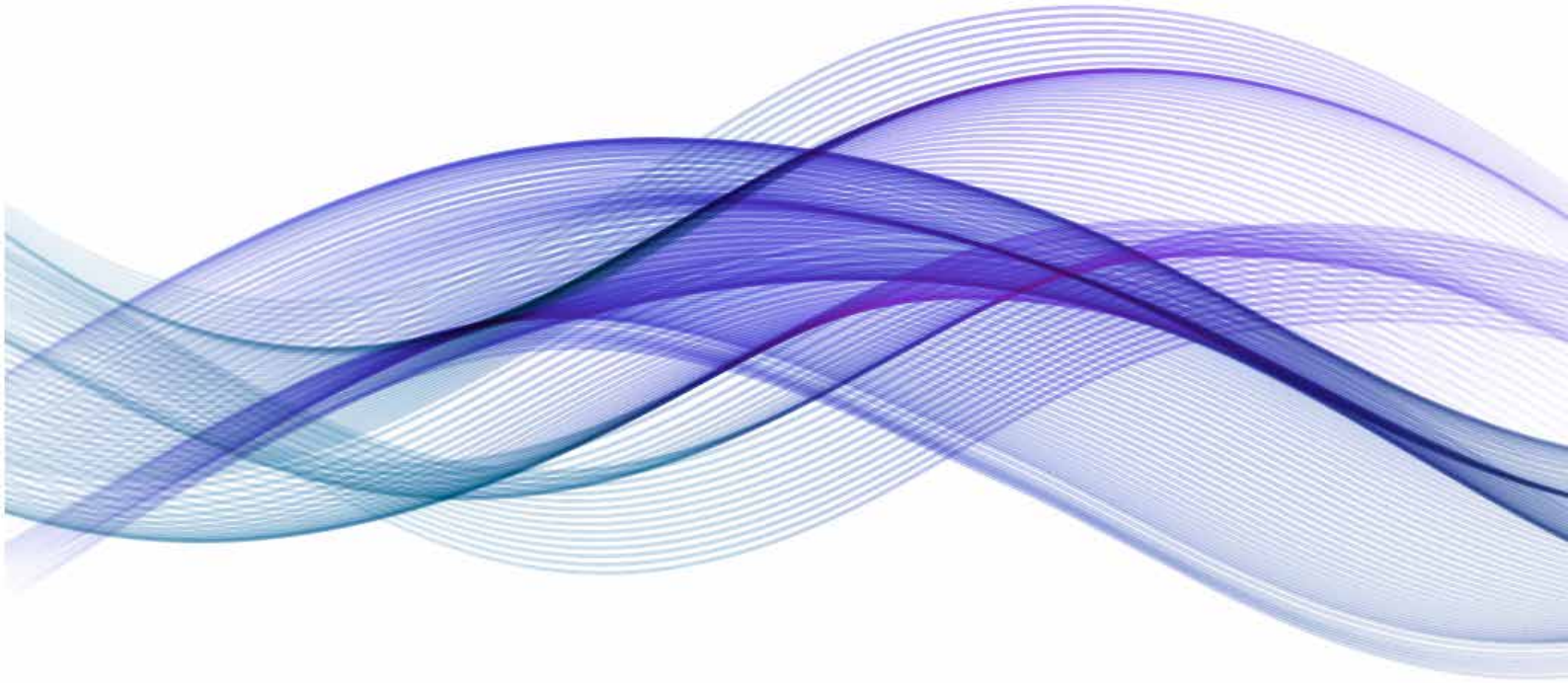


Ministry of Defence

de&S

Defence Digital Twin Implementation Road Map and Development Framework

TEAM DEFENCE INFORMATION

Ministry of Defence

de&s

CONTENTS

Section	Page
KEY FINDINGS	2
INTRODUCTION	3
DEFENCE DIGITAL TWIN IMPLEMENTATION ROAD MAP AND DEVELOPMENT FRAMEWORK PURPOSE	3
FRAMEWORK DEVELOPMENT APPROACH	4
THE UK DEFENCE DIGITAL TWIN ROADMAP DEVELOPMENT FRAMEWORK	6
SUMMARY OF WORK STREAM FINDINGS	8
UK DEFENCE DIGITAL TWIN ROAD MAP - TWIN HIERARCHY	10
DATA AND INFRASTRUCTURE	13
SENSE AND DECISION MAKING	14
ENABLERS	16
CHANGE	18
NEXT STEPS	20

TEAM DEFENCE INFORMATION

KEY FINDINGS

The following are key Digital Twin Road Map and Development Framework findings:

1. Digital Twins are valuable because they reduce business friction, can optimise delivery of Defence support, enable decisions to be made more effectively and speed up investment decision making.
2. The MOD can build on the work being undertaken by the UK Infrastructure including their international standards, plus participation in the anticipated UK Government Digital Twin technology and skills investment and support the development of International Standards suitable for Defence projects.
3. MOD's £2bn investment over the next decade in the digital backbone infrastructure including secure cloud capability, management processes, plus skills development are key enablers for Support Digital Twins.
4. Defence should start building Digital Twins at the equipment level and through standards and architectures that allow Digital Twins to be aggregated build towards Capability Digital Twins over the next decade.
5. Technology is readily available from industry to enable the adoption of Digital Twins, the creation of the Digital Thread, minimising network load demands and for data visualisation.
6. Access to data including the commercial aspects requires planned management and investment.
7. Support Digital Twins are part of the wider Digitisation of the engineering life cycle.
8. Logistics, Asset Management and Support use cases for Digital Twins will need to be created.
9. Digital Twins will require a multi-year investment programme and needs an active Defence Community-of-Interest (COI) to support their wide adoption and the creation of an effective Development Framework. It is suggested that this COI and investment is started immediately to ensure the right requirements are built into the MOD's digital backbone creation programmes.
10. Defence should learn from early proof of value activities and use existing projects to create the Development Framework.

INTRODUCTION

Digital Twins are connected digital representations of physical things, unlocking value by reducing business friction and enabling improved insights that support better decisions, leading to better outcomes in the physical world.

They can enable decisions to be made at pace to address changing threats. For Defence support Digital Twins should help manage the Defence logistics and support enterprise by reducing business friction to enable successful delivery of the required operational effect.

The Defence Digital Twin Road Map and Development Framework builds on the previous White Papers for Digital Twins [1] and Information Architecture [2]; it is also based on the MOD Digital Strategy for Defence [3] - Delivering the Digital Backbone and unleashing the power of our data.

DEFENCE DIGITAL TWIN IMPLEMENTATION ROAD MAP AND DEVELOPMENT FRAMEWORK PURPOSE

Defence is at the beginning of its Digital Twin journey and this short paper provides a summary of the activities required to create a Digital Twin Development Framework and support rich conversations between the MOD Support Command Functions, DE&S and industry about the investment required to make it a reality.

The aim of the road map is to define the elements necessary to create an enduring framework for UK Defence that will support the adoption of Digital Twins as business-as-normal and form part of the wider digital enterprise. It identifies framework elements that can be either adopted or modified from existing industry good practice and those items that Defence need to create.

It will be followed by the development Framework Road Map representations including a suggested programme that shows alignment and the sequence elements are to be addressed in, especially where do we start.

[1] https://secure.teamdefence.info/filerequest.php?id=1006901

[2] https://secure.teamdefence.info/filerequest.php?id=1007326

[3] Defence Digital Strategy – which provides for investment in enabling technologies such as secure hyperscale cloud, secure next generation networks, data standards, enterprize-scale software solutions, etc.

FRAMEWORK DEVELOPMENT APPROACH

Delivering the Development Framework is a considerable challenge and will require joint working between MOD and industry.

When practicable the Development Framework was built on existing industry investments including:

- the work being undertaken by the Centre for Digital Built Britain, in particular the National Digital Twin Programme Road Map [4] ;
- ISO 19650 standard for managing information over the whole life cycle of a built asset using building information modelling (BIM);
- Industry 4.0 standards;
- Skills Framework for the Information Age (SFIA); and
- cloud technologies, distributed ledgers and commercial equipment/platform support tools.

ISO 19650 provides a useful starting point for Defence but is designed for the built environment. Defence will therefore need to develop Defence Standards for equipment (products), platforms, soldier systems, services, capabilities, etc. however the longer-term vision should be to support the development of an International Standard.

Also, to ensure that the Development Framework was complete the Burke-Litwin Performance and Change Model[5] was considered.

The Development Framework also needs to align and build on the Defence Support Strategy and the Digital Strategy for Defence. This £2bn investment over the next decade in the digital backbone infrastructure including secure cloud (in the next two years), management processes, and skills development are key enablers.

The Road Map sets out how the Development Framework should be built and how the elements fit together to enable effective information management across the Defence enterprise. In order to make the delivery of the Framework more manageable, it was broken down into five streams of interconnected components, these being:

- Governance and Life Cycle;
- Data and Infrastructure;
- Sense and Decision Making;
- Enablers; and
- Change

The Digital Twin Road Map Development Framework also follows slightly modified Gemini principles[6]
Figure 1 - Defence Gemini Principles to enable alignment on the approach to information management across Defence to make it easier to share data in the future. Enshrined in these values is the notion that all Digital Twins must have a clear purpose, be trustworthy and function effectively. They are deliberately simple, but their implications are far-reaching and challenging.

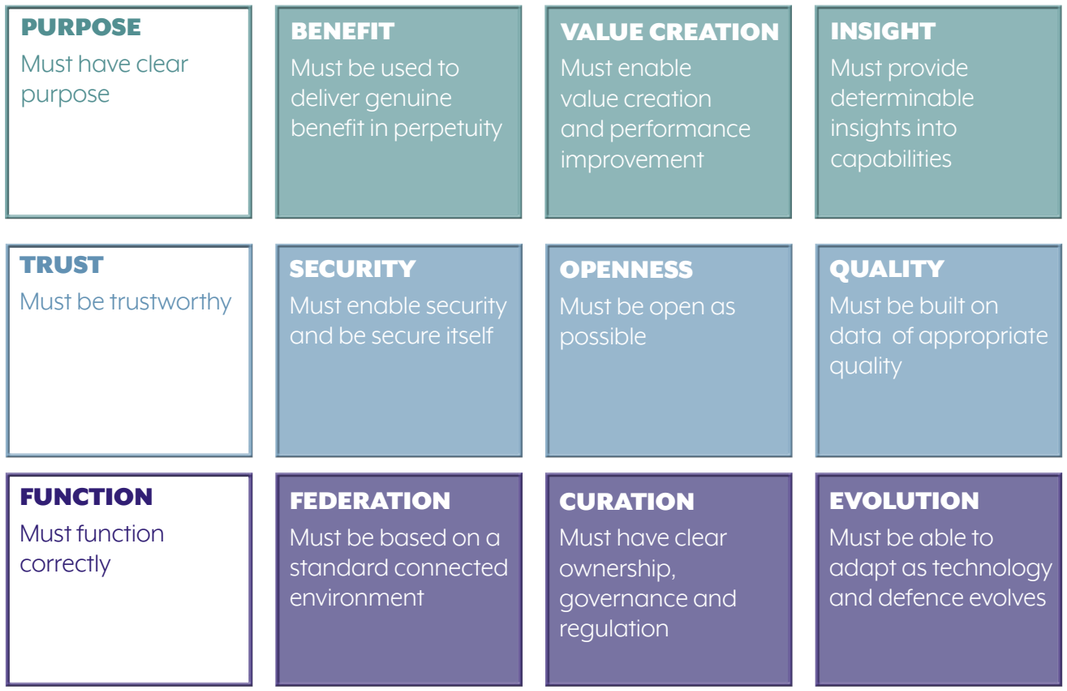


Figure 1 - Defence Gemini Principles

[4] https://www.cdbb.cam.ac.uk/DFTG/DFTGRoadmap

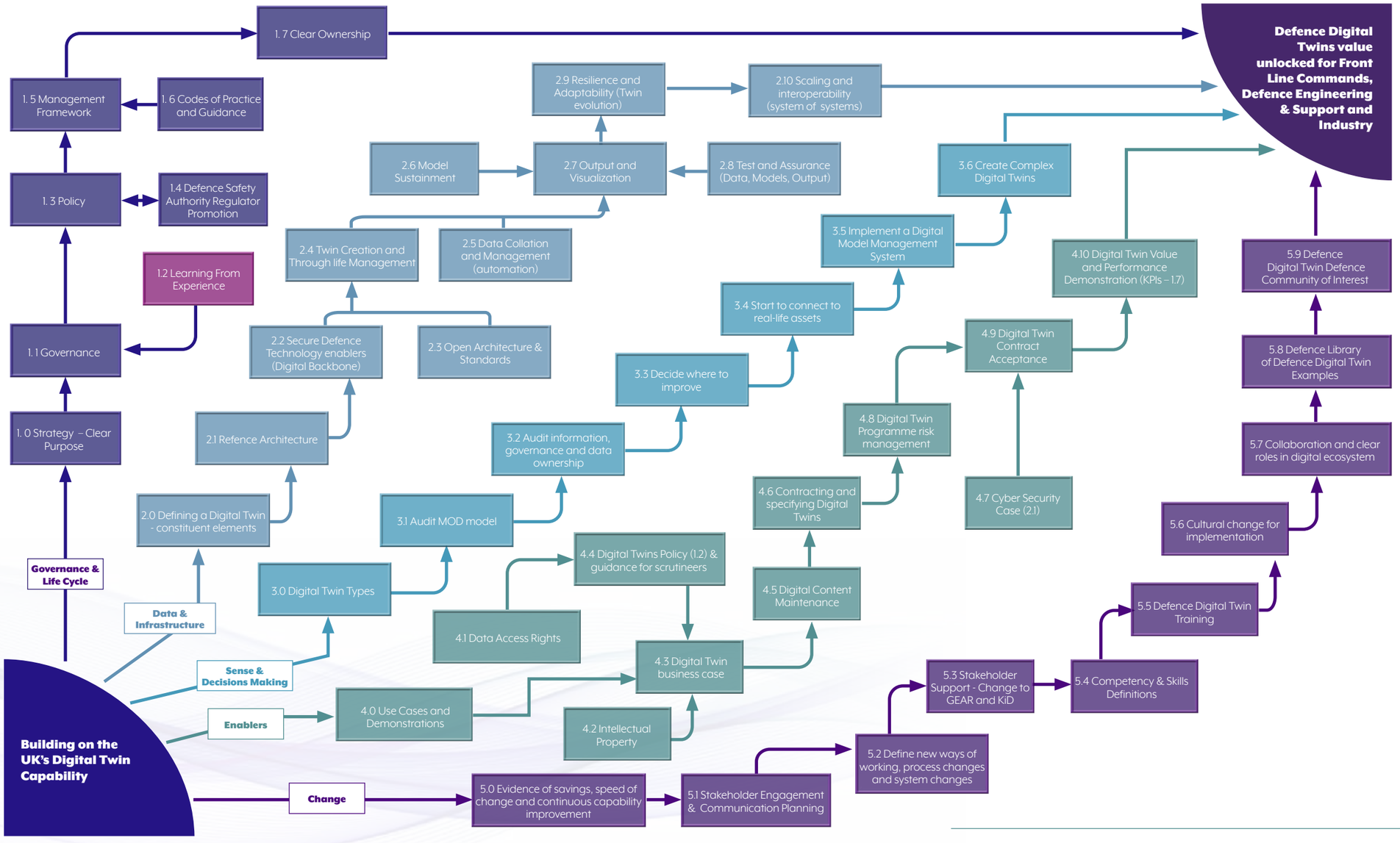
[5] W W Burke & G H Litwin. (1992). A Causal Model of Organizational Performance and Change. Journal of Management. Vol 18. No 3 (1992) p 529.

[6] https://www.cdbb.cam.ac.uk/DFTG/GeminiPrinciples

An overall Road Map Development Framework (Figure 2) was produced by a large group of 70 plus Team Defence Information participants and will be published separately

UK Defence Digital Twin Roadmap Development Framework

Figure 2 – UK Defence Digital Twin Road Map



The UK Defence Digital Twin Roadmap development framework

This Road Map has been created to show how the provision of effective information management across Defence will enable better, faster, secure and safer decisions, leading to financial savings, affordability, improved asset performance, increased capability drum beat development and support the UK's security priorities.

This Road Map considers the Centre For Digital Built Britain Gemini Principles.

The aim at this evolution of the Road Map is to identify what can be adopted or modified and what Defence needs to create.

SUMMARY OF WORK STREAM FINDINGS

Governance and Life Cycle

This work stream considered what Leadership direction would be necessary for Defence including the Defence Digital Twin vision and noting that the" Change" work stream considered the need to motivate the rest of the organisation to achieve the vision. The move to digitise Defence Engineering can be shown as an extension to the systems engineering life cycle through a digital mirror (Figure 3), an example of the extended life cycle developed by Rolls-Royce.

Figure 3 – Rolls-Royce Digital Physical Life Cycle

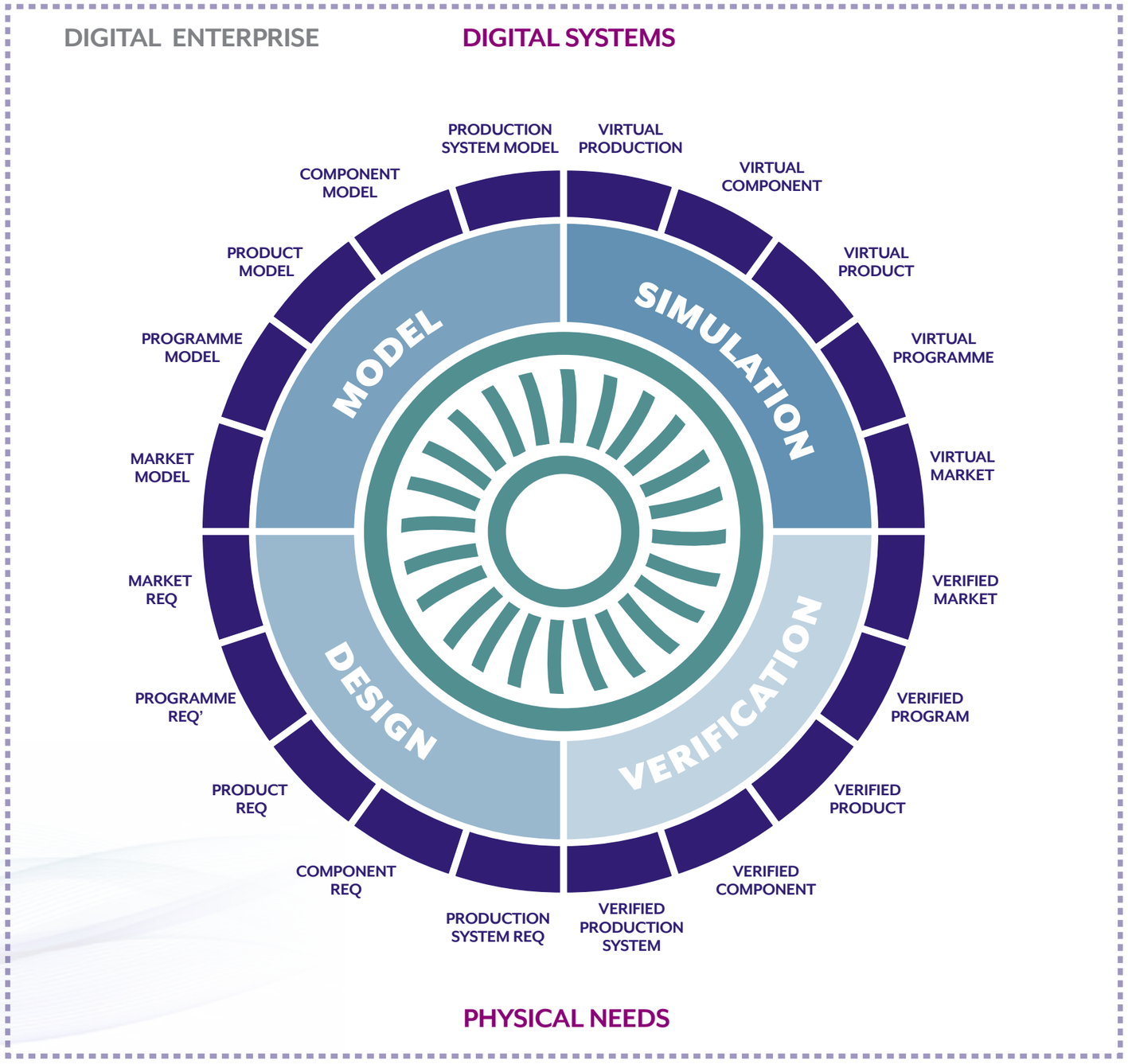
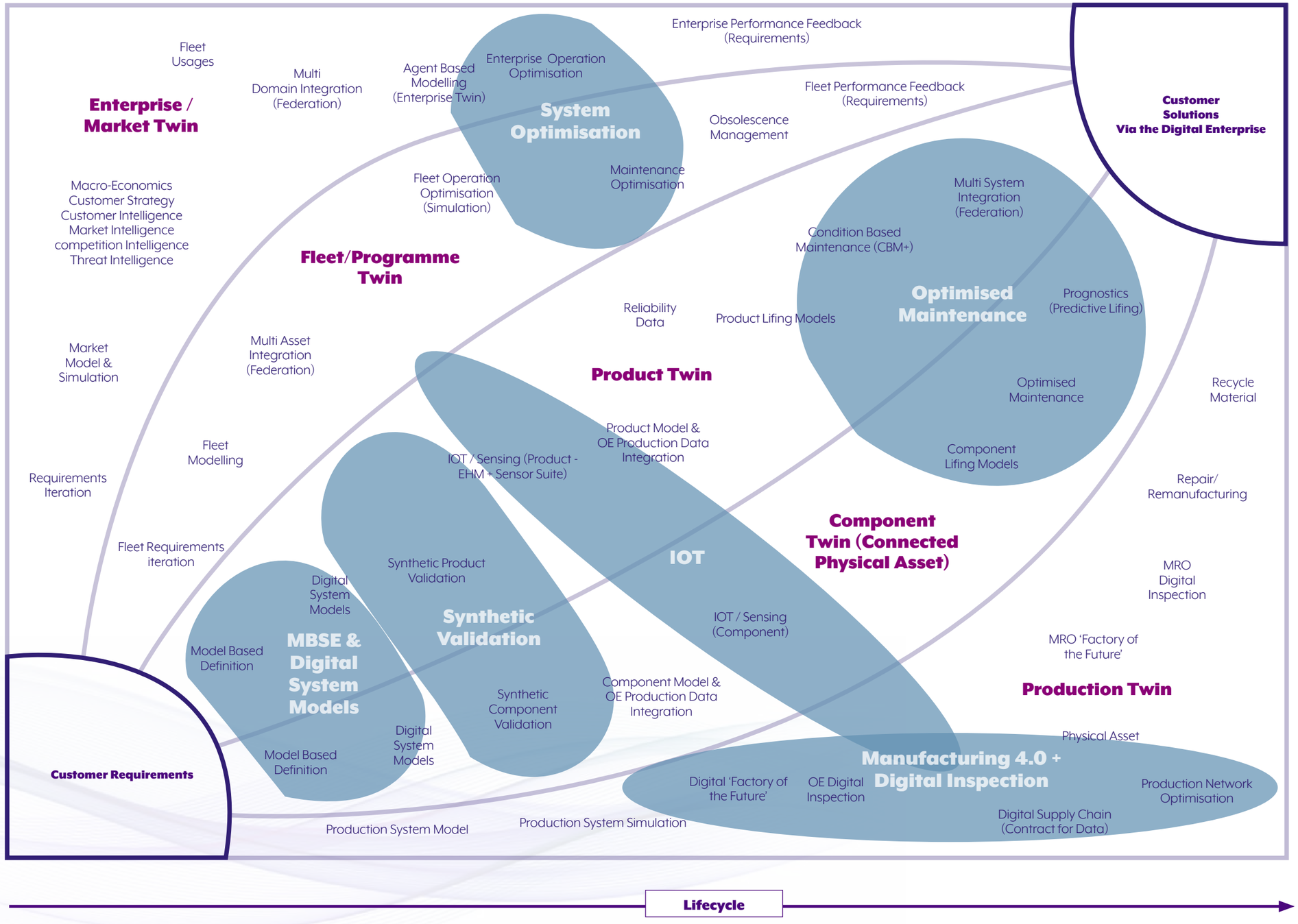


Figure 4- UK Defence Digital Twin Road Map - Twin Hierarchy



Building on the lifecycle model identified in Figure 3, a second road map was defined to complement the UK Defence Digital Twin Road Map, this derivative road map is intended to guide the practicable application of Digital Twins within the Defence enterprise. This map recognises the 'Digital Twin Hierarchy' and summarises the creation and aggregation of data within the enterprise from supply chains to components, components to products, products to fleets of products and finally into enterprise Digital Twins, as shown in Figure 4.

The Twin Hierarchy also identifies technology themes through the lifecycle. This paper seeks to facilitate the navigation of complementary (and foundational) technology developments that support Digital Twinning capability. For example, identifying a development route that covers digital system models and model-based engineering, Manufacturing 4.0 and contracting for data through supply chains, remote sensing and internet of things, synthetic validation, condition-based maintenance and enterprise modelling. The Twin Hierarchy plots a pathway for the derivation of clear Value Streams through the application of the robust and sustainable twins that are created by following the Digital Twin Roadmap.

The Twin Hierarchy addresses the Digital Twin uses through their lifecycle and across the digital enterprise. The model also supports recommendations pertinent to Governance. Value creation opportunities exist in isolation, within each horizontal twin layer, however greater potential is realised when vertical integration is also achieved. Governance and sponsorship of the Digital Twinning transformation must therefore reside throughout the Defence digital enterprise (as also must accountability for data ownership).

The final summary finding by this workstream relates to change management, adoption and particularly KPIs of value realisation. Digital Twinning is an opportunity available across a digital enterprise. Many pilot studies have suffered from the failure to recognise the requirement for a minimum level of 'digital maturity' (established data supply chains) in their pilot study environment. The twin value proposition/KPIs become heavily eroded as lengthy and retrospective efforts are required to digitise currently analogue process flows. Care must be taken to ensure that all the pathway recommendations within the Digital Twin Roadmap are closely followed, as are those in the Twin Hierarchy, to accelerate progress and assure the generation of value in realising a cost competitive Defence digital enterprise. The elements of this work stream include the following:

ITEM	TITLE	ADOPT	MODIFY	CREATE	RECOMMENDATION
1.0	**Strategy (Clear Purpose)**			✓	▸ Align with the Digital Strategy for Defence ▸ Maximise the use of industry standards and common technical standards to enable interoperability ▸ Define a coherent Digital Twin hierarchy ▸ Define the application of Digital Twins for Support, Asset Managements, Integrated Test and Evaluation, Logistics, etc.
1.1	**Governance**			✓	Defence Digital Twin enterprise principles: ▸ Single pan-Defence governance is put into place to drive coherence, trust, interoperability and re-use ▸ Coherent approvals and acquisition processes ▸ Assurance (Availability, Protection and Usability) of the digital function ▸ KPI to evaluate the Digital Twin
1.2	**Learning from experience**			✓	As Defence develops and explores the use of Digital Twins the good practice findings are captured in the data, digital backbone and Digital Twin standards.
1.3	**Policy**			✓	Digital Twin JSP created and supporting JSPs (935, 604 etc.) are updated.
1.4	**Defence Safety Authority Regulatory Promotion**			✓	The Defence Regulatory Authority promotes the use of Digital Twins to improve safety
1.5	**Management Framework**		✓		The Digital Twin methods, processes, task, resources and tools builds on Centre for Digital Built Britain work and this Road Map.
1.6	**Codes of Practice and Guidance and contracting standards**		✓		Codes of practice, guidance and contracting standards need to be developed however these can be based on ISO19650 [7], Industry 4.0 standards [8], JSP 440 [9] and 604 [10], etc. These need to provide the minimum standards that would enable the Digital Twin system to work and achieve the Gemini principles
1.7	**Clear Ownership**			✓	The framework needs Single Pan-Defence owner to enable Digital Twins to build to an Enterprise Twin.

All the above will need to be create specifically for Defence. The exception being (1.5) Management Framework and (1.6) Codes of Practice and Guidance and contracting standards. However, these need to provide the minimum standards that would enable the Digital Twin system to work and achieve the Gemini principles.

[7] ISO 19650 - Organization of information about building and civil engineering works - Information management using building information modelling (BIM).

[8] http://i40.semantic-interoperability.org/

[9] The Defence Manual of Security

[10] Defence networks governance

DATA AND INFRASTRUCTURE

Through the adoption of Digital Twins, we are looking to move Defence norms and values away from documents and towards data.

Digital Twin demands secure and resilient data sharing among Defence domains, manufacturers and allied forces, which is possible with robust data and open interoperability standards and supporting infrastructure enabled by the Defence Digital backbone. Development of such standards in Defence will be complex, time consuming and require intensive collaboration among all stakeholders.

The implementation of Digital Twin in defence will require a universally accepted Data Strategy, which will include new methodologies such as test and assurance processes for models and a "grey box" testing framework, to ensure a smooth transition period demonstrating the positive impact of technology.

Critical to success in this new approach to data sharing will be trust. Investment across the defence enterprise in practical demonstrations of security and protection of intellectual property will be essential. Such methods and processes will require rigorous testing plans that are often prone to public scrutiny for the trust in system design.

Digital Twin in defence should evolve over time in terms of complexity and scalability with addition/upgrade in equipment from many manufacturers and information owners across all domains e.g. warships. Although a federated defence enterprise vision in defence would be beneficial but how it will be achieved is questionable and there is no illusion that it will be easy to achieve. The elements of this work stream include:

ITEM	TITLE	ADOPT	MODIFY	CREATE	RECOMMENDATION
2.0	**Defining a Digital Twin - constituent elements**		✓		Based on ISO 19650 Part 1 and Guidance D including the architectural styles and onotologies.
2.1	**Reference Architecture**			✓	Defence creates a reference Digital Twin deployment of models that is defined by a Defence Standard.
2.2	**Secure Defence Technology enablers (Digital Backbone)**		✓		Upgrading MOD Cloud capabilities to a Secure Hyper-scale Cloud and changes to the supporting cyber secure JSP604 and JSP440.
2.3	**Open Architecture & Standards (Data, Models)**	✓			Use Industry 4.0 standards and other associated industry standards. Define the defence Digital Twin ontology/taxonomy.
2.4	**Twin Creation and Through-Life Management**		✓		Create Defence Standards based on ISO 19650 Part 1
2.5	**Data Collation and Management (automation)**		✓		Use Industry 4.0 standards however these will need to be amended to address Defence security requirements including the consideration of Fog and Edge computing
2.6	**Model Sustainment**		✓		Define the model sustainment processes based on ISO 19650 Part 3.
2.7	**Output and Visualisation**		✓		Based on industry standards create Defence Standards to: ▸ Improved data quality [11] ▸ Provide rigorous test and evaluation of Black Box ▸ Model validation both structural and physical ▸ Reinforced training & learning for machine learning ▸ Adopt standard models when practicable (electrical, software, mechanical)
2.8	**Test and Assurance (Data, Models, Output)**		✓		Adopt a Defence open architecture standard based on industry good practice to allow Digital Twins to be built from components to the enterprise.
2.9	**Resilience and Adaptability (Twin evolution)**		✓		Adopt a Defence open architecture standard based on industry good practice to allow Digital Twins to be built from components to the enterprise.
2.10	**Scaling and interoperability (system of systems)**			✓	Develop Defence Standards to enact the Digital Twin enterprise principles

Much the of the above can be based on existing industry standards however Defence will need to create its own reference architecture (2.1) and its approach to scaling and Digital Twin interoperability – building up from equipment to platforms (e.g. Planes, Vehicles and Dismounted Soldier Systems) to fleets and eventually capabilities. This will require principles and minimum standards to be defined.

[11] ISO 8000 Data quality

SENSE AND DECISION MAKING

The complex composition of information, models, supply chain and people require stringent decision making along the lifecycle in Defence Digital Twin programmes. This work stream fractionates the decision-making tools to ensure maximum value and accuracy in Defence Digital Twin journey.

There are hundreds of ways of digitally modelling something from simple data lists, flowcharts, diagrams, 3D CAD, 5D BIM, virtual reality walkthroughs, physics-based simulations, process simulations and more. The closer to reality the model is in look and feel the easier it is for people to understand but the harder it is to create, so a balance must be made between effort and value. A digital model becomes a Digital Twin when it is connected to real-life data and it shares behaviours and/ or characteristics with its physical counterpart. The data does not have to be a live stream, it might be incremental readings or even manually entered. But if a digital model cannot take in data from the real world it doesn't become a Digital Twin. In most cases the data will be automatically imported/ exported. Therefore, the digital model and the data stream from the real world must be aware of what the data is and where it maps to – including appropriate units alignment. This needs to be done in a robust fashion so that if there are changes to the type of data that it is flagged and checked as still accurate. An important aspect of enabling export and import is ensuring that information exchange is coherent and adequately described/captured to support the necessary analysis and decision support. Within the Defence environment, we will need to understand the importance of latency and delay in the information exchanges.

Once a Digital Twin is established, data can be analysed for trends to help real-life results prediction. Analysing all the instances of an outcome (e.g. failure of a bearing) will give a statistical probability of future failures and the appropriate remedy action. Data Science is generally the art of combining traditional statistical analysis with computer science techniques to create by training repeatable and testable models on scales that would be otherwise impossible. The reasoning behind this function's definition rather than classical statistics is the scale and volume of data involved; the advent of increased computer processing power has meant that statistical models can be built using black-box techniques (machine learning/AI) although these still need to be assured to provide confidence in the outputs. Machine Learning gets its name from the concept of the model parameters are not explicitly set, but instead 'learned' by the model by feeding it example data. Much like the advent of machine learning producing accurate predictive models, new techniques around neural networks (or Deep Learning) are showing remarkable accuracy with broad ranges of uses.

Accuracy of information, results and the fidelity of digital models are crucial in Defence Digital Twin programmes. The accuracy of these elements depends upon factors such as maintaining, communication capacity management and prioritisation, individual model performance analysis, data science tools and methods selection. It is vital to maintain an aligned configuration; if the physical asset changes, the digital twin will need to be changed to match. Digital methods such as PLM can be used to manage configurations between physical and digital assets. The complex nested Digital Twins at programme level can be difficult to manage as small changes in digital models can have very big effects on data outputs if the changes are not managed effectively. Overall, MOD will require set of principles for standardising Digital Twin development that can be adopted by wider organisation and stakeholders. The elements of this work stream include the following:

ITEM	TITLE	ADOPT	MODIFY	CREATE	RECOMMENDATION
3.0	**Identify Key Digital Model Types**	✓			▸ List out all the main digital model types that MOD already uses, and categorise the different tools and methods used to create them. ▸ The development of insertion policies associated with each model in line with standards such as the European Component Oriented Architecture or Future Airborne Capability Environment.
3.1	**Audit MOD models**	✓			With Stakeholders: ▸ Confirm the MOD Model can be un-picked and understood by future generations, so people know what it's doing? ▸ Confirm the MOD Model has an easy IO method, like an open API, or standard IO with ASCII, CSV etc? ▸ Confirm the MOD Model offers real value? ▸ Confirm the MOD Model has proven accuracy?
3.2	**Audit information, governance and data ownership**	✓			▸ Join consortia, organisation and standards bodies that are defining approaches and standards associated with Digital Twins; ▸ Ensure all equipment, modelling, data extraction, transport and analytical tools provide digital data in a usable format; ▸ Gain data access and exploitation rights for existing equipment, modelling, data extraction, transport and analytical tools; ▸ Ensure data access and exploitation rights for future equipment, modelling, data extraction, transport and analytical tools from point of purchase; ▸ Build information and data adapters to allow data to be exploited; ▸ Maintain a library/catalogue of information and data adapters for exploitation through life and across Defence.
3.3	**Decide where to improve**		✓	✓	▸ Re-model where needed, adding value as a must if doing so; ▸ Standardise on methods and tools as much as possible, focussing on openness and interoperability; ▸ Identify nested and connected requirements and start creating complex models.
3.4	**Start to connect to real-life assets**		✓	✓	▸ Use a robust standard method as much as possible. Don't re-invent the wheel each time with bespoke Defence Standards and solutions; ▸ Extract value, store data for future analysis.
3.5	**Implement a Digital Model Management System**			✓	▸ Decide how to manage change, configuration, validation; ▸ Create or use an Enterprise Architecture that delivers now, and in the future.
3.6	**Create Complex Digital Twins**			✓	▸ Connect digital models together in a robust way; ▸ Increase the accuracy and performance of individual models; ▸ Optimise system model performance by running high-resource models at the right time.
3.7	**Iterate 3.3 to 3.6 until you reach the required Platform level vision**			✓	

Some above elements require adoption as per the current industrial practices whereas Defence needs wider coordination among different standards, acquisition processes, GEAR[12], etc., for realising different types of Digital Twin and modelling based on mission requirements. A shift to Model-Based System Engineering (MBSE) and Model Based Design (MBD) approaches for managing information and digital models is required to support virtual testing and evaluations activities.

[12] Engineering Skills Framework - Gov.uk

ENABLERS

The key success of Digital Twin in defence ecosystem substantially depends on trust and how data and digital models can flow freely and securely among different users and stakeholders, along with shorter development lead times to achieve practical beneficial capabilities and value.

This work stream articulates different enablers to simplify the security, cost and benefit implications along the Digital Twin lifecycle in defence support.

The implications of IP ownership, export control, security requirements, information resilience and technical solutions & standards are crucial as data is created, stored and accessed in or by a Digital Twin environment. Current defence legal frameworks, standards and practices may not be suitable for thorough use and implementation of Digital Twin. Defence policy must articulate the requirement that the value of Digital Twins is realised for defence customers and across industry. The policies for Digital Twin can be complex to create, communicate and gather support across the range of stakeholders. Due to their complex networked and cloud-based systems, Digital Twins may have high costs and security implications. Existing MOD policy and mandated standards already require specific attention to issues of obsolescence and cyber security, but these will need substantial review to ensure that the new Digital Twin ecosystem grows in scale and capability in an optimal and secure way.

Existing legal IP frameworks are typically not designed specifically to cater for what should or should not be done in the context of Digital Twinning. An understanding of all legal repercussions within the defence stakeholder ecosystem is vital to define how MOD, Original Equipment Manufacturer/Primes and Service provider interface and collaborate with each other to gain value collectively, as shown in Figure 5 - Data flows. Issues such as warranties for performance, liabilities associated with misuse, how compliance can be monitored and what constitutes a trade secret may need new approaches in this context. However, there will still be a need for organisations to capture and secure rights in order to make the case for investment. Existing law and regulatory processes around data protection and cyber security may also be challenged by aspects of the Digital Twin approach. Data ownership, data governance and access control are all important features affecting IP in this area.

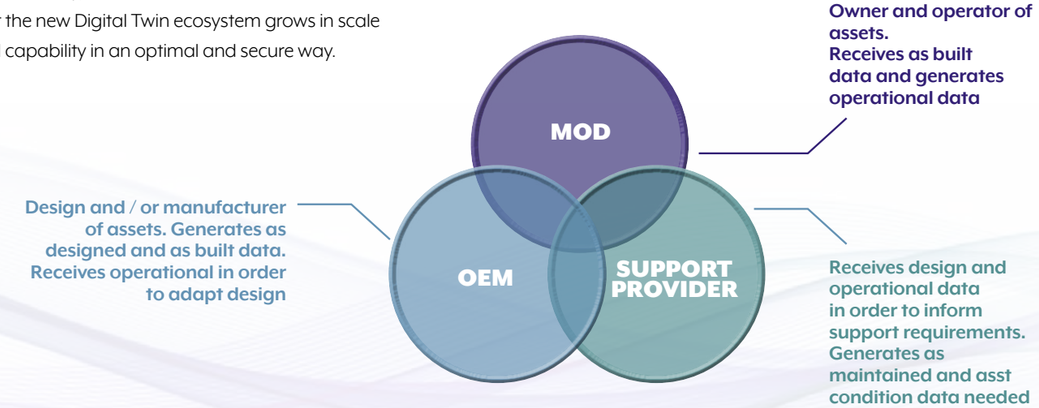


Figure 5 - Data flows

Emerging technologies such as distributed ledgers are being promoted to create "smart contracts": computer programs which run automatically, in whole or in part, without the need for human intervention. They can be used to record and perform the obligations of a legally binding contract. Smart contracts can take the form of a mixture of both natural language and coded terms or even a contract which is written wholly in code. Smart contracts could increase productivity and certainty in business and reduce the need for individual contracting parties to have to trust each other with the trust residing in the code. Smart contracts should be considered as a way of allowing speed of access to intellectual property, to manage the data layers and the resultant new intellectual property. There are questions about the circumstances in which a smart contract will be legally binding, how smart contracts are to be interpreted, and the remedies available where the contract does not perform as intended and further investigation is required. The elements of this work stream include the following:

ITEM	TITLE	ADOPT	MODIFY	CREATE	RECOMMENDATION
4.0	**Use Cases and Demonstrations**		✓		Logistics, Asset Management and Support use case for Digital Twins will need to be created to provide a library of use cases (based on Cranfield academic model).
4.1	**Data Access Rights**		✓		Develop standards based on ISO 19650 Guidance and use existing DEFCONs.
4.2	**Intellectual Property**		✓		Develop standards based on ISO 19650 Guidance and use existing DEFCONs.
4.3	**Digital Twin business case**		✓		Build on Industry good practice examples from different domains and use the evidence developed by the Centre for Digital Built Britain.
4.4	**Digital Twins Policy (1.2) & guidance for scrutineers**		✓		Provide guidance for investment appraisal and evaluation and update JSP 507.
4.5	**Digital Content Maintenance**		✓		
4.6	**Contracting and specifying Digital Twins**		✓		Create a Defence Standard based on ISO 19650 Guidance E and existing Industry good practice. New Defence assets should be architected to enable the use of Digital Twin technologies and the benefits they bring.
4.7	**Cyber Security Case**		✓		Change JSP604 and JSP440 to define what is required and how vulnerabilities and threats managed based on ISO 19650.
4.8	**Digital Twin Programme risk management**			✓	Expand Defence Knowledge In Defence (KiD) guidance.
4.9	**Digital Twin Contract Acceptance**		✓		Create Defence KiD guidance based on ISO 19650 Part 2.
4.10	**Digital Twin Value and Performance Demonstration (KPIs)**		✓		Use industry good practices examples develop by the Centre for Digital Built Britain.

Much of the above elements can be adapted as per the existing best practices and standards, however Defence will require new approaches/frameworks to manage Digital twin programme risks (4.6). Several emerging risks around interoperability, integration and dependencies on Defence Systems will require significant attention to ensure effective Digital Twin/s system delivery.

CHANGE

Change is never easy but is a fundamental key focus area in the norms and values of the UK Defence to successfully adopt the right culture, behaviours and mindsets needed for transformation over time.

In adopting Digital Twins, leaders in Defence require transition to be able to specify their needs from a Digital Twin, then use and exploit the outputs. Proactively attending to people and organisational concerns are the key to managing risks associated to transformational activities.

Digital Twin requires Defence to move from traditional disaggregated cold data stores and documents for decision making to new Cloud based data models and capabilities. The collaborative efforts among different stakeholders, from identifying to sustaining the change are hard to manage due to complexity of supply chain and contracts rapid technology change and evolution. Managing and achieving a sustainable pace of change to enable the adoption of Digital Twin in Defence will require coordinated efforts by policy makers (1.3), code of practice (1.6) and governance (1.1) to ensure its effectiveness and efficiency throughout adopters' value chains. Governance in defence will play a key role in deriving policies whose mandates identify and require practitioners to address Digital Twin programme risks.

This workstream breaks this down from realisation/necessity to make and sustain the change for Digital Twins in the Defence ecosystem. The key elements of this include the following:

ITEM	TITLE	ADOPT	MODIFY	CREATE	RECOMMENDATION
5.0	**Make the case - Evidence of opportunity, benefits, savings,**	✓			Use examples developed by the Centre for Digital Built Britain.
5.1	**Make it ready - Stakeholder engagement and communication planning.**			✓	Use Team Defence Information to create a community of interest with Key MOD champions.
5.2	**Define new ways of working, process changes and system changes.**		✓		Update GEAR and KiD to support the adoption of Digital Twins. ▸ KiD Simulation ▸ Modelling advice
5.3	**Make the change - Stakeholder Support - Change to GEAR and KiD**		✓		DDaT Capability Framework; https://www.gov.uk/government/collections/digital-data-and-technology-profession-capability-framework
5.4	**Competency and Skills Definitions and Development**			✓	Develop Defence Digital Twin specialist training benchmarking best practice.
5.5	**Defence Digital Twin Training**			✓	Develop and implement a change programme using example projects, community of interest and tools to help embed leadership behaviour and approaches.
5.6	**Cultural change for implementation e.g., digital mindset**			✓	Create framework for data ecosystem and deploy in future creation of Digital Twin.
5.7	**Sustain the change - Collaboration and clear roles in digital ecosystem**			✓	Between MOD, Original Equipment Manufacturer /Prime and Support Provider, all are critical and can benefit
5.8	**Defence Library of Defence Digital Twin Examples**			✓	Logistics, Asset Management and Support use case for Digital Twins will need to be created to provide a library of use cases (based on Cranfield academic model).
5.9	**Defence Digital Twin Defence Community of Interest**			✓	Use Team Defence Information to create a community of interest to help develop Policy, Standards, Guidance and Training.

Much of the above elements need to be created for Defence with some exceptions for Stakeholder Support (5.2) and Competency & Skills Definitions (5.3) by modifying as per GEAR, KiD and DDaT framework. Training will be required to enable technology adoption. The collection of evidence for change (5.0) can be adapted as per current best practices to check the effectiveness of the required change and further capability development in Digital Twin Defence programmes.

The MOD Transformation and Change community have developed the Change Management in Defence (CMiD) Methodology and toolkit can be accessed via MODNet on their CMiD Teams Site. The toolkit provides templates users are able to access and use. The Transformation Change Community can be contacted at Transformation-ChangeCommunity@mod.gov.uk for more information.

NEXT STEPS

Although in some military domains we are well on our way to the implementation of Digital Twins for Defence, there is still a long way to go to realising the full benefits.

In each of the five different work streams we have identified further work and development challenges, but there are some core overarching activities that are also required. The following four step plan highlights the main activities required to ensure the Defence stakeholders can maximise the potential value of Digital Twins, lowering through life costs and enabling intelligent decision support, see Figure 6 - Next Steps below.

Figure 6 - Next Steps

STEP 1

- Lean in and Learn through the Community of Interest
- Establish Minimum Viable Products

STEP 2

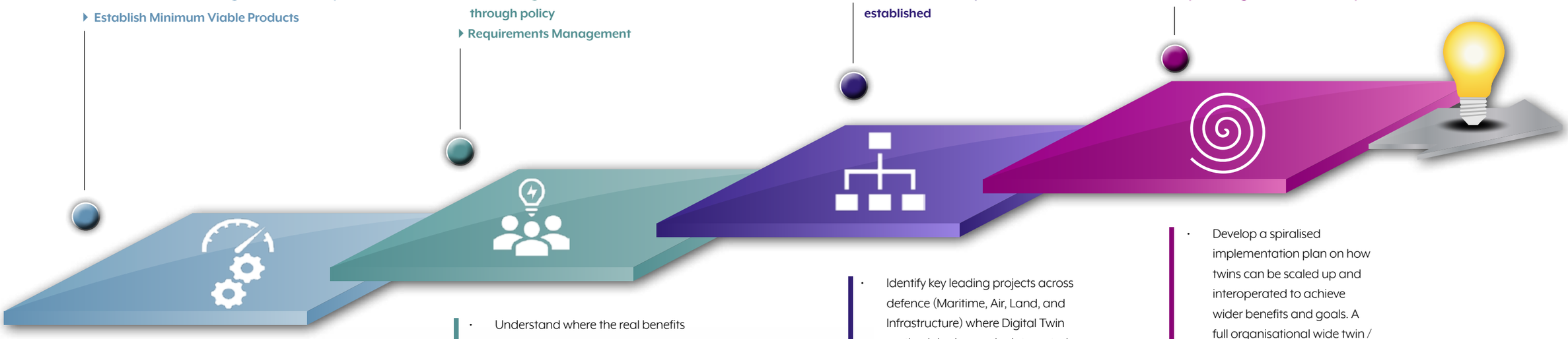
- Establishing the vision and direction through policy
- Requirements Management

STEP 3

- Networks of viable products established

STEP 4

- Spiral Integration Plan Developed



- We need to agree and define a working group of individuals across MOD who are responsible for Digital Twin implementation.
- Learn from early proof of value.
- Publish the Defence Strategy and Policy

- Understand where the real benefits can be derived, considering project specifics across defence and start to build the requirements and business case.
- Create the Defence Standards, define the GEAR products, KiD guidance and complete the training needs analysis

- Identify key leading projects across defence (Maritime, Air, Land, and Infrastructure) where Digital Twin methodologies can be integrated into, in order to create a series of leading MVPs to test the concepts using secure MODCloud solutions.

- Develop a spiralised implementation plan on how twins can be scaled up and interoperated to achieve wider benefits and goals. A full organisational wide twin / network cannot be built in one go but instead stepped up with each iteration loop.

Step 2/3 in the next 24 Months

In the next 6 Months Step 1

TIMELINE – STARTING IMMEDIATELY

TEAM DEFENCE INFORMATION

6A Pinkers Court
Briarlands Office Park
Gloucester Road
Rudgeway
Bristol
BS35 3QH

+44 (0)1454 410 550
secretariat@teamdefence.info