
cds
Defence
&Security

cds Defence &Security

Safe, Secure, and Sustainable by Design

Ryan Griffin

Head of Business Unit

Capability Sustainment

Martin Nash

Head of Business Unit

Cyber Security and Information Assurance Services

Introduction

Ryan Griffin

Head of Business Unit

Capability Sustainment

Maximising equipment readiness and long-term operational resilience

A background in delivering pan-defence projects in the Support domain for the UK Ministry of Defence and holds prominent positions on international standards committees. As an Incorporated Engineer with a Masters degree in Through-Life System Sustainment, Ryan is passionate with his participation in thought leadership to drive improvements in defence equipment dependability.

Ryan joined CDS DS in 2024 and manages a multi-discipline portfolio with projects in all domains, including space. He has led the development of creating the digital engineering ecosystem and is currently exploring the secure use of Artificial Intelligence for Lifecycle Management.

- SX000i Steering Committee
- IPS Defence Interest Group (industry)
- TDI Working Groups (inc. Do Support Better)
- CLEP People Lead

Martin Nash

Head of Business Unit

Cyber Security and Information Assurance Services

Managing evolving cyber threats and assuring digital resilience.

As a long-time veteran (left the RN in 2006), Martin joined CDS DS as the Head of CS&IA Services in 2020 to formally establish a new business unit. Since then, the team has grown from 12 to 65+.

Martin leads a team of security cleared, and cyber security certified professionals providing a wide breadth of cyber security expertise and services that enable clients to operate securely, develop the right security culture and realise the benefits of their technology and cyber security investments. Martin is passionate about the protection of information assets through-life and strives to enable businesses with ongoing, assured operational resilience.

- ADS Cyber Resilience Group
- NCSC Assessment Panel for Academia
- Board member on a regional Cyber Resilience Centre

CDS Defence & Security in numbers

30
Years in Operation

200
People

4
Business Units

3
Global Locations

Driving “Resilient by Design”

SAFE BY DESIGN

- Designing equipment not just to perform its mission, but to **operate, be maintained, and ultimately disposed of safely** throughout its service life.
- Identifying and mitigating **hazards** and the potential harm to users and other personnel.
- Ensuring the organisational culture, policy and procedures also enable **safe operation**.

SECURE BY DESIGN

- **7 SbD principles** based on understanding, identifying, managing and mitigating security risk.
- Designing equipment not just to deliver capability, but to remain **resilient, trusted, and protected** against evolving cyber threats throughout its service life.
- Includes a focus on organisational IT systems, supply chain, culture, policy, process, and procedures which also support risk managed **cyber security and secure design** of equipment.

SUSTAINABLE BY DESIGN

- Designing equipment not just for the mission, but to be **sustained efficiently** throughout its service life.
- Ensuring **availability**, and **environmental sustainability** requirements are balanced with **whole life cost.**
- Integrating **Human Factors** into the design to ensure user friendliness and reduce the **training** burden.

Why is Resilience Important in Design

UK DEFENCE JOURNAL

Type 45 Destroyer has spent most of its life in maintenance

The Guardian

Army faces crisis in Apache pilots fiasco

Pilot training for Britain's new US-designed Apache attack helicopters is running three years late and any further delay would lead to a serious capability gap for the armed forces, an independent watchdog warns in a damning report released today.

THE TIMES

£2-30 IN CORONET DE D Wed 24-2024

Army, Navy and RAF say their lives are at risk from poor equipment

Cybersecurity INSIDERS

Hackers launch cyber attacks on British Army, Royal Navy and Office for Nuclear Security

By Naveen Goud [Join Cybersecurity Insiders]

MOD data breach shows supply chain security continues to be a top priority

Not for the first time, a Western government agency suffered a major data breach where third-party contractors were exploited as a likely weak link.

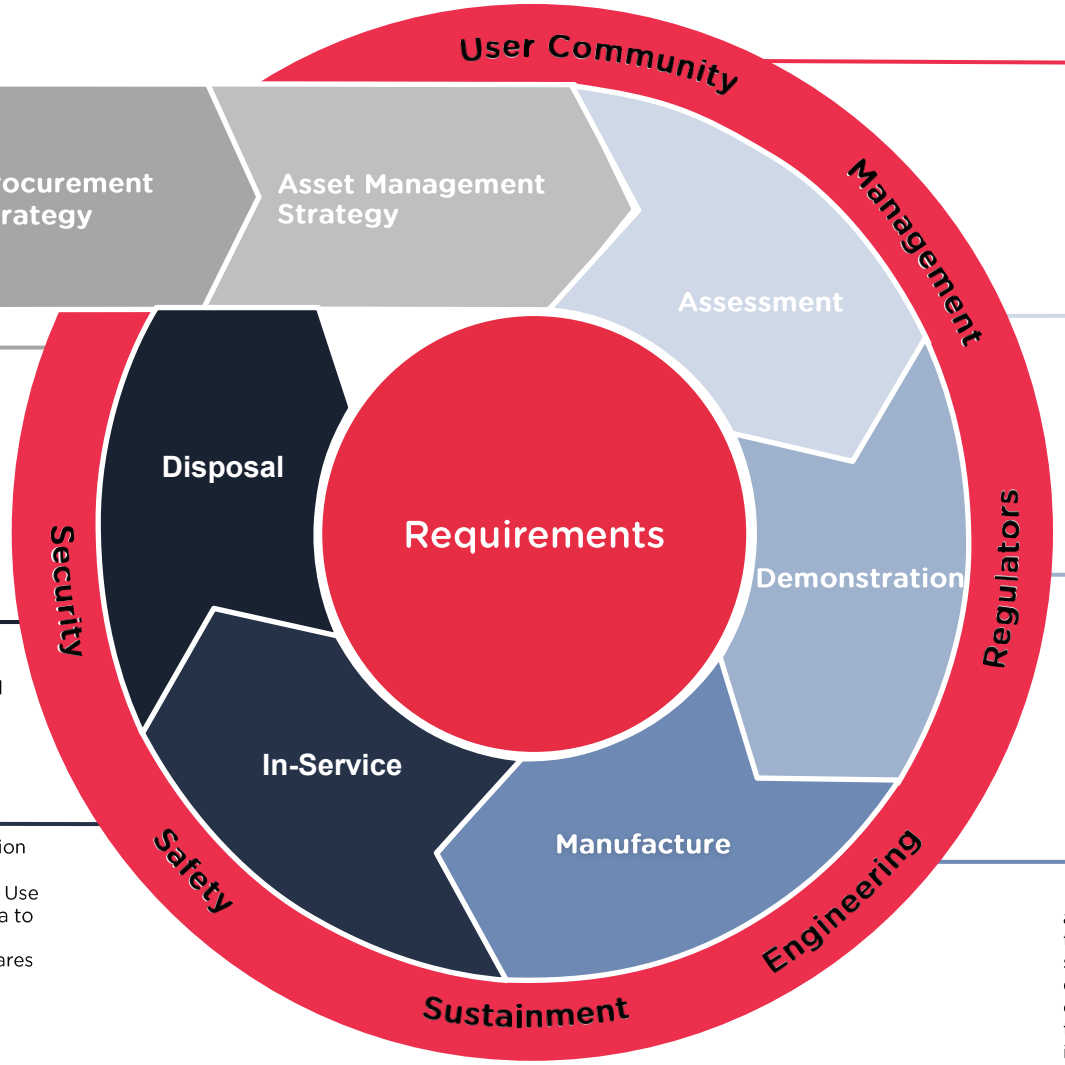
EXPERT COMMENT PUBLISHED 9 MAY 2024 — 3 MINUTE READ

Where “Resilient By Design” Sits within Asset Management

Asset Management 10-box Model (ISO 55000)

Lifecycle Delivery Applied in a Defence Environment

Conceptual Documents → **Procurement Strategy** → **Asset Management Strategy**



Concept & Strategy: Embed safety, security and sustainability objectives in capability strategies and enterprise planning. Ensure Defence Lines of Development (DLoDs) include explicit Safe/Secure/Sustainable design intent. Use early threat, hazard and support analyses to influence future capability choices.

Disposal: Ensure safe and secure decommissioning, dismantling, and data sanitisation. Minimise environmental and safety hazards in disposal. Reuse or recycle components while maintaining security and safety controls.

In-Service: Maintain safety certification and security assurance through change management and continuous assurance. Use incident, vulnerability, and reliability data to update design artefacts. Manage configuration, software updates, and spares securely and safely. Sustain integrated product support to ensure capability readiness.

Requirements: Define high-level safety, security and sustainment requirements in the Concept of Analysis and System Requirements Document. Identify critical assets, safety functions, and through-life support dependencies. Conduct early trade-offs (performance vs. safety/security/sustain burden).Promote integrated thinking through joint concept studies and IPT collaboration.

Assessment: Develop detailed Safety, Security and Supportability Cases and plans. Carry out risk, vulnerability, and supportability analyses to inform design selection. Ensure assurance evidence and models (FMECA, threat analysis, LORA) are aligned across domains. Use design reviews to verify emerging system concepts meet “resilient by design” principles.

Demonstration: Verify that designs meet safety integrity levels, security accreditation boundaries, and support metrics (MTBF, MTTR). Integrate safety and security testing into developmental and acceptance trials. Validate logistic support elements, spares, and training against design assumptions. Maintain configuration control to protect certified and accredited design baselines.

Manufacture: Apply safe manufacturing and cyber-secure supply chain practices. Verify that production processes preserve safety and security assurance evidence. Ensure support documentation (maintenance data, fault codes, digital twins) is accurate and secure. Embed through-life quality and assurance monitoring into industrial partners.

Mapping Standards

Overarching

ISO 55000 Asset Management
PAS 280 – Through-Life Engineering Services

Risk Management

ISO 31000 – Risk Management

Lifecycle Delivery

- IEC 61508 / RTCA D0178c – Safety Critical Software
- IEC 61511 / RTCA DO254 – Safety Critical Systems
- ASD/AIA SX000i – IPS Requirements
- ASD/AIA S1000D – Technical Publications
- ASD/AIA S2000M – Material Management
- ASD/AIA S3000L – Logistics Support Analysis
- ASD/AIA S4000P – Preventative Maintenance
- ASD/AIA S5000F - Feedback
- ASD/AIA S6000T - Training
- ISO / IEC 62402 – Obsolescence Management
- ISO 14001 – Environmental Management

Purpose and Context

No current provision for cyber security within the ISO 55000.

We would recommend that Cybersecurity is captured within the “Purpose and Context” as a key element to be included in every area.

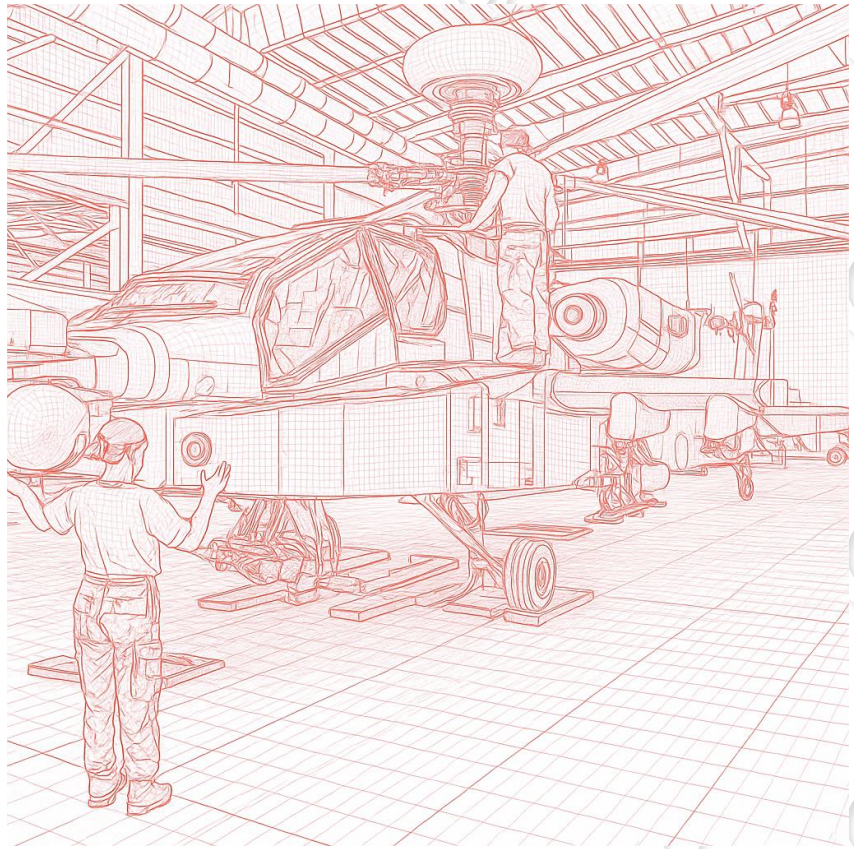
- NIST – Cyber Security in the US
- NCSC – Cyber Assessment Framework (UK)
- ISO 27001 – Information Security
- ISO 27002 – Security Controls
- ISO 27017 – Cloud Security

More Integrated Thinking

The key to success is ensuring the setting up of Integrated Design Teams (IDT's). These IDT's are critical to:

- Bring capability, safety, security, and sustainability together from the outset.
- Enable early risk reduction and avoid costly rework.
- Provide integrated assurance across the products lifecycle (CADMID).
- Maintain through-life continuity from concept to disposal.
- Align stakeholders and regulators in one forum.

IDTs make sure capability is designed as a whole system — effective in battle, safe to use, resilient to threats, and sustainable through life



Defence Asset Lifecycle

Concept → Assessment → Demonstration → Manufacture → In-Service → Disposal

Designing equipment not just to deliver effect, but to be safe, resilient, and supportable from the outset.

Aim: Influence Requirements

Concept | Assessment | Demonstration | Manufacture | In-Service | Disposal

cds Defence & Security

SECURE BY DESIGN

SAFE BY DESIGN

SUSTAINABLE BY DESIGN

Establish Personnel

- Governance structure and reporting cadence to Senior Responsible Owner (SRO)
- Establish an integrated Design Team consisting of system engineers, support, safety and security.
- Committees to cover safety, security, supportability, training, and human factors.
- Stakeholder management plans to ensure effective communication

Security Strategy & Management Plan

SbD Principle 1: Understand and Define the Context.

SD Principle 2: Plan Security Activities.

SbD Principle 3: Implement Continuous Risk Management.

Safety and Environment Strategy and Plan

Establish a structured safety management plan to define responsibilities, methods, and governance for safety assurance throughout the lifecycle.

Support Strategy and Plan

Produce a plan manage support application. Covering design for support (supportability analysis), design of support and managing of support through life including; spares, training, documentation, support equipment, and facilities

Define User Requirements

- Embed safety so it is treated as a fundamental design driver, not an add-on.
- Embed availability, maintainability, sustainability, and cost-of-ownership targets from the outset.
- Embed security controls and physical security measures from the outset.

Preliminary Analysis

Conduct threat, vulnerability, and risk modelling for proposed architectures. Define baseline security risks & requirements. Identify supply chain security and information assurance needs.

Preliminary Analysis

Perform preliminary hazard and system safety analyses (PHA, SHA). Establish a Safety Case strategy. Integrate human factors and survivability principles into early designs.

Preliminary Analysis

Develop the initial through-life cost, carbon, and availability model. Influence designs for maintainability, reliability, and sustainability. Identify support concepts (e.g., contractor vs. organic) and critical logistic risks.

Aim: Influence Requirements

Concept → Assessment → Demonstration → Manufacture → In-Service → Disposal

cds Defence & Security

SECURE BY DESIGN

Organisational Security

SbD Principle 5: Engage & Manage the Supply Chain

This includes orgnisational culture training and awareness.

Trade off Analysis & Risk Capture

- Use modelling, simulation, and concept demonstrators to explore trade-offs and validate assumptions
- Conduct integrated risk assessments covering capability, hazards, cyber threats, and support risks, to avoid siloed decision-making.
- Ensure risks are managed not only for operation, but also for maintenance, upgrades, and disposal.
- Involve operators, maintainers, cyber/security specialists, and regulators together in concept reviews.

System Requirements & Acceptance Testing Plan

Setting the System Requirements and how they are to be accepted. 85% of through-life cost will become committed by these requirements

- Support – Including reliability, maintainability, transportability, support resources etc.

Security – requirements to ensure the system remains secure.

SbD Principle 4: Define Security Controls

Safety – ensuring each requirement does not hinder safe operation and maintenance.

Security Assurance

Establishing the framework for through life risk management of cyber security risks.

SAFE BY DESIGN

Establish LSAR

- Record all initial analysis in the LSAR to ensure tracking of information through-life.
- Conduct initial modelling on the LSAR to determine forecasted availability, safety, and whole life cost.

Safety Case

Collation of evidence that demonstrates that the risks are sufficiently identified, managed and mitigated too As Low as Responsibly Practical (ALARP).

SUSTAINABLE BY DESIGN

Supportability Case

Collation of evidence that demonstrates that the risks of not meeting the mission, availability target and environmental sustainability.

Concept | Assessment | Demonstration | Manufacture | In-Service | Disposal

Building confidence that the system design meets safety, security, and support goals before entering service.

Aim: Influencing Design

Concept → Assessment → Demonstration → Manufacture → In-Service → Disposal

cds Defence & Security

SECURE BY DESIGN

SAFE BY DESIGN

SUSTAINABLE BY DESIGN

Configuration Management

- Configuration control to protect design integrity and assurance baselines
- Maintain control of design baselines so that modifications to hardware, software, or support solutions are properly assessed for safety, security, and logistic impact.

Failure Analysis

- Analysis conducted on both hardware and software components of a system.
- Identification of failures that could cause harm to people, including the loss of sensitive information that could lead to loss of life.
- Identification of failures that impact the mission and availability.
- Identification of failures that impact the environment.
- Use of different analysis methods: FMECA / FMEA / HAZOPS / FTA / ETA / STPA

SbD Principle 6: Assure, Verify and Test

- Apply secure coding, configuration, processes, and hardening practices to the asset.
- Conduct asset penetration testing, vulnerability assessments, and red teaming.

Dependability

Influencing the asset design:

- Reliability
- Maintainability & testability, including tools / test equipment
- System safety
- Transportability
- Component / Material selection – supply vulnerabilities and environmental impact

Reliability Centred Maintenance (RCM)

A risk-based approach to maintenance scheduling. Using the results of failure analysis to identify Items/systems that can not be allowed to fail therefore require preventative maintenance.

- **Cyber Security -** Items / systems that are required to keep sensitive information secure
- **Safety -** Items / systems that are required to keep operators and maintainers safe.
- **Sustain -** Items / systems that are mission critical and/or protect the environment from harmful elements.

Aim: Influencing Design

Concept | Assessment | Demonstration | Manufacture | In-Service | Disposal

cds Defence & Security

SECURE BY DESIGN

SAFE BY DESIGN

SUSTAINABLE BY DESIGN

Task Analysis

Identification, analysis and documentation of all steps required to operate and maintain a system

- **Cyber Security -** Review of information needed by operators and maintainers - Identify areas that are vulnerable to insider threat
- Operator Task Analysis includes workload, ergonomics, qualifications, human-machine interfaces and safety controls.
- Maintenance Task Analysis includes time to repair, frequency, space envelopes, required qualifications, and safety controls.

SbD Principle 6: Assure, Verify and Test

Conduct continuous threat, vulnerability and vetting of any suppliers and/or service providers to the asset or wider capability.

Manage and respond to security incidents.

Digital Resource Plan

- What digital infrastructure is needed and where. Including software, hardware and connectivity.
- How the software, hardware and connectivity will be sustained through-life.
- Consideration of software licensing structures and costs.
- **Cyber Security -** Who and how software security patches are going to rolled out and assuring compliance

Disposal Planning

Disposal happens through-out in-service not just at the end of the asset's life.

- Based on environmental considerations the following disposal options should be considered in order of:
  1. Prevention
  2. Reduce
  3. Reuse
  4. Recycle
  5. Energy Recovery
  6. Disposal (landfill)
- **Cyber Security -** Who and how security related items (e.g. data drives) will be disposed of securely

Level of Repair Analysis

- First a noneconomic decision criteria to make the initial support decisions
- Then an economic model to determine the most cost effective & environmentally friendly to provide support for the system

Aim: Influencing Design

Concept | Assessment | Demonstration | Manufacture | In-Service | Disposal

cds Defence & Security

SECURE BY DESIGN

Security Controls

SbD Principle 4: Define Security Controls

Review and update security controls for the system.

SAFE BY DESIGN

Hazard Controls

Identification of Hazard and Accident Controls (risk mitigation) for necessary support facilities, safe use, operating environments, transportation and storage.

SUSTAINABLE BY DESIGN

Support Resource Planning

Identification of necessary resources to sustain the asset. Facilities, infrastructure, spares, support/test equipment and personnel.

Technical Publications & Training Package

Training and technical publications are key to ensuring personnel can operate, maintain, and dispose of equipment effectively, safely, and securely.

- **Training -** Based on the Training Needs Analysis (TNA) - develop and verify training materials for maintenance and operating procedures to ensure safe and secure use in service.
- **Technical Publications -** Create and validate user manuals, maintenance instructions, and e-learning resources; capturing warnings and cautions.

System Demonstration and Acceptance

- Use prototypes, test rigs, and representative environments to validate operational safety, resilience under attack, and maintainability in realistic conditions
- Validate safety, security, and sustainability requirements through trials, modelling, and testing
- Conduct formal safety tests (e.g., fail-safe tests, emergency shutdowns, tolerance and overload conditions).
- Verify operator workload, ergonomics, and human-machine interfaces, including those that prevent unsafe actions or conditions.

Security Assurance

Collation of evidence that demonstrates that the organisation and asset security risks are sufficiently identified, managed and mitigated within risk appetites

Safety Case

Collation of evidence that demonstrates that the risks are sufficiently identified, managed and mitigate too As Low as Responsibly Practical (ALARP).

Supportability Case

Collation of evidence that demonstrates that the risks of not meeting the mission, availability target and environmental sustainability.

Concept → Assessment → Demonstration → Manufacture → In-Service → Disposal

Sustaining safe, resilient, and affordable operations through-life whilst ensuring equipment is safely decommissioned, securely disposed, and sustainably managed.

Aim: Influence Optimisation

Concept → Assessment → Demonstration → Manufacture → In-Service → Disposal

cds Defence & Security

SECURE BY DESIGN

SAFE BY DESIGN

SUSTAINABLE BY DESIGN

Configuration Management

- Configuration control to protect design integrity and assurance baselines
- Maintain control of design baselines so that modifications to hardware, software, or support solutions are properly assessed for safety, security, and logistic impact.

Monitoring & Feedback

- Continual monitoring for Insider threat and Cyber Vulnerabilities across the asset, organisation and supply chain
- Use of the Data Reporting, Analysis, and Corrective Action System (DRACAS) to monitor performance
- Analysing data from DRACAS to model identify areas for optimization
- Ensure changes and feedback are also applied to training and technical publications
- Delivery of training courses and implementing feedback
- Continual capture of risks, analysis, and mitigations

Security Incident Response

Necessary people, process and authority to respond to incidents where information is at risk of / has been compromised.

Security Assurance

SbD Principle 7: Enable through-life management

Assure that the organisation, assets and supply chain continue to adhere to all SbD principles.

Assure that information and assets are security disposed of at end of life

Safety Incident Response

Necessary people, process and authority to respond to incidents where people are at significant risk of / have been harmed.

Safety Case

Collation of evidence that demonstrates that the risks are sufficiently identified, managed and mitigate too As Low as Responsibly Practical (ALARP).

Sustainability Incident Response

Necessary people, process and authority to respond to incidents where missions and/or environments are impacted because of the asset sustainment.

Supportability Case

Collation of evidence that demonstrates that the risks of not meeting the mission, availability target and environmental sustainability.

Summary



The 5 Key Points of Resilience by Design

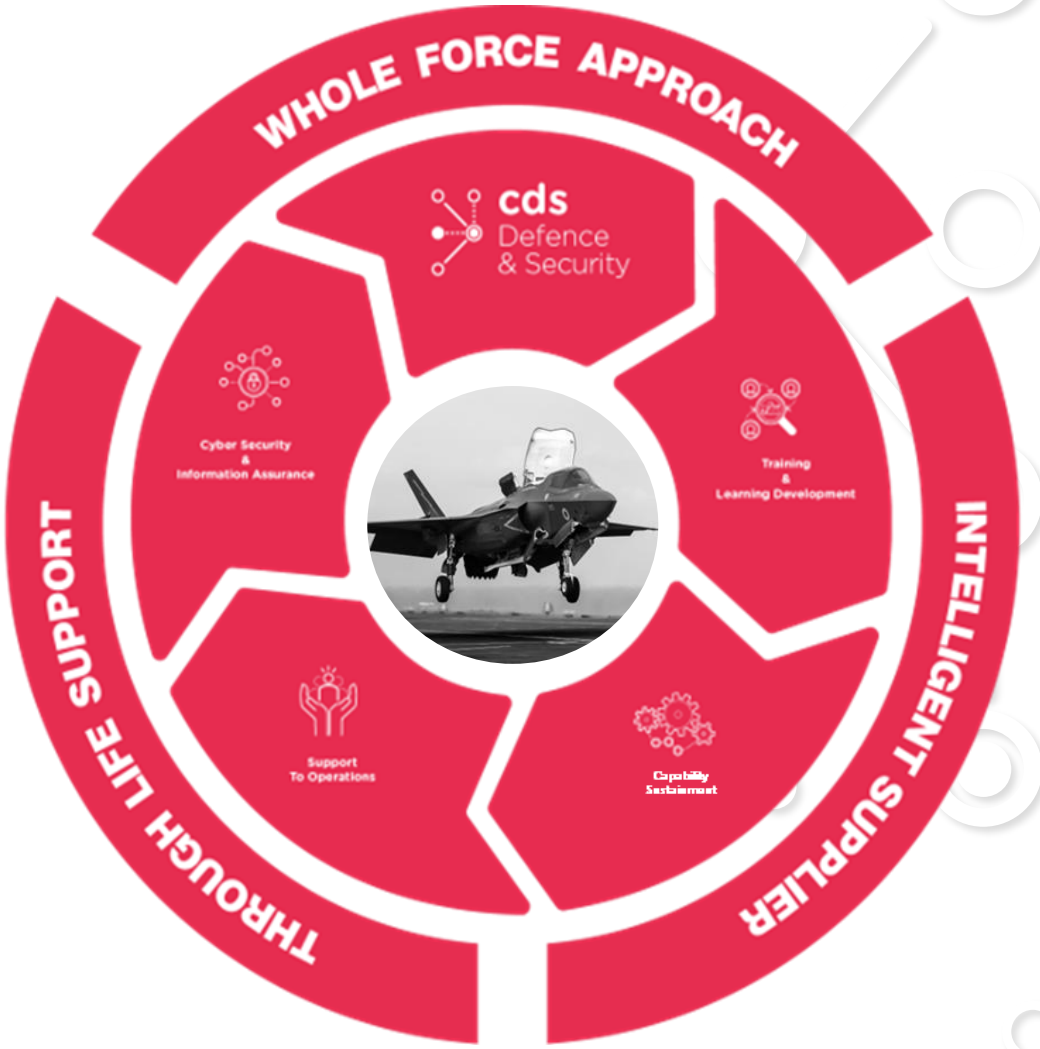
1. **Asset Management -** "Resilient by Design" is an ongoing process through-life, that covers the asset, organisation, and supply chain. The holistic approach should be focused on gaining value from assets and mitigating any risks to it achieving its mission.

2. **Requirements –** ensure capture of capability, sustainability, security and safety is critical to success. Approximately 85% of whole life cost is committed by the end of the acceptance phase.

3. **People -** Integrated Design Team's make sure an asset is designed as a whole system — effective in battle, safe to use, resilient to threats, and sustainable through-life.

4. **Integrated Activity -** "Resilient by Design" requires multiple viewpoints and trade-offs within activities throughout the concept, design, and fielding of new assets.

5. **Continual Monitoring and Improvement –** Analysis and modelling of data can provide confidence in delivery and meeting requirements. Once in-service, monitoring (including insider threat) incident response, and continual improvement are key activities.




cds
Defence
&Security