Australian Government
Defence

Capability Acquisition and Sustainment Group (CASG)
Office of the Deputy Secretary
Department of Defence Canberra ACT

Digital Engineering Strategy

2024

Digital Engineering
Embracing Complexity
Enabling Outcomes

To defend Australia and its national interests in order to
advance Australia's security and prosperity
www.defence.gov.au

Acknowledgement of Country

Defence acknowledges the Traditional Custodians of the lands, seas and air in which we live, work and train. We pay our respects to their Elders past and present. We also pay our respects to the Aboriginal and Torres Strait Islander men and women who have contributed to the defence of Australia in times of peace and war.

Digital Engineering Strategy

Office of the Deputy Secretary
Capability Acquisition and Sustainment Group

Department of Defence
Canberra, ACT, Australia

Email: digital.engineering@defence.gov.au
Web: www.defence.gov.au

CG: NOV027-23

Table of Contents

ACKNOWLEDGEMENT

The Department of Defence wishes to acknowledge the United States Office of the Under Secretary of Defense for Research and Engineering for their support in the development of the Australian Defence Digital Engineering Strategy. The Department is grateful for access to both the original US Digital Engineering Strategy published in 2018, as well as the generously shared insights, experience, and lessons learned by the team.

FOREWORD

The National Defence Strategy 2024 sets the strategic direction and reforms required in response to our strategic circumstances. It is clear Defence must focus on the rapid development of deterrent capabilities, acquisition of disruptive technologies and shift to the mindset of delivering a minimum viable capability at speed, to achieve our critical defence objectives.

Our ability to outpace threats requires the entire engineering ecosystem to work faster, smarter, and be more connected than ever before. In partnership with industry, academia, and with allied and international partners, Defence must efficiently and effectively integrate new capabilities into the ADF. We must be adaptive to changes in approaches to warfighting and evolve business practices to drive innovation and accelerate the delivery of capability.

This Digital Engineering Strategy describes the approach to standardise digital engineering across the Defence enterprise. By streamlining and contemporising our processes to leverage revolutionary technologies, increase virtual simulation and digital twin modelling and applying a data driven approach, we will create the foundation to meet Defence's emerging missions.

Digital engineering tools and environments will foster increased collaboration with industry, nationally and internationally, and encourage the re-use of data to realise time and cost efficiencies in our procurement processes.

Industry is already embracing digital transformation. This Strategy intends to more closely align Defence with Industry 4.0, realising real-time decision making through the optimisation of technology.

This Strategy is aligned with the Defence Data Strategy and will support the engineering practices required for the delivery of innovation identified through the Advanced Strategic Capabilities Accelerator (ASCA). Digital engineering will be supported by the implementation of Enterprise Resource Planning to modernise, integrate and transform Defence's approach to managing its finances, human resources, logistics, engineering, maintenance and estate operations.

Our digital engineering goals are outlined in this Strategy, to realise the acceleration of capability development in an unprecedented way. Embracing digital engineering will spur success through risk taking in a digital environment, rapid fielding of minimum viable products, and an agile approach to secure optimal outcomes for Defence and for Australia's future.

I look forward to working with you to realise the significant efficiencies and opportunities this Strategy offers.

Chris Deeble AO CSC
Deputy Secretary

Capability Acquisition
and Sustainment Group

“Technology has a significant impact on the character of warfare and deterrence, and will shape the changing balance of power” – Defence Strategic Review 2023

INTRODUCTION

The National Defence Strategy reinforced the requirement for a fully integrated and more capable ADF, operating seamlessly across five domains.

Realising speed to capability by enabling rapid fielding of minimum viable products and shortening procurement timelines requires an integrated digital approach, underpinned by digital engineering that spans Defence, industry, and academia.

Over the past decade, the world has seen significant digital technological advancements. Modern digital tools and techniques are now more readily available to assist with data-driven and evidence-based analysis.

Defence’s ability to rapidly translate disruptive new technologies into capability requires agile and timely engineering practices.

Defence engineering practices must evolve quickly in order to convert virtual digital designs and models into real world capability. We must transition to supporting visualisation of design and the analysis of risk and safety to our people and provide confidence to our regulators.

Defence’s industry partners are embracing the benefits of digital transformation that increases the speed at which capability can be designed and offered for delivery.

This document lays out a Defence-wide strategy to guide investments in digital engineering data driven tools, digital infrastructure, cultural change and workforce development to enable Defence to experiment, innovate and collaborate more effectively. It recognises the importance of empowering our people to adopt a data-driven approach, places value in the use of models to inform decision-making and is aligned with whole of Australian Government and Defence data strategies.

Digital engineering is an integrated digital approach that uses authoritative sources of systems data and models as a continuum across disciplines to support lifecycle activities from concept through disposal[1]

Technological advances in processing capabilities and computing speed empower this paradigm shift from the traditional design-build-test methodology to a model-analyse-build methodology. This is accomplished through integrated modelling of systems and systems of systems. This approach can enable Defence to experiment and test decisions and solutions in a virtual environment before they are delivered to the Australian Defence Force.

[1] Adapted from US DoD Digital Engineering Strategy, 2018.

For years, Defence and its industrial partners have been pioneering in the use of digital engineering systems and tools in the delivery and sustainment of our warfighting capability.

We now embark on a journey with this strategic vision to integrate and connect these efforts into a collective roadmap to accelerate our progress delivering complexity in the future force.

PURPOSE AND VISION

The strategy guides the planning, development, and implementation of digital engineering transformation in Defence.

The Defence vision for digital engineering is to modernise how Defence designs, develops, delivers, operates, sustains, and evolves needed capabilities. Digital engineering offers an integrated digital approach to address complexity in a collaborative, multi-disciplinary environment to explore shortfalls and options early, at a lower cost, and at reduced risk than traditional approaches.

Defence will connect people, processes, and data securely across the Defence engineering enterprise including industry and international partners. This enables the use of models and common data to digitally represent missions, capabilities, and products in the virtual world. Defence will incorporate technologies such as super-computing, high performance computing big data analytics and artificial intelligence to improve the digital engineering practice. This will both enable sovereign capacity and interoperability by design with allies and partners.

Digital engineering will accelerate innovation through advanced digital technologies to solve problems in new and groundbreaking ways. Transitioning to digital engineering will address long-standing challenges associated with complexity, uncertainty, and rapid change in deploying and using capabilities designed for the defence of Australia and in a coalition and joint setting to enable the vision of Industry 4.0.

Providing a more agile and responsive engineering environment enables digital engineering to support engineering excellence and a foundation which scales to meet the rapidly changing threat landscape. Digital engineering across Defence will improve traceability between product-level engineering and the missions and capabilities in which the products feature. This enables better informed decisions, enhanced communication, and increased confidence in a more efficient engineering process, leading to improved operational effectiveness.

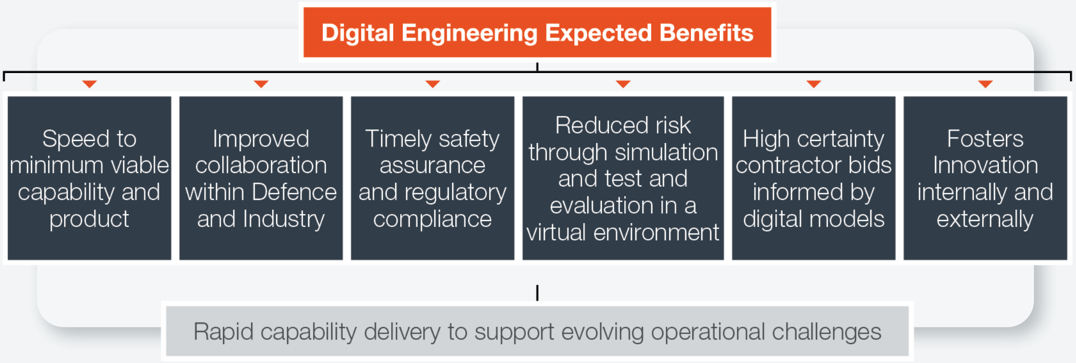
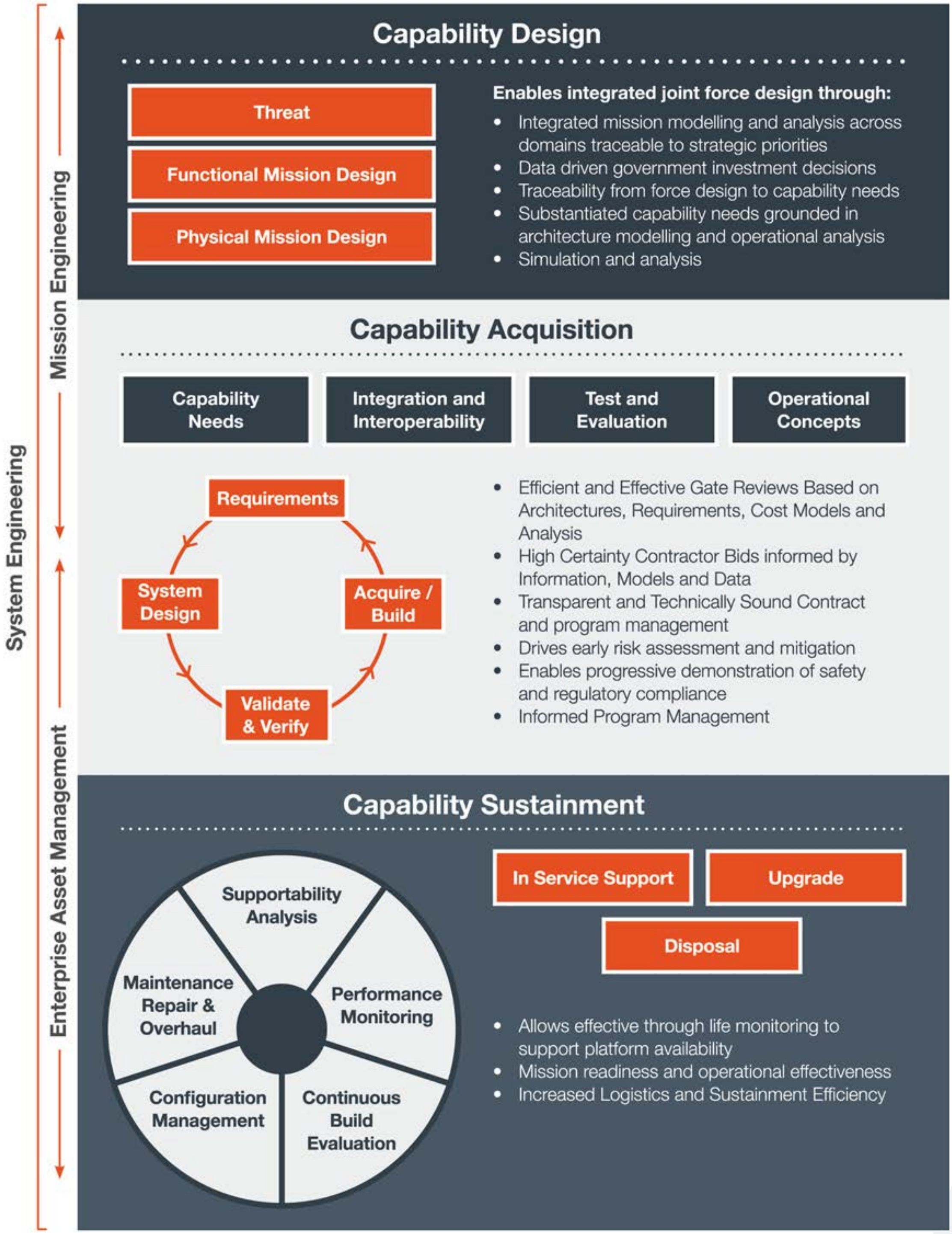

Digital Engineering Expected Benefits
Speed to minimum viable capability and product
Improved collaboration within Defence and Industry
Timely safety assurance and regulatory compliance
Reduced risk through simulation and test and evaluation in a virtual environment
High certainty contractor bids informed by digital models
Fosters Innovation internally and externally
Rapid capability delivery to support evolving operational challenges

Figure 1: Expected Benefits of Digital Engineering

Drives transformation to accelerate delivery of world class Defence capability

DEFENCE DIGITAL ENGINEERING



Capability Design

Enables integrated joint force design through:

- Integrated mission modelling and analysis across domains traceable to strategic priorities
- Data driven government investment decisions
- Traceability from force design to capability needs
- Substantiated capability needs grounded in architecture modelling and operational analysis
- Simulation and analysis

Capability Acquisition

- Efficient and Effective Gate Reviews Based on Architectures, Requirements, Cost Models and Analysis
- High Certainty Contractor Bids informed by Information, Models and Data
- Transparent and Technically Sound Contract and program management
- Drives early risk assessment and mitigation
- Enables progressive demonstration of safety and regulatory compliance
- Informed Program Management

Capability Sustainment

- Allows effective through life monitoring to support platform availability
- Mission readiness and operational effectiveness
- Increased Logistics and Sustainment Efficiency

Figure 2: Defence Digital Engineering

STRATEGIC GOALS

1. Culture and Workforce

Defence culture is transformed, and workforce is empowered to adopt and deliver digital engineering.

This goal underpins Defence's commitment to promote a cultural change through investments in training, assurance, education, strategic communication, leadership, and continuous improvements to realise a digital engineering practice across Defence.

2. Models

Development, integration, and use of digital models informs decision making.

This goal establishes the formal planning and development for use of digital models as an integral part of performing engineering activities. When coupled with authoritative data, digital models provide a clear, shared, and transparent understanding of current and proposed missions, capabilities, and products. These provide ongoing opportunities to assess options at lower cost and risk to inform decisions, with the objective of improving operational outcomes.

3. Data

Trusted, enduring and authoritative data is a fundamental input to speed capability delivery.

This goal enables access, management, use, and exchange of shared data. Authorised stakeholders will have access to current, authoritative, common and trusted information that is fit for purpose. Coupled with the second goal, this goal moves the primary means of driving the engineering and integration process from paper-based documents to agile digital models.

4. Innovation

Technological innovation is enabled by digital engineering.

This goal infuses advancements in technology, including artificial intelligence and machine learning, advanced modelling and simulation, data analytics and advanced computing and provides the platform to transform the engineering practice. By digitally connecting stakeholders, processes, and data, Defence organisations will have the ability to rapidly make decisions, allowing them to adapt to modernise capabilities. This also creates opportunities to leverage innovative technologies that learn, adapt, and act autonomously.

5. Environment

Defence's digital environment effectively enables collaboration and evolution of digital engineering.

This goal promotes the establishment of a robust environment at multiple classification levels to enable digital engineering. It incorporates distributed infrastructure as well as collaborative trusted systems, to access data and models while protecting intellectual property honouring security classification.

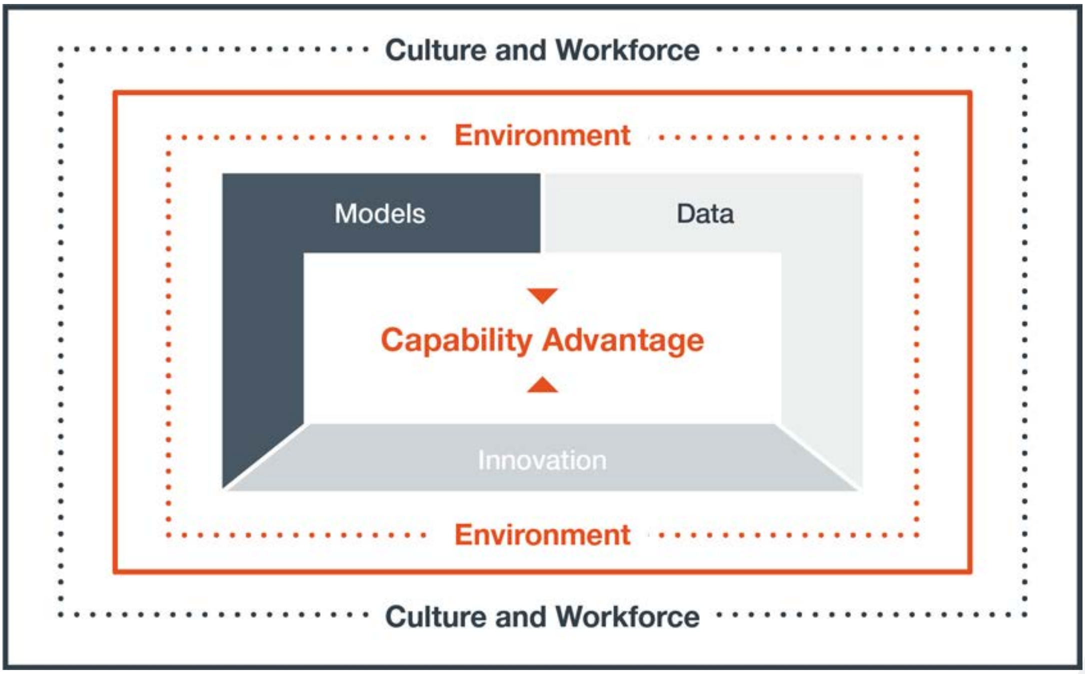


Figure 3: Digital Engineering Strategy

DIGITAL ENGINEERING GOALS AND FOCUS AREAS

GOAL 1. Defence culture and workforce is empowered to deliver digital engineering

This goal takes a deliberate systematic approach to planning, implementing, and supporting Defence's digital engineering transformation. This transformation requires Defence to move beyond the process and technology aspects of digital engineering to address workforce challenges such as people and culture, which includes shared values, beliefs, and collective behaviours. These norms and beliefs fundamentally influence how people behave and perform operations.

Defence will transform the workforce by promoting a cultural change through training, education, strategic communication, leadership, and continuous improvements including investing in shared resources and providing incentives for moving to a digital engineering practice.

1.1 Improve the digital engineering knowledge base

Defence will attract, develop and retain a suitably qualified digital engineering workforce, enabling successful delivery of Defence Capability.

The current Defence digital engineering knowledge base is at various levels of maturity. A concerted effort across Defence will be needed to continually improve, update, and further organise this knowledge base. As organisations solve challenges and institutionalise digital engineering, Defence will leverage existing initiatives to share best practices about effective courses of action and lessons learned to allow the broader community to collaborate and learn from each other. Best practices will be collected and made available for reuse or adaptation in a strategic, enterprise-wide effort to inform, involve, and mobilise Defence and its partners.

Defence will advance digital engineering policy, guidance, specifications, and standards. Currently a wide range of standards enable digital engineering languages, processes, architecture frameworks, but no set of digital engineering guidance covers the range of data and models that must be captured and exchanged with all parties involved. As appropriate, Defence will encourage commonality in terminology, develop a shared understanding of concepts, and promote consistency and rigor in implementing digital engineering.

Defence will look for opportunities to streamline contracting, procurement, legal, and business practices. Opportunities exist for leveraging digital artefacts to support contracting and legal teams to enable rapid capability procurement. Model-based approaches may require changes to Defence processes for planning, evaluating, awarding, and managing procurements.

1.2 Lead and support digital engineering transformation efforts

Transformation requires management of change. Driving a culture of innovation, experimentation, and continuous improvement involves shaping organisational team and individuals' values, attitudes, and beliefs about the transformation. Defence leaders enable the transformation process by encouraging and energising people to contribute and grow. Such leaders provide the framework for change. These leaders seek to engage people to accept and embrace changes through communicating and executing a vision and strategy; building and leveraging a wide range of knowledge and innovation; and demonstrating and rewarding tangible results.

To encourage adoption, Defence leaders will build and communicate the vision and strategy for digital engineering. An effective vision and strategy will help clarify the purpose, direction, and priorities for the organisation. It is essential to build open and frequent communication strategies through multiple channels that provide awareness and a common understanding to stakeholders across disciplines and organisations, including mechanisms for people to ask questions and provide feedback. Leadership should work to remove barriers and address obstacles to change, provide resources and enable new roles and responsibilities to support implementation of the digital engineering vision and strategy.

A wide range of stakeholders are developing digital engineering solutions across various elements of the Defence digital engineering enterprise. Tapping into stakeholders' skills and ingenuity can bring insights and ideas that contribute to collectively advancing the state of practice. Defence can use alliances, coalitions, and partnerships across government, industry, academia to co-create and deploy concepts to facilitate the sharing of information and resources.

Defence will identify leadership teams (e.g., champions, sponsors, etc.) that are accountable to actively manage and implement digital engineering transformation efforts. Leadership will initiate broad-based action that generates short-term wins as well as long-term outcomes. Developing metrics and criteria for success, creating incentives, monitoring progress, rewarding behaviour, and taking corrective action are all critical to improve results across the enterprise and should be established and agreed to by multiple levels of leadership.

CAPABILITY ACQUISITION AND SUSTAINMENT GROUP (CASG)

AIR6500-1 Joint Air Battle Management System (JABMS) Project

The AIR6500 Strategic Partner, Lockheed Martin Australia, has finalised the design, initiated development and integration of a digital ecosystem comprising, among other elements, a Software Integration Laboratory, complex Digital Twin Solutions, and a suite of digital engineering and model-based system engineering tools supporting Modelling, Simulation and Operational Analysis.

AIR6500's Digital Ecosystem enables interoperability across the Integrated Air Missile Defence (IAMD) C4ISR solutions realised through collaborative design, development, integration, verification, validation, in-service support and evolution throughout the AIR6500 series of projects.

Furthermore, the AIR6500's Digital Ecosystem aims to expedite disruptive technology integration, enable rapid capability insertion and promote sustainability through reuse, commonality and autonomy.

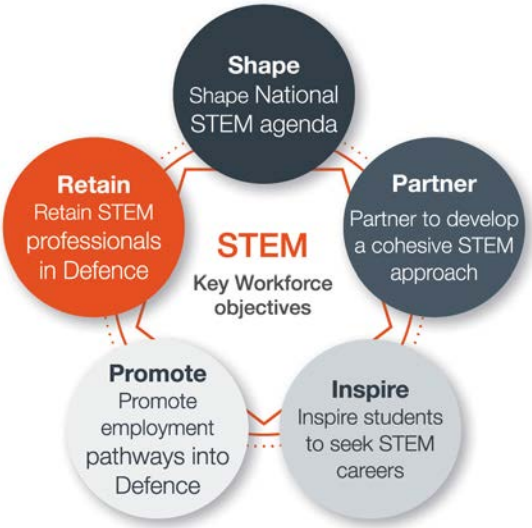
1.3 Build and prepare the workforce

The workforce of the future is geographically dispersed, multi-disciplinary, and multi-generational. Establishing and codifying mechanisms to transfer knowledge, competence, and skills by training and educating the workforce at all levels will be key to developing a competent, digital engineering-capable cadre, especially in the Science, Technology, Engineering, and Math (STEM) workforce.

Training and education are critical components to developing the knowledge, competence, and skills for the workforce to support digital engineering.

This is vital to individuals, teams, and Defence as a whole. Defence will need to holistically—and routinely—educate and train the workforce in new concepts and methods, processes, and tools to keep pace with progress being made. These include computational science, artificial intelligence, and advanced modelling.

Defence will ensure active participation and engagement across the workforce in planning and implementing transformation efforts. Training and education are not the only driver of organisational culture change. Defence must encourage the application of that knowledge through the formation of new habits and behaviours. While training and education are important, "doing" is critical to an organisation gaining experience and adapting to new ways of operating. Engaging stakeholders, whether internal or external to the organisation, allows for active participation in deciding, designing, and delivering digital capabilities.


Shape
Shape National STEM agenda
Partner
Partner to develop a cohesive STEM approach
Inspire
Inspire students to seek STEM careers
Promote
Promote employment pathways into Defence
Retain
Retain STEM professionals in Defence
STEM
Key Workforce objectives

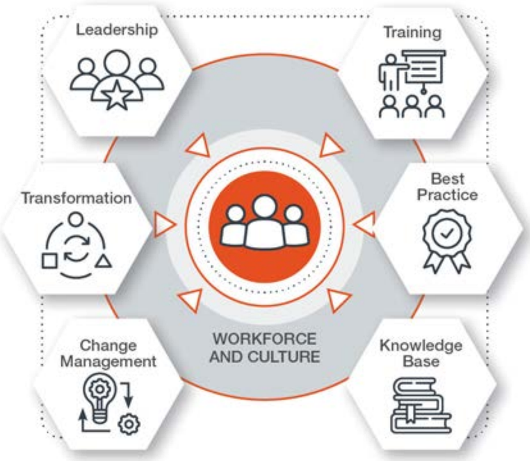


Figure 4: Workforce and Culture Transformation

GOAL 2. Development, integration, and use of digital models informs decision making and design

Digital models can provide a precise and versatile representation of a system, phenomenon, entity, or process. In early phases of the lifecycle, product-level models enable virtual exploration of solutions before they are instantiated. Over a solution's lifecycle, digital models mature and provide digital representations to support design, development and manufacturing decisions and evolution of the product post-fielding. Models of capabilities and missions can provide a shared representation of the complex integration of products and capabilities to understand relationships and dependencies and assess mission effectiveness and gaps.

This goal focuses on the formalised application of modelling which can support the definition and development of integration of systems. There are many different types of models that are developed, integrated, and used continuously across the lifecycle. Formalised modelling of systems and missions can provide a shared representation of current architectures and capabilities as the basis for digital exploration of potential changes and their technical and operational impact. This supports integration of capabilities and products to address gaps and meet operational mission objectives.

Various disciplines and domains can concurrently operate in a virtual environment on different aspects of missions, capabilities, and products. In some cases, instead of discarding and redeveloping models, the collection of digital models evolves and is used over time. In other cases, different phases or epochs call for different digital models.

ROYAL AUSTRALIAN AIR FORCE

Concept Development and Analysis for the Air Combat Program

The Air Combat Program (ACP) has established a process for analysis of wide-ranging mission characteristics, including modelling of relevant red and blue system of systems and design concepts of force employment (CONEMP) to complete the missions. These concepts are validated using computational simulations. This process supports the ongoing requirement to re-assess Air Combat capability preparedness in response to identified emerging threats or triggered by calls from the Joint Force Authority to design force employment options for missions based on the ADF Theatre Concept.

The ACP intends to modernise this process by using digital engineering practice, so that every capability gap, opportunity as well as capability investment decision can be readily demonstrated with authorised data in a repeatable fashion; and traceable across all layers of SoS architectures.

US DoD. 1998. "'DoD Modeling and Simulation (M&S) Glossary" in DoD Manual 5000.59-M. Arlington, VA, USA: US Department of Defense. January. P2.13.22. Available at http://www.dtic.mil/whs/directives/corres/pdf/500059m.pdf

2.1 Formalise the planning for digital models to support engineering activities and decision making

Defence organisations and industry will develop plans for model creation, curation, and integration. These plans will describe how models will be realised as work activities are performed, and as analyses and decisions are supported. This includes the coordination and sharing of model data, as addressed in Goal 3. The development of models ultimately assures the appropriateness of investments to achieve required operational effects.

2.2 Formally develop, integrate and curate models

Collaborative engineering efforts will be supported by a set of shared models which address different aspects of the missions, capabilities, and products. Defence organisations and industry will develop models that are accurate, complete, trusted, and fit for purpose. This will include identifying data gaps and Innovation Science and Technology (IS&T) support required to meet future model needs. Models will be developed according to policy, guidance, standards, and modelling best practices. The Defence organisations will capture and maintain model provenance and pedigree to establish trust, credibility, accuracy, and a basis for judging model use. Model-based reviews, audits, and trust, based on validation and verification, are essential to effective collaboration.

2.3 Use models to support engineering activities and decision making

Defence organisations and industry will use models to communicate, collaborate, and perform engineering activities. Models will be used as the basis for defining, evaluating, comparing, and assessing alternatives, and making decisions. The models will span multiple uses from Joint Force design to individual product development and will provide a shared representation that enables concurrent engineering, cross-disciplinary trades, and other engineering activities.

Models are used to answer questions, reason about solutions, support decisions, and communicate clearly at different levels of fidelity over time. For products, models are used to support full lifecycle activities. For missions and capabilities, models provide the ability to understand the current state of operational capabilities and to explore digitally how changes could impact operational capabilities which will inform investment options early with data driven analysis.

ROYAL AUSTRALIAN NAVY

Digital Mission Models for Risk Reduction CONEMP of Electromagnetic Manoeuvre Warfare Capabilities

Navy Intelligence & Information Warfare (NI&IW) is employing Digital Mission Engineering (DME) and Model Based Systems Engineering (MBSE) techniques as part of a Risk Reduction Study to inform development of the SEA 5011 Program Concept of Employment (CONEMP). This work will inform the RAN of feasible techniques, processes and architectures for operational employment of Electromagnetic Manoeuvre Warfare (EMMW) capabilities. Insight gained through this work package will inform decisions on forward options across multiple NI&IW projects and initiatives.

Key outcomes include applying DME to identify gaps with current EMMW processes and technology, enabling data-driven recommendations for closing said gaps, and advancing current Navy analytic competencies to include an enduring Digital Engineering (DE) capability to bring speed to capability deployment.

GOAL 3. Trusted, enduring, and authoritative data is a fundamental input to digital engineering

Stakeholders across organisations will have the ability to access, employ, manage, protect, and analyse shared, authoritative data to enable the use of models to drive decision making. In alignment with the Defence Data Strategy, digital engineering will move to data serving as the basis for connecting traditionally siloed elements to provide integrated information exchange. This gives stakeholders the ability to collaboratively work within and through the shared data and models using shared knowledge and resources.

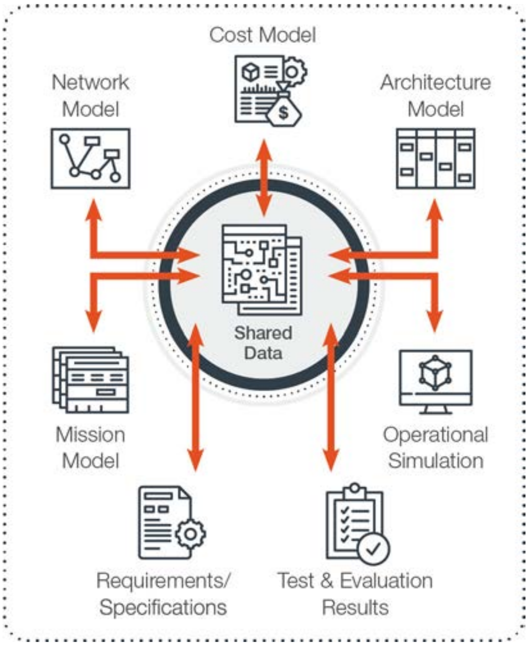


Figure 5: Examples of models connected via shared authoritative data

3.1 Define, manage, and share authoritative data

Data is authoritative within a controlled digital engineering environment on how it is developed and how it is used. It is critical to maintain the pedigree and understand the provenance of the data to ensure its appropriate use. Shared authoritative data serves as the central reference point for models.

Maintaining authoritative data sources will provide traceability, capture historical knowledge, and connect authoritative versions of models.

Properly maintaining the appropriate authoritative sources of data will mitigate the risk of using inaccurate model data and will support effective control of current and historic configuration data.

The realisation of sources of authoritative data requires effective upfront planning to support models as addressed in Goal 2. Setting clear expectations for defining, developing, and using the trustworthy data across disciplines is imperative. Having access to shared, authoritative data facilitates a collaborative process across the boundaries of engineering disciplines, distributed teams, and domains as well as across missions, capabilities, and products. The goal is to ensure the availability of the right data to the right person for the right use at the right time.

3.2 Govern the sources of authoritative data

Defence will establish policies and procedures to ensure proper access, maintenance, and use of the authoritative sources of data. Governance will ensure the data is formally managed, trustworthy, and used appropriately. This will allow stakeholders to collect, share, and maintain needed data accurately. Establishing procedures to maintain the integrity and quality of the data will ensure consistency and accuracy of the authoritative data, and enable stakeholders to make decisions about whether data is fit for purpose and can be used with confidence.

Establishing access and controls is necessary to ensure authorised users have access to the right information at the right time and will allow an uninterrupted exchange of data across organisational boundaries. It is important to make data discoverable and readily available to all intended recipients. Maintaining access and control criteria can ensure information will be appropriately protected and retained.

An effective and robust governance process involves responsibilities at various levels. Managing policies, procedures, and standards will ensure proper governance of the authoritative data and enhance data quality across the enterprise. Executing governance should result in increased stakeholder confidence in the integrity of the authoritative sources of data.

3.3 Use authoritative sources of data over time

Defence will use authoritative data to produce digital artefacts, support reviews, conduct analyses and trades, and inform decisions. Data sources will be used to develop, manage, and communicate information which will equip users with common knowledge needed to coherently plan, design, sustain and evolve missions, capabilities, and products.

For products, as the technical baseline matures, preserving the knowledge across lifecycle phases is essential so that technical reviews can be conducted from the authoritative models and data sources on a continuous basis. For missions, baseline or current capability can be represented and analysed from operational and technical perspectives to identify gaps and alternatives and to assess options and inform capability needs and investment decisions.

Use of authoritative data will enable teams to work collaboratively, and integrate their work across domains, disciplines, and organisations.

As established in Goal 2, models serve as a continuum across the product development lifecycle and across capabilities and missions over time. This will fundamentally change the current document-based process to one that uses models as the technical underpinnings for acquisition decisions.

This Digital Engineering strategy will drive the adaption of the Digital Strategy and Roadmap within the engineering discipline.

ADF HEADQUARTERS

Authoritative Digital Models of the Joint Force using the Joint Mission Design Framework (JMDF)

Defence has established a ‘top-down’ design process for the joint force that translates strategic guidance into structured joint mission designs. These designs are used to define and assure the ‘system of systems’ (SoS) needed to conduct ADF joint missions.

Digital Engineering is an essential foundation for capture, analysis, and sharing of joint mission designs as the common and authoritative reference for the many stakeholders involved in capability development.

GOAL 4. Technological innovation is enabled by digital engineering

This goal infuses advancements in technology, including artificial intelligence and machine learning, advanced modelling and simulation, data analytics and advanced computing and provides the platform to transform the engineering practice. By digitally connecting stakeholders, processes, and data, Defence organisations will have the ability to rapidly make decisions, allowing them to adapt to modernise capabilities. This also creates opportunities to leverage technologies that learn, adapt, and act autonomously.

4.1 Digital transformation drives innovation in engineering practice

Realising a digital enterprise, automating tasks and processes, and making smarter, faster decisions all require the next frontier of technologies. With the adoption of digital engineering, Defence will leverage digital transformation to enable a data-driven, model-based approach in a digitally connected environment.

This enables agile lifecycle activities and the ability to adopt an evergreen approach to develop and integrate capabilities. The outcome will be an enduring digital representation that provides continuous insight and knowledge over time. Opportunities exist in engineering capabilities at scale, where the advantage is in representation of relationships, dependencies and complexities across products and assessment of collective technical and operational mission benefits.

Advances in artificial intelligence have given rise to cognitive technologies that are able to perform tasks that traditionally required human reasoning. Machines are now able to build knowledge, continuously learn, understand natural language, and reason and interact more naturally with human beings than traditional systems.

As opportunities to incorporate artificial intelligence arise, Defence will advance the engineering practice by utilising these technologies, evaluating opportunities to pilot them, and demonstrating options for creating value with them.

There has been an exponential growth of data in various formats and from different sources. Defence's vision is to build an enterprise capability that securely leverages data and analytics to enable insights and achieve faster and better data-driven decisions by capturing and continuously assessing engineering data as the missions, capabilities and products evolves.

Appendix A shows a conceptual digital engineering lifecycle model that shows how digital engineering could enable transformative approaches to engineering practice.

Finally, advances in distributed computing technologies allow for collaborative engineering analyses and advanced large-scale simulation and test and evaluation supporting decision making across the enterprise. These and other innovation science and technology advancements fuel new opportunities to evolve the engineering practice.

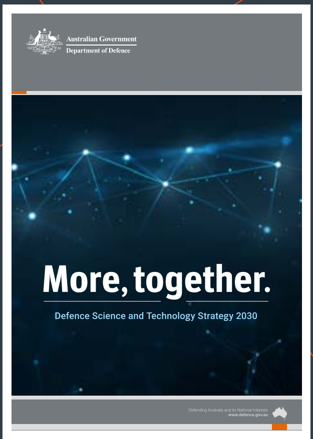
DEFENCE SCIENCE AND TECHNOLOGY GROUP

Underwater Vehicle Hydrodynamics and Acoustics

The Defence Science and Technology Group Hydrodynamics and Acoustics disciplines have developed significant validated computational/simulation capability to model the dynamic, propulsion and acoustic characteristics of underwater vehicles, enabling the design and evaluation of the vehicles behaviour.

This has enabled DSTG to rapidly provide Anduril Australia with the hydrodynamic design of the Ghost Shark vehicle and its optimisation to meet various mission requirements. The team were able to adapt the tools developed for larger submarine platforms to enable Anduril to rapidly iterate the design and provide Defence with a new undersea capability.

The project required DSTG to work collaboratively with industry and other Defence partners in developing and complementing the digital simulation and prediction tools to provide rapid solutions to complex design, manufacturing, and operational challenges. This capability will continue to evolve and make a significant contribution to the acquisition and deployment of complex underwater vehicles.


Australian Government
Department of Defence
More, together.
Defence Science and Technology Strategy 2030
Defending Australia and its National Interests
www.defence.gov.au

4.2 Innovation advances in Defence capability through digital engineering

Digital engineering enables technological innovation to improve engineering practise and integration of advanced technology into defence system capability outcomes. By allowing investigation of the impacts of innovative approaches to systems implementation virtually, Defence can examine and capitalise on the same technologies which will enhance the engineering process. These include automation, artificial intelligence, distributed computing, big data, computational science, and advanced networking. Digital engineering allows engineers to entertain new innovative approaches to address emerging operational needs in a virtual environment at a lower cost and lower risk – accelerating innovation in Australian capability development.

Opportunity to collaborate in the digital engineering ecosystem creates an environment for engaging with a broad range of partners globally increasing the reach into new technical areas. Model based design can allow for exploration of wider options for integration of technologies and advanced simulation creates a venue for assessing potential impact on product development, capability delivery and mission outcomes, all contributing to the goal of increasing operational effectiveness.

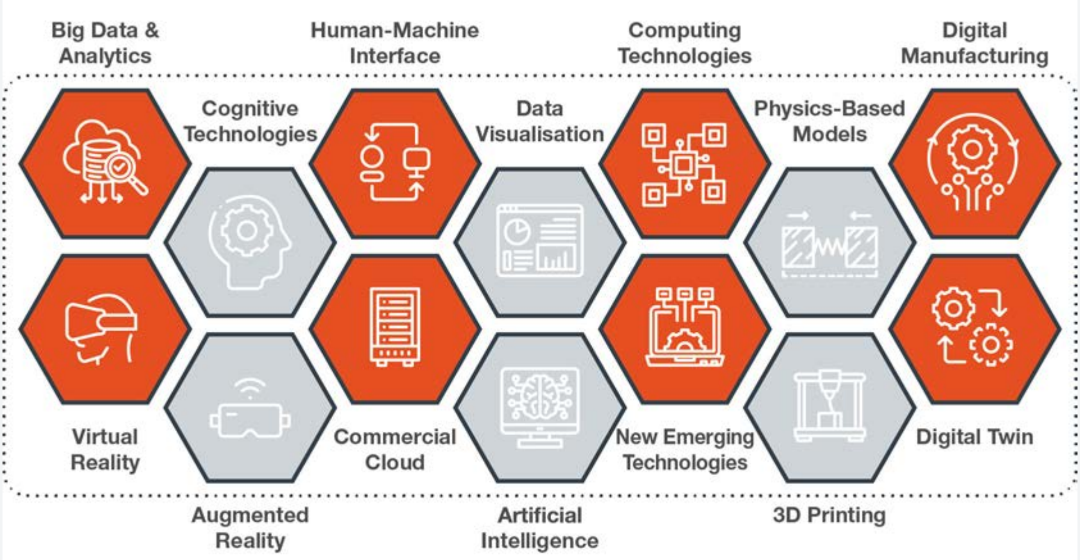


Figure 6: Examples of Advanced Technologies

GOAL 5. Defence's digital environment effectively enables collaboration and performance of digital engineering

The success of digital engineering depends upon having a digital environment that supports collaboration across the engineering enterprise. Building upon current Defence and industry capabilities, digital engineering requires a consolidated, collaborative trusted environment that enables the engineering enterprise. This includes establishing digital engineering methods, processes, and tools, and deploying underlying infrastructure to execute in a collaborative way while assuring protection of data, models, and intellectual property.

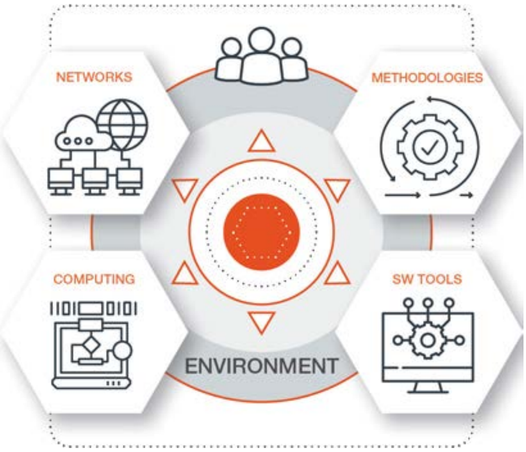


Figure 7: Defence Digital Environment

5.1 Develop, mature, and use digital engineering methodologies

Effective use of a digital engineering enterprise requires transforming from a document-based to a model-based approach. As a result, Defence will evolve its extant engineering practice to work, manage, develop, and deliver solutions to take advantage of evolving capabilities as discussed in Goal 4.

Defence will support this effort by researching, maturing, and implementing engineering methods and processes across an evolving digital engineering practice building on international practices and standards. This may result in Defence updating engineering processes, manuals, and instructions, as required. At a minimum, these new engineering methods should incorporate technological innovations, authoritative sources of data, formalised modelling, workforce, and cultural opportunities to improve quality, productivity, and efficiency.

Defence will evaluate, identify, invest in, and apply tools for stakeholders to implement digital methodologies. The tools need to incorporate a mix of scalable solutions driven by the requirements of stakeholders across disciplines and domains.

Defence will focus on protection of sensitive and classified information as well as operational standards and data sharing rather than mandating specific tools.

Key factors for digital engineering tools include visualisation, analysis, data and model management, model interoperability, workflow, collaboration, and extension/customisation support. Developing, maturing, and implementing innovative digital engineering tools will provide people with the technology needed to increase engineering efficiency.

5.2 Develop, mature, and use digital engineering infrastructure

Digital engineering shares infrastructure that enables a collection of hardware, software, networks, and related equipment spanning geographical locations and organisations. Digital engineering infrastructure is a crucial enabler and foundation for advancing the state of the practice. This includes critical infrastructure such as supercomputing and supporting software, physics-based models and research networks as well as important collaborations with international partners to share and develop capability in areas of common interest.

Reliable, available, secure, and connected information networks are necessary to perform digital engineering activities across Defence. The networks must include computing infrastructure and enterprise services at multiple classification levels that securely facilitate shared access to models and authoritative data. The right infrastructure will help improve collaboration, enhance learning, facilitate information sharing, and enable data-driven decision making.

Defence will plan, resource, and deploy hardware and software solutions to enable digital engineering needs of the workforce and associated digital engineering activities. Modular approaches and a wide range of hardware and software solutions to provide flexible scalability, sizable cost savings, and rapid deployment when establishing the digital enterprise will be considered to ensure a fit-for-purpose solution. Defence will conduct an environmental scan to identify commercial off the shelf solutions used by Industry and International Partners where possible to standardise Defence's approach with commercial best practice and tools which have open-source integrations for data exchange to facilitate integration and reuse of tool data.

> Undertaking this digital engineering journey will identify the needs for future networks, cloud infrastructure and systems. It will also inform the planning of this essential capability within the Defence Digital Group.

Australian Government
Defence

Ready to Fight and Win in the Digital Age

2022 Defence Information and Communications Technology Strategy

5.3 Secure IT infrastructure and protect intellectual property

A digital engineering transformation relies on the protection of models and data classification, availability, confidentiality, non-repudiation, and integrity. Given the amount of information residing in models, Defence must manage cyber risks and secure digital engineering environments against attacks from internal and external threats.

Defence, with support from industry and academia, will ensure intellectual property and sensitive information is protected, including need to know and export control constraints, while promoting collaboration and innovation.

Digital engineering stakeholders must protect infrastructure, while facilitating the realisation of digital engineering goals. Defence, industry, and academia will address the risk posed by collaboration and access to the vast amounts of information in models. Methods, processes, and tools will be updated and developed as needed to address any unique challenges of digital engineering collaboration among different networks and levels of security.

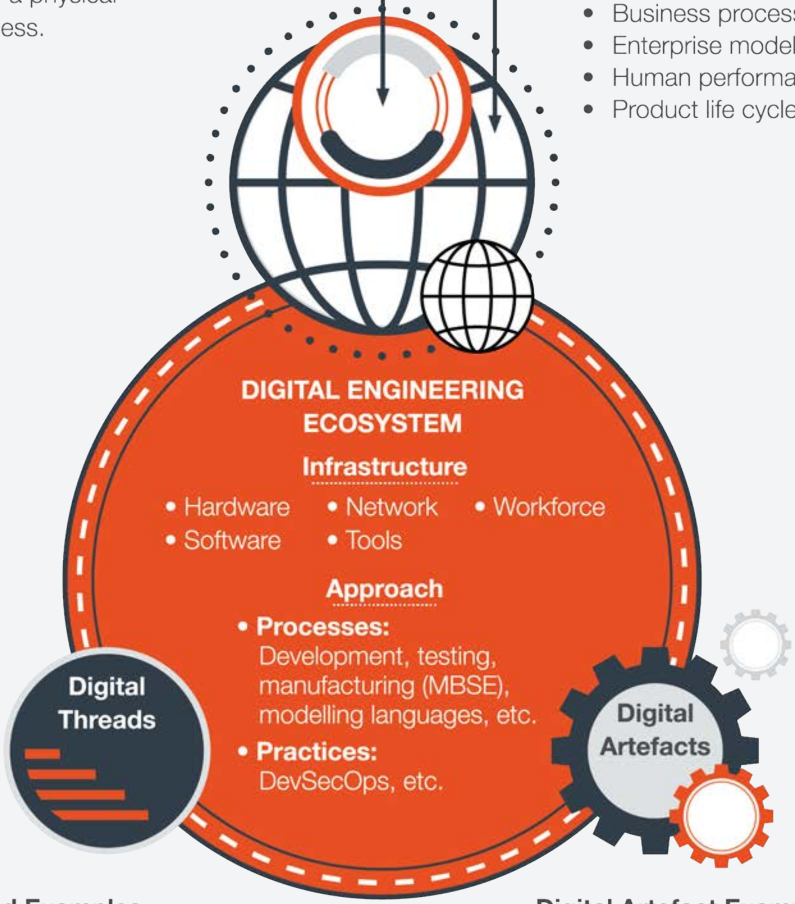
Defence will protect intellectual property while using models to collaborate. Where necessary, Defence will update its methods, processes, and tools to enable data and model exchanges while protecting property rights for government, industry, academia, and international partners. Identification and protection of intellectual property is an extremely complex challenge that Defence and partners must address together. All involved have the responsibility to protect copyrights, trademarks, patents, and competition-sensitive information while balancing the need to exchange relevant information between stakeholders.

Digital Twin

A computerised representation (integrated set of models) that serves as the real-time digital counterpart of a physical object or process.

Digital Model Examples

- Requirements model
- Structural model
- Functional model
- Architecture model
- Business process model
- Enterprise model
- Human performance models
- Product life cycle models



DIGITAL ENGINEERING ECOSYSTEM

Infrastructure

- Hardware
- Network
- Workforce
- Software
- Tools

Approach

- **Processes:** Development, testing, manufacturing (MBSE), modelling languages, etc.
- **Practices:** DevSecOps, etc.

Digital Threads

Digital Artefacts

Digital Thread Examples

- Requirements analysis
- Architecture development
- Design and cost trades
- Design evaluations and optimisation
- System, subsystem, and component definition and integration
- Cost estimations
- Training aids and devices development
- Development and operational tests
- Product support

Digital Artefact Examples

- Specifications
- Technical drawing
- Design documents
- Interface management documents
- Analytical results

Figure 8: Digital Engineering Ecosystem from US DOD Digital Engineering Standard

CONCLUSION

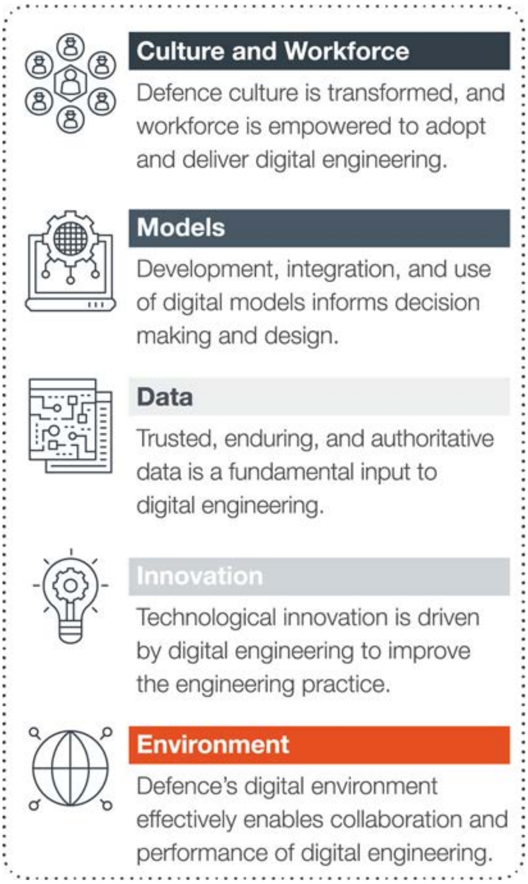
As the global threat landscape continues to evolve, remaining competitive and modernising Defence's digital environment to meet the exigencies of the day is an imperative for Defence. Accelerating delivery of capability is a must and the time is now to enhance the Australian Defence engineering ecosystem.

This Digital Engineering Strategy outlines Defence's five strategic goals for a Defence-wide digital engineering initiative that will accomplish just that. The goals promote the use of digital representations and the use of digital artefacts as a technical means of driving innovation into the engineering process and communicating across a diverse set of stakeholders.

The strategy also addresses a range of disciplines involved in the acquisition and procurement of national Defence systems. It encourages innovation in the way Defence builds, tests, fields, and sustains Defence products and integrates them into needed capabilities and effective operational missions, and how Defence trains and shapes a workforce to embrace these practices.

The goals identified in this strategy provide the foundation for Defence to continuously transform and evolve its capabilities to better deliver the integrated force needed to defend Australia and its interests.

Applying this strategy will enable Defence to strengthen overall adoption of digital engineering competencies to grow and optimise the efforts in acquiring new and evolving existing capabilities while sustaining it into the future. This, in turn would enable Defence to more effectively mature capability lifecycle in line with the global practises and cutting edge technologies.



Culture and Workforce

Defence culture is transformed, and workforce is empowered to adopt and deliver digital engineering.

Models

Development, integration, and use of digital models informs decision making and design.

Data

Trusted, enduring, and authoritative data is a fundamental input to digital engineering.

Innovation

Technological innovation is driven by digital engineering to improve the engineering practice.

Environment

Defence's digital environment effectively enables collaboration and performance of digital engineering.

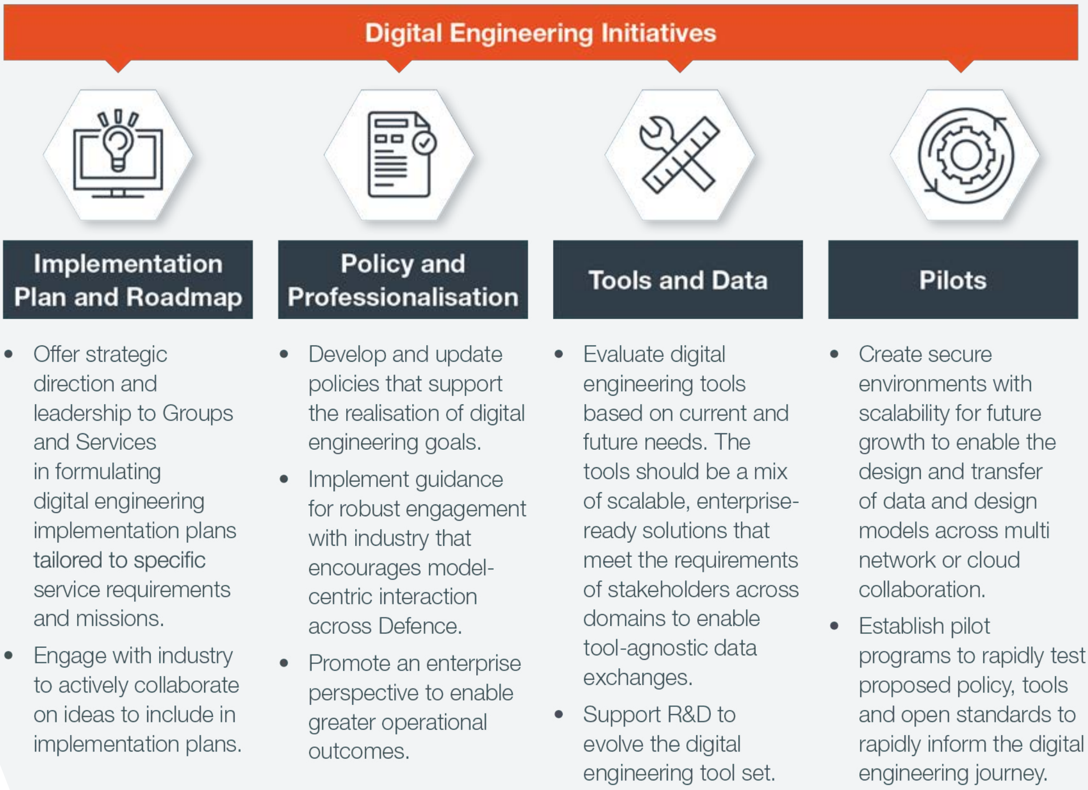
Figure 9: Defence Digital Environment Goals

NEXT STEPS

Capability Acquisition and Sustainment Group, as the lead for engineering policy across Defence, led the development of this strategy and serves as the Defence advocate for digital engineering, working with Groups and Services. With the adoption of the strategy, CASG will work with Defence digital engineering champions, as well as industry, to enable implementation. CASG will coordinate with stakeholders as they develop specific implementation plans, which together will constitute a Defence-wide roadmap for achieving the goals set forth in this strategy. In collaboration with DSTG, Defence Groups, Services and Agencies, CASG will identify digital engineering research needs to resolve limitations within existing tools and identify options for evolution of the digital engineering tool set.

The 2024 version of the Digital Engineering Strategy is an initial position by Defence to enable consultation with stakeholders across Industry and Government to co-design a Roadmap and Implementation Plan to uplift digital engineering in support of the strategic goals identified.

This is the start of a digital transformation journey within engineering practice for capability acquisition sustainment.



Digital Engineering Initiatives

Implementation Plan and Roadmap

- Offer strategic direction and leadership to Groups and Services in formulating digital engineering implementation plans tailored to specific service requirements and missions.
- Engage with industry to actively collaborate on ideas to include in implementation plans.

Policy and Professionalisation

- Develop and update policies that support the realisation of digital engineering goals.
- Implement guidance for robust engagement with industry that encourages model-centric interaction across Defence.
- Promote an enterprise perspective to enable greater operational outcomes.

Tools and Data

- Evaluate digital engineering tools based on current and future needs. The tools should be a mix of scalable, enterprise-ready solutions that meet the requirements of stakeholders across domains to enable tool-agnostic data exchanges.
- Support R&D to evolve the digital engineering tool set.

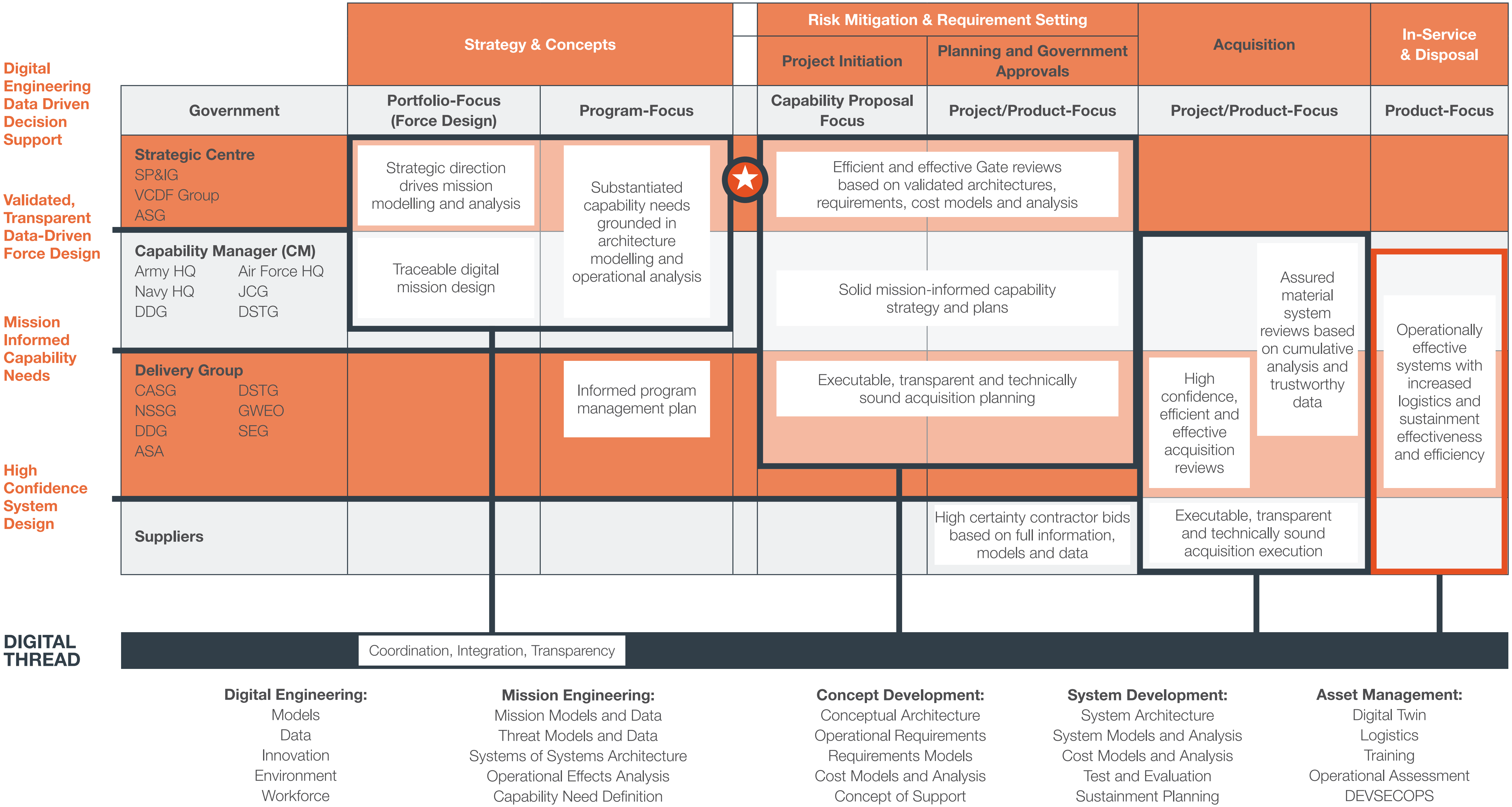
Pilots

- Create secure environments with scalability for future growth to enable the design and transfer of data and design models across multi network or cloud collaboration.
- Establish pilot programs to rapidly test proposed policy, tools and open standards to rapidly inform the digital engineering journey.

Figure 10: Digital Engineering Initiatives

APPENDIX A

Conceptual digital engineering capability lifecycle model



Digital Engineering Data Driven Decision Support

Validated, Transparent Data-Driven Force Design

Mission Informed Capability Needs

High Confidence System Design

Strategy & Concepts

Risk Mitigation & Requirement Setting

Project Initiation

Planning and Government Approvals

Acquisition

In-Service & Disposal

Government

Portfolio-Focus (Force Design)

Program-Focus

Capability Proposal Focus

Project/Product-Focus

Project/Product-Focus

Product-Focus

Strategic Centre
SP&IG
VCDF Group
ASG

Capability Manager (CM)
Army HQ
Air Force HQ
Navy HQ
JCG
DDG
DSTG

Delivery Group
CASG
DSTG
NSSG
GWEO
DDG
SEG
ASA

Suppliers

Strategic direction drives mission modelling and analysis

Traceable digital mission design

Substantiated capability needs grounded in architecture modelling and operational analysis

Informed program management plan

Efficient and effective Gate reviews based on validated architectures, requirements, cost models and analysis

Solid mission-informed capability strategy and plans

Executable, transparent and technically sound acquisition planning

High certainty contractor bids based on full information, models and data

Assured material system reviews based on cumulative analysis and trustworthy data

High confidence, efficient and effective acquisition reviews

Executable, transparent and technically sound acquisition execution

Operationally effective systems with increased logistics and sustainment effectiveness and efficiency

DIGITAL THREAD

Coordination, Integration, Transparency

Digital Engineering:
Models
Data
Innovation
Environment
Workforce

Mission Engineering:
Mission Models and Data
Threat Models and Data
Systems of Systems Architecture
Operational Effects Analysis
Capability Need Definition

Concept Development:
Conceptual Architecture
Operational Requirements
Requirements Models
Cost Models and Analysis
Concept of Support

System Development:
System Architecture
System Models and Analysis
Cost Models and Analysis
Test and Evaluation
Sustainment Planning

Asset Management:
Digital Twin
Logistics
Training
Operational Assessment
DEVSECOPS

SP&IG = Strategy, Policy and Industry Group
VCDF = Vice Chief of the Defence Force
ASG = Associate Secretary Group
HQ = Headquarters

JCG = Joint Command Group
DDG = Defence Digital Group
DSTG = Defence Science and Technology Group
CASG = Capability Acquisition and Sustainment Group

NSSG = Naval Shipbuilding and Sustainment Group
GWEO = Guided Weapons and Explosive Ordnance
SEG = Security and Estate Group
ASA = Australian Submarine Agency