# Countering Capability – A Model Driven Approach

**Robbie Forder, Douglas Sim**
Dstl
Information Management
Portsdown West
Portsdown Hill Road
Fareham
PO17 6AD
UNITED KINGDOM

rforder@dstl.gov.uk, drsim@dstl.gov.uk

## *ABSTRACT*

*The increasing complexity and agility of systems in the battlefield means that processes for countering them need to be increasingly sophisticated. This paper describes the application of MODAF architectural views to help better understand the Red force systems and tactics. The approach was explored in a C-IADS scenario. This approach revealed significant opportunities to exploit vulnerabilities in Red force capability and is believed to be efficient because it accommodates change.*

## 1.0 INTRODUCTION

The nature of warfare is becoming increasingly complex and networked. War-fighting Capabilities are delivered by complex socio-technical networks of people, organisations and systems. In order to counter an enemy's capability we need to exploit weaknesses in this network, applying effects to counter that capability. How do we know where best to apply effects to counter these systems?

Fundamental to solving this problem is the need to understand the complex nature of the systems and tactics deployed by a potential Red force. This is essentially an intelligence problem, a highly complicated one which is appropriate for architectural modelling. The approach taken to architecting these problems has two stages:

- The first stage is to define a generic model that describes a range of possible scenarios involving red and blue forces along with services and equipment types attributed with possible attack vectors.
- The second stage is to instantiate the generic model with relevant information when a threat has been defined.

This paper is based upon a short investigation, conducted by Dstl in early 2012 which explored how we might counter a networked Integrated Air Defence System (IADS). It describes the overall concepts of how to use the defence architectural frameworks to develop counter-capability and provides insights in how these concepts can be realised.

Finally the paper provides some conclusions from the short investigation on the utility of this approach.

# 2.0 THE CONCEPTS OF CAPABILITY AND COUNTER CAPABILITY

## 2.1 The Defence Architectural Frameworks and Capability Thinking

The defence architecture frameworks were created to provide understanding of the complex nature of defence systems, Human Activity Systems (HAS), System of Systems, etc. Their aim was to help address a number of stakeholder concerns. Traditionally they have been most widely used to support acquisition problems by linking the solution to operational needs.

Key to these frameworks is the notion of capability. However, what is meant by capability is open to interpretation by different types of stakeholder. The INCOSE Capability Working Group identified eight world views of capability:

- Equipment Capability
- Capability Planning
- Capability Trade-off
- Service Capability
- Dynamic Capability Reconfiguration
- Capability Systems Engineering
- Enterprise Planning
- Organisational Capability

In the context of this document, capability is defined as "the ability to do something". This is not a synonym for a piece of equipment. It needs to take in to account the different lines of development such as the ability to acquire, train resource, support etc. The holistic nature of capability thinking in this sense is useful to understanding how we might apply effects to a red force capability using a blue force capability; encouraging us to think outside of the box.


**Figure 1 Understanding Capability in Terms of Lines of Development**

## 2.2 Red and Blue Capability

The ability of the defence frameworks to model capability (in its broadest sense) makes it possible to construct a set of views that show how one capability counters another. A simple notional relationship linking the threat capability to the countering capability is required. (e.g. Capability Addresses Threat).

The problem of thinking at this level is the lack of context, without which it is not possible to assess how appropriate a particular counter-capability may be. For example, if we need to counter a small demonstration which is rapidly turning into an unlawful riot; then using this model we could theoretically quell the riot using any capability which delivers an effect which would disperse the demonstration, even extremes such as indirect fire, which is clearly inappropriate. To solve this problem we need to address the threat capability in context through the use of the OV-5 Operational Activity Model.

Business Process Modelling Notation (BPMN) was used in the OV-5 to show the dynamic interaction between a Red and Blue force during the engagement phase of the scenario: BPMN is a standardised graphical notation for specifying business processes in the form of a model. This notation supports both business users and technical users. At one level it provides a degree of simplicity while being able to represent complex semantics.

BPMN was selected as the preferred notation because of its ability to explicitly show the various events that control the dynamics of the process. This ability to show events was vital to the process of mapping effects.

The following OV-5 example uses BPMN to show the choreography between a Red and Blue force during the engagement phase of the scenario: It illustrates how effects could be applied in a traditional example.

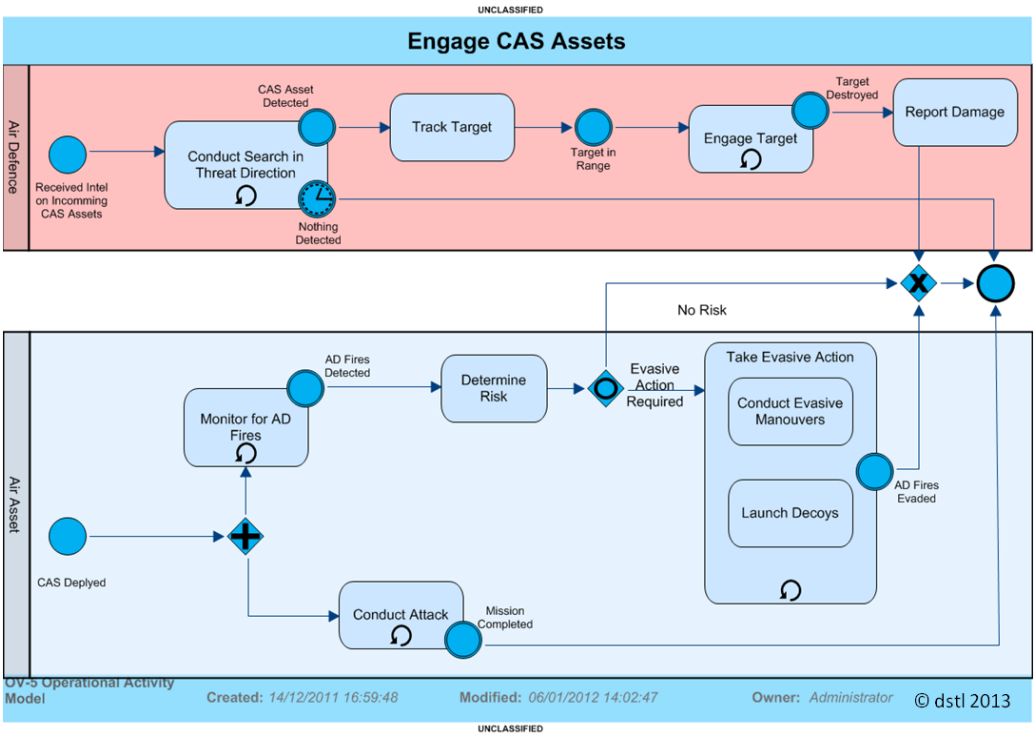


**Figure 2 OV-5 Showing a Typical CAS Scenario Using BPMN Notation**

The Counter Integrated Air Defence Systems (C-IADS) example used the OV-5 to choreograph the interactions between a Red Force conducting an Asymmetric Warfare Integrated Air Defence Systems

(IADS) scenario against a Blue Force Rotary Wing Close Air Support scenario.

The concept integrated within this scenario was not a highly technical approach as in early warning radars, fire control radars etc. The integration was more a socio-technical one, utilising simple commercially available equipment and manpower such as observers, mobile telephone communications and handheld surface to air missiles - but none the less, still an integrated system.

If we consider the problem from a capability perspective, looking across the different lines of development provides numerous potential intervention points for effects. The following example shows an earlier planning phase from the Red Force perspective, all of which could provide potential points for applying effects:

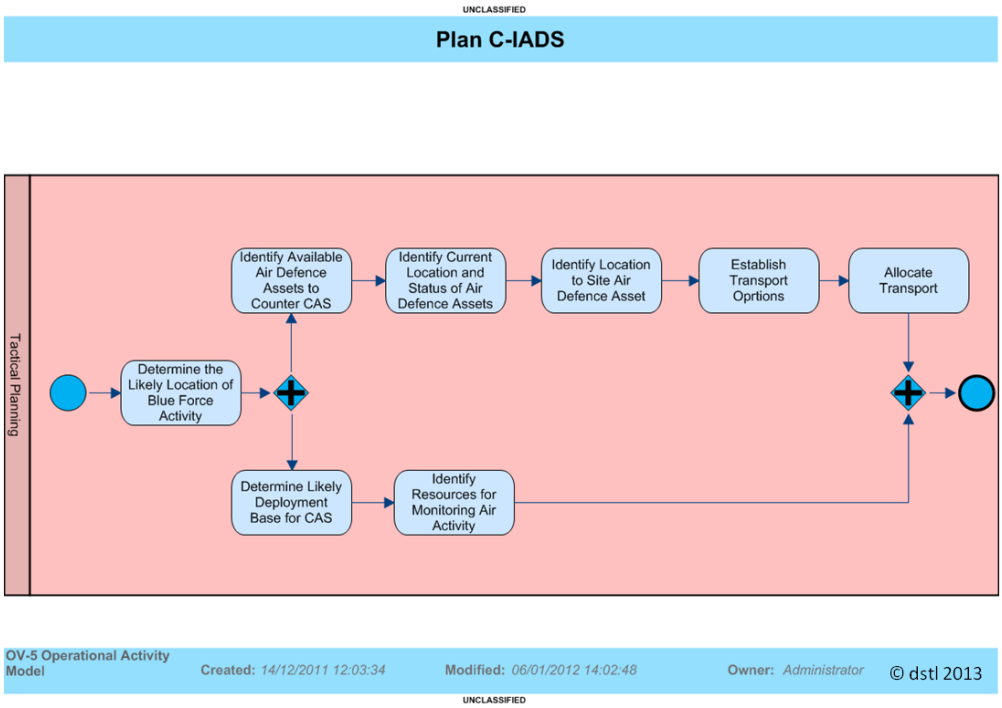


**Figure 3 Exploring the Wider Capability**

The Red and Blue force concept can also be extended into services, where it is possible to model two sets of services, through their various levels of abstraction, and show explicitly how one Blue Force service could be use to counteract a Red Force service.

A service is no more than a highly-cohesive specification of capability at some level so it's fairly straightforward to define the properties of a Blue service to counter a specified Red service. The services approach could also introduce White services (i.e. services that apply to non-military stakeholders), this would allow a better understanding of the potential impact of a particular course of action.

## 2.3 Effects-based Thinking

Application of effects sits within capability thinking, consequently operational modelling is best suited to describing what effect to apply where. System modelling provides a better indication of how the desired effect is to be delivered.

Modelling the Red Force operational activities reveals opportunities for intervention. By analyzing apportioning the risks from the Red Force perspective we are identifying Blue Force opportunities. In essence Blue Force opportunities are really the inverse of a Red Force risk.

The service approach adds a richer dimension to the operational activity model where the business services are orchestrated by the activities then broken down into various supporting services. This allows the identification of specific vulnerabilities in the service hierarchy.

The OV-2 Operational Node Relationship Description provides another mechanism to identify areas for intervention; needlines. Note here that needlines do not just represent information flow, they can also be used to represent people, materiel or energy.

An intervention at the operational level shows where effects can be applied. The related systems views are required to understand how. Potential intervention at this level will help to either neutralise or degrade a capability, since a single needline can be implemented in a variety of ways, often with primary and fallback modes. If we looked directly at the system level (the how) risks without considering the operational level then it is likely that alternative methods of implementing the needline would be missed.

Having identified where desired effects are best applied and understanding their impact at a logical level, it is possible to identify how these effects might be applied and the level of degradation achieved. To do this it is necessary to map attack vectors at the system level (see Figure 4). The detail of system modelling required is driven by the desired method of attack. For example, a kinetic effect may only need a fairly abstract model with good location information, whilst a cyber attack might need a detailed network topography with associated hardware and software components.

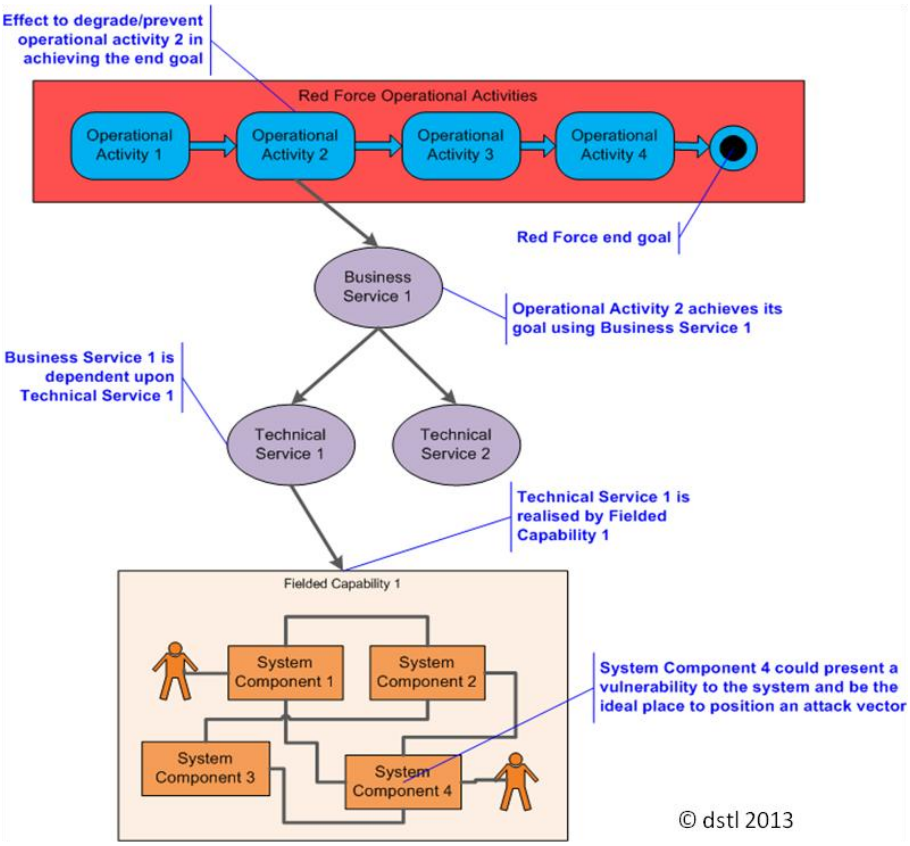


**Figure 4 Walking the Architecture from Desired Effect to Candidate Attack Vector**

The contribution that system makes to capability is realised through function, therefore attack vectors should be aimed at functions. The defence frameworks provide the direct linkage from function to either operational activity or service provision. A function can be implemented by alternative systems or system components, so provides a better resolution for achieving a desired effect.

## 2.4 Handling Uncertainty

One of the problems of modelling Red Capability is that it is usually intelligence led and consequently doesn't fully describe the Red Force; it may lack detail or consist of conflicting descriptions. Capability configurations can be used to represent the Red Force physical resources aspect of capability. Capability configurations can be black boxed or opaque boxed to represent a degree of unknown capability. It is possible to attribute measures of performance against these capability configurations based upon estimates and predictions; which can be used to support a counter-capability as the information evolves:

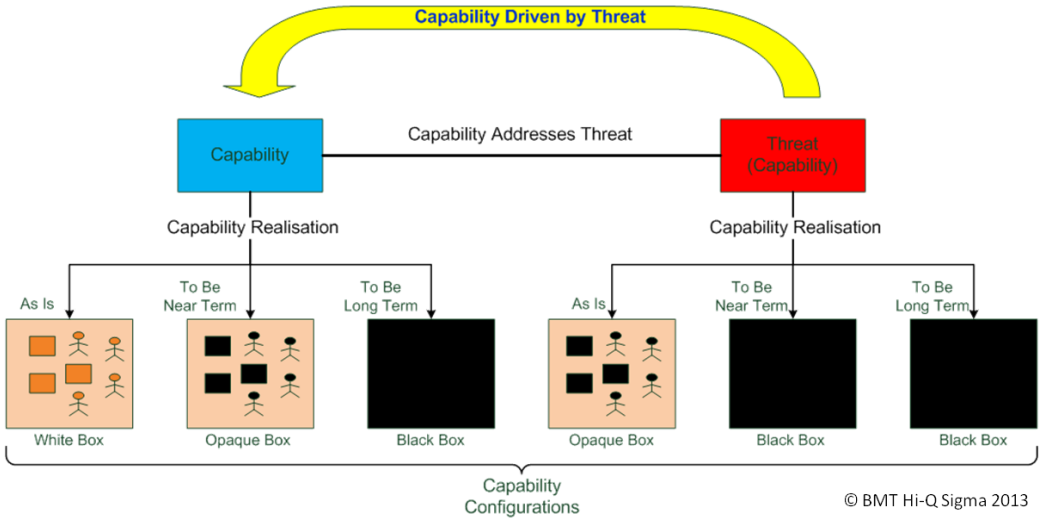


**Figure 5 White, Opaque and Black Box Capability Configurations**

## 3.0 CHANGES TO THE META-MODEL

To enact the approach documented in Section 2 it is necessary to adapt the MODAF meta-model by adding two simple relationships:

- Capability Addresses Threat - which is an association between two capabilities
- Service Counters Service – which is an association between two services

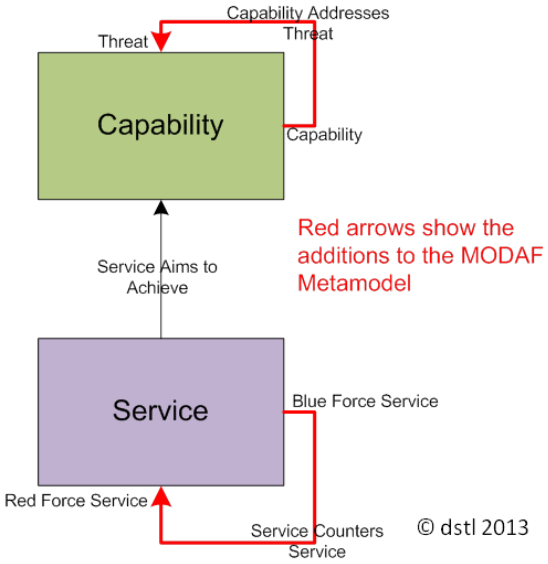


**Figure 6 Changes to the MODAF Metamodel**

## 4.0 IMPLEMENTING THE CONCEPTS

### 4.2 Generic Systems Modelling

To fully understand the Red Force capability in order to identify attack vectors, a set of generic systems

models are needed that provide systems understanding at the domain level. The level of abstraction of these models is driven by strategic concerns. Even at a fairly high level of abstraction, see Figure 7 below, it is possible to attribute measures of performance which will help establish levels of degradation following the application of effects.

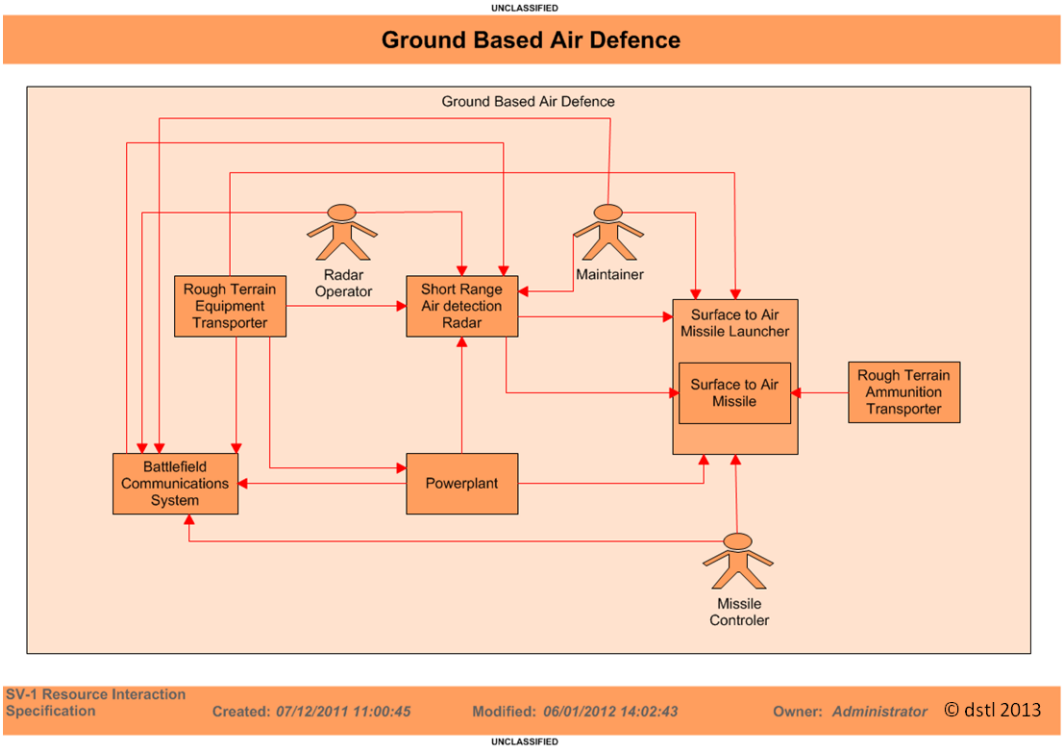


**Figure 7 Generic Capability Configuration**

The above example shows a notional generic Ground Based Air Defence System in the form of a capability configuration which includes the roles as well as the system equipment components. All of these can be attributed with measures, usually via its associated functions; however to apply values to the attributes would need a lower level of modelling. It is also possible to attribute potential attack vectors and work out, through the traceability provided by the framework, how different effects will impact upon the wider system. The inclusion of the human aspect in these capability configurations opens the door to conducting how effects might impact upon the socio-technical aspects of the system.

Attributing measures is best done at the functional level, rather than directly to the systems components, this provides a better top-down analysis from either business process and/or service perspectives. This approach does pose a problem in that functions would need to be replicated for multiple systems with the same functionality, but with differing measures. The remedy for this is to place the measures on the linkage between the system and the function (MODAF Function Provision); however not all modelling tools will support this approach.

## 4.2 Instantiating the Generic Model

How an instance is defined can be subjective. The true instance usually means that it physically exists at a single location at a single point in time. To model to this degree would result in a range of carbon-copy fielded capabilities with the only difference being one or two attributes to do with location. The only time that this may be necessary is if the instance we connected to was a wider architecture with other instantiated

information.

In terms of understanding vulnerability, only the lowest level of abstraction needs to be the *architectural instance.* This is determined by the level at which the attributes pertaining to the design can be populated. This approach should expose the majority of attack vectors. Location-related information can then be applied as a set of attributes in the form of a list.

The generic Capability Configurations would only be realised into architectural instances in response to strategic concerns. The generic architecture, due to its more abstract nature, will tend to be more enduring; the agile properties will be more prevalent in the architectural instance reinforcing the benefits of a two stage approach.

This two stage process enables more efficient use of resource than a single stage. The dynamic nature of the environment means that any detailed work done prematurely will be wasted. The two stage process allows this detailed work to be done later, i.e. just prior to implementing effects.

Through the application of the defence architectural frameworks it is possible to walk the architecture in order to fully understand how the Red Force capability can be countered by the Blue Force and the consequences in doing so. Where necessary, the attributes and values can be pulled from the architectural modelling tools into operational analysis tools, such as simulation and network analysis tools, in order to explore the options, in detail, for exploiting attack vectors in support of applying effects.

## 5.0 CONCLUSIONS

This study focused on creating a model that would allow the application of effects to support conventional warfare. The study showed that only small changes were necessary to the MODAF meta-model to enable the framework to be applied in new directions; developing capability to counter complex integrated systems based upon intelligence information.

The service paradigm provides a good mechanism to understand where to apply effects to maximise their impact. For example, it may be possible to impact any lower-level service from a group of collaborating services in order to degrade or destroy the higher-level business service.

Appropriate attribution of the architectural constructs provides two significant benefits;

- A mechanism to understand the provenance and reliability of the information from which they were derived,
    - enabling a more evidence-based approach to decision making in the targeting process.
- The ability to measure the effectiveness of each intervention, at a variety of levels of abstraction
    - to assess what level of degradation in Red Capability has been achieved and ultimately has this delivered the desired operational effect.

The approach allowed up-front architecting work to be kept to a minimum by only creating the generic architectures, applying the attributes for different types of component at the system level and the types of attack vector that might be applied. Detailed architectural instantiations only need to be created when the threat becomes strategically important, providing a model of what to do, with the where and how only being modelled if and when necessary.

# 6.0 GLOSSARY

**Capability**

The ability to do something

**Capability Configuration**

A composite structure representing the physical and human resources (and their interactions) that when brought together provide one or more Capabilities.

**Effects**

The result, outcome, or consequence of an action

**Fielded Capability**

An actual, fully-realised capability that realises a Capability Configuration.

**Needline**

A relationship between Nodes representing a bundle of Information Exchanges.

**Nodes**

A logical agent that performs operational activities.

**Operational Activity**

A logical process, specified independently of how it is carried out

**Service**

An implementation-independent specification of a packaged element of functionality and/or capability

# 7.0 LIST OF ABBREVIATIONS

| | |
|---|---|
| C-IADS | Counter – Integrated Air Defence System |
| DLoD | Defence Lines of Development |
| IADS | Integrated Air Defence System |
| INCOSE | International Council on Systems Engineering |
| MODAF | MOD Architectural Framework |