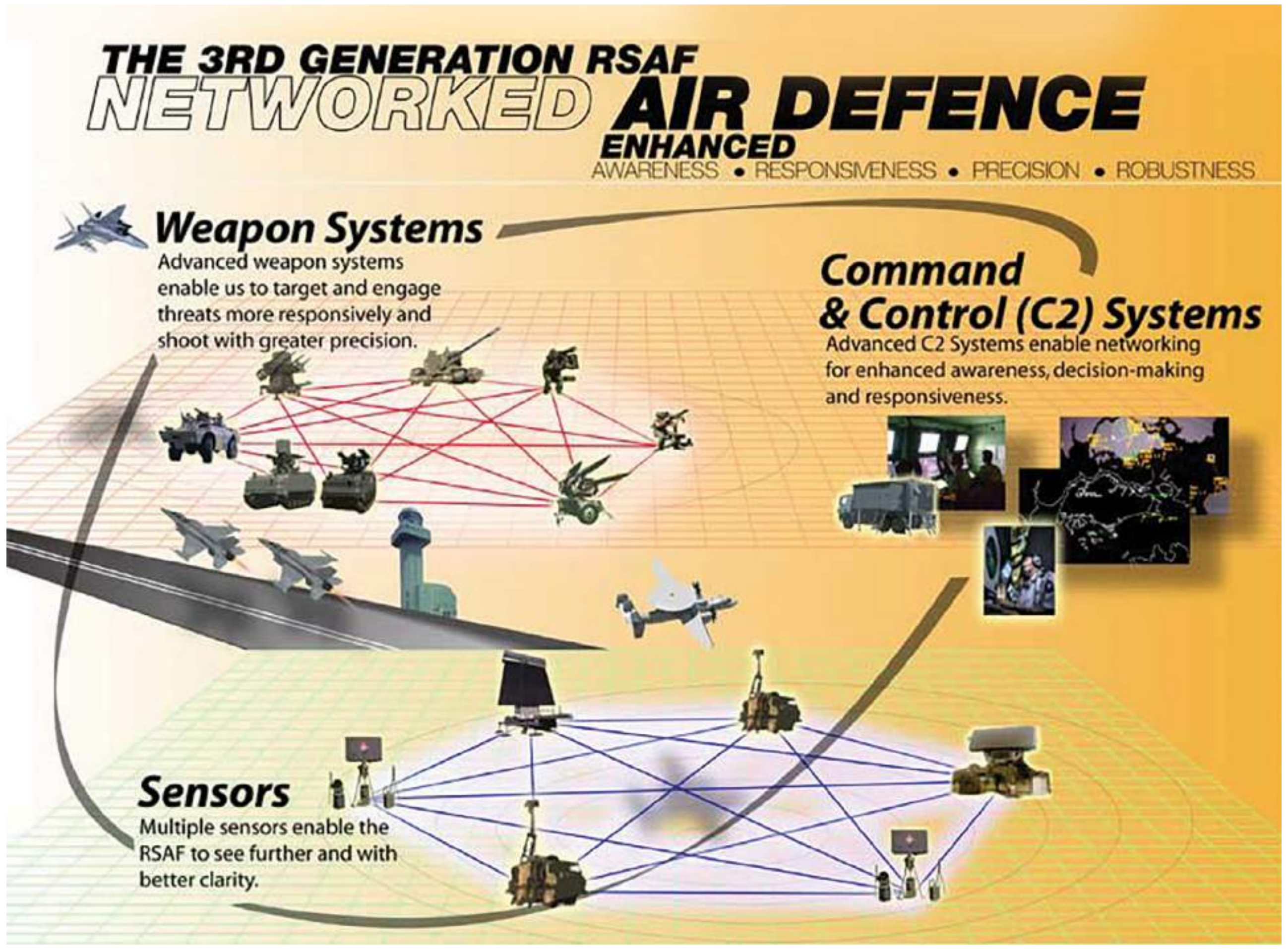
Island Air Defence as a System-of-Systems in the 2000s

The Third Generation Networked IAD was unveiled publicly in 2007. The Networked Air Defence system enhances the existing multi-layered air defence with the application of networked concepts to tightly integrate existing and new sensors, C2 and weapon systems for enhanced awareness, responsiveness and precision. There are three notable qualities in enhancing our IAD from a collection of systems to an SoS.

First, it is more robust and survivable. The networking of the various sensor, C2 and weapon systems together prevents a single point of failure, thereby enhancing the robustness and survivability of the overall air defence system. With networking, the degradation of any single sensor, C2 and/or weapon system will have minimal impact on the entire system as there are several other sensors, C2 and/or weapon systems that will continue to function.

Second, it is more responsive and effective in defeating aerial threats. The IAD SoS has enhanced awareness and responsiveness to see farther, respond faster and engage targets with greater precision. The Networked Air Defence system effectively reduces the sensor-to-shooter cycle between the time a target is detected and the time it is engaged. In addition to responsiveness, networking also provides greater strike effectiveness. In the past, a weapon system or shooter relied on its own sensor to detect and track targets. Today, however, the shooters and sensors are connected. Tracking data from a particular sensor, such as the FPS 117 or Giraffe Agile Multiple Beam Radar, can be relayed to the shooter most suitable to eliminate a particular threat. The whole idea is to command these weapon systems centrally on the network. It is now possible to select the best shooter, using the best tracking radars, to intercept any incoming targets more efficiently and effectively.

Third, it has the flexibility and ease for growth. The IAD system integrates existing and newly operationalised capabilities, while allowing for easy plug-and-play of future capabilities in the network. Underpinning these networked capabilities in our IAD is an SoS architecture that has the flexibility to allow subsequent insertions of the latest sensor systems and weapon systems to interoperate in a network-centric manner. This is to ensure that our IAD capabilities would maintain a cutting edge. As a result, after 2007, new sensor and weapon systems, such as the G550 AEW Aircraft, Surface-to-air PYthon and DERby (SPYDER) SAM system and the Aster 30 SAM system, could be successfully inserted into our networked IAD.


THE 3RD GENERATION RSAF
NETWORKED AIR DEFENCE
ENHANCED
AWARENESS • RESPONSIVENESS • PRECISION • ROBUSTNESS
Weapon Systems
Advanced weapon systems enable us to target and engage threats more responsively and shoot with greater precision.
Command & Control (C2) Systems
Advanced C2 Systems enable networking for enhanced awareness, decision-making and responsiveness.
Sensors
Multiple sensors enable the RSAF to see further and with better clarity.

Networked Island Air Defence unveiled in 2007

References:

Kuok, R., Yong, P. H., Othman, W., Puan, N. A., Nathan, S. R., Pillay, J. Y., … Lim, T. K. (2015). *Up close with Lee Kuan Yew: Insights from colleagues and friends.* Singapore: Marshall Cavendish.

Chapter Two

CONCEPTS TO CAPABILITIES

A Historical View of Concept Formulation for Island Air Defence

We saw in Chapter 1 how careful analysis of mission requirements and the use of Operations Research studies to support urgent acquisition decisions for a single component system in IAD was carried out, such as rationalising the rate of fire as a critical parameter for our anti-aircraft guns and selecting the Oerlikon 35mm twin-barrel gun system over the Bofors 40mm single barrel gun. In this chapter, we will take a complementary perspective of how concepts and capabilities for the overall IAD were shaped over time. We will also see some of the corresponding qualities within the DTC as an Enabling SoS that would allow it to support the SAF in requirements definition for complex systems, so as to evolve and realise large-scale complex defence systems, such as the network-centric IAD SoS.

Rapid Build-Up of Basic Systems for IAD in the 1960s – 1970s

Following Singapore's independence from Malaya in 1965, our defence build-up, in particular air defence capability, was determined to a large extent by the abrupt announcement in 1968 that the British Forces would be withdrawn by 1971. Over this early period of building up a credible air defence system, our pioneers from MINDEF and the Defence Technology Group (DTG) worked against the odds and came up with an impressive record.

By the early 1970s, we had set up a basic air defence capability based on new purchases and inherited systems from the RAF stationed in Singapore. We had two Marconi Surveillance radars (one main S316L/S and one backup S319L), two Plessey HF 200 height finding radars and an advanced GL161 C2 system from the RAF located in Bukit Gombak under the command of the Bukit Gombak Radar Station. For weapons, we had the 35mm guns covering low-level air defence and the Bloodhound SAM system covering the High Altitude Air Defence.

Expanding a Multi-layered IAD in the 1970 – 1980s

A multi-layered IAD was beginning to take shape, and it became obvious that our IAD's initial inventory of systems would need to be augmented. In the mid 1970s, the first mobile radar AN/TPS-43DX was acquired and put into operation, followed by the second mobile radar ITT-RS320 and the Plessey Processing and Display Cabin in the early 1980s. For SAM systems, the Rapier and I-Hawk entered service in the 1980s. For fighter aircraft, first to arrive was the pre-owned Hawker Hunter in the early 1970s, followed by the pre-owned A4 Skyhawk and soon after the supersonic air defence fighter jet F-5E in 1979.

Air Defence Master Plan 1978

Even at a time when there was a critical need to meet very urgent operational needs in the early years, our defence technology pioneers demonstrated the ability to formulate requirements and acquire systems with the resources available and yet keep the big picture in mind. Amid operational demands and acquisitions of additional air defence weapons, sensors and C2 systems, MINDEF took a systems approach and embarked upon master-planning effort, rather than acquire new systems in a "piece-meal" manner and hope that they would somehow work as an integrated whole one day.

In 1978, Dr Goh Keng Swee, then Minister for Defence commissioned then LTC Lui Pao Chuen to develop the first air defence master plan. Prof Lui recalled "I felt that it had to be a joint effort [with the SAF] when Dr Goh Keng Swee tasked me to do the study". As Prof Lui had already spent three years contemplating this study, he had all the materials available. The team he put together had to put certain scenarios to war-game, and the product was the Air Defence 1978 Report. This was the first time the SAF had a dedicated study for the development of a major ORBAT in the SAF based on inputs from our own people. Before that, we always had to depend on consultants.

This was to set the stage for MINDEF and the DTC's culture of master-planning. In the air defence domain, this discipline of conducting operational and engineering master-planning continued in the late 1980s and early 1990s, led by planners from the RSAF and Systems Engineers from the DTG.

"Ops-Tech" Integration

Other than rationalising the suite of systems needed by our existing IAD, the 1978 Air Defence Study led to the formation of the SADA formation in 1979 and the Air Force Systems Command in 1983 – two organisations that later merged to form Air Defence Systems Division in 1995. This represented a holistic approach to capability development, where both new operational and technological concepts were formulated "hand-in-glove" so that the eventual new capabilities were not just "new machines", but new organisations which could exploit these new machines in a transformational manner.

This example of integrated "Ops-Tech" partnership early in the capability development life cycle sowed the seeds in developing a rigorous and systematic approach to systems acquisition by MINDEF and the DTC. It set the tone for future co-operation where comprehensive project requirement studies and mutual consultation are embedded in the evaluation, procurement and management of new systems. Into the 1980s and early 1990s, the whole project management process was continually rationalised and improved to ensure that only the most cost-effective systems were acquired to meet Singapore's needs. Collectively, DTC and SAF users earned the reputation of being "smart buyers" and "smart users" respectively in the eyes of many international defence systems contractors. Exemplary outcomes in this period included the integration of the American I-Hawk SAM system with the Swedish Super Giraffe, and likewise the RBS-70 and the 35mm guns with the Basic Giraffe to improve their capabilities.

From SAM-centric to Fighter-centric Air Defence in the 1980s

A major paradigm shift in IAD occurred following the acquisition of the E-2C airborne early warning aircraft in the 1980s. Up to that point, in spite of our best efforts to tackle low-flying aircraft threats with capable radar and weapon systems such as the tactical Giraffe low level air surveillance radar and the Rapier and RBS-70 SAM systems, ultimately ground-based air defence systems (GBAD) were still subject to the "tyranny of line of sight (LOS)". With the E-2C now as an airborne radar, the "tyranny of LOS" was broken and low-flying threat aircraft could be detected at much longer ranges. To complement the airborne radar's extended reach, the natural choice of a complementary weapon system became the air defence fighter. As a result, in terms of a multi-layered response to air intruders, the first layer now became fighters, instead of SAM systems such as I-Hawk that was limited by its 40km range and LOS. This "fighter-centric" air defence was further bolstered by the acquisition of the capable F-16 fighters in the late 1980s.

Optimisation of the Larger System of IAD

By the 1990s, with almost two decades of experience, the DTC and the SAF grew from proficiency to mastery in operating the systems in our inventory. We arrived at a stage where we could exploit the systems' capabilities to the fullest as well as overcome their limitations. Added emphasis was placed on optimising their performance as a larger system, and their related areas of systems acquisition, integration, training, organisation and more.

An example was the Sensor Master Plan that aimed to overcome shortcomings of the existing sensors by introducing advanced sensors, carefully integrated to form a coherent whole, to provide overall system-level robustness. The suite of sensors provided overlap of coverage in various dimensions, such as space and frequency, as well as radar functional modes. Each radar acquired under the Sensor Master Plan was carefully defined, adapted or specially developed to meet Singapore's unique requirements. It was a product of comprehensive Ops-Tech partnership with concerted efforts in engineering studies involving both experienced RSAF air defence planners cum operators and DSO Radar/Electronic Warfare Systems Engineers. The outcome was a master plan that when realised would provide a comprehensive recognised air situation picture around Singapore to support various missions of the RSAF. The study also included the top-level systems integration approach to be taken by MINDEF's engineering team.

Many more capability master plans were developed as such a practice became the norm in MINDEF's capability planning process. The master plan for Singapore's network-centric IAD was conceptualised in the 2000s and it signified the new generation of networked air defence capability for the SAF.

From Fighter-Centric to Network-Centric IAD in the 2000s

In the 1990s and 2000s, the primary threat to air defences around the world shifted from fighter aircraft to stand-off munitions. Examples included long-range air-to-ground missiles that enabled adversarial aircraft to attack while staying out of harm's way. This required an IAD that could respond faster, since missiles would typically fly faster than aircraft and would be harder for conventional radars to detect. The air defence's ability to defeat missile threats and robustness to withstand some extent of missile hits would also be critical. A new suite of sensor and weapon systems synergistically integrated with a responsive command, control and communications (C3) system could optimally handle stand-off munition threats.

Leveraging advancements in infocomm technologies and emerging network-centric concepts, the DTC and the RSAF developed a network-centric IAD, where the GBAD evolved from operating in firing units to operating networked "common pools" of sensor and weapon systems that could be optimally paired by the C3 system against specific threats. Moving away from the firing unit concept also meant better robustness. This was because each firing unit typically had a dedicated radar, and if the radar was defeated by a missile, the firing unit could be rendered ineffective. In a network-centric concept, another radar suitable for the mission could be selected from the "common pool" to bridge the gap.

This Third Generation networked IAD was a product of Ops-Tech partnership at the very early stage of capability development. While the RSAF was formulating the operational concept, the DTC complemented it with a systems architecture approach (also known as Systems Architecting or SA) to drive the operating concept and architecture from firing unit-based to network-centric. This was crystallised in synergistic IAD master plans from both the operational and engineering perspectives to translate concepts into SoS capabilities.

MINDEF's Long-Term Planning Process Today

In realising the Third Generation SAF, MINDEF acquires and deploys cutting-edge weapon systems and information technology so that the SAF's operations are characterised by speed, precision, knowledge and integration. The strength of the SAF is multiplied by our ability to network the various systems and capabilities, so that the overall fighting system is much more capable than the sum of the individual parts. Advanced C3 systems, enabled by information technology and networking, now allow rapid dissemination of information to give commanders and their subordinate units better awareness, and enable them to exercise better control and self-synchronisation in order to operate as a tightly integrated system.

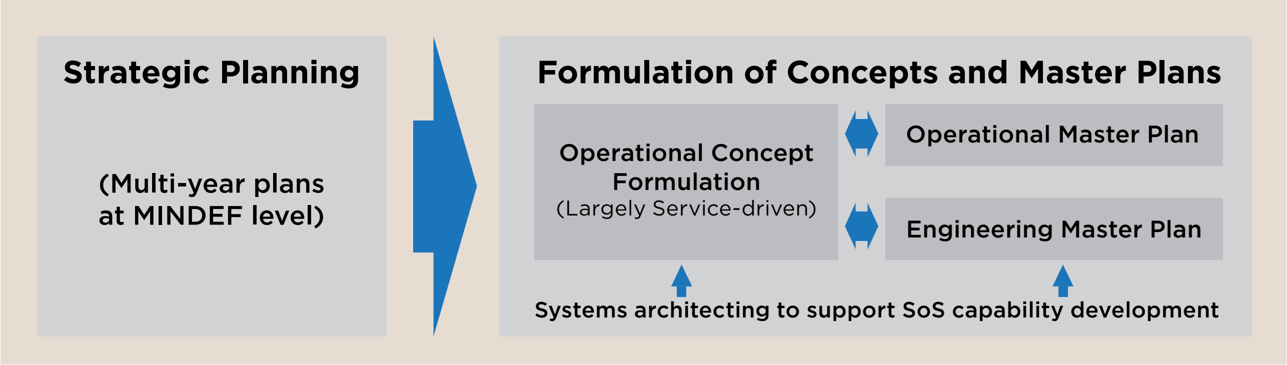
In consideration of these, the first step is to formulate the "big picture" of defence capabilities before new defence equipment are acquired. Today, MINDEF and the DTC have a codified approach to long-term planning to facilitate the formulation of new concepts in defence into Defence SoS capabilities. This includes the stages of Strategic Planning and Formulation of Concepts and Master Plans.

Strategic Planning

The Strategic Planning stage involves formulation of long-term strategic directions for the development of the SAF in response to advances in technology, the anticipated threat landscape, constraints in resources and phasing out of old systems over a planning horizon of 10 years and beyond. This process involves agencies from both MINDEF and the DTC.

Analysis during this strategic planning stage is at a highly aggregated level, looking at problems from the macro-system perspective. These planning efforts aim to provide coherent strategic directions to guide the capability development of the SAF, Research and Technology (R&T) thrusts, and development of defence industries. Experiments may also be conducted to explore new operational and war-fighting concepts. Ops-Tech Visioning can be done to derive innovative system concepts to address the SAF's key operational challenges and to drive R&T requirements.

The end product of the Strategic Planning stage is a multi-year MINDEF/SAF Plan that will define the key development milestones for a pre-determined number of years ahead, both in terms of force structure build-up and "softer" areas such as human capital development, training and education. It will be an integrated document synergising and articulating operational, technological and other defence and security related dimensions.


Strategic Planning
(Multi-year plans at MINDEF level)
Formulation of Concepts and Master Plans
Operational Concept Formulation
(Largely Service-driven)
Operational Master Plan
Engineering Master Plan
Systems architecting to support SoS capability development

MINDEF Long-Term Planning Process

Formulation of Concepts and Master Plans

In the next stage, Operational Concept Formulation (OCF) looks at the medium-term planning horizon to develop concepts as the basis for the capability development master plans, i.e. Operational Master Plan (OMP), and the Engineering Master Plan (EMP). OCF and capability development master-planning is iterative and collaborative. These master plans show the milestones for capability build-up, the resource requirements (e.g. infrastructure, equipment, manpower etc) and the training requirements.

Systems Architecting

With the Third Generation SAF being a task-organised networked force, it is vital to have a systematic approach to design complex networked capabilities such as the Third Generation networked IAD. A systems architecture study enables the effective formulation of the OCF, OMP and EMP for such complex networked capabilities. With Ops-Tech collaboration initiated upfront during the OCF stage via a systems architecture study, both the SAF and Defence Science and Techonology Agency (DSTA) counterparts would be in a good position to jointly assess and mutually agree on the need for an EMP. Once that need is firmed up, the work on the EMP can be expected to proceed in parallel with the OMP.

The systems architecture study analyses the capability from an SoS perspective, where different types of systems and technologies are considered in formulating innovative operational concepts for investigation. The SA methodology encompasses the art and science of designing effective operational capabilities – one where various types of systems operate together in an integrated and coherent manner to deliver a quantum increase in warfighting capabilities, more than what the sum of the individual systems can provide. It is a collaborative and often iterative innovation process between operational users and technical subject matter experts, synergising future technology with future operations, and enabled by a robust systems architecture design.

The DTC's SA journey began in late 2003 with three senior staff as DSTA Systems Architects with the charter to discover and exploit new capabilities that could support the SAF. As SA gained buy-in with MINDEF leadership and the demand for SA grew, the DSTA Masterplanning and Systems Architecting (DMSA) Programme Centre was subsequently set up in 2006.

"Recognising that we need to view defence capabilities as outputs of complex system-of-systems, DSTA has established a masterplanning and systems architecting business area to ensure coherence, fit, consistency and flexibility in developing new capabilities. The focus is to develop system architectures that will provide system level coherence …"

Richard Lim, then Chief Executive of DSTA, announcing the formation of the DMSA Programme Centre at the DSTA Suppliers Brief at Asian Aerospace 2006 on 22nd February

The key roles of DMSA were to develop SoS architectures for the SAF and to spearhead the build-up of SA as a strategic competency within DSTA.

Several years down the road, with a growing number of Defence SoS being developed and an expanding base of Systems Architects being groomed, SA was codified in 2012 in MINDEF's DCM systems manual as an integral approach during MINDEF's Long-Term Planning Process.

Enabling Tools

The formulation of advanced operational concepts and their complex systems during the Long-Term Planning stage involves both "art" and "science". To facilitate such work with sufficient analytical rigour, MINDEF and the DTC had invested in laboratories equipped with the necessary hardware and software tools, allowing both operational and technical subject matter experts to develop and evaluate alternative concepts. Two such labs are the SAF Centre for Military Experimentation (SCME) and the DSTA Analytical Lab.

Experimentation of Future Operational Concepts

The SCME is the one-stop centre for all SAF experiments. Through experimentation, the SAF can acquire new war-fighting knowledge, develop innovative operational concepts and doctrines to enhance mission planning. SCME was established in 2003 with three laboratories – the Command Post of the Future Lab, Battlelab and the C4I Lab. These laboratories provide users and engineers with an environment to explore, experiment and demonstrate technology capabilities for the SAF's future force.

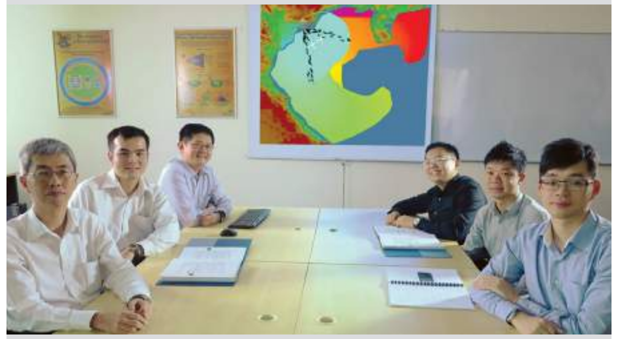
The SAF and the DTC began planning for SCME in mid 2002 because it realised that in future, physical boundaries of air, land and sea would be made artificial by the increasing reach of weapons and sensors. Hence, SCME is an integrated effort between the SAF and DTC where technologists work alongside military experimenters to transform Singapore's defence capabilities.

SCME undertakes a multi-year strategy, which will systematically build up a highly re-configurable C2 system. This also involves the integration of an indigenously built modelling and simulation engine to create a rich repository of re-usable models and exercise scenarios as new models are created to meet specific experimentation requirements.

Battle Lab in SCME

Analysis to Support the Engineering of Complex Systems

To augment the DTC's foray into SA to design coherent SoS for the Third Generation SAF, the DSTA Analytical Lab was set up in 2008 to help engineers design, model and analyse the next generation defence systems. In terms of front-end studies, the DSTA Analytical Lab has demonstrated its ability to help identify suitable technical solutions before implementing a Defence SoS, e.g. for IAD or Maritime Security. Insights from these studies influence the choice of systems for EMPs. Operations Analysis (OA), Modelling and Simulation (M&S) tools are heavily used.



A team of analysts from the DSTA Analytical Lab

The DSTA Analytical Lab also enables a major paradigm shift in the approach in designing systems, harnessing M&S to enable the DTC and the SAF to move beyond learning from legacy platforms (actual systems) to learning from future platforms (simulated). This was epitomised in the example of the RSN's Littoral Mission Vessel (LMV), where a mock-up of a first-of-its-kind Integrated Bridge-Combat Information Centre-Machinery Control Room (IBCM) was simulated in the DSTA Analytical Lab. This allowed the RSN to test the IBCM concept with its sailors on various simulated scenarios, leading to a clear understanding of the requirements for IBCM layout, work flow and crew manning before implementing the IBCM.

Approaches to Systems Realisation

After the Long-Term Planning Process, the requirements definition and acquisition of new defence equipment will take place. This will be realised through acquisition projects.

The OMP and EMP guide the implementation of multiple projects in an integrated and concurrent manner over multiple years. For example, the IAD OMP and EMP formulated in the 2000s guided the requirements for new systems such as radars and weapons, paving the way for projects to acquire systems such as the SPYDER and Aster 30 SAM systems. These new systems will be integrated via the IAD architecture and enhance the IAD SoS. The Appendix provides more details on the DTC's SA and SoS approach.

In addition, each individual acquisition project is carefully scrutinised to ensure that the most cost-effective solution is acquired to meet our operational needs.

Systems Acquisition

Through the years, the DTC has adopted a pragmatic approach in our defence acquisition, summarised as follows:

- Acquire off-the-shelf systems, wherever possible
- Build – design and develop, only where necessary
- Collaborate with partners

We only buy what we need, and what is most suitable and cost-effective for us. We buy very sophisticated and highly capable equipment, but only when it is needed. Often we do not need to buy the latest piece of equipment, when upgrading or refurbishing can do the job. When we replace older equipment with more modern ones, we often do not need to replace them on a one-for-one basis.

For example, our A-4 Skyhawks first came into operational service in refurbished condition in 1974. The Skyhawks subsequently underwent an engine and avionics upgrade in the late 1980s. When they retired from operational service, the Skyhawks had served the RSAF for 30 years.

We replaced them with smaller numbers of more modern fighters.

The SM1 tanks which have been retired, were bought as second-hand AMX-13 tanks from various countries in the late 1960s and refurbished. In the late 1980s, they were upgraded to the SM1 standard and were phased out after over 40 years of service in the SAF.

Beyond acquisitions and upgrades, we design and develop solutions only where necessary, in order to meet our unique operating requirements. In doing so, we would carefully nurture the industry for selected capabilities to be built up and sustained.

We collaborate with partners, both locally and internationally, where there are convergence of interests and mutual benefits. This can take place in multiple forms. For instance, through strategic outsourcing, we could tap industry's capacity and free up our internal resources. With research institutes, both locally and abroad, we could rapidly harness technologies from both military and dual-use domains for defence applications. Collaboration with foreign governments can also help to overcome our local constraints.

Command and Control Systems Development

Early in the DTC's journey, we recognised that it was important to build up an indigenous capability to master the development of C2 systems, particularly in the software domain. This is a strategic capability that will enable the SAF's operational processes and doctrines to be optimally embedded into our C2 systems. It involves very close collaboration between operational users and defence engineers in the design of C2 systems that cannot be easily replicated. This will also provide flexibility to introduce new operational concepts and processes readily, discovered in the course of the SAF's operations, exercises and test-and-evaluation, to evolve and enhance the C2 capabilities continuously.

The preceding paragraphs on the development of the IAD through the decades are a case in point that illustrates the need for tight integration of the sensor, shooter and underlying C2 systems. The application of the networking concept synergises their individual capabilities through heightened communication efficiency and awareness, and reduces the sensor-to-shooter cycle between the time a target is detected and the time it is engaged. There are many more such examples across the SAF's operating domains. The numerous Defence Technology Prizes awarded to project teams and individuals over the years are testament to the significance and impact of this capability.

Chapter Three

SOFTWARE SYSTEMS DESIGN AND REALISATION

Overview

Software systems are vital in defence SoS. This chapter will cover two broad categories of software systems that have been designed and realised by the DTC through the years:

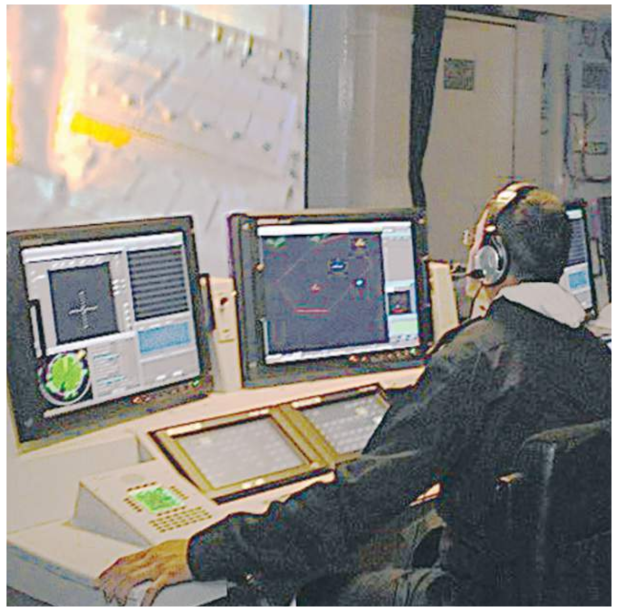
- C2 systems that enable enhanced situational awareness and operational effectiveness during military operations.
- Enterprise IT systems that enable enhanced operations across diverse domains such as the management of human resource (HR), supply chain, finance, procurement, learning, training and knowledge.

Definition of C2 Systems

Today's military missions are simultaneously more complex and more dynamic than in the past. Achieving mission success demands the collective capabilities, resources and collaborative efforts of many military entities.

C2 can be defined as the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations. C2 systems, by extension, are systems that support the commander in these efforts.

Examples of military missions supported by C2 systems include surveillance against suspicious or hostile acts, wartime and peacetime communications, network-centric warfare and disaster relief.



A typical C2 system

C2 Pillar Functions

There are four main functions – situational awareness, planning, tasking and control, and collaboration – that form the basis of most C2 systems:

- *Situational Awareness.* For C2 to be carried out across entities executing a common mission, it is important to have a common understanding of the environment, status and deployment of friendly and hostile forces. Thus, the entities need to share a common situation picture with additional information tailored to their specific needs. To construct the Common Situation Picture (CSP), information of the battlefield has to be gathered via reconnaissance capabilities. This information then needs to be processed, evaluated, fused for dissemination and finally displayed as the CSP. These steps require the use of powerful, real-time computing capabilities.

- *Planning.* A key function of a C2 system is to help users make decisions and carry out planning to achieve the desired outcome. Various decision support tools are needed to help users analyse the situation and come up with different options based on the resources available. The C2 system can then facilitate evaluation of these options for faster and better decision making. A wide range of planning capabilities is needed to address different needs such as to optimise the use of resources. Examples of capabilities addressing this need include platform optimisation, route optimisation and more.
- *Tasking and Control.* Once planning is done, the C2 system is needed to help commanders allocate tasks to the various sub-entities and ensure that the tasks are received in a timely and clear manner. The C2 system must help users monitor and control the execution of tasks. Should a change of plan be needed, the C2 system must also assist users to react to the change and carry out an alternate plan.
- *Collaboration.* Throughout the various stages of operation, the different entities involved need to work as a team. The collaboration functions of the C2 system enable the coalition of entities to plan and execute the operation coherently. Effective collaboration tools make it easier for the various entities to work towards a common goal.

C2 Competency Build-Up Journey

1970s

In the 1970s, most of our military capabilities – sensors, weapons and platforms – were procured overseas and largely stovepiped in nature. While production was left to the defence industries, operational requirements were conceived in-country, grounded firmly in perceived threats unique to Singapore.

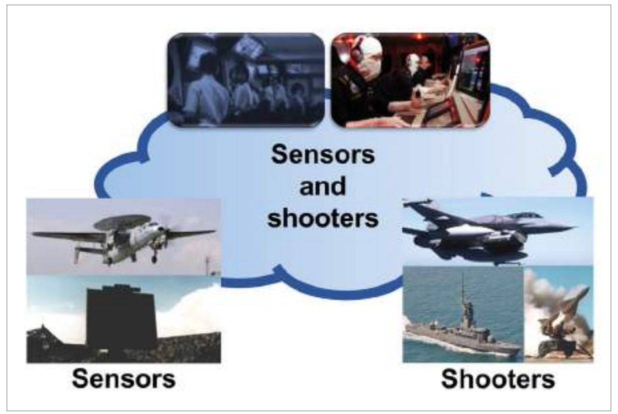
There were strong imperatives to develop in-country technical expertise that would enable us to maximise the potential gains of a combined SoS to meet all specific operational requirements. Relying on stovepiped solutions to address all perceived threats would have been expensive in terms of equipping and logistics, demanded expansive manning, and yet be ineffective in dealing with multi-layered threats.

The first-generation C2 system was thus conceived as part of the build-up of our air defence artillery unit in the late 1970s.

1980s

We began to recruit computer science and engineering graduates to be groomed in systems design and development as part of the strategy to nurture in-country competency in C2 systems development. In the early 1980s, these new defence engineers were deployed for on-the-job training stints in overseas acquisition projects with established defence contractors. One such example was the Air Defence Ground C2 System.

The defence engineers were trained in Sweden's Ericsson Radio System AB to construct a new ground C2 system from design to deployment, and were part of the software development team tasked to implement core components of the real-time C2 system. They also took on the role of systems engineers in hardware designing and test management.



Engineering an integrated C2 capability

In the naval domain, a Coastal Surveillance C2 System for the Coastal Command Centre and a shipboard Action Information System for the MCVs were also taking shape in Sweden through the same approach.

Upon completion of these immersive stints, the engineers brought home profound systems knowledge and were hands-on to provide system support, troubleshoot faults and implement upgrades of the application software and firmware of the operationalised systems.

The strong commitment of MINDEF to pursue C2 competency in-country had also contributed to the formation of Singapore Engineering Software Pte Ltd (SES) in 1986, jointly owned by ST Electronics and Ericsson Radio System AB, to provide further support in the transfer of C2 know-how. SES has since evolved to become ST Electronics (Info-Software Systems) Pte Ltd, a key command, control, communications, computers and intelligence solutions provider in Singapore today.

During the same period, another key defence system – the United States Navy's E-2C Hawkeye – was being procured via Foreign Military Sales from Grumman Corp (which would later become Northrop Grumman Corporation). In late 1985, a team of 12 software engineers was attached to Grumman Corp in USA for 14 months to learn about the E-2C software. We needed this competency so that we could be self-reliant to carry out E-2C software changes upon their return. Besides the full life cycle of the E-2C software development, the engineers also learnt good practices like upkeeping personnel's expertise and system capabilities through staging regular system refreshes.

1990s

We began local development of C2 systems in the 1990s. Several C2 development projects were initiated.

Upgrading the Mission C2 System of E-2C

The E-2C's original mission suite consisted of a mission computer, a 10-inch diameter monochrome display and a 4-inch alpha-numeric display. As our AEW missions matured in the 1990s, there was an increase in workload for the E-2C operator. The system was found to be increasingly inadequate in coping with operational demands for missions. The system was limited in control functions and man-machine interface features, with many functions requiring frequent operator actions. This resulted in an undue burden on the already heavy operator workload and distraction from actual mission execution. The display, with its limited monochrome features, did not facilitate the operator in the quick assimilation of information and the building of situational awareness.

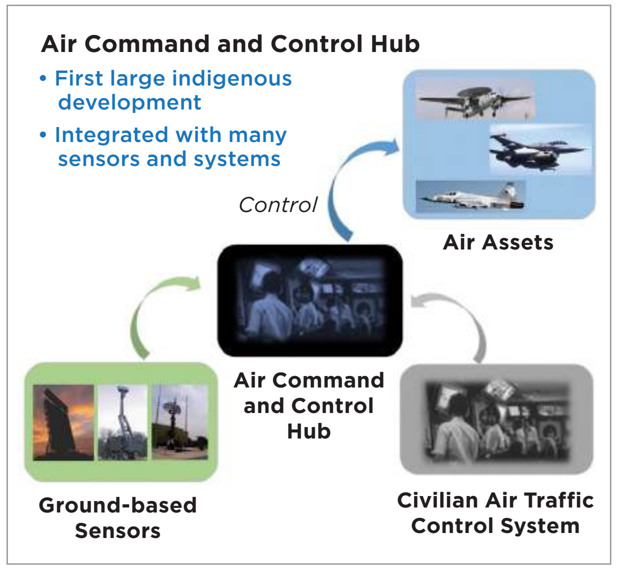
Hence, there was an operational need to upgrade the aircraft with modern computer and display systems in the most cost-effective manner in order to enhance the E-2C operator's efficiency and effectiveness amid an increasing workload, as well as to overcome system obsolescence issues.

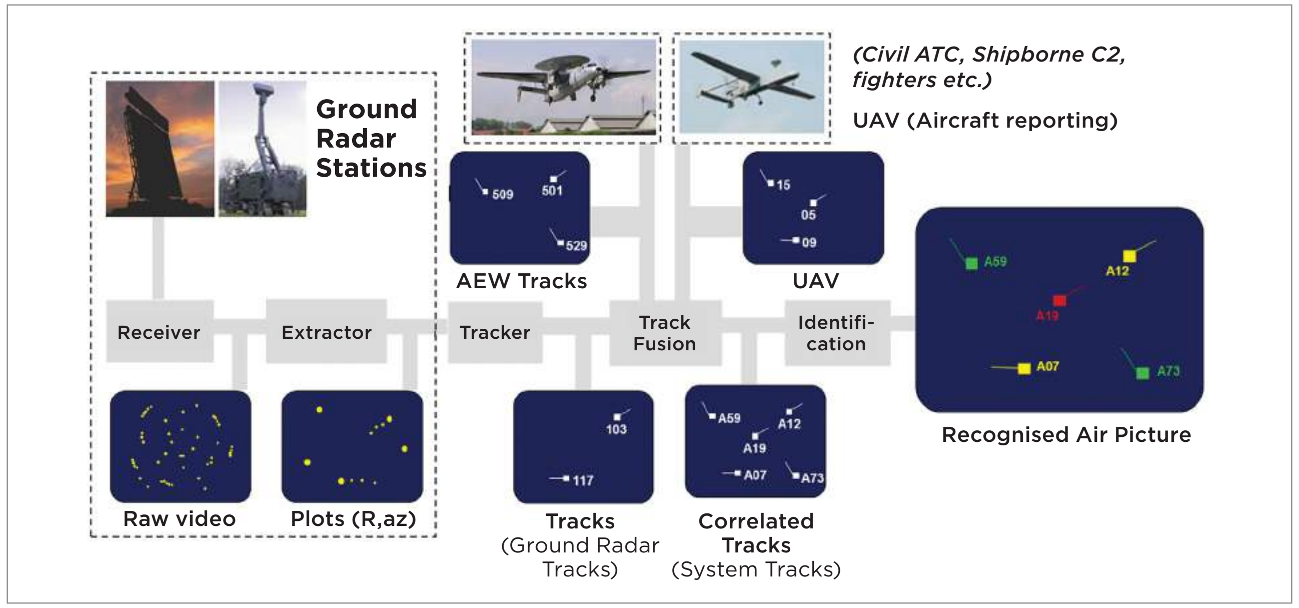
In the 1990s, MINDEF approved the E-2C Mission Control System Upgrade to enhance the operational efficiency and effectiveness of the E-2C controllers and their role in Airborne Early Warning and Control missions. Prof Lui Pao Chuen, then Chief Defence Scientist in MINDEF, commented that the level of confidence in our ability to implement the in-country upgrade was high "because of the conscious investments made over the years in building up our in-house capability on E-2C systems and software".

The E-2C upgrade project was also a complex and challenging programme. It not only demanded extensive software development, but also hardware development and systems integration. Beyond the complex real-time software, there was also the need to integrate it with legacy aircraft systems like the radar, IFF system and navigation systems, via non-standard protocols and in real-time with responses in milliseconds. There was also a challenge in developing hardware suitable for an airborne environment, with various options considered. The technology landscape in the 1990s was slowly gearing towards commercial off-the-shelf (COTS) computing and display technologies. Leveraging COTS hardware allowed us to change our design with greater flexibility. Using field programmable gate array in our interface cards allowed us to use software to define the hardware logic, which could then be easily re-programmed when hardware design needed changes. The concept of enclosing all the commercial cards into a rugged enclosure allowed us the flexibility to redefine the system logic as the project progressed. Additional computing power was added, computers upgraded, interfaces redesigned, as well as instrumentation and data-logging implemented. All of these were achieved with minimal system modifications, which was an unprecedented feat for aircraft systems then.

Developing Air C2 Hub

With the successful delivery of the Air Defence and Air Traffic Control Systems, MINDEF's leadership rationalised and decided to embark on a new generation Air C2 Hub (AC2H) to revolutionise the propriety Air Defence and Air Traffic C2 systems. This was to become our first in-house, large-scale development programme. Another first was that we had capitalised on the advancement in COTS products to modernise our C2 capabilities, which until then had been powered by proprietary equipment.


Air Command and Control Hub
• First large indigenous development
• Integrated with many sensors and systems
Control
Air Assets
Air Command and Control Hub
Ground-based Sensors
Civilian Air Traffic Control System



Schematic views of AC2H

With COTS, system equipping and maintenance was significantly cheaper. More importantly, the adoption of COTS opened up avenues for quicker capability refreshes and insertions.

The outcome of the programme was an indigenous and complex AC2H that was extensively integrated, highly available and adequately configurable to support stringent, multi-role missions of the RSAF.

In a separate track, the Coastal C2 system was also rejuvenated using COTS solutions by another in-house development team.

In-house Development – Confronting the Challenges

To produce a C2 system in-country was challenging – we had to deliver the required C2 capabilities within the same timeline and budget as established foreign contractors had they been contracted for the project.

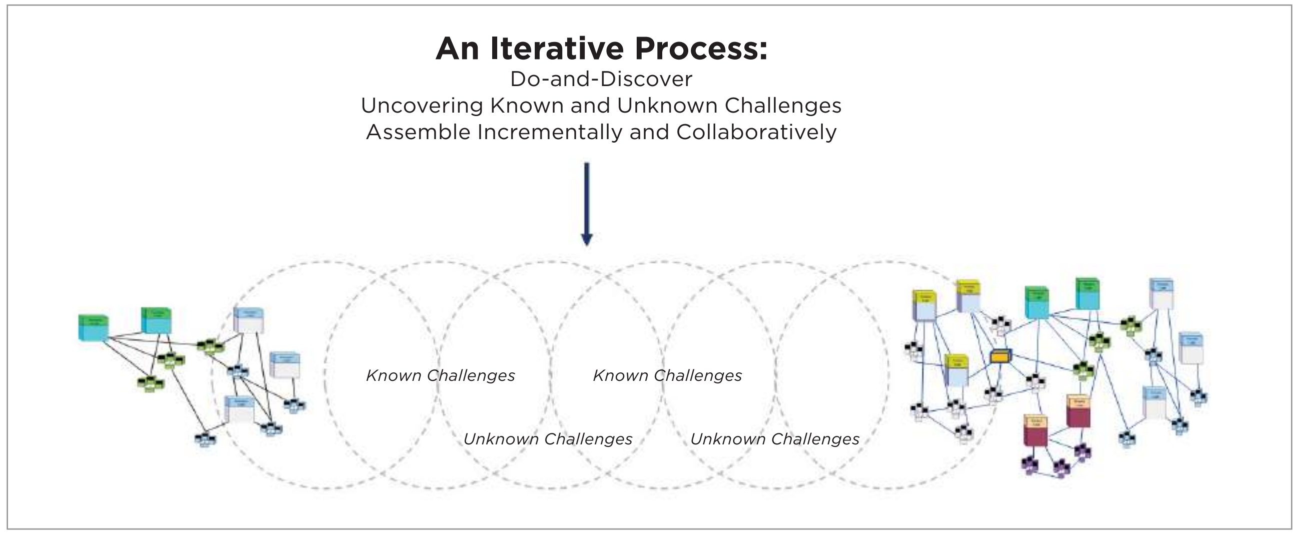
The team met daily to discuss software designs and gathered weekly to review codes. The team also had to confront many technical challenges in meeting stringent, mission-critical and real-time requirements of the AC2H.

To mitigate development risks, the team dissected the system requirements into modular sub parts, and took to solving them iteratively. Trials were conducted every six months to insert new functionalities and technologies, and to validate the robustness of the evolving systems architecture continually. With this continuous validation process to evolve the AC2H, stakeholders interacted frequently and reinforced shared vision and passion.

For servers, we moved from proprietary computers to UNIX computers; for network, we moved from Fiber Distributed Data Interface to Gigabit Ethernet. We selected COTS software components carefully as building blocks for the middleware that was to be the software foundation on which the AC2H was developed.

We assessed and tested several COTS products, eventually adopting one that was built for real-time and reliable distribution of financial data for banks and brokerages world-wide. It had the required robustness and fail-safe features already built in. We were the first to adopt it for a military application.

To effectively support the high-tempo and precise operations of the AC2H, there was a need to have a coherent situation picture and decision support systems to allow users



Iterative Development Process

to concentrate on their missions and to make quick and accurate decisions. Together with expertise from the sensor community in the Defence Materiel Organisation, we specified the requirement for a multi-sensors tracker and acquired it through a competitive tender so that we could get the best-of-breed product in a cost-effective manner. In addition, we also worked with defence scientists from the DSO to develop the algorithm and decision support systems for identification of radar detections and conflict alert.

In 2002, we successfully delivered a robust AC2H fit for the RSAF.

2000s and Beyond

Building upon the success and experience of developing the AC2H, the team embarked on the design and development of the C2 system for the Third Generation Air Defence System. As mentioned in Chapter 1, the Third Generation Air Defence is based on a networked concept that integrates new and existing sensors as well as C2 and weapons systems into an SoS. To network these systems, the team designed and developed the C2 Network (C2N), which provides a conduit for tactical information to be exchanged in real time among all combat systems in the network. The C2N manages the sensors and weapons centrally and is able to assign the best sensor and weapon pair to achieve a high kill probability for successful engagement of incoming air threats. The processing for the sensor and weapon assignment takes place continuously and is able to reassign the sensors or weapons dynamically in the event that some of the assets become unavailable, ensuring continued engagement.

To realise the networked capabilities, it is critical that all systems within the C2N work well not only as an individual system, but collectively as an SoS. Emphasis was hence placed in the design of the communication between systems and the approach for system integration at the onset of the project. As timeliness of information is crucial for air target engagement, the status and latency for the inter-system communications are continually measured and monitored so that any deviation can be alerted for corrective actions to be taken. The C2N was also designed to ease the integration of combat systems into the SoS and is scalable for the addition of new and future systems. To facilitate this, the team adopted international standards to perform systems integration and defined new local standards when such standards were unavailable. In doing so, the team avoided suppliers lock-in and gained the freedom to choose the best sensors and weapons to meet the RSAF's operational requirements.

In 2014, the team delivered the first spiral of the Island Air Defence with the SPYDER weapon system successfully integrated as part of the C2N.

Enterprise IT Systems

While C2 systems focus on aspects of planning, directing, coordinating and controlling military forces and operations, Enterprise IT systems focus on orchestrating business processes and the automation of business functions that encompass complex business rules and policies that form the fundamental operations of an enterprise's business. Enterprise IT involves a diverse range of IT capabilities that support the organisation's functions both internally and externally.

Within the organisation, an individual employee's IT needs would start with productivity tools such as Email, Document Editing Tools and Calendar that would typically be pre-installed within the personal computing device. At the team level, this would include collaboration tools such as shared folders, messaging and meeting applications that support team communications and work. At the organisation level, the solutions support the operation of organisational functions such as HR, logistics, procurement, finance as well as softer organisational functions that include innovation, engagement and knowledge management.

Extending out of the organisation, Enterprise IT supports the delivery of services to the organisation's customers – NSmen, full-time national servicemen (NSFs), as well as the general public for MINDEF and the SAF. Enterprise IT systems also support the conduct of business with other organisations through supply chain integration, electronic commerce portals and links to financial institutions.

Being integral to the organisation, IT operations have become critical to ensure business continuity. From a strategic perspective, the use of IT has been instrumental in achieving significant productivity gains, better decision outcomes, organisation agility and the ability to support the transformation of business models and services.

Enterprise IT Portfolio

A portfolio approach is taken to manage Enterprise IT to provide a framework to prioritise and manage IT investment. The portfolio comprises the following key segments:

- Logistics Enterprise
- Personnel Admin and Finance
- Defence Infrastructure and Information

These segments work in tandem to shape the IT landscape for MINDEF and the SAF.

Enterprise IT Competency Build-Up Journey

People are the valuable resource that make up the whole organisation. Generations of leadership in MINDEF and the DTC have led effectively in the use of IT. Beyond harnessing IT to realise productivity gains to help an SAF dependent on a conscript force, many of these leaders have gone on to contribute in other ways in service of the nation.

1970s

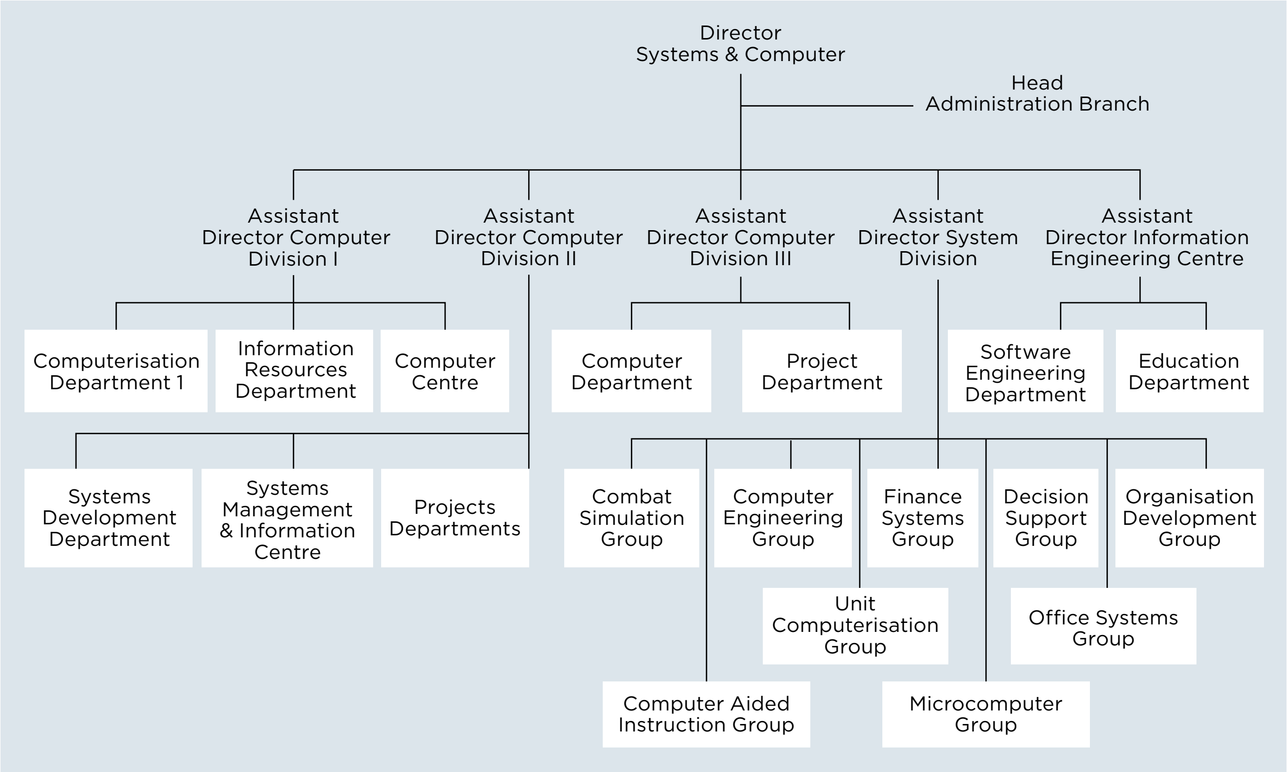
Structure and Industry

In July 1970, in addition to the Data Processing Department, the Systems and Research Branch (SRB) was set up under the leadership of Mr Philip Yeo[1]. With the British making the decision in 1968 to withdraw its military presence from Singapore, there was a need to review Singapore's ministerial structures, procedures and methodologies. The set-up of the SRB was a first step towards the endeavour to institutionalise “systems thinking”. To build up the expertise in “systems thinking”, personnel certified medically unfit for physically demanding roles and with good tertiary qualifications were identified and posted to SRB to fulfil their National Service duties. In 1973, the Finance Systems Branch (FSB) was also created and SRB was reframed as the Logistics Systems Branch (LSB) to further harness IT.

In 1979, these entities – Data Processing Department, FSB and LSB – were amalgamated into a single system and computer entity to form the Systems and Computer Organisation (SCO) under the leadership of Dr Tan Chin Nam[2]. The push for the build-up of a pool of IT professionals went beyond defence so that Singapore's IT industry might benefit. This led to the set-up of the National Computer Board.

[1] Mr Philip Yeo Liat Kok joined MINDEF in 1970 to set up the SRB. In 2007, he was appointed Chairman for Spring Singapore and was the first Chairman of the National Computer Board (now known as the Infocomm Development Authority of Singapore).

[2] Dr Tan Chin Nam was the first Director for SCO. He retired from the Administrative Service as the Permanent Secretary of the Ministry of Information, Communications and the Arts in 2007. He also served as Chairman of the Board for the National Computer Board from 1987 to 1994.


Director
Systems & Computer
Head
Administration Branch
Assistant Director Computer Division I
Assistant Director Computer Division II
Assistant Director Computer Division III
Assistant Director System Division
Assistant Director Information Engineering Centre
Computerisation Department 1
Information Resources Department
Computer Centre
Computer Department
Project Department
Software Engineering Department
Education Department
Systems Development Department
Systems Management & Information Centre
Projects Departments
Combat Simulation Group
Computer Engineering Group
Finance Systems Group
Decision Support Group
Organisation Development Group
Unit Computerisation Group
Office Systems Group
Computer Aided Instruction Group
Microcomputer Group

Organisation Chart of SCO

SCO staff during the 1980s

Early Computerisation and the Emergence of an Online Culture

In pushing for computerisation, it was believed that computers must be made available for the heart of operations, such as in logistics. Around the mid 1970s, computerised systems in the area of unit accounting, vehicle management and general equipment management were available in MINDEF. The first operational computer to meet MINDEF's increasing computerisation requirements was also purchased. This was the NOVA 3D (with a 25Mb memory) developed by Data General. Computerisation covered manpower and payroll processing, as well as ammo, ordnance supply, general equipment and Air Force logistics bases which drove greater efficiency and productivity.

Soon, MINDEF found the NOVA inadequate, leading to the purchase of three HP3000s in 1977 which proved more successful. The online culture in MINDEF had taken root by that time and MINDEF was largely regarded as being ahead of the rest of the Public Service in the area of computerisation. Not only were systems online, but remote database access was also possible. This was a significant capability then when connections to the bases were via phone lines. This led to a build-up of Supply Management Systems, Finance Management Information Systems and Procurement Information Management Systems.

Most importantly, the process had built up a talent pool of system engineers and computer-literate staff[3]. The system engineers also worked with other ministries in national-level studies, such as the National Income Study, MRT study and simulation studies on traffic patterns.

1980s

Proliferation of Personal Computers and the Start of Office Automation

The first personal computers (PC) were implemented in the late 1980s. These were IBM PCs and were initially costly replacements to typewriters. Proliferation soon picked up rapidly as the PCs offered significant productivity improvements while their cost reduced significantly with the flood of IBM-compatible PCs in the market. These PCs were largely standalone terminals then. This was the start of office automation in MINDEF and the SAF.

Software Engineering Practice

With the significant rise in demand for systems development, there was a push for new methodologies such as Information Systems Planning and the first computer-aided software engineering tool. This was led by Mr Lim Swee Say[4] who headed the Information Engineering Centre. There was also an emerging need for technical standards to facilitate exchange of information between PCs (which used different office productivity tools) and between systems.

A corporal from MINDEF, working on an IBM 3278 terminal in Tanglin Camp in the 1980s.

1990s

Networking on an Island-wide Scale

The arrival of the local area network led to the next wave of office automation capability. Unit level emails and file servers which enhanced communication and collaboration were made available.

A more significant breakthrough occurred when computers in all SAF camps could be connected over island-wide corporate information highways (or Wide Area Network) securely. At the same time, a smart card infrastructure – the SAF Card – was developed to enable secure authentication and authorisation. For the first time, MINDEF and SAF users could communicate seamlessly and work much more efficiently at the enterprise level. This also meant that collaboration could take place across MINDEF and the SAF in a secure manner. It was a significant achievement that set the benchmark across the public sector. The office automation network was the largest Intranet network in Singapore.

[3] Raising computer literacy was very important in that period. A System Education Centre was established to provide skilled manpower and hone the corresponding competitive edge. Not only were computer staff trained, so were users.

[4] Mr Lim Swee Say also served at Singapore's National Computer Board as Chief Executive from 1986 to 1991, and as Chairman from 1994 to 1998.

2000s

The Electronic Commerce Frontier

The MINDEF Internet Procurement System is the first government Internet-based procurement system. With this electronic commerce portal, suppliers could view business opportunities, bid for contracts and invoice for payment. This made it easier and faster to do business with MINDEF.

During that time, all procurement functions were put online, ranging from lower value decentralised purchases to acquisition of platforms and the purchase of spares to support maintenance repair operations. With this success, MINDEF was then asked to provide a one-stop electronic procurement portal for the whole of government. This led to the birth of Government Electronic Business (GeBIZ) in June 2000.

By the end of 2003, GeBIZ had evolved into a full-fledged procurement portal built in-house based on business knowledge and technical capability gained from prior implementations of MINDEF procurement systems. GeBIZ has since been enhanced continuously with new capabilities, including the use of analytics for governance and to assist buyers and suppliers.

Since its inception, GeBIZ has grown to serve 16,500 buyers across 143 government agencies and 72,400 suppliers, providing greater control and visibility over government procurement processes and policy implementations. More importantly, the system supports the compliance with procurement policies and guidelines, which are underpinned by Government Procurement Principles (Transparency, Fair and Open Competition, and Value for Money), International Agreements (such as Free Trade Agreements facilitated by the World Trade Organisation) and the Singapore legislation.

Common but Not So Common

Interoperability and integration were serious challenges in the design and implementation of IT systems. At the user computing device level, for example, PCs, variations in office productivity suite software led to issues in accessing documents that were created in another PC. Also, it was not uncommon to hear about incidents where one team had installed a piece of software and tested it to be working, only to realise the next day that another team had installed another piece of software which consequently caused the entire system to malfunction due to compatibility issues.

With this need to realise interoperability and integration, technical architecture standards were drafted at an organisation level. These included the Common Operating Environment (COE) which is still in practice today, in which a standard client computing configuration (including all software and settings) is created for a PC, mobile device or server. The intent was to standardise the technical standard, product and version of product used. This ensured that different products were properly tested against the COE prior to being installed for users. Appropriate governance forums were also set up to ensure that this practice was followed. This is still observed today to ensure quality and integration of solutions at the enterprise level.

Consolidation and Forming the Core

The benefits of reaping productivity gains had led to a widespread proliferation of applications in all functions. Silos started to form, resulting in challenges in cross functional integration as well as in ensuring data consistency. Commercially, Enterprise Resource Planning (ERP) platforms started to mature and establish integration across organisation functions and supply chains. An enterprise approach to IT was eminent.

The core of the Enterprise IT is centred on Enterprise Systems (ES) for Logistics (which covers finance, maintenance, supply and inventory management), Enterprise HR (eHR) (which covers the HR management of SAF combat personnel, Military Domain Experts, Defence Executive Officers, NSFs and NSmen) and ES for Innovation, Learning and Knowledge (eSILK).

The ES journey began in 2005 when an enterprise approach was taken to harmonise the logistics processes of the Army, the Republic of Singapore Navy (RSN), the RSAF, and Joint. The assets managed within ES (Logistics) ranged from platforms, such as aircraft, naval vessels and tanks, to buildings and IT systems. This was a world's first, whereby the Tri-Service ERP system was implemented and processes optimised to achieve better interoperability and operational efficiency across the SAF.

The eHR system followed this journey in 2009 when 52 custom-built legacy applications were migrated into one common core HR system, covering a total population of about 80,000 employees of various schemes in MINDEF and the SAF. This achieved better administrative efficiencies and data quality with “single source of truth” of Human Capital (HC) data, and paved the way for more effective HC trending, analysis and policy formulation.

Additionally, eSILK was deployed across networks of different security classifications to provide common repositories and platforms for document sharing, collaboration and records keeping. In a larger context, eSILK also enabled effective knowledge management for MINDEF and the SAF. With these core systems in place, new capabilities have and will continue to be built to extend from this base.

Managing Complexity through an Enterprise Architecting Approach

An Enterprise Architecture (EA) approach is formalised and ingrained in the way IT systems are implemented[5]. The EA approach establishes a common language and understanding of technology, solutions, information and business that extend from earlier technical architecting works. This abstraction allows the complexities of the Enterprise IT landscape to be managed effectively in a systemic and holistic manner.

The EA approach focuses on being pragmatic, sustainable and to serve as a framework to facilitate business integration, drive business efficiency and achieve systems implementation in alignment with strategic goals. All EA artefacts are captured in a single repository for the whole organisation. Concurrently, the methods and tools have become effective means to manage the implementation of "process heavy" Enterprise IT applications and their changes. Model-driven development approaches (i.e. business processes and rules are modelled and the code generated from these models is used to build business applications) have been adopted for both ERP and bespoke application implementations to achieve greater agility and flexibility through a better understanding of impact to changes and better designed systems.

2010s

IT as an Enabler for Business Transformation

The concept of IT as an enabler for business transformation emerged as a strategic advantage in the emergence of new global enterprises and reinvention of traditional enterprises. The push for innovation in IT

[5] The articles entitled “The Organisation Compass – Enterprise Architecture” and “Driving Business Transformation through a Process-centric Approach” published in DSTA Horizons in 2007 and 2009 respectively document the practice of EA in IT.

is not just in technology for automation or better records keeping, but it is also in the application of IT to generate greater business value through new business models or doing business differently.

This was strategic in the push for MINDEF.com and electronic commerce. In early 2000s, the MINDEF.com initiative was started by Mr Peter Ho Hak Ean, then Permanent Secretary for Defence Development. The portal (currently named NS.sg) is a one-stop site for NSmen and NSFs. Beyond contributing to the electronic government landscape, the portal forges organisation functions together and serves as the basis to integrate business processes and information to deliver a unified service front.

Another more recent and noteworthy initiative is LEARNet. Coined the initiative for the learning transformation of the SAF which started in 2011, LEARNet serves not only as the platform for learning[6] for our soldiers, but also as a vehicle of transformation in the way the SAF conducts its training and learning. At its core is a change in learning pedagogy from the traditional classroom-based and instructor-led method, to a self-directed and collaborative approach. This change is necessary to keep pace with the way Gen-Y soldiers learn and to tap opportunities to make learning more efficient, effective and engaging. The network sets the stage to establish learner-to-content, learner-to-instructor and learner-to-learners connections. This change is also supported by structural changes in training institutes, reviews of curriculum and content, instructor training and the set-up of the SAF Centre of Operational Learning. Thereby, the SAF is in a good position to take the lead in adult learning and organisation learning.

Challenges To C2/IT Systems

Cyber attacks have grown into a business where criminals would steal and sell personal data from credit cards and corporate data such as intellectual property as well as develop and sell attack toolkits. Hackers could even be hired to conduct cyber attacks on organisations. It has been estimated that the total value of cyber crime has surpassed that of the world's drug trade.

Predecessor organisations of DSTA have been developing cybersecurity since the 1980s. To give a concerted push in developing this critical capability, DSTA formed the IT Security Division in 2002 by bringing together about 30 cybersecurity staff from various parts of the organisation. Today, it has grown into the Cybersecurity Programme Centre of about 130 staff.

The key success factors have been the management's vision and the commitment of passionate engineers. With a continuous stream of projects from MINDEF, it has allowed the cybersecurity team to grow exponentially.

Moving Forward

The IT industry faces rapid changes in technology, competitive products and offerings, and constant innovation. Sustaining our engineering leadership is critical to ensure that we maintain our ability to be responsive and agile while acting as a critical enabler to business changes and transformations.

The DTC continues to sustain its engineering expertise through in-house implementation of selected large-scale projects. This allows hands-on opportunities for engineers and ensures that technical skills are kept up-to-date.

Our ability to evolve operational and business concept of operations; our expertise in C2 and IT SA and design; and our track records in software systems development and SoS capabilities delivery have well positioned the DTC to evolve from realising SoS capabilities to contributing in Singapore's Whole-of-Government Smart Nation initiatives.

A nation where people live meaningful and fulfilled lives, enabled seamlessly by technology, offering exciting opportunities for all. We should see it in our daily living where networks of sensors and smart devices enable us to live sustainably and comfortably. We should see it in our communities where technology will enable more people to connect to one another more easily and intensely. We should see it in our future where we can create possibilities for ourselves beyond what we imagined possible.

Prime Minister Lee Hsien Loong at the Smart Nation Launch on 24th November 2014

[6] LEARNet covers the set-up of a user-centric learning portal, smart classroom to support collaborative learning and equipping of mobile tablets and devices to support self-directed learning.

References:

Builder, C. H., Bankes, S. C., & Nordin, R. (1999). *Command concepts: A theory derived from the practice of command and control.* Santa Monica, California: RAND.

Chapter Four

OPERATIONS AND SUPPORT ENGINEERING

Introduction

The SAF needs reliable and maintainable defence systems that are readily available and of high quality to satisfy its mission requirements and operational tasks. Achieving specified levels of reliability, availability and maintainability (RAM) for a defence system is important as it can affect the system downstream in terms of its readiness and safety, the associated logistics support, and the life cycle cost (LCC). Cost is computed using not only procurement costs, but also the long-term costs incurred in maintenance, driven by RAM, and other factors through the system's life cycle. Success in military campaigns and Humanitarian Assistance and Disaster Relief (HADR) operations cannot be achieved without good quality, ready, safe, reliable and maintainable systems, along with the associated logistics support.

Logistics support is not merely about adequate and timely spare parts provisioning. It is also about the support and test equipment, facilities, technical documentation, training, manpower plan, maintenance plan, packaging, handling, storage, transportation and contractor technical services required to support the operation and maintenance of a defence system – this is known as Integrated Logistics Support (ILS). Good, reliable and maintainable systems will entail an agile, robust and sustainable ILS.

It is important that good RAM and ILS must be deliberately and comprehensively planned for and designed into the defence systems upfront and early on, as well as meticulously and diligently followed through in the implementation of a programme. Treating RAM as being subsequent to design can result in unreliability and inferior supportability being discovered at the end of the development, with the consequent remedial action causing additional expenses and delay. This must therefore be avoided. Good quality ILS has a major effect on the availability of the defence systems. The most cost-effective ILS is one that is developed and procured as part of the main defence contract. However, the adequacy of the acquired ILS is made known only during the operations and support (O&S) period. This practice is commonly referred to by MINDEF as O&S engineering.

The SAF has demonstrated the high readiness (through high serviceability levels) of its defence systems in a number of peace support operations and HADR missions at both regional and international levels. In Operation Flying Eagle, the SAF deployed three Landing Ship Tanks, eight CH-47 Chinooks, four Super Puma helicopters, six C-130 transport aircraft and two F-50 utility aircraft for the 2004 tsunami relief effort. During the New Zealand earthquake in February 2011, 116 SAF personnel, a C-130 transport aircraft and a KC-135 tanker aircraft were deployed to Christchurch to provide disaster relief and to support the evacuation of civilians and emergency workers. In the March 2014 Malaysian Airline MH370 Search and Rescue Operation, the SAF deployed at short notice C-130s; Fokker-50 Maritime Patrol Aircraft; Formidable-class frigate RSS Steadfast with a Sikorsky S-70B Naval Helicopter on board; submarine support and rescue vessel MV Swift Rescue with divers on board; as well as missile corvette RSS Vigour to search for the missing plane. In fact, the crew of RSS Steadfast had just returned to Singapore for less than two days from an overseas exercise with the Royal Malaysian Navy when they were activated for the search-and-locate operation on 9th March. However, they still responded swiftly.

Sources: MINDEF Fact Sheet, 19th September 2014: Singapore Armed Forces' Overseas Operations
MINDEF News Release, 11th March 2014: SAF Continues to Assist in Search for Missing MH370

Operation Flying Eagle

Defence systems are designed to have good RAM for long product life and typically outlive most of their internal components, giving rise to parts obsolescence. Obsolescence is therefore inevitable and it affects all systems. In the past decade, parts obsolescence was accelerated by the rapid wave of progress in electronics and material innovations especially driven by COTS information technologies, systems and applications, and related R&D investments. Thus, it has become a great challenge for military agencies to sustain their defence systems. Obsolescence affects system supportability, safety and mission readiness. In order to overcome obsolescence, high costs and significant efforts may be incurred. Existing methods to mitigate obsolescence risk include minimising proprietary parts, options to purchase additional spares throughout the life cycle and mid life upgrades to provide cost-effective continuity of support for the defence systems. New approaches may be necessary to maximise the value of defence systems throughout their life cycles.

The SAF maintains high readiness and serviceability of its defence systems due in large part to the good and diligent work of the engineers and logisticians of the DTC. The DTC has placed great importance on RAM, ILS and obsolescence management. It has given due attention to their early and proper planning and design, as well as the relevant approaches, processes, methodologies and tools since the early days. This laid a strong foundation for new initiatives to better support the SAF into the future.

This chapter shares the DTC's journey in defence systems O&S engineering through the following sections: RAM, ILS, obsolescence management and engineering personnel. The sections are supplemented with additional reading materials in the Appendix which elaborates on spare parts provisioning optimisation and performance-based support strategy.

Reliability, Availability and Maintainability

Introduction

Reliability and Maintainability (R&M) are vital operational characteristics of defence systems and have a dominant impact on both operational effectiveness and LCC. The provision of defence systems with acceptable levels of R&M is essential to the achievements of operational effectiveness, economy of in-service maintenance support, and optimised LCC.

To ensure that the necessary levels of R&M are achieved, realistic systems availability requirements must be set, together with a management strategy laid out. This strategy reflects a continuous and evolutionary approach to the achievement of R&M goals. The management of the R&M tasks should be an integral part of the project activity from front-end planning to the acceptance of the system into service.

It is essential at the outset of the operational needs definition that R&M requirements are carefully studied in the context of the total operational requirements, and that early in-depth consideration is given to the project objectives. Unrealistic and ambiguous requirements can lead to unnecessary expenditure of money, time and effort, and may result in the failure to meet systems availability and operational requirements.

Environmental requirements should also be duly considered as the R&M of defence systems are affected by their operating, transportation, and storage conditions.

This section gives an overview of the R&M engineering evolution as well as its design philosophy and approach in defence capability management.

Evolution of the R&M Engineering Capability in MINDEF

Quality Assurance Department, Defence Science Organisation. R&M engineering practice started out in the early 1980s with a small group of engineers from the Quality Assurance Department (QAD) in the DSO supporting in-house development. Headed by Mr Koh Wee Liam[1], QAD had a role in ensuring good mechanical design and packaging, quality as well as reliability of DSO developmental systems and production contracts with the industry. Driven by the need to support cutting-edge in-house developmental projects, QAD gradually built up its capabilities in reliability engineering, quality assurance, and electronic testing. Environmental engineering, another branch of engineering related to R&M engineering also emerged. Basic environmental testing facilities built up in DSO included equipment to conduct temperature, humidity, sine vibration, shock and drop testing of small items. A small tank and shelter were also improvised to conduct rain and immersion tests. With a major RSAF programme under development at the time, temperature-altitude chambers and vibration shakers were acquired to conduct testing on larger and heavier items to meet specific environmental conditions. These facilities also provided the means to conduct temperature-altitude testing and random vibration testing. Environmental measurement equipment such as sensors and data loggers were also acquired to capture relevant data for comparison with test profiles and database purposes.

Reliability Technology, Defence Materials Organisation. The capabilities built up by QAD were later leveraged to provide support to other acquisition arms in MINDEF towards the later part of 1980s. QAD was subsequently renamed Reliability Technology (RT) to better reflect its role and became part of the DMO, which was formed when the SPO and Materials Management Organisation (MMO) were merged in 1986. RT had to concurrently support complex acquisition and developmental projects under DMO as well as developmental projects in DSO. RT was to ensure that acquired weapon systems had high mission availability with reduced manpower support requirements at low LCC. Staff from RT were also attached to overseas Resident Programme Offices. The opportunities to work closely with the original equipment manufacturer's (OEM) R&M departments provided invaluable experiences and knowledge in incorporating R&M designs during early system developments. RT supported many major developmental programmes such as the Missile Corvette (MCV) Programme, Mine Countermeasure Vessel Programme, Patrol Vessel Programme, A-4 Upgrade Programme and F-5 Upgrade Programme.

Systems Effectiveness Assurance Division, Defence Science and Technology Agency. In the mid 1990s, RT was renamed Systems Effectiveness Assurance Division (SEAD) to better reflect its spectrum of work and its expanded vision to be more operationally focused and system oriented so as to influence hardware and logistics design upfront. With the formation of the DSTA in 2000, SEAD was renamed Systems Engineering (SE). Over this period of time, SE engineers had built up more robust capabilities in RAM and environmental engineering with added focus on front-end planning to define systems' RAM requirements. This was done through a comprehensive front-end availability analysis taking into consideration both operational and logistics inputs. Some of the major programmes supported by SE engineers over these later years included the Frigate Programme, Naval Helicopter Programme, LST Programme, MCV upgrade programme, Littoral Mission Vessel Programme, Submarine Programme, unmanned aerial vehicle programmes, All Terrain Tracked Carrier Programme, FH88 Programme, FH2000 Programme, Self-Propelled Howitzer Programme, as well as tracked vehicle and infantry fighting vehicle (IFV) programmes.

Codification of the RAM Approach

R&M Design Philosophy

a. *Reliability.* Reliable systems have a high probability of performing their required functions for a stated period of time when subjected to specified operational conditions of use and environment. The operational use and environment, therefore, need to be taken into account at the outset of the design process. The design should also be robust to cater for expected variations in production processes, quality, or materials and components. Mean-Time-Between-Critical-Failure or Mean-Time-Between-Failure (MTBF) are two measures of reliability.

b. *Maintainability.* The ease with which equipment can be returned to a usable condition after failure and the time taken for preventive maintenance are important design criteria. Those items which need to be removed, adjusted or inspected most often, for whatever reason, should have the easiest accessibility. Maintainability design is therefore significantly reliability-driven rather than reliability dependent. Mean-Time-To-Repair (MTTR) is a factor of measurement in maintainability. R&M are related activities which need to be fully integrated into all other project activities.

c. *Availability.* Availability is a measure of the degree to which an item is in an operable state and can be committed at the start of a mission, where the mission is called for at an unknown point in time. Availability as measured by the user is a function of how often failures occur and corrective maintenance is required; how often preventive maintenance is performed; how quickly indicated failures can be isolated and repaired; how quickly preventive maintenance tasks can be performed; and how long logistics support delays contribute to downtime.

d. *Design for Support.* The need for defence systems to meet requirements of high availability, effective troubleshooting and fast turnaround of failed systems, lean manning and lower support costs requires implementation of smart maintainability design and technologies early in the programme phases. Apart from maintainability requirements on

[1] Koh Wee Liam started his career as a design engineer in DSO handling prototype fabrication and environmental testing capability. For his contributions in advancing logistics engineering practices within the Ministry of Defence and Life Cycle Management, he was awarded the Defence Technology Prize (Individual) in 1995.

equipment design like size and weight constraints, accessibility and testability requirements, other new maintainability initiatives have also been explored. Some examples of maintainability initiatives implemented in programmes based on cost effectiveness considerations include enhancing equipment diagnostics capability, implementing health and condition monitoring of systems, developing predictive maintenance capabilities, employing interactive electronic technical manuals for maintenance, and providing network enabled maintenance management capabilities.

R&M Approach in Defence Capability Management

R&M Engineering

In line with the R&M design philosophy, it is important to note that the RAM drives the logistics support aspects and hence has a significant effect on the LCC of the system. The R&M of defence systems is also affected by their operating, transportation, and storage conditions. Therefore, the RAM approach is to ensure that the RAM requirements, including the environmental aspects, are well taken care of during system acquisition as well as the O&S period.

The R&M engineering, management, test and verification approach was mainly based on established International Standards and practices, viz., US and European defence standards, industry standards as well as commercial standards. Capability was built up to undertake fundamental R&M engineering and management tasks for electronic systems developed in-house. These tasks included performing R&M modelling, R&M predictions, Failure Modes, Effects and Criticality Analysis; identifying and managing R&M critical items, Testability Analysis; establishing a Parts Control Programme, Failure Reporting, Analysis and Corrective Action System; as well as conducting R&M verifications.

Environmental Engineering

The effect of the operating environment on military equipment is an important consideration to achieve system designs with high availability. There is a need to look beyond our local environment with the SAF's increased role in operations other than war. Military operations present challenging environments to systems and equipment, such as during extended deployment in harsh climates and explosion of ordnance in close proximity. Thus, there is a need to design and qualify systems to ensure reliable system operation in the envisaged environment over their service life. Environmental qualification can be done by testing, analysis or other acceptable means. To this end, both military and commercial standards for environmental design and qualification have been embraced to deliver cost-effective systems.

The environmental engineering, management, test and verification approach was adopted mainly from established International Standards and practices, viz. US and European defence standards, industry standards as well as commercial standards. To facilitate environmental engineering and management in acquisition, DSTA developed the Environmental Requirements Management Guide. This document addresses the environmental requirements management and assurance process, and provides a basic comparison of various environmental standards and the relevant templates for use. More importantly, some typical environmental data are made available to benchmark environmental requirements in acquisition documents for the RSAF, the Army and the RSN systems whether acquired standalone or installed in different platform types.

RAM/Quality Assurance Environmental Handbook

The RAM and environmental approaches are codified into the RAM/Quality Assurance (QA)/Environmental Handbook which forms part of the MINDEF LCM, and later DCM guides and manuals. The LCM and DCM policies call for acquisition of reliable, maintainable, environmentally robust and high performance defence systems that can effectively improve combat readiness, reduce logistics manpower requirements and minimise LCC. The RAM/QA/Environmental Handbook was structured to guide project engineers to perform RAM/QA/Environmental engineering and assurance tasks in the various phases of the LCM and DCM processes. It is an accumulation of all in-house experiences and technical knowledge from the RAM/QA/Environmental practitioners in the DTC.

Applications

RAM and environmental engineering have been diligently applied to the SAF's programmes. An example is the application of RAM engineering, management and verification in naval system designs to not only meet RAM requirements, but also to allow naval systems to withstand and operate under stringent environmental conditions such as high shock levels attributed to underwater mines and explosions. This is one area where much knowledge and competency have been built up in shock requirements definition, measurement, analysis and testing to complement the project management team. Over time, RAM and environmental engineering expertise have grown broader as staff supported more RSAF, Army and RSN programmes. While the participation of SE engineers in major developmental programmes has ensured that all the platform and combat systems delivered to the SAF are highly reliable, maintainable, available and able to operate in harsh military environments, their active involvement in these programmes has also enabled the practices and methodologies in RAM and environmental engineering to be tested, fine-tuned and benchmarked with best defence acquisition practices along the way.

Reliability Growth Testing

Modern and state-of-the-art military systems are becoming increasingly complex and reliability problems may invariably exist due to design deficiencies. Increasingly, MINDEF also needs to develop its own defence systems to meet its unique operating requirements. An effective solution is to apply reliability growth testing (RGT) early in the development phase in an attempt to identify and eliminate design deficiencies early on in the system's life cycle. The key advantage of conducting RGT early is that design modifications are most cost-effective if made early in the system's life cycle. A successful reliability growth programme depends on a good reliability test programme at the front-end planning stage, as well as realistic and valid assessment of the system's reliability during testing. Planning and assessment of reliability growth requires the use of mathematical models.

The Bionix Infantry Fighting Vehicle (IFV) was conceived in 1989 when none of the commercially available IFVs could meet our needs. Almost eight years later, MINDEF translated this vision for an indigenous IFV into reality. It was one of the early platforms to undergo RGT. The developmental testing carried out for the Bionix IFV could be generally broken into three distinct phases, namely:

- *Experimental Phase* – Testing of two experimental vehicles (XV1 and XV2) from 1990 – 1992
- *Testbeds Phase* – Testing of three Testbeds (T1, T2 and T3) from 1993 – 1995
- *Final Prototypes Phase* – Testing of three final prototypes (1, 2, and 3) and one pre-production model, from 1995 – 1997

The actual reliability performance during RGT was tracked using the US Army Material Systems Analysis Activity growth model as described in MIL-HDBK-189. The performance was compared with the planned growth curves regularly to determine if the reliability growth was progressing satisfactorily. An engineering analysis on the impact of fixes (those introduced late in the test phase or those introduced after the end of the test phase) was carried out during the Testbeds test phase. The outcome of the RGT was a Bionix IFV that met the reliability requirements of the Army before being introduced into service.

A widely used mathematical model in reliability growth planning is the power law model known as the Duane model. Deterministic in nature, the Duane model is suitable for reliability growth planning. A new mathematical model currently being used in the industry and the US Department of Defense for the analysis of reliability growth is the Non-Homogeneous-Poisson-Process model known as the Crow Extended Reliability Growth Model. Traditional growth models address reliability growth based on fixes incorporated during the test or at the end of the test. These approaches are known as test-fix-test and test-find-test respectively. However, in today's environment – with a compressed test schedule and limited available resources for testing – a more common test strategy is the test-fix-find-test (Crow, 2004).

DSTA has successfully applied the RGT methodology using the Duane model and Crow Extended Reliability Growth Model to both the Self Propelled Howitzer and Tracked Vehicle programmes, and reliability goals were adequately met after necessary design improvements.

Rapid Introduction of Off-The-Shelf (OTS) and Commercial Off-The-Shelf (COTS) Equipment

Given the rapid advancement of commercial technology in recent years as well as the increased R&D investment by commercial companies, there has been a shift in the defence acquisition landscape towards the adoption of more COTS products and components. As a result, there has been more widespread use of OTS and COTS equipment as solutions to meet user requirements.

To reap the associated benefits of an OTS or COTS solution, new RAM and environmental engineering approach and methodologies have been identified or refined for use so as to enable the cost-effective acquisition of these products. The use of OTS and COTS equipment has also necessitated a review of the acceptability of commercial test standards and corresponding data to substantiate compliance to RAM and environmental requirements.

Integrated Logistics Support

Introduction

ILS is a composite of all the support resources necessary to ensure effective and economical support of a system's operations throughout its life cycle. It is an integral part of weapon system acquisition and O&S, and represents a major portion of the system LCC. The ILS concept integrates the operational system with the support system. The operational system consists of a set of resources (such as hardware, software and trained personnel) and functions required for the system to perform its intended missions. The support system includes the resources (such as support and test equipment, maintenance personnel, as well as spares and documentation) and functions required for the effective and economical support of the operational system through its intended life cycle.

Arrival of our first two E-2Cs at Paya Lebar Airbase in March 1987

When MINDEF acquired the E-2C AEW aircraft in the 1980s, it set a target to be self-reliant enough to operate and maintain the system within two years of the delivery of the first aircraft, while other countries sometimes chose to rely on foreign help, even after many years of operation. The project team set out to learn from the USN the systematic processes and methods required to carry out a comprehensive and robust ILS planning and implementation.

When the first E-2C aircraft arrived in Singapore in 1987, the project team had already put in place the required logistics, operational and support infrastructure to enable the RSAF Squadron to begin flying immediately. Not only were the hardware and logistics purchased and installed in time, the equally important tasks of training adequate numbers of operators, engineers, technical officers and technicians on a continual basis had been planned for and implemented. This enabled the RSAF to maintain its intended operational readiness throughout the life cycle of the aircraft. This sound ILS groundwork laid more than 30 years ago has been codified by the DTC into the LCM manual. The rigorous and comprehensive ILS planning and implementation continues to be practised to this day to ensure the readiness of the SAF.

ILS Planning

The quality of the ILS has a major effect on the operational availability of the weapon system. The USN initiates each E-2C foreign military sales project with a massive LPC. During the LPC, each and every main and subsystem (hardware and software) – and sometimes individual components of the aircraft system – are examined from the perspective of mission needs. The operational, logistical and other local support needed to fulfil the mission are derived and documented thoroughly in an implementation plan called the Technical and Logistics Development Plan.

The Singapore team assigned for the LPC spent considerable time first learning how the USN did things, then aligning expectations and finally examining and outlining alternative cost-effective approaches to meet local and relevant industrial support needs. The support required for the E-2C – spares, ground support equipment, a software development facility and training – were specified and decisions taken whether to buy them through the USN or directly from their manufacturers. This saved us an enormous amount of money. In all, teams from the RSAF, DSO, ST Aerospace, other local companies and SPO spent five weeks cooped up at a local hotel working with 40 USN, Grumman and subcontractor personnel during the LPC. The USN had estimated the LPC to last 13 weeks but it was completed in five weeks. The learning has enabled us to codify and develop our own maintenance plan through an analytical process known as the Logistics Support Analysis (LSA).

Field deployment of system where "O" level maintenance tasks would be done

Logistics Support Analysis

LSA provides the scientific process component of the ILS. It is the analytic process used to identify, define, analyse and quantify the integrated configuration list as well as the ILS requirements and resources needed for cost-effective logistics support of the system. It consists of two parallel sets of activities, maintenance support analysis and support analysis, to ensure the systematic development, implementation and execution of ILS in order to provide maximum readiness.

Maintenance Plan

Maintenance planning is a process to develop all the anticipated maintenance requirements for the system. It also proposes who will carry out the required maintenance tasks and at which maintenance level (i.e. Operator "O" level on site; Intermediate "I" level in workshop or hangar; or Depot "D" level at contractor premises), as well as the estimated duration of each task. The maintenance plan forms the basis for other recommendations of ILS elements.

ILS Elements

Initial Supply Support. This includes all consumables (e.g. expendable items like batteries for day-to-day operations), repair materials and spares parts that are required to replace production parts that are in need of repair. For each system, the set of spares that is required is determined through computer simulation using inputs such as the operation and training profile, component characteristics (e.g. MTBF and MTTR) and repair capabilities (e.g. turnaround time). The E-2C project was a unique valuable opportunity for the Singapore project team to practise and gain proficiency in the provisioning of spares for a complex system, where we did most of the ILS activities ourselves instead of relying on USN's subcontractors. In the provisioning of spares for the various systems and subsystems of the E-2C, we asked the Aviation Supply Office in Philadelphia to generate the listing of spares with their reliability data based on USN usage data. We then worked out the provisioning list based on our support concept and flying profiles.

Systems Documentation. Documentation includes operator manuals, technical manuals, software documentation and all other information that are required for the operation and maintenance of the system. These documents were provided with the delivery of the E-2C, which enabled the RSAF to operate and maintain the aircraft.

Training. Different types of training are tailored for different target groups. Operator training provides the end users and systems administrators with knowledge on systems usage and configuration management. Maintenance training allows the technicians to perform corrective and preventive maintenance. In the SAF, the train-the-trainer concept is widely adopted. Instructors from military institutes develop internal training programmes based on the original equipment manufacturer's training syllabus. For complex systems, SE training may also be conducted for military officers and DTC engineers. In the case of the E-2C, after the "roll-out" of our first two E-2Cs at Grumman, they were used for pilot and "wizzo" (weapon systems operator) training. Upon completion of the flight training, the two planes were flown to San Diego from the Grumman plant in Bethpage, preserved for sea transportation across the Pacific Ocean, and shipped to the USN naval base at Subic Bay. The sea journey took about three weeks and after off-loading at Subic Bay the E-2Cs were stripped of their preservation, made operational again and flown to Brunei. RSAF pilots flew our E-2Cs from Brunei to a memorable welcome at Paya Lebar Airbase in March 1987.

Support and Test Equipment. Support and test equipment are items that support the operation and maintenance of the system. They include physical tools as well as test, handling and calibration equipment.

Facilities. During the 25 years of operation, the E-2C squadron called Tengah Airport its home. In the air base, there were hangars, a maintenance workshop and supply house to ensure that the aircraft fleet was well maintained and supported to meet its flying demands. As an ILS element, facilities can be categorised into permanent or mobile. This depends on their intended use. Permanent facilities include maintenance facilities, (e.g. hangars), supply facilities (e.g. warehouses) and training facilities (e.g. training simulators) required to support the system. Mobile facilities such as maintenance vehicles and portable generators are not fixed to a location.

Initial Contractor Technical Services. This is to provide an initial trouble free set-up of the weapon system. This is performed during the system introductory stage to solve initial technical problems, provide supervision, guidance and assistance for operation and support tasks.

Contractors' Maintenance Services. Depending on each system's maintenance support concept and plan, contractors are engaged in performing or supplementing preventive and corrective maintenance at different levels of maintenance support. At the depot level, contractors typically undertake repairs using shop replaceable units.

Logistics Support Management Plan. The Logistics Support Management Plan (LSMP) ensures that the ILS activities carried out during the project phase and transition to O&S phase are comprehensive and within the budget allocated before the defence system is handed over to the end user. LSMP helps to optimise logistics resource utilisation across projects and avoid duplication of logistics arrangement for related projects. LSMP covers the ILS package implementation requirements. In instances where the O&S implementation details extend beyond the ILS package (such as end user organisational structures, manpower build-up, logistics sustenance build up development of internal maintenance processes and procedures, and other anticipated sustenance considerations), all the stakeholders in the end user logistics departments and O&S agencies will be jointly responsible for the development of the LSMP.

The RSAF operated the E-2C for 25 years before it was replaced by the G550 AEW aircraft. During its service, the E-2C also participated in many overseas exercises such as Exercise Pitch Black where its availability was put to the test. Because of the initial comprehensive ILS planning and implementation taken by DSTA and the RSAF, along with good follow-on support, the RSAF was able to exploit the aircraft to the fullest capability. An early head start with good ILS planning set the foundation for effective maintenance support downstream. Similarly, if the ILS planning had not been done properly upfront, then it would have been an uphill task subsequently to ensure the desired aircraft availability was met.

Source: DSTA Horizons – Estimation Model for Integrated Logistics Support Cost and Annual Recurrent Expenditure in C3 Projects

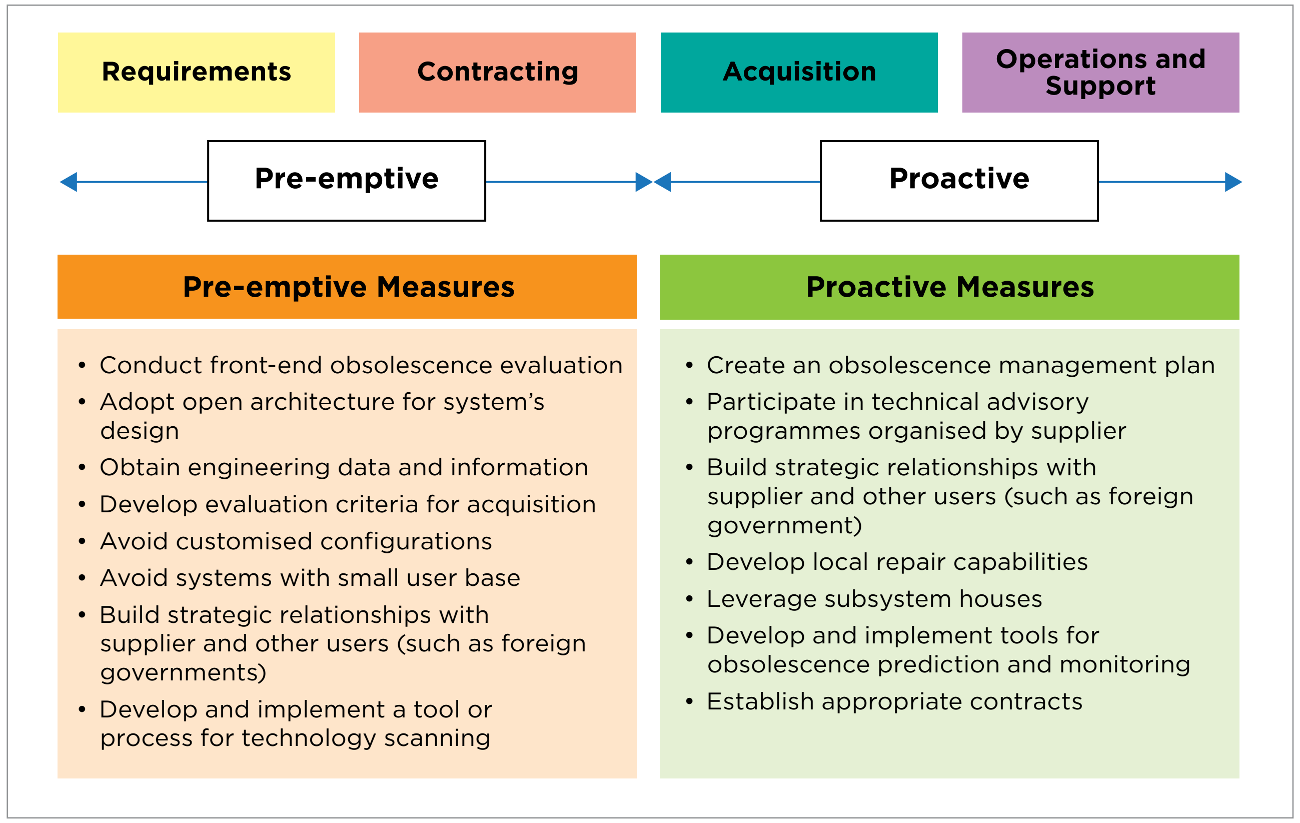
LCM Manual

The approach to logistics management learned during the LPC evolved into a value-added robust process for MINDEF and the SAF, described as the "LCM" of projects. All subsequent projects adopted this methodology and in June 1990, it was formally accepted and documented as the MINDEF LCM Manual, which clearly defined the ILS requirements for project systems. This was further codified into the Logistics Management Information System (LMIS) and implemented using the German software, SAP R/3. The LCM methodology ensures that all aspects of the system life cycle are considered in arriving at relevant and cost-effective solutions. It can be said with some degree of confidence that MINDEF and the SAF are now able to get the best value for its money when acquiring weapon systems. In 2012, the LCM Manual was replaced by the DCM Manual to take into account the increased sophistication of systems being acquired or developed, and the need for more Ops-Logs coordination and integration taking a capability perspective.

Obsolescence Management

Introduction

Obsolescence is inevitable and affects all systems, especially military systems which are designed for a long product life. Military systems typically outlive most of their internal components, giving rise to parts obsolescence. In the past 10 years, parts obsolescence has been accelerated by the wave of progress in electronics and material innovations. Thus, it has become a greater challenge for military agencies to sustain their systems. Obsolescence affects system supportability, safety, and mission readiness. In order to overcome obsolescence, high costs and significant efforts may be incurred. Existing methods of obsolescence management are inadequate to ensure cost-effective continuity of support for the system. A new approach was thus established to maximise the value of the military system throughout its life cycle.



Pre-emptive Measures

- Conduct front-end obsolescence evaluation
- Adopt open architecture for system's design
- Obtain engineering data and information
- Develop evaluation criteria for acquisition
- Avoid customised configurations
- Avoid systems with small user base
- Build strategic relationships with supplier and other users (such as foreign governments)
- Develop and implement a tool or process for technology scanning

Proactive Measures

- Create an obsolescence management plan
- Participate in technical advisory programmes organised by supplier
- Build strategic relationships with supplier and other users (such as foreign government)
- Develop local repair capabilities
- Leverage subsystem houses
- Develop and implement tools for obsolescence prediction and monitoring
- Establish appropriate contracts

Measures to manage obsolescence

Key Principle and Measures

The key principle of obsolescence management is to manage obsolescence throughout the project or system's life cycle – from front-end planning, acquisition to the O&S phase – in order to execute the most cost-effective strategy. Depending on the project phase, pre-emptive or proactive measures can be adopted.

Pre-emptive Measures

Pre-emptive measures should be adopted in the early phase of project implementation. Any risk of obsolescence should be identified early to avoid problems downstream. One option is to explore adopting open architecture systems which can be modified more easily if the need arises. Due consideration has to be given to the selection of the system and the contractor. Conducting market surveys and risk assessments are suitable methods to aid the selection process.

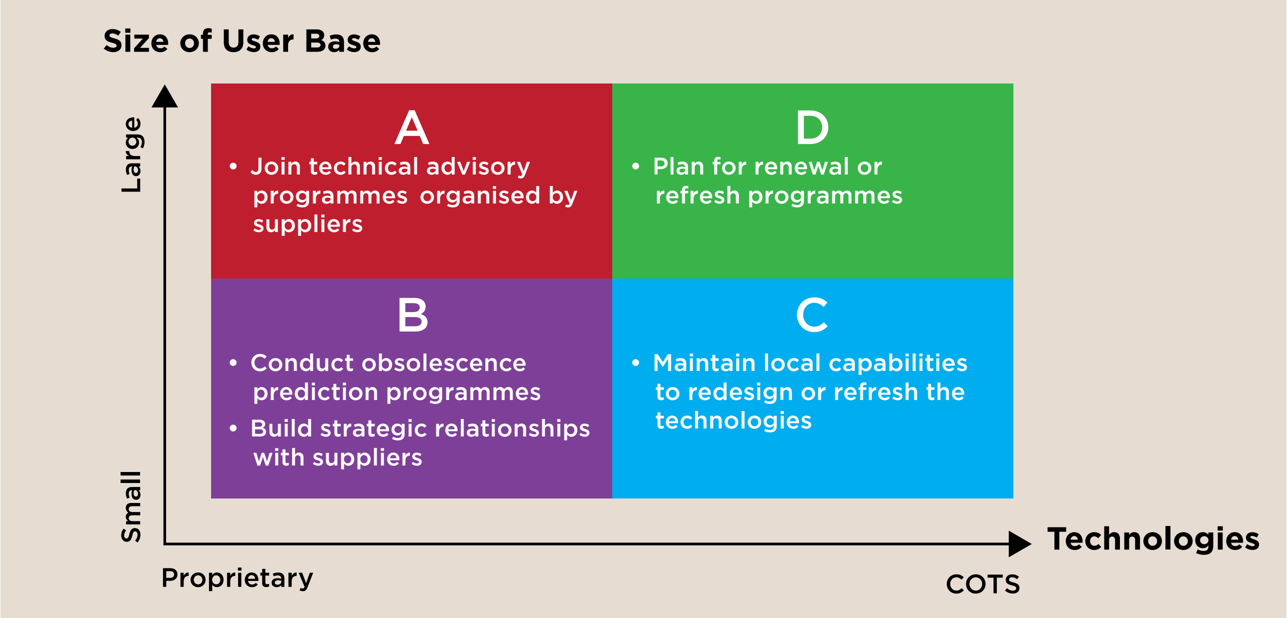
Proactive Measures

Proactive measures should not only be adopted during the contracting phase but also while transiting to the O&S phase. The project team should engage the contractors constantly to monitor any obsolescence issues. Establishing depot level maintenance capabilities (i.e. local repair capabilities) would help to alleviate the impact of obsolescence. Such measures would help to establish through-life support for the acquired system and achieve the maximum benefit for end users.

Obsolescence Management Framework

A framework has been derived based on the collective experience of project teams in DSTA. It is a 2-by-2 matrix consisting of two variable factors: size of user base and the technologies used within the system.

Size of user base can be large or small depending on the number of international


Size of User Base
Large
Small
A
• Join technical advisory programmes organised by suppliers
D
• Plan for renewal or refresh programmes
B
• Conduct obsolescence prediction programmes
• Build strategic relationships with suppliers
C
• Maintain local capabilities to redesign or refresh the technologies
Technologies
Proprietary
COTS

Obsolescence management framework

operators. Technologies used in the components and hardware of the system can be proprietary or COTS products.

Using this framework, the project team can identify the quadrant applicable to the system and employ the relevant measures for obsolescence management. Measures include obtaining user group membership for the technical advisory programmes, developing local capabilities and using obsolescence prediction programmes.

Large User Base – Proprietary Technology (Quadrant A)

Military systems in this category have a large user base and are likely to have a funded, sustainable, and formal process by the suppliers to deal with obsolescence issues. By joining the technical advisory programmes, project teams can gain access to direct operational assistance and consultation with the suppliers.

Small User Base – Proprietary Technology (Quadrant B)

Military systems in this category are likely to face the most challenging obsolescence management issues. Due to the small user base, the suppliers may not invest in resources to track or manage obsolescence. Although COTS is used to lower costs in many instances, the suppliers will have built-in proprietary firmware. Thus, it is necessary to have specially tailored obsolescence management programmes such as using obsolescence prediction programmes for planning and mitigation, as well as establishing appropriate contracts and building strategic relationships with the suppliers.

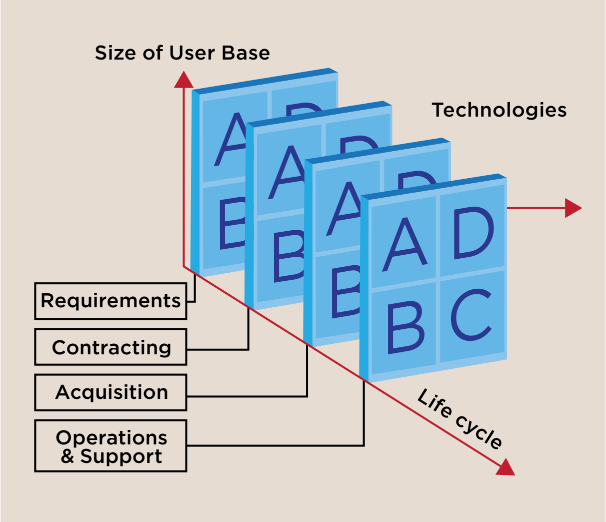
Small User Base – COTS Technology (Quadrant C)

This category is populated by customised and specially developed products or systems. For example, the command and control system software is developed in-house while hardware systems are mainly bought off the shelf. Although the software is proprietary, developing it in-house reduces the risk involved during migration to a newer COTS hardware. Thus, maintaining local capabilities to redesign or refresh the technologies is the key requirement for this category.

Large User Base – COTS Technology (Quadrant D)

Military systems in this category are characterised by short product life cycles (PLC) and lower acquisition costs. Similar to consumer electronic products, the approach is to plan for fleet renewal at every PLC. Some examples of this category include computers, communication sets and optics equipment. Other systems that fall in this category are commercially produced aircraft used for training purposes. Fleet renewal of such systems has to be planned carefully as it can involve substantial budget and effort.

The project team then uses the framework to review and evaluate the relevance of the adopted measures and options in the various phases of the system's life cycle.



Using the framework in various phases of the life cycle

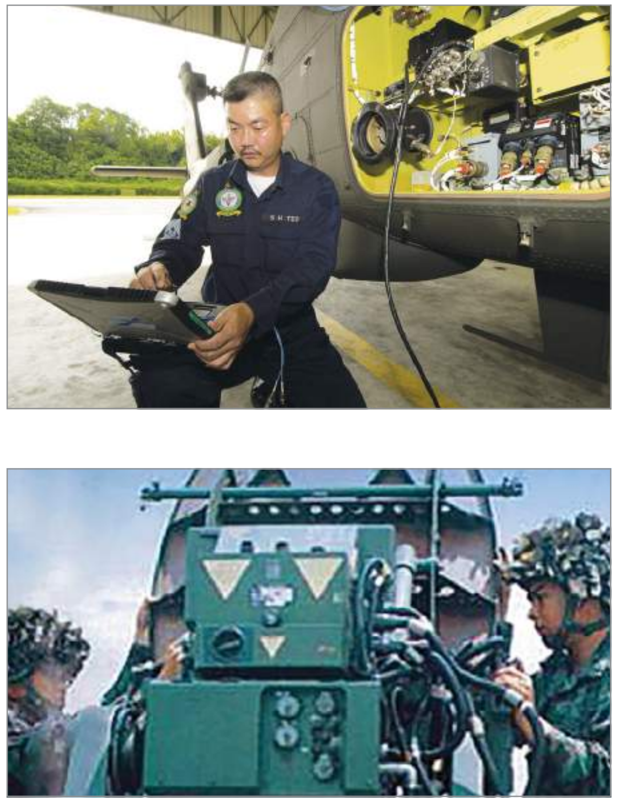
Engineering Personnel

Introduction

In the 1990s, MINDEF and the SAF had already expected to face increasing competition from the private sector for good quality engineers. While we would pro-actively introduce appropriate measures to respond to the changing needs and to match the private sector in attracting and retaining our fair share of engineers from the market, we also had to augment this with the need to utilise our scarce engineering resources wisely. A long-term initiative called the Engineering Resource Deployment (ERD) was launched in the 1990s to position MINDEF and the SAF to meet an anticipated challenge in the future of a declining resource of engineers.

Engineering Resource Deployment

The logic for ERD was based on the following considerations. First, other than improving the efficiency in the use of scarce engineering resources, it also fosters better retention of engineering expertise by providing more varied and challenging work. Second, it provides better opportunities to streamline and optimise processes through adoption of best practices. Third, ERD would also enable us to respond to the rapidly changing technology by shortening the feedback loop from the O&S to future acquisitions.



Engineering personnel in the SAF

Challenges

However, as the proposal called for the transfer of most O&S engineering functions from the Service Logistics Departments (SLD) to the DTG, the three Services had a number of concerns. Their first concern was whether ERD could provide a tight operations-engineering interface, especially with platforms. There was also the perception that ERD would result in the loss of its own engineering capabilities by relying on another organisation outside its existing chain of command for the O&S support of their weapon systems.

Pilot Programme

Given these concerns, an ERD pilot programme was implemented in October 1995. The scope covered O&S engineering for non-platform systems and excluded operational logistics functions. Operational logistics functions (such as maintenance, materials support, training and certification as well as quality control) are day-to-day ground level O&S activities which will continue to be planned, managed and executed in the units, squadrons or bases. This ensures that O&S activities are performed professionally and in a timely manner so as to meet the system readiness requirement. Under the ERD, MINDEF and the SAF defined O&S engineering as those engineering activities carried out during the system O&S period of LCM or longer time/term horizon (such as system performance and cost effectiveness analysis, fault investigation, logistics/maintenance engineering, design of system enhancements/modifications/upgrades, system retirement, and technical advice to operators). O&S engineering activities are generally also termed as System Management.

Under the ERD pilot, the initial non-platform systems selected were standalone and tri-Service (i.e. common across the Services) in nature – command, control, communications, computers and intelligence; radar; electro-optics; guided weapons; armament; training systems; and ground support equipment. The O&S manpower of selected areas was transferred from the SLDs to DMO and the Command, Control, Communications and Computer Systems Organisation (CSO). The DTG assumed the role of system manager for the systems and equipment involved and undertook both acquisition and O&S engineering work. Operational logistics functions remained in the SLDs, and Services retained responsibility for the O&S engineering of all platform systems. The purpose of the pilot was to demonstrate the advantages and practicalities associated with ERD. Work flows, linkages and responsibilities of the ERD organisations vis-à-vis the SLDs, operators and bases were worked out before the pilot programme were refined. The progress of the ERD pilot was closely monitored at the ERD Implementation Committee and the ERD Quarterly Meeting chaired by Deputy Secretary (Technology) (DS(T)) and Permanent Secretary (Defence Development) respectively. In addition, direct feedback was obtained from the latter's visits to units and maintenance agencies affected by the ERD pilot programme.

The pilot programme surfaced a number of challenges, many of which were transitional, and some structural and cultural. With the collective commitment and endeavour to make ERD succeed, many teething problems and transitional issues were resolved. The pilot was also a valuable learning experience for all parties involved. Some of these challenges were:

- *Demarcation of Responsibilities.* Some ambiguous areas surfaced during the pilot implementation, but they were resolved via a case-study approach. Examples were planning for overseas deployment and issuing authority for common engineering instructions. Some of the more difficult issues were surfaced to the ERD Implementation Committee for resolution.
- *Personnel Management.* Several changes were made in the management of technical staff under ERD. The objective was to ensure equitable distribution of engineering talent in the HQs, maintenance bases and the DTG. Changes in the job rotation system were also made.
- *Sustenance of Quality Support.* The Services had stressed the need to sustain quality system support in the long term, especially with the phasing in of new staff not familiar with requirements and working relationships with the Services. As such, the job rotation system had to ensure that personnel have sufficient exposure and experience with ground appointments and a good "feel" for the requirements of operations.
- *Strong and Robust Communication.* Improvements to strengthen the communication in the day-to-day working relationship between the ERD organisations, SLD HQ, bases and users were implemented. These included structured and informal interactions, clearer points of contact and provision of interim updates for long lead time jobs.

Implementation

Following the successful pilot programme, ERD was implemented in 1997 and framed along two broad trajectories whereby the Services would continue to be responsible for the system management of platforms and sub-systems which are tightly integrated to these platforms, where subsequently DSTA would centrally manage non-platform systems, selected platform-based sub-systems and systems that served the common interests of all three Services.

Since its implementation, changes have been seen in the following areas:

- *Building of Deep Engineering Expertise.* The complexity of modern platforms and weapon systems has necessitated the build-up of deep domain expertise to exploit the limits of the networked sensors and shooters of the Third Generation SAF. The need to organise for system effectiveness and mission success places tension on the need to organise for resource efficiency under ERD. This healthy tension paves the way to look at ways to further strengthen the integration of systems knowledge and expertise across DSTA and the Services to enhance operational flexibility, responsiveness and system effectiveness for the SAF to deliver sustainable mission success.
- *Transforming the Entities.* DSTA and the Services have continued to progress and have built up a range of engineering and logistics functions aligned to the evolving needs of MINDEF and the SAF. The constant pressures to transform and right-size within each organisation have resulted in each organisation re-examining its fundamental value prepositions. The continued optimisation efforts undertaken by the organisations have resulted in each having a very lean manpower set-up, with virtually no overlaps in roles between DSTA and the Services.

Ops-Tech Integration

Over the years, the ERD initiative has facilitated cross-deployment to take place, enabled tighter ops-tech integration, and increased the level of interconnectedness and interdependency between the SAF and DSTA. Today, SAF Military Domain Expert Scheme (MDES) officers and DSTA engineers attend the same DSTA Academy Intermediate Systems Engineering and Management as well as Advanced Systems Engineering and Management courses. For the SAF MDES officers, attending these courses forms part of their route-of-advancement requirements. The immersion allows the SAF military engineers and DSTA engineers to learn and interact using the same acquisition and systems management "language", thereby achieving smoother end-to-end capability development.

The opportunity of learning together goes beyond military engineers to combat/ operation officers from the Army, the RSN, the RSAF and Joint Service. Today, DSTA Academy's wealth of knowledge and experience in capability development – from front-end masterplanning and architecting, acquisition and development management, to the operationalisation of military capability are curated and shared via workshops held yearly for the benefit of SAF capability development planners and operational managers.

References:

Crow, Larry H. (2004). An extended reliability growth model for managing and assessing corrective actions. *IEEE Proceedings of the Annual RAM Symposium* (pp. 73-80). doi: 10.1109/RAMS.2004.1285426

Chapter Five

SYSTEMS ENGINEERING METHODOLOGIES AND TOOLS

Introduction

The previous chapters related how the pioneers in the DTC developed and delivered defence systems, which included the formulation of concepts for defence systems and SoS, design, development and deployment of software systems, and O&S engineering that enables systems to be sustained through their operational life cycle. The chapters revealed an underlying life cycle approach to systems engineering that MINDEF and the DTC adopted.

This chapter will explain the systems life cycle approach, the LCM framework that underpins the process of conceptualisation to operations and support, up to the retirement of the systems. It will uncover the key systems engineering methods and tools used in the DTC to generate and analyse options, integrate systems and address system safety.

Life Cycle Management

The Need for a Total System Approach

In defence systems, we often talk about a system from a life cycle perspective – beginning from its conceptualisation, evaluation, design and production, introduction into service and sustenance during service; and finally into retirement and disposal. We measure the success of a defence system by its capability, operational availability and support resources needed over its life span, and not simply its ability to meet the contracted cost, schedule and performance specifications. If a holistic approach was not taken upfront, various pitfalls in the following fictional story could surface.

The Weapons Systems Steering Committee had approved a big sum to purchase a complex system through competitive bidding. A few months after the contract was signed, the project team put up another paper asking the Committee to approve another big sum to purchase a computer simulation training system as the trainer requirement had been left out in the earlier approved paper. Although the Committee felt that the price quoted by the system manufacturer was on the high side, they did not have much choice but to approve it because they faced a monopolistic situation.

A few months later, another shock came. The project team asked for approval to build a new infrastructure to house the trainer. New requirements like these kept on creeping in as the project progressed.

Three years after the main contract signature, the system was delivered together with the trainer. However the new building which was built to house the trainer was not ready because the approval for the building works started too late.

Things got worse a few months after system delivery. The operators started complaining about the poor reliability of the system. Spares were used up faster than expected. Despite all the pressure the Project Team applied on the manufacturer, engineering solutions were just not coming fast enough because the contract did not provide any motivation to the manufacturer. Although the operators were getting the repairs free of charge, the repair turnaround time took such a long time that the spares soon depleted. The Authority was forced to approve another big sum to buy extra emergency spares. Because the spares were bought after the production stage, the price went up by 30%. The explanation for the higher costs from the manufacturer was that there was no economies of scale and they had to restart the production line just for this urgent order.

Due to the poor reliability of the operational system and the long and uncertain repair turn-around time, the operators decided that they had to have more in-country maintenance capability. When the quotation eventually came from the original equipment *manufacturer, it was another big investment and the deal was totally biased to their advantage.*

Years later, the local maintenance capability was established, and the repair turn-around time was greatly improved. While celebrating the achievement of Full Operational Capability, it was also noted that that there was excessive dead stock in the inventory. Most of the dead stock were high-cost spares bought during the earlier crisis, but were now made redundant as a result of the setting up of the local maintenance capability.

The many costly pitfalls in the above scenario can be avoided if a total system approach and long-term perspective in planning and decision making was taken.

Development of MINDEF's Life Cycle Management Framework

In 1986, Mr Lim Siong Guan, then Permanent Secretary (Defence), saw the need for a holistic approach to acquire and manage SAF equipment. A high-level committee was formed in 1987 to develop the MINDEF LCM framework. The committee comprised members from MINDEF, DMO and the SAF, and headed by COL Wesley D'aranjo, then Director (DMO). The LCM would holistically consider the acquisition of defence systems and induction of new capabilities for the SAF, sustenance and upgrade of the system for optimum operational readiness and retirement of the system at the end of its useful life. This was essentially a "system life cycle" (SLC) approach.

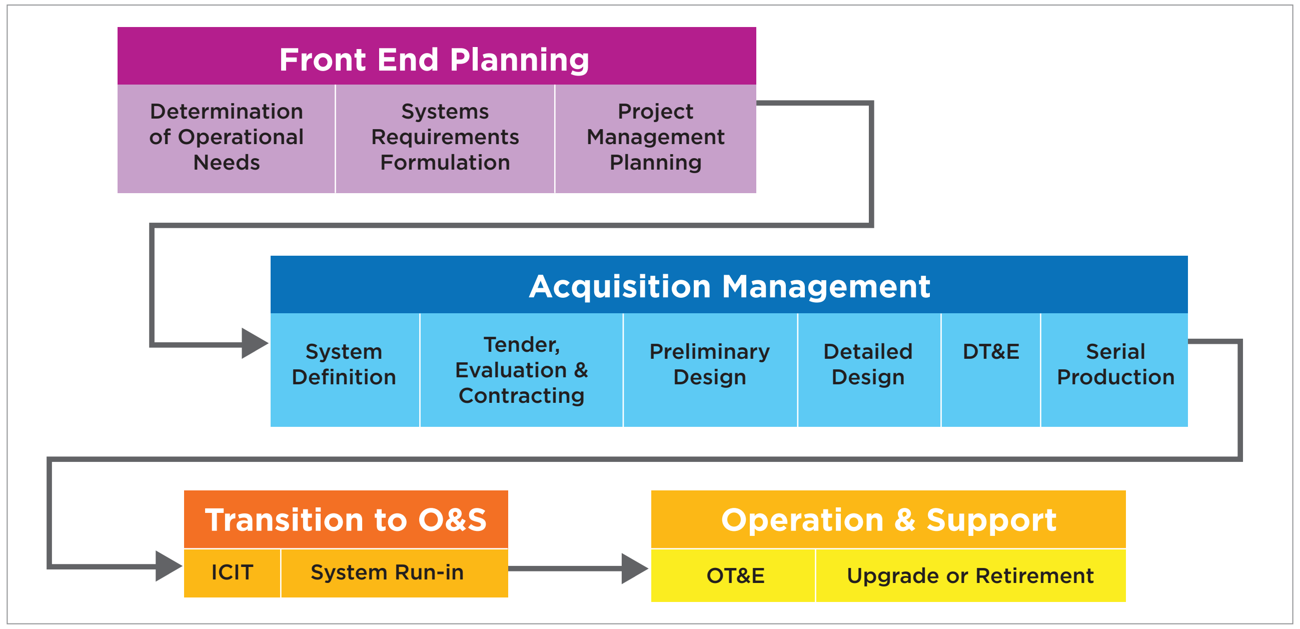
The LCM framework put together the wealth of knowledge, experience and the lessons learnt by DTC engineers over years of acquiring and supporting defence systems. For example, when acquiring new defence equipment (e.g. aircraft, ships, armoured vehicles etc), the associated equipment such as training simulators, in-country engineering capability, spares and support equipment must be defined upfront and tendered at the same stage with the "prime" equipment where possible. This would ensure maximum leverage and price competitiveness in the competitive bidding process, and achieve maximum value for money. System performance and reliability requirements must also be addressed during the tendering and project management phases and not left to chance after the equipment is fielded. Furthermore, engineering support from the OEM must be defined and provisioned for in the contract, especially for complex systems. This would include negotiating for engineering data release and engineers' training on the design perspective of the system.

External consultants were engaged to complement the committee. One of them was Professor Melvin Kline, a specialist and practitioner in LCM systems from the US Naval Postgraduate School. Another consultant was engaged to help establish and implement the ILS methodology, drawing from his experience in large-scale projects. Supporting the committee in developing the methodology and writing the LCM document was a team of systems engineers from DMO and the logistics departments of the three SAF Services. Mr Koh Wee Liam, who was the Assistant Director in DMO, played a key role in developing the LCM framework and was subsequently awarded the Defence Technology Prize (Individual) in 1995 for his contributions. The LCM manual, which codified the LCM framework, was promulgated in 1990.

MINDEF's LCM – The Process

In terms of an SLC process, the LCM framework can be expressed in a simplified form in these phases: Front-End Planning, Acquisition Management, Transition to Operations and Support, Operations and Support, and System Retirement.

The process begins with the formulation of projected operational high-level needs from MINDEF/SAF's longer-term plans. These needs are transformed into specific and realisable operational capability requirements. In the acquisition phase, the solution that is able to meet the required operational capability and has the best operational benefit for the dollar spent is selected from a range of alternatives. Clear roles and responsibilities for all stakeholders are defined at every stage of the LCM process from acquisition to project implementation, system delivery, operations and support and finally to retirement of the system. The life cycle ends with the physical disposal of the weapon system at the end of its useful life. During the operations and support phase, the operational service life of the system may be extended to meet changing operational scenarios through mid-life upgrades and technology insertions.



Summary of the phases in LCM for a system

MINDEF's LCM – a Total System Approach to Capability and Cost

Key tenets to the LCM framework include the use of a total system approach and the LCC of a system.

In planning and acquiring a defence system such as a new fighter aircraft, the project team considers not only the performance of the new "prime" equipment (i.e. the fighter), but also how the equipment is to be utilised and supported in peacetime and wartime throughout its entire operational life. Considerations here will include an evaluation of the growth potential of the system for upgrades during its operational life, the involvement of in-country defence industry, and development and sustainability of in-country capabilities.

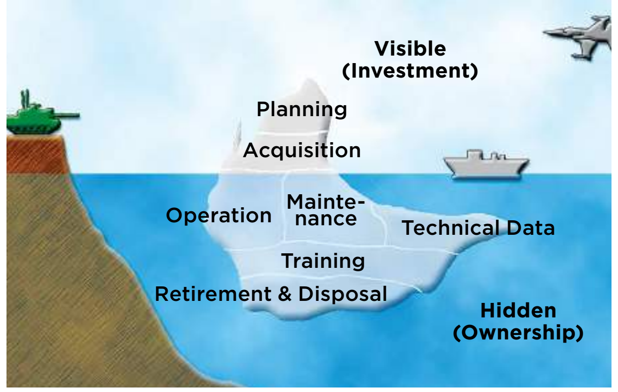
The LCM approach provides balanced focus among Reliability, Maintainability, Supportability (RMS) and technical performance throughout the acquisition activities. RMS are cost drivers and key parameters to system availability, mission success and sustainability. Highly reliable and maintainable systems will mean that the systems can be utilised for more mission sorties and there is less demand for technicians and other logistics burden, which in turn also helps to enhance mobility and survivability of the combat forces.

The LCM approach also demands a high degree of concurrent activities. Conflicting requirements from operations, logistics and engineering are traded off early, taking a long-term view using LCC. Requirements from operations, training, logistics and infrastructure development are systematically integrated into the contracts. While more time may be required during the system definition and tender evaluation stages because of wider coverage, we can catch up in the implementation and deployment stages and shorten the time taken for the overall cycle.

A system's LCC comprises the initial acquisition cost that covers the "prime" equipment, spares and support equipment, as well as the cost of operations and maintenance support throughout the system's life cycle (which can be 30 years or even longer). This is estimated based on projected operational usage, reliability data obtained from the OEM and field data from other major users. Finally, acquisition of a weapon system may require specific obligations from the purchasing country to the government of the exporting country with regard to the future disposal, transfer or resale of the system upon retirement.

Knowledge of the total cost for every major acquisition will facilitate proactive engineering efforts or contract initiatives to manage the cost drivers. For example, all high-cost items, including those that are required for future maintenance and supply support, could be exposed to competitive bidding to enhance value-for-money in our acquisition. In some cases, an increased expenditure upfront could help reduce the LCC.

The use of LCC ensures that there will be less hidden or unknown costs and thus avoid the potential hazard of "ice-berg" cost consequences. For a well-managed defence system with a useful life of more than 15 years, the future O&S cost can amount to around 60% of the system's LCC.



Total cost visibility requires oversight of the "hidden" costs

For an aircraft, the O&S phase would include heavy maintenance (typically known in the industry as maintenance, repair and overhaul or MRO), modifications and upgrades to meet changing scenarios, engineering support from the OEM, spare parts management and consumption, obsolescence management, reliability engineering to improve availability, and training. The O&S cost of an aircraft during its entire SLC can amount to around 60% of the system's LCC. It is thus a major chunk of the LCC and an important consideration of the project team when evaluating competing solutions.

Subsequent Improvements to MINDEF's LCM Framework

After its introduction, MINDEF's LCM framework continued to evolve and was strengthened with new methodologies.

Since 1993, the Analytic Hierarchy Process (AHP) has been in use for the evaluation and selection of all major systems to improve objectivity in evaluation. The use of operations analysis and M&S tools for tactical and campaign analyses have subsequently been incorporated as an enhancement to the AHP process. The approach of LCC also evolved into Total Cost of Ownership (TCO), to better reflect the total cost of owning a new capability that would include indirect costs.

Over the years, solutions to the SAF's operational requirements moved from off-the-shelf weapon system purchases to projects involving significant amount of customisation and projects that were highly developmental in nature. This led to a new project risk management methodology. Contractual requirements were enhanced to cover systems which are developmental in nature, where the risks are managed, where delivery schedules and performance parameters have some degree of flexibility and where critical milestones are catered for the SAF and DSTA to review the project and exit if it is clear that the desired system performance and operational capability will not be met.

Another key initiative is the implementation of system safety processes to enhance the safety of systems in the SAF. Safety is a core value of the SAF. The first Weapon Systems Safety Advisory Board was set up in MINDEF and the SAF in 1991 to provide impartial and independent advice to the SAF on the safety of its weapon systems. In the late 1990s, the SAF, together with the DMO, embarked on a journey to introduce the concept of system safety to further enhance its safety framework and this was formalised in 2005. With the experience gained from the implementation of the system safety process for the safety assessment of ordnance, munitions and explosives (OME), in 2006 MINDEF, the SAF and DSTA expanded the system safety concept to the safety assessment of weapon systems such as aircraft, ships and land fighting vehicles. Subsequently, the system safety methodology for MINDEF, the SAF and DSTA was formalised in 2010. Since then, all weapon systems and OMEs have been subjected to a rigorous process of system safety assessment prior to the systems being operationalised. The system safety assessments are also reviewed when there are major upgrades or changes to the operational profile of the weapon systems.

Overall, the MINDEF LCM framework ensured and provided a measure of value-for-money in all major acquisition of defence systems in MINDEF and the SAF. "Value" in the SAF's perspective is defined by operational capability, availability of the system and growth potential. "Money" is defined by the SLC cost.

Defence Capability Management

Strengthening the Management of Defence Capabilities

The adoption of the LCM framework from 1990 strengthened MINDEF, the SAF and DTC as smarter buyers, users and implementers for single systems. Nevertheless, several developments through the same period gave MINDEF the impetus to review and evolve the framework of LCM.

First, MINDEF had gone through several organisational reviews since the original LCM framework was formulated. These included the formation of new entities in the DTC[1], with substantial organisational re-structuring and consequently process changes. While each entity brought a strategic perspective and sharper focus on its respective areas of responsibility, the general trend towards decentralisation and specialisation had also given rise to new domain areas and some functional overlaps. A top-down review of the LCM framework would serve to clarify the related systems and processes for capability planning, delivery and sustenance in MINDEF and the SAF.

Second, there was an increasing pace of technological change. With greater competition and innovation, the life cycles of technologies were getting shorter, rendering systems obsolete faster than before.

[1] These included the corporatisation of DSO National Laboratories in 1997, formation of DSTA in 2000, Future Systems Directorate in 2003, and DRTech in 2006 respectively.

Networked and integrated capabilities had also become the norm because of the way technologies and warfare were evolving. These developments brought about complexities, which required the LCM to evolve in order to manage. For example, more networked capabilities and shorter life cycles would mean that the different phases of technology management had to be more integrated, and capability development planning had to be more holistic.

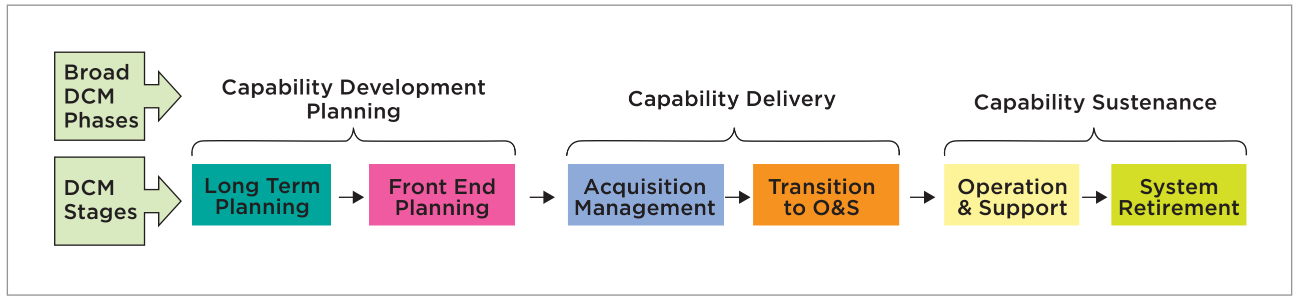
Third, the SAF had transitioned from a "platform-centric" force to a network-centric force via its Third Generation SAF transformation journey. This increased complexities with more interconnected systems and hub-like structures that the DTC needed to adapt to work with seamlessly. More high-end capabilities, often involving indigenous development, were also sought in the Third Generation SAF. The acquisition and use of military technologies from foreign sources also became more complex with tighter control measures in place to prevent the access to such technologies by unauthorised parties. Against this backdrop, issues of technology access, security and transition became increasingly important and thus required more focus in the LCM.

In 2010, a strategic review of the LCM framework was initiated to position it to meet future challenges of managing increasingly complex and networked weapon systems in the SAF, maximising coherence across the defence ecosystem and enhancing our ability to push the boundaries of technology. The review concluded that the existing LCM framework was fundamentally sound and functioning well, but could be enhanced to provide a more holistic capability-based framework. New paradigms and processes were needed to plan for and implement defence systems from the perspective of a larger capability and not just a single system, especially for complex and large-scale systems.

Defence Capability Management Framework

The LCM framework was thus expanded into the DCM framework to provide a more holistic framework framed in three phases: Capability Development Planning, Capability Delivery and Capability Sustenance. This would be enabled by a systematic and coordinated management process, with a clear demarcation of responsibilities by relevant parties and well-defined decision points.

The Capability Development Planning phase involves the conceptualisation of the broad defence capabilities required to fulfil the SAF's missions and the strategies to develop such capabilities over a certain time horizon. In the Long-Term Planning stage, the focus is at the capability level, with outputs such as force-level operational concepts and the corresponding SoS architectures and capability development master-plans. In the Front-End Planning stage, the details of individual systems that compose a defence capability of interest are examined, with outputs such as their operational requirements and the broad implementation approaches.



Broad Phases and Stages of Defence Capability Management

The Capability Delivery phase involves the execution of the implementation approaches to deliver the required defence capabilities to the SAF. In the Acquisition Management stage, the approved operational requirements are translated into engineering specifications, followed by the selection of the most cost-effective solution to meet these specifications. Following the implementation of the selected solution, the Transition to O&S stage marks the start of the transition of the implemented solutions into operational capabilities as the SAF begins to operate the new defence systems and equipment.

The Capability Sustenance phase involves the sustenance of the delivered capabilities to ensure a high state of readiness and performance. Systems may be upgraded periodically, when necessary, to maintain their relevance. Finally, systems that are obsolete are disposed of expeditiously so as to free up resources to manage replacement or new capabilities.

The DCM manual, which codifies the DCM framework, officially replaced the LCM manual in 2012. It comprises two parts. The DCM System specifies the "what", "why" and "who". The DCM Guide provides the "how" in the form of detailed guidance, techniques and methodologies.

Operations Research

Background

The modern field of operations research (OR) or operations analysis[2] arose during World War II (WWII). Because of the war effort, there was an urgent need to allocate scarce resources to the various military operations and to the activities within each operation in an effective manner. Scientists in the United Kingdom and the United States looked for ways to make better decisions by applying a scientific approach to solve problems in areas such as logistics, operations planning and training schedules.

Some of the diverse problems studied by the OR groups during WWII included search patterns to be employed against submarines, protection of merchant ships, strategic bombings effectiveness and survivability, and evasive actions to be taken by a ship under kamikaze attack. The efforts of the OR groups contributed to the winning of the Air Battle of Britain and the Battle of the North Atlantic.

Story 1: What is the Real Objective, the Right Measure-of-Effectiveness?

Early in WWII, a great number of British merchant vessels were sunk or seriously damaged by Axis aircraft attacks in the Mediterranean. The answer was to equip these ships with anti-aircraft guns and gun crews.

*This was done at great expense of men and equipment, badly needed elsewhere. Questions concerning the soundness of this allocation of scarce resources were raised when reports showed that the gun crews were shooting down **only 4%** of all attacking aircraft. This was poor showing!*

Question: Were the anti-aircraft guns and crews worth the cost of installation?

*On careful consideration, it was realised that the guns were not there primarily to shoot down German or Italian aircraft. Their objective was **to protect the merchant vessels.** And in fact, as figures accumulated, it became apparent that the anti-aircraft guns and crews were doing the job rather well! Of the ships attacked, **25% of those without protection sank**, while only **10% of the ships with protection were lost.***

[2] Operations Research, also known as Operations Analysis, is a discipline that entails the application of scientific techniques and quantitative methods to improve decision-making.

Story 2: Where to apply armour?

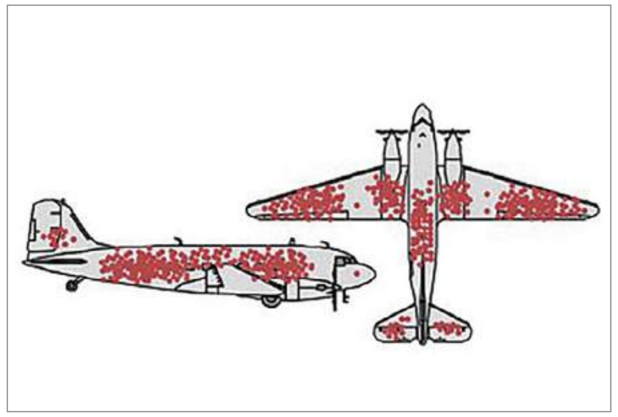


Illustration of analysing damage to bomber aircraft due to Anti-Aircraft guns

During WWII, the Royal Air Force lost many planes to German anti-aircraft fire, so they decided to armor them up. But where should the armour be put? The obvious answer was to look at planes that returned from missions, count all the bullet holes in various places, and then put extra armor in the areas that attracted the most fire. Obvious but wrong. If a plane makes it back safely even though it has, say, a bunch of bullet holes in its wings, it means that bullet holes in the wings aren't very dangerous. What you really want to do is armor up the areas that, on average, don't have any bullet holes. Why? Because planes with bullet holes in those places never made it back. That's why you don't see any bullet holes there on the ones that do return.

Some of the primary tools used by operations analysts are statistics, optimisation, stochastics, queuing theory, game theory, graph theory, decision analysis, and simulation. Because of the computational nature of these fields, OR also has ties to computer science, and operations analysts regularly use custom-written or off-the-shelf software. A large amount of computation is usually required to solve the problems considered by OR. As such, the rapid advancements in computer technology in the last few decades have given a tremendous boost to OR. Problems, which would have required the use of a mainframe three decades ago, can now be solved on a personal computer.

This new science is known as "operational research" in the United Kingdom and as "operations research" in most other English-speaking countries, though OR is a common abbreviation everywhere. It is the discipline of applying advanced analytical methods to help make better decisions[3]. Within the UK military and UK Ministry of Defence, the term "operational analysis" is used instead as OR stands for "Operational Requirement". The practitioner is commonly called an operations analyst. With expanded techniques and growing awareness, OR is no longer limited to only operations, and the proliferation of computer data collection has relieved operations analysts of much of the more mundane research. But the operations analyst must still know how a system operates, and learn to perform even more sophisticated research than ever before. In every sense the name OR still applies, more than a half century later.

Operations Research in MINDEF – 1970s

Prof Lui Pao Chuen said in his acceptance speech when he was conferred "Honorary Fellowship of the OR Society of Singapore" on 12th November 2000:

"Our first OR analyst, Captain Henry Cheong was sent to learn about OR in UK in 1968. He learnt by doing apprenticeship at the Defence Operational Analysis Establishment (DOAE). We were all ready to apply OR to force planning and equipment selection decisions on his return. In 1971, Naval Postgraduate School (NPS) in the US was identified to be the best school for military OR training. I was the first to be sent to NPS. In 1972, two more staff (Lee Kheng Nam and Lim Lay Geok) were sent to NPS to read OR. Major Henry Cheong also went to NPS in 1973. By 1975 we had four NPS graduates in OR. But we were not yet ready for OR! We never got to set up the OA Department that we were sent to NPS for. "Tyranny of the Urgent" made all of us project managers on our return. The dilemma was that we needed good analysts and we also needed project managers with the same stock of high quality staff. As project management was more important OR had to be sacrificed. It was very difficult to do OR in the 1970s. There was no time, no data and no manpower. There was no user to work with, and decision makers had no patience for OR. Qualitative arguments were the norm. Minister did OR in his head and wondered why the analysts were so slow to understand."

Dr Goh Keng Swee, Singapore's first Minister for Defence, was pointing out the lack of rigour and discipline in applying OR or systems thinking in problem solving. In 1975, he created a new designation – SPD – and then LTC Lui Pao Chuen was appointed to the role. His job was "to Dream, to Deliberate and to Do" if Dr Goh decided to implement the project. The areas of focus were Air Defence, Command and Control, and Air Force Infrastructure. Examples of applications of OR by the SPD were in:

- OA Study on detection of ground targets by pilots and probability of destroying targets with fighters, which led to replacement of the operational solution of "Close Air Support" by "Battlefield Air Interdiction" for increased effectiveness of air support for ground operations
- OA Study on probability of survival of ground targets with dispersion, camouflage, deception and hardening which led to the conclusion that passive defence was the most cost-effective solution to enemy air attacks to minimise investment in SAM
- OA Study on reliability of Bloodhound SAMs which demolished the argument for replacing the Bloodhound

The A-4 — an example of a fighter capable of providing air support for ground missions

The Bloodhound SAM

[3] From INFORMS based on "Operations Research: The Science of Better"

Operations Research in MINDEF – 1980s

OA grew in the 1980s. In 1983, then COL Lui Pao Chuen (and later, Chief Defence Scientist) established the Operational Analysis Department (OAD) within the SAF's Joint Operations and Planning Directorate (JOPD), after pioneering initial OA work for the SAF.

An Operations Analysis Branch (OAB) was also set up in the DSO (which was later renamed DSO National Laboratories) to specialise in M&S of weapon systems in an operational environment. One of the first projects of OAB was the development of a simulation model to compare the performance of different weapon systems under a variety of scenarios to support the RSN's missile corvette acquisition programme. OAB grew in DSO to become Operations Research Laboratory (ORL) in 1988.

In 1986, COL Lui Pao Chuen became MINDEF's first Chief Defence Scientist (CDS). JOPD's OAD and a small OR section from DSO were amalgamated into CDS' Office (CDSO) to become CDS' OA arm.

As military OA M&S was not a widely applied field in Singapore, operations analysts were sent for formal training in military OA theory and applications at, for example, the Royal Military College of Science, UK. Military OA specialists from overseas were also enlisted to build up the expertise of the analysts rapidly.

Operations Research in MINDEF – 1990s

In 1990, it was decided that OR would be more effective, when the OR capability resided with the SAF users. Thus, OAD was decentralised into the Army OA Branch with G5, the Air Force OA Branch with Air Operations Department, and the Naval OA Branch reporting to Chief of Staff, Naval Staff. At the same time, an OA outfit was formed in DMO to apply OA during the acquisition and support of systems. There was also the Joint OA Branch (decentralised to JOPD in 1995), MINDEF OA Branch, and Combat Modelling Branch. The OA outfits were later consolidated into today's three OR groups in DTC consisting of SAF OR Office in Joint Plans and Transformation Department to apply OA in force structuring and capability planning, DSO ORL to apply OA to guide R&D and Centre for OR in DSTA to apply OA in SA and acquisition. The OR community has grown from four analysts to about 80 analysts today.

The demand for OA studies grew, and in order to achieve better results, OA M&S took on increasing sophistication with higher resolution and speed. The models of weapons systems and combat platforms increased their depth of performance details, requiring more detailed engineering studies of the relevant weapons and combat platforms. One example is the study of anti-armour weapons equipped with shaped charge warheads, deployed against armoured vehicles.

The simulation of the combat interplay between weapons and targets became more complex with the incorporation of tactics and counter-actions undertaken by each side. As a result, the more sophisticated M&S started to converge with other simulation applications. The simulated combat interaction among forces at different levels also took on increased breadth. For example, for campaign level scenarios, different land, naval and air units under various force structures were made to undertake different missions, employing different weaponry and platforms. Operations analysts used such simulation techniques to analyse the results of various combat strategies and tactics.

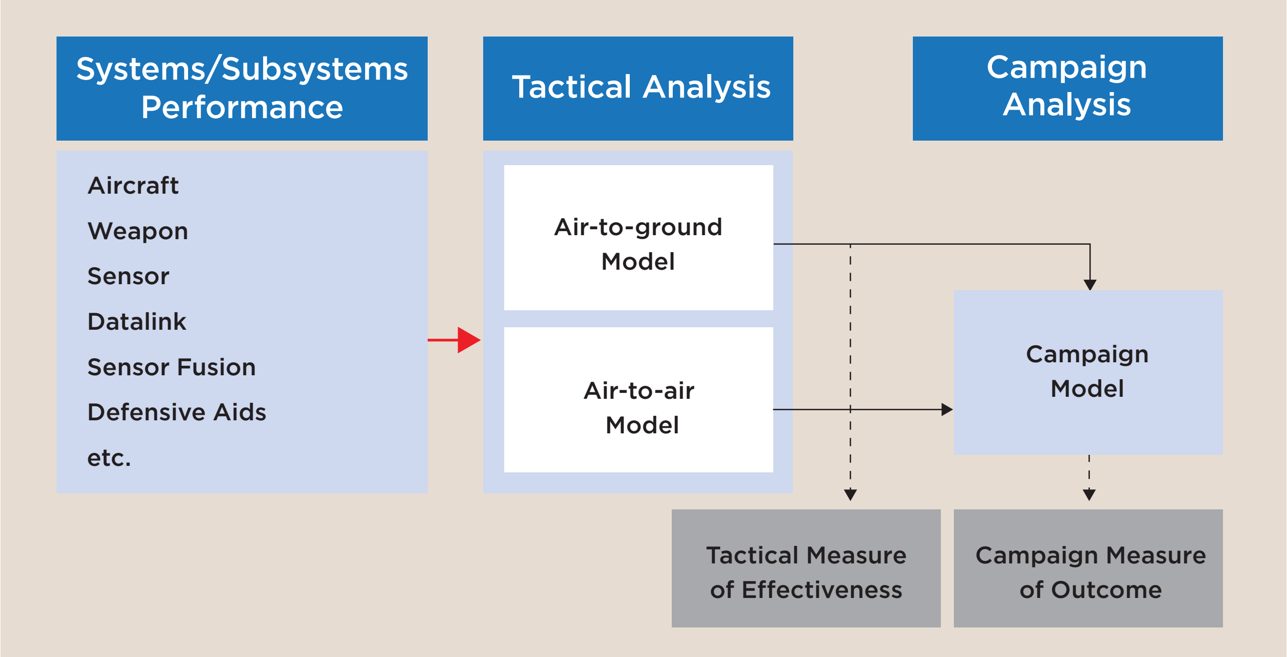


Illustration of a framework to apply OR to evaluate competing fighter aircraft candidates during the tender evaluation process

Operations Research in MINDEF – 2000s

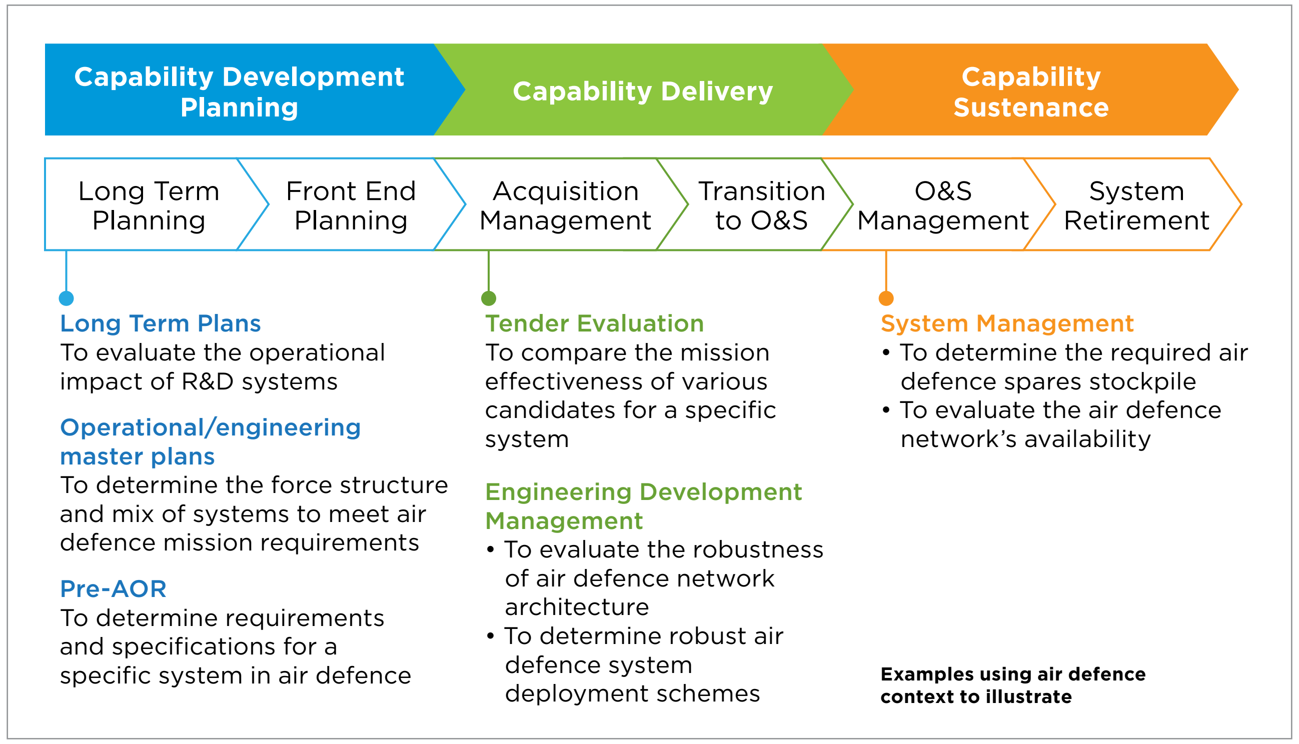
The use of OR grew to encompass the evaluation of major SAF platforms and systems. The first use of OR at the turn of the millennium was on the attack helicopter evaluation. The application of OR with M&S to model each potential candidate in mission enabled the project team to assess each one based on operational effectiveness.

The Next Fighter Replacement Programme (NFRP) is an example of how OR studies supported acquisition programmes. Under the NFRP, the RSAF intended to acquire a new multi-role fighter jet to replace the ageing A-4SU Super SkyHawks.

Operations Analysts from DSTA, DSO and the RSAF collaborated and worked with technical Subject Matter Experts (SMEs), operational planners and RSAF fighter pilots in the modelling and analysis to assess the candidate aircraft, which eventually led to the selection of F-15SG. Air-to-air combat and air-to-surface models enabled the detailed study of combat capabilities of each NFRP candidate's different aircraft configurations, mission roles and game plans in current and projected combat environments. These tactical fight outcomes were aggregated and used in a campaign level simulation model to determine and compare the relative contribution of each NFRP candidate to the overall RSAF mission.

Critical infrastructure vulnerability assessment (CIVA) also has its roots in the military OA capability in DSO. OA analysts applied these Modelling Simulation and Analysis methodologies and tools to model the interdependencies in our critical national infrastructures, so as to study issues of national security centred around critical infrastructure protection. CIVA activities have been applied in pandemic modelling, maritime trade-lane study, electrical facility study, internet infrastructure study, power grid studies, and oil/gas supply chains modelling. It contributed to the build-up of a trusted, in-country expertise that can rigorously assess risks to Singapore's national infrastructure in all sectors.

Application of OR has grown to be used in any phase of the DCM Framework.



Capability Development Planning

Capability Delivery

Capability Sustenance

Long Term Planning

Front End Planning

Acquisition Management

Transition to O&S

O&S Management

System Retirement

Long Term Plans
To evaluate the operational impact of R&D systems

Operational/engineering master plans
To determine the force structure and mix of systems to meet air defence mission requirements

Pre-AOR
To determine requirements and specifications for a specific system in air defence

Tender Evaluation
To compare the mission effectiveness of various candidates for a specific system

Engineering Development Management
- To evaluate the robustness of air defence network architecture
- To determine robust air defence system deployment schemes

System Management
- To determine the required air defence spares stockpile
- To evaluate the air defence network's availability

Examples using air defence context to illustrate

Possible areas to apply OR in DCM phases

Modelling and Simulation

Background

The impetus for using M&S systems in many armies has traditionally been driven by the need to overcome various constraints, such as the lack of training areas, rising costs in conducting actual training and the fact that equipment for training is sometimes unavailable. For the SAF, the situation is no different.

In fact, the SAF faces even more acute constraints in resource-scarce Singapore. After all, the "little red dot" measures just approximately 700 square kilometres, faces falling birth rates and has had to grapple with challenges such as the Asian financial crisis, the "dot-com" bust and the SARS epidemic.

What better way to overcome these constraints than to employ M&S technologies to conduct training in virtual space? With M&S technologies advancing by leaps and bounds over the last decade, such a solution is not only increasingly viable as a key strategy for the SAF; it has also become strategically advantageous, enabling the SAF to turn constraints into strengths.

Besides simply increasing the opportunities for training and enhancing its quality and realism, the SAF has also harnessed the power of M&S for purposes beyond training. Specifically, the technology has been capitalised on for operations such as mission planning and rehearsals, decision support, and for test and evaluation purposes.

Arising from the need to transform the SAF to meet new challenges in the battlefield of the future, M&S has also become an essential driver and indispensable technology for military experimentation in the support of force transformation.

The First Wave: The Embryonic Years (1980s to early 1990s)

The SAF's first foray into M&S began in the early 1980s. This era of standalone simulations was fuelled by the emergence of graphics and Image Generator (IG) technologies, which developed in tandem with the advancement in computer and display technologies.

The maturity of two-dimensional (2D) graphics enabled the development of the shore-based Tactical Training Centre for the RSN. Tactical scenarios were simulated and presented in monochrome 2D graphical symbology to train ship commanders in various tactical decision-making situations. Soon after, 3D IGs began to emerge. For the first time, the real world could be replicated graphically in a synthetic 3D environment to a degree of realism acceptable for training.

This quickly led to the development and delivery of various types of flight simulators for the RSAF to train pilots for its fleet of A-4S and F-5Es, as well as the AS332 and AS550 helicopters.

For the Army, the Artillery Fire Control Training System (AFCTS) was the first training system. Delivered in 1983, the AFCTS was used to train forward observers in call-for-fire and artillery ranging procedures. The system comprised a projection system made up of 11 slide projectors to simulate and display the delivery and impact of artillery fire.

The principal technology driver of this first wave of M&S systems was the emergence of Graphics and IG technologies.

Typical 3D image generated by IG

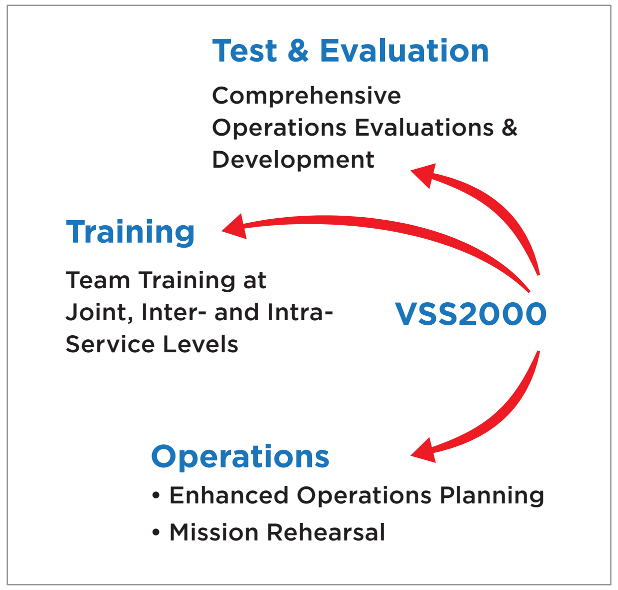
The first wave can be characterised by the deployment of simulators, which were generally standalone and single-purpose. Most were focused on honing the psycho-motor skills of individual operators such as gunners and pilots prior to "live" training.

The Second Wave: The Fledgling Years (Mid 1990s – 2000)

The M&S industry matured considerably in the 1990s – the second wave. Spurred by the advent of broadband networking, "Distributed Networked Simulation" was the rallying call, and the focus shifted rapidly from standalone training to team training and joint or integrated warfare training.

The global simulation industry responded with great enthusiasm. New technologies and concepts soon emerged, enabling geographically separated simulators to be networked for joint training in common synthetic environments, as if they were a single simulator. It was this era that gave birth to distributed simulation protocols. In addition, Computer-Generated Force technology progressed, facilitating intelligent automated behaviour of simulated entities that reduced the need for large teams of exercise support personnel to "move the pieces".

Recognising the immense potential of M&S, the SAF formulated and launched a major programme called the Vision for SAF Simulation 2000 (VSS2000) in 1995 to capitalise on the rapid M&S technology advancement. VSS2000 envisaged the strategic use of SAF simulators in three dimensions – Joint Training, Operations, and Test and Evaluation (T&E). The main emphasis was on joint training through integration at both the systems level, i.e. simulation-simulation and simulation-operational systems integration, and the Services level.



Test & Evaluation

Comprehensive Operations Evaluations & Development

Training

Team Training at Joint, Inter- and Intra-Service Levels

VSS2000

Operations

- Enhanced Operations Planning
- Mission Rehearsal

VSS2000 Thrusts

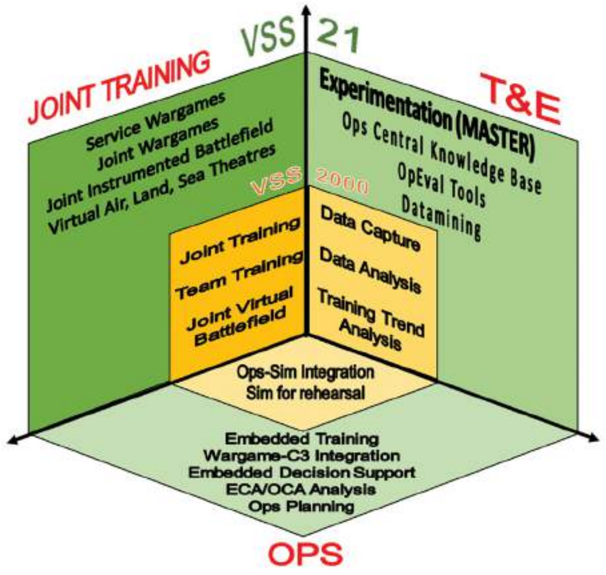
The second wave saw the transition from standalone simulation to distributed, networked simulation in common synthetic environments, aided by advances in networking technologies. During this period, the SAF also implemented many flagship simulation systems, and pioneered new M&S concepts such as "plug-and-play", "simulation-C2 interoperability", and "embedded simulation".

The Third Wave: Soaring to Greater Heights

In the new millennium, the SAF was on the threshold of another wave of M&S evolution. The SAF and DSTA unveiled VSS21, a new M&S masterplan in January 2001. VSS21 continues to be anchored on the three thrusts established in VSS2000. However, the key objective of VSS21 is to exploit M&S for the purpose of force development and modernisation through experimentation under the Test and Evaluation (T&E) dimension.

M&S-based experimentation serves as an objective platform to provide the digital probing ground for testing and experimentation of new warfighting concepts to meet the requirements of the 21st century.

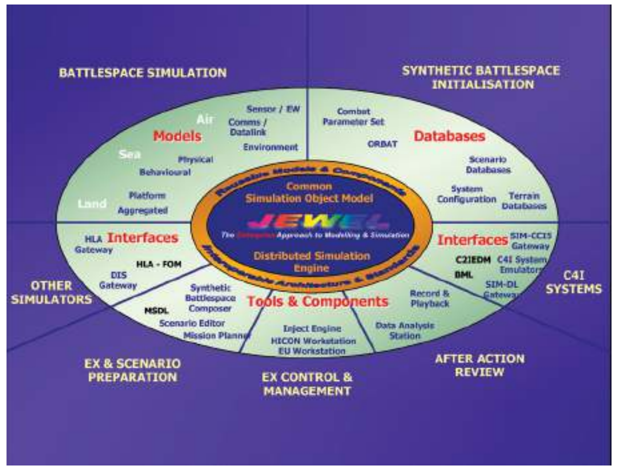
New concepts and technologies can be appropriately "modelled" and represented in simulation for experiments configured and conducted in a "Synthetic Theatre of War". Such capability also permits inexpensive evaluation of innovative concepts and technologies to determine their operational utility and payoffs prior to development, fielding and implementation.



VSS21 Thrusts

Experimentation using M&S

Underlining the importance of M&S-based experimentation, the SAF set up the SCME in November 2003. Dubbed the "key to the SAF of the future" by Minister for Defence Teo Chee Hean, the SCME would leverage M&S technologies and tools to conduct experiments on new warfighting concepts and innovative technological capabilities.



JEWEL Framework

An initiative to promote the reuse of M&S models and components is the JEWEL (Joint M&S Environment for Wargaming and Experimentation Labs) framework, which is a means to attain composable simulations for the SAF.

Coming of Age

M&S in the SAF has advanced tremendously over a short span of time. From pioneering implementation by pushing the edge through two decades of innovation, the SAF entered another evolution in the new millennium.

M&S in the SAF has matured to be a key enabling technology for the Third Generation SAF and its transformation efforts.

Evaluation Methodology

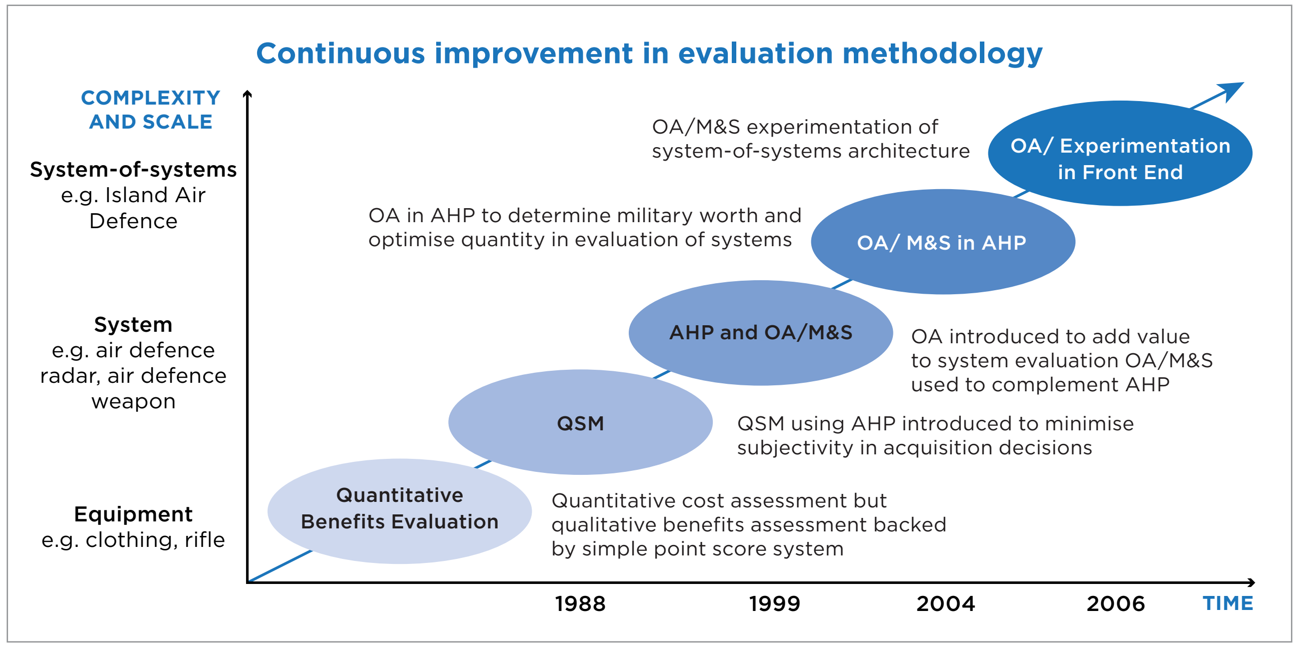
Evolution of Evaluation Methodology to Support System Acquisition

This timeline depicts the evolution of our evaluation methodology.

Equipment and systems we acquire became more and more complex, as the SAF's capability advanced over the years. We adopted more and more sophisticated methods of evaluation. These progressed from qualitative evaluation and lowest cost methods to quantitative selection methodology (QSM) and AHP to OA M&S.

Before QSM – Buying Products

In the early days, equipment evaluation was based on the traditional government procurement guidelines to acquire based on the lowest price. We bought what we could afford. Then, most equipment (rifles, clothing,


Continuous improvement in evaluation methodology
COMPLEXITY AND SCALE
System-of-systems
e.g. Island Air Defence
System
e.g. air defence radar, air defence weapon
Equipment
e.g. clothing, rifle
Quantitative Benefits Evaluation
Quantitative cost assessment but qualitative benefits assessment backed by simple point score system
QSM
QSM using AHP introduced to minimise subjectivity in acquisition decisions
AHP and OA/M&S
OA introduced to add value to system evaluation OA/M&S used to complement AHP
OA/ M&S in AHP
OA in AHP to determine military worth and optimise quantity in evaluation of systems
OA/ Experimentation in Front End
OA/M&S experimentation of system-of-systems architecture
1988
1999
2004
2006
TIME

Evolution of evaluation methodology to support system acquisition and the increase in complexity over time etc.) requirements were very straightforward. It was easy to determine if they were met.

QSM and AHP to evaluate systems

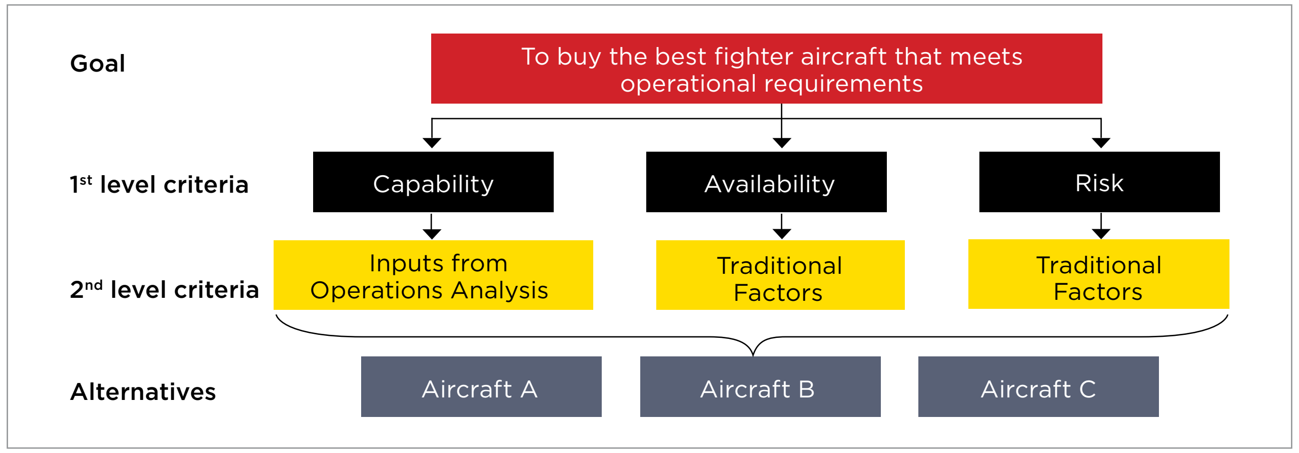
In 1988, MINDEF approved the QSM for the acquisition of weapon systems in MINDEF so as to minimise the subjectivity of selection. It formalised the concept of value-for-money in the evaluation of systems. QSM used the AHP for benefits assessment. After a few years of implementation, a review was conducted. It was recognised that the AHP methodology provided a structured framework for making acquisition decisions, a significant improvement over a previously ad hoc environment. Since 1993, it has become a tradition to apply the AHP method to high-value acquisition projects that involves competition.

Enhanced with OA/M&S

In the late 1990s, we began to use OA and M&S to complement AHP, as part of QSM. The key benefit of OA/M&S lies in its ability to represent and integrate both engineering and operational factors together, play out their interactions and dynamics, and produce measures of effectiveness (MOE) which are operational performance indicators for the military worth of each system's candidate. As we became more and more confident, we moved a step further to use OA/M&S as the sole means to assess the capability of candidates.

Applying OA to complement AHP has resulted in an enhanced AHP framework. In this enhanced framework, the capability branch under the first level criteria of the AHP tree is evaluated using OA techniques. The traditional factors such as payload, maneuverability and survivability have been replaced with tactical and mission analysis. Tactical analysis can help to assess the military worth of a candidate system and its capability in an engagement level, while mission level analysis helps to assess the force level contribution. The key benefit of this approach is its ability to consider both engineering and operational factors in a dynamic scenario to produce the MOEs that serve as indicators of military worth for the various alternatives.

DSTA has been using the enhanced AHP Methodology to evaluate weapon systems and platforms such as the F-15SG Eagle, Apache Longbow Helicopter and the Formidable-class Stealth Frigate. The enhanced AHP framework brings better clarity and appreciation among all stakeholders and decision makers on each candidate system's contribution, should it be selected, to the SAF's success in specific operational missions.



The Enhanced AHP Modelling Framework

Synergistic effects of a networked sensor, weapon and platform capabilities of a candidate system stood out strongly. Similarly, standalone weapon systems and platforms that offered limited or no integration with the SAF networked SoS resulted in less military utility in an operational context. It also offered insights into potential weak links in systems design, rules of engagement and supportability issues. For example, leveraging a platform with high endurance may result in more onboard systems failure and unexpectedly lead to poorer mission effectiveness.

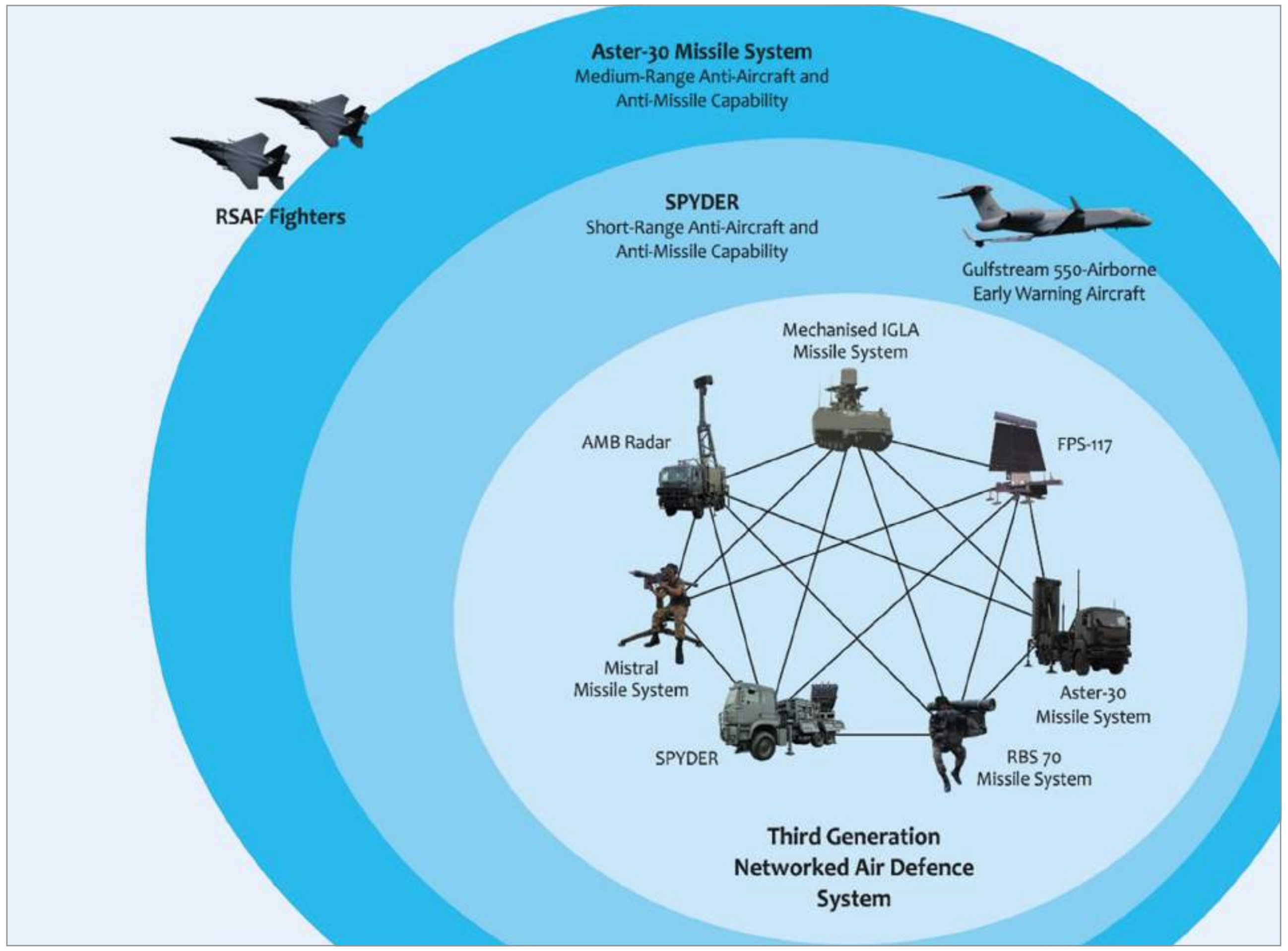
Going Front-end to Evaluate SoS

The transformation of the SAF to exploit rapidly emerging technologies and concepts has been a strategic imperative for the Third Generation SAF. This led to changes in organisation of forces, with more emphasis on less visible technologies such as information systems, precision weapons, unmanned platform technologies. SoS capabilities (e.g., the networked IAD SoS) would be the result. Front-end design and evaluation of the SoS architecture is part of the process. Compared to a fighter, the networked IAD SoS is much more complicated.

Large Scale Systems Integration

Background and Motivation

One of DTC's strategies in capability development for the SAF is to exploit the international defence materiel market and acquire what we require off-the-shelf. As the SAF progresses in response to changing demands, its operations have become more integrated and complex. Available solutions and systems from leading defence systems


Aster-30 Missile System
Medium-Range Anti-Aircraft and Anti-Missile Capability
RSAF Fighters
SPYDER
Short-Range Anti-Aircraft and Anti-Missile Capability
Gulfstream 550-Airborne Early Warning Aircraft
Mechanised IGLA Missile System
AMB Radar
FPS-117
Mistral Missile System
Aster-30 Missile System
SPYDER
RBS 70 Missile System
Third Generation Networked Air Defence System

The RSAF's Networked IAD SoS unveiled in 2013 houses thus may not meet its unique requirements. It is known that weapon systems from these systems houses are developed and funded (partially or fully) by their own armed forces, so their design optimisation and operating environment would not be the same as what the Third Generation SAF needs.

The DTC has thus developed the much needed competency to manage and perform large-scale systems integration programmes as well as secret-edge defence R&D capabilities. This is a key competitive advantage of MINDEF. DSTA is able to procure the best-of-breed systems, leverage experience and competencies from the larger DTC and integrate these acquired systems to meet the SAF's unique operational requirements. The insights into broader SAF mission needs and know-how to perform systems integration also enables DSTA to optimise the performance of the integrated combat systems at a higher level. Being a MINDEF statutory board, DSTA has developed a good reputation in safeguarding sensitive technical information shared by collaborators and system suppliers. Defence contractors are more willing to share technologies with DSTA and provide support in integrating their systems indigenously since DSTA is not in direct competition with them.

Building Up Phase (1980s – 1990s)

The DTC journey for the competency build-up for large-scale systems integration started with a naval platform programme in 1985 – the MCV. Due to the lack of critical experience in leading and managing advanced systems integration, MINDEF engaged established foreign consultants to support operational planners in the front-end requirement studies and programme definition. The RSN and DTC members participated in these studies to learn about the operations and technical trade-offs.

The MCV building programme was the RSN's second strike craft after the Missile Gun Boats. The new warships were to be equipped with modern and sophisticated combat systems sourced from various suppliers performing dedicated functions. They included the Surveillance Radar System from Sweden, Fire Control Radar from Israel, Anti-Ship Missile System from the USA and Towed Array Sonar from France. In order to ensure that they could perform as an integrated combat suite with flexibility and optimum performance, MINDEF needed a technical team with the specific expertise and technical management experience to lead the systems integration. A leading American systems house was appointed as the Systems Integrator (SI) which was supported by technical staff from Singapore Electronic & Engineering Limited (SEEL, which subsequently became ST Electronics).

Due to the sensitive nature of some combat systems such as the Fire Control System, Point Defence Missile System and Electronic Warfare System, the release of sensitive technical information to a non-Singaporean SI was not possible and technical data sharing was heavily regulated. This was one lesson learned – that such restrictions would severely limit the ability of the SI to perform and optimise the overall systems integration. The involvement and participation by ST Electronics and DTC's PMT members in the systems integration work was essential for the transfer of systems integration knowhow (methodology and process) to ST Electronics. The DTC was only marginally able to exploit this opportunity for learning, principally due to the nascent stage in its build-up – MINDEF just did not have enough engineers for the myriad of technology projects in the midst of an urgent capability build-up of the SAF. Despite the limitation, this marked the beginning of a systematic build-up of local capability in the combat systems integration domain.

With the experience gained from the MCV programme, DMO took over the main role of the top-level systems integration design for the Mine Countermeasure Vessel (MCMV) programme. The Swedish company Karlskronavarvet (KKrV) was subsequently engaged to manage the MCMV programme as a turn-key project. The decision to go for a turn-key programme was a deliberate one. The DTC with its young cohort of engineers was unable to cope with multiple large-scale programmes initiated by the SAF. To continue the build-up of SI capability, a group of engineers from DMO was sent to KKrV, working closely together with the professionals in the integration and testing of the systems.

Maturing Local Systems Integration (1990s – 2000s)

The experience of working together with the experts as well as its involvement in the MCV and MCMV programmes provided DMO with valuable expertise and confidence to take up the SI role in subsequent naval programmes. The acquisition of 12 new Patrol Vessels (PV) was the next programme that came along. In 1991, it was decided that the SI role for the PV programme was to be taken up by DMO. From the local industries, ST Electronics also participated in the work by contributing technical personnel to perform the Installation, Checkout, Integration and Testing (ICIT) activities. Using the PV programme as the capability development platform, DMO worked out the SI design activities and built up an archive consisting of the SI Handbook. The SI Handbook captures the essential planning, design, management and testing activities, systems engineering process and procedures, as well as when and how such work should be carried out. Different software tools were also acquired to aid in the design work. In the current era, many of these tools have been replaced by more sophisticated and capable alternatives.

Having successfully led the SI effort of the PV programme, the team from DTG led by DMO embarked on another RSN ship building programme, this time a much bigger ship – the LST. Adopting a similar approach, the Defence Technology Group (the DTG later formed the main constituents of the MINDEF statutory board – DSTA) undertook the design of the platform and integration of combat systems with the local defence industries and assumed total programme responsibility. These vessels were developed and built entirely locally, signaling DTG's achievement and maturity in building up the systems integration capability over the decade from the MCV and MCMV programmes.

Dr Tony Tan, then Deputy Prime Minister and Minister for Defence summed up the achievement at the Commissioning Ceremony of RSN Patrol Vessels in September 1996 and then in March 2000, for the Landing Ship Tank (LST), RSN's largest class of naval vessels.

"The Patrol Vessel Programme uses innovative new technology to ensure combat effectiveness with manpower efficiency. The success of this programme is a strong testimony of the maturing of our Defence Industries and the Defence Technology Group.... These ships are also the first to have their combat systems fully integrated, checked out and tested by the Defence Technology Group and Singapore Technologies..... Finally these ships are the first to have locally developed command and control and integrated communication systems and are the first warships in the region to be equipped with waterjet propulsion. All these achievements highlight the ability of our local defence technology capability to design, build, integrate and deliver sophisticated warships and weapon systems to the SAF."

"....I wish to take this opportunity to commend and congratulate the team from the RSN, Defence Technology Group and Singapore Technologies for the successful management and implementation of this LST project. The LSTs, equipped with modern combat systems fully integrated and

tested by Singapore Technologies and Defence Technology Group, are testimony to the ability of our local defence industry to deliver sophisticated warships and combat systems to the Singapore Armed Forces....."

Strategic Value Add – Large-Scale Systems Integration (2000s and beyond)

MINDEF launched the RSN Frigate Programme at the turn of the century in early 2000 to replace the aging Missile Gun Boats. It was the most complex naval development and systems integration programme undertaken by DSTA. More than 15 major contracts were awarded to local and foreign suppliers for the design, development, integration and testing of the various platforms and combat systems. DSTA took the full responsibility to ensure proper integration of the combat systems to the platform to meet the RSN's operation requirements. The challenges involved incorporating state-of-the-art stealth technologies to manage radar, infra-red, visual, acoustic and magnetic signatures. In addition, there were also demands to venture into unknown territories that were "uniquely Singapore". With manpower constraints, lean manning and the use of highly integrated automation systems were also key requirements. The RSN desired to have a crew of about 71 to operate the frigate. Many navies typically used about double the number for the same class of vessel.

Integrated Project Management Team

The acquisition of the frigates came at the time where the different defence acquisition organisations such as DMO, CSO and Lands and Estates Organisation (LEO) were being re-organised. In 1995, they were consolidated at the Defence Technology Towers and subsequently DSTA was formed in 2000. The re-organisation and the impending technical challenge of the programme sparked the formation of Integrated Project Management Team (IPMT) with engineers from different technical domains working very closely under a single team structure to deliver the desired operational capabilities. Instead of a system-centric approach, engineers from sensor, network, C2, and guided weapon domains collaborated to work together according to operation-centric requirements such as Anti-Aircraft, Anti-Ship Missile defence.

Scenario Requirement Analysis

Having an IPMT facilitated the analysis of the requirement and the system implementation from an end-to-end perspective. In the Frigate Programme, DSTA introduced the process of Scenario Requirement Analysis where the IPMT and the user worked closely together to describe how all systems in a particular scenario (e.g. Anti-Air Warfare) should work together. Every stage of each warfare scenario, from detection, tracking, weapon designation right up to engagement, was examined and the technical requirements for each system to fulfil the scenario were documented. The output was a Scenario Requirements Document (SRD) for each scenario. The SRD was used to derive the system specifications of a system as well as interface specifications between systems. It was also used in the later stage of the programme to work out the test cases to validate the various warfare scenarios.

Integration Management

One of the success factors learnt from the previous programme was to have good integration management. Integration Management involves the management of all project tasks related to the systems integration. This includes scheduling, rescheduling of activities, resource planning and performing critical path analysis. Over the years, DSTA has also established efficient work processes and technical templates to document and iterate its integration design painstakingly. It also involves a systematic approach to develop interface specifications and test protocols to validate the integrated system performance, providing repeatability and quality assurance. These would prove critical as platforms mature and require specific system upgrades. The captured information would allow a partial change of a component of the integrated suite without the need to overhaul it entirely.

Progressive Testing Regime

It was very important for integration design problems to surface and be corrected early in the programme before they snowballed and became unmanageable. In the Frigate Programme, DSTA adopted a progressive testing regime by increasing the depth of integration at each stage. The first integration test was the Preliminary Integration Test (PIT) which aimed to verify the integrity and correctness of the interface specifications and to weed out problems that might have been caused by misinterpretation of syntax and semantics.

The next major integration test was the Shore Based Integration Test (SBIT) which was conducted in the Shore Based Integration Centre (SBIC) housed in Changi Naval Base. The SBIC is a dedicated set-up using actual combat systems constructed to perform combat systems integration tests. To minimise cost, the programme did not acquire additional sets of combat systems for the integration tests. Instead, the first set of combat systems was used and kept at the test centre and eventually transferred for use on the last frigate.

The SBIT was done in two stages. The first stage was the pairwise integration testing. It complemented the PIT that was performed earlier. While simulators or prototypes were used in PIT, this test validated the interface between the actual hardware. The complete systems also allowed the verification of response time, update rate and message sequencing which was not possible in the PIT. After the pairwise integrations were checked, the next stage was Scenario Integration Testing. The objective of this test was to verify the functional integration at the individual warfare scenario level (e.g. Anti-Air Warfare) and multi-scenario level. For each scenario, the complete sequence of actions was tested from detection of targets, tracking, command and control, designation to weapon station, to final engagement of target. One other key point is with the extensive use of simulation tools. This had greatly facilitated the testing of complicated tactical scenarios that are difficult to perform out at sea, such as validating maximum target handling capacity, complicated flight profiles, network loading and endurance tests.

Engineers at work at SBIC

With the SBIT completed, the focus was placed on the ICIT on board the ship. Sets of tests similar to those during SBIT were done to ensure the performance of the systems in the actual configuration on board the ship, followed by the Sea Acceptance Test. At sea, the integration of combat systems at the respective warfare scenario levels was tested, verifying the scenario requirements defined at the beginning of the programme. Live-firing is involved at this stage and is the climax of the integrated test programme – with a successful live-firing being the ultimate and tangible proof of performance in the real operational environment.

The systems integration experience gained from the various naval platform programmes has benefited subsequent programmes such as the MCV upgrade, littoral mission vessel and the submarine programmes.

System Safety

Introduction

The idea of safety is not new. Since prehistoric days, man has had an intuitive understanding of safety risks associated with dangers posed by predators and the natural elements, resulting in the need to evaluate the dangers and to react appropriately with the objective of self-preservation. Over time, and with increasing complexities of modern inventions and innovation, the concept of safety gradually shifted from addressing natural threats to human-created hazards.

In the context of the acquisition of modern weapon systems, the concept of safety has further evolved into that of system safety, with the objective of identifying, to the best of ability, all real and perceived hazard potential associated with the system. In turn, solutions are then introduced to eliminate or mitigate mishap risks even before the system goes into operation. Where mishap risks cannot be further mitigated, at least the existing mishap potential is known, accepted and can be monitored.

The modern history of system safety can be traced to a technical paper presented to the Institute of Aeronautical Sciences in 1947, entitled “Engineering for Safety”. It advocated, “Safety must be designed and built into airplanes just as are performance, stability, and structural integrity. A safety group must be just as important a part of a manufacturer’s organisation as a stress, aerodynamics, or weight group.”

It is noteworthy that prior to this paper, safety was generally achieved through a Fly-Fix-Fly approach. This was unacceptable for obvious reasons, especially in the Space and nuclear domain. Still, it was not until the early 1960s that the concept was applied formally by contract, in response to general dissatisfaction with the existing approach to aircraft design. This led to the publication of the first MIL-STD-882A in 1977, which emphasised system safety as a management science.

System Safety Concept

What exactly is system safety? Simply put, system safety is the effort to make things as safe as practical by systematically using engineering and management tools to identify, analyse and control hazards.

“As safe as practical” may be expressed as the “best degree of safety”, “optimum safety”, or “optimum mishap risk management” within constraints (such as operational effectiveness, cost, time, etc).

Existing	Superseded by	Published date	Remarks
MIL-STD-882	MIL-STD-882A	June 1977	Focus on risk acceptance as criterion Inclusion of Hazard Probabilities.
MIL-STD-882A	MIL-STD-882B	March 1984	Major reorganisation of MIL-STD-882A. Detailed guidance in requirements. Addressed software tasks.
MIL-STD-882B	MIL-STD-882C	January 1993	Integration of hardware and software safety efforts.
MIL-STD-882C	MIL-STD-882D	January 2000	Allocation of responsibility for system details to designer.

Evolution of MIL-STD-882 series

It can be inferred from the generally accepted descriptions of system safety, and its MIL-STD-882 definition, that a viable System Safety Programme requires the existence of a structured system of identifying, categorising and analysing hazards followed by the consequential elimination, mitigation or amelioration of the identified risks.

Risk Acceptance

The objective of any System Safety Programme is to provide visibility of mitigated safety risks for management's acceptance. In this aspect, two principles are useful as aids in risk acceptance, namely Hazard Control Precedence and Mishap Consequences.

Hazard Control Precedence: In identifying hazards and developing controls, the generally accepted precedence is as follows:

- Design for minimum risk
- Incorporate safety devices
- Provide warning devices
- Develop procedures and train personnel

Mishap Consequences: In the context of a military organisation, the impact may affect any of the following:

- Health and Safety of Personnel
- Functional Capability of a unit
- Public Image and Reputation
- External Environment
- Budgetary Write-offs

Realistically, all risk elimination or mitigation solutions will incur an investment, either in time, effort or cost. In the final analysis, given that a system safety team has expended all reasonable effort at risk mishap mitigation, it is still conceivable that there may be some level of residual risk. At this stage, the team is obliged to inform management of any residual risks and make recommendations on the acceptability of such risks. It is then the management's responsibility to decide whether or not the remaining risk is acceptable, taking into consideration expendability of existing resources against the implication of any potential mishap consequences.

System Safety Methodology

After an accident with the 155mm Gun Howitzer in March 1997, it was recognised and acknowledged that there was a need for a deliberate and structured management of safety, and the impetus for implementation of system safety was initiated, starting with the Armament Systems. It has since progressed, through a 2002 SAF System Safety Joint Directive, from addressing just Armament Systems to a more encompassing requirement to cover all weapon systems throughout its entire life cycle. DSTA embarked on the system safety methodology which entails hazard identification and risk analysis. DSTA saw the need to provide a more structured approach in safety assurance for the acquisition of weapon systems for the SAF. By 2003, the implementation strategy was developed and the system safety assurance methodology was adopted in DSTA and the SAF.

The acquisition of the Gulfstream 550 and the development and construction of the Underground Ammunition Facility were identified as pilot programmes incorporating system safety. The Residual Mishap Risk Management Framework for the RSAF was endorsed by the Chief of Air Force. The RSN and the Army followed and approved their Residual Mishap Risk Management Frameworks. MINDEF agencies were added to the framework subsequently and the entire MINDEF Mishap Risk Management Framework was finally endorsed by a MINDEF's Weapon System Safety Advisory Board. The MINDEF LCM Committee endorsed the System Safety Guidebook for use within MINDEF and DSTA. Topics on system safety awareness were developed and incorporated into various DSTA Milestone Courses.

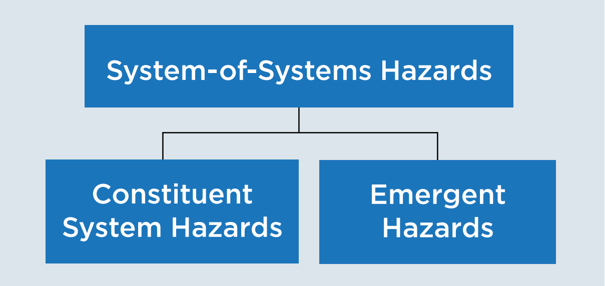
Since 2000, there has been significant progress made in applying system safety during the process of acquiring guided weapon and armament systems and equipment for the SAF. It is a value-added service that DSTA provides to make our systems and equipment safer. DSTA has helped to enhance the knowledge and application of system safety principles and techniques in the engineering community and to a wider audience. The System Safety Society (Singapore Chapter) is an organisation set up for this purpose. Frameworks have also been put in place to encourage engineers to practise system safety as a professional discipline and specialisation. The directives, life cycle manuals and dedicated system safety guidelines of MINDEF have been aligned with the guiding principles of system safety.

An example of artillery gun firing by the PRIMUS

From System Safety to System-of-Systems Safety Assessment

System-of-Systems Hazards

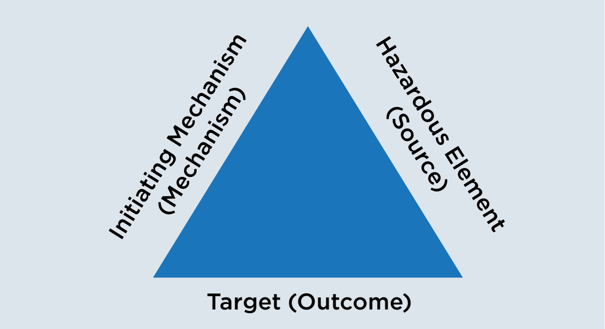
Due to the emergent behaviours brought about by the SoS, the hazards associated with the SoS are no longer limited to the summation of all the hazards found within each constituent system's hazard space. SoS hazards are described as those that may occur within the SoS. These SoS hazards, as illustrated in Figure, can be categorised into two main groups; constituent system hazards and emergent hazards. A constituent system hazard is a hazard that is attributable to a single system operating in a standalone mode, while an emergent hazard is defined as a hazard that results from the newly formed relationships and is not attributable to a constituent system.



SoS Hazards

Hazard Theory

A hazard can be defined through the use of the Hazard Triangle, where it is described to comprise three components; namely the Hazard Element (HE), the Initiating Mechanism (IM) and the Target.



Hazard Triangle featuring the three hazard components

Each of the techniques above, when used in isolation, would not be able to provide the desired comprehensive emergent hazard treatment. However, by combining the three techniques, we are able to relate the developed emergent hazard to the Hazard Triangle concept.

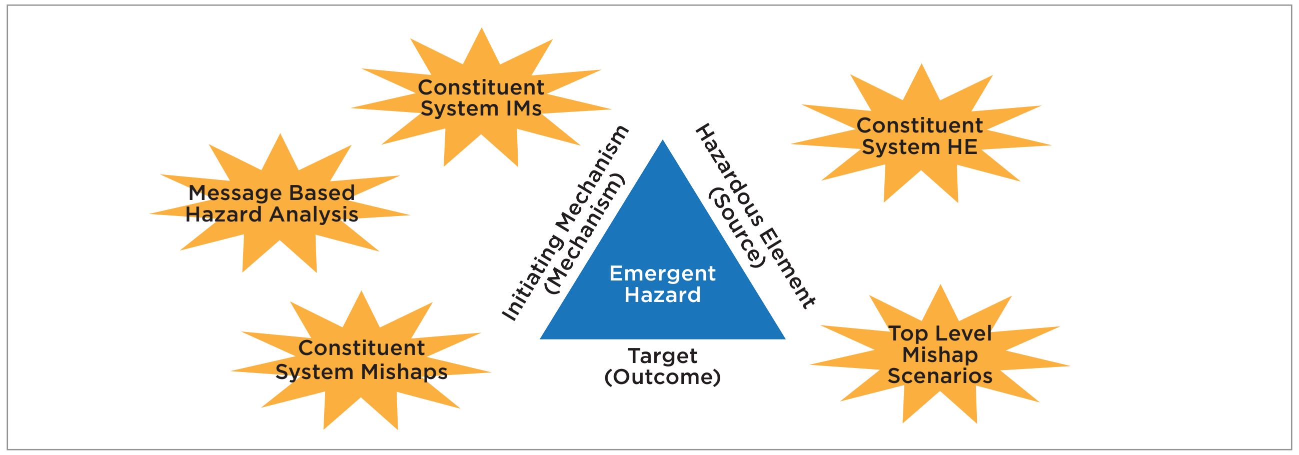
Hazard Element (HE) – HE is derived from the Constituent System Hazard Analysis.

Initiating Mechanism (IM) – The Message Based Hazard Analysis addresses the interoperability and interactions between Constituent Systems, providing insights into potential IMs at the SoS level. This complements the identification of IMs from the constituent system hazard analysis which may also have implications at the SoS level.

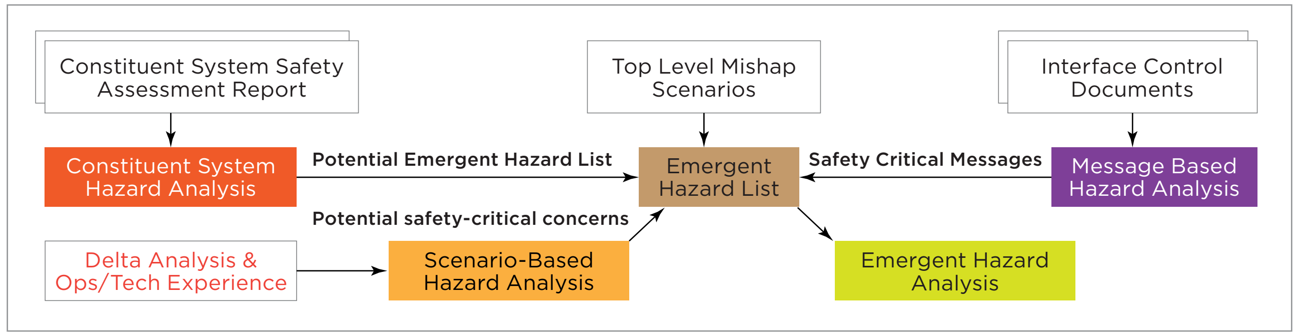
Target or Outcome – Based on the Constituent System Hazard Analysis, we can analyse outcomes that may be due to the emergent behaviour of the networked SoS, appreciating the fact that there are no new mishaps outcomes. The Top Level Mishap Scenario Analysis will also complement the alignment of mishaps to the IM and/or HE at the SoS level. A diagram illustrating the various Emergent Hazard Identification elements is shown here.

SoS Safety Analysis Techniques

The two most widely used System Safety Standards (MIL-STD-882[5] and Defence Standard 00-56 Part 1 & 2[6]) do not provide guidance on how to identify and assess these emergent hazards. The NPS thesis by Redmond[10] which provides a recommendation for an SoS Interface Hazard Analysis Technique also does not provide any insights into where or how to develop the actual hazard list. A possible approach to uncover potential emergent hazards and assess the risk associated with each emergent hazard is presented here.


Constituent System IMs
Message Based Hazard Analysis
Constituent System HE
Initiating Mechanism (Mechanism)
Hazardous Element (Source)
Emergent Hazard
Target (Outcome)
Constituent System Mishaps
Top Level Mishap Scenarios

The Emergent Hazard Analysis Approach


Constituent System Safety Assessment Report
Top Level Mishap Scenarios
Interface Control Documents
Constituent System Hazard Analysis
Potential Emergent Hazard List
Emergent Hazard List
Safety Critical Messages
Message Based Hazard Analysis
Potential safety-critical concerns
Delta Analysis & Ops/Tech Experience
Scenario-Based Hazard Analysis
Emergent Hazard Analysis

Emergent Hazard Identification

[5] US Department of Defense Standard Practice for System Safety
[6] UK Ministry of Defence Safety Management Requirements for Defence Systems

The emergent hazard analysis is conducted to develop the emergent hazard list from the combined perspectives of Top Level Mishap Scenario, Constituent System Hazard Analysis, Message Based Hazard Analysis and Scenario Based Hazard Analysis. The process requires the analysis of top level mishap scenario, the potential emergent hazards identified from the Constituent System Hazard Analysis, the safety critical messages from the Message Based Hazard Analysis and the safety critical concerns from the Scenario Based Hazard Analysis. The list of potential emergent hazards derived from Top Level Mishap Scenario, Constituent System Hazard Analysis and Scenario Based Hazard Analysis serves as the basis for the emergent hazard. For each safety critical message derived from the Message Based Hazard Analysis, an assessment is made to determine if it is associated with the list of the potential emergent hazard. Should a safety critical message be found not to be associated with any emergent hazard based on the earlier analysis, a new emergent hazard could be the outcome.

References:

Redmond, P. J., Michael, J. B., & Shebalin, P.V. (2008). Interface hazard analysis for system of systems, *IEEE International Conference on System of Systems Engineering* (pp. 1-8). doi: 10.1109/SYSOSE.2008.4724202

Chapter Six

ORGANISATION AND PEOPLE DEVELOPMENT

While previous chapters have outlined the DTC's systems engineering methodologies, this chapter will present how the DTC has evolved over the years from its humble beginnings in 1966 until today, including a glimpse of the larger Defence Technology Ecosystem (DTE) beyond the DTC. These organisational developments took into account factors such as MINDEF leadership's response to the SAF's evolving requirements and capability transformation as well as the need to optimise the use of finite engineering manpower resources. This chapter also covers aspects such as manpower build-up, organisational learning and competency development in the DTC.

Brief History on the Evolution of DTC Organisations

1966 – 1970s

The DTC started modestly with the Test, Evaluation and Acceptance Section of the Logistics Division in 1966 as the engineering and technical outfit within the Ministry of Interior and Defence. As reflected in its name, the section was to conduct the testing and evaluation of all stores and equipment that would be purchased by the Logistics Division. This marked the first instance where technical work was performed by a dedicated unit beyond the basic procurement-related functions. In 1968, the Technical Department was established in the Logistics Division to be responsible for all engineering and maintenance matters.

The early 1970s saw the formation of four new defence technology units in MINDEF to manage the acquisitions of weapon systems and build up engineering and scientific capability urgently from scratch to support the growing needs of the SAF. It also marked the start of the journey of defence R&D in Singapore, which was the aspiration of Dr Goh Keng Swee, Singapore's first Minister for Defence. Dr Goh firmly believed that only through technology would Singapore, a tiny city state, be able to defend itself. The Science and Management Group established in 1970 was tasked with the strategic planning and implementation of capability projects for the SAF. The Systems Integration and Management Team (SIMT) was formed in 1972 to oversee the evaluation, selection and integration of weapon systems, and most importantly the management of the first missile gunboat programme. The Electronics Test Centre (ETC) – the genesis of present day DSO National Laboratories – was established to build up secret-edge defence R&D capabilities.

The SIMT and ETC subsequently combined to form DSO in 1977. This organisation was endowed with the best engineering graduates and returning Public Service Commission scholars.

SCO was established by Mr Philip Yeo in 1979 by amalgamating the Data Processing Department, Finance Systems Branch, and Logistics Systems Branch, to undertake large-scale and systematic automation of MINDEF and the SAF's finance, personnel and logistic functions via computerisation. The Public Service then was lagging behind the private sector, in particular the banking industry, in exploiting computers by a good 10 years. The leaders of this community of pioneer IT professionals later moved on to the newly established National Computer Board to spearhead computerisation efforts for the whole Public Service.

1980s

The Second Generation SAF saw the upgrading and modernising of the three Services from the early 1980s to late 1990s. As Singapore's economy grew stronger, more resources were allocated to the SAF to speed up its capabilities build-up.

To support the SAF's urgent operational needs to build up a credible fighting force equipped with advanced defence technological systems, MINDEF set up SPO. SPO was to manage the acquisition of weapon systems and large-scale capability development programmes such as the acquisition of the E-2C Hawkeye AEW, MCV programme, C2 systems and airbase development programmes. The acquisition and engineering elements in the Logistic Division which had been focusing on the Singapore Army's needs were re-grouped and MMO was established.

Similarly, the Lands and Estates Department was transferred out of the Logistic Division and established as LEO. Three years later in 1986, MMO and SPO combined to form the Defence Materials Organisation (DMO; subsequently renamed as Defence Materiel Organisation in 1996) to ensure efficient use of technical manpower and greater consistency in systems acquisition. The procurement functions in MMO and SPO were transferred out to form the Defence Procurement Division (DPD) – this was part of the strategic move to enhance checks and balances in MINDEF's acquisition functions.

The DTC's evolution in the 1980s marked the inception of the concept of a defence technology community with the official formation of the DTG in 1986. Headed by the DS(T), the DTG consolidated the various groups of defence engineers and scientists involved in the acquisition of defence equipment, systems and R&D. MINDEF hoped that this would bring about integration and synergy among these entities and that they would be able to better support the SAF. The force multiplier potential of technology in the advancement of the SAF's fighting capability was recognised and decision makers in MINDEF were determined to build up and develop the engineering talent pool urgently and more systematically to support the modernisation push of the SAF. A Resource Planning Office was later set up in 1987 to support DS(T) in strategic planning and resource allocation.

The spirit behind the formation of the DTG is elaborated in the following extract of a keynote address by Mr Lim Siong Guan, then Permanent Secretary (Defence), at the DTG Seminar on 25th February 1986.

"DTG is not just organisations, but organisations, people and scientific and technical expertise united in a common mission – to provide the best possible technological support to help make the best possible SAF …

My appeal to all this morning is to see the wider picture and recognise our wider interests. We will all be able to get the same broad picture if we are all in the same helicopter …

DTG is to be the central repository of all scientific and technical expertise in MINDEF, including the SAF. This is not only to be in terms of knowledge, experience, ability and application, but also in terms of development and allocation of the people, know-how and management systems … We do not have enough manpower, and even less time, for such expertise to be duplicated between DTG and the Services …

[People in DTG are] all scientific, engineering and technical people who deliver DTG expertise. They are not only from DMO, LEO, DSO and SCO. They are in G4 MINDEF, in ALD, in NLD … They are spread about to avoid duplication and to get us the important close working relationships between operations staff and technical staff, between the Services and DTG …

If we all can be clear on the principle that DTG is first expertise, then people, then organisations, we would have taken a significant step in setting clear future directions for DTG …"

There was also a significant increase in the quantity and diversity of Engineering and Scientific Personnel (ESP) in the DTG in MINDEF during the 1980s to 1990s. This phenomenon can be traced back to a key decision made to raise the number of ESPs from around 250 in 1983 to 1,200 over the long term, as elaborated in the story on the "1,000 Engineers Vision" (pages 102-103).

1990s

The 1990s saw efforts in converting MINDEF entities into Executive Agencies. The motivation behind the Executive Agency model is essentially about changing the behaviours of organisations and the individuals within. The Executive Agency system allowed organisational performance to be measured directly, and the increased visibility enhanced accountability for actions and responsiveness to customer needs.

DSO and LEO became the first Executive Agencies in 1991, with DMO and DPD following suit in 1996. CSO was also established as an Executive Agency in 1995 from elements of SCO, DSO, and DMO that were involved in Command, Control, Communications and Intelligence-related systems. The generally positive experience with the Executive Agency model gave MINDEF the confidence to corporatise DSO subsequently.

In 1997, MINDEF also implemented the ERD framework, which was elaborated in Chapter 4. Through ERD, the DTG took over the O&S engineering of various systems that served the common interests of all three Services. This served to foster efficiency via consolidation of resources and better retention of engineering personnel by providing more varied and challenging work.

To meet the challenges of defence science and technology in the 21st century, a series of restructuring in the DTC occurred in the late 1990s to 2000.

In 1997, DSO was corporatised to allow it more flexibility to manage its people, subject R&D effort to the discipline of the market place for greater efficiency and responsiveness, and create a more conducive environment for innovation, creativity and risk-taking. It was also renamed DSO National Laboratories.

With the corporatisation of DSO, MINDEF needed an independent entity to manage the R&D budget and programmes. The Directorate of Research and Development (DRD) was established in 1997 as a member of the DTG to fulfil this role. The R&D budget was divided into two portfolios – S70 and D30, where 70% of the budget was allocated to the Services to manage and the remaining 30% to DRD to manage. The intent was to give the Services ownership of the more downstream R&D that will impact them in the short term, while providing DRD the mandate to invest in more upstream and longer term R&D that, if successful, would yield huge operational payoffs to the SAF. DRD helped MINDEF nurture a group of strong R&T managers who had in-depth understanding of the various operational challenges faced by the SAF as well as strong technological and systems know-how to prospect and evaluate R&T opportunities.

To facilitate the contracting of projects with DSO and other partners, DRD established Master Contracts with DSO, ST and the Universities.

DRD was also given the task to enlarge the R&D service provider to beyond DSO and Singapore. A DTG Development Office or DDO was set up within DRD to grow international collaboration.

In 1999, a further restructuring of the DTG led to the creation of the Defence Technology and Resource Office (DTRO) as the MINDEF staff agency for core technology functions of policy formulation, strategic planning, resource allocation and performance monitoring.

In 2000, DSTA was established as a statutory board to separate policy and implementation functions; offer more flexibility for promoting innovation, efficiency, and nurturing talent; and yet remain closely aligned with MINDEF's strategic objectives. DSTA was formed by combining the six organisations in DTG and two organisations from the Defence Administration Group – namely SCO and the Defence Medical Research Institute (DMRI).

The thinking behind these restructuring efforts can be gleaned from the following excerpts of a speech by Mr Peter Ho, Permanent Secretary (Defence Development) at the MINDEF Workplan Seminar in 1999.

"The DSTA builds on a central organisational paradigm in MINDEF. This paradigm is rooted in the principle that MINDEF is best placed to determine what should be done, while the service provider is best placed to determine how to do it.

With the formation of DSTA, MINDEF will be able to focus on policy, planning and resource allocation – its core functions. Implementation issues of defence technology will not distract it …

Decentralisation can take place within integration. We want tight integration at the strategic policy, planning and resource allocation level – where the payoff through integration is the greatest. At the same time, decentralisation of the implementation functions will enhance speedy execution, responsiveness and efficiency …

… all the major changes in the Joint Staff, the Executive Agencies, DSO National Laboratories, and now DSTA – are all linked in an ongoing effort to promote Integrated Defence Development. We should not see the separation of the DTG from MINDEF to form DSTA as a weakening of the organisation, but rather as a win-win organisational response to ensure that while we give autonomy and flexibility, everything we do remains integrated at all levels to ensure that the SAF is able to remain "First and Foremost" into the 21st Century."

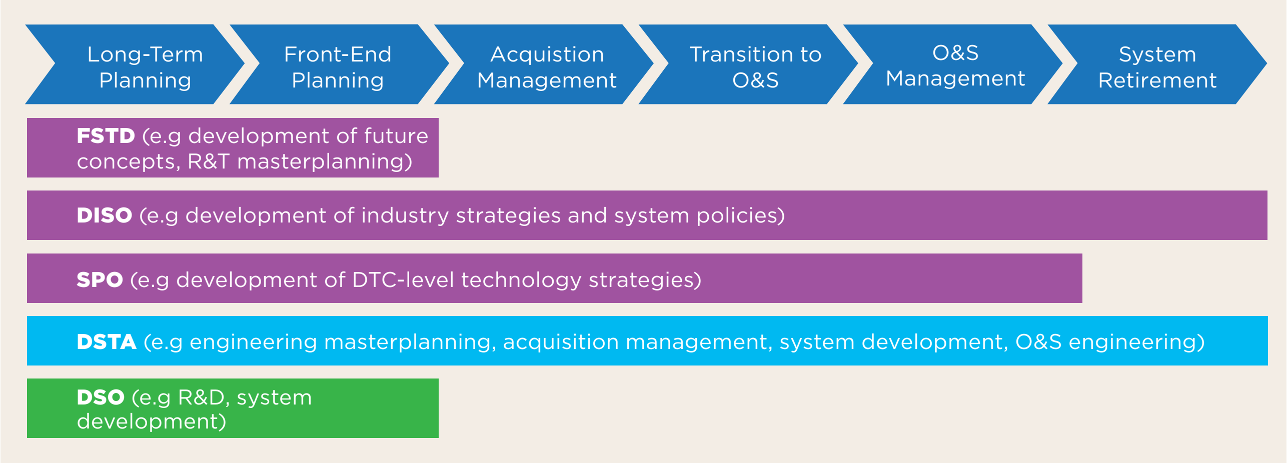
2000s and Beyond

In 2002, the Future Systems Directorate (FSD) was formed as a MINDEF entity to develop advanced operating concepts alternate to those in the mainstream. This came at a time when the SAF embarked on its Third Generation transformation journey in 2004.

In 2006, the Defence Research and Technology Office (DRTech) was formed from the spin-off of the technology plans group within DTRO while the remaining two groups (Technology Policy and Systems) were reorganised into the Defence Industry and Systems Office (DISO). DRTech was further restructured in 2009 to bring together disparate R&T planning and management elements under a single entity. DRD was subsumed within DRTech.

As both their roles matured, in 2012, FSD and DRTech were merged into the Future Systems and Technology Directorate (FSTD) to entrench the ops-tech synergies of advanced concept development and technology masterplanning structurally.

As of 2016, MINDEF's current engineering resource mainly resides in two organisations – DSTA and DSO. There are now around 2,200 engineers in DSTA and 1,400 scientists and engineers in DSO. In addition, there are also about 1,100 military engineers serving in the SAF as Military Domain Experts Scheme (MDES) officers. The DTC currently comprises five organisations – Strategic Planning Office, FSTD, DISO, DSTA and DSO National Laboratories. The figure overleaf gives a broad overview of their respective areas of focus within the framework of MINDEF's DCM.


Long-Term Planning

Front-End Planning

Acquistion Management

Transition to O&S

O&S Management

System Retirement

FSTD (e.g development of future concepts, R&T masterplanning)

DISO (e.g development of industry strategies and system policies)

SPO (e.g development of DTC-level technology strategies)

DSTA (e.g engineering masterplanning, acquisition management, system development, O&S engineering)

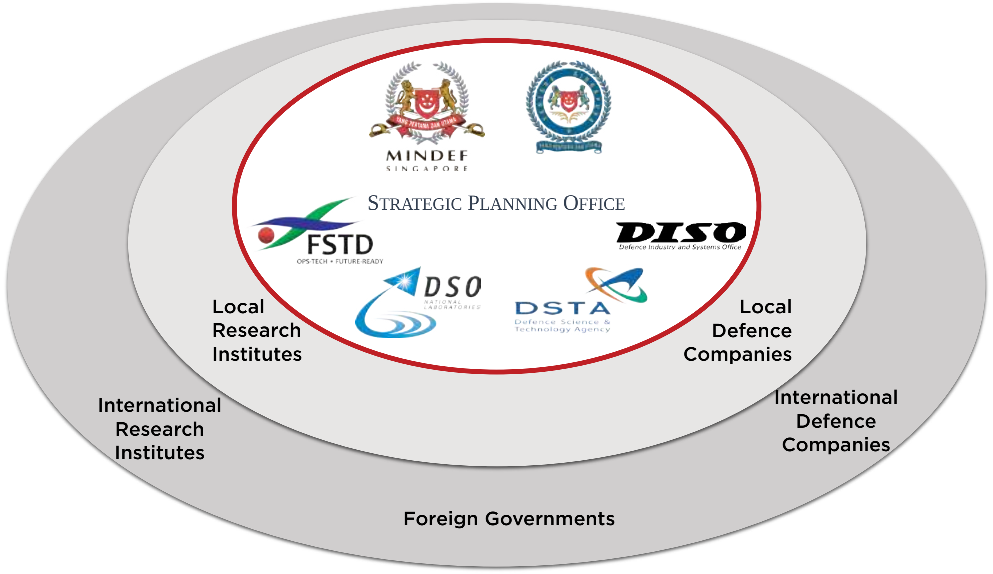
DSO (e.g R&D, system development)

Overview of DTC organisations and exemplar focus areas in the context of DCM

Defence Technology Ecosystem

Expanding beyond the DTC, there is a larger DTE that includes local industry (e.g. ST Engineering companies such as ST Aerospace, ST Kinetics, ST Marine, ST Electronics), local research institutes (e.g. Temasek Labs, Agency for Science, Technology and Research), and foreign partners (foreign governments, international research institutes, international defence companies). The DTE supports MINDEF's approach to defence technology and engineering in the following ways:

- *Acquire off-the-shelf systems whenever possible.* This aims to exploit market efficiencies as a smart buyer. This approach includes acquiring best-of-breed systems and integrating them into a large-scale system or an SoS.
- *Build (design and develop) only when necessary.* This could include cases of technology being unavailable for purchase in the market, unique requirements that the market cannot support and needing to nurture local industry to build up selected capabilities.
- *Collaborate with partners.* This includes strategic outsourcing to harness the capacity of industry and collaboration with research institutes and foreign governments.


MINDEF
SINGAPORE
STRATEGIC PLANNING OFFICE
FSTD
DISO
DSO
DSTA
Local Research Institutes
Local Defence Companies
International Research Institutes
International Defence Companies
Foreign Governments

The Defence Technology Ecosystem

Organisational Learning and Knowledge Sharing

"While some things must be kept secret, you must also allow information to flow so that knowledge can be accumulated… Knowledge, if not shared, is lost…

If you don't know what you don't know, then you are making decisions based on only a subset of available knowledge… That's a very serious loss. So I'm an advocate of openness and shared data."

Prof Lui Pao Chuen
Extracted from the book "Singapore's Scientific Pioneers", page 65

As the DTC progressively expanded and evolved in organisational structure and grew its pool of ESP, intentional efforts were made to share and harness the knowledge gained and lessons learnt and impart them to succeeding batches and generations. This went beyond an individual's on-the-job training within a discipline or department, and extended towards an organisational-wide approach, where new value can be derived from the intersection of disciplines. Examples of initiatives to facilitate such organisational learning can be seen at both the DTC and organisational levels.

At the DTC level, then CDS Prof Lui Pao Chuen developed the first run of MINDEF's Defence Management and Systems Course (DMSC) in 1996, a pinnacle leadership programme to prepare future leaders in the DTC. The course was developed based on Harvard Business School's Case Method of instruction and captured rich lessons learnt from the DTC's experiences. DMSC's content has since been enhanced with the continued contributions of many senior members in MINDEF who personally reviewed the curricula and facilitated participants' learning. DMSC has also served as an excellent avenue for building strong linkages and relationships between different organisations within MINDEF and the DTC.

DMSC's structured approach in transferring knowledge and experience gained from numerous defence projects to succeeding generations has also been propagated at the organisational level. For example, the DSTA College was formed in 2004 (and subsequently evolved into DSTA Academy in 2012) to adopt a similar approach in developing and strengthening DSTA's core competencies in the management of large-scale complex projects, via route-of-advancement courses in systems engineering and project management. Another example is the DSO Leadership Development Programme.

Apart from courses, DSTA's adoption of SA in 2004 also fostered organisational learning. This involved an interdisciplinary approach to uncover and harness the rich and diverse knowledge across entities within DSTA – itself an amalgamation of eight organisations in 2000, so as to derive new insights in developing SoS architectures and complex systems to realise networked capabilities for the Third Generation SAF. Subsequently in 2006, a dedicated Programme Centre for masterplanning and SA was established. Other initiatives included the annual DSTA Learning Festival between 2003 to 2008 to heighten the awareness of all staff on the importance of collaboration and continuous learning, as well as the establishment of the Directorate of Organisation Capability Development (OCD) and eight Competency Communities (CC[1]) in 2006. The CCs served as "knowledge communities" comprising people of like-minded professional interests, and where knowledge could be germinated, created and shared.

Effective organisational learning requires not just institutional mechanisms and infrastructure for knowledge sharing, but also a culture of knowledge sharing. In a knowledge-intensive organisation, staff need to be empowered with the right information and mandate to be effective knowledge workers. Often, the right information resides with different people from various parts of the organisation.

Staff can be resistant to sharing information due to reasons such as entrenched mindsets. Examples are the "need-to-know" and "knowledge-is-power" mindsets. As a result, information resources may not be well organised and shared, and in turn staff need to spend a significant amount of time and effort looking for information.

To cite an example, such challenges were reviewed in DSTA in its journey as a learning organisation, and the notion of "right-to-ask" was proposed and formalised to complement the "need-to-know" principle. This refers to an inherent right to ask for information if staff are unable to locate it. While the notion of "knowledge-is-power" would still be valid, the paradigm "knowledge-sharing-is-power" would be more powerful. By not sharing knowledge, a staff would miss the chance to impart knowledge and be recognised. This new paradigm has since gone a long way towards enhancing knowledge sharing and information resource management in DSTA.

Competency Development

In addition to organisational learning, the DTC's qualitative growth hinges on its ability to nurture strong engineering and scientific expertise. The DTC has a broad range of competencies, ranging from systems engineering skillsets to technical disciplines. Other than on-the-job training, various approaches to formal training and education have been institutionalised within the DTC.

For example, DSTA Academy currently conducts a series of route-of-advancement courses to meet the needs of engineers in DSTA, MINDEF and the SAF and train them in systems engineering skillsets. These courses comprise the Basic Systems Engineering and Management (BSEM), Intermediate Systems Engineering and Management (ISEM), and Advanced Systems Engineering and Management (ASEM) courses that are primarily targeted at DSTA engineers, while the Intermediate Domain Systems Course and Advanced Domain Systems Course are targeted at the SAF's MDES engineers. DSTA Academy is also entrusted with the running of and continued improvement to the DMSC. Since its inception, 39 batches of BSEM, 40 batches of ISEM and 11 batches of ASEM have graduated as of April 2016.

For in-depth training in technical disciplines, a key avenue to nurture DSO scientists has been PhD studies. Prof Su Guaning attributed MINDEF's investment in DSO via PhD scholarships as a key enabler for DSO to build up its deep technical expertise in areas such as electronic warfare. The pool of R&D scientist and engineers with PhD qualification provided DSO the confidence to push the frontiers in R&D and independently develop solutions where there was no precedent to take reference from, instead of its earlier mode of relying on tried and tested approaches and staying within the safety of grounds covered by others (Juliana Chan, 2015, pp 80-81).

For DSTA, in-house courses on technical disciplines helmed by senior management and specialists within the respective DSTA business units are directly responsible for competency development of staff, with DSTA Academy maintaining oversight of the technical courses.

[1] The eight CCs were: (1) Platform; (2) Sensing and Connectivity; (3) Guided Weapons and Armaments; (4) Command & Control and Information Technology; (5) Building and Infrastructure; (6) Systems Engineering; (7) Corporate and (8) Procurement. The OCD and CC construct had since evolved into new structures, where all Programme Centres (PCs) in DSTA, i.e. business units, are directly responsible for competency development of their staff.

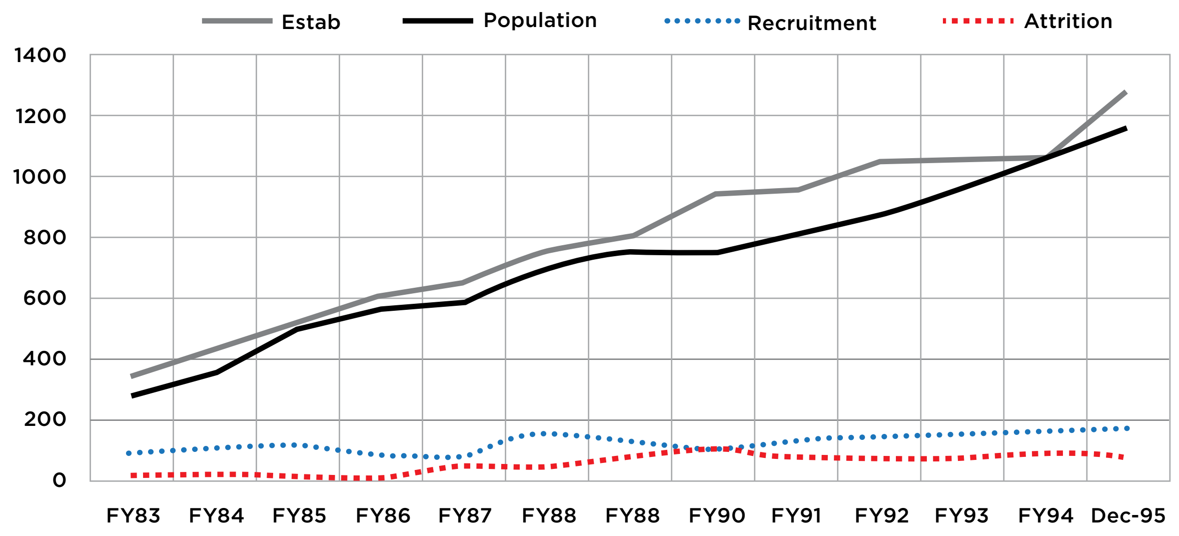
“1,000 Engineers Vision” – Engineering Manpower Build-up and Transformation

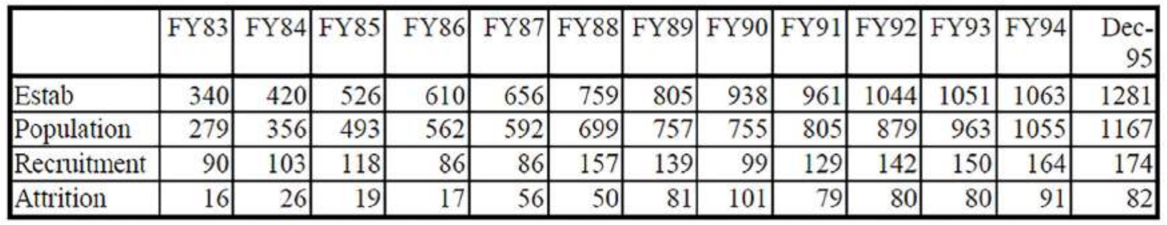
The size of the defence budget is one measure of the resources that a country is willing to invest in its defence capability. The second measure would be the total number of personnel in the defence community. The third would be the size of skilled technical manpower directly employed in defence.

Using Sweden's and Israel's number of engineers per one million US dollars of defence budget as a benchmark, MINDEF estimated that for the defence budget projected in 1983, the number of engineers needed would be around 1,200. There was a great mismatch between supply and demand, given that in 1982, MINDEF had only around 200 graduate engineers. A very difficult task laid ahead – to persuade decision makers to agree to grow the engineer population by nearly 500%, from around 200 to 1,200.

In a 1983 MINDEF HQ meeting chaired by then Minister for Defence, Mr Goh Chok Tong, it was agreed that MINDEF should double its population of engineers to 500, and a vision of 1,000 engineers would be for the long term. Thereafter, MINDEF and the SAF was allowed to increase 100 engineers a year to ramp up the population of engineers rapidly to 500.

Amid annual recruitment and natural attrition, the DTC's engineering manpower grew at a steady rate from 1983 to 1995 and it achieved its long-term goal of 1,200 engineers within 12 years.





	FY83	FY84	FY85	FY86	FY87	FY88	FY89	FY90	FY91	FY92	FY93	FY94	Dec-95
Estab	340	420	526	610	656	759	805	938	961	1044	1051	1063	1281
Population	279	356	493	562	592	699	757	755	805	879	963	1055	1167
Recruitment	90	103	118	86	86	157	139	99	129	142	150	164	174
Attrition	16	26	19	17	56	50	81	101	79	80	80	91	82

Manpower build-up in the DTC from 1983 to 1995

The rise was due to the increase in the number of engineering graduates from the National University of Singapore (NUS) and Nanyang Technological University (NTU) since 1987, as well as the aggressive recruitment campaigns mounted by MINDEF. The quality of engineering graduates recruited also improved due to the concerted promotion of numerous undergraduate training awards and the increase in the number of awards given out to in-service engineering staff.

On the other hand, the three most frequently mentioned reasons for engineers leaving MINDEF were: ‘for better prospects and greater challenges in the private sector’, ‘dislike scope and nature of work’ and ‘dissatisfied with rate of promotion and advancement’. These feedback had a significant influence in MINDEF's strategic decision on the corporatisation of DSO and the setting up of DSTA as a MINDEF statutory board.

Competition from the Private Sector in 1995

In 1995, the demand for engineering expertise became very competitive at the national level. With the government's emphasis and support for R&D programmes in the private sector industries and the plan to expand the semiconductor industry, the demand for researchers and engineers in the private sector rose very significantly.

Singapore then had four wafer fabrication plants in operation, with two more under construction and another six planned in the pipeline. Each wafer fabrication plant would require between 1,000 and 1,500 workers of which 50% would be technical staff (engineering diploma holders and professional engineers). Supported by the Economic Development Board and the National Science and Technology Board, several incentive schemes were implemented to encourage students to take up courses that could support the manpower needs of these new growth areas. This posed a challenge to MINDEF's continual effort to recruit good engineering graduates.

In response to the increased demand for engineers to meet the needs of the booming local wafer fabrication industry, NTU and NUS increased their capacities for both full-time and part-time engineering courses starting from 1996.

Thus, it was fortunate that MINDEF leadership supported the aggressive build-up of engineering staff in 1983. Otherwise, it would have been even more challenging to support the SAF's fast pace of modernisation and assimilation of newly acquired and technologically advanced systems due to the shortage of engineers by the mid 1990s.

Source: DSTA Academy

A Learning DSTA

The following extracts from "A Learning DSTA" produced in 2006 by DSTA, highlight its aspiration to be a learning organisation.

"Learning takes central place in our organisation and in society today. Knowledge continues to grow at an exponential rate. What we know or have mastered from yesterday may soon become out-of-date. As individuals and as an organisation, we run the risk of becoming irrelevant if we do not learn to refresh our knowledge base and embrace new ideas quickly enough.

DSTA operates at the intersection of several domains – technology, military operations, defence technology community and innovation. We possess multi-disciplinary competencies and operate within several industries – IT, defence and construction. This diversity accords us a melting pot of opportunities for innovation. To strengthen Singapore's defence and security, we need professionals who possess deep technical competencies in at least one technology area, as well as sufficient breadth to understand, apply and integrate across a spectrum of technologies. We term this a T-shaped competency model …

As an organisation, we seek to encourage learning, knowledge sharing and innovation. We have in place the organisation framework for learning and growth that is tightly linked to our strategic objectives. DSTA College was formed in 2004 to institutionalise the process of transmitting valuable organisation knowledge and experience. This framework will be further strengthened as we continue on our organisational excellence journey as embodied in the Enhancing Business Model, or EBM, initiative.

In the current phase, we will seek to provide a better balance between long-term and short-term priorities. The consolidation of 60 divisions (operating units) into 13 larger operating units will foster better integration, sharpen accountability for project delivery in the short and medium term and provide greater flexibility in the deployment of our people. Each DSTA member will belong to one of eight professional communities grouped by competency areas. He or she will belong to one of these professional communities. Our respective professional community will facilitate the development of competencies, best practices and standards of professional practice that will guide us in our work and develop us in our professional area. The professional communities will also promote knowledge sharing and innovation …

The organisation is a reflection of collective behaviour. All of our organisational development efforts can perhaps be viewed through this perspective. We want our organisation structures to enhance rather than hamper the productivity of our knowledge workers. We want to have systems and processes that encourage and stimulate knowledge and information flow. We desire a family culture where mutual trust and confidence abound. We envisage DSTA to be a place where everyone plays a part to build the community based on shared vision and values, and contributes to its character. This is the essence of a Learning Organisation …"

Richard Lim
Chief Executive
September 2006

The DSTA "T-shaped" competency model

The idea of a "T-shaped" competency profile of DSTA engineers was introduced in 2006. A person's competency profile may be represented by the letter "T", illustrated in the figure below. The Basic and Business Competencies form the horizontal part of the "T", while the Technical Competencies (comprising diverse engineering, architecture and information technology disciplines) form the vertical part of the "T".

A DSTA engineer should have breadth of knowledge in Basic and Business Competencies, and depth of knowledge in one or more Technical Competencies. This is the desired competency profile given the increasingly complex and multi-disciplinary projects that DSTA is taking on. An example is the RSN's Frigate programme, where DSTA is in charge of system integration and managing 17 sub-contractors from five countries.

The T-shaped paradigm would enable successful engineering and management of complex systems in DSTA:

- Being T-shaped means the ability to keep the "big picture" in mind while collaborating with diverse expertise on the details. When tackling a difficult problem, rather than being limited by their functional domains or comfort zones, T-shaped engineers are able to think out-of-the-box, harnessing knowledge across the organisation and exploring ideas and solutions across DSTA or even DTC to gain insights.
- Being T-shaped facilitates innovation, which occurs at the intersection of disciplines, be it with diverse technologies or between operations and technology. A T-shaped engineer has sufficient breadth of knowledge and the ability to converse in the "language" of specialists in different domains and application contexts. This allows the engineer to apply his/her own deep knowledge across different situations, and to facilitate joint efforts between two or more specialists in specific domains to harness their strengths to tackle complex problem.
- With strong basic and business competencies, T-shaped engineers have the soft skills that are effective in teamwork, and build trust both within DSTA and with partners. They are more likely to be able to manage a multi-disciplinary team with diverse expertise and personalities.

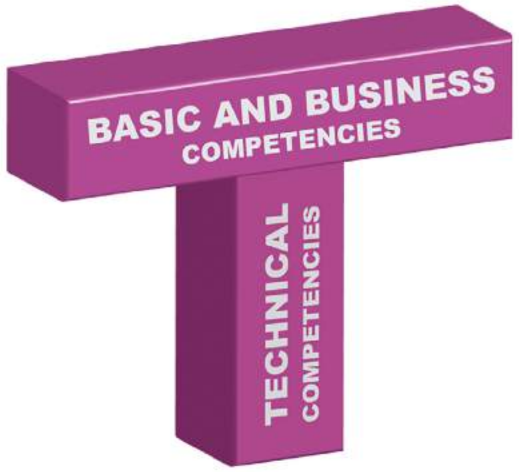


Illustration of the T-shaped competency model

Basic Competencies

- Communications
- Customer Orientation
- Problem Solving
- Teamwork and Alliance Building
- Leading
- Staff Management

Business Competencies

- Master Planning and Systems Architecting
- Systems Design and Systems Integration
- Project Management
- System Management
- Safety Management and Defence Contracting

and more...

Technical Competencies

- Aeronautical Systems
- Land Systems
- Naval Systems
- Guided Weapons and Armament
- Sensor Systems
- Communications Systems
- Networks
- C2IT

and more...

References:

Chan, J., Chua, G., Sim, S., & Tan, R. (2015). *Singapore's scientific pioneers.* Singapore: Asian Scientist Publishing Pte Ltd.

Chapter Seven

BEYOND DEFENCE

Extending DTC's Enabling System-of-Systems for the Greater Benefit of Singapore

The systems thinking approach and engineering competencies built up over the years in delivering capabilities to the SAF have also found applications beyond defence. More recently, in line with the whole-of-government approach to tackle numerous complex issues that cut across agencies, the DTC has worked actively with other government agencies by providing technical support, often in collaboration with the defence industry. This chapter shares how DTC has been functioning as an Enabling SoS at the national level beyond military defence.

Command, Control, Communications and Computers Network Projects for National Security

The Home Team, which comprises 10 agencies[1], requires C2 capability for effective execution of its mission to keep Singapore safe and secure. With diverse threats facing the Home Team, a modern and well-designed C2 system that remains alert to anomalies is key for commanders and operators to respond swiftly. This would mean having to coordinate, command and control their ground resources. For example, the Police Coast Guard (PCG)[2] has a critical need for C2 capability to enhance coastal surveillance and its operations to stamp out illegal smuggling into Singapore through the Straits of Johor. This is both a security and economic issue for Singapore, which entails a mammoth task for PCG as the terrain in the Straits of Johor favours smugglers. The long but narrow stretch of coast provides ample points for the smugglers to make a lateral dash to Singapore's northern coastline. To patrol and intercept such transgressions effectively, tremendous amounts of resources would be needed, especially in low-light conditions at night. Such asymmetrical operations thus required PCG to leverage technology.

In the early 1990s, the Singapore Police Force (SPF) decided to upgrade the capability of PCG. One of the projects was to develop an integrated surveillance and C2 system. As SPF and the Ministry of Home Affairs (MHA) had no resident expertise, they engaged a foreign consultant to study the operational requirements for the PCG C2 systems. In 1991, the consultant delivered the Specific Operational Requirements and among other new systems, it recommended the acquisition of five high-end military radars to be sited along the northern coast of the island. The requirements were approved by MHA, and the SPF project team was directed to seek MINDEF's input as its DTG had experience in implementing a coastal surveillance system for the RSN.

The SPF project team initially sought MINDEF's support to receive sensor information from the RSN's coastal radar systems. This was because the use of the consultants' proposed systems, together with the Port of Singapore Authority's (PSA) radars, did not provide sufficient coverage for the southern coast. Chief Defence Scientist Prof Lui Pao Chuen and DS(T) BG Wesley D'aranjo of MINDEF both learned about the consultant's proposed solution and assessed that a much more capable and economical solution could be derived from exploiting the sensor (Radar and Electro-Optics), systems integration and C2 development experiences

[1] The Home Team comprises the Ministry of Home Affairs, the Singapore Police Force, the Singapore Civil Defence Force, the Singapore Prison Service, the Central Narcotics Bureau, the Home Team Academy, the Immigration and Checkpoints Authority, the Internal Security Department, the Casino Regulatory Authority and the Singapore Corporation of Rehabilitative Enterprises.

[2] The PCG is a unit under the Singapore Police Force.

and expertise in DTG. As there was also a requirement to develop new towers along the northern coast, LEO's capability would be tapped to provide the much needed technical and programme support. MINDEF hence offered to help MHA in implementing the programme.

Understandably, the SPF team had reservations for it had been thinking of awarding this new capability project via a turnkey programme to a reputable engineering agency which could develop such systems. Up until then, the DTG had never been involved in any MHA projects and the DTG had not shared its sensor and C2 system development capabilities with any agencies beyond MINDEF and the SAF. After technical and operational discussions, the DTG led by Command, Control, Communications and Intelligence Systems Organisation (CSO, renamed in 1997 as Command, Control, Communications and Computer Systems Organisation), was given overall responsibility for systems engineering and project management of the PCG C2 capability development in November 1993. MINDEF and MHA principals wanted to ensure that the new capability would synergise with the SAF's existing coastal surveillance capability and be implemented within a tight time line and cost-effectively.

A joint project steering committee, co-chaired by DS(T), MINDEF and Chief of Staff (SPF), MHA, was established to oversee the project, set policy guidelines and resolve conflicts. Permanent Secretary (Defence Development), MINDEF and Permanent Secretary (Home Affairs) met every six months to review progress and provide strategic directions. The leadership provided by higher management facilitated collaboration among staff from MHA and MINDEF to a large extent.

In implementing the project, a key challenge was to design a system that would enable PCG to keep track – i.e. constantly knowing the precise location, of all vessels, especially small vessels (e.g. speedboats) that were fast and highly maneuverable. In the waters around Singapore's northern coastline, it was essential to minimise the time needed to detect and track such small vessels so as to allow PCG's response forces sufficient time to intercept them. In the waters around Singapore's southern coastline, the high density of large vessels (e.g. container ships) presented other challenges to detect and track the vessels of interest moving in the vicinity. Nonetheless, the DTG team had extensive experience from past projects that implemented systems in such difficult operating conditions. This would require extensive engineering effort to adapt the tracking system for site-specific conditions. The project steering committee concurred that the radar tracking system, which was the "brain" for the C2 surveillance, had to be designed and developed in-house given the very challenging operating environment and demands. A small group of CSO engineers, with expertise in tracking systems, embarked to develop a robust multi-radar tracking system, called the Radar Data Processing Subsystem (RDPS). The RDPS would provide PCG a coherent maritime situation picture by integrating the data from different types of coastal radars (from PCG, RSN and MPA) and utilising unique tracking algorithms to track the highly-maneuverable small vessels and to manage the detection phenomena expected.

In 1999, the surveillance and C2 capability was delivered successfully to the SPF. There were significant savings reaped as the systems engineers in DMO and CSO assumed the responsibility of systems integration instead of relying on a prime contractor. Besides, the DTG team was able to develop the C2 architecture and implement the whole programme by leveraging commercially available navigation radars and state-of-the-art electro-optics sensors to provide optimal surveillance coverage.

With the success of this capability development programme, MINDEF and MHA formed a joint management committee, which marked the start of the DTG's involvement in several programmes to enhance the Home Team's operational effectiveness. In one of the programmes, CSO (as part of DTG) developed and delivered a vehicle tracking system to track the locations of prison vehicles transporting inmates to hospitals and courts. This was done by integrating CSO's in-house products and commercial off-the-shelf technology. For the first time, the Singapore Prison Service had the ability to track the locations of its vehicles accurately. Back then, this was quite a feat as GPS, GIS and mobile computing technologies were still relatively new.

Working with PCG raised the profile of CSO as the go-to agency for command, control, communications and computers (C4) network capability development. Soon, several MHA agencies such as SPF and the Singapore Civil Defence Force enquired about CSO's support. To meet this demand, CSO decided to create a new division dedicated to these national security agencies. This led to the formation of the Dual-Use System Division in 1996, which comprised mainly C2 experts from CSO and sensor experts from DSO. The idea was to have CSO's C2 experts lead the support to national security agencies, with the assistance of experts in communications, network and other technological domains from the rest of CSO and DSO. A Memorandum of Understanding (MOU) was signed to formalise this collaboration where CSO could provide project management support to MHA in the area of C4. The intent was to help MHA build up not only its C4 capability but also its in-house competency, so that MHA could eventually manage its own C4 capability development while CSO simply provides technical consultancy. A case in point was the development of the replacement system for the 999 and 995 call system. With CSO at the helm to manage the project, SPF and SCDF staff were also incorporated into the project management team for transfer of know-how in both C2 competency and project management.

Today, the SPF and the SCDF's C2 systems integrate people, technology and processes, allowing real-time communication of voices, data, images and videos from incident locations to the Command Centre. These systems are complemented by mobile data terminals that track resource locations, perform mobile screening, and allow exchange of situational awareness between frontline officers and Incident Commanders. The systems include other advanced features that automate dispatch of resources to incident locations as well as dash-board functions to track incident load and incident response time, and to flag sensitive incidents automatically for supervisory intervention. In 2007, DSTA provided technical consultancy to SPF and the SCDF to renew their C2 capabilities. Since then, both the SPF and the SCDF have acquired their next-generation 999 and 995 C2 systems, providing them with the operational capabilities to meet their evolving needs.

Risk Assessment and Horizon Scanning

In a globalised and interdependent world, threats to national security can develop quickly and cause interconnected failures, with an example being the threat of terrorism post-9/11. While scenario planning has been in the toolkit of policy-makers to plan for the future, it is not effective at spotting weak signals of events that could have a serious impact on national security.

Following strategic surprises such as the 9/11 attacks, Jemaah Islamiyah's plots to carry out a bomb attack on Singapore and the Severe Acute Respiratory Syndrome (SARS) crisis, the Singapore Government felt an urgent need to build a more comprehensive set of tools to better anticipate future threats. Hence, the Risk Assessment and Horizon Scanning

(RAHS) Programme was started in 2005 as part of the National Security Coordination Secretariat in the Prime Minister's Office to develop new tools for strategic anticipation and national security.

The RAHS system and processes stemmed from three key ideas:

- *Sense-making in a Complex Environment:* Events in the world today exist in a complex space, where simple cause and-effect cannot fully explain observed phenomena. Competitive advantage belongs to those who can make sense of non-linear, emergent phenomena and those who know the right strategies to apply.
- *Thinking Systematically about the Future:* Technological advances in data analytics could be tapped to develop, track, and monitor possible future trajectories using foresight methods and system tools.
- *Connecting the Dots:* Each dot in the space of data has to be linked and connected to assist the human to detect the proverbial 'needle in the haystack'.

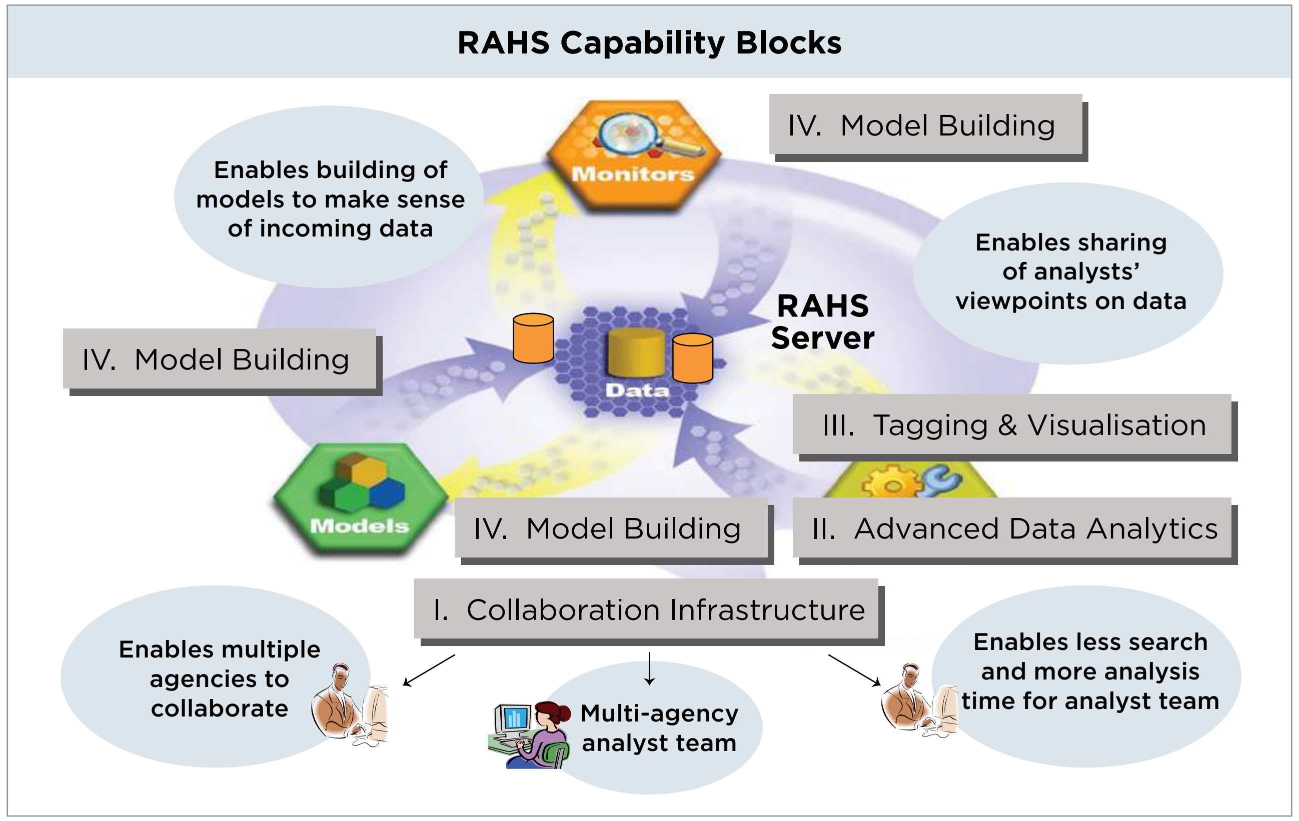
Developing a system to support RAHS involved complex and challenging engineering problems. First, RAHS analysts would require a system that can support the mental process of discovery rather than deduction, because threats identified through RAHS are evolving rapidly. Supporting a discovery mental process would also help analysts to identify patterns from seemingly disparate data, which mechanical systems are weak at. Second, there were no existing RAHS systems to refer to and a new cognitive-based system was needed to exploit new concepts in RAHS. Third, the RAHS System would have to be updated constantly because its concept was still evolving. RAHS also uses a wide range of technology such as text analytics and modelling which are developing rapidly. Therefore, a robust process was needed to manage changes to the system and continually validate the system against the analysts' operations which are constantly changing.

The idea of RAHS came from Mr Peter Ho, then Permanent Secretary of Defence. It originated from what was known as Large-Scale Integrated Search and Analysis (LISA). Peter Ho had linked up with John Petersen, founder of non-profit research organisation Arlington Institute, which led to the LISA project funded by DRD and FSD and a collaboration between the institute and DSO where each provided some intellectual property. The development, with COTS being used, was done at Arlington Institute where DSO had attached staff. LISA supported analysts in the systematic collection, organisation and analysis of unstructured texts. Peter Ho had spoken broadly about the needs of the whole-of-government and about weak signal detection. He also synthesised the ideas of Founder of Cognitive Edge Dave Snowden, John Petersen, IBM Fellow Jeff Jonas and Director of the DARPA Information Awareness Office John Poindexter, and drew upon Shell's Civil Service Scenario Planning Methodology. The RAHS idea was hence born, with LISA providing the software platform for it.

Using the RAHS System, analysts can systematically model future scenarios and track the likelihood of these scenarios emerging. More importantly, the analysts can work in a collaborative environment to share insights and analyses.

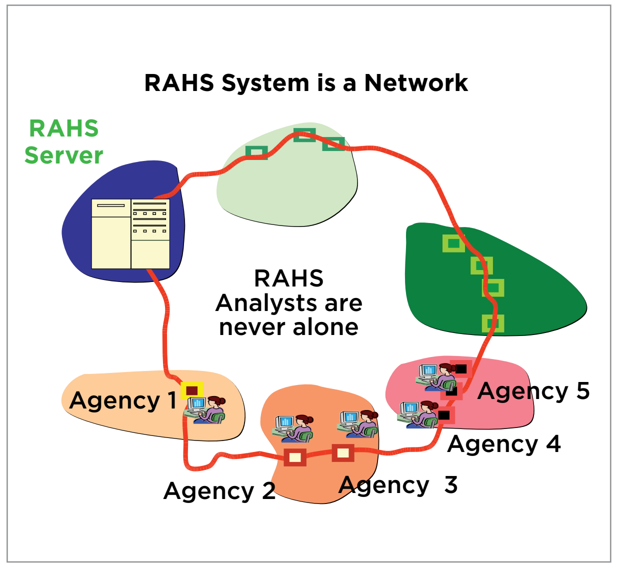
To connect the dots, entity resolution works[3] on networks of structured data where each node represents data while links represent relationships between data. Such networks provide more information and context to analysts instead of individual segments of data analysed in silo.

[3] Entity Resolution takes structured data and fuses data belonging to the same real world entity together. This is a key step in deriving an organised knowledge base.


RAHS Capability Blocks
Enables building of models to make sense of incoming data
Monitors
IV. Model Building
Enables sharing of analysts' viewpoints on data
RAHS Server
IV. Model Building
Data
III. Tagging & Visualisation
Models
IV. Model Building
II. Advanced Data Analytics
I. Collaboration Infrastructure
Enables multiple agencies to collaborate
Multi-agency analyst team
Enables less search and more analysis time for analyst team

RAHS Capability Blocks

The Horizon Scanning Centre (HSC) was set up, followed closely by the establishment of the RAHS Experimentation Centre (REC). The REC, staffed and managed by DSTA, was set up to research on and experiment with new technological capabilities to support foresight methods. Together, HSC and the REC have developed products, methods and technologies for use by government agencies. The REC delivered RAHS version 1.6 in 2007 with capabilities to support research and analysis using extraction, modelling and survey tools. The system was upgraded to version 2.0 in 2012 to enable theme extraction and added applications to support sentiment analysis. The next-generation tool code-named RAHS 4.0 is being conceptualised as an integrated system architecture to strengthen the bridging of foresight and policy work.



RAHS System is a Network

Rapid Response during SARS

The outbreak of the SARS virus took the world by surprise. Amid concerted global efforts to contain the disease, speedy tracing of contacts with SARS patients was identified as a critical measure. Hence, at the onset of SARS, the Ministry of Health (MOH) set up a centre for contact tracing, where manpower resources were deployed to track and trace probable SARS cases manually. Of particular priority was the tracing of contacts in hospitals, where most SARS infections in Singapore occurred. Being manual and reliant on fragmented data, the tracing process was, however, laborious and potentially prone to errors.

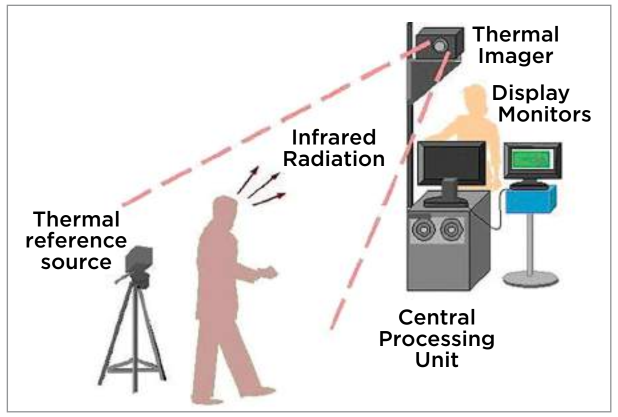
DSTA responded to MOH's request, joining forces with ST Electronics to develop a more efficient means of contact tracing. With a keen sense of mission, the team rapidly developed a Contact Track and Trace (C-T&T) system and Hospital Movement Tracking System, based on radio frequency identification (RFID) technology. With this system, movement in a certain area of the hospital is recorded automatically. When needed, the people a patient has come in contact with can be traced quickly using the search and query capability of the system. The system is set up to store information on visitors for 21 days, well above the incubation period of the SARS virus of 10 days.

Another urgent need at the height of SARS was for a fast, safe, user-and-public-friendly means of screening masses of people for fever. This was especially crucial at immigration checkpoints to control the import of new SARS cases. Responding to MOH's call to provide screening devices that could be deployed to identify potential SARS cases, DSTA explored the use of thermal imaging sensor technologies and developed the Infrared Fever Screening System (IFss) with ST Electronics.

The IFss is an innovative system solution that applies advanced radar concepts to enable very high probability of detecting a target in the surveillance space, while keeping the false alarm rate under control. It uses a military thermal imaging sensor operating in 3-5 micron waveband (as this was readily available from the SAF's inventory then) as a sensor, to capture the infrared (IR) radiation from the neck, facial and temple areas of the subject under test (as the subject walks past the set-up). This IR radiation is then compared against a calibrated thermal reference source placed in the field of view of the IR camera. The threshold setting was carefully derived based on extensive data (skin IR radiation of febrile and non-febrile individuals) gathered from trials carried out at the Accident and Emergency Departments of Singapore General Hospital and Alexandra Hospital, Changi Airport and Army Camps. When the IR camera picks up someone with a suspected elevated body temperature (due to a higher skin temperature as detected by the IR camera), he or she is subjected to a 'confirmation process' whereby a conventional thermometer is used to take his or her core body temperature. The IFss solution, being non-intrusive and easy to operate, was deployed quickly across Singapore and at airports across Asia as the first line of defence against cross-border spreading of SARS. This was a classic case of military technology being adapted for civilian application.

The project subsequently won many awards for its outstanding engineering achievement, as well as the Tech Museum Innovation Award 2004.

At the onset of the SARS outbreak, DSO responded to MOH's request to support SGH's Pathology Laboratory in identifying the etiological agent of SARS. DSO housed one of the few facilities in Singapore that was capable of handling dangerous agents such as the SARS virus. This high containment facility, also known as the Biosafety Level 3 (BSL3) laboratory, had been designated as the National Single Portal of Entry after the 9/11 attack in 2001 to analyse chemical and biological agent contaminated samples. At the height of the SARS crisis, DSO joined the Singapore Clinical SARS Consortium, and was tasked to work with the Genome Institute of Singapore (GIS) to develop and validate a diagnostic kit to detect the virus. GIS was provided with initial part sequences of the Coronavirus from DSO's preliminary investigations. Despite risks involved, the professionalism and dedication of DSO's scientists spurred them on in providing diagnostic support for clinical samples, so as to lighten the load of the hospitals. More than 1,600 clinical samples for the SARS virus were screened during this period. DSO's scientists also provided further assistance to national hospitals, such as the National University Hospital, to test the protective hoods used by the medical community in high risk situations.



An overview of how the IFss works.

The team received the US Tech Museum Award in November 2004 at a gala dinner that was attended by leaders from Silicon Valley and delegates from the United Nations.

Review of Lab-acquired SARS Infection

Following the review of the lab-acquired SARS infection case at the Environmental Health Institute (EHI), an Implementation Committee was set up within ENV[4] to oversee the implementation of the Review Panel's recommendation. The Implementation Committee was assisted by a Technical Advisory Group (TAG) chaired by CEO of DSO Mr Quek Tong Boon. Tasked to look into two main areas, the TAG proposed an action plan to fumigate the laboratories for the destruction of BSL 3 viruses, and reviewed the biosafety procedures and training programme.

Fumigation of the BSL 3 laboratory was carried out jointly by staff from EHI and DSO in accordance with TAG's action plan. Preparation for the fumigation and safety checks included verifying uni-directional air flow, sealing of air vents, setting up of quick release of the air vent seals for subsequent purging of the fumigant, installing of fumigation equipment with controls switch that were outside the BSL 3 laboratory, and placing biological indicators at various locations in the laboratory. All SARS coronavirus cultures were also deactivated at this stage.

After completing the fumigation, neutralisation and purging of the laboratory, the EHI BSL 3 laboratory was deemed to be fumigated successfully, validated by the complete deactivation of biological indicators placed in various locations of the laboratory. The laboratory was declared safe to enter after the National Environment Agency confirmed that the residual levels of the chemicals used were within guidelines.

In addition to managing the laboratory fumigation processes, the TAG also proposed

[4] ENV was known as the Ministry of Environment in 2003. It is now known as Ministry of the Environment and Water Resources – MEWR

changes to the laboratory's processes, standard operating procedures and training programme. The findings and recommendations from the review were presented to the Implementation Committee, which concluded responsibilities of the TAG.

Chem-bio Defence Capabilities to Enhance Singapore's National Security

With the increased threat of chemical weapons used in modern conflicts, DSO has expanded its R&D work to include a range of chem-bio defence capabilities. One such solution that DSO developed against chemical agents is the Scentmate – a novel, fast and effective screening kit for individuals suspected of exposure to nerve agents. This technology can assist in rapid on-site screening during a chemical attack.

DSO has also developed decontamination technologies including the Demul-X. The main draw of Demul-X is its ability to decontaminate a wide range of chemical and biological agents effectively, ranging from nerve to blister agents. It is also formulated with relatively non-toxic and environment-friendly ingredients. These properties were lacking in decontamination formulations before the mid 2000s.

After the September 11 World Trade Centre attacks, letters suspected to be contaminated with anthrax spores began to pop up in the US and many other countries, including Singapore. Though it was initially meant only for research, the BSL 3 laboratory was quickly identified as the only operating facility in Singapore that could handle the suspicious letters and anthrax spores. A procedure for collecting, receiving and processing the suspected anthrax samples was worked out. The samples sent in for analysis and verification included letters with white powder, as well as powder collected from indoor environments, mailboxes and a variety was maintained with the Criminal Investigation Department in collecting evidence to trace the culprits responsible for the perpetration of anthrax scares or hoaxes.

At DSO's Biosafety Level 3 facility, scientists supported the Ministry of Health in diagnostic testing of clinical samples for the presence of SARS virus during the outbreak in March 2003

Underpinning these developments were the capabilities and infrastructures built up over the years. In 2003, DSO achieved its first Organisation for the Prohibition of Chemical Weapons (OPCW) status, joining a select group of 14 other laboratories in the world to be designated. It was also the only laboratory in South East Asia to achieve the designation, and to possess the ability to receive samples from OPCW to test for suspected chemical agents. This achievement took seven years, 10 tests and the unwavering effort of many staff and it is a testimony to their “can-do” attitude and the management's strong belief in the scientists' competency.

Floating Platform and National Day Parade Support

The idea of a floating platform was conceived by the organising committee of the National Day Parade (NDP) in 2007, as a new venue was required for NDP while the National Stadium[5] would be demolished to make way for the new Singapore Sports Hub. Believed to be the world's largest performing stage, the floating platform was designed to be a multi-purpose facility on the Marina Bay for mass spectator events, sporting activities and cultural performances. It generates a usable space of 120m by 83m on water and was designed to carry a heavy load comprising at least 9,000 people, 200 tonnes of stage props and three 30-tonne vehicles. A 27,000 seating capacity gallery was built along the shoreline, facing the floating platform. This gallery allows spectators to view various events on the platform and on water against the backdrop of the Singapore city skyline.

The floating platform is one of the most technically challenging floating structures of its size, in view of the many unique considerations. As the platform's chief planner and developer, DSTA had to keep in mind not just the size of the platform and the load it could bear, but also make sure that the structure can be relocated and reconfigured to meet the requirements of different events. As a result, the platform is made of smaller platforms of pontoons, each comprising hundreds of parts. Two hundred pontoons were envisioned initially, but a unique system of connectors allowed this number to be reduced to 15. Designed to be light but robust, the connectors interlocked the pontoons like a jigsaw puzzle. Assembling the pontoons and connectors took one month. Six pylons were fixed onto the seabed to act as the floating platform's foundation. Heavy-duty rubber rollers were used to gently guide the stage vertically to keep it from being rocked by tides and currents. Three link ways, which connected the floating platform to the land, had special integrated joints to keep them steady.

[5] Most NDPs were held at the National Stadium before the floating platform was developed.

The stage centrepiece for NDP 2011 transformed itself throughout the event with exciting visual and lighting effects. The DSTA team also powered the floating platform with 10km of cables and 26 generators for a spectacular light and sound extravaganza.

For NDP 2012, the DSTA team procured in a new manner by establishing more multi-year contracts, thereby facilitating more efficient and effective processing of many recurrent purchases

With a larger stage closer to the seating gallery at NDP 2013, the DSTA team prowled the ground to measure sound levels and fine-tune the system to deliver optimal sound coverage.

The platform design had to contend with environmental conditions. The shallow water at the site limited the platform depth, while the changing tides put constraints on both the positioning of the platform with respect to the shore, as well the gradient of the access bridges that linked the platform to the land. Furthermore, the floating platform was relatively flexible and exhibited elastic behaviour, so hydro-elastic analyses of the stage under the action of waves were needed.

Safety was a primary consideration – specifically personnel safety and safety against structural damage. Hazards associated with the platform's accidental contact with cruise boats and sports craft were analysed. The effect of translational accelerations of the floating platform on the performers was investigated as a large number of personnel were expected to remain on stage for prolonged durations.

Extensive full-scale load tests were conducted on the platform at the site to evaluate the design and ensure the stage could withstand the large load. The success of the floating platform opened up new possibilities in space creation, complementing other initiatives such as land reclamation and building underground caverns. While the floating platform was initially conceived as an interim venue to host five NDPs, it has since hosted seven NDPs.

Beyond contributing towards a new venue to host NDP in 2007, DSTA has also contributed its expertise to support NDP over the years in numerous areas – including building the stage, implementing a robust power supply, installing high-fidelity sound systems, ensuring fireworks safety and procuring parade essentials like props and fun packs.

The two-tier stage of NDP 2014 was the largest ever to be constructed in NDP's history, with a capacity of 1,800 performers and their props, 18 towers and 10 elevating platforms.

DSTA also provided consultancy on safety for Singapore's largest ever fireworks display at NDP 2015.

Humanitarian Assistance in the Fukushima Incident

In early March 2011, a magnitude-9 earthquake off the Pacific coast of Tohoku, Japan triggered powerful tsunami waves that disabled all electrical and cooling systems at the Fukushima Daiichi Nuclear Power Plant. This incident resulted in the release of significant amounts of radioactive materials from three reactor units into the environment. Owing to the unanticipated incident for which no prior risk assessment was done, its dynamic nature and the disruption of communication means within the tsunami devastated zone, there was global consternation on the true extent of the disaster. This generated immense pressure on various governments to dispense prompt advice on the appropriate protective measures for their citizens residing in Japan, as well as appropriate contamination monitoring and control for goods and people travelling out of Japan into their country.

In anticipation of potential plans to extend HADR efforts to Japan, MINDEF and the SAF approached DSO for assistance to provide better clarity on the rapidly developing nuclear disaster and assess the potential impact to HADR forces that could be sent to Japan. Relying on her nascent capability in radiological dispersion modelling developed in response to radiological dirty bomb threats, and an understanding of what will be released by the nuclear reactor in case of a severe accident, DSO was able to provide probable and possible worst case impact scenarios to MINDEF and the SAF within 48 hours of activation – in spite of the absence of detailed technical information on the weather conditions and accident progression at the incident site. Based on these impact assessment studies, DSO reassured MINDEF and the SAF that radiological contamination would not impact Narita Airport, which was the planned landing point for the SAF's HADR forces. In addition, DSO also shared with other national agencies that radiological hazard zones would be confined within Japanese geographical boundaries even in the worst case scenarios. These findings corroborated the initial impact findings reported by other countries, which helped to maintain a measured and calm response from our national agencies. DSO's radiochemistry team was also activated to support the Agri-Food and Veterinary Authority of Singapore in the analysis of radioactive cesium in food supplies from Japan, which was conducted continuously for the following 12 months.

DSO's radiological dispersion and impact assessment capability has been put to good use in support of MINDEF and the SAF and other national agencies. This came about because of the foresight from MINDEF to fund the build-up of radiological and nuclear defence capabilities in DSO back in 2009. Although another disaster is not welcomed, DSO stands ready to support MINDEF and the SAF and other national agencies if similar needs should arise in the future.

Critical Infrastructure

After Singapore gained independence in 1965, it was necessary to build up local protective design capabilities quickly for the development of key installations, defence infrastructure and facilities. Early protective design methodologies were based on protection against well-prescribed threats. However, advances in technology have resulted in globalisation and increased connectivity that have also changed the threat space. For example, warhead technology has advanced with more powerful explosives as well as different kill mechanisms such as shaped charges, runway denial rounds, fragmentation rounds and thermobaric charges. Fuse technology has also progressed to facilitate the development of penetrating warheads. These weapons of enhanced capabilities can be developed rapidly, making it harder for protective infrastructure to keep up with commensurate protection levels without overwhelming costs and disruptions to operations.

Beyond spurring military weapons technology developments, worldwide connectivity has increasingly emboldened terrorist activities, spinning off emergent threats. Terrorism has evolved over the years, from one where there was little connectivity and where knowledge in bomb making was confined to a few, to a highly connected environment where decentralised, non-hierarchical leaderships collaborate, tap on and share knowledge online easily. Furthermore, such decentralised but connected terrorist networks have become harder to detect.

To avoid being under-designed in protection against potential threats, DSTA developed radically different approaches to critical infrastructure protection. Infrastructures should not only be able to withstand attacks, but also recover after an attack and resume function. As such, it is necessary to build resiliency into critical infrastructures. Resiliency allows infrastructure systems to sustain limited extent of damage, with recovery systems put in place to ensure return to normalcy within a short time. A balance needs to be struck between providing full physical hardening and designing to allow partial damage with swift system recovery. Design for resiliency can be achieved through a right combination of protective engineering design, system redundancy, design robustness and contingency planning to counter asymmetrical threats or disruptions.

In this extended paradigm, it is possible to design facilities for protection without defining a precise threat. This is done by expanding the area of coverage beyond the immediate facility, considering systems vulnerabilities and designing to incorporate mitigation systems. Beyond the design of buildings, the concept of developing protection options without a precise threat can also be applied to infrastructure networks, including networks for power and fuel. Vulnerabilities can include a single-point-of-failure, common mode failure and areas where even rudimentary forms of protection do not exist. These vulnerabilities may be overcome by various strategies, for example to overcome single-point-of-failure in the system, one can incorporate alternate distribution paths to critical nodes, or provide physical separation of critical distribution nodes.

Improving resiliency through system design in space alone may not suffice. Operational characteristics such as time and usage patterns need to be considered, as how people respond to a threat plays an important role in achieving mission success. Hence, understanding people's response to crises over time and the various usage of infrastructures through different stages of a crisis will be essential. Building hardened shelters in public underground train stations may provide protection to masses of travelling commuters in times of crisis. However, people in high-rise residential buildings may not be able to get to the public shelter in time. For them, individual household shelters meet their protection needs better because they can get to the shelters quickly and can carry on with other activities in between alerts. This allows a greater level of normalcy even in times of tension, benefiting the population as it is better able to weather prolonged periods of tension in crises.

The probability of threat occurrence and severity of its consequences can fluctuate over the time-space domain. Beyond the focus on modelling weapon effects on buildings, modelling and simulation can be extended to workflow analysis, and can enable design optimisation for survivability and resiliency. For facilities where mass congregation of people or vehicles is expected during operation, modelling to simulate human and traffic flows will provide critical inputs to planners, designers and stakeholders on the adequacy of infrastructure system for mission support. Ground exercises are needed to validate planning and design assumptions. From this understanding, an estimate of how much and where protection and resiliency can best be injected into a building system can be made.

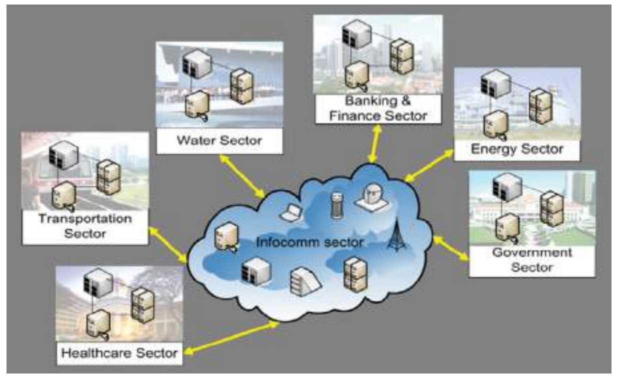
DSTA developed a systematic and iterative approach to identify credible threats and address the comparative risks and vulnerabilities. DSTA has conducted a large body of research work on explosion effects, structural response and progressive collapse in collaboration with local research institutes and overseas collaborators. DSTA has also built up computational know-how to model explosion effects. Explosive tests were conducted to ensure the validity of the research outcomes and models against realistic threats. These are examples of works that allow build-up of expertise in critical infrastructure vulnerability.

CIVA also has its roots in the military Operations Research capability in DSO. Our OR analysts applied their military Modelling Simulation and Analysis (MSA) methodologies and tools to issues of national security, centred around critical infrastructure protection. CIVA MSA activities have covered pandemic modelling, maritime trade-lane study, electrical facility vulnerability, internet infrastructure study, power grid study, and oil/gas supply chains modelling. This contributed to the build-up of a trusted, in-country expertise that can rigorously assess risks to Singapore's national infrastructures in all sectors.

As Singapore is a "wired-up" modern city-state, its Critical Infocomm Infrastructures (CIIs) are essential in our daily lives. As part of the Singapore Infocomm Security Masterplan, the Infocomm Development Authority (IDA) carried out the 2007 to 2009 Critical Infocomm Infrastructure – Surety Assessment (CII-SA). This was a first-ever attempt to survey and assess our nation's CIIs comprehensively and systematically.

IDA had intended CII-SA as two phases: high-level sweep and detailed assessment. DSO was appointed the technical manager for both phases. While defining the project scope, DSO proposed that IDA also include information interdependency analysis as systems interdependency was important in connected networks, since “the net is the computer”. The DSO team was hence tasked to analyse the CII interlinked dependencies and relative criticalities, and investigate the vulnerabilities of selected CIIs.

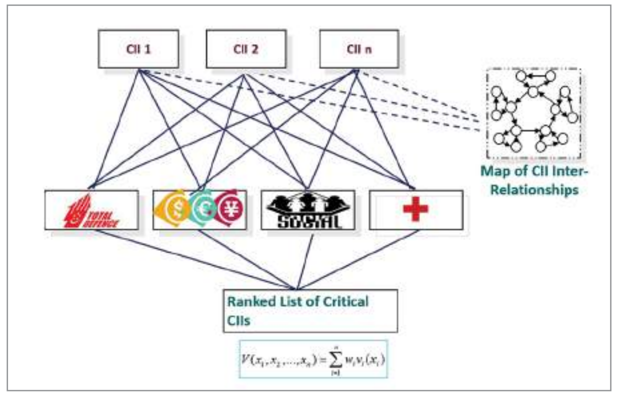
Phase 1 involved systematic data gathering. The IDA-DSO core team liaised with more than 10 Critical Infrastructure sector/sub-sector regulators and more than 100 organisations with CIIs within six months. Dealing with such a diverse group of regulators, sub-regulators and organisations, each with its own uniqueness and characteristics, the team learnt how best to elicit the required information from specific sectors and not to generalise. Workshop facilitation and soft skills were essential to build trust with the ground-level individuals whom the team interacted with.



Seven critical infrastructure sectors

Simultaneously, the methodological approach was developed from scratch, covering precise definitions of CII; derivation of national-level criteria, scales, thresholds; disruption impact estimates; ratings of physical and cyber security readiness postures; and reviews for basis, consistency and soundness. The approach was a fusion of metrology, mathematical modelling, and multi-criteria decision analysis.

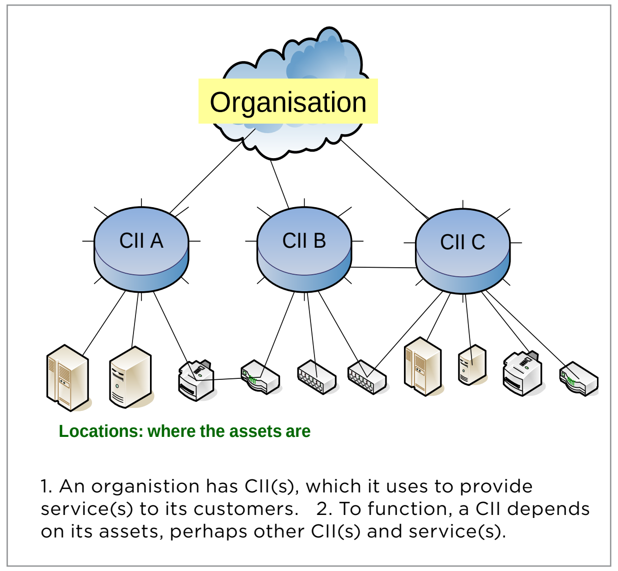
The team eventually identified various critical CIIs in Singapore's key sectors, and ranked them by their relative criticality. The CIIs' static dependencies were also mapped. Quantitative impact assessments – or informed estimations of some more obscure CIIs – were done for all the CIIs identified. Overall, much insight was gained, and the quantitative assessments provided a tangible basis for deciding how to enhance the CIIs, akin to the old adage “what you can't measure, you can't manage”.


CII 1
CII 2
CII n
Map of CII Inter-Relationships
Ranked List of Critical CIIs
$V(x_1,x_2,...,x_n)=\sum_{i=1}^{n} w_i v_i(x_i)$

CII Ranks and Dependencies

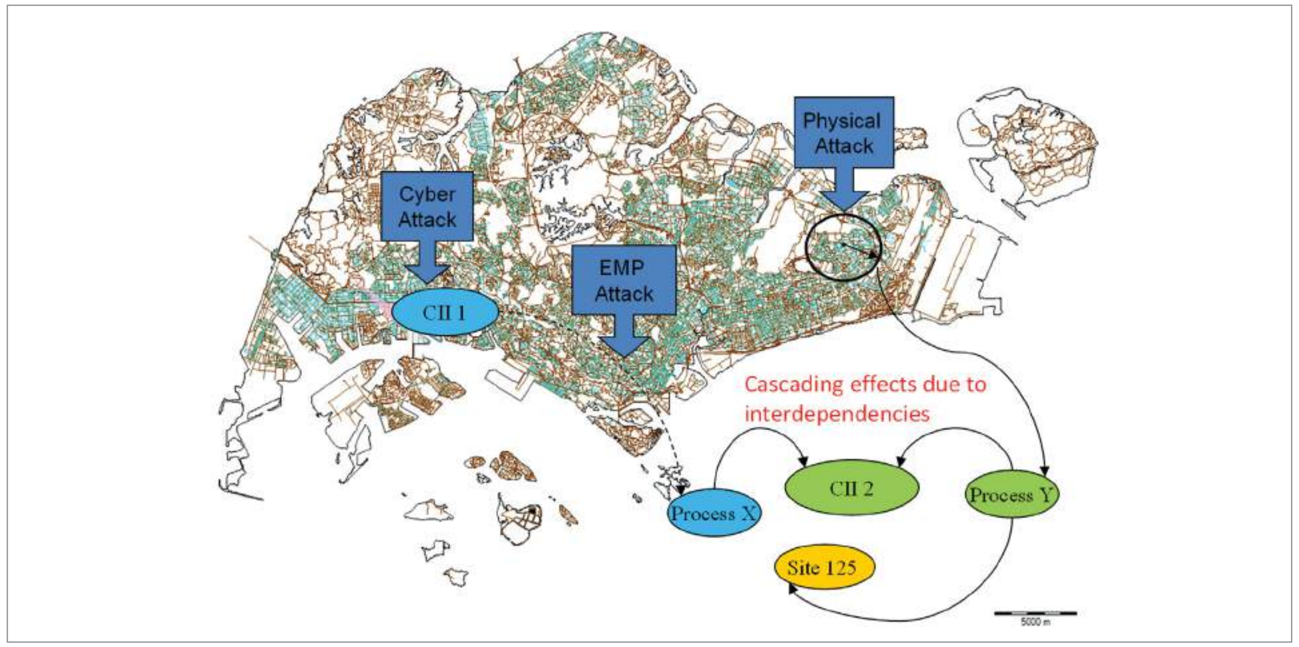
The Phase 1 findings were accepted by the National Infocomm Security Committee in early 2008 and go-ahead for Phase 2 given. Phase 2 covered detailed all-threats vulnerability assessments (VA) of a data centre and selected telecom sites. DSO applied its consequence-based methodology to the data centre and telecom sites. Our physical security, cyber, Supervisory Control and Data Acquisition, electromagnetic and weapon effect subject matter experts interviewed the CII operators, walked the grounds, probed corners, measured this and simulated that – to uncover non-obvious gaps and vulnerabilities that can lead to the CIIs being taken out, with the resulting undesired consequences.

Separately, another Phase 2 sub-team conceptualised and developed a CII interdependency model which can trace cascading disruptions due to infocomm dependencies. DSO analysts came up with the hierarchical, infocomm-based, service-oriented concept, supported by assets and telecommunications. This allows for impact forecast given a service disruption, which could be due to one or multiple asset failures, or breakdowns in telecommunications.



1. An organistion has CII(s), which it uses to provide service(s) to its customers. 2. To function, a CII depends on its assets, perhaps other CII(s) and service(s).

Hierarchical, Infocomm-Based, Service-Oriented Concept



Infocomm Inter-Dependency Analysis – Cascading Effects

The CII MSA model was used to trace the cascading impact of CII disruptions. The findings of interest, especially on key installations, were shared with MHA and SPF. These findings guided the CII owners to plug the vulnerabilities uncovered at the data centre and telecom sites.

The analysis of CII interdependencies came in useful too, when local financial institutions experienced IT system outages in mid 2010 and 2011. DSO was able to assess quickly that the outages were unlikely to spread, and that the adverse consequences were limited due to recovery processes that kicked in as planned. Building on the CII-SA work, DSO embarked on the surety assessment of other CIIs in Singapore in 2012.

Spreading the Practice of Systems Engineering

Systems engineering is a critical competency for all DSTA engineers. Project managers and their team members have to apply systems engineering in every phase of the project life cycle in order to be able to deliver an operationally effective and supportable system to the end user. Systems engineering brings with it a way of thinking, analysing and problem solving that considers not just technical but also non-technical factors. To promote systems engineering and ensure standards for good practices, DSTA collaborated with the Institution of Engineers Singapore (IES) in 2008 to launch Singapore's first certification programme for Systems Engineering professionals – the Certified Systems Engineering Professional or CSEP Certification Programme. IES also set up a technical committee to work out the certification process.

DSTA provided leadership by heading the committee and reviewing the body of systems engineering knowledge, largely distilled from the MINDEF LCM Manual. DSTA also established the Systems Engineering Course recognised by IES, derived from DSTA College milestone courses in 2008. Giving full support to the initiative, DSTA engineers contributed to case studies, conducted training and sat on the certification board.

In 2013, this certification scheme evolved into the Chartered Engineer Programme which provides professional recognition to qualified engineers across all sectors. First rolled out to the Aerospace, Chemical, Environmental, Marine and Systems fields of engineering, the programme was supported by industry leaders who signed an MOU at the opening ceremony of the inaugural World Engineers Summit held in Singapore in 2013. The MOU was witnessed by Deputy Prime Minister Teo Chee Hean, who is also Coordinating Minister for National Security and Minister for Home Affairs. DSTA was one of the 12 leading local engineering employers. Aimed at engineers who are in fields that do not require them to be registered as Professional Engineers, the Chartered Engineer title is an external validation of their experience, expertise and practising competence. This accreditation enables employers and government to access assured levels of professional competence and increase their business competitiveness in the global markets. It also serves to raise the standing of engineers in the society and encourage the younger generation to take up engineering as a career.

Chapter Eight

ADVANCING THE DTC'S SYSTEMS APPROACH THROUGH THE GENERATIONS

Is the DTC Future Ready?

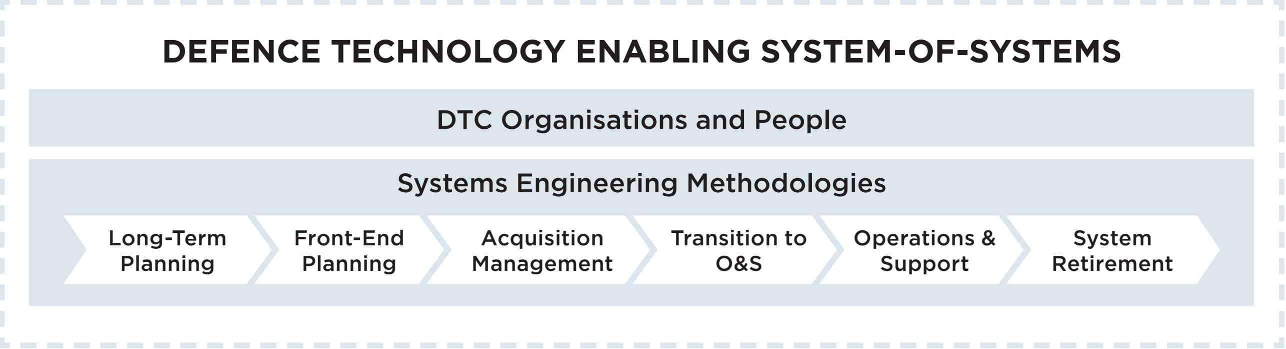
Today, our DTC is an Enabling SoS which comprises a strong network of organisations and a critical mass of engineering and scientific personnel who practise well-established systems engineering methodologies.

At its 50th anniversary milestone, the DTC is in a position of strength. Amid a time of well-deserved celebration, looking ahead, it may also be appropriate to ask two interrelated questions.

The first question is whether the DTC as an SoS can continue to enable the SAF and Singapore to maintain their competitive advantage by overcoming the challenges arising from an interconnected, complex and rapidly changing global environment. The Normal Accident Theory (Charles Perrow, 1984) offers a pessimistic view that in a world that is tightly coupled and interactively complex, system-induced accidents or failures are waiting to happen. Others have argued using the concepts of resilience engineering that we can successfully overcome these challenges, allowing us to design and develop even more complex and tightly integrated systems using potentially high-risk technologies such that we can operate at a higher level of performance yet avoiding catastrophic system failures.

The second question is whether the DTC as an SoS can ensure its continued vitality and relevance in the face of rapid continuous change. The methods and methodologies described in this volume have allowed the DTC to succeed, but is the system fleet-footed enough to make the necessary changes to maintain its vitality and relevance? What has not been sufficiently described in this volume are the soft factors relating to people, organisations and culture that have brought about the DTC's present success. Can the DTC continue to lead and enable the innovation necessary to ensure future success in an increasingly complex operating environment?

These are important questions that we may not have the answers to right now. We can, however, begin by reflecting upon some of the key qualities of our people over a 50-year journey that has brought the DTC to where it is today.


DEFENCE TECHNOLOGY ENABLING SYSTEM-OF-SYSTEMS

DTC Organisations and People

Systems Engineering Methodologies

Long-Term Planning → Front-End Planning → Acquisition Management → Transition to O&S → Operations & Support → System Retirement

Illustration of the DTC as an enabling SoS

Key Success Factors in the DTC

Key qualities displayed by successive generations of DTC members have included:

- Adopting an SoS perspective using long-term thinking, and integrated approaches, while applying systems thinking.
- Maintaining an adequate level of investments in new technologies and competencies, balanced by instilling the values of prudence and excellence at the organisational level.
- Cultivating an organisational habit of pragmatism and mission-focus, yet with the mindfulness and flexibility to be resilient to disruptive trends and shocks and to ensure that established mental models remain relevant.
- Embracing a "dare to dream" and "can do" entrepreneurial spirit to break new ground, and maintaining the appropriate risk appetite to continually test and extend the boundaries of possibilities.
- Taking responsibility to understand and master the systems to be implemented, epitomised by a "learn by doing" ethos.
- Ensuring analytical rigour in evaluating options for decision-making.
- Seeking and nurturing talents for leadership succession at all levels of the organisation.

Systems engineering leaders who exemplified the aforementioned qualities had been instrumental in infusing a similar systems approach "DNA" to others around them. If we were to trace the lineage of such systems engineering leaders in the DTC, our search would lead us to one of Singapore's pioneering leaders, Dr Goh Keng Swee.

As Singapore's first Minister for Defence, Dr Goh was known to be a hard taskmaster and a great systems thinker with a highly inquisitive mind. He applied a systems approach and introduced modern management science and rational economic thinking in the management of MINDEF and the build-up of the SAF. In fact, when Dr Goh returned to MINDEF in 1970 as its third Minister for Defence after serving three years as Minister for Finance, he demanded everyone in MINDEF to be more conscious of the importance of learning and applying modern management control techniques. The circumstances then were that MINDEF was growing rapidly in size and complexity after National Service was institutionalised in 1967, and given the urgent mission of building up the defence of Singapore arising from the withdrawal of the British forces.

He would demand for data and rigour in staff work before making any decision. He had the intellect and capacity to traverse easily from laying out the strategic geopolitical perspectives of issues to drilling into specific details when the problem demanded it.

He developed and trusted his staff, often empowering them with great authority even when they were at a young age. Dr Goh never believed in relying on "turn-key" contracts for defence equipment in building up Singapore's defence capability. He strongly felt that the process of doing the project – taking "systems responsibility" ourselves – presented great opportunities for our defence engineers and scientists to learn.

He was a man of action and because of the circumstances and extremely hostile environment immediately after Singapore's separation from Malaysia, Dr Goh instilled a great sense of urgency, the organisational habit of strategic and systems thinking, thoroughness and prudence in MINDEF and the SAF's leadership team.

Dr Goh Keng Swee – The first Systems Engineering Leader and Teacher in MINDEF

Minister for Defence, Dr Goh Keng Swee (left) being welcomed by MAJ Michael Teo during Dr Goh's visit to Tengah Air Base in 1976

"The first generation of political leaders – like Dr Goh Keng Swee… were men of principles and conviction. The values they brought would be transmitted to the young civil servants who worked directly for them. This pioneering generation of civil servants in turn would rise to become heads of ministries, passing on time-tested values to their younger counterparts. In this inter-personal way, before induction or training was systematised, values were transmitted and methods of doing things spread through a process of osmosis."

"Among the first generation of ministers, it is Dr Goh Keng Swee who is most often cited by senior civil servants today as a key influence in their personal lives, and in the Civil Service as a whole. Dr Goh was a visionary and implementor extraordinaire, whose capabilities and interests ranged far and wide. An economist by training, he was instrumental in the whole gamut of Singapore's early nation-building efforts: industrialisation, defence, finance, education… His wide range of interests meant he worked with a cross-section of civil servants from different generations. Some civil servants in their 50s or early 60s and still active in Public Service today recall him with affection and respect."

"Said Eddie Teo, [who was Director of Security and Intelligence Division before serving as Permanent Secretary for Defence from 1994 to 2000] chairman of the Public Service Commission, on Dr Goh, "His secret was his ability to reach down to very young officers and deal with them one to one because once he does that, then he develops in you total loyalty… So he had this ability to reach out to the people that he wanted views from. He doesn't care about rank and hierarchy and all that. And in return, I think these young officers then felt motivated to work, stay in the Civil Service, whereas if you observed hierarchy and just talked to the director and ignored all the other people, you don't develop that kind of personal loyalty."

"Apart from the spirit of austerity, Dr Goh is said to have imparted two other key values to the Civil Service. One is a habit of rational economic thinking… Dr Goh's other major influence on the Civil Service lay in his own personality. He was a temperamental, passionate man given to exploring wild ideas, who started off with the premise "why not" when confronted with a new scheme. He expected officers working for him to act likewise. The result: a high-energy, risk-taking culture was embedded in the ministries Dr Goh headed. And because he was so powerful and charismatic a leader, his staff knew they had his backing even if they did not quite play by the rules. Philip Yeo [one of the longest continuous serving administrative officers in MINDEF] is candid that without Dr Goh, he would never have cut it as a civil servant. Mr Yeo… was the resident maverick in the public sector, saying Dr Goh shielded him from other higher-ranking officers' wrath."

"Herman Hochstadt, who was Permanent Secretary in several ministries through the 1970s and 1980s, described Dr Goh as someone who fostered an entrepreneurial, risk-taking culture by the way he dealt with mistakes. "What he tried to put forward is that you can make a mistake but if it's a genuine mistake, you make it, but don't make it again. Don't make the same mistake again. Then if I tell you to do something, get it done. Don't just run off somewhere and keep quiet." Lim Siong Guan, who also worked for Dr Goh [and served as Director of Logistics Division as well as Permanent Secretary for Defence], recalled that he was a minister who gave even junior officers a lot of leeway, so that young officers cut their teeth on exciting projects."

(Extracted from "Pioneers Once More – The Singapore Public Service 1959 - 2009", pages 72-74).

Dr Goh shared his knowledge freely with his staff. He would explain his decisions and in the process coach and develop his staff into confident leaders. Those who had worked directly with Dr Goh became good systems thinkers and teachers as they led the build-up of MINDEF and the SAF.

"It's people and organisations that live and grow and appreciate over time, while equipment depreciates. It's people that make the difference, not the hardware."

Prof Lui Pao Chuen
Extracted from the book "Singapore's Scientific Pioneers", page 65

A lineage of systems engineering leaders emerged out of Dr Goh's influence, be it directly or indirectly, and made an impact in shaping the DTC to where it is today. Among them, many were honoured for their contributions during the DTC Pioneers' Dinner on 6th May 2015 – Dr Tony Tan, Mr Lim Siong Guan, Mr Philip Yeo, Mr Teo Ming Kian, Mr Peter Ho, Prof Lui Pao Chuen, BG (Ret) Wesley D'aranjo and Prof Su Guaning.

There are also many other unsung heroes who had left a mark in shaping the DTC as an Enabling SoS comprising a diverse range of capabilities, infrastructures, encoded best practices as well as confident and competent engineering and scientific professionals.

Extending DTC's Legacy through Future Generations

"Over the past decade, there have been instances when other agencies lamented their loss of such professional expertise. During those moments, MINDEF and the SAF can count ourselves fortunate that our leaders had recognised the critical need to develop our indigenous technology and engineering capabilities for our defence needs, and have thus retained this essential community. Many of you here recognise the often used phrase – the secret edge weapon. The weapon that gives us an edge in protecting us. Let me say that today that the DTC is our secret edge weapon."

Dr Ng Eng Hen
Extracted from keynote address at the DTC Pioneers' Dinner on 5th May 2015

As we reflect on the development and growth of the DTC, one cannot help but recognise the impact of the first generation of leaders who led MINDEF and the SAF. It started with Dr Goh Keng Swee, the first Minister for Defence, who seeded and cultivated the organisation culture that enabled many generations of systems engineering leaders in the DTC to dream, do and share lessons learned to build defence capabilities for a strong SAF.

Today, the DTC possesses a cutting edge because of its people who have continually grown with time and experience. They are the backbone and lifeblood of the DTC Enabling SoS, and their ingenuity, passion, and shared vision are crucial ingredients in facing and dealing with the unknowns of tomorrow. So, as the DTC navigates into its next 50 years of unchartered waters in an increasingly complex world, it is our hope that new generations of Singaporeans will arise to take on the mantle of defence engineers and scientists to extend the legacy of our systems engineering leaders, and secure the happiness, peace, prosperity and progress of Singapore.

Key Leaders in Systems Engineering

As Deputy Prime Minister and Minister for Defence from 1st August 1995 to 31st July 2003 and Deputy Prime Minister and Coordinating Minister for Security and Defence from 1st August 2003 to 31st August 2005, **Dr Tony Tan Keng Yam** was instrumental in the development of the DTC. Under Dr Tan's leadership, Singapore built up its defence industry infrastructure in areas that were strategic to MINDEF and the SAF. He oversaw the corporatisation of the Defence Science Organisation as DSO National Laboratories in 1997. This move allowed the organisation to develop collaborative links with research establishments. Under his guidance, the first Temasek Laboratories – a collaboration between DSTA and the National University of Singapore – was established in 2000. The transformation of the DTC through the consolidation of defence technology organisations under a single statutory board, DSTA, would not have been possible without Dr Tan's foresight, leadership and guidance. The formation of DSTA coalesced MINDEF's efforts in defence technology acquisition and management. The steady investment of resources towards the development of an indigenous defence technology capability under Dr Tan's leadership gave the SAF a strategic technological edge.

The contributions of **Mr Teo Chee Hean** to the DTC started when he was with the SAF. As a Naval officer, he worked closely with DSO on the use of technology to advance the RSN's capabilities. As Head of Naval Plans and subsequently as Chief of Navy, his far sightedness and strategic perspectives were instrumental in the visioning, conceptualisation and development of the Navy to what it is today. The long-term plans that he put in place led to the build-up of many significant capabilities in the DTC through the different projects that it undertook for the Navy over the last few decades, including the development of the Changi Naval Base, the frigates and the submarines. As Director of Joint Operations and Planning Directorate, Mr Teo was one of the early advocates for better integration between the technology and operations communities to build trust and confidence between the two communities – well before the term "ops-tech integration" was coined. As Second Minister for Defence in the 1990s and later on as Minister for Defence till 2011, he was instrumental in rationalising and restructuring the C3 communities within the DTC. The directions and guidance that he provided as Minister had strategic impact on the transformation of the SAF into the Third Generation fighting force. The SAF's Third Generation journey has led to the build-up of strong indigenous capabilities in critical areas for our defence in DSO, DSTA and in our local defence industry.

As Permanent Secretary (Defence), **Mr Lim Siong Guan** developed strategic ideas and programmes that bolstered MINDEF's ability to plan for the future, yet had the capability to respond to different challenges and unexpected developments. Under his leadership, the SAF embarked on the upgrade and modernisation of its services to become a Second Generation fighting force. He expanded and strengthened defence relations with key countries. There was increased collaboration between MINDEF and the local defence industry. Mr Lim launched the MINDEF Productivity Movement to encourage innovations and initiative in MINDEF and SAF operations including defence technology, and introduced scenario planning to deal with different possible futures. He established the Joint Operations Committee that brought about better integration within the SAF as well as with the logistics and manpower divisions in MINDEF, which later developed into the Joint Operations and Planning Directorate. Mr Lim introduced the concept of Total Defence to enhance and encourage the holistic commitment of all Singaporeans in defending the nation.

Mr Philip Yeo Liat Kok was instrumental in building up Singapore's defence industry and strengthening the indigenous engineering capability in providing the secret edge in defence. He was concurrently also the founding Chairman of the National Computer Board from 1981 to 1987. Under his leadership, MINDEF systems engineers spearheaded the national computerisation effort of Singapore. Because of his determination and persistence, MINDEF was the first ministry to computerise in a significant way, paving the way for the rest of the public sector to adopt computerisation. As the Chairman of the DSO Executive Committee, Mr Yeo led DSO to refocus and become steadily more capable in several core areas, including electronic warfare, guided systems and cryptography. He drove efforts to build the competency of defence scientists and engineers by creating postgraduate and training opportunities, which raised Singapore's engineering capability to develop breakthrough work and defence innovations. Under his leadership, MINDEF adopted a higher profile to recruit engineers and scientists from local universities, which augmented MINDEF's manpower resources to staff defence technology projects and begin new project teams.

Mr Teo Ming Kian led the DTG formed in 1986, to bring about a new synergy and integration to the logistics, technology and research arms of MINDEF and the defence industry. He sharpened DTG's mission to "Engineering the Nation's Defence" by leveraging technology as a force multiplier for the SAF. To achieve the mission, Mr Teo built an engineering and technological capability to acquire, customise, upgrade and indigenously develop and produce systems and equipment to meet the specific needs of the SAF. Under his leadership, MINDEF moved from being a "smart buyer" to being able to selectively develop in-country defence capabilities as well as ensuring life-cycle operational readiness. He was instrumental in pushing for the design and development of systems such as the FH88 Howitzer, the Bionix Infantry Fighting Vehicle, the Endurance class LST and the Super Skyhawk. He also strongly supported the build-up of several secret-edge capabilities in the DSO. The success of these programmes, which demanded quantum leap in local production capabilities and risk appetite, provided the confidence for subsequent development of other new defence systems.

Mr Peter Ho Hak Ean played a pivotal role in driving the transformation of the SAF into a Third Generation military. He initiated the modernisation of Singapore's defence capability to enable the SAF to exploit new concepts and technologies to better deal with new threats. His foresight and leadership strengthened Singapore's defence and security. Mr Ho pushed for the corporatisation of DSO in 1997. He oversaw the formation of DSTA in 2000. He played a key role in creating the necessary "white space" for defence research and technology efforts. His leadership was instrumental in strengthening defence technology collaboration with other countries. Mr Ho charted the way forward for defence engineers and scientists to contribute beyond defence. The Risk Assessment and Horizon Scanning Experimentation Centre was his brainchild. The centre now serves as a shared platform for analysts from different agencies to collaborate on perspective sharing, modelling and research. Mr Ho played an instrumental role in rallying crucial support across ministries and agencies, and enabled the DTC to make impactful contributions in the fight against the SARS outbreak in 2003.

Professor Lui Pao Chuen was one of the first scientists who joined MINDEF. Since taking charge of the Test, Evaluation and Acceptance Section in 1966, he had built Singapore's engineering capabilities to manage large-scale defence programmes. He led the development of the SAF's first command and control systems, and contributed significantly to master planning and project implementation efforts that turned Tengah Air Base and Paya Lebar Airport into modern operational airbases. As Singapore's first Chief Defence Scientist, Professor Lui guided the development of various technology agencies to explore new technologies and innovative concepts. He spearheaded the development of Singapore's first Underground Ammunition Facility. He played a vital role in planning and developing the network of radar, weapon systems and civil defence shelters for Singapore's integrated air defence. In the 1980s, Professor Lui advocated the creation of a 1,000-strong community of engineers and scientists. His emphasis on people development has grown the DTC into a world-class defence technology outfit. He steadily built up operations analysis and systems engineering expertise in MINDEF. He steered efforts to tap the capabilities of local universities and research institutes, which paved the way for the establishment of Temasek Laboratories in the various universities.

Er. BG (Ret) Wesley D'aranjo was pivotal in transforming DMO into a highly professional and respected systems acquisition authority. He institutionalised a total system approach in project management and led the design of MINDEF LCM. As DS(T), he had executive authority over all organisations of the DTG. He was instrumental in building Singapore's capabilities in defence R&D, large-scale systems integration, development and acquisition, and procurement and contract administration. He oversaw C4I development, building and infrastructure development and corporate planning for DTG, as well as strategic resources and defence industrial capability. He played a pivotal role in advancing the command and control capability that became the core of the C3 Systems Organisation and later the IT group in the DSTA. He provided professional direction to the Logistics Departments of the SAF. Er. BG (Ret) D'aranjo placed much emphasis on nurturing scientific and engineering expertise, and contributed significantly to the build-up of technological capabilities in MINDEF and the SAF. Through his efforts, MINDEF built closer ties and embarked on R&D initiatives with several international research institutes, military establishments and the local academic and scientific community.

Professor Su Guaning was one of Singapore's first defence research engineers and led the initial build-up of electronic warfare capability in Singapore. Under his stewardship, DSO grew in capability and size to become the largest research institute in Singapore with world class competencies in defence technology. He led the corporatisation of DSO to ensure clarity of mission, autonomy and responsiveness to the SAF's needs, serving briefly as Chief Executive Officer in 1997. Professor Su was instrumental in pushing for the establishment of DSTA and became its first Chief Executive in 2000. He established DSTA as an innovative and effective organisation in providing defence technology support to MINDEF and the SAF. He established DSTA as a knowledge-based organisation, with sound defence technological competencies – in acquisition management, operations and support, technology management and information technology. Under his leadership, DSTA made great strides in meeting the evolving needs of the SAF and delivering cutting-edge solutions to the SAF. DSTA also extended its collaborative network to include renowned institutions and agencies, including the US Defense Advanced Research Projects Agency (DARPA).

References:

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies.* Princeton, New Jersey: Princeton University Press.

Chua, M. H. & Kwek, K. (2010). *Pioneers once more: The Singapore Public Service, 1959 – 2009.* Singapore: Straits Times Press.

Chan, J., Chua, G., Sim, S., & Tan, R. (2015). *Singapore's scientific pioneers.* Singapore: Asian Scientist Publishing Pte Ltd.

Chapter Nine

BEYOND DTC50

By Quek Tong Boon, Co-chief Editor of DTC50 Book Series

Ten years ago, nobody had heard of the iPhone, iPad or ISIS. Yet today we live in a world with our lifestyles shaped by the likes of the iPhone and iPad, and with ISIS[1] claiming responsibility for many of the terrorist attacks worldwide over the last two years. The Economist, in its 2nd January 2016 article on "Election Forecasting – Prediction 2016", concluded that "at the time of writing, PredictIt[2] reckons that the fight for the Republican nomination is between Ted Cruz and Marco Rubio, and that Hillary Clinton has a 54% chance of becoming the next president." No mention of Donald Trump at all! Speculating about the future is a perilous undertaking[3]!

Given mankind's egregious record of predictions, to predict what the DTC would be like or which technologies would prevail for our defence in the coming decades would be to repeat a perennial folly. We will instead highlight some of the driving forces that could shape the evolution of our defence technology landscape over the next decade or so.

In the DSO 30th Anniversary Commemorative Book "Creating the Technology Edge" published in 2002, as then Chief Executive Officer of DSO National Laboratories, I wrote in the concluding chapter entitled "Back to our Future" that advances in sensors, communications, information processing, networks and unmanned systems "would have profound impact on the future of warfare. Analogous to what is happening in the commercial business world; the transformation in the military is towards operations that are more integrated and knowledge-based". The commentary also observed that expertise built up for defence could be adapted to address the more complex national security challenges that have emerged in the 21st century, especially in the wake of the September 11 World Trade Centre attacks in the US in 2001.

Since 2002, the world has become even more connected. Social media has not only taken off but also become integral to many people's lifestyles. Advances in computer processors, software, sensors and nanotechnology have surpassed expectations at the turn of the century. Only the most optimistic would have predicted then that by 2016, we would have computers and algorithms that can listen and speak to us, write prose, beat human champions at the ancient oriental game of Go (considered cognitively more complex than chess) and diagnose diseases! The iPad2, launched in 2011, was benchmarked in a 2012 study by researchers at the University of Tennessee to be as fast as the Cray-2 vector supercomputer, the world's fastest computer in the 1980s.

The continued advancement and proliferation of the above technologies, in tandem with emerging technologies such as additive manufacturing, robotics, cloud computing, machine learning, natural language processing, augmented reality, precision medicine and neurotechnology, promise to disrupt the way we live, work, play and interact in the coming decades. Take play, for example. Augmented reality was the

[1] Islamic State of Iraq and Syria, also known as Daesh or ISIL (Islamic State of Iraq and the Levant). It became prominent in early 2014 when it drove Iraqi government forces out of key cities in western Iraq.

[2] PredictIt is a New Zealand-based prediction market that offers prediction exchanges on political and financial events. It is owned and operated by Victoria University of Wellington.

[3] One of the rare exceptions is the observation made by Dr Gordon Moore in 1965 for semiconductor development, encapsulated in what has since been called Moore's law. Its prediction on the exponential increase in number of transistors that could be packed into a chip has been largely on track for the last 50 years but there are some recent indications that it could finally be running out of steam.

wind in the sails of the Pokémon GO[4] mania that swept through Singapore within hours after its launch on 6th August 2016, mirroring its worldwide phenomenal success. In the manufacturing sector, relentless digitisation has led to new operating paradigms that usher in the age of Industry 4.0[5], a term first used in 2011 at the Hannover Fair. This purported "fourth epoch" of the Industrial Revolution promises increased flexibility in manufacturing, mass customisation, increased speed, better quality and improved productivity. Additive manufacturing will also enable rapid prototyping, decentralised production and on-demand logistics – disrupting traditional supply chain models.

In 2014 professors Erik Brynjolfsson and Andrew McAfee of the Massachusetts Institute of Technology published their seminal book "The Second Machine Age." Since then, countless articles have echoed their vision of the rise of smarter machines that could work tirelessly on routine jobs, and increasingly, on jobs that require higher cognitive skills too.

Unfortunately, the abuse and nefarious use of technology has also become more pervasive, more intense and more sophisticated. Criminals cloaked by encryption and the dark web can now operate more stealthily. Social networks have made it easier for terrorists to globalise their messages of hate and violence; extremist propaganda and radicalising appeals jostle alongside inane videos and news bites on social media.

In the defence domain, our systems have become more networked and knowledge-based, enabling greater integration and precision in SAF operations over the last decade. This is exemplified by several of the stories that we have shared in this DTC50 book series, in particular this book on systems-of-systems.

Our defence systems will be transformed by the next wave of technological advances. How so will depend, in part, on the answers to the following questions: What would be the parallel in defence to Industry 4.0 or our digital economy? How far can we leverage the innovations spawned by the digital revolution to significantly mitigate our security and demographic challenges? Can concerns related to security, safety, ethics and complexity of autonomous capabilities be adequately addressed and managed to avoid the dystopian nightmares of sci-fi movies? With information becoming an increasingly important dimension of warfare, how will it shape the evolution of warfare and threats? More generally, will non-kinetic means of warfare finally come of age to complement the use of kinetic means in future warfare? At the hardware level, the premise that computer chips would do more and more, yet cost less and less, in accordance with Moore's law, has driven many of the innovations over the 50 years. When this law hits its limits, what will be the impact on the pace and nature of technological innovation?

Digitisation provides opportunities for the defence community at three levels. First, internally within our organisations and in the products, systems and solutions that we develop, enablers such as machine learning, robotics and additive manufacturing have the potential to significantly increase their leverage and multiplier effects.

At a second level, harnessing the potential of analytics, cloud computing, cyberspace, networks, the internet of things and perhaps even blockchain[6], could allow us to reap benefits at the cross-organisational and system-of-systems levels. Employed judiciously, such technology will drive global optimisation and integration of our resources and assets to an extent not possible before.

At the third level, technological enablers combined with changes in mindsets, processes, systems and structures could transform how we lead, educate, organise, train, and operate. Increasingly competent and smart machines, working in unison with our soldiers, commanders and planners (themselves possibly augmented by advances in the cognitive and biomedical domains), could enable us to overcome challenges that are even more complex and intractable than what we have been able to do so far.

At the same time, we should be mindful of the opportunities created by the availability of COTS technologies for military use. Many technologies that we take for granted today such as the computers, internet, and global navigation can trace their origins to the R&D investments by the US defence community. However, it is exploitations by the commercial sector that have made possible their economies of scale, accessibility and affordability, to the extent that even the US military is heavily reliant on the commercial sector to provide dual-use technologies today.

Will the commercial sector continue to adopt technologies seeded by defence R&D? Looking at the examples of autonomous vehicles and more generally robotics, the answer is probably still yes. Over the last few years, driverless vehicles have come to the forefront of public awareness. It was however the series of three grand challenges organised by the DARPA from 2004 to 2007 that sparked interest in the development of autonomous vehicles. Since then, DARPA has focused its grand challenges in the areas of robotics and cybersecurity. The finals of the fourth DARPA grand challenge took place in June 2015. Spurred by the 2011 Fukushima nuclear disaster, its theme was on robotics to aid in disaster recovery. There was intense interest by the industry in the proceedings and outcome of the challenge. Weeks before the challenge itself, news leaked out that Uber was hiring 40 researchers from National Robotics Engineering Center (NREC) of the Carnegie Mellon University to kick-start its own autonomous car capability. As the loss accounted for about a third of NREC's robotics talent pool, the exodus dealt a blow to the centre's capabilities. Other everyday technologies which have benefitted from past defence investments include the Apple Inc's Siri[7] software assistant and iRobot's Roomba vacuum cleaning robot: the room-cleaning algorithm used in Roomba is similar to the mine-hunting algorithm that iRobot developed for the US military.

Fortunately, this flow of ideas is bidirectional. The defence sector is increasingly benefiting from technologies that originate from the private sector too. Large technology corporations such as Google, Microsoft, IBM, Amazon and Space X are now investing in moonshot projects ranging from quantum computing to reusable space launchers which in the past would have been driven more by government R&D agencies.

Greater reliance on the more nimble commercial sector for defence technologies will change technology refresh rates and developmental cycles. In some areas such as software and algorithms, there is a blurring of lines between research, development, engineering, production, and even operations.

[4] A location-based augmented reality video game initially released in selected countries by Nintendo on 6th July 2016.

[5] Industry 1.0: Water/steam power to mechanise production; Industry 2.0: Electric Power for mass production; Industry 3.0: Electronics and ICT to automate production; Industry 4.0: Digital revolution characterised by fusion of technologies that is blurring the lines between the physical, digital, and biological spheres.

[6] The technology that enables secure bitcoin transactions to take place.

[7] The Siri intelligent software assistant which is now part of Apple Inc's iOS is an offshoot of the DARPA-funded CALO project. CALO ("Cognitive Assistant that Learns and Organizes") was an artificial intelligence project that attempted to integrate numerous AI technologies into a cognitive assistant for military applications. In fact, the name CALO was inspired by the Latin word "calonis," which means "soldier's servant".

These trends could change the nature and dynamics of the relationships between the users, developers, industry, and service providers in the coming years. They could also accelerate the pace of defence capability developments in future. In order to tap on the high tempo and highly creative energy of companies operating at the cutting edge of technology, the US Department of Defense has recently set up an office known as DIUx (Defense Innovation Unit Experimental) with outposts in Silicon Valley and Boston to accelerate the flow of innovations from non-traditional sources to US warfighters.

Within Singapore, the success of Block 71 at Ayer Rajah is a hopeful sign that our initiatives to promote entrepreneurship and encourage start-ups in Singapore could finally be bearing fruits. Echoing trends across the Pacific, the DTC has contributed to the genesis of some successful high-technology start-ups in Singapore. Some, such as D'Crypt Pte Ltd (dealing with the design and development of cryptographic technology and devices) and Lighthaus Pte Ltd (dealing with the design and development of optronics technology) were founded by ex-DSO[8] staff. Others, such as Hope Technik, Microfine Materials Pte Ltd and Denselight Semiconductors Pte Ltd cut their teeth by working on defence-related projects during their formative years. In the coming years, I expect the relationship between the defence industry and our start-up scene to become yet more entwined, contributing to a more vibrant innovation ecosystem in Singapore.

How we in Singapore organise ourselves and what systems and policies we put in place in future to develop our technologies, manage our acquisitions and undertake our logistics could be fundamentally impacted by these trends.

Singapore’s size and resource limitations should not limit our ability to be bold in our dreams, holistic in our approach and daring in our executions. In fact, many of the stories shared in this DTC50 book series were sparked by the desire to overcome or mitigate our constraints and limitations. We owe much of what the DTC is capable of today, as typified by the system in the opening page of each of the 4 books in the series, to the scientists and engineers who laid the foundations for such capabilities. Who are the people whose decisions and actions will weave the DTC75 or DTC100 narrative? What technologies and capabilities that they develop will come to the fore? Only time will tell. Our future generations of defence scientists and technologists are still studying in our universities and schools today. Their dreams, decisions, projects and actions in the DTC will shape our future stories.

What will remain evergreen is this: the DTC’s ability to continue to attract scientific, technological and engineering talents from each cohort will undergird its ability to sharpen the cutting edge for Singapore’s defence and national security. Our future generations must respond to problems that are likely to be less well-defined, with technologies and solutions that are less well-trodden, less proven, more adaptive and less structured. Curiosity, risk-tolerance and experimentation must be even more integral to the DTC DNA in the future.

It has been an exciting five decades for the various generations of defence scientists, engineers and technologists. Our inexperience did not deter us from having bold dreams; our resource limitations did not diminish our tenacity to execute them; our failures did not discourage us from picking up, learning from them and getting our jobs done. That in essence is how we have been able to engineer the defence technological capabilities of Singapore to what they are today. We hope that the stories that we have shared will inspire those who are taking over the batons from us to have the same guts and gumption to engineer our future defence with ingenuity. As Peter Medawar, the British scientist said in his 1959 book, The Future of Man,

> *“The bells which toll for mankind are — most of them, anyway — like the bells of Alpine cattle; they are attached to our own necks, and it must be our fault if they do not make a cheerful and harmonious sound.”*

[8] D’Crypt was co-founded by Antony Ng and Chew Hwee Boon in 2000 and Lighthaus by Phua Poh Boon in 2011. All were ex-DSO researchers.

References:

Chew, M., & Tan, B. (2002). *Creating the technology edge.* Singapore: DSO National Laboratories.

Dongarra, J., & Luszczek, P. (2012). Anatomy of a globally recursive embedded LINPACK benchmark. *IEEE Conference on High Performance Extreme Computing* (pp. 1-6). doi: 10.1109/HPEC.2012.6408679

Kagermann, H., Lukas, W. D. & Wahlster, W. (2011, April 1). Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. Industriellen Revolution. *VDI Nachrichten*, pp. 2.

Brynjolfsson, E. & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies.* New York: W. W. Norton & Company.

Appendix to Chapter 2

Systems Architecting as an Approach to Develop System-of-Systems

SA is considered both an art and a science to realise SoS capabilities.

SA is an art because an SoS solution is often derived from discussions and negotiations with multiple stakeholders of individual systems. This involves managing and balancing divergent stakeholder interests in order to achieve a "global optimum" for the SoS solution. Often, it is not possible to arrive at the SoS solution purely through engineering analysis due to the interests of individual stakeholders. The SA team may have to bring certain stakeholders on board to communicate SoS concepts with the goal of arriving at a consensus (or at least a compromise) on the SoS solution. For example, the considerations in determining if an air defence SoS should have more airborne or ground-based systems may go beyond analysing their respective system performances, and also include non-measurable factors such as managing the continuity of various air defence squadrons and personnel skill sets. This is especially so should there be significant changes proposed to the existing air defence force structure. Indeed, the SoS solution is often derived through consultation with key decision makers and stakeholders, and by leveraging the holistic experiences of leading domain experts and thinkers, senior commanders, as well as other established large-scale systems engineering practitioners.

On the other hand, SA is a science because it uses architecture as a tool for addressing global integration, consistency and integrity in SoS design. It can also involve an analytical exercise to determine the optimal combination of resources (people, organisation, equipment and weapon), systems (hardware, software and network) and their interactions to achieve the desired outcome. For example, a more capable air surveillance network may reduce the need for more fighters on alert, thereby lessening the stress on ground resources. Operations research as well as modelling and simulation may be carried out to analyse such interdependent relationships and determine the optimal combination.

Comparing SA and Traditional Systems Engineering

Taking another angle to appreciate how SA would be a new competency within the DTC, we could compare and contrast it with the traditional Systems Engineering (SE) approach that had been largely practised within the DTC up to the 1990s.

	Traditional Systems Engineering	Systems Architecting
Scope	User Requirements, System Design and Development, Project Management, Maintenance and Retirement	Operational and Systems Concept Formulation/Force Structure and Capability Development
Stakeholder	Usually one major customer	Multiple, Interdependent Relationships
Emphasis	Deals with measureable, Technical Feasibility and Design	Deals with immeasurable, collaboration, heuristics, added ilities such as flexibilty, adaptability and scalability
Timeframe	System Life cycle	Multiple, interacting system life cycles
Trade Off	System level	Enterprise level

Comparison between traditional SE and SA

The scope for traditional SE encompasses the specific user requirements, system design and development, project management, maintenance support and retirement, while SA is concerned with operational and systems concept formulation, force structuring and capability development. The traditional SE approach is applied when the space constraints are well defined to develop a system while SA is applied when the solution space is much larger and operational concepts are generally evolving. For example, the acquisition of a system may typically be undertaken within the constraints or assumptions such as available power supply, physical space, rules and regulation. Taking an SA approach can facilitate the re-examination of such constraints or assumptions to open up new possibilities and solutions for the desired capability.

In SA, the needs of multiple and interdependent stakeholders have to be addressed. In traditional SE, each system usually has a major stakeholder, i.e. the customer who funds the system acquisition and development. Hence, SA emphasises collaboration among stakeholders towards a common goal. Similarly, SA needs to address multiple, interconnected and evolutionary system life cycles to maintain a robust and coherent SoS architecture.

As mentioned earlier, an SoS is simply too complex to be treated by quantitative engineering analysis, technical feasibility study or design alone. SA is hence employed to help the designer to visualise, conceptualise, plan, create and build such an SoS. It aims to bring together various systems with the purpose of achieving operational capabilities greater than the sum of what each individual system can provide.

SA deals significantly with non-measurables using non-quantitative tools and guidelines based on practical lessons learnt. In addition, SA seeks to address non-functional attributes known as "ilities". Some examples of "ilities" are flexibility, scalability and adaptability of an SoS architecture.

Last but not least, trade-offs are made at the enterprise level for SA instead of at the system levels for traditional SE. In summary, SA deals with a much greater level of complexity and scale due to multiple interacting systems.

DTC's Journey in Systems Architecting

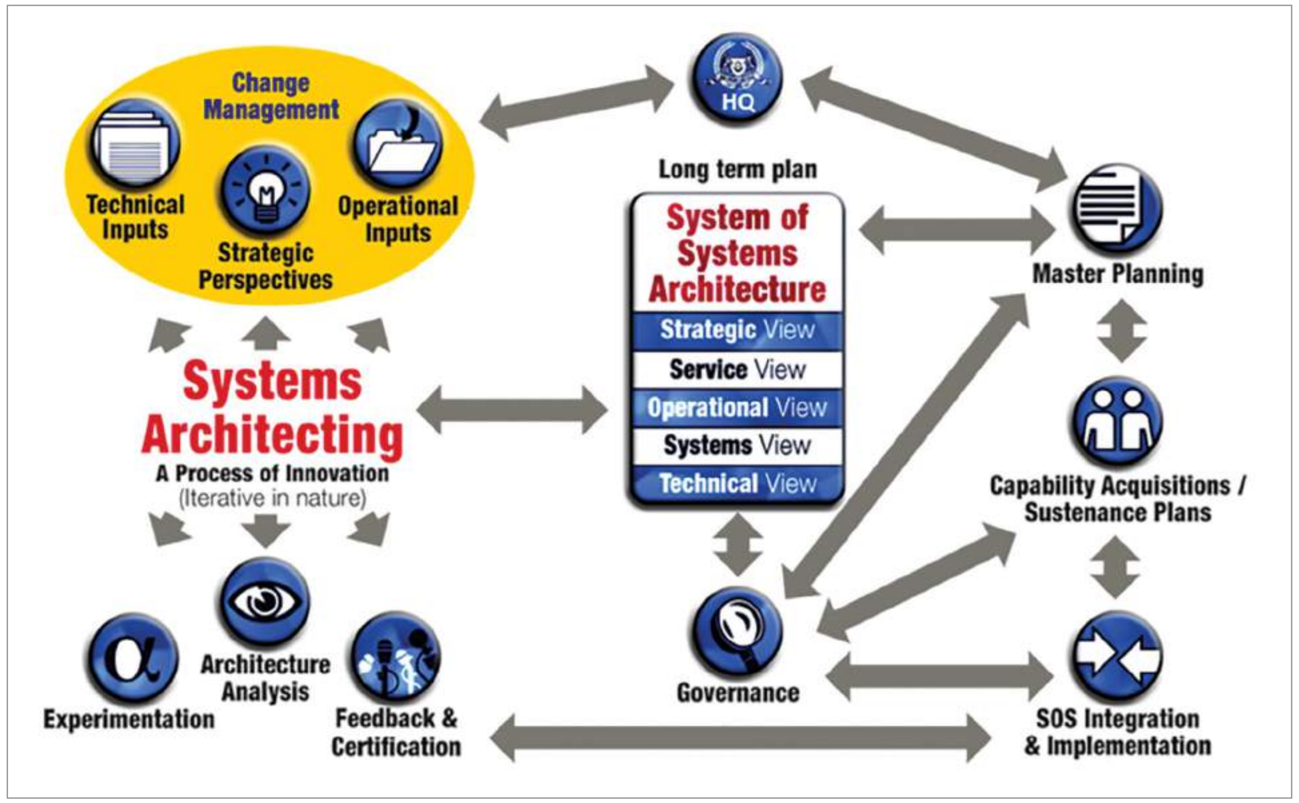
For SA to be successful, it was and still is truly an approach that involves stakeholders in MINDEF, the SAF and the DTC collaborating and converging towards desired Defence SoS solutions. A holistic set of considerations for SA is summarised in the SA Framework for the DTC.

SA Framework

The purpose of the SA framework is to guide our work in developing a robust, coherent and enduring SoS architecture. Building an effective SA involves innovation and is iterative in nature.

- Inputs from the strategic, operations and technical perspectives are important ingredients. The strategic perspective considers the political, environmental, social, and technological factors, as well as the strategic intent put forth by key stakeholders. The operational perspective looks into the mission objectives, potential threat assessment, existing capabilities, resources and operational constraints. The technical perspective takes into account the existing technological capabilities, legacy systems, emerging technology and the physical environment. Where necessary, architectural studies using operational analysis, modelling and simulation techniques, as well as experiments, may be conducted to evaluate alternative architectures.

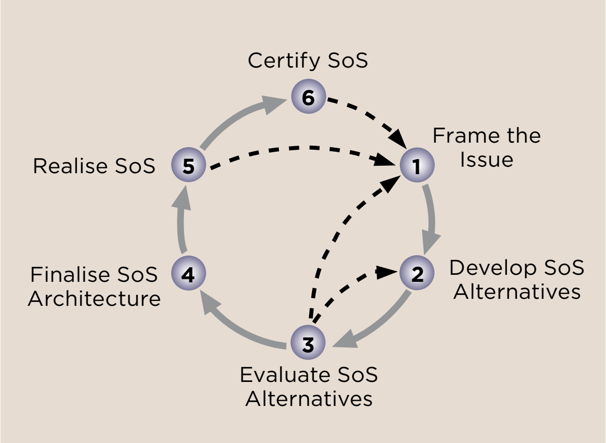
- While the strategic, operations and technology domains are important ingredients for SA, it is the creativity of the integrated SA team in exploiting new technologies, organisational and systems boundaries to devise new and realistic concepts of operations that will determine the effectiveness of the SA. SA involves the active collaboration and co-creation of the SoS architecture by all domain experts. Quality facilitation and effective change management during the SA process is emphasised to expand systems and organisational boundaries as well as to generate dialogue among stakeholders.
- The SoS architecture can be described in operational and technical views. In general, design artefacts can aid in effective communication, knowledge retention and managing complexity. The SoS architectural views can serve as a common language for multiple stakeholders to communicate in a consistent manner. The focus is usually on the organisational boundaries and systems interface. More importantly, these views can highlight integration issues among the component systems and become part of a framework to facilitate SoS governance. Governance will play a critical role in effective synchronisation, interoperability and management of multiple programmes to realise the SoS capabilities. To date, an Enterprise Architectural Framework for developing C2 systems has been established with a governance process to facilitate the alignment of technical implementation with operational needs.
- The endorsed SoS architecture will guide the formulation of various master plans. These views serve as the blueprint for development of various OMP and EMP. Approval of these OMPs and EMPs will lead to individual system acquisitions and sustenance plans. The SoS integration and implementation of component systems will be led by the various IPMT. Verification, validation and certification efforts of the SoS will serve as feedback to ascertain if the intent and desired capabilities of the SoS have been realised.



SA Framework

The SA Process

In addition to the above framework, a six-step SA process has been developed to guide Systems Architects in their work.



The SA Process

This process adopts a life cycle perspective and is developed with simplicity and flexibility in mind. It is also iterative in nature, which is expected as the realisation of SoS spans many years. Hence, changes in external environment, for example, may warrant a need to re-examine the SoS architecture. The dotted arrows represent the need to refer back to the earlier steps to verify and evaluate the SoS when necessary. This process is generic in nature and can also be extended to different levels of SoS complexity from capability to individual component system.

- Step 1 – Frame the Issue
  SA is driven primarily by the user's purpose and needs. A successful system is one where the user's intent is served at an affordable cost within an acceptable period of time. Hence, the first step in the architecting process is to frame the issue. It aims to discover the higher intent of user-articulated needs and objectives, and to discover the underlying assumptions, constraints and limitations. This allows a rich and unified picture to be formed in order to address the issue. This step will facilitate the involvement of necessary stakeholders so that the right issues are addressed. This will require an examination of strategic, operational and technical perspectives to gain a deeper understanding of the matter in hand.

- Step 2 – Develop SoS Alternatives
  This step is undertaken to generate a broad range of alternative SoS architectures to address capability gaps. The emphasis is on the exploration of the solution space and to consider solutions involving any combination of doctrine, organisation, personnel, training, systems facilities, emerging technologies, rules and regulation. The architecting team can consider factors such as an alternative SoS concept of operations, network connectivity between specific systems, upgrading of existing systems, and/or new systems acquisition and development.

- Step 3 – Evaluate SoS Alternatives
  This step involves the evaluation of the set of SoS alternatives in terms of performance, robustness, "ilities" and cost. Software models would need to be developed to represent each SoS architecture. These models may have already been developed during the development of SoS alternatives and may be used for evaluation purposes. In parallel, test and evaluation parameters must be defined so that those important test criteria are built into the models. During the evaluation process, new insights from the analysis may result in the need to reframe the issue and/or to refine the SoS design. The architecting team is expected to iterate steps 1, 2 and 3 of the SA process. Eventually, the outcome of the evaluation is a recommendation of an SoS architecture that has been assessed for its desired attributes for management's decision.

- Step 4 – Finalise SoS Architecture
  The output of SA is an endorsed SoS architecture. This SoS architecture is described in terms of architectural views in accordance with the EA framework and governance guidelines. The documentation will facilitate promulgation, communication, masterplanning and realisation of the SoS architecture. The finalised SoS architecture will facilitate the formulation of the various capability development plans. These master plans will chart the milestones for capability build-up, resource and training requirements.

- Step 5 – Realise SoS
  The realisation of the SoS architecture will usually be led by a Programme Director or a Senior Programme Manager supported by the IPMT. There will be different programme teams responsible for the acquisition and development of various component systems in the SoS architecture. Where necessary, a Technical Working Group or SoS Steering Committee may be formed to provide management guidance to the IPMT. Since each component system will likely have different developmental milestones, the need to work closely among IPMTs to address interoperability and integration issues cannot be over-emphasised. Appropriate SoS Integration Labs may be set up to address integration issues as early as possible using emulators of the component systems. During the course of SoS realisation, any deviation of the SoS architecture will need to be raised at appropriate governance forums for endorsement. Since the realisation of SoS may take many years, external environments such as disruptive technologies may invalidate the assumptions made during the architecting process. This may result in the need to initiate the SA process again.

- Step 6 – Certify SoS
  Verification, validation and certification of the SoS are essential activities during this process. Verification and Validation (V&V) is the process conducted to check that the SoS meets specifications and fulfils its intended purpose as defined in Step 1 - Frame the Issue. In general, verification is a quality process to ensure that a system complies with specification and is conducted throughout the systems development phase. Validation is the process to establish a certain degree of confidence that a system accomplishes its intended mission and addresses stakeholder needs. Both aspects are essential as verification ensures that “we built it right” while validation ensures that “we built the right thing”. Therefore, at this stage, the SoS will be evaluated and validated for its capability and performance with respect to the master plan. When the SoS is successfully verified and validated, the SA team can proceed to certify the SoS with customers and stakeholders.

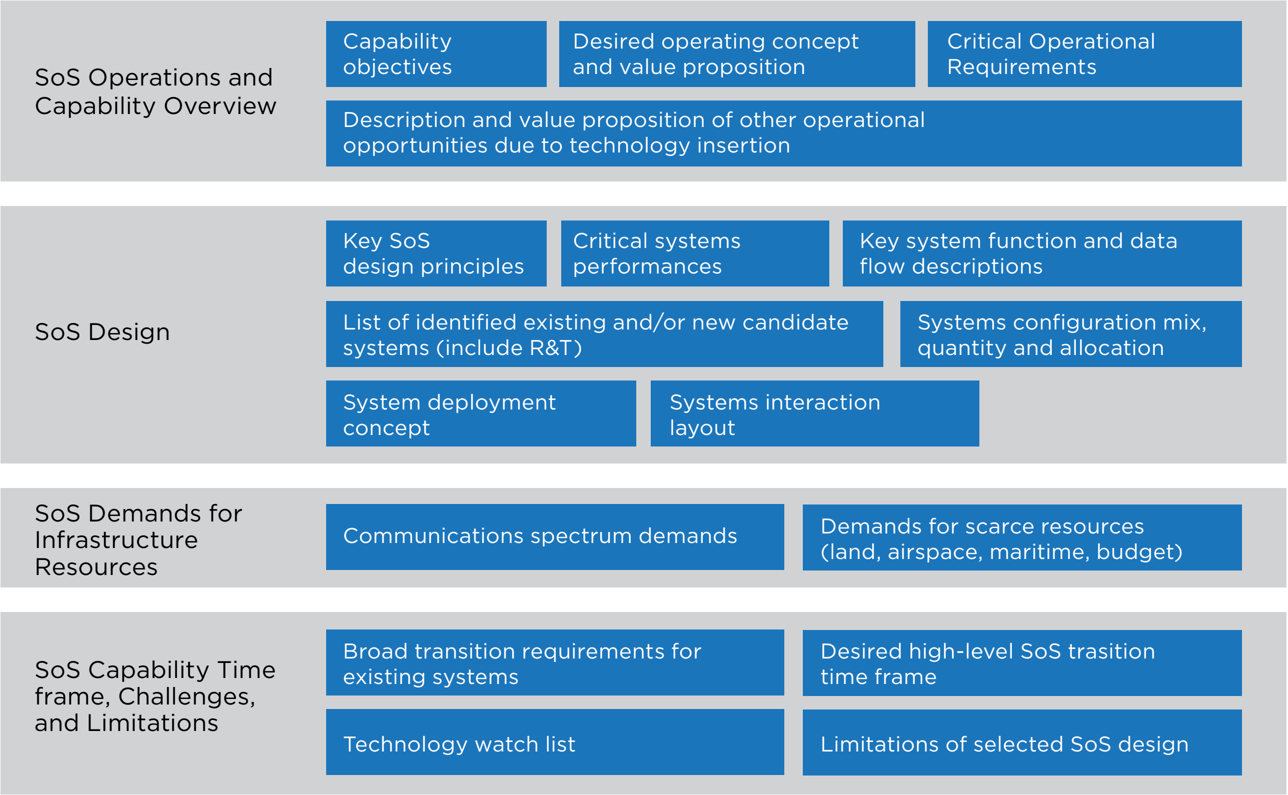
It is notable that an SoS may not have a completion date. Unlike a single system which will be developed, fielded and eventually retired, an SoS will need to be enduring to deliver the intended capabilities until it is no longer relevant. Hence, an SoS can evolve through many master plans and renewal of component systems. The process of V&V may lead to new insights or discovery of undesired emergent behaviour. Lessons learnt will be produced as feedback for the next cycle of the SA process. It is important to continue regular monitoring of SoS operations to look out for any emergent behaviour. In addition, the operations of SoS must be reviewed in the context of changes in external environments for deficiency as it may trigger the need for a new cycle of SA.

Effective Transition between Architecting to Implementation of SoS

In the above 6-step process, one of the critical transition points is from Step 4 to Step 5. While Step 4 is about the SA team concretising a “blueprint” for the SoS (i.e. SoS architecture), Step 5 often involves the implementation of this blueprint by various project teams for the SoS. A certain level of clarity and details is needed to guide SoS implementors in seeing through the SoS blueprint to fruition. Based on SA studies, the figure below highlights important information on the SoS architecture that should be documented to facilitate the subsequent phase of implementing the SoS, making the SoS architecture “actionable”.

- **SoS Operations and Capability Overview**
  The overview reveals the high-level operational context of the SoS so that the operations manager and systems architect can have a broad and common understanding of the SoS capability. The desired concept of operations, corresponding value propositions and critical requirements are documented using various types of illustration (Operational Views 1, 2 etc. based on the US Department of Defense Architecture Framework) and written text. Inserting a new technology to meet the SoS capability objectives may create potential operational opportunities in other SoS. The assessment of these opportunities should be recorded in the architecture and reviewed as part of another SoS construct. Hence, the assessment helps to ascertain if system provisions should be made for interoperability and realisation of the potential opportunities.

- **SoS Design**
  The design forms the core of the architecture. It covers various aspects to explain how constituent systems are identified and designed to fit into and be coherent with the SoS layout. Thus, the


SoS Operations and Capability Overview
Capability objectives
Desired operating concept and value proposition
Critical Operational Requirements
Description and value proposition of other operational opportunities due to technology insertion

SoS Design
Key SoS design principles
Critical systems performances
Key system function and data flow descriptions
List of identified existing and/or new candidate systems (include R&T)
Systems configuration mix, quantity and allocation
System deployment concept
Systems interaction layout

SoS Demands for Infrastructure Resources
Communications spectrum demands
Demands for scarce resources (land, airspace, maritime, budget)

SoS Capability Time frame, Challenges, and Limitations
Broad transition requirements for existing systems
Desired high-level SoS trasition time frame
Technology watch list
Limitations of selected SoS design

Key aspects of an actionable SoS architecture design helps to rationalise the impact of an impending change in the SoS. Information and considerations on the design, such as design principles, system interactions, system performances and configurations, are documented to support the analysis as well as the test and evaluation of the architecture. This ensures that the SoS is verified and validated for its intended capability, and that it has been implemented correctly as well.

- **SoS Demand for Infrastructure Resources**
  Requirements such as communication infrastructure need to be surfaced early to the relevant governing bodies to strike a balance among competing demands. Otherwise, the identified systems which require these resources may not be usable, thus affecting the SoS' capability performance significantly.

- **SoS Time Frame, Challenges and Limitations**
  This aspect provides the SoS programme manager with an overview of the transition requirements, challenges and limitations of evolving constituent systems. Thus, an implementation timeline can be established for the newly evolved SoS architecture. The intent is to communicate this information to various constituent system owners to ensure that stakeholders are fully apprised of the challenges and new limitations. This aspect should also document the lessons learnt so that important insights are passed on for future evolution.

Realising SoS

It would be necessary to have an IPMT with the right members to implement the SoS, led by a Programme Director or a Senior Programme Manager that possesses very strong leadership qualities and with a proven track record in project delivery. A Programme Steering Committee comprising senior leadership from MINDEF, the SAF and the DTC would be critical to provide strategic guidance and cross-organisational support to the PMT. It will also support the necessary governance in the complex business of realising an SoS.

The SoS would often be implemented via multiple projects that could be running in a parallel or staggered manner with centralised oversight, instead of one single "super project". This factors in considerations such as keeping project execution agile and selecting the best systems from competing defence contractors.

As each project progresses, a better understanding of each system's eventual capability will be formed. This may warrant adjustments to the requirements of individual systems in order to preserve the performance of the SoS.

For example, more stringent performances may be required of a particular future system B in order to mitigate unexpected shortfalls encountered in implementing an earlier project A. In the event that this cannot be done, it may be necessary to review and adjust the SoS architecture. The necessary options and decisions would be deliberated through the IPMT and Programme Steering Committee.

Such governance would likewise apply in managing the configuration of the SoS as the individual systems undergo updates in the details of their hardware, software or processes over their life cycles.

SoS Verification and Validation

SoS V&V poses another challenge due to the scale of the systems involved. It may not be practical or possible to test the entire SoS through a full-scale live test, although this could be the most realistic, due to the resources that would be required. On the other hand, computer-aided simulation offers an efficient means to test many possible scenarios for the SoS, albeit in a less realistic manner than tests with actual equipment (for example, the whole suite of actual radars, missile and C2 systems for IAD, together with simulated threats flying live.)

A possible approach would be to rely on a combination of tests involving either simulated systems, actual systems or both. The testing could comprise tests at up to four levels – from single-system tests (e.g. for a new radar system), to pair-wise tests (e.g. a new radar system connected to a C2 system or weapon system), to testing a "slice" of SoS (e.g. a selection of new/existing radar, C2 and weapon systems that could interoperate within the SoS) and, where possible, to a full-scale test of the SoS. Besides testing the SoS performance, other important aspects include the management of the safety and emergent behaviour of the SoS.

References:

Maier, M. W., & Rechtin, E. (2000). *The art of systems architecting* (2nd ed.). Boca Raton, Florida: CRC Press.

Valerdi, R., Axelband, E., Baehren, T., Boehm, B., Dorenbos, D., Jackson, S., … Settles, S. (2007). A research agenda for systems of systems architecting. *INCOSE International Symposium, 17*, 1892–1908. doi:10.1002/j.2334-5837.2007.tb02992.x

Appendix to Chapter 3

Leveraging the Enterprise Architecture Framework for Business Alignment and Agility

Developing Joint Systems

In 2004, the SAF embarked on a journey of force transformation into the Third Generation SAF, a joint military that synergises its various capabilities across the air, sea and land dimensions to achieve optimum effects.

One of the key operational goals then was to deliver increased speed of command. The aim was to do so not just more quickly but also much more effectively, which called for new structures and processes for faster decision-making and better battle management to deal with the changing nature of security threats. Faster Observe-Orient-Decide-Act (or 'OODA') cycle stems from faster sense-making, which in turn hinges on our ability to assimilate information, understand the situation, communicate, problem solve and decide.

A key part of this transformation was the Integrated Knowledge-based Command and Control (IKC2) paradigm that enabled a more integrated and networked SAF.

The integration of operational concepts with system development has been key to the SAF's development of IKC2. On one hand, substantive competencies have been built up in the SAF's C4 community, DSTA, DSO and other local industries. The operations community, on the other hand, has been actively defining the operational concepts, doctrines, information flow and process loops. This has given the technical agencies the clarity and direction to provide appropriate systems and solutions to meet the demands of the Third Generation SAF.

As military systems become increasingly interconnected under the IKC2 paradigm, a coherent and holistic strategy is needed to manage interoperability across C2 systems. At the same time, systems need to be sufficiently agile to respond to changes in requirements and support a full spectrum of operations ranging from peace-time to war-time operations.

In 2006, MINDEF and the SAF adopted EA to facilitate self-alignment within their organisations. The EA framework achieves this by providing structures, processes and guidelines to integrate developments from multiple agencies within MINDEF and the SAF and guide them towards top-driven enterprise vision and objectives.

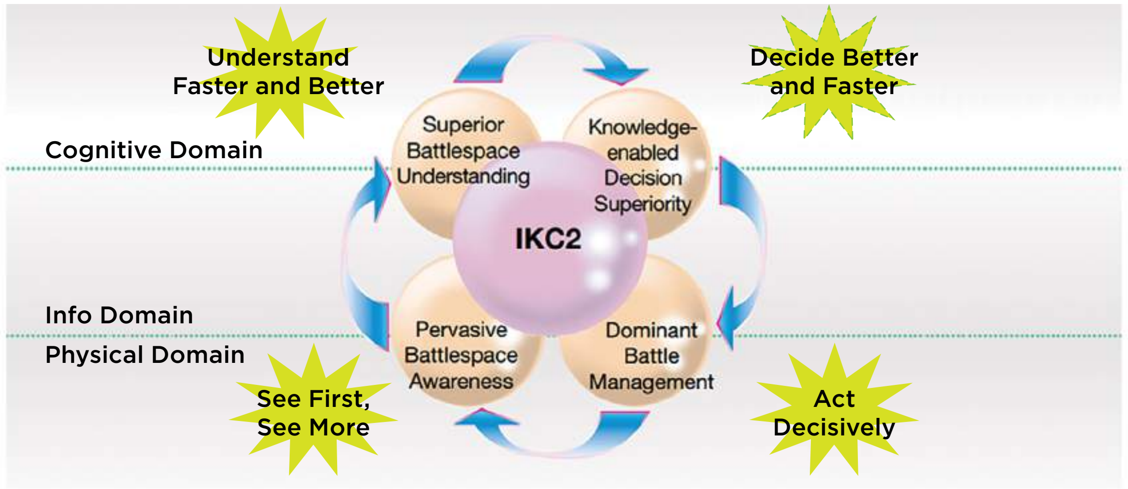
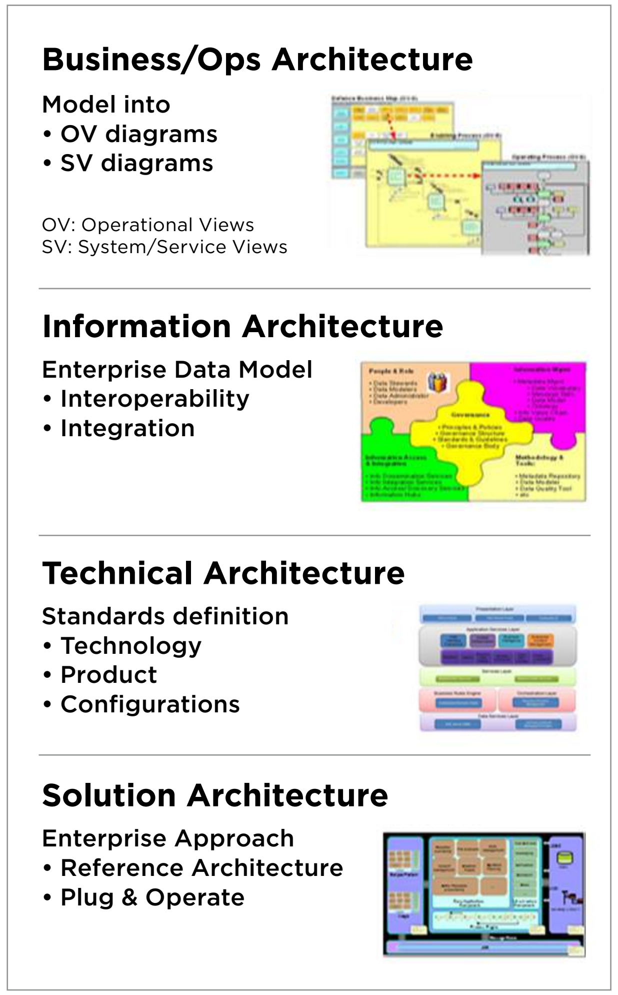


Illustration of IKC2 Operational Concept

The framework comprises four main components:



Business/Ops Architecture

Model into
- OV diagrams
- SV diagrams

OV: Operational Views
SV: System/Service Views

Information Architecture

Enterprise Data Model
- Interoperability
- Integration

Technical Architecture

Standards definition
- Technology
- Product
- Configurations

Solution Architecture

Enterprise Approach
- Reference Architecture
- Plug & Operate

EA Framework

- *Enterprise Business/Operational Architecture (EBA).* EBA is the expression of the enterprise's key operational strategies and their impact on operational functions and processes. The primary intent of EBA is to provide a common language for articulating operational requirements, policies, business processes and supporting technologies needed to achieve a high level of information and system operability. It also enhances visibility of the operations to facilitate quick response to change.
- *Enterprise Information Architecture (EIA).* The information that an organisation needs to fulfil its raison d'être is analogous to blood in the human body – precious and life sustaining. It flows across the organisation to support military operations and facilitates decision-making. EIA includes data models, information exchange matrix and knowledge management plans. It documents the party responsible for the data as well as where and how it was created, read, updated or deleted. EIA examines the information flow across business processes and reveals the architecture requirements for information exchanges within the enterprise.
- *Enterprise Solutions Architecture (ESA).* An ESA is a model of the applications and infrastructure components that satisfies a set of operational requirements. It serves as an input for operational users and developers in their planning and creation of the project portfolio, so that they can satisfy enterprise business and information architecture requirements. ESA captures the software design components on current inventory of applications, components and existing reference architectures complete with system interfaces. ESA examines design trade-off decisions (e.g. usability vs security) to fulfil EBA and EIA requirements (commonly known as functional requirements), as well as to meet non-functional requirements (e.g. interoperability, maintainability).
- *Enterprise Technical Architecture (ETA).* ETA is a logically consistent set of principles, standards and guidelines that serves as a guide in the design, acquisition, implementation and management of C2 systems. Using ETA to govern technology choices helps maintain coherence to facilitate interoperability across systems, integration with legacy systems and technology obsolescence management.

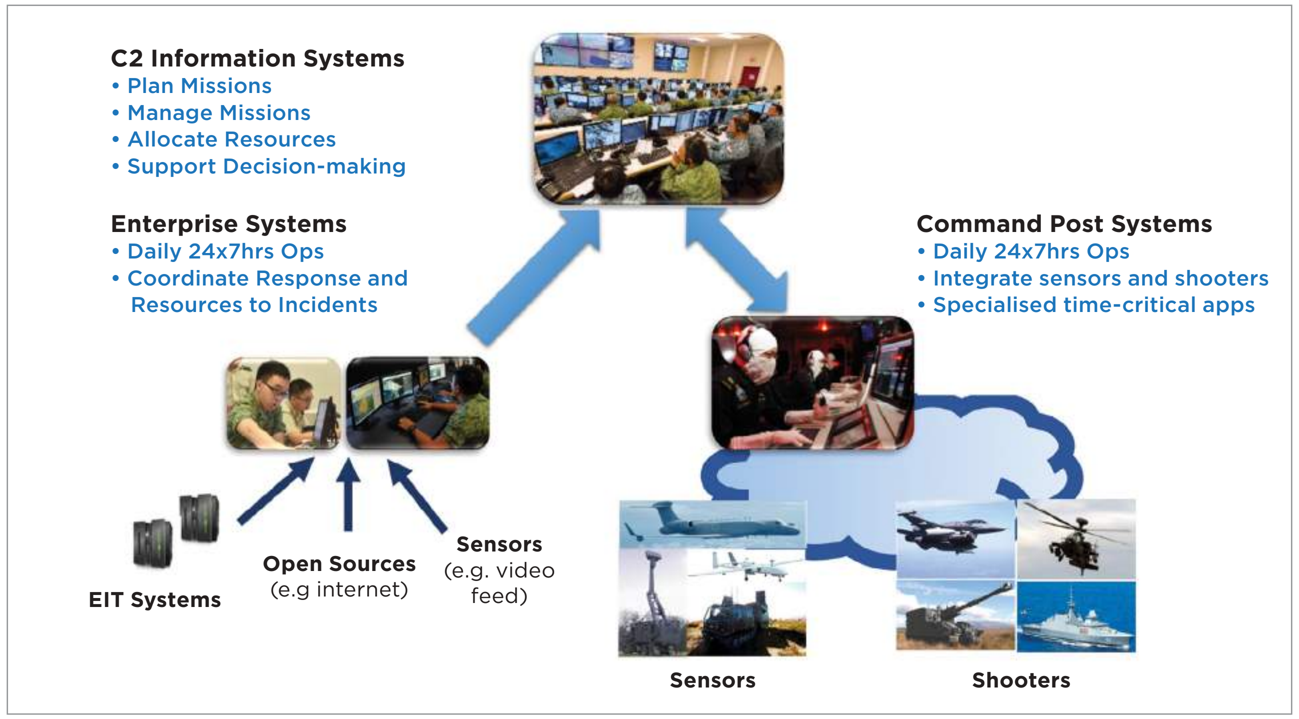
The EA Framework is used to guide the design and development of IKC2 systems to ensure connectivity and interoperability. For example, architectural views of the EA Framework are used to capture the business models, functions, processes, system solutions, and technical perspective of the desired System of Interest such as:

- C2 Information Systems that allow greater integration across the Services at the planning level. A central software library of reusable software modules that are systematically consolidated to achieve efficiency in development time and cost.
- Digitised Command Post Systems that use sensor information from different Services to better execute missions. For example, a Division Command Post on the ground could receive information from unmanned aerial vehicles and transmit this to its tactical forces.
- Enterprise Systems that leverage COTS such as SAP to manage operational transactions. Such systems allow the Third Generation SAF to manage resources and coordinate daily operations. An example is the Logistics Enterprise System.

Service Oriented Architecture – Foundations For Operational Agility

The EA Framework also puts in place a Service Oriented Architecture (SOA) strategy to develop software as part of Solution Architecture. Such a software development approach will achieve the following benefits:

- *Operational Agility.* The Third Generation SAF is a joint military that synergises its various capabilities across the air, sea and land dimensions to achieve optimum effects. To achieve this, fighting forces and supporting systems capability need to be organised and reorganised rapidly to meet evolving operational needs and operate in a highly networked manner to maintain an information edge. The SAF must constantly change its strategies and business processes to stay ahead. Thus, it has become a requirement for modern C2 systems to be able to adapt quickly and efficiently to reflect those changes. SOA is a concept that advocates such adaptive C2 systems (i.e. service-oriented rather than technology-oriented). In the traditional approach, changes to the C2 systems are often difficult and costly, and SOA is positioned to change that.


C2 Information Systems
- Plan Missions
- Manage Missions
- Allocate Resources
- Support Decision-making

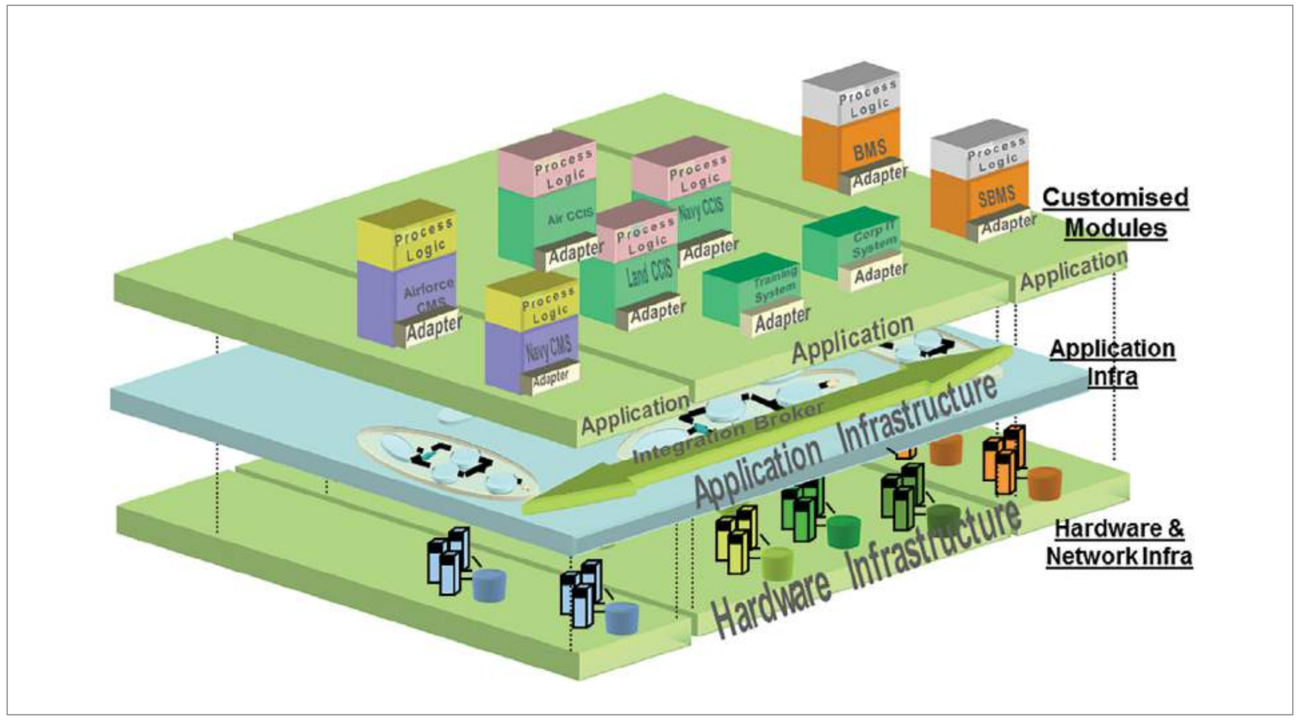
Enterprise Systems
- Daily 24x7hrs Ops
- Coordinate Response and Resources to Incidents

Command Post Systems
- Daily 24x7hrs Ops
- Integrate sensors and shooters
- Specialised time-critical apps

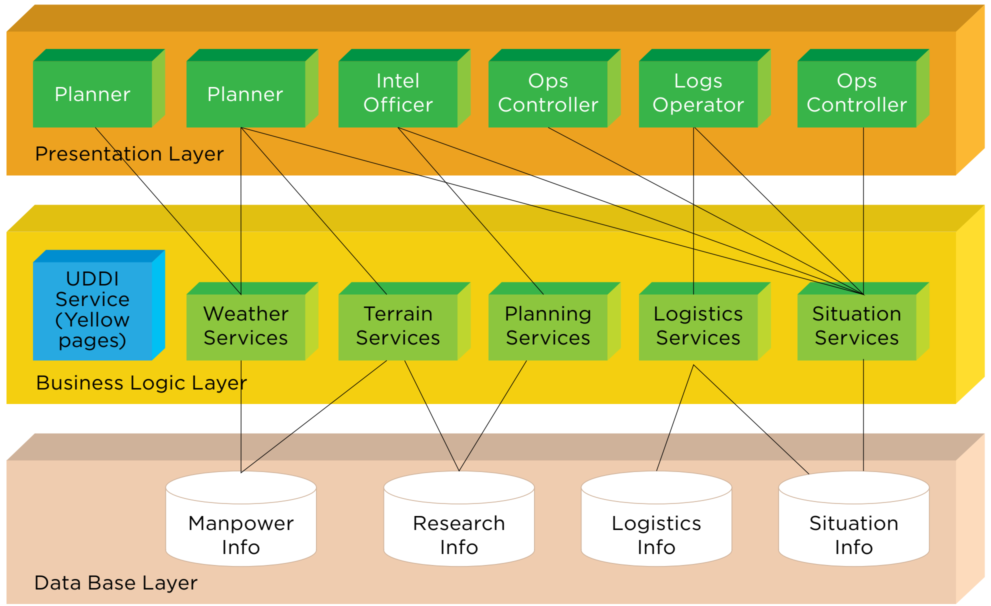
Systems of Interest

- *Seamless Integration.* Optimising collaboration between various operational departments or divisions would be an advantage. In particular, if systems have to be integrated due to business process optimisation, the SOA concept can be used to enable collaboration across clearly defined interfaces. In this way, the strengths of the individual areas can be maintained, while simultaneously leveraging the potential synergies.
- *Cross-agency Collaboration.* Moving ahead, military operations cannot work in isolation and it is essential for the SAF to collaborate with other agencies. SOA allows products and software services to be provided within the company or by external vendors.
- *Support for outsourcing and out-tasking.* The trend of outsourcing process steps to an external provider that treats these steps as a core competency is growing all the time. Using de-coupled services to map processes makes these distributed scenarios easier and faster to implement.
- *Reuse.* In the traditional approach, only codes and algorithms could be reused. With SOA, the reuse of actual applications is now possible. Composite applications are made up of reusable components that can be used to form other composite applications. This allows new applications to be built with less time and resources. SOA also allows legacy systems to be modified for reuse rather than rebuilding everything from scratch to replace them.

From the EA Framework formulation, SOA would enable IKC2 systems to better react to the SAF's evolving needs. The SOA architecture allows more efficient communication and collaboration among different operational units. Its centralised repository ensures information is accurate and up-to-date, which is vital to the SAF's operations. The reuse of components means faster development with reduced risk, thus the new and reliable IKC2 applications can be developed in a much shorter time.



SOA for C2 Information Systems



Logical view of the Common Repository, showing how software is organised in three complementary layers, namely the Presentation Layer, Business Logic Layer and Data Base Layer. The Presentation Layer captures the user interface software tailored for different user roles. The Business Logic Layer captures the functionalities required by different users. The Data Base Layer defines the data associated to various business functions and workflows.

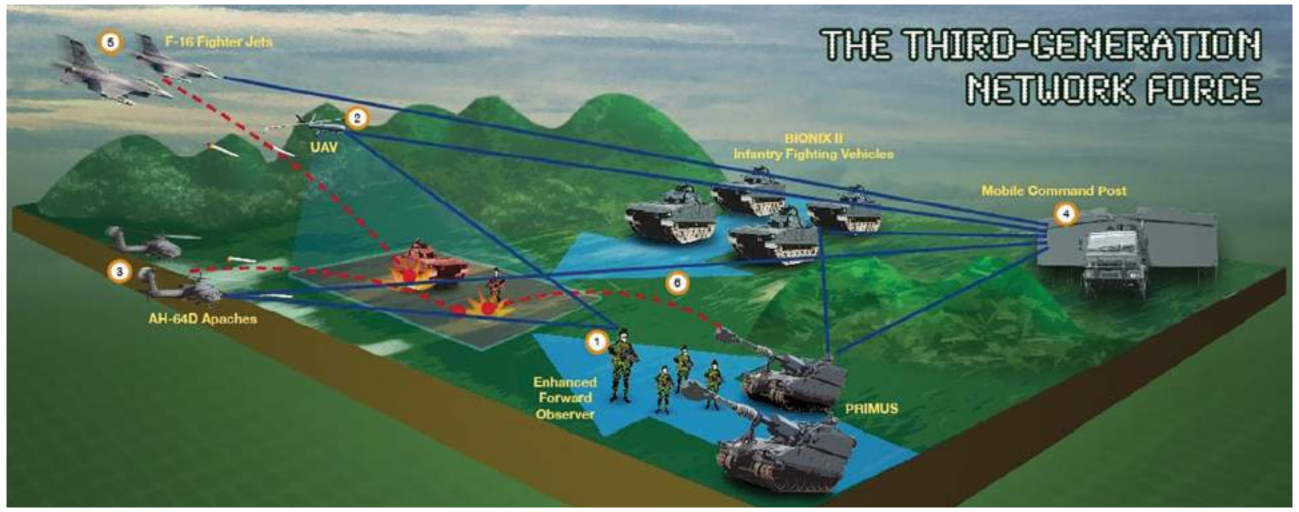
Common Repository

The common repository keeps the system business applications and technical component services that developers can draw upon to rapidly assemble and deploy IKC2 systems. As the repository applications and services are thoroughly tested for operational deployment, the assembled IKC2 systems can achieve a high degree of assured quality for operational trial and deployment. The common repository is an enterprise asset that must be properly maintained, continually expanded in the number of reuseable components and evolved through a rigorous quality management process. If new applications and services need to be developed to meet new operational requirements, they will be developed in addition to the IKC2 baseline systems.

Reference Architecture Framework – Divide and Conquer in Realising SoS

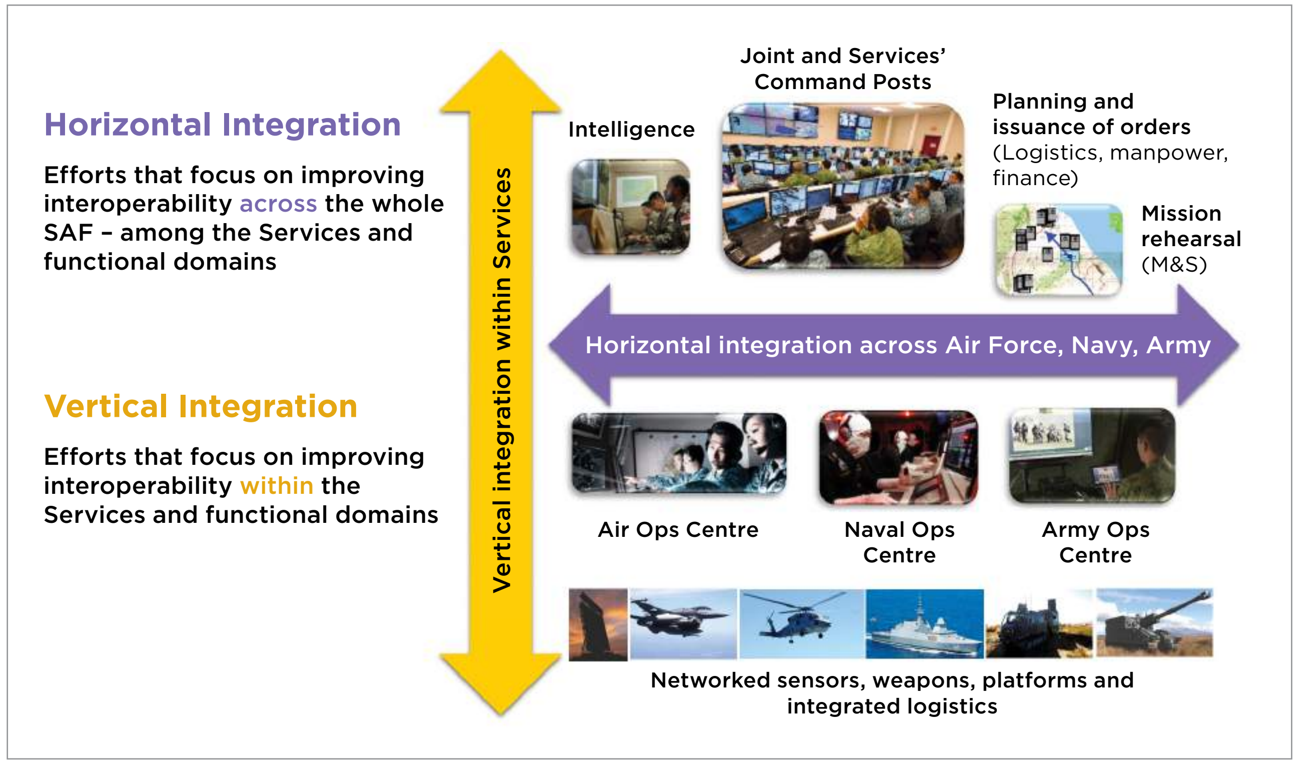
The Third Generation Networked Force pushes the envelope of C2 systems development beyond IKC2. Complex functionality of systems, diverse computing environments and the rapid pace of technological evolution add to the challenge. At the same time, systems need to continue to deliver capability while operational concepts are being explored or evolving.

The Reference Architecture Framework is designed to address and manage the complex solutions landscape. Reference Architecture is a set of cohesive, well-tested, and proven template solutions for a class of systems with similar requirements, and it can be scaled to include future requirements. It consists of design considerations, architecture and solution patterns, technology standards and reference implementations.


THE THIRD-GENERATION NETWORK FORCE
5
F-16 Fighter Jets
2
UAV
BIONIX II Infantry Fighting Vehicles
Mobile Command Post
4
3
AH-64D Apaches
6
1
Enhanced Forward Observer
PRIMUS

An illustration of IKC2 operations, with the numerical sequence broadly showing how a network of sensors (1 and 2) and shooters (3, 5 and 6) collaboratively locate and defeat targets of interest, with a command post (4) providing oversight.

In order to evolve technical systems while maintaining interoperability and agility amid changing operational environments, the framework maintains three levels of architecture types – Target Architecture, Reference Architecture and Overarching Architecture. Individual project implementations (Target Architectures) can align themselves by referencing suitable Reference Architectures. While the Reference Architectures take care of alignment and integration within a cluster of IKC2 systems, the Overarching Architecture is an important element in enabling horizontal and vertical integration to achieve the capability of the Third Generation Networked Force.


Horizontal Integration

Efforts that focus on improving interoperability across the whole SAF – among the Services and functional domains

Vertical Integration

Efforts that focus on improving interoperability within the Services and functional domains

Vertical integration within Services
Intelligence
Joint and Services' Command Posts
Planning and issuance of orders (Logistics, manpower, finance)
Mission rehearsal (M&S)
Horizontal integration across Air Force, Navy, Army
Air Ops Centre
Naval Ops Centre
Army Ops Centre
Networked sensors, weapons, platforms and integrated logistics

Overarching Architecture – System-of-Systems Integration

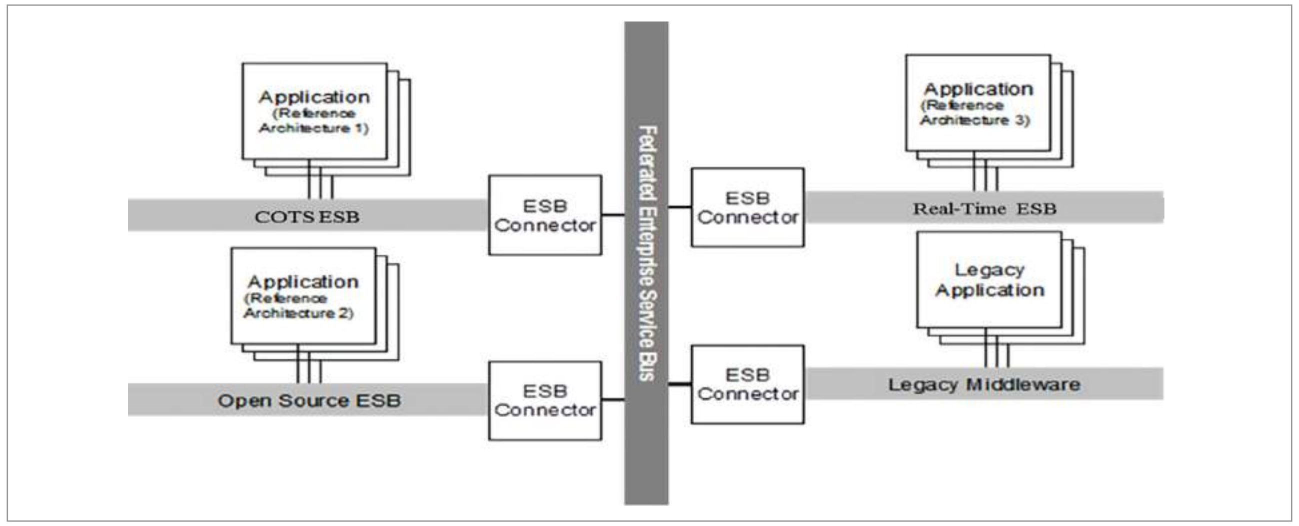
The Reference Architecture Framework provides the following benefits:

- *Reuse.* The Reference Architecture ensures that software modules developed in one project can be reused in another project whenever there is a common requirement. Such reuse is not limited to client applications – depending on the reference architectures, system modules, server applications will also be available for reuse through reference architecture alignments.
- *Faster System Delivery Time.* The availability of tested and proven solution patterns from the Reference Architecture helps expedite the development and delivery of systems. Reuse of well-tested and proven solutions ensures the quality of the delivered systems.
- *Inter-operability by Design.* The Reference Architecture ensures that systems referencing the same reference architecture will be interoperable through employing standard technologies, solutions and well-defined services and interfaces.
- *Independent Evolution of Architectures.* IT technologies evolve at phenomenal rates. The need to control the diversity and standardise the technologies within an enterprise has led to the development of ETA. However, technology development is essential for the continuing development of operational capability of the enterprise. The segregation of the enterprise into sub-enterprises enables the technologies employed within each sub-enterprise to be evolved. It takes into consideration impact within the domain, yet remains fairly independent of the other domains. This enables the ETA to evolve at a faster pace.

Building Foundation and Competency

To meet the demands of the Third Generation Network Force, our engineers need to continuously enhance the Federated Enterprise Bus to evolve the Overarching Architecture. The Overarching Architecture needs to maintain a coherent interpretation of Service Orientation across the diverse technical implementations for all Reference Architectures.

The implementation solutions need to match and mediate the service definitions between the clients and service providers. They need to provide the bridging solutions between different technology standards, propagating the necessary service management information across the whole enterprise solution landscape. These are the basic functionality of an Enterprise Service Bus, except that in this case, it is used to connect multiple Service Oriented Reference Architectures – hence the name Federated Enterprise Service Bus. The Federated Enterprise Service Bus enables information exchange across COTS systems, Open Source systems, Legacy Systems and Real-Time systems. It is the foundation of SoS Integration.



Federated Enterprise Service Bus to enable SoS Integration

Model-Driven Architecture – Generating Software Codes

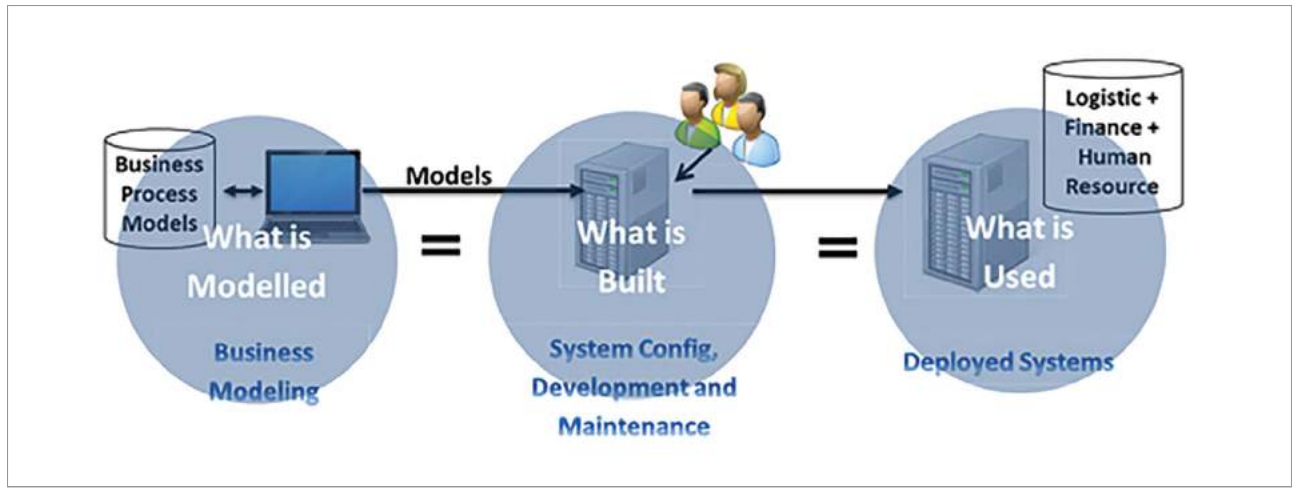
Besides enabling SoS integration, flexibility to make new changes and "speed to delivery" are key considerations in the design of our C2 systems.

Following the advancement of Software Engineering, architecture models that are used to capture business/operational processes, functionalities and information flow can be integrated to COTS products to generate software codes. This software design approach is commonly known as the Model-Driven Architecture (MDA).

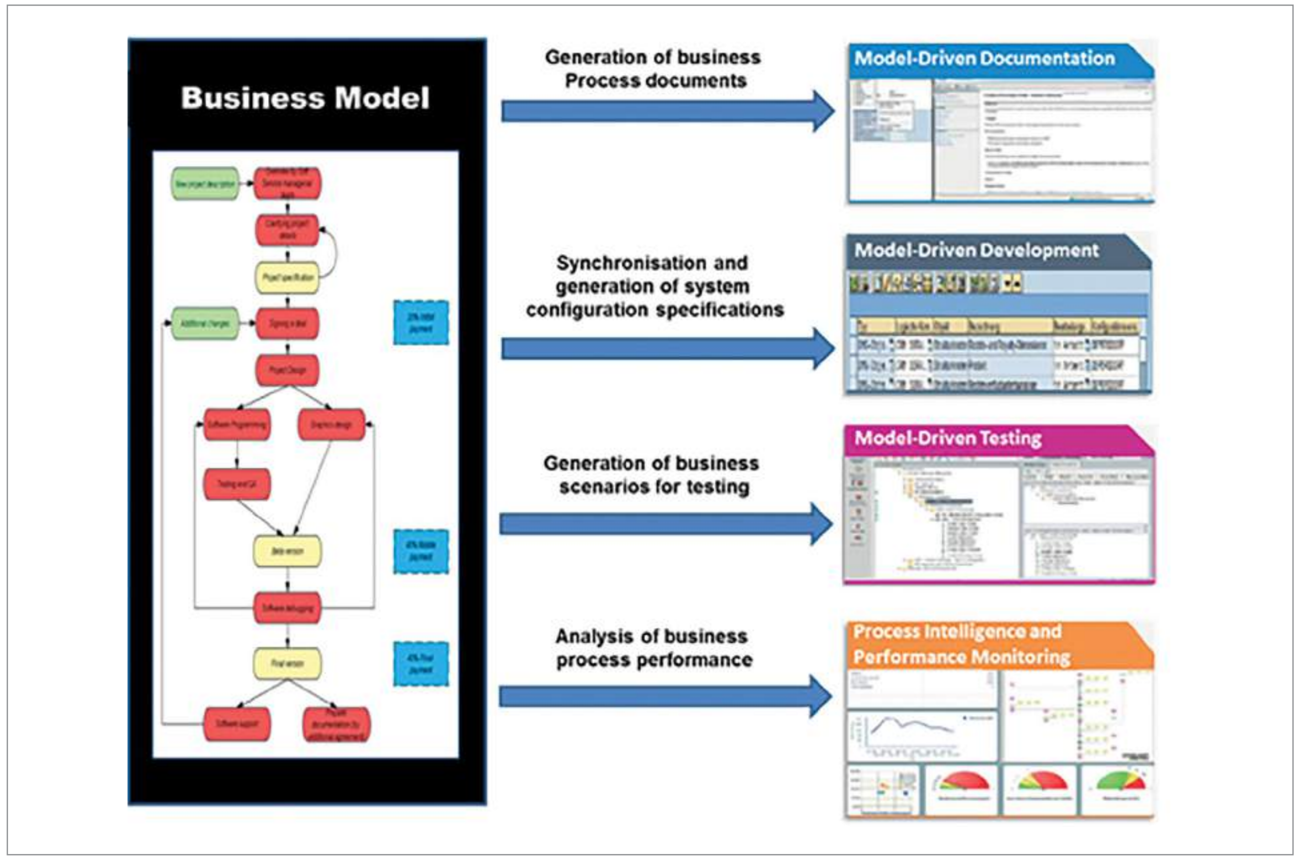
Architecture Modelling is the key to MDA in a software development process. The MDA approach uses models to define business processes, functionalities of a system and information flow. These models are then translated and linked electronically to vendor-specific tools for execution. Some examples of the tools are Business Process Management System (BPMS), SAP Solution Manager, Rapid Application Development Tool and Case Management Tool.

For example, the C2 community uses BPMS in combination with SOA to capture operational requirements and changes. BPMS enables new operational capabilities which involve the flow of tasks among different operational units to be developed and deployed faster as compared to traditional development done through coding. BPMS gives users a much needed operational agility as they operate in a more dynamic environment.

Another example would be the use of the SAP MDA solution by the logistics community that allows process implementations, system configurations as well as test scenarios to be generated automatically through business models stored in a central repository. Through early prototyping and better communication across users, issues and conflicting requirements are reduced during implementation. Overall, system development effort and time is significantly reduced as compared to conventional systems development methods, thereby enhancing the pace and agility of how systems are designed, built and tested.



MDA


Business Model
Generation of business Process documents
Synchronisation and generation of system configuration specifications
Generation of business scenarios for testing
Analysis of business process performance
Model-Driven Documentation
Model-Driven Development
Model-Driven Testing
Process Intelligence and Performance Monitoring

SAP MDA Capability

Appendix to Chapter 4

Spare Parts Provisioning Optimisation

Introduction

Deciding on the quantity of spares was an intimidating challenge because of the high costs involved. Relying on the E-2C spares list given by the USN would have cost many tens of millions of dollars. The costs were higher, probably due to the relatively smaller number of E-2Cs compared to other aircraft types. So, without the benefit of operational experience on the E-2C, and relying on the reliability data provided by the ASO in Philadelphia, we had to decide on the spares to buy, item by item. We could have played it safe and purchased what the USN recommended. Instead, we took a calculated risk by using a yet untested (by us) software programme on spares provisioning called OPUS; we asked relevant questions of various knowledgeable USN personnel, and then made our own judgement. OPUS is a software provisioning tool to determine the spares holding necessary to achieve a desired operational availability. This became a standard tool for calculating and provisioning our spares in other future projects. We sometimes wondered if anyone would thank us for saving tens of millions of dollars if a plane was grounded for want of a spare!

OPUS – for Single System Scenarios

One of the most prominent and critical elements in the LCC of a system is the cost of spares needed to support it during the O&S phase. The availability of a much needed spare part could make the difference between victory and defeat. The methods used in predicting the cost of spares vary substantially in complexity and accuracy, ranging from the overly simplistic and generally less reliable, to the highly advanced, rendering more precise results. Although the use of computers has greatly reduced the enormous task in spares computation, the fundamental requirement in ensuring accurate input data still remains a job for logisticians.

The commonly used method in determining the spares quantity is the Poisson Distribution, employing the "Confidence Level" (also commonly called Confidence Factor, Safety Factor and Probability of No Stockout).

The equation is:

$$P = \sum_{x=0}^{s} \frac{e^{-n\lambda t}(n\lambda t)^{x}}{x!}$$

where,

P = Probability of meeting all spares demand within the turnaround time
s = Number of spares
n = Quantity of items in the system
λ = Failure rate of the item
t = Average turnaround time

To calculate the spares quantity, the equation is solved iteratively by increasing the number of spares (parameters) until P becomes equal or greater than the desired confidence level. This method of spares provisioning is clearly deficient. Notice that the cost of the item is not considered. Also, the spares quantities are determined one at a time with no interaction among the items in the system. Thus, the system as a whole is not really considered.

OPUS is a spares provisioning software developed by Systecon, a Swedish Consultant Company. It also uses the Poisson Distribution but the deficiencies faced by the Poisson Distribution have been taken care of in the program. In early 1988, two engineers from the Reliability Technology-Defence Materials Organisation validated the OPUS software in the military environment. The RSAF F-5 was used as it has long in-service application and well recorded performance data. The results showed that OPUS optimises the number of spares required with respect to the cost and turnaround time of the items, with a savings of about 15% over the Poisson Model.

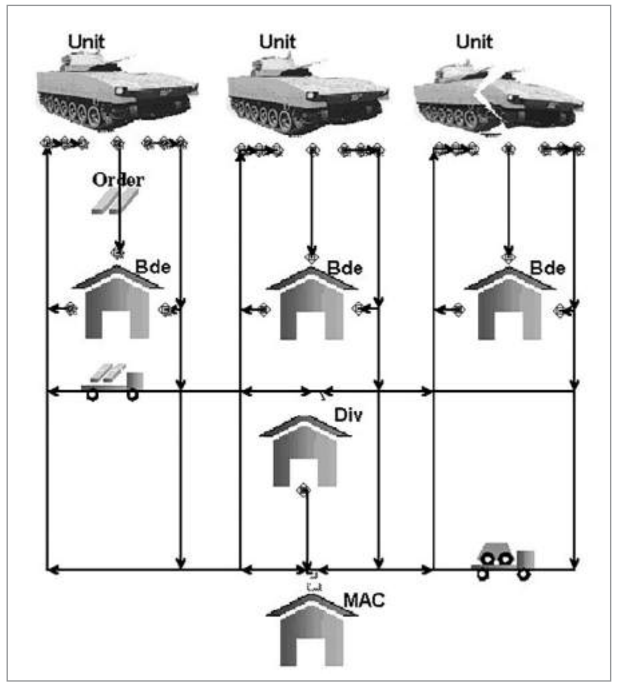
opus8	Simple Possion Model
1. Is a cost optimising model	1. Does not optimise
2. Considers the system effectiveness as a whole with interation between subsystems, LRUs, SRUs etc (ie considers system's Probability of No Stockout [PNS])	2. Treats each items separately, does not consider the system effectiveness (ie considers item's PNS)
3. Models the support organisation	3. Does not model the support organisation
4. Accounts for repairs done	4. Treats items like non-reparables
5. Considers the cost of each item	5. Does not consider cost at all
6. Takes a reasonable amount of risk to recommend low level of high cost items	6. Takes very low risk. Tends to stock sufficiently high for all items and hence requires higher total cost investment
7. Calculates a selected number of points, i.e. need not fix investment or measure of effectiveness such as Operational Availability	7. Calculates only one assortment of spares for a fixed PNS
8. Takes criticality of individual items into consideration	8. Takes all items to be of equal importance

Comparison between OPUS and Poisson Model

PIPER – For Large-Scale Fleet Scenarios

Not one to sit on its laurels, the DTC embarked in the year 2000 to develop a spares provisioning software to manage spare parts for large-scale fleet scenarios. It is well known that such study is a complex one. In particular, one needs to optimally allocate spare parts across multi-echelons (i.e. organisation unit and sub-unit levels) of maintenance agencies.

PIPER (or 'Pipeline Simulator') is a Monte Carlo simulation model developed by the DTC to manage spare parts for the Army. The model solves problems such as the evaluation of maintenance support concept, the impact of combat damage and workshop loading. This model provides full access to the source code for customisation and integration with other models or Management Information Systems. It is also designed to be scalable whereby models and new functionalities are created via the addition of "building blocks". It analyses multiple combat units, quantifies the effect of sharing spares and men, handles war scenarios (time varying utilisation rate, combat damage and attrition, operating hours of workshops) and explicitly models repair manpower required, heavy transporter vehicles and periodic re-supplies. A combinatorial technique of analytical marginal analysis and heuristics is employed for optimising spares and maintenance resources in PIPER.



Example of modelling maintenance of tracked vehicles using PIPER

The PIPER model is built using Extend (developed by Imagine That Inc.), a simulation tool widely used by academics and the simulation industry. The PIPER model consists of four echelons of repair agencies. Systems can be deployed at any of the four repair echelons. System repair is carried out at the second, third and fourth repair echelons. All four echelons hold a suite of maintenance resources (i.e. test equipment and technicians to service the repair jobs). The maintenance resources follow a user-defined operations schedule (i.e. the operating hours of workshops). The quantity of maintenance resources is allowed to change over time. The transport time and milk-run frequency among the various repair agencies can be defined to take special values and to override the default parameters. This may be used to represent certain Line Replacement Units transported by special mechanisms such as helicopter lift, pseudo stores or repair echelons. The milk-run frequency may be variable over the timeline and a frequency of zero milk-run can be used to represent a temporary stoppage of supply (i.e. enemy action or truck getting "lost"). The model is synthesised from building blocks present in the PIPER libraries.

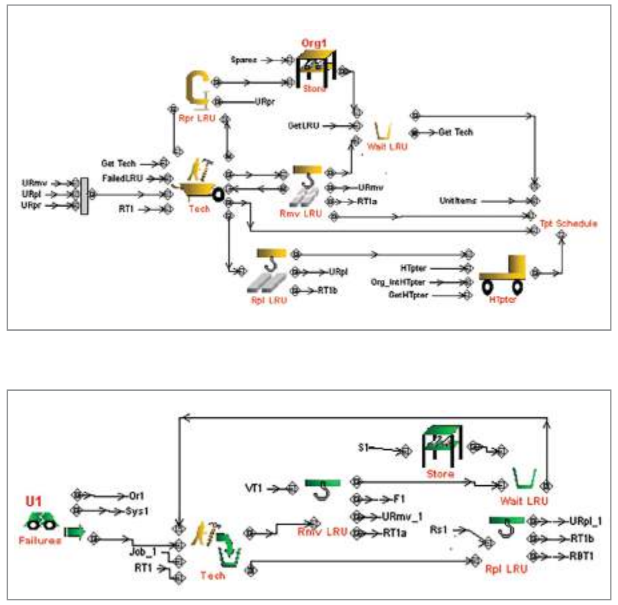
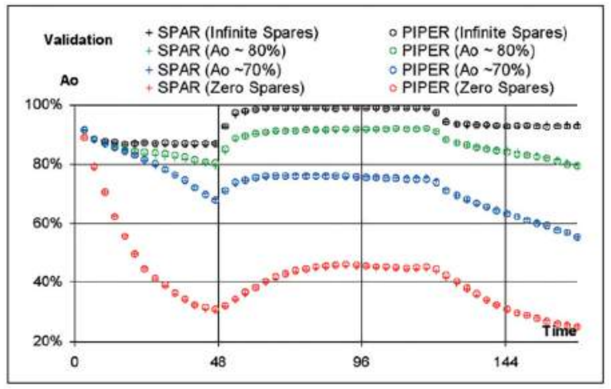


Illustration of model details in PIPER

Validation against other commercial tools such as SPAR (a tool developed by Clockwork Solutions) shows good agreement between the two models. The following figure shows the result of validation from two Army case studies. It should be highlighted that the validation focused on the simulation aspect of the model and the validation on the optimisation algorithm was not addressed in this portion.



Validation of PIPER model from two Army case studies

Performance Based Logistics

Introduction

The military environment is complex and dynamic. In the past, a defence force only needed to protect the nation's sovereign territory. Today, defence forces are called upon for relief and coalition operations in continents far away from home. Furthermore, their capabilities have become more integrated and lethal, with the seamless integration of new and legacy systems into one robust network. Yet, beneath such military prowess is the unseen but essential support structure that keeps each weapon system up and running. The complexity of these support tasks creates frequent unintended deviations from plans. The problem is compounded by ageing systems, which are often deployed beyond their planned useful life. Hence, beyond the traditional method of preventive and corrective maintenance and support, the SAF enters into partnership with defence companies for an outcome-based logistics support arrangement for an agreed-upon level of system readiness.

Performance Based Logistics (PBL) refers to "the purchase of support as an integrated, affordable, performance package designed to optimize system readiness and meet performance goals for a weapon system through long-term support arrangements with clear lines of authority and responsibility" (Defense Acquisition University, 2005).

Under the traditional acquisition approach, the SAF buys a system and its related parts and services, and invests the necessary capital and manpower to support its complex logistics and maintenance activities. When the system malfunctions, the faulty items are sent to the contractor, whose profitability increases as more malfunctions occur. The contractor earns more when the system performs below its reliability specifications. Moreover, most of a system's LCC occurs at the O&S phase. The intention of PBL is to leverage contractors' expertise and resources, and incentivise them to come up with innovative ways to reduce O&S costs while achieving the desired level of operational readiness.

PBL – An Aligning and Optimising Strategy

PBL seeks to address the undesirable status quo of traditional support structures by aligning the business goals of the contractor with the performance goals of the SAF. This is achieved by paying the contractor based on how well it fulfils performance metrics (e.g. systems availability, spares shortage) that contribute directly to the system's operational readiness.

The following figure contrasts the traditional acquisition approach with PBL where the SAF pays the contractor according to the system's ability to achieve its specifications. The contractor's profitability function is now inversely proportional to the number of equipment malfunctions and he is incentivised to become aligned with the SAF's goal of keeping malfunctions to a minimum.

Traditional	PBL
System Malfunctions ↑	System Malfunctions ↓
Contractor Revenue ↑	Contractor Revenue ↑

Alignment of goals using PBL

Traditional Support vs PBL Strategy

Traditional Support	PBL Strategy
Objectives The SAF buys spares and related services. Contractor is paid more as more items fail.	**Better Alignment of Objectives** The SAF buys a certain level of performance. Contractor is paid when performance is met, may be paid more for better performance.
Mission Readiness Contractor does not have direct penalties if Mission Readiness is not met.	**Enhanced Mission Readiness** Contractor has to maintain the agreed level of performance to secure bonus payment.
Reliability Improvements Contractor has no incentive to improve reliability related indicators to maximise payment.	**Reliability Improvements** With improved reliability, contractor reduces the frequency of maintenance, which increases his profit.
Cost Fewer economies of scale possible as the SAF has widely differing systems and contracts are not aggregated.	**Lower Cost** Contractor enjoys savings from economies of scale, better planning and design, optimisation of manpower, maintenance and storage of spares.
Resource Allocation The SAF resources have to be deployed to support all areas. This method disperses the focus and may not be the most effective.	**Better allocation of Resources** Some resources may be provided by contractor, freeing up SAF resources to be deployed in other critical areas.
Maintenance Footprint With more and more types of systems, maintenance footprint will only increase.	**Reduced Maintenance Footprint** The SAF can use the contractor's existing infrastructure and resources instead of duplicating them.

Differences between traditional support and PBL

PBL Implementation

PBL is used in many defence forces (including that of the United States, United Kingdom, Canada and Australia) under different names, to different extents and with slightly different guidelines. In the SAF, some instances where PBL has been implemented are as follows:

- PBL for the RSAF's fleet of F-5 aircraft was implemented in 2009 with ST Aerospace. Under the PBL arrangement, ST Aerospace provides the full logistics and maintenance support for the F-5 fleet. The scope of work includes the support of flight line, intermediate and depot level servicing, engineering support and material support.
- In 2009, the RSN implemented Availability Based Contracting (AvC) for its small craft together with ST Marine. Two years later, the implementation of AvC for the patrol vessels was carried out with ST Marine and ST Electronics. Besides the small craft AvC scope of work which included maintenance and supply services, the contract for the patrol vessels included "pit-stop" services like berthing and fuelling to alleviate the ship crew's workload.

Issues PBL Aims To Address

An ageing fleet will suffer from a decreasing number of available systems and frequent malfunctions. The increasing complexity of each malfunction also contributes to higher costs for the same level of operational readiness. PBL attempts to address this cost increase by better allocating resources and optimising performance per unit cost.

Optimising Allocation of Resources

In essence, PBL encourages the concept of "each does what it does best". Resources are directed to where they are best utilised, driving the development of each party's unique ability. Each contributor is allocated only the expenditure that will push it to the level of performance required from it. Resources saved can be used for motivating the achievement of other higher priority performance targets. Equipment serviced by its OEM can be supported by the OEM's existing logistics system. The OEM's support cost could be more competitive than the military's in-house support costs due to the large total volume it services and its expertise in supply chain activities. By leveraging contractors' investments in expensive maintenance infrastructure and capability, the savings in capital, space and manpower can be better deployed to other critical areas.

Improved and Consistent Mission Readiness

When payment is based on systems performance, there is motivation for contractors to ensure that the performance consistently meets the required levels. With a well-defined structure and transparent grading system, the contractor can be motivated to deliver the optimal level of performance, instead of under or over performing.

Reliability Improvement

Being concerned with supplying the required mission readiness, the contractor will strive to improve systems' reliability as it is a key contributor to overall performance. Contractors will then be motivated to keep malfunctions to a minimum and to incorporate reliability improvements at the design stage or during upgrades.

Reduced Maintenance Footprint

PBL encourages the consolidation and development of strengths – the vertical equivalent of mergers and acquisitions. Resources will be used to their fullest potential, minimising wastage from duplication or sub-optimal use.

References:

Defense Acquisition University. (2005). *Performance based logistics: A program manager's product support guide.* Fort Belvoir, VA: Author

Appendix to Chapter 5

Modelling and Simulation Tools for Systems Architecting

Background

The concept of Model-based Systems Engineering (MBSE), pioneered by Wymore (1993), has become one of the tracks in the International Council on Systems Engineering Vision 2020 (INCOSE 2007). The objective is to replace documents with models as the primary products or artifacts of Systems Engineering processes. MBSE is the formalised application of modelling to support system requirements, design, analysis, verification and validation, beginning in the conceptual design phase and continuing throughout the development and later life cycle phases. M&S tools are the means for applying MBSE in SA[1].

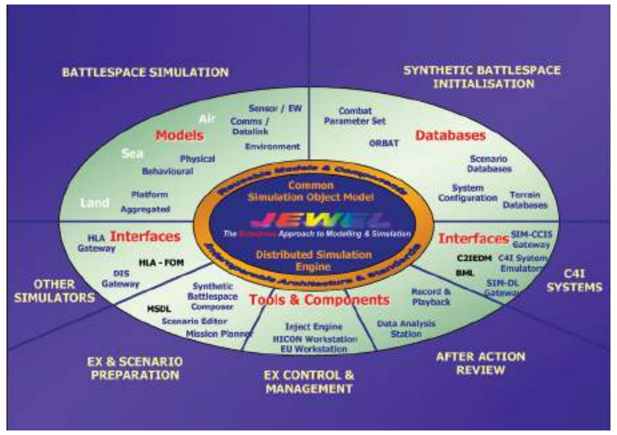
There are generally two categories of M&S tools: Discrete Event Simulation and Real-Time Simulation:

- *Discrete Event Simulation.* This is the concept of using event sequences to model communication, processes and changes in entity states. These models can be executed faster than real time, providing a shorter turnaround for simulated outcomes. They are suitable for exploring the complex web of SoS interactions among a host of systems working interdependently. Discrete event simulation could be applied to determine the optimal connectivity or effect of relationships in the SoS architecture, since a large range of configurations can be explored with the fast, repetitive simulation runs of event-based models. Examples of discrete event simulation tools include Map Aware Non-uniform Automata (MANA) for modelling of agent behaviors; ExtendSim, a dynamic process modelling tool; and OPNET, which is designed for communications network modelling and analysis.
- *Time-stepped Simulation.* For the representation of physical systems and effects such as motion, which is continuous in nature, it is easier and more efficient to use time-stepped simulation with regular updates at the individual model level. Using discrete events would incur larger overhead costs from the numerous events being sent and received among the various entities across the same time period. Time-stepped simulation can also accommodate man-in-the-loop, which is especially useful for evaluation and validation of SoS with decision making in real time. Some of the M&S tools based on time-stepped simulation are Joint Conflict and Tactical Simulation (JCATS), for individual and tactical combat environments, Extended Air Defense Simulation (EADSIM), for air defense domain experimentation and Joint Force Analysis Simulation (JFAS), to support joint force operational studies. Another time-stepped simulation tool that we developed in-house is the Joint M&S Environment for Wargaming and Experimentation Labs (JEWEL). JEWEL consists of a repository of models, databases, components and interfaces, supported by a common simulation engine architecture, with key emphasis on reusability and interoperability with external simulation and military systems.

M&S for Systems Architecting

Areas where M&S are used for SA are the visualisation of SoS concepts and issues; the evaluation of SoS performance and robustness; and the validation of systems functionality and interoperability in the context of the SoS.

[1] See Chapter 2 for more information on Systems Architecting.

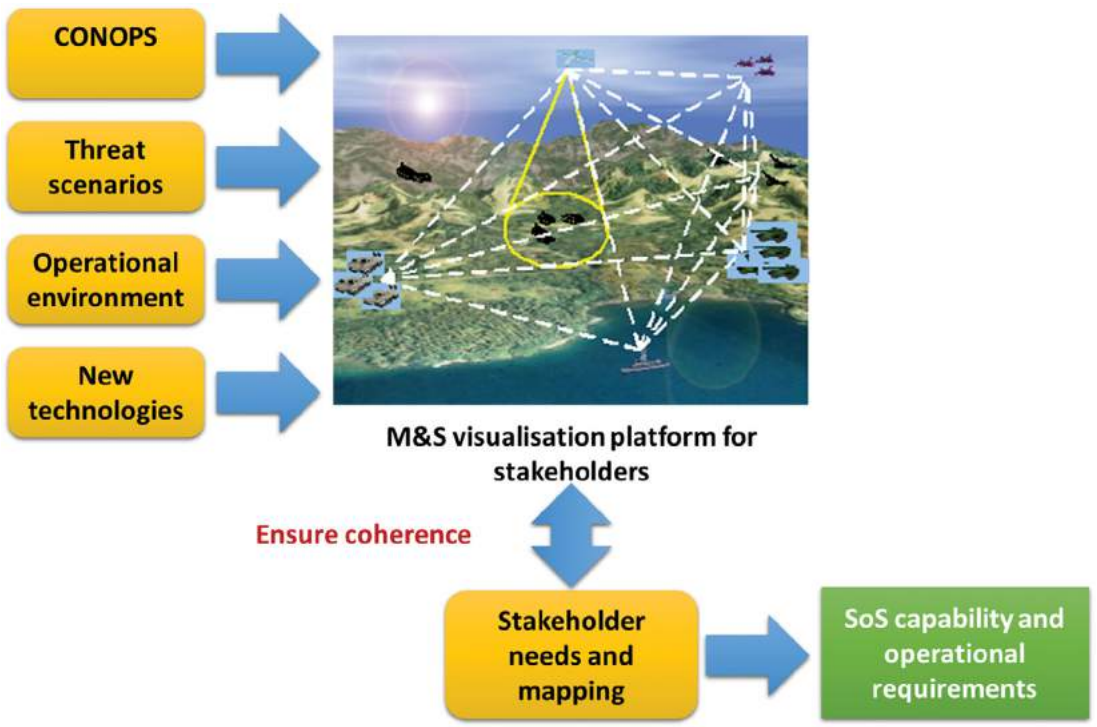


JEWEL Framework

M&S for SoS Concept Visualisation

M&S can represent and visually play out the concept of operations (CONOPS) through dynamic movement and actions enacted by high-level units. Threats and their high-level strategies can be modelled in the form of computer-generated adversarial forces. Similarly, operational environments such as urban landscapes can be simulated with terrain, buildings and weather models. The result will be a synthetic visual and animation platform for stakeholders to communicate their needs in a given SoS context, while allowing for the flexibility of modifying scenario conditions and inserting new technology models. The heuristic nature of the framing the SoS constraints and constructing the architecture can now be dissected into a less abstract form through M&S visualisation for stakeholders with different viewpoints and perceptions to generate a consensual set of capabilities and operational requirements for the SoS architecture.

In the case of our military SoS example, the SoS concept of operations was articulated using the Operational View 1 (OV-1) of the US Department of Defense Architecture Framework. However, OV-1 was limited in the sense that only a static view of the concept is shown. We leveraged the time-stepped M&S tools to enrich this view by simulating the dynamic flow of operational concepts in action, providing a greater level of clarity in representing the concepts to stakeholders.


CONOPS
Threat scenarios
Operational environment
New technologies
M&S visualisation platform for stakeholders
Ensure coherence
Stakeholder needs and mapping
SoS capability and operational requirements

M&S as a Visualisation Platform for SA

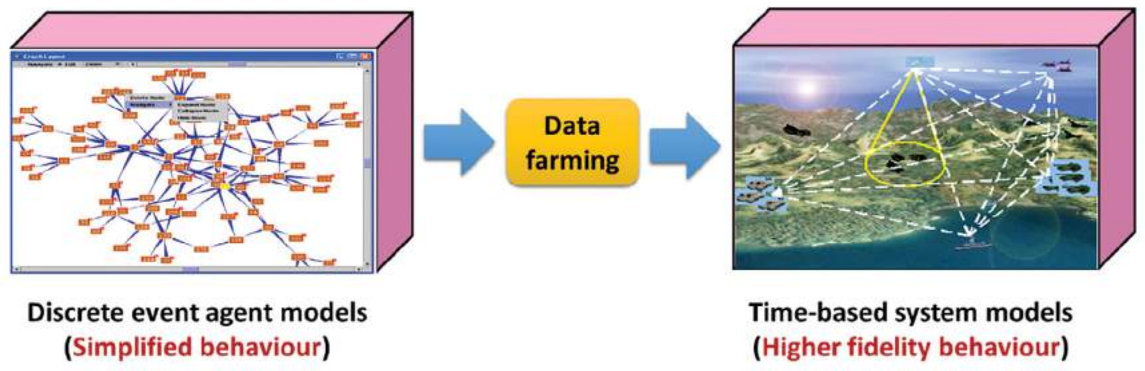
M&S for Architecture Evaluation

Quantitative measures of evaluating SoS alternatives are needed to provide a comprehensive level of assessment, especially for identifying capability gaps in the SA process. Time-stepped M&S can be one of the means, through providing a synthetic environment with individual systems, threats and interactions modelled to play out the capabilities of each SoS architecture alternative in the context of multi-scenarios. Data corresponding to the Measures of Effectiveness (MOE) or Measures of Performance (MOP) drawn from the SoS capabilities are logged and compared to determine the final SoS architecture to be selected.

The models required for SoS evaluation have to be at a sufficient fidelity level for individual platforms, weapons, sensors or military IT systems. However, there could be many parameters that can be modelled for each system. Given the range and number of systems and threats in a SoS evaluation scenario, it would be too time-consuming and inefficient to model and tune these parameters for evaluation. Data farming, the concept of exploring a large parameter space across numerous fast simulation runs, can help to identify which are the inter-related parameters that have a significant impact on the MOE/MOPs. This idea has been explored by the US Joint Test and Evaluation Programme, under the Joint Test and Evaluation Methodology (JTEM), to reduce the evaluation and test space for complex adaptive SoS in a joint mission environment. Data farming requires M&S tools based on discrete event agent-based models for fast computation. Under the Model-Experiment-Model approach, simplified agent behaviour models with an initial set of parameters and inter-relationships are experimented with large numbers of data farming runs to uncover the significant parameters of concern. These parameters will in turn be incorporated into higher fidelity time-stepped system models for SoS evaluation.

On evaluating SoS performance, the higher fidelity models can simulate the physical effects of real time interactions between systems, units and the environment, achieving a more realistic assessment of the SoS capability in meeting operational needs. Human operators are employed in the environment as red team players to detect vulnerabilities within the SoS or discover counter-strategies that may work against the SoS. The results are used as a measure of robustness in the architecture. Vulnerability can be assessed by selectively injecting system failures into the synthetic SoS representation, and checking if alternative paths exist in the network to ensure the SoS can still function effectively under these circumstances.

To accurately model and evaluate the SoS architectures, the required MOE/MOPs must be tied to the model outputs. If these criteria are too abstract or broad to be quantified in the time-stepped M&S environment, they would be broken down into measurable constituents. For example, shared situational awareness can be represented as timeliness of update, precision of information received and accuracy of detections with ground truth.



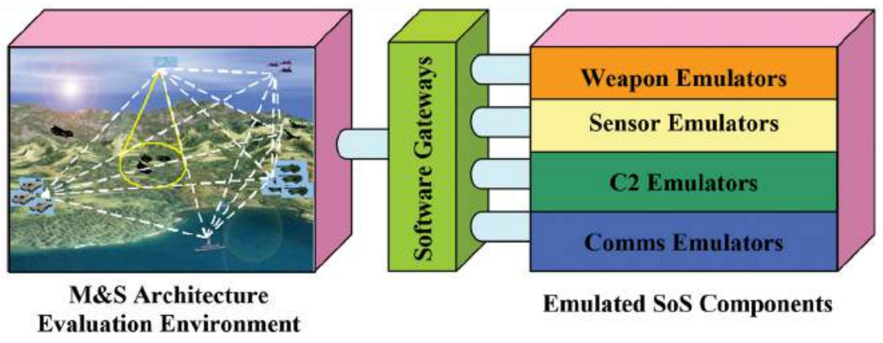
Model-Experiment-Model Approach

In evaluating our military SoS, we made use of different modelling tools for various aspects of the SoS and employed the “Model-Experiment-Model” approach with the evaluation environment, instead of using data farming. Models simulating the military domain would generate a set of outputs such as timing and information flows, which are then fed into warfare models simulating combat behaviour and their effects in meeting SoS objectives. Their resultant actions and attrition are then re-inserted back into the military models to be re-evaluated with a new set of initial conditions. The process is repeated for a number of cycles to obtain a reasonable list of evaluated outcomes for assessment, based on the range of conditions to be explored, as determined by design of experiment techniques.

Capitalising on the value of the models that have been developed for each instance of SoS architecture evaluation, the models are designed and built based on a common set of architectural specifications, such as the JEWEL framework, to support future reuse in other SoS studies. This can greatly reduce the evaluation period. Data obtained from various sources during the evaluation are also stored in a knowledge management repository, instead of having to procure them again from the relevant parties, which might lead to longer delays for future evaluation.

M&S for SoS validation

The final step in the SA process requires an environment to test the interoperability among systems within the SoS and verify the SoS architectural capabilities offered by these systems. To replicate the SoS architecture and test conditions with actual systems in a “live” environment incurs extensive resources and manpower costs, and some scenarios are impractical for testing as they might lead to collateral damage. Customisable time-stepped M&S tools such as JEWEL offers another alternative by emulating the individual systems in terms of interfaces, consoles and processing logic. This allows SoS interoperability to be tested even before the systems are acquired or developed. The technique has been applied for C2 systems development, but we are expanding the concept to include weapons, sensors, communications and other SoS systems elements. The emulated systems will be integrated with the same M&S environment used in the evaluation stage via customised software gateways. This allows the same set of evaluation conditions and scenarios to be tested with the



Using M&S emulation and the M&S evaluation environment as a SoS test-bed emulated system interfaces. With the aid of the emulated consoles, human operators can be involved too, ensuring a more robust SoS test environment with real-time operational inputs. Any interoperability issues discovered can be rectified by modifying the modules in emulated systems, as opposed to the more expensive task of modifying actual systems. It can also serve as a virtual environment for experimenting with man-machine interface designs in manned system consoles (e.g. the effects of information overload on operator's performance) and algorithm designs in decision support systems (e.g. data fusion rules), before they are developed.

Other than tackling SoS interoperability, the test-bed can be used to validate the performance of the SoS, using the same set of operational scenarios and threat environments. Any limitations posed by the emulated systems on the SoS performance can be resolved by modifying the workflow process, re-designing the emulated systems logic or restructuring the architecture. When the entire SoS has been tested, the emulators can be replaced by actual systems as they come online, to verify the conformance of acquired or developed systems with the SoS design. This replacement is facilitated by designing the emulator software gateways to comply with the same specifications as in the real systems. The outcome is a more comprehensive SoS validation with a shorter timeline and lower costs.

The military SoS that we designed made use of the above M&S techniques in the SoS interoperability testing phase. The SoS performance validation was carried out concurrently with emulated systems testing to root out any issues posed by various scenarios on the users' application workflows and other SoS elements. In this way, some of the emulated interface tests can be avoided, as new changes in the workflow to handle SoS performance issues may require modifications to the initial system communication interfaces. A System-of-Systems Integration Lab (SoSIL) was set up for this purpose. This is similar to the SoSIL employed by Boeing for the Future Combat Systems (FCS) programme to integrate and test system elements within the FCS SoS architecture before deployment.

The completion of the SoS validation process does not mean the end of the M&S facility set-up. As the SoS exists over a long period of time, any evolving changes in technology or operational environments and their impact on the SoS can be reviewed using the same synthetic environment. The SoSIL can also double up as a virtual training facility in the future for new system operators, with customisable scenarios, simulated threats and red force player stations.

Conclusion

M&S tools for discrete event and time-stepped simulation can serve as a visualisation platform for stakeholders to communicate and determine SoS needs. Alternative SoS architectures can be evaluated using a time-stepped simulation environment with configurable threat scenarios, environmental conditions and red team players. The evaluation metrics can be determined through data farming by discrete event models and planted in a higher fidelity time-stepped M&S environment for automatic logging during the simulation to facilitate analysis for architecture selection. To resolve SoS Interoperability issues during SoS development, system emulators built using customisable M&S tools can be linked to the same M&S evaluation environment for testing even before the systems are acquired or developed. These emulators can be replaced by actual systems during factory conformance or acceptance testing. This would greatly reduce design and modification risks before the SoS is deployed. Some of the challenges faced include convincing stakeholders to leverage M&S capabilities in SA, trade-offs between more realistic M&S solutions or faster SoS architecture turnarounds with less design considerations and getting quality data from subject matter subjects for SoS validation.

Harnessing Synergy Of OA, Simulation, and Operational Test and Evaluation

Introduction

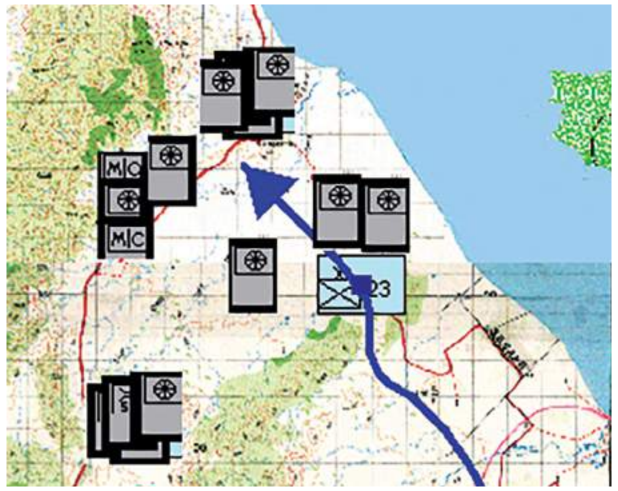
OA, Simulation and Operational Test & Evaluation[2] (OTE) in the form of field trials are important M&S tools used by the SAF. OA is a versatile tool to support decision in planning and operations whereas simulation, which in this context refers to wargame and simulator, is a tool that is expanding its role from supporting training to supporting force planning and operations as well. On the other hand, OTE can be seen as a useful tool to collect data, and provide feedback and support to OA and simulation. It is important to fuse the complementary functions they play in planning, acquisition, operations and training to ensure that the SAF maintain the critical operational edge in the complex battlefield of the future.

Impetus for Synergy

The impetus for synergistic employment of OA, Simulation and OTE trials is due to their inherent strengths and limitations as a result of the way they mimic the combat systems, combatants and the environment.

To Each Its Best – OA, Simulation and Field Trial

With combatant, combat systems and operational environments entirely either modelled or simulated, OA requires relatively less cost, manpower and time compared to war games, simulators and field trials to examine concepts and combat systems from the campaign to engagement level. These strengths give OA the ability to perform many iterations in a relatively short time for evaluation of alternative concepts and technologies and sensitivity analysis to identify the critical or sensitive parameters. Its strengths are also its limitations. The lower model fidelity of combatant, combat system and environment, especially in C2, places constraint on the ability of OA to study their tactical interactions in details.



Example of an OA or constructive simulation tool

The strength of war games is its ability to configure the simulation according to the C2 structure and allow battle planning staff to interact with one another in a real-time command post environment. However, the rather substantial manpower and time required to support a single simulation run does not permit it to run sufficient runs and compare various alternative concepts and technologies to obtain conclusive results. As for simulators, its strength is that it has higher

[2] OTE programmes are designed to determine and, wherever possible, enhance the overall operational effectiveness of a system by evaluating the operational effectiveness and suitability of a system under realistic operational conditions. Throughout the rigorous Operational Tests, the OTE Planning Team will determine if operational effectiveness and suitability requirements have been satisfied and will develop the initial procedures for employment of the system.

fidelity than war games and OA in that it allows a small team of operators to interact with one another and with part of the real combat system physically.

The highly realistic interactions make virtual simulation suitable for examining combatant interactions in detail. However, the high cost of simulators only permits it to examine concepts and combat systems up to mission-level. Also, the need for operators to man it and the relatively long duration for each trial make simulators less ideal when many iterations are needed or many different scenarios and parameters are to be examined.

The possession of highest realism as a result of having live combatants and combat systems forces operating in live environment with instrumented system is the main strength of OTE. It allows a measurement of combat system performance as close as possible to actual combat. The need for a considerable amount of resources and space to support a field trial means that it should be judiciously employed.

SAF soldiers conducting a live firing exercise at the Murai Urban Live Firing Facility.

What's In It For The Synergy?

Individually, OA, Simulation or OTE each has its limitation and may not be able to address the wide range of issues involved. By fusing their strengths through synergistic employment, the following benefits can be achieved:

- *Confidence and Quality of Assessment.* OA, Simulation and OTE provide successively higher levels of fidelity that can be capitalised to support, check or substantiate the overall experimentation results. OA is valuable for first-level assessments, Simulation for higher-fidelity results incorporating human-in-the-loop at critical decision nodes, and OTE for determination of actual "in-environment" performance. Used in concert, they engender greater confidence in the validity and quality of the results.
- *More Thorough and Comprehensive Analysis.* All three domains are complementary as they can support analysis at different stages of the capability development process. Together they provide a comprehensive range of test environment and experimentation options for more thorough analysis.
- *Focus and Cost Effectiveness.* Each tool can be used to identify key issues and parameters for more focused investigation at the next level of experimentation. This ensures a more productive and more cost-effective process. This is particularly true for OTE which entails significant real (and expensive) resources and where test windows are hard to come by.
- *Higher quality models.* Lastly, OTE data collected from realistic operational exercises and trials can be used for calibration of unit/force performance models and weapon/sensor models used in all M&S applications (training, operational decision support and experimentation).

Areas of Synergy

The synergistic employment of OA, Simulation and OTE can lead to the following four areas of synergy:

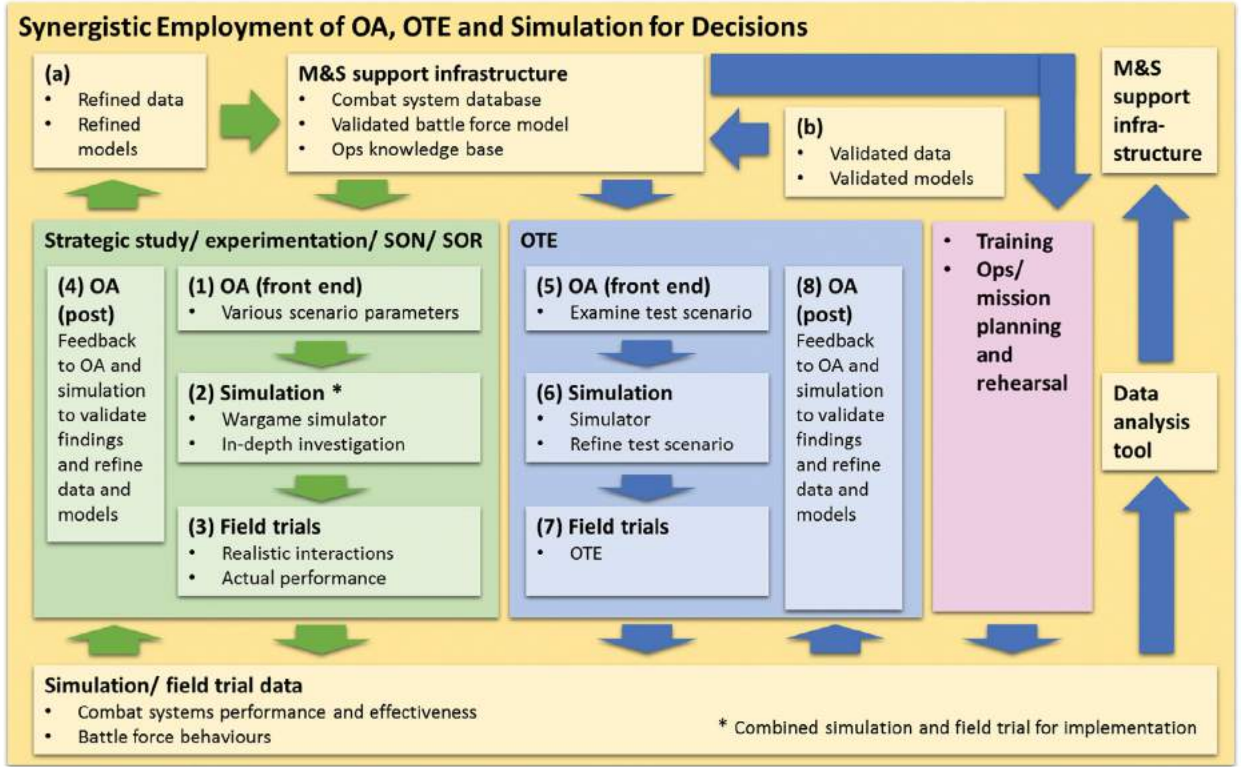
- Providing a more comprehensive, credible and cost-effective M&S support for decision-making.
- Greater sharing of data and knowledge to provide more accurate models and results.
- Greater sharing of models for training, experimentation and OA, ops support to optimise M&S resources
- Co-evolution of experiment, tactics and doctrine, training to achieve better integration of force transformation and force employment.

Synergy for Decision-making

The synergistic employment of OA, Simulation and OTE will support the effective force planning and effective force employment. Force planning will include long-term strategic study, experimentation, concept formulation and SON/SOR. Force employment will cover OTE, training, tactics and doctrine development, and operations and mission planning and control. There are two broad processes for synergistic employment of OA, Simulation and OTE, namely Analysis (Front-end)-Validity Check-Analysis (Post) [A(FE)-VC-A(P) Process] and Model-Test-Model [M-T-M Process].

A(FE)-VC-A(P) Process

- *Analysis (Front-end).* For a thorough assessment of a new concept or system of systems, the effects of different variables, conditions and scenarios should be examined through many computations. The lower fidelity OA tool is well suited as the quantitative tool for such a front-end assessment to evaluate the new concept or SoS because of its lower cost, and better and faster computation capability. It can also identify those critical issues and parameters to maximise the return of simulation and live trial. Though the front-end analysis provided by OA tools can provide some good assessment, its findings are inconclusive because it cannot adequately address the human dimension of planning and execution.
- *Validity Check.* In the next stage, synthetic validity check on data used in and findings of the front-end analysis can be conducted using the higher fidelity simulation either in the form of war games or simulators to examine the human dimension of planning and execution of the promising


Synergistic Employment of OA, OTE and Simulation for Decisions
(a)
• Refined data
• Refined models
M&S support infrastructure
• Combat system database
• Validated battle force model
• Ops knowledge base
(b)
• Validated data
• Validated models
M&S support infra-structure
Strategic study/ experimentation/ SON/ SOR
(4) OA (post)
Feedback to OA and simulation to validate findings and refine data and models
(1) OA (front end)
• Various scenario parameters
(2) Simulation *
• Wargame simulator
• In-depth investigation
(3) Field trials
• Realistic interactions
• Actual performance
OTE
(5) OA (front end)
• Examine test scenario
(6) Simulation
• Simulator
• Refine test scenario
(7) Field trials
• OTE
(8) OA (post)
Feedback to OA and simulation to validate findings and refine data and models
• Training
• Ops/ mission planning and rehearsal
Data analysis tool
Simulation/ field trial data
• Combat systems performance and effectiveness
• Battle force behaviours
* Combined simulation and field trial for implementation

concept or system identified in front-end analysis. When necessary, the live trial that has the highest fidelity should be conducted to collect realistic data for operational validity check. In certain circumstances, a combination of war games, simulator and field trials is used to support the validity check.

- *Analysis (Post).* The findings of the validity check will be used to calibrate the OA inputs and models employed in the front-end assessment. The calibrated OA tool can then be employed to refine the assessment. Similarly, the live trial findings can also be used to calibrate the simulation inputs and models so that the simulation findings can be refined.

M-T-M Process

This process is primarily for OTE and live experimentation. The conduct of OTE and live experimentation involves substantial resources and effort. To maximise the test resources, a synergistic process known as the Model (Pre-Test)-Test-Model (Post-Test), can be employed.

- *Model.* OA and simulator are used to support test planning to examine the criticality of data and test scenarios to focus the collection effort.
- *Test.* Once the data to be collected is identified, the normal OTE planning and execution will be carried out to collect them. Statistical analysis will be conducted on the data collected.
- *Model.* The OTE data will be used to calibrate the battleforce models in OA and simulation and the validated data and models will form part of the M&S repositories. The calibrated OA can also be employed to refine the assessment, if necessary, on tactics and doctrine, and operations and mission plans.

Conclusion

While OA tools play an important role in quantitative measurement of operational, mission and system effectiveness, they lack a comprehensive representation of the complex combatant's cognitive ability that can deal with the full range of future combat situations. Such inadequacy of OA can be complemented by Simulation and OTE that allows human participation to examine decision-making process, interactions between combatant, and interactions between combatant and combat system. Synergistic employment allows us to exploit their combined strengths to better examine the full spectrum of issues involved.

Analytic Hierarchy Process for Tender Evaluation

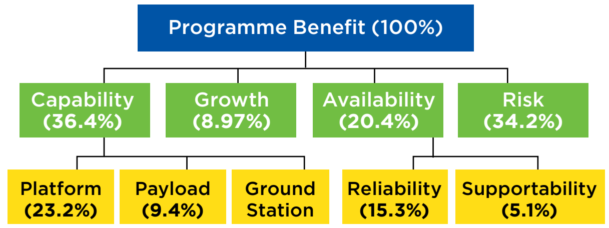
Introduction

In 1988, MINDEF approved the use of quantitative selection methodology as a method of supplier selection for weapon acquisitions. The AHP was chosen and applied in several projects before it was formally mandated in 1993 for use in all complex and high-value weapon acquisitions.

Following the successful implementation of the AHP for weapons and platforms, its use was extended to design-and-build construction projects, software developmental projects and more recently, outsourcing tenders for MINDEF and the SAF. The success of DSTA in acquiring cost-effective solutions has also garnered the interest of the Public Service as a whole and in 2005, the Singapore Tourism Board engaged DSTA as a consultant on the selection of proposals for its integrated resorts. This led to other ministries and government agencies seeking to apply AHP for their projects. In 2009, the Ministry of Finance (MOF) found it opportune to make AHP a mandatory evaluation tool for all complex and high value government acquisition projects. This policy was incorporated into the MOF's revised Instruction Manual on Procurement issued in June 2009.

Development of AHP Evaluation Model

AHP is a decision-making support tool developed in the 1970s by Thomas Saaty, a mathematics lecturer from the University of Pittsburgh, USA. The process requires the establishment of a hierarchy of criteria and sub-criteria which is important to reach a decision objectively and systematically. This is especially true when there are multiple stakeholders with different criteria and needs. These criteria and sub-criteria are weighted to determine their relative importance in reaching the decision, eventually forming the AHP model. As part of the evaluation framework, the AHP model – or what is commonly called the AHP tree – will need to be finalised and approved prior to the close of the tender to ensure that the model is objective and does not favour any particular submitted proposal.



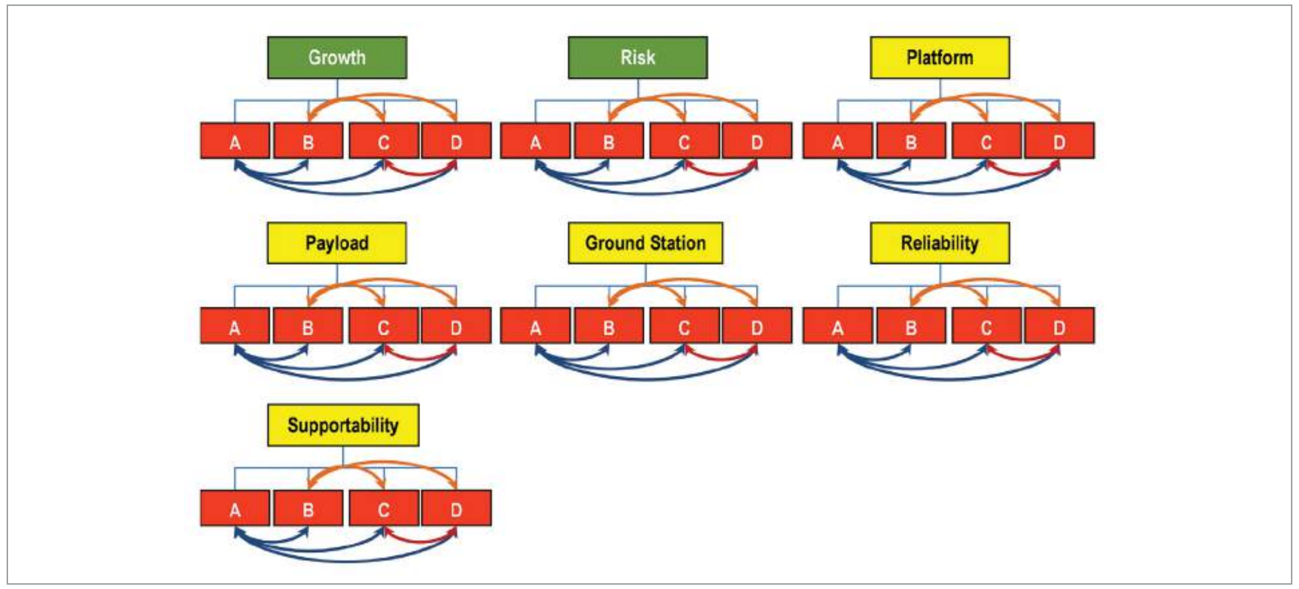
Example of an AHP hierarchy of criteria and sub-criteria with weightages

Contrary to some decision-making methodologies where the weightages of criteria are estimated, AHP has a scientific and systematic approach to help decision makers sieve out the relative importance of criteria and sub-criteria as well as allocate the weightages accordingly. This scientific approach to determine weightages is done via pair comparison, otherwise known as pairwise comparison. Saaty (1980) provided a scale for the pairwise comparison, together with eigenvectors and eigenvalues mathematical principles, to derive the weightages of criteria from the pairwise comparison matrix at a particular level of the AHP model. The allocated weightages from pairwise comparison reflect the importance of criteria that would influence the evaluation outcome.

Proposal Evaluation

In the evaluation of programme proposals, pairwise comparison is again applied to all of the proposals under each of the last level criterion in the AHP tree. A scale is used for the pairwise comparison with the level of importance changed to level of preference. The end result will be a ratio of scores for each proposal with respect to the weight of the criterion. The summation of all the derived benefit scores for each criterion would give the overall benefit score of each proposal.

Price proposals will only be released after the completion and approval of the programme proposal evaluation report, where the programme benefit scores for each proposal is fixed. The evaluation team would then proceed to conduct a benefit-cost evaluation to determine the most cost-effective proposal with the greatest benefit per dollar for contract award. For cost proposal assessment, the evaluation team does not consider only the front-end acquisition cost of the system. It takes into account the system's LCC or TCO, which include the cost of operating, maintaining and supporting the system throughout its planned life cycle with the SAF. The rationale for using LCC or TCO is to ensure that the acquired system is not only cost-effective in the initial acquisition phase, but also for the rest of its operating service life. This key application of AHP helps DSTA, MINDEF and the SAF ensure that the acquired system is cost-effective yet sustainable.



Proposal evaluation using pairwise comparison for Proposals A, B, C and D under each last level criterion

Conclusion

The ability to apply AHP effectively for tender evaluation has enabled DSTA, MINDEF and the SAF to acquire optimised and cost-effective systems and capabilities. Besides the standard academic methodology, deep understanding of the relevant technology domain, key application considerations and the ability to relate to the operational needs of users are also imperative in identifying the most suitable solution. Many of the experiences in AHP application are institutionalised in DSTA's courses, workshops and guides conducted by experienced practitioners to ensure that robust evaluation practices are employed by future evaluation teams.

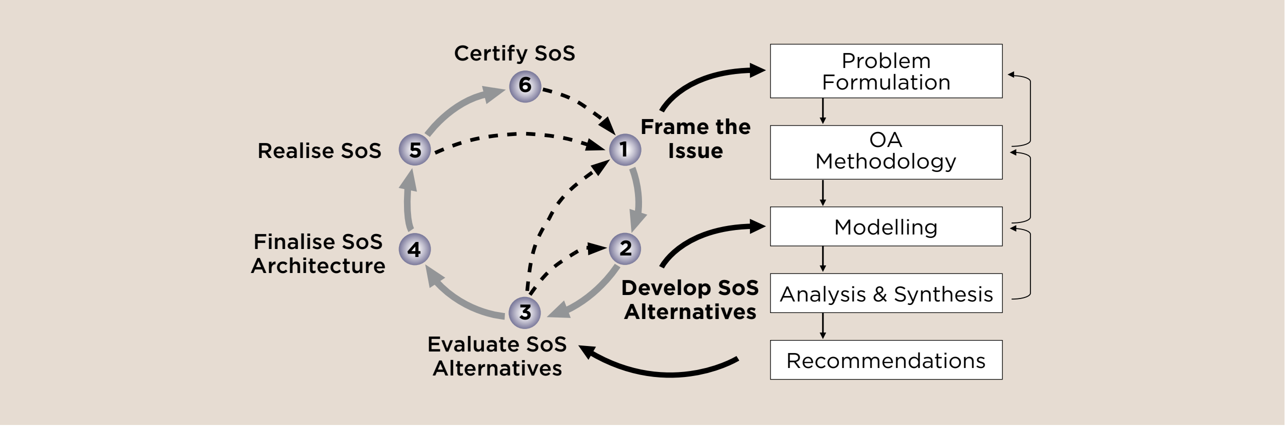
Operations Analysis to Evaluate SoS

Introduction

The SAF embarked on a transformation journey to become a Third Generation armed forces several years ago. The Third-Gen SAF comprises a sophisticated network of sensors, communication systems, high-end fighters, stealth frigates and main battle tanks. The systems for a Third-Gen SAF will be increasingly complex, versatile and intertwined as components of SoS. DSTA has leveraged OA discipline to analyse the effectiveness of SoS and evaluate SoS options as part of the SA process.

The DSTA SA process consists of six iterative steps. During the problem formulation phase, OA analysts support DSTA Systems Architects in framing of issues and to formulate the problem statement. After the problem statement has been defined, OA analysts would work on the appropriate approach to analyse the problem, while DSTA Systems Architects continue with the development of alternative systems architecture. These alternative systems architecture serves as input for the OA model.

Throughout the SA process, operations analysts work closely with SA team to verify and valid the model(s), and to analyse the various SoS alternatives using the model(s). Results and insights generated from the analysis are then presented to the appropriate decision-making forum. The outcome may warrant further analysis as new issues are illuminated from the study.



Applying OA to evaluate SoS

Model-Experiment-Model Approach

Simulation is one of the many techniques used in OA. With the advancement in computing technologies, M&S has evolved into a mature discipline with wide ranging applications. Over the years, the SAF has forged ahead, harnessing M&S for areas beyond training, including operational mission planning and rehearsal, decision support, as well as test and evaluation. In recent times, M&S has also become an essential technology and tool for military experimentation.

JEWEL consists of a repository of models, databases, components and interfaces, supported by a common simulation engine architecture, with key emphasis on reusability and interoperability with external simulation and military IT systems. JEWEL serves as the simulation environment for SAF military experiments, and is also used extensively in SA using a Model-Experiment-Model approach.

The Model-Experiment-Model approach leverages different OA techniques, namely, mathematical programming and simulation, as an iterative process to study the effectiveness and behaviour of SoS. An example of a complex SoS is the integrated air defence network that comprises early warning aircraft, fighter jets, ground surveillance radars, and surface-to-air missile systems supported by a C2 network. The integrated air defence network is dynamic in nature where its component systems interact and reinforce with each other for mutual benefits.

With Model-Experiment-Model approach, an analytical model can be developed to optimise the multi-layer integrated air defence network. For example, this analytical model aims to optimise the weapon target allocation with an objective function to maximise survivability of key installations subject to a set of constraints such as weapon availability, cost and manpower. This model would optimise a proposed integrated air defence systems architecture. This optimised architecture is included as an input to the simulation environment for the conduct of experimentation. In the simulation environment, multiple scenarios are considered to analyse the robustness of the proposed architecture. The simulation results serve as a feedback to fine-tune the analytical model, leading to the need to consider additional constraints like priority list of key installation, for example.

Using this approach, the overall SoS dynamics, performance and effectiveness of various alternative systems architectures in multiple scenarios may be analysed and evaluated.

Networked System Availability

Introduction

The next-generation SAF is seeing revolutionary changes in operation tempo, mission definition and combat service support. Systems are becoming more interconnected and interdependent to leverage the network and information as force multipliers. For instance, a typical defence capability will consist of not one but several systems, namely weapons systems connected to communication and sensor systems, with each possibly taking the form of a complex network. Planning done at the system (platform) level is no longer adequate to ensure mission success for such network-centric operations. As such, the availability of a single system is no longer sufficient, and the networked system availability is a much better representation.

Today, the in-house developed Optimised Decisions in Networks (ODIN) tool equips DSTA, MINDEF and the SAF with the ability to quantify networked system architecture and to identify critical links or bottlenecks that enhance design decision of the architecture. It provides the means to examine network robustness and survivability under complex threat environments. ODIN seeks to perform resource (spares, technicians) optimisation at the network or SoS level to ensure they are considered holistically to meet stringent demands.

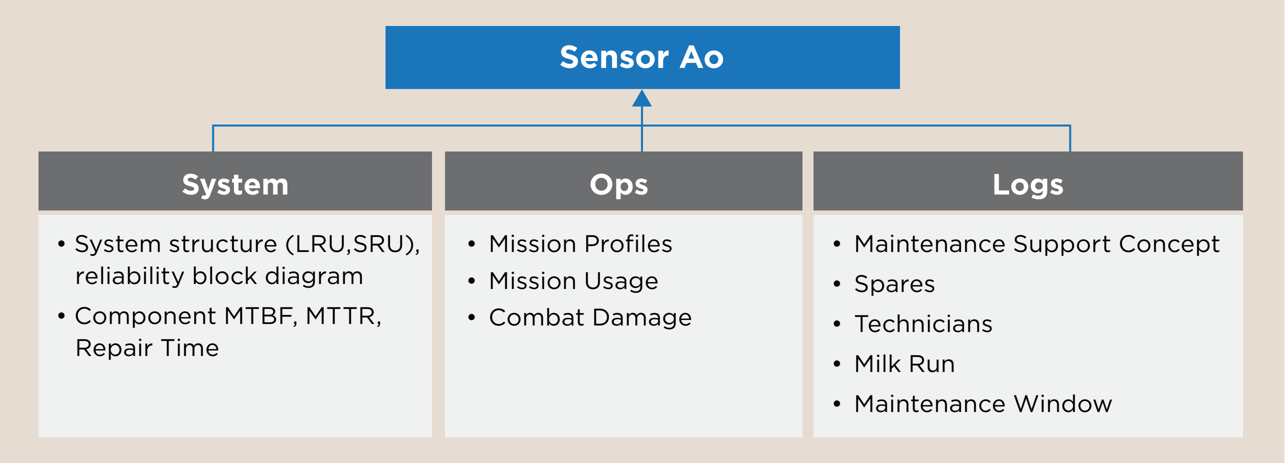
Networked system availability is defined as the availability of the interconnected systems at an end-to-end level. It quantifies the availability of having a link from one point to the other while having to route through the various component systems. Each of the component systems has its individual system level availability (Ao) defined by system level dependency on system, operational and logistics factors. Many often argue that such networked Ao can be obtained by simply multiplying them together using analytical formulae. This will derive a quick answer to the simple series-parallel type of networked system. However, such a method is very restrictive. First, typical networked systems are often meshed to meet the network redundancy requirements and it is difficult to formulate the analytical equation. Second, it is not possible to capture the interoperability and interdependency that occurs simultaneously across the multiple system types. The largest drawback lies in the analytical formulae multiplying the average of each component system Ao and hence losing the interdependency effect across systems that is the critical basis to the availability of a networked system. In the next section, the limitation of applying system level availability to an increasingly networked system environment is further illustrated.

ODIN analyses interdependent factors across networked systems to ensure mission readiness

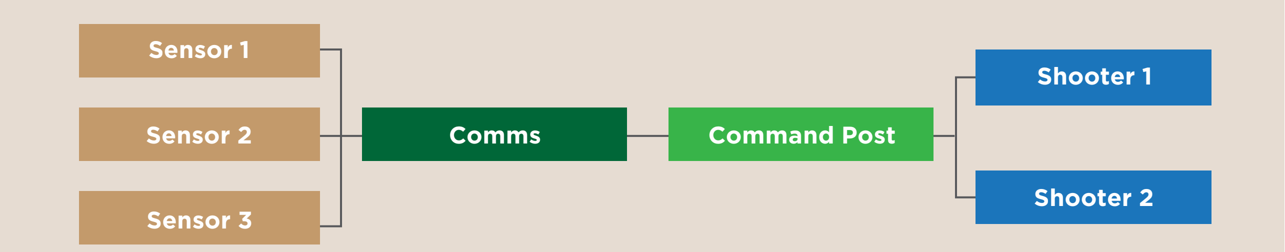
Key Capabilities:

1. ODIN provides the ability to evaluate and optimise for end-to-end availability across networked system.
2. ODIN boosts the robustness and resiliency of network architecture through network analysis.
3. ODIN contributes to mission readiness by optimising resources at networked system level.

Overview of key capabilities in ODIN



Factors influencing the sensor availability



Ao (Networked System) =

$$[1-(1-Ao_{Sensor\ 1})^{*}(1-Ao_{Sensor\ 2})^{*}(1-Ao_{Sensor\ 3})]^{*}Ao_{Comms}{}^{*}Ao_{CommandPost}{}^{*}[1-(1-Ao_{Shooter\ 1})^{*}(1-Ao_{Shooter\ 2})]$$

Where Ao (Networked System): Availability of interconnected system end-to-end;

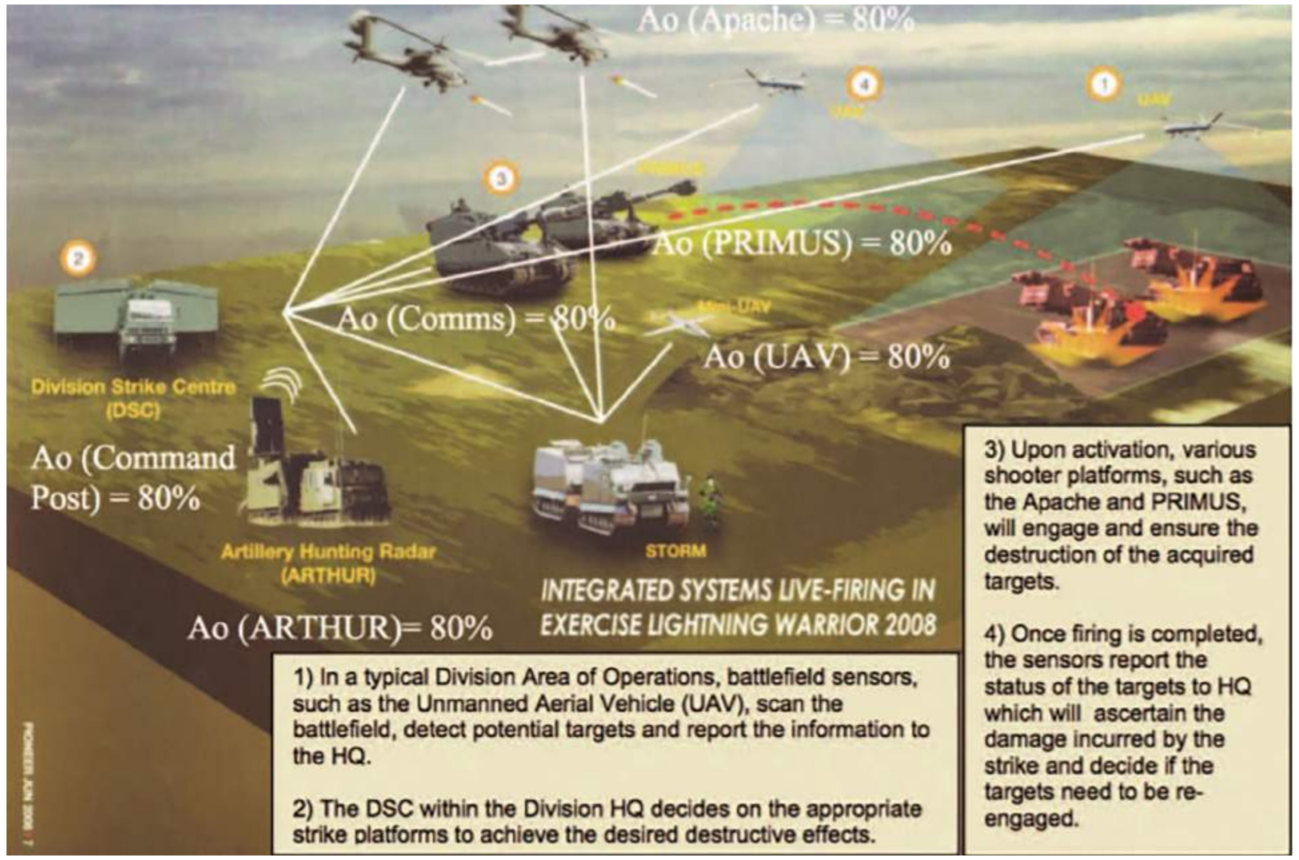
$Ao_{Sensor\ 1}$: Availability of sensor system i;
Ao_{Comms} : Availability of comms system;
$Ao_{CommandPost}$: Availability of Command Post system;
$Ao_{Shooter\ j}$: Availability of Shooter system j

Analytical computation for simple networked system availability

Analysing Networked System Availability

Using an integrated system live-firing exercise, sensors in the form of an unmanned aerial vehicle or Artillery Hunting Radar (ARTHUR) are used to conduct battlefield surveillance and detect potential targets. Images of the ground surveillance are sent back to the command post via a communication network that allows the commander to decide on the appropriate strike platforms to take out the adversaries. From the command post, the target positions and information are sent via a communication network to the strike platform, which will engage and ensure the destruction of the acquired targets. It is evident that the mission success of acquiring and destroying the adversary is dependent on the integrated working of all systems types inclusive of communication networks. Should any of the systems be down, the mission will fail.

Typically, Ao, spares and resources are evaluated and allocated for each individual system – for example, Ao of 80% for each of the sensor and shooter systems. Such measurement is unable to reflect the interdependency of the various systems across the communication network for the mission. It may also potentially lead to under or over provision of resources and impact the logistical readiness of the systems.


Ao (Apache) = 80%
UAV
Ao (PRIMUS) = 80%
Ao (Comms) = 80%
Mini-UAV
Ao (UAV) = 80%
Division Strike Centre (DSC)
Ao (Command Post) = 80%
Artillery Hunting Radar (ARTHUR)
STORM
Ao (ARTHUR)= 80%
INTEGRATED SYSTEMS LIVE-FIRING IN EXERCISE LIGHTNING WARRIOR 2008

1) In a typical Division Area of Operations, battlefield sensors, such as the Unmanned Aerial Vehicle (UAV), scan the battlefield, detect potential targets and report the information to the HQ.

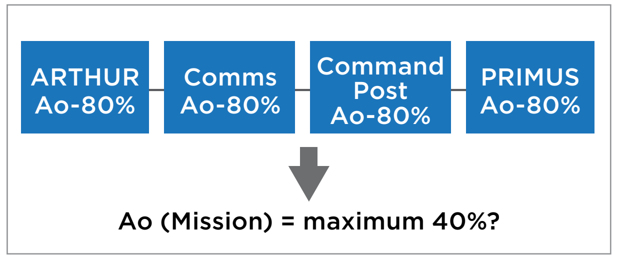
2) The DSC within the Division HQ decides on the appropriate strike platforms to achieve the desired destructive effects.

3) Upon activation, various shooter platforms, such as the Apache and PRIMUS, will engage and ensure the destruction of the acquired targets.

4) Once firing is completed, the sensors report the status of the targets to HQ which will ascertain the damage incurred by the strike and decide if the targets need to be re-engaged.

An example of an integrated systems live-firing exercise

A simplified "acquire and destroy" mission calculation is shown in the following figure, where ARTHUR is used as the sensor, PRIMUS as the weapon system, command post as the C2 centre, and a fixed communication network as the means of information and data transmission. By adopting a standalone system as the criteria for resource or maintenance support planning, the planner would ensure an Ao of about 80% for each of the individual system. However, from the "acquire and destroy" mission definition, it would require all the systems to be functioning together. If the planner's resource planning for each system is at 80% Ao, the entire networked system would have a maximum logistical readiness of only 40% by simple multiplication. Therefore, resource planning should be carried out at the networked system level. Planners can no longer perform their resource and maintenance support planning by treating each system as a standalone system. With the interdependency among the systems, the Ao of each system may no longer be treated independent of one another. Measurement of the performance of the networked system "acquire and destroy" mission needs to be performed within the model itself.



Simple illustration of integrated mission Ao computation

Extending Network Ao Computation

With such a complex network structure, system level Ao measurement can no longer suffice as a good MOE as it becomes more dynamic and largely dependent on the context. Two MOEs will first be defined and how these MOEs are used will be illustrated.

Mission Ao/Probability of Mission Success

Mission Ao will see tighter integration between the operational and logistical context. This MOE requires the operational context to define how the operators had intended to interoperate the systems to ensure mission success. This mission Ao is highly dynamic and dependent on mission definition.

The mission Ao is defined as the "acquire and destroy" mission. It measures the probability of having sensors acquire the targets and transmitting the information to the appropriate shooters for them to take out the adversaries simultaneously. Mission Ao can also take the form of division to brigade Ao which measures the end-to-end availability from division to brigade by factoring the means for commanders to communicate to ensure mission success.

Matrix of System-to-System Ao

In some scenarios such as a large communication network, single networked system Ao does not adequately represent and evaluate the performance of such a large networked system. Instead, a paradigm shift towards the use of upper triangular matrix of system-to-system Ao proves to be a better MOE when there are multiple source-sink pairs and bi-directional traffic profiles. This matrix MOE allows one to evaluate each pair of system-to-system Ao and aids in identifying the weak links and bottlenecks at a quick glance. For example, system-to-system availability of system 24 to system 58 is low at 22.8% while system-to-system availability from system 51 to system 58 is at 73.2%.

Implementation and Case Studies

The MOEs discussed earlier were implemented within ODIN tool and further illustrated using two case studies.

Case Study 1: Networked System Architecture Evaluation

As part of the architectural evaluation of the robustness of the Networked Air Defence design in meeting its mission objectives, end-to-end network availability from sensor to C2 to shooters was performed. Several key considerations such as sensor network were factored in since there were no dedicated sensor-to-shooter pairs. In addition, shooters were dispersed across large geographical locations and linked back to the central C2 system. Moreover, there was the need to handle the IT infrastructure and communication equipment to provide the connectivity among sensor, shooter and C2. Adding to the complication was the different network configurations across different mission phases. All these were modelled through the ODIN multiple network layers that were interconnected and inter-linked to provide end-to-end mission readiness.

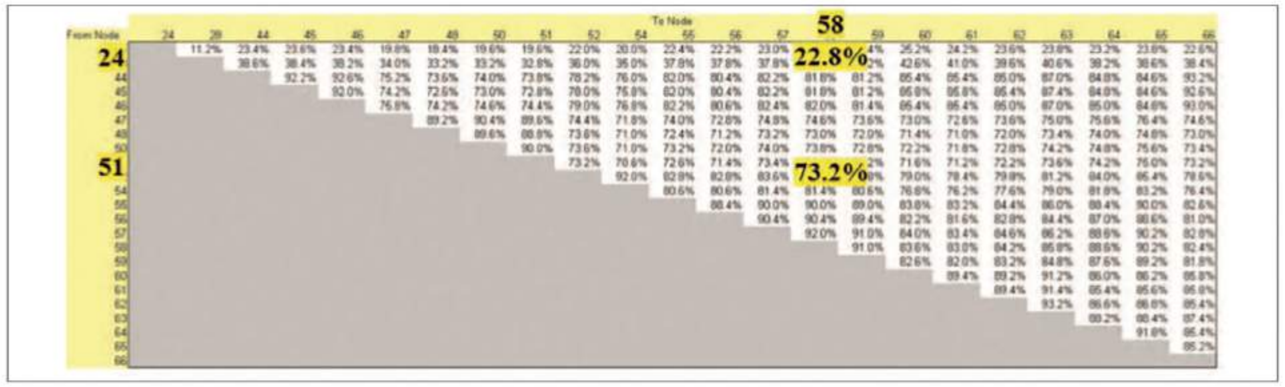

From Node
To Node
24
51
58
22.8%
73.2%

Illustration of the upper triangular matrix tabulation of system-to-system Ao

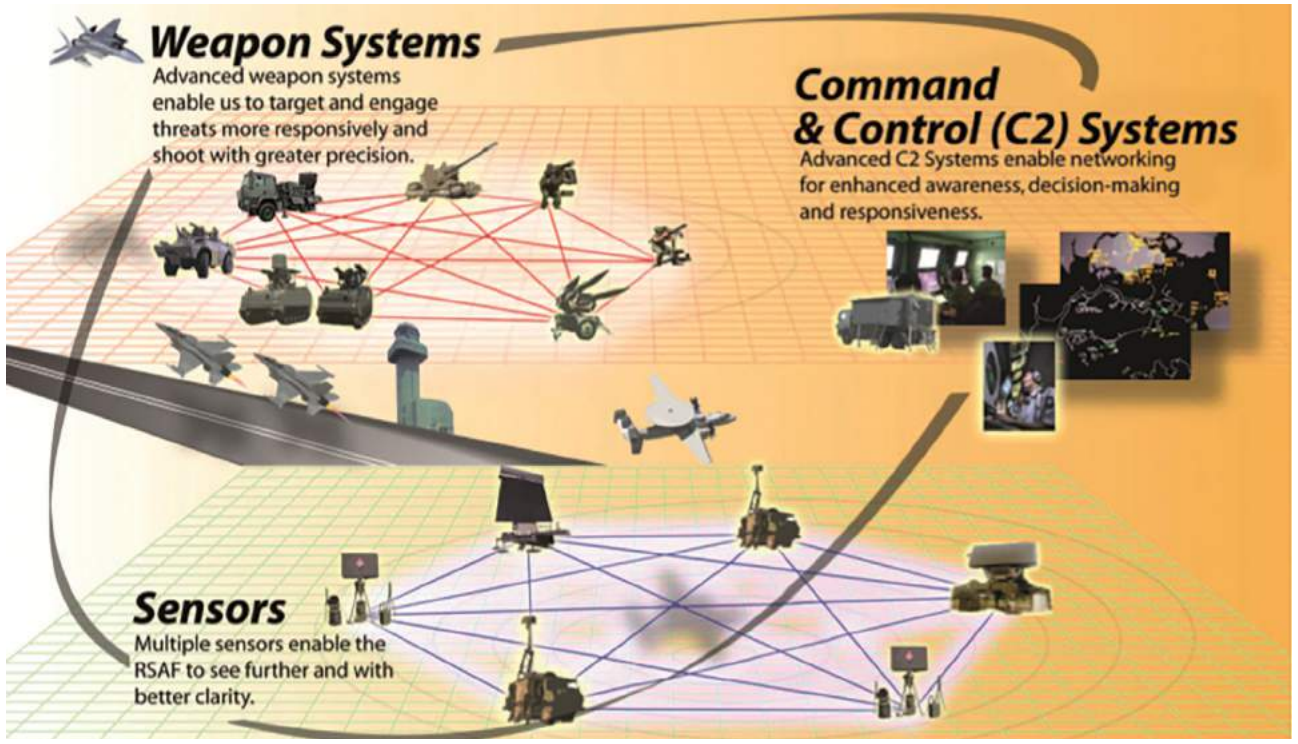

Weapon Systems
Advanced weapon systems enable us to target and engage threats more responsively and shoot with greater precision.
Command & Control (C2) Systems
Advanced C2 Systems enable networking for enhanced awareness, decision-making and responsiveness.
Sensors
Multiple sensors enable the RSAF to see further and with better clarity.

Illustration of the RSAF's Networked Air Defence

In terms of methodology, interactions of the systems were viewed as a network with multiple nodes and links. Performance was measured in terms of the ability to pass through from the source to the sink node without encountering any interruptions from any broken links or nodes. Such breakage could be a result of individual system failures, threat scenarios or each system's unique logistical factors.

Due to the different capabilities of the sensors and shooters in terms of range and threat types, no single mission Ao could be defined. Instead, a matrix of MOEs based on the threat and campaign type was used. For example, against threat X, availability was measured from Sensor A or B to Shooter I or II. ODIN enabled the mission readiness of Networked Air Defence to be evaluated in totality despite the independent management of individual systems. This ensured robustness in networked system architecture design with respect to connectivity between the component systems. This was achieved through the quantification and identification of weak links and/or vulnerabilities which enabled the optimisation of the Networked Air Defence Ao through improved connectivity configuration and incorporation of system redundancy.

Case Study 2: Networked System Resource Optimisation

A C4 system consists of many component systems connected together in a functional relationship. Typically, Ao is measured and resources are catered for at a system or node level. However, it does not provide a commander with a sense of the state of mission readiness. Hence, this study aimed to evaluate end-to-end network Ao from division to brigade level by piecing together the radios, phones, Command Control Information System to trunk communication equipment. ODIN provided the means to quantify the network Ao down to data versus voice. Such an approach ensured that the spares deployment from different equipment was well balanced with respect to end-to-end availability.

Optimising end-to-end Ao requires trade-off across multiple factors. For network architecture, it involves deciding between the number of radio links and the number of radio redundancies available for each system node. There is also trade-off among the various system configurations as well as the logistics input of spares deployment and support to determine the response to system and network downtime.

With ODIN, the modelling approach takes a step back to look at the fundamental functional level. Instead of the physical series-parallel reliability block diagram modelling, functional routing within and across the systems are modelled so that the system configuration design and differentiation between the voice (V) and data (D) routes can be captured accurately. The following figure shows the different possible routing paths to reach end-to-end between the voice-to-voice and data-to-data system nodes.

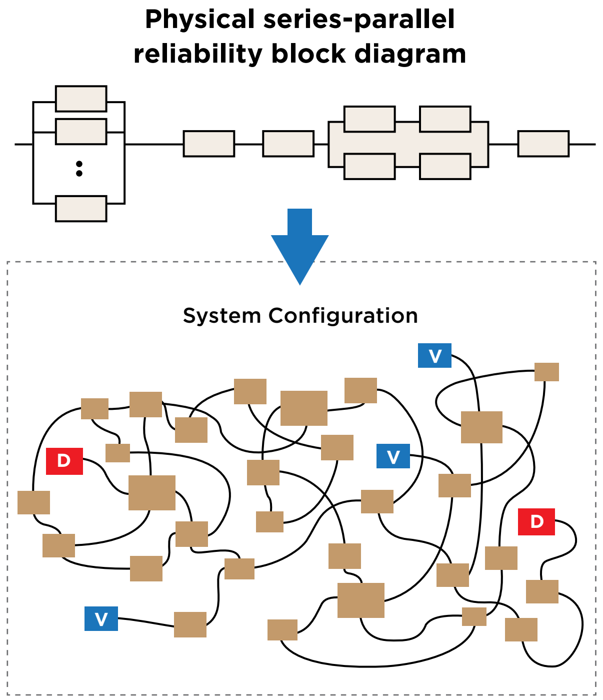


Illustration of physical series-parallel reliability block diagram modelling versus functional network routes modelling

Through such detailed modelling, overall end-to-end network Ao can be optimised globally across various factors including increased client redundancy, improved response time in spares support, review of system configuration design to achieve spares optimisation across systems, as well as operations and logistics at the network level. It involves the levelling of resources across the different component system nodes such as providing identified bottlenecks with higher resources.

System Safety In Guided Weapons and Armament

In the field of guided weapons and armament, System Safety is particularly important due to the potentially destructive consequences of malfunction or system failures e.g. severe or irreparable equipment damage, serious injuries, permanent disabilities and even fatalities. Basic safety considerations within a defined system may not be adequate for the increasing system-to-system integration. Further thinking at an SoS level is required to provide safety analyses outside the set of stand-alone system boundaries. When applied at the development or acquisition phase, System Safety is most effective and has a high potential of influencing design – this aids in the incorporation of the necessary safety features.

There are many areas that require System Safety measures and these include human-machine interface and software implementation. Thus, a multi-disciplinary approach is required. A System Safety Working Group is also needed to assist the project management team to brainstorm all possible hazards. Taking reference from the governing standards and guidelines, safety measures are implemented to eliminate or mitigate the hazards. In considering complex systems such as air platforms or guided weapon systems, the number of hazards can sometimes be in the range of hundreds. Thus, rigorous consideration and mitigation of all possible hazards are required to make the system as safe as possible. Through these thinking processes, the potential for all hazards is mitigated to "as low as reasonably practicable".

Residual risks refer to risks which cannot be reduced further as they are often inherent in the activity itself. As part of risk management, these residual risks and mitigation measures need to be communicated clearly to the end users for their acceptance. The case of a car travelling above the speed limit can be taken as an example. The driver is aware that he is exceeding the speed limit and acknowledges the consequences of being caught by a traffic camera or getting into an accident. He decides that speeding is necessary to reach the destination on time and accepts the risks of speeding. As a risk mitigation measure, he may install tyres with enhanced road-holding capabilities and check his car's braking effectiveness regularly. The concept of risk quantification and communication of residual risks to the end user for acceptance as part of the System Safety process emphasises the importance of enforcing mitigation measures on the ground.

System Safety in Development – Hand Grenade Throwing Bay

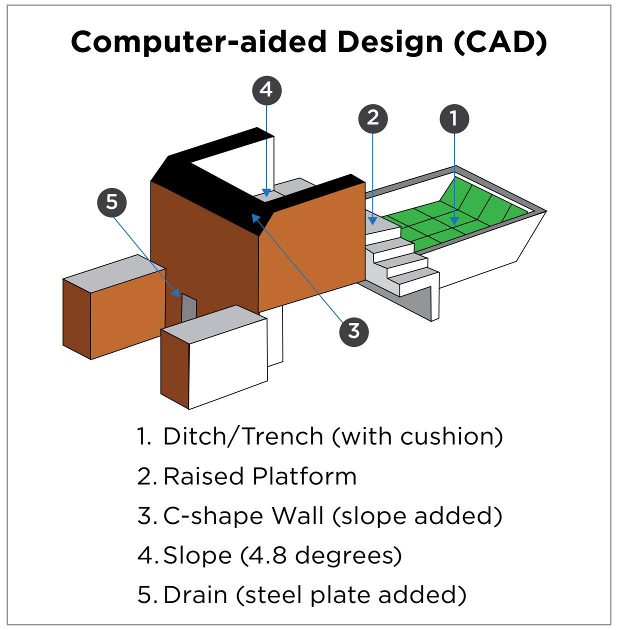
The redesigning of the Hand Grenade Throwing Bay is a good illustration. The project was an early test bed for DSTA's System Safety framework. Safety measures for the throwing bay were deliberated at a safety review workshop as the members were familiar with the facility and could contribute to the hazard analysis during the workshop. The end product is very similar to the Grenade Range in Pulau Tekong today, which is used by SAF recruits during the hand grenade throwing exercise as a rite of passage in National Service.

There were existing design guidelines for grenade throwing bays but they did not meet the training requirements of the SAF. The earlier version of the throwing bay was built as a short U-shaped wall to serve as a shield from grenade fragments that could be projected towards the thrower. If a grenade were to land behind or in the bay, both the thrower and the safety officer have to take cover on the other side of the wall. They have to run and climb over the wall in a short time frame of four and a half seconds. However, this reaction time is possible only if the thrower is an experienced soldier.

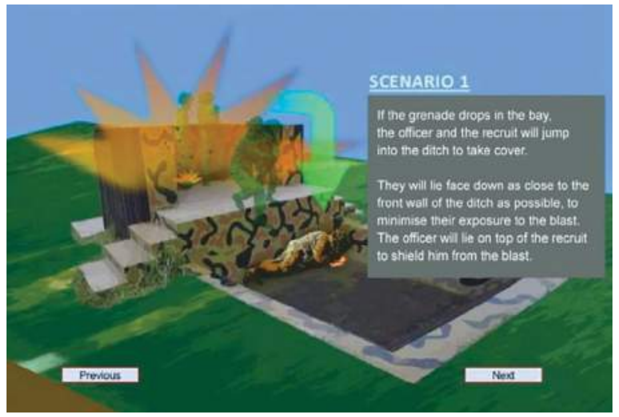
For most recruits, having only completed two months of Basic Military Training, this would remain a challenge despite the numerous drills they had with dummy grenades. Should a live grenade drop accidentally in the throwing bay or behind it, the recruits may not react fast enough to escape from danger. Therefore, the design had to be focused on incorporating safety features that offered greater physical protection. A System Safety approach was adopted at the stage of conceptualising the design.

From the brainstorming session during the workshop, a new design was developed. With this design, if a grenade lands in the bay, both the thrower and safety officer would jump into a ditch. If the grenade lands in the ditch, both of them should stay in the grenade bay, using the raised platform as a shield from the blast. There is no longer a need to run or climb to safety, reducing the physical demands on inexperienced recruits.

The effectiveness of the redesigned Hand Grenade Throwing Bay was unexpectedly demonstrated on the morning of 8 March 2008. Second-Lieutenant (2LT) Kok Khew Fai was the safety officer at one of the four grenade throwing bays at Pulau Tekong Hand Grenade Range. Upon command, a recruit armed the grenade, pulled out the safety pin and held on to the arming lever. He then released the arming lever and swung back his right arm to lob the grenade overhead. However, the grenade slipped from his hand and landed four metres behind them.


Computer-aided Design (CAD)
4
2
1
5
3
1. Ditch/Trench (with cushion)
2. Raised Platform
3. C-shape Wall (slope added)
4. Slope (4.8 degrees)
5. Drain (steel plate added)

An engineering drawing of the bay design showing the design features implemented after the identification of possible hazards. The features protect the personnel if the IA drills are executed correctly

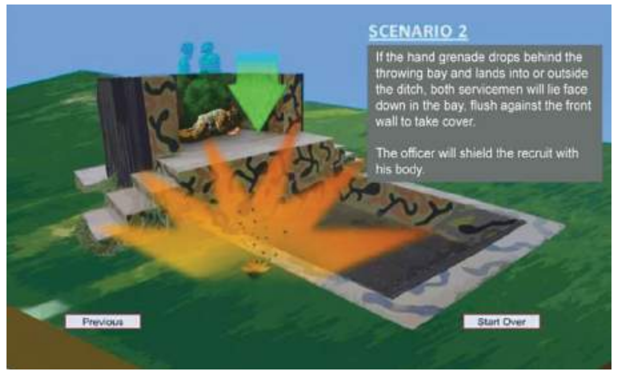


SCENARIO 1

If the grenade drops in the bay, the officer and the recruit will jump into the ditch to take cover.

They will lie face down as close to the front wall of the ditch as possible, to minimise their exposure to the blast. The officer will lie on top of the recruit to shield him from the blast.

Scenario where the grenade drops in the bay



SCENARIO 2

If the hand grenade drops behind the throwing bay and lands into or outside the ditch, both servicemen will lie face down in the bay, flush against the front wall to take cover.

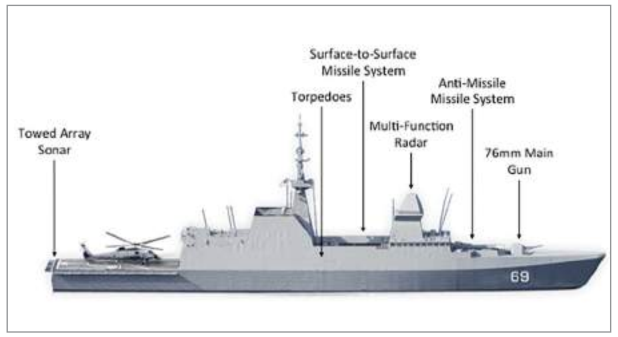
The officer will shield the recruit with his body.

Scenario where the grenade drops behind the throwing bay

Within seconds, 2LT Kok pulled the recruit down and shielded the recruit from the impending blast. The grenade exploded in four and a half seconds. When the fragments finally settled, both the recruit and 2LT Kok emerged from this harrowing experience safely. For 2LT Kok's bravery, he was awarded the SAF Medal for Distinguished Act or Pingat Jasa Perwira (Tentera). This incident proved the effectiveness of the grenade throwing bay which was designed and conceptualised through the use of the System Safety methodology.

System Safety in SoS Integration – Frigate Air Defence Suite

The integration of the Aster Anti-Missile Missile (AMM) system with the RSN Formidable-class frigates is an early example of DSTA's application of System Safety at the SoS level. The traditional approach of applying the methodology with focus on the weapon system was no longer sufficient because the Aster AMM system functions as part of the larger Anti-Air Warfare defence suite (or AAW suite). The behaviour of the other systems in the suite, such as the Multi-function Radar, Combat Management System and Navigation Distribution System have downstream effects on the operation of the Aster AMM system. As a result of complex interactions among systems, most cases of emergent behaviour are not immediately obvious and have to be identified and managed for safe operations.



Combat systems on the RSN Formidable-class Frigate

To address the safety concerns and potential hazards, a System Safety approach at the suite level was applied from the design stage by a team comprising subject matter experts of various systems in the suite. In addition to the comprehensive safety assessment performed on the Aster AMM system, a top-level safety analysis on the functional flow of the suite was performed during the development phase. Several hazards were identified and all associated software and hardware functions, or modes leading to these hazards, were analysed.

Following the analysis, several safety related gaps in the functional flow were discovered. Design changes were implemented to eliminate these gaps. In addition, safety-critical functions at the suite level were identified systematically using the Hazard and Fault Tree Analysis methodology. These functions were code-checked, peer-reviewed, closely tracked and verified in greater depth to prevent uncontrolled changes. As part of the verification, safety testing was conducted at the software unit, system and suite levels. Risks that could not be entirely mitigated by design were highlighted as residual risks for acceptance, and appropriate recommendations were provided to the users to further reduce the risk to as low as reasonably possible. The RSN has successfully conducted two Aster live-firings which validated the AAW suite.

An Innovative Application of System Safety Methodology

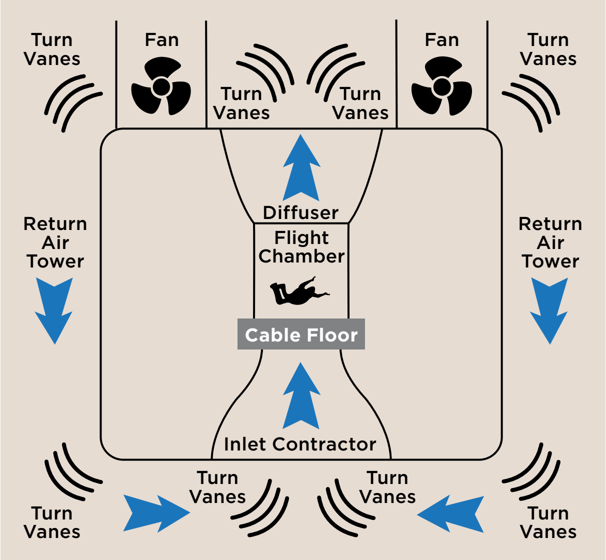
Introduction

System safety uses a risk management strategy based on the identification and analysis of hazards, as well as the application of mitigation controls through a systems-based approach. For the military, system safety practice is guided by the MIL-STD-882D US Department of Defense Standard Practice: System Safety.

DSTA PMT leveraged the system safety process in the Ministry of Defence Life Cycle Management, to influence the safety assurance for a proprietary commercial facility which has been tapped for military training. In addition, the article presents various challenges faced by the PMT and the relevant strategies adopted in response. The Goal Structuring Notation was an effective tool used to present the safety argument.

Vertical Wind Tunnel

The Vertical Wind Tunnel (VWT) combines a series of fans, ducts and vanes to produce a vertical laminar stream of air by recirculating wind energy. This recirculating laminar airflow provides stable lift to the personnel within the flight chamber, simulating a free fall. While "flying" in the flight chamber, the flyer can execute various flight manoeuvring techniques.



Layout of a typical VWT

Training in the controlled environment of VWT facility brings along numerous benefits, such as minimised risks of mishaps as compared to going for live jumps at high altitudes. Live jumps are inherently hazardous with incidents including parachute malfunction and sudden inclement weather. With risks minimised, personnel can develop confidence and fine-tune their free falling technique in a controlled and safe environment to complement live jumps. The mishap severity associated with "flying" in the VWT is reduced significantly as compared to an actual skydive.

Utilising a VWT also reduces substantial cost and time for the SAF. An actual jump would incur the high cost of using an aircraft. Furthermore, there is only a short window of opportunity for each jump due to the need for the aircraft to take off, transit to the drop zone and then land. In the case of the VWT, the free faller could make use of extended time blocks in the VWT to perfect his techniques without the need to get on board an aircraft repeatedly for each free fall. This allows the SAF to manage training slots effectively and efficiently, shortening the learning curve for novices and maintaining currency of their skills.

The VWT was designed originally for public use. Members of the public using the VWT would only need to put on a jumpsuit and helmet. Military personnel, however, are required to carry additional equipment and accessories, which may affect their safety and the performance of the VWT.

As the VWT is a proprietary licensed commercial facility, the DSTA PMT had limited influence on its design aspects. Furthermore, information about the design was limited due to intellectual property protection. Thus, innovative approaches were used to secure the required safety assurances for our military free fallers while ensuring that members of the public could continue enjoying the facility as before.

Challenges

The VWT was the first of its kind to be built in Singapore, and the PMT had no prior experience in the acquisition management of such systems. In addition, the contractor operates a franchise licence from Sky Venture International (SVI) which builds, operates, and maintains 32 VWTs around the world. This franchise licence meant that the scope of the system safety analysis was not easy to define. The proprietary and closed nature of the system's design restricted the release of detailed information about the system.

The PMT brainstormed and developed various ways of overcoming the problem of limited available information. One of the possible solutions was to examine existing reports and compliances which could be used as a basis to justify the belief that the use of the VWT was inherently safe for the SAF. Employing this idea, the PMT rationalised that the proof of compliance to local legislative licensing requirement and the contractor's commissioning certificates could form a basis for safety assurance. This primary approach was documented (see section on Innovative Application of System Safety Activities).

The contractor responsible for the operation and maintenance of the VWT was Sky Venture Singapore (SVS) which is a franchisee of SVI. With SVI's extensive experience in international operations and its excellent track record in safety, one could be reasonably confident that the VWT was safe and met all commercially required levels of safety. The proven facility design, well-written safety manuals, as well as the safety operational procedures and checklists were part of a programme to ensure that daily operations would be safe.

Nevertheless, the need for military equipment and free fall techniques in the VWT warranted additional safeguards to enhance safety. System safety was used to value add to the existing safety systems, through the methodical discovery of atypical hazards which are faced by military free fallers but not the general public. These hazards were documented in the Preliminary Hazard List (PHL) which is discussed in the following section.

Innovative Application of System Safety Activities

One of the key challenges to the programme was to determine how to provide primary safety assurance to the military users without compromising proprietary information, given that the system was unique and proprietary to SVI.

Before the VWT could be open for public entertainment, it had to comply with legislative requirements whereby the service provider had to provide evidence to show that the VWT was safe for public use. Leveraging this need for compliance to legislative requirements, the PMT obtained the same information from SVI to assess the VWT for military free falls. The legislative approvals and certifications are summarised as follows:

- *Legislative Requirement: Public Entertainment Licence and Conformity Assessment Body Certification.* Under Singapore's Public Entertainments and Meetings Act, entertainment that is provided at any place accessible by the public requires a Public Entertainment Licence from the Singapore Police Force. To obtain this licence, the attraction has to be certified by a competent body, which is the Conformity Assessment Body, as having met relevant technical and safety standards. SVS thus had to obtain the Public Entertainment Licence prior to commencement of operations.
- *Legislative Requirement: Certificate of Statutory Completion and Fire Safety Certificate.* SVS hired Registered Inspectors who specialise in the architectural, mechanical and electrical aspects of safety to certify the building and fire safety works. SVS also appointed personnel as Qualified Persons, who had to submit all documents related to fire safety works to the Registered Inspector to perform the safety assessment. When the details of the assessment were submitted and found to be satisfactory by the Singapore Civil Defence Force and the Building Construction Authority, the Certificate of Statutory Completion and Fire Safety Certificate were issued.
- *Applicable Certification: Original Equipment Manufacturer Commissioning Certificate.* During the final stages of constructing the VWT, SVI provided technical support to test and commission the VWT. This ensured the correct installation and safety of the VWT. Upon completion, SVI issued a commissioning certificate to SVS, validating the functional and safety aspects of the VWT.
- *Applicable Certification: SVS Instructors Certification.* SVS instructors are trained personnel who ensure the safety of flyers in the wind tunnel. In the event of an emergency situation, the instructor's ability to prevent injuries to the flyer is crucial. SVS consistently keeps its instructors current by following a stringent set of requirements laid out by the International Bodyflight Association (IBA). IBA certifications issued to SVS instructors and tunnel operators are submitted to the SAF for periodic reviews.

With these proof and certifications of compliance with legislative requirements, the PMT could use them as evidence for the system safety assessment within MINDEF. This approach is unique and different from the acquisition of weapons-related systems and platforms, where system safety techniques such as Fault-Tree Analysis and Functional Hazard Analysis are typically used as the means of providing safety assurance.

The PMT, SVS and the SAF worked collaboratively to apply the System Safety methodology and techniques for the VWT to enhance the existing safety documentation. One area of collaboration was the development of a PHL, which was the first step in the System Safety process to identify potential hazards associated with the use of this system. To identify these hazards, the PMT needed a certain level of background information and engineering details which could not be revealed due to SVI's intellectual property rights.

The PMT adopted a three-pronged approach to develop this PHL:

First, dialogue sessions were conducted with SVS and SVI to extract potential hazards based on their experience in operating other VWTs. By analysing the safety features of the VWT, the PMT was able to retrospectively visualise the hazards that the safety features might be trying to protect against. Once the PMT had an idea of the possible hazards, it deliberated if such hazards could develop into other forms of hazards based on the unique utilisation of the VWT by the SAF.

Second, dialogue sessions were held with members of the SAF who are experienced skydivers or instructors to gather potential operational and training hazards. These dialogue sessions provided valuable information so that the PMT could sieve out credible hazards from the PHL.

Third, the PMT visited VWTs overseas to get a first-hand account of the safety features and issues relating to the use of such a system. While some hazards were universal, the PHL helped to identify hazards that were associated with the unique military applications of the VWT. The table below shows some of these hazards and the relevant mitigation measures.

The ability to identify hazards unique to military applications led to the incorporation of mitigation measures to reduce the mishap risk. For instance, a procedure was enforced to ensure that trainees do not exit the VWT from a flying position. With information on these hazards, the SAF Commanders are able to make a better informed decision to manage their training requirements effectively and safely. The identification of the atypical hazards highlighted that system safety complements the existing safety management systems of SVS.

S/N	Hazard Description	Casual Factors	Mitigation Measures
1.	Military equipment falls off flyer	Failure of equipment securing mechanism	Introduce a locking mechanism (capable of withstanding gravitational forces) to allow the flyer to strap and hook military equipment close to his body
2.	Flyer carrying military loads attempts to exit VWT from a flying position, impacting the exit	Unstable lying position due to added equipment bulk	• Introduce a soft cushioning at the exit-cum-entrance of the flight chamber • Enforce the rule that military flyers with equipment shall exit only from a standing position
3.	Kinetic energy of recirculating objects	Presence of loose objects (shoes, gloves, goggles, etc.)	• Use existing features such as the plenum, turn vanes and cable floors to impede flying objects from recirculating in the VWT • Conduct more frequent checks at points where loose objects are collected, to eliminate potential recirculation of such objects

PHL

Goal Structuring Notation (GSN) is a graphical argumentation notation used to explicitly document the elements of any argument. It originated from the University of York in the early 1990s, but it was only formally recognised in November 2011 as a tool to improve the structure, rigour and clarity of safety arguments during the presentation of safety cases.

For this VWT programme, GSN was used initially to define the challenges at hand and to list the possible solutions to these challenges. Subsequently, it was also used as a representation tool to present a top level view of how the VWT was at an acceptable level of safety for use. These functions of the GSN facilitated easier understanding of the safety issues. Thus, the PMT used the tool for an effective presentation of safety cases to members of the safety boards.

When the elements of GSN are connected together, a goal structure is formed. Goal structures document the chain of reasoning in the argument with the relevant substantiating evidence. The principal purpose of a goal structure is to show how goals are broken down successively into sub-goals, until a stage where claims can be supported by direct reference to available evidence.

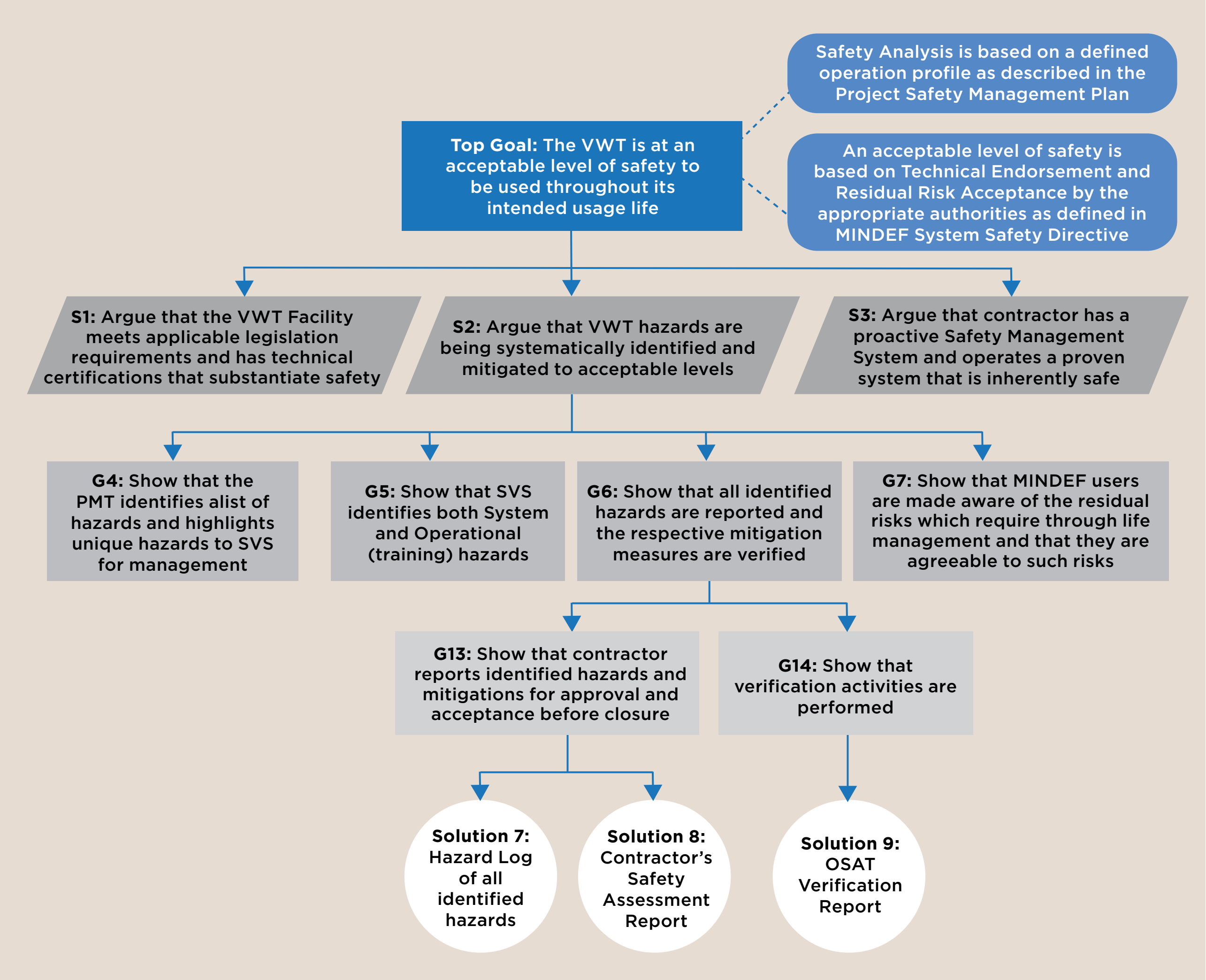
The defined top goal for the GSN of the project was: “The VWT is at an acceptable level of safety for use throughout its intended usage life”. The GSN has two contextual entries displayed on its right, which are important to capture the context for interpreting the top goal.

The top goal is further expanded into three separate strategy blocks namely S1, S2 and S3. Each strategy block is a reasoning step which interfaces between the top goal and the sub-goals. The descriptions in S1, S2, and S3 support the top goal. This GSN continues to be developed until sufficient evidence is found to substantiate the top goal. The evidence collected is represented by solution blocks. For instance, solution 9 “OSAT (or ‘On-Site Acceptance Test’) Verification Report” is the evidence that G14 “Show that Verification activities are performed” has been achieved.

When reading the GSN tree, the reader is guided through the assurance argument in a structured manner. This provides a bird's eye view of the safety argument, which can enable someone without any prior system knowledge to review the argument.

GOAL	A goal, rendered as a rectangle, presents a claim forming part of the argument.
STRATEGY	A strategy, rendered as a parallelogram, describes the nature of the inference that exists between one or more goals and another goal.
CONTEXT	A context, rendered as a rectangle with rounded corners, presents a contextual artefact. This can be a reference to contextual information or a statement.
SOLUTION	A solution, rendered as a circle, presents a reference to evidence.

Basic symbols of GSN


Safety Analysis is based on a defined operation profile as described in the Project Safety Management Plan
Top Goal: The VWT is at an acceptable level of safety to be used throughout its intended usage life
An acceptable level of safety is based on Technical Endorsement and Residual Risk Acceptance by the appropriate authorities as defined in MINDEF System Safety Directive
S1: Argue that the VWT Facility meets applicable legislation requirements and has technical certifications that substantiate safety
S2: Argue that VWT hazards are being systematically identified and mitigated to acceptable levels
S3: Argue that contractor has a proactive Safety Management System and operates a proven system that is inherently safe
G4: Show that the PMT identifies alist of hazards and highlights unique hazards to SVS for management
G5: Show that SVS identifies both System and Operational (training) hazards
G6: Show that all identified hazards are reported and the respective mitigation measures are verified
G7: Show that MINDEF users are made aware of the residual risks which require through life management and that they are agreeable to such risks
G13: Show that contractor reports identified hazards and mitigations for approval and acceptance before closure
G14: Show that verification activities are performed
Solution 7: Hazard Log of all identified hazards
Solution 8: Contractor's Safety Assessment Report
Solution 9: OSAT Verification Report

A portion of the GSN diagram used for the VWT programme

Conclusion

System safety is typically applied for the acquisition of weapons-related systems and platform-type defence capabilities, taking reference from the Military Standard: MIL-STD-882D (2000). Hence, applying the system safety requirements from MIL-STD-882D to a commercial programme posed several challenges which called for innovative approaches.

Applying system safety to this unique programme benefitted all parties. First, MINDEF and the SAF acceptance authorities were equipped with information on the unique hazards of using VWT in a military context – thus they were able to decide on how to use it appropriately in SAF's training. Second, system safety helped to ensure a safe, realistic, reliable and cost-effective training environment for the SAF. Third, the PMT was exposed to new tools and methodologies through its collaboration with a commercial service provider, gaining knowledge that can be applied to similar programmes in the future. Finally, SVS enhanced its competency in applying a risk-based process and it could adapt similar techniques to meet local legislative requirements of the Workplace Safety and Health Act.

References:

Wymore, A. W. (1993). *Model-based systems engineering.* Boca Raton, Florida: CRC Press.

Thio, S. J., Kong, S. T., Tan, S. F., & Yeo, L. C. (2006). JEWEL: M&S environment for the SAF. *Proceedings of the Inter-service/Industry Training, Simulation, and Education Conference.* Arlington, Virginia: National Training and Simulation Association.

Beach, T. & Dryer, D. (2007). Application of design of experiments and data farming techniques for planning tests in a joint mission environment. *Proceedings of the International Data Farming Workshop 15.*

Ericson, C. W. (2005). *Hazard analysis techniques for system safety.* Hoboken, New Jersey: John Wiley & Sons. doi: 10.1002/0471739421.

Kelly, T. P. (1998). *Arguing safety: A systematic approach to managing safety cases.* Retrieved from the University of York, Department of Computer Science website: https://www-users.cs.york.ac.uk/tpk/tpkthesis.pdf

Kelly, T. P., & Weaver, R. (2004). *The goal structuring notation: A safety argument notation.* Retrieved from the University of York, Department of Computer Science website: https://www-users.cs.york.ac.uk/tpk/dsn2004.pdf

ACKNOWLEDGEMENTS

Engineering Systems-of-Systems would not have been possible without the hard work, support and encouragement of many people. General thanks are also due to the teams at DSO National Laboratories, MINDEF Communications Organisation, MINDEF Centre for Heritage Services, Air Force Information Centre, Defence Industry and Systems Office, Defence Science and Technology Agency, and many others – too numerous to name – who have assisted us in one way or another, in the production of this book.

Authors

Ms Chang Chai Fung joined the DTC in 1985 as an engineer in DSO. She was the Programme Manager for the AC2H project, which received the Defence Technology Prize in 2002. Since 2006, she has worked on various areas related to Enterprise Architecting and Governance, Masterplanning and Systems Architecting in DSTA, and is currently Head Business Process Management, MINDEF.

Mr Chia Ban Seng joined the DTC in 1999 as an operations analyst in DMO. Since 2000, he has worked on various projects in the areas of operations research, system-of-systems, systems architectures, masterplanning, training and simulation, and design innovation in DSTA. He is currently Head (OR – Methodology) in DSTA.

Mr Chung Wai Kong received his Bachelor of Engineering (Honours) degree from Nanyang Technological University in 1997. He further obtained a Master of Science in Computer Science from NPS in 2005. He is the Head of Capability Development (CMS Development) in DSTA, where he oversees the capability development of Combat Management Systems (CMS) for the SAF. He has successfully led teams to deliver CMS capability to the RSN, including the Frigate CMS and the upgraded MCV CMS.

Mr Frank Teo Yong Khiang joined DSO in 1982 and served in DMO for six years before returning to DSO National Laboratories. In the 1990s, he led the establishment and certification of both organisations' ISO 9001 Quality Management System. In the 2000s, he headed the Systems Engineering Centre in DSO National Laboratories to strengthen the mechanical design, electronics prototyping, quality, reliability, maintainability, logistics and system safety capabilities. During this period, he also served as Senior Assessor for the national Business Excellence Scheme. Since 2010, he has been the Assistant Director overseeing the training of programme managers and systems engineers in DSO National Laboratories.

Mr Leow Aik Siang graduated from NUS with a First Class Honours Degree in Computer Science. He also holds a Masters in Management of Technology from Georgia Institute of Technology. He has also held appointments as Head Engineering in Enterprise IT, Head Capability Development for Knowledge Management and Deputy CIO in the DSTA CIO Office. He is the current Director (Enterprise IT) in DSTA and is leading the acquisition, implementation and sustenance of Corporate IT capabilities for MINDEF and the SAF spanning across logistics, human resource, NS administration and knowledge management. He is also involved in driving new capabilities in the areas of mobility, analytics, and internet-of-things.

Professor Lui Pao Chuen graduated from Singapore University in 1965 with a degree in Physics. In 1966 he enlisted in the SAF on a Short Service Commission and served as Officer-In-Charge in the Test, Evaluation and Acceptance Section, Logistics Division, Ministry of Interior and Defence. He retired from the SAF in 1986 and continued to serve MINDEF as Chief Defence Scientist. He retired from MINDEF in 2008 and is currently advisor to the National Research Foundation, Prime Minister's Office, six Ministries and Government Agencies, and to President of NUS and President of NTU. He also serves on the board of 12 research institutes and corporations and is a member of the Board of Trustees of Singapore University of Technology and Design and the Scout Council of Singapore.

Professor Quek Tong Boon is currently Advisor to DSO National Laboratories and Chief Executive of the National Robotics Programme. He was the Chief Defence Scientist in MINDEF from 2008 until 30th June 2016. He graduated from the University of Cambridge in 1977 with a Bachelor of Arts (Honours) in Engineering and Master of Arts in Engineering in 1981. In 1985, he obtained his Master of Science in Electrical Engineering from NUS. After completing his full-time NS in 1980, he joined DSO. From June 1994 to December 1997 he was the Director of DMO before becoming CEO of DSO National Laboratories from January 1998 to January 2004. He has contributed to the build-up of various capabilities in the defence technology ecosystem over the years, including those related to guided weapons, unmanned systems, microsatellites, chemical-biological defence and systems engineering. He was the leader of the DSO project that won the inaugural Defence Technology Prize (Team) in 1989. He also established various research laboratories and centres in the academia, such as iTrust at the Singapore University of Technology and Design, and Temasek Laboratories and the Singapore Institute for Neurotechnology at NUS.

In over three decades of service in MINDEF, RADM (Ret) Richard Lim has had roles in all phases of the systems development life cycle of large-scale defence systems. He has held the positions of Deputy Secretary (Technology), Chief Executive DSTA, Chief of Navy, and Director Joint Operations and Planning. He continues his professional interest in systems engineering, and serves in advisory and board positions in both the private and public sectors. He is Chairman of ST Logistics, a board member of ST Marine and the National University Health System, and Deputy Chairman of Land Transport Authority. He is also Chairman of the governing board of St. John's Island Marine Laboratory and Chairman of the National Maritime Safety at Sea Council.

Mr Tan Yang How, a Radar Systems Engineer and DSTA Systems Architect, has served in numerous positions in MINDEF and DSTA. He was Director (Naval Systems) and Director (DMSA) before being appointed Founding President of DSTA Academy in April 2012 to steer the organisation's Systems Engineering and Programme Management Training. During the 2003 SARS crisis, he led the invention and wide-scale operationalisation of the Infrared Fever Screening System in Singapore. The innovative work gained much recognition, earning several accolades and awards including the USA Tech Museum Award. He was the 1997 Defence Technology Prize Individual Award Recipient for his work in the radar domain, and was conferred Public Administration Medals in 2000 (Bronze) and 2003 (Silver).

Mr Teo Chee Wah joined the DTC in 1988. He graduated in France in 1986 under the Singapore Public Service Commission Scholarship with an Honours in Electrical Engineering. Subsequently, he was awarded the DSTA Postgraduate Scholarship in 1993 and graduated with a Master of Science in Telecommunication and Signal Processing from the Imperial College of Science, Technology and Medicine, University of London. In his tour of duties in the DTC, Chee Wah has assumed several significant appointments. Notably, in DSTA, he led the Sensors Systems Division, served as the Deputy Director of DMSA, as well as the Faculty Head in DSTA Academy. In MINDEF, he served as the Head of Defence Technology Office (Europe) in Paris, France, and Deputy Director (Industry), DISO. He is currently the Deputy Director (Sensors) in DSTA. Mr Teo was awarded the Public Administration Medal (Bronze) in 2009.

Mr Teo Koon Kiat began his career as a reliability engineer in DSO in 1986. Thereafter, he was posted to DMO to work on acquisition programmes in the areas of reliability and maintainability, quality assurance and logistics support analysis. From 2013 to 2016, he was seconded to DISO to oversee the build-up and sustainment of strategic capabilities in the local defence industry. He is currently a Senior Principal Engineer at DSTA.

Mr Teo Siow Hiang joined the DTC in 1983 as an engineer in DSO. He was then sent on overseas attachment to work on a defence project before returning to join DMO, and then to DSTA when it was formed in year 2000. Since joining DTC, he has worked in various areas in systems engineering, operations research, and systems architectures. These areas have spanned the capability domains of air (such as fighter aircraft), land (the Advanced Combat Man System), sea (the Formidable-class Frigate) and Joint (in intelligence, surveillance and reconnaissance). He is a Chartered Engineer (Systems Engineering) in the Institution of Engineers. He is also a member of the International Council on Systems Engineering, the Institute of Electrical and Electronics Engineers, and UK Operations Research Society. He has written, presented and published numerous papers in systems engineering and operations research. He is currently Assistant Director (Advanced Programmes) in DSTA.

Er. BG (Ret) Wesley D'aranjo obtained his degree in Electrical and Electronics Engineering (First Class Honours) from the University of Manchester Institute of Science and Technology in 1975. From 1975 to 1979, he served as an Air Engineering Officer at the ADRU, SADC. From 1979 to 1984 he was appointed Head Engineering Group of Project Management Team 2 and then Assistant Director 2 in the SPO. From 1984 to 1986, he served as Deputy Head Air Logistics (Electronics and Weapons) in the RSAF and concurrently Deputy Director (Radar and C2), SPO. From 1985 to 1987 Er. BG (Ret) D'aranjo was appointed Deputy Director (Lands and Armaments) in SPO. He was appointed Director of DMO from 1987 to 1991, and concurrently from 1987 to 1988, the Deputy Director (Weapons and Systems) at DSO, before being appointed Deputy Secretary (Technology) from 1991 to 1997. For his many contributions to the DTC over the years, he was awarded the Defence Technology Medal (Outstanding Service) in 2015.

Contributors

Mr Alagesan Kulanthaivelu
Dr How Khee Yin
Prof Lai Kim Fatt
Dr Loke Weng Keong
Mr Quek Gim Pew
Mr Seah Peng Leong
Dr Tan Boon Huan
Ms Tan Chong Shan
Mr Tay Yeow Koon
Mr Teo Tiat Leng
Mr Teo Yew Kheng
Mr William Lau Yue Khei

Editor

RADM (Ret) Richard Lim Cherng Yih

Editorial Support Team

Mr Chia Ban Seng
Mr Chiam Dasen
Ms Chua Seow Kie
Ms Pearly Chua Siew Ting
Mr Tan Huang Hong
Mr Tan Yang How

Sitting (left to right)
Mr Teo Tiat Leng, Prof Lai Kim Fatt, Ms Chang Chai Fung, RADM (Ret) Richard Lim Cherng Yih,
Mr William Lau Yue Khei, Dr Loke Weng Keong, Mr Quek Gim Pew, Dr Tan Boon Huan
Standing (left to right)
Er. BG (Ret) Wesley D'aranjo, Dr How Khee Yin,
Mr Alagesan Kulanthaivelu, Mr Tan Yang How, Prof Lui Pao Chuen, Mr Teo Koon Kiat,
Mr Teo Yew Kheng, Mr Chia Ban Seng
Not in picture
Mr Chung Wai Kong, Mr Frank Teo Yong Khiang, Mr Leow Aik Siang,
Prof Quek Tong Boon, Mr Seah Peng Leong, Ms Tan Chong Shan, Mr Tay Yeow Koon,
Mr Teo Chee Wah, Mr Teo Siow Hiang

Photo/Chart/Diagram Credit:

1. Defence Science and Technology Agency: Cover picture, pages 34-35, 37, 40*, 42*, 43, 63, 64, 65 (left), 72, 79-85, 89, 92 (right top and bottom), 93, 99, 102, 104, 105, 111, 113 (top), 115-116, 136, 138, 139, 141, 145, 146*, 147-148, 149 (bottom)*, 150-152, 154-156, 159-161, 163, 165, 167-173, 175, 177 (left top, middle and bottom), 178, 181-183
2. DSO National Laboratories: pages 111 (bottom), 114, 119, 120
3. Er. BG (Ret) Wesley D'aranjo: pages 4 (bottom), 5, 6, 12, 13 (bottom), 15 (top left and right), 18, 22 (top), 25 (left), 27, 28, 59
4. Ministry of Defence: pages 2 (top), 4 (top), 25 (middle), 30, 34, 36, 39, 46, 47, 65 (right top), 71, 74, 77 (top), 85, 92 (left), 99, 102, 124, 144, 149 (top), 164, 165, 172 (top), 174, 177 (right)
5. Mr Cameron Moll: page 76
6. Mr Richard Lim Cherng Yih: preface, page 122
7. Mr Tan Yang How: page 113 (bottom)
8. National Security Coordination Secretariat: page 111
9. Professor Lui Pao Chuen: pages 3, 9, 10, 13 (bottom), 22 (middle and bottom), 23
10. Republic of Singapore Air Force: page 2 (middle and bottom), 7, 13 (top), 15 (bottom), 16, 53, 65 (right bottom), 77 (bottom)
11. Republic of Singapore Navy: page 25 (right)
12. Singapore Army: page 60

* Schematic diagrams that include source photographs from MINDEF and the SAF.

GLOSSARY

Acronym	Description
A(FE)-VC-A(P)	Analysis (Front End)-Validity Check-Analysis (Post)
AA	Anti-aircraft
AAW	Anti-air warfare
ADRU	Air Defence Radar Uit
AEW	Airborne Early Warning
AHP	Analytic Hierarchy Process
AMM	Anti-missile missile
ARTHUR	Artillery Hunting Radar
ASEM	Advanced Systems Engineering and Management
ASO	Aviation Supply Office
ATE	Automatic Test Equipment
AvC	Availability Based Contracting
BPMS	Business Process Management System
BSEM	Basic Systems Engineering and Management
BSL	Biosafety Level
C2	Command and control
C2N	Command and control network
C4	Command, control, communications and computers
C4I	Command, control, communications, computers and intelligence
C4ISR	Command, control, communications, computers, intelligence, surveillance and reconnaissance
CAF	Chief of Air Force
CC	Competency Community
CDS	Chief Defence Scientist
CDSO	Chief Defence Scientist's Office
CII-SA	Critical Infocomm Infrastructure - Surety Assessment
CIP	Critical infrastructure protection
CIVA	Critical infrastructure vulnerability assessment
COE	Common Operating Environment
CONOPS	Concept of Operations
COTS	Commercial off-the-shelf
CSEP	Certified Systems Engineering Professional
CSO	Command, Control, Communications and Computer Systems Organisation
CSP	Common Situation Picture
C-T&T	Contact Track and Trace
DARPA	Defense Advanced Research Projects Agency
DCM	Defence Capability Management
DMO	Defene Materials Organisation
DMRI	Defence Medical Research Institute
DMSA	DSTA Masterplanning and Systems Architecting
DMSC	Defence Management and Systems Course
DPD	Defence Procurement Division
DRD	Directorate of Research and Development
DRTech	Defence Research and Technology Office
DS(T)	Deputy Secretary (Technology)

DSO	Defence Science Organisation
DSTA	Defence Science and Technology Agency
DTC	Defence Technology Community
DTE	Defence Technology Ecosystem
DTG	Defence Technology Group
EA	Enterprise Architecting
EADSIM	Extended Air Defense Simulation
EBA	Enterprise Business/Operational Architecture
EBM	Enhancing Business Model
EHI	Environmental Health Institute
EIA	Enterprise Information Architecture
EMP	Engineering Master Plan
ERD	Engineering Resource Deployment
ERP	Enterprise Resource Planning
ES	Enterprise System
ESA	Enterprise Solutions Architecture
ESP	Engineering and Scientific Personnel
ETA	Enterprise Technical Architecture
ETC	Electronics Test Centre
FCS	Future Combat Systems
FMS	Foreign Military Sales
FSB	Finance Systems Branch
FSD	Future Systems Directorate
FSTD	Future Systems and Technology Directorate
GBAD	Ground-based air defence
GeBIZ	Government Electronic Business
GES	Ground Entry Station
GIS	Genome Institute of Singapore
GOSPO	Government of Singapore Programme Office
GSN	Goal Structuring Notation
HADR	Humanitarian Assistance and Disaster Relief
HC	Human Capital
HE	Hazard Element
HR	Human Resources
HSC	Horizon Scanning Centre
IAD	Island Air Defence
IADS	Integrated Air Defence System
IAFU	Improved Assault Fire Unit
IBCM	Integrated Bridge-Combat Information Centre-Machinery Control Room
IBM	International Business Machines Corporation
ICIT	Installation, Checkout, Integration and Testing
IDA	Infocomm Development Authority
IES	Institution of Engineers Singapore
IFF	Identification Friend or Foe
IFss	Infrared Fever Screening System
IFV	Infantry fighting vehicle
IG	Image Generator
IKC2	Integrated Knowledge-based Command and Control

ILS	Integrated Logistics Support
IM	Initiating Mechanism
INCOSE	International Council on Systems Engineering
IPMT	Integrated Project Management Team
IRS	Interface Requirements Specifications
ISEM	Intermediate Systems Engineering and Management
IT	Information Technology
JATCC	Joint Air Traffic Control Centre
JCATS	Joint Conflict and Tactical Simulation
JEWEL	Joint Modelling and Simulation Environment for Wargaming and Experimentation Labs
JFAS	Joint Force Analysis Simulation
JTEM	Joint Test and Evaluation Methodology
LCC	Life Cycle Cost
LCM	Life Cycle Management
LEO	Lands and Estates Organisation
LISA	Large-Scale Integrated Search and Analysis
LMIS	Logistics Management Information System
LOA	Letter of Offer and Acceptance
LPC	Logistics Planning Conference
LSA	Logistics Support Analysis
LSB	Logistics Systems Branch
LSMP	Logistics Support Management Plan
LST	Landing Ship Tank
M&S	Modelling and simulation
MANA	Map Aware Non-uniform Automata
MBSE	Model-based Systems Engineering
MCMV	Mine Countermeasure Vessel
MCV	Missile Corvette
MDA	Model-Driven Architecture
MDES	Military Domain Expert Scheme
MHA	Ministry of Home Affairs
MIAFU	Modified Improved Assault Fire Unit
MICOM	US Army Missile Command
MINDEF	Ministry of Defence
MMO	Materials Management Organisation
MOCC	Mobile operations control centre
MOE	Measure of Effectiveness
MOH	Ministry of Health
MOP	Measure of Performance
MOU	Memorandum of Understanding
MPA	Maritime Port Authority
MRO	Maintenance, repair, and overhaul
MRT	Mass Rapid Transit
MSA	Modelling Simulation and Analysis
MTBCF	Mean Time Between Critical Failure
MTBF	Mean Time Between Failure
M-T-M	Model-Test-Model

MTTR	Mean Time To Repair
NAVAIR	United States Navy Naval Air Systems Command
NDP	National Day Parade
NFRP	Next Fighter Replacement Programme
NPS	Naval Postgraduate School
NSCS	National Security Coordination Secretariat
NSF	Full-time National Serviceman
NSmen	National Servicemen
NTU	Nanyang Technological University
NUS	National University of Singapore
O&S	Operations and Support
OA	Operations Analysis
OAB	Operations Analysis Branch
OCD	Organisation Capability Development
OCF	Operational Concept Formulation
ODIN	Optimised Decisions in Networks
OEM	Original equipment manufacturer
OME	Ordnance, munitions and explosives
OMP	Operational Master Plan
OODA	Observe, orient, decide, act
OPCW	Organisation for the Prohibition of Chemical Weapons
OPUS	Optimisation of Units as Spares
OR	Operations research
ORBAT	Order of Battle
OSAT	On-Site Acceptance Test
OTE	Operational Test and Evaluation
OTS	Off-the-shelf
OV	Operational View
PBL	Performance Based Logistics
PC	Personal computer
PCG	Police Coast Guard
PD	Project division
PHL	Preliminary Hazard List
PIT	Preliminary Integration Test
Pk	Probability of Kill
PLC	Product life cycle
PMT	Project Management Team
PV	Patrol Vessel
QA	Quality Assurance
QAD	Quality Assurance Department
QSM	Quantitative selection methodology
R&D	Research and Development
R&M	Reliability and Maintainability
R&T	Research and Technology
RAAF	Royal Australian Air Force
RAF	Royal Air Force
RAHS	Risk Assessment and Horizon Scanning
RAM	Reliability, availability, and maintainability
RDPS	Radar Data Processing Subsystem
REC	RAHS Experimentation Centre
RFID	Radiofrequency identification
RFN	Robotförsöksplats Norr
RGT	Reliability growth testing
RMAF	Royal Malaysian Air Force
RMS	Reliability, Maintainability, Supportability
RSAF	Republic of Singapore Air Force
RSN	Republic of Singapore Navy
RT	Reliability Technology
SA	Systems architecting
SADA	Singapore Air Defence Artillery
SADC	Singapore Air Defence Command
SAF	Singapore Armed Forces
SAM	Surface-to-air missile
SAMCO	Singapore Aerospace
SAP	Systemanalyse und Programmentwicklung
SARS	Severe Acute Respiratory Syndrome
SBIC	Shore Based Integration Centre
SBIT	Shore Based Integration Test
SCME	SAF Centre for Military Experimentation
SCO	Systems and Computer Organisation
SE	Systems engineering
SEAD	Systems Effectiveness Assurance Division
SEEL	Singapore Electronic and Engineering Limited
SES	Singapore Engineering Software
SI	Systems Integrator
SIMT	Systems Integration and Management Team
SLC	System life cycle
SLD	Service Logistics Department
SME	Subject Matter Expert
SOA	Service Oriented Architecture
SON	Statement of Needs
SOR	Specification of Requirements
SoS	System of systems
SoSIL	System-of-Systems Integration Lab
SPD	Special Projects Director
SPF	Singapore Police Force
SPO	Special Projects Organisation
SRB	Systems and Research Branch
SRD	Scenario Requirements Document
SVI	Sky Venture International
SVS	Sky Venture Singapore
T&E	Test and evaluation
TAG	Technical Advisory Group
TCO	Total Cost of Ownership
TDR	Target data receiver
TIR	Tracking and illumination radar

UK	United Kingdom
USN	United States Navy
V&V	Verification and validation
VA	Vulnerability assessment
VIP	Very Important Person
VSS2000	Vision for SAF Simulation 2000
VWT	Vertical Wind Tunnel

INDEX

DEFENCE TECHNOLOGY COMMUNITY

"ENGINEERING SINGAPORE'S DEFENCE – THE EARLY YEARS" Book Series

Editorial Panel

Co-Chief Editors of Series	:	Prof Quek Tong Boon Prof Lui Pao Chuen
Editor, Engineering Land Systems	:	Prof Lui Pao Chuen
Editor, Aviation Engineering	:	Mr Tay Kok Khiang
Editor, Engineering Our Navy	:	RADM (Ret) Richard Lim Cherng Yih
Editor, Engineering Systems-of-Systems	:	RADM (Ret) Richard Lim Cherng Yih
Panel Members	:	Prof Su Guaning RADM (Ret) James Leo Er. BG (Ret) Wesley D'aranjo Mr Quek Gim Pew Mr Tan Yang How Mr Chua Poh Kian Ms Surine Ng Pei Gek

Sitting left to right: Mr Tan Yang How, Prof Su Guaning, Prof Quek Tong Boon, Prof Lui Pao Chuen, Mr Quek Gim Pew
Standing left to right: RADM (Ret) James Leo, RADM (Ret) Richard Lim Cherng Yih, Ms Surine Ng Pei Gek, Mr Tay Kok Khiang, Er. BG (Ret) Wesley D'aranjo, Mr Chua Poh Kian

Published by Ministry of Defence, Singapore
303, Gombak Drive
Singapore 669645

Designed by
Advalanche Integrated Advertising Pte Ltd
114 Lavender Street #03-64
Singapore 338729

ISBN 978-981-11-2347-4

Printed by
First Printers Pte Ltd
203 Henderson Industrial Park
#07-09 Singapore 159546