PYRAMID Exploiter's Pack Version 4.1

Annex D – Glossary Issue 12.1

This document has been prepared, as part of the PYRAMID Exploiter's Pack, in order to set out a generic approach to implementation of the PYRAMID Architecture. The PYRAMID Reference Architecture has not been created for any specific system. It is the user's responsibility to ensure that any article created using this document meets any required operational, functional and safety needs. The Author accepts no liabilities for any damages arising due to a failure of the user to verify the safety of any product produced using this document, nor for any damages caused by the user failing to meet any technical specification.

For further information regarding how you can exploit PYRAMID on your project, provide feedback following your review of the PYRAMID Exploiter's Pack V4.1, or have a technical query that you would like answering, please contact the PYRAMID Team using the following email address. PYRAMID@mod.gov.uk

This publication is available at https://www.gov.uk/government/publications/pyramid/pyramid-programme

EXECUTIVE SUMMARY

The MOD’s PYRAMID programme introduces a change to the current method of avionic systems design and procurement, aiming to make the next generation of air systems affordable, capable and adaptable by the adoption of an open architecture approach and systematic software reuse.

This Glossary document forms part of the PYRAMID Exploiter’s Pack and defines a common set of terms, abbreviations and acronyms used in the Exploiter’s Pack.

CHANGE HISTORY

Date	Issue	Description of Changes
04/08/2014	1	First Issue
04/12/2014	2	Updated with DOORs Definitions for SRR.
03/02/2015	3	Updated in response to DSTL review of Mission System Requirements Specification.
26/01/2016	4	Added new definitions Removed Standards section Added section for deprecated terms
22/02/2017	5	Updates as detailed in the TIKAL Problem Report PR000745. This includes: Addition, removal and update of definitions as per PR000745. Changing 'Height' in the table in Section 5.3 to 'Length' Addition of MGRS, UPS and GARS to Section 6. Removal of the US DoD Autonomy Levels from Section 9.
29/11/2017	6	Addition, removal and update of definitions as defined in the Problem Report PR001377.
18/07/2018	7	Updated in line with DEFCON 705
30/09/2018	8	Updates as detailed in the TIKAL Problem Report PR001806. This includes updating the report as an output in line with DEFCON 703
11/11/2019	9	Updates as detailed in PR001830. This PR covers the updates required for the PRA Exploiter's Pack.
16/01/2020	9.1	Updated in response to Customer comments against PRA Exploiter's Pack.
December 2020	10	Complete update of the Glossary to form Annex D of the PRA: • Complete re-ordering of the References (now a subset from the PRA main document) • Removal of generic front text (now included in the PRA main document). • Update to PRA-related term definitions.

Date	Issue	Description of Changes
		• Terms reduced to only those applicable to the PYRAMID Exploiter's Pack, removing all unused legacy TIKAL terms and all general aviation and military terms. • Example Deployment Lifecycle, Deprecated Terms, Maturity Levels, Units of Measure, Coordinate Frames, Frequency Bands, NIIRS Ratings, Landing System Categories and Technology Readiness Levels removed from the document. • Abbreviations and Acronyms used within the PYRAMID Exploiter's Pack introduced into this document – the previous Glossary Annex A (BAES-FCAS-UCAS-TKL-DOC-21508) has been retired.
October 2021	11	Addition of Introduction text. Section 2 (Definition of Terms) split into PYRAMID terms and other terms. Update to Section 2 (Definition of Terms) and Section 3 (Abbreviations and Acronyms) to include/remove entries necessary for Version 3 of the PYRAMID Exploiter's Pack.
December 2022	12	Document markings aligned to reflect MOD provided guidance. Contents of Section 2 (Definition of Terms) has been combined into a single table with PYRAMID Specific Terms highlighted accordingly. Update to Section 2 (Definition of Terms) and Section 3 (Abbreviations and Acronyms) to include/remove/re-categorise entries necessary for Version 4 of the PYRAMID Exploiter's Pack.
September 2023	12.1	The document has been updated due to now being released via Open Government License v3.

List of Effective Pages

24 pages UK OFFICIAL

24 pages in total

TABLE OF CONTENTS

TABLE OF TABLES

REFERENCES

The reference numbers are consistent across all the documents in the PYRAMID Exploiter's Pack. This means that in this document, when a reference is not used, the corresponding reference number will not appear in the reference list.

Public Domain Document References:

Public domain references below contain information which is proprietary to that referenced third party. Any information from this source is subject to separate rights and terms and is not subject to the terms of DEFCON 703 or DEFCON 705.

Reference	Title, Document Number, Issue & Date
[16]	Design and Airworthiness Requirements for Service Aircraft, Defence Standard 00-970 Part 0, Issue 21, 28 March 2019
[38]	SAE International / EUROCAE, Guidelines for Development of Civil Aircraft and Systems, ARP-4754A, 2010
[41]	Information technology - Security techniques - Information security management systems - Overview and vocabulary, BS EN ISO/IEC 27000:2018
[43]	NATO Glossary of Terms and Definitions, AAP-06, Edition 2018
[45]	M. Endsley, 1988, Design & Evaluation for Situation Awareness, Proceedings of the Human Factors Society 32rd Annual /Meeting (pp. 97-110), Santa Monica, CA: Human Factors Society
[46]	Safety Management Requirements for Defence Systems, Defence Standard 00-56 Part 2, Issue 5, February 2017
[62]	Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, ISO 7498-2:1989

1 Introduction

The MOD’s PYRAMID programme introduces a paradigm shift to the current method of avionic systems design and procurement, aiming to make the next generation of air systems affordable, capable and adaptable by the adoption of an open architecture approach and systematic software reuse.

1.1 Scope

The PYRAMID Exploiter's Pack Annex D: Glossary (this document) includes definitions for PYRAMID-relevant terms and those abbreviations and acronyms used throughout the PYRAMID Exploiter's Pack.

1.2 Purpose

The purpose of this document is to provide the definition of a common set of terms and abbreviations relevant to the PYRAMID Exploiter's Pack.

1.3 Document Structure

This document has the following sections:

1.3.1 Introduction

This section.

1.3.2 Definition of Terms

Section 2 provides a list of terms and definitions used within the PYRAMID Exploiter's Pack. The list includes PYRAMID specific terms and other terms that are used extensively throughout the pack. References for any non-project related sourced definitions have been included where appropriate.

1.3.3 Abbreviations and Acronyms

Section 3 provides a list of abbreviations and acronyms used throughout the PYRAMID Exploiter's Pack.

2 Definition of Terms

Table 1: Definitions of PYRAMID Exploiter's Pack Terms defines two types of term:

Pyramid specific:

These terms have a bespoke meaning within the PYRAMID Exploiter's Pack. PYRAMID specific terms are indicated by a highlighted background.

Other terms:

These terms, whilst crucial to the understanding of the PRA, do not have a bespoke meaning within the PYRAMID Exploiter's Pack. In addition to their definition some terms also include additional information within their description to give the context of how the term applies within the PRA.

Name	Description
Accountability	Property that ensures actions performed by an entity may be traced uniquely to that entity. Ref. [62]
Accreditation	The formal, independent assessment of an ICT system or service against its IA requirements, resulting in the acceptance of residual risk in the context of the business requirement and information risk appetite. This will be a prerequisite for approval to operate.
Achievability	The ability to accomplish a requirement successfully.
Action	An activity defined in terms of what needs to be done. Actions are executed by coordinating resources.
Attribute	An element of data that forms part or all of an interface on a service.
Auditability	The ability to obtain audit evidence and evaluate it objectively to determine the extent to which the audit criteria are fulfilled.
Authenticity	Property that an entity is what it claims to be. Ref. [41]
Authorisation	Approval given to a system, process or action in order that it may be carried out without direct crew control.
Authorised Operator	Any person, user, or operator with validated credentials allowed to interact with a system to carry out a system role.
Automated	The operation of a system or the execution of processes or actions following a predefined sequence of logical steps without recourse to direct crew control.

Name	Description
Autonomous	The operation of a system or the execution of processes or actions in accordance with defined rules in order to bring about a desired state without recourse to direct crew control.
Availability	Property of being accessible and usable upon demand by an authorised entity. Ref. [41]
Bridge	An interconnection enabling component services (provided and consumed) to be connected together.
Capability	The ability to do something, or the ability to perform a particular function based on internal factors only. A system's or components capabilities are derived from the resources it has at its disposal, and the uses it is able to put them to.
Catastrophic	Failure conditions that result in the death of one or more people. Catastrophic outcomes are considered DAL A within the PRA safety considerations.
Certification	The confirmation that the system complies with the applicable regulatory requirements (as agreed with the certifying authority, e.g. for airworthiness this is the MAA).
Communications Agnostic	Not being aware of where communications signals originate or go, or the route via which those signals travel.
Communications Aware	Being aware of where communications signals originate or go, or the route via which those signals travel.
Communications Capability	The ability to deliver data over a communication infrastructure.
Communications Service	The overall service provided to enable the flow of traffic across channels and links.
Component	A reusable configurable unit, defined by a role and a distinct set of responsibilities, entities and services, for a cohesive subject matter area.
Component Behaviour	The behaviour required from a component in order to fulfil its responsibilities within the system and provide its services.
Component Specification	The precise requirement of the component as part of a specific deployment, described in terms of its services and/or entities.
Component Variant	A distinct, tailored version of a component, specialised in order to satisfy a specific resource profile or operational context.

Name	Description
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes. Ref. [41]
Conflict	A state where the resources (e.g. fuel or bandwidth) required for two or more actions cannot be satisfied simultaneously.
Constraint	A limitation on the behaviour of a PYRAMID compliant deployment at any level (whole system or constituent part).
Consumed Service	A service that defines work done outside of the component that the component depends upon in order to fulfil its responsibilities.
Counterpart	A representation of something (either physical or conceptual) that is viewed differently in different places or different aspects of it are considered in different places. For example there may be two different representations (i.e. counterparts) of a missile, where from one perspective it is viewed as a destructive effector and from another perspective it is viewed as a releasable object with a specific mass.
Critical	Failure conditions that result in major injury to people, loss of aircraft or a large reduction in safety margins. Critical outcomes are considered DAL B within the PRA safety considerations.
Cryptographic Plan	A plan for the overall use of cryptography, including applied segregation and use of Cryptographic Material.
Cyber Attack	A deliberate and malicious exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences.
Data Driving	The configuration of either the specification or the internal structure of a component via the use of data in order to support different Exploiting Programmes or end-user scenarios without the need for wholesale redesign.
Deletion	The removal of data by a component arising from a change of retention strategy.
Deployable Asset	Any physical hardware (e.g. role fit equipment) carried on an Exploiting Platform that can be deliberately separated from the Exploiting Platform during a mission.
Deployment	A set of hardware and software elements forming a system (or part thereof) that satisfy the overall system requirements.

Name	Description
Design Integrity	The extent to which the design is free from flaws that could give rise to or contribute to hazards, or to failure modes that contribute to a hazard. Ref. [46]
Dumb Asset	A deployable asset that does not have a data interface with the Exploiting Platform.
Equipment	Hardware or a combination of hardware & software, that provides a capability or resource to the system under consideration.
Exchange	An interaction between a deployment of the PRA and another system for the purposes of passing data or information between them.
Executable Software	A computer file that contains encoded instructions capable of being executed by a processing unit. Executable software can be composed of one or more PRA components.
Execution Platform	The infrastructure supporting the execution, communication, etc. of application functionality, e.g. ECOA, ARINC 653, Linux, Windows, and the computing hardware.
Exploiter	An organisation involved in the design and development of PYRAMID components or the design of PRA compliant systems.
Exploiting Platform	A product (e.g. an air vehicle, ground station, or a test rig) that incorporates a deployment of the PRA.
Exploiting Programme	A programme, e.g. Typhoon or TEMPEST, incorporating a deployment of the PRA.
Extension Component	A developed component that separates out or extends the functionality provided by a parent component whilst remaining within its subject matter.
Extension Point	A consumed service that defines the parent component’s dependency upon an extension component for a single purpose.
Extension Set	A set of one or more extension components that implement the same extension point.
Feasibility	The practicality of achieving a solution.
Flight	A collection of one or more aircraft, potentially of dissimilar types, performing roles and tasks to achieve the overall mission.
Flight Lead	The vehicle responsible for coordinating the activities of a flight to meet the objectives specified for the mission or supplied by the crew.

Name	Description
Flight Member	Any aircraft that forms part of a flight. Each member of the flight acts in support of the overall flight aims and of the other flight members.
Handover	The process of performing a command and control transfer from one operator to another operator, e.g. between pilots on a twin-seat aircraft, operators on a single workstation, or across control stations.
Health Data	Health data includes all data that is required as input for assessing the health and capability of the system. It includes, but is not limited to: - Hardware and software configuration data. - Fault and error codes (BIT reports). - Sensor data (including, but not restricted to, specific sensors for monitoring health and structural integrity). - System control, command and mode data. - Consumables data. - Usage data (for life and usage monitoring). - Manual measurements (requested and volunteered).
Integrity	(Safety context) The probability that the system will provide a specified level of safety. Ref. [16] (Security context) Property of accuracy and completeness. Ref. [41]
Item Development Assurance Level	The level of rigour of development assurance tasks performed on item(s). Ref. [38]
Logging	The process of identifying and retaining items of data received by or generated within a component as part of that component’s normal operation that need to be retained for possible later use but which are not required as a direct result of that component’s role.
Major	Failure conditions that result in minor injury to people, major damage to the aircraft or a significant reduction in safety margins. Major outcomes are considered DAL C within the PRA safety considerations.
Mission	One or more aircraft ordered to accomplish one particular assignment. Ref. [43]

Name	**Description**
Mission Plan	The plan for the particular flight of one or more air vehicles from start-up / turnaround to shutdown / turnaround. Describes the planned flightpath and timings that the air vehicle should follow and the air vehicle’s assigned mission objectives to be achieved in order to meet the tasking. A Mission Plan may be modified whilst an air vehicle is in flight as the result of dynamic re-tasking.
Mission Support System	Non-real-time systems which support the real-time operational elements of the systems (e.g. mission planning, data extraction etc.).
Non-Repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities. Ref. [41]
Objective	A high level goal which either defines the purpose of the mission (e.g. the requirement to suppress enemy air defences) or is otherwise required of the mission (e.g. the requirement for aircraft survivability) that is assigned to the system to support a broader strategic goal.
Parent Component	A developed component that supports the use of extension components.
Platform Independent Model	A representation of a system that is independent of the execution platform.
Platform Specific Model	A representation of a system that incorporates the execution platform.
PRA Element	A model artefact that defines or provides guidance on the purpose of a component (e.g. role, responsibilities and service definitions).
Protection Domain	A grouping of components within a platform specific deployment context that have similar segregation requirements (e.g. for security, safety or specific functionality reasons) that are separated from other domains such that they are unable to interfere with the resources or processing in that domain. Communications between protection domains is strictly regulated.
Provided Service	A component service that defines work done by that component.
PYRAMID Reference Architecture	The PRA is an open air system reference architecture comprised of re-useable Platform Independent Model components and guidance for Exploiters, where 'reference architecture' is 'recommended structures and policies to form a deployment solution'.
Recording	The process of retaining identified data items received by or generated within a component that need to be retained for future use.
Resource	An asset that can be used for executing an action.

Name	Description
Retention	The keeping of important data for future use or reference.
Retention Strategy	A set of specific retention rules and supporting information covering which data is to be captured and retained and the conditions for retention (including duration, classification, etc.).
Sanitisation	(Security context) The process of deliberately, permanently and irreversibly removing or destroying data to make it unrecoverable.
Security Domain	A grouping of elements (e.g. components and data) with similar security requirements that are managed by a defined security policy such that groupings remain separate unless specific controls are in place (e.g. data encryption).
Security Enforcing Function	Function relating to specific controls that provide protection to the system (e.g. providing cryptography). Failure of a SEF could lead to a security breach.
Security Related Function	Functions that support the security activities within the system but are not directly involved in enforcing the separation of security boundaries or preventing cyber attacks. Failure of a SRF will not directly lead to a security breach but may diminish the system's ability to detect or counter a threat (e.g. security event logging).
Service	The means by which a component is asked to do something, or by which a component gets something done for it. A service is formed of interfaces and activities.
Service Oriented Architecture	An architectural pattern in computer software design in which application components provide services to other components, independent of vendor, product or technology.
Simulation	An imitation of a process or scenario, e.g. the performance of a mission for training or rehearsal purposes.
Situation Awareness	The perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. Ref. [45]
Storage	The action or method of storing data for future use.
Storage Media	The media used to store data.
Subject Matter	The definition, semantics and behaviour associated with a topic or subject. This is used to define the bounded scope of a PRA component.

Name	Description
System Integrator	An organisation involved in the wider integration of a PYRAMID based system.
Task	The specification of a goal which needs to be achieved by an Air Vehicle (e.g. transit to a location, search an area, or attack a target).
Test	A procedure or method intended to establish the state, performance and capability of something.
Trust	The confidence that a component or other system element will behave as expected.

Table 1: Definitions of PYRAMID Exploiter's Pack Terms

3 Abbreviations and Acronyms

Name	Description
A/A	Air to Air
A/S	Air to Surface
AAR	Air-to-Air Refuelling
ACAS	Airborne Collision Avoidance System
ACID	Atomic, Consistent, Isolated, Durable
ADS-B	Automatic Dependent Surveillance – Broadcast
AEK	Algorithm Encryption Key
AGL	Above Ground Level
AIXM	Aeronautical Information Exchange Model
AMRAAM	Advanced Medium-Range Air-to-Air Missile
API	Application Programming Interface
ARINC	Air Radio Incorporated
ASRAAM	Advanced Short-Range Air-to-Air Missile
ATC	Air Traffic Control / Controller
ATIS	Automatic Terminal Information Service
ATS	Air Traffic Services
BIT	Built In Test
BS	British Standard
C2	Command and Control
CAT	Clear Air Turbulence
CBIT	Continuous Built in Test
CEP	Circular Error Probability

Name	Description
CIA	Confidentiality, Integrity and Availability
CIK	Cryptographic Ignition Key
CMS	Core Mission System
COMSEC	Communications Security
CPDLC	Controller - Pilot Datalink Communications
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSMU	Crash Survivable Memory Unit
CTT	Controlled-Trajectory Termination
DAIS	Defence Assurance and Information Security
DAL	Development Assurance Level
DDS	Data Distribution Service
DEK	Data Encryption Key
DEW	Directed Energy Weapon
DME	Distance Measuring Equipment
DMZ	De-Militarized Zone
DoS	Denial of Service
EAL	Evaluation Assurance Level
ECM	Electronic Countermeasures
ECOA	European Component Oriented Architecture
EED	Electronic Explosive Device
EM	Electro-Magnetic
EMCON	Emissions Control

Name	Description
EMF	Electromagnetic Field
EN	European Standard
EO	Electro-Optical
ERA	Entity, Relationship and Attribute
ES	Electronic Surveillance
EUROCAE	EURopean Organisation for Civil Aviation Equipment
EW	Electronic Warfare
FAA	Federal Aviation Administration
FACE	Future Airborne Capability Environment
FPGA	Field-Programmable Gate Array
GDPR	General Data Protection Regulation
GMT	Greenwich Mean Time
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSN	Goal Structuring Notation
GUI	Graphical User Interface
HF	High Frequency
HMI	Human Machine Interface
HMS	His Majesty's Ship
HOTAS	Hands On Throttle And Stick
HW	Hardware
IA	Information Assurance
IAS	International Accreditation Service

Name	**Description**
IBIT	Initiated Built in Test
ICT	Information and Communications Technology
ID	Identifier
IDAL	Item Development Assurance Level
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IFF	Identification Friend or Foe
ILS	Instrument Landing System
IM	Instant Message
INS	Inertial Navigation System
IP	Internet Protocol
IPS	Intrusion Protection System
IPSec	Internet Protocol Security
IR	Infrared
IRST	Infrared Search and Track
ISO	International Organisation for Standardisation
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
IV	Interaction View
IVDL	Inter Vehicle Data Link
JPEG	Joint Photographic Experts Group
KEK	Key Encryption Key
KUR	Key User Requirement

Name	Description
LAR	Launch Acceptability Region
LDAP	Lightweight Directory Access Protocol
LDP	Laser Designator Pod
LIDAR	Light Detection and Ranging
LRU	Line Replaceable Unit
MASS	Master Armaments Safety Switch
MB	Megabyte
MBD	Model Based Design
MBSE	Model Based Systems Engineering
MDA	Model Driven Architecture
MIKEY-SAKKE	Multimedia Internet Keying - Sakai-Kasahara Key Encryption
MIP	Multilateral Interoperability Programme
MITM	Man In The Middle
MOD	Ministry of Defence
MSA	Minimum Safe Altitude
MSD	Minimum Separation Distance
MSS	Master Safety Switch
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
O	Official
O-S	Official Sensitive
OMG	Object Management Group
OMI	Operator-Mission Interface

Name	**Description**
OSD	Office of Security of Defence
OTAR	Over The Air Rekeying
PBIT	Power Up Built in Test
PC	Personal Computer
PIM	Platform Independent Model
PMDH	Post Mission Data Handling
PNG	Portable Network Graphics
PQMS	PYRAMID Query Management System
PRA	PYRAMID Reference Architecture
PRI	Pulse Repetition Interval
PRIME	Protocol Requirements for IP Modular Encryption
PSM	Platform Specific Model
QFE	Q code - pressure at airfield runway
QNH	Q code - pressure adjusted to mean sea level
QoS	Quality of Service
RA	Resolution Advisory
RCD	Residual Current Device
RCS	Radar Cross Section
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFI	Request For Information
RoE	Rules of Engagement
RTB	Return To Base

Name	**Description**
RTCA	Radio Technical Commission for Aeronautics
RTPS	Real Time Publish Subscribe
S&RE	Suspension & Release Equipment
SA	Situation Awareness
SAE	Society of Automotive Engineers
SAM	Surface to Air Missile
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communications
SC	Security Check
SCEO	Secret - Coalition Eyes Only
SEAD	Suppression of Enemy Air Defences
SEF	Security Enforcing Function
SID	Standard Instrument Departure
SIEM	Security Information & Event Management
SIGMET	Significant Meteorological Information
SIP	Session Initiation Protocol
SNEO	Secret - National Eyes Only
SOA	Service Oriented Architecture
S.O.L.I.D.	Single-responsibility principle Open-closed principle Liskov substitution principle Interface segregation principle Dependency inversion principle
SOS	Store On Station

Name	**Description**
SOUP	Software of an Unknown Pedigree
SRF	Security Related Function
SSR	Secondary Surveillance Radar
SSUN	Single Statement of User Need
SysML	Systems Modelling Language
TA	Traffic Advisory
TACAN	Tactical Air Navigation System
TB	Terabyte
TCAS	Traffic alert and Collision Avoidance System
TCP	Transmission Control Protocol
TDL	Tactical Data Link
TLS	Transport Layer Security
TOA	Terminal Operation Area
TRANSEC	Transmission Security
TS	Top Secret
TTP	Techniques, Tactics & Procedures
UAS	Unmanned Air System
UAV	Unmanned Air Vehicle
UC	Use Case
UCS	UAV Control System
UHF	Ultra-High Frequency
UK	United Kingdom
UML	Unified Modelling Language

Name	Description
US	United States
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VoIP	Voice Over Internet Protocol
VOR	VHF Omnidirectional Range
VPN	Virtual Private Network
WIUK	Weapons Integration UK

Table 2: Abbreviations and Acronyms