Assessment of Compatibility Between the PYRAMID Reference Architecture and the FACE® Technical Standard

Document No.	BAES-FCAS-PYR-ENG-RPT-106239
Issue	1
Date	May 2024

This document contains information owned and attributed to:

- The Open Group, L.L.C
- UK MOD (as Crown owned copyright)
- BAE Systems

Information ownership is as follows:

- The Open Group, L.L.C.' copyright information pertains to figures from FACE® documents (Ref. [6], [7], and [8]) and statements solely relating to FACE® documents (Ref. [6], [7], and [8]).
- The Crown copyright information pertains to figures from PYRAMID documents (Ref. [1], [2], [3], [4], and [5]) and statements solely relating to PYRAMID documents (Ref. [1], [2], [3], [4], and [5]).
- The BAE Systems copyright and proprietary information pertains to figures and information comparing FACE documents (Ref. [6], [7], and [8]) and PYRAMID documents (Ref. [1], [2], [3], [4], and [5]), or assessment of FACE documents (Ref. [6], [7], and [8]) and PYRAMID documents (Ref. [1], [2], [3], [4], and [5]).

The source of the information used to produce Figures in this document is listed below:

Figure & Title	Source	Ownership
Figure 1: PRA Components	PYRAMID Exploiter's Pack Issue 4.1	UK MOD
Figure 2 FACE® Architectural Segments	FACE® Technical Standard edition 3.2	The Open Group, L.L.C.
Figure 3: Scope of Concerns Considered for Architecture Assessment	Created as part of Task 8 (CAAP/ 701552387) under the CAAP International Framework Agreement (CAAP/700008174).	BAE Systems
Figure 4 FACE® Segments and FACE Interfaces	FACE® Technical Standard edition 3.2	The Open Group, L.L.C.
Figure 5 Examples of Bridges Performing Semantic Conversations	Created as part of Task 8 (CAAP/ 701552387) under the CAAP International Framework Agreement (CAAP/700008174). Based on information contained within: • PYRAMID Exploiter's Pack Issue 4.1	BAE Systems (UK MOD)
Figure 6 FACE® Model Architecture	FACE® Technical Standard edition 3.2	The Open Group, L.L.C.
Figure 7 Detailed Structure of the TS Segment	FACE® Technical Standard edition 3.2	The Open Group, L.L.C.
Figure 8 Fault Management Cycle State Machine	FACE® Technical Standard edition 3.2	The Open Group, L.L.C.
Figure 9 Data Flow in BALSA ADS-B Data Transfer Use Case	FACE® Software Supplier Getting Started Guide edition 3.x	The Open Group, L.L.C.

The source of the information used to produce Tables in this document is listed below:

Table & Title	Source	Ownership
Table 1 Comparison of PRA and FACE® Architecture Concerns	Created as part of Task 8 (CAAP/ 701552387) under the CAAP International Framework Agreement (CAAP/700008174) and updated. Based on information contained within: • FACE® Technical Standard edition 3.2 • PYRAMID Exploiter's Pack Issue 4.1	BAE Systems (The Open Group, L.L.C.) (UK MOD)
Table 2 PRA Components Mapped to FACE® Segments	Created as part of Task 8 (CAAP/ 701552387) under the CAAP International Framework Agreement (CAAP/700008174) and updated as part of TQMS task PD-148 under Contract 701575545 for TIKAL Stage 3. Based on information contained within: • FACE® Technical Standard edition 3.2 • PYRAMID Exploiter's Pack Issue 4.1	BAE Systems (The Open Group, L.L.C.) (UK MOD)
Table 3 FACE TSS Capabilities and Relevant PRA Components	Created as part of Task 8 (CAAP/ 701552387) under the CAAP International Framework Agreement (CAAP/700008174) and updated as part of TQMS task PD-148 under Contract 701575545 for TIKAL Stage 3. Based on information contained within: • FACE® Technical Standard edition 3.2 • PYRAMID Exploiter's Pack Issue 4.1	BAE Systems (The Open Group, L.L.C.) (UK MOD)
Table 4 BALSA Instances of PYRAMID Components	Created as part of Task 8 (CAAP/ 701552387) under the CAAP International Framework Agreement (CAAP/700008174) and updated as part of TQMS task PD-148 under Contract 701575545 for TIKAL Stage 3. Based on information contained within: • FACE® Software Supplier Getting Started Guide edition 3.x • PYRAMID Exploiter's Pack Issue 4.1	BAE Systems (The Open Group, L.L.C.) (UK MOD)

EXECUTIVE SUMMARY

The UK 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. The PYRAMID technical solution is underpinned by the PYRAMID Exploiter's Pack, which contains the PYRAMID Reference Architecture (PRA). The PYRAMID Exploiter's Pack and information about PYRAMID is available on the UK government website: https://www.gov.uk/government/publications/pyramid.

The Future Airborne Capability Environment® Technical Standard, or FACE® Technical Standard, is developed and maintained by The Open Group FACE Consortium. The FACE Technical Standard defines a reference architecture intended for the development of portable software components targeted for general purpose, safety, and/or security purposes. It tackles barriers to software modularity, portability, and interoperability.

An assessment has been carried out to determine the feasibility of deploying PYRAMID software components for systems conforming to the FACE Technical Standard. This report provides an assessment of the compatibility of PYRAMID and the FACE Technical Standard, based on the latest versions of the respective open architectures at the time of writing:

- PYRAMID Exploiter's Pack Issue 4.1, containing the PYRAMID Reference Architecture (PRA).
- FACE Technical Standard edition 3.2.

The main conclusion of the initial assessment is that the FACE Technical Standard and PYRAMID are compatible and suitable for use for military aircraft. Furthermore, the FACE Technical Standard and the PRA are complementary standards where:

- The PRA primarily provides definitions for the scope and responsibilities of standardised software components (software applications) which make up the full set of components needed for a military air vehicle system.
- The FACE Technical Standard primarily provides requirements for standardised interfaces and data models, enabling a standard approach to software component interaction and integration with each other, the operating system, equipment and other systems.

This means that, when used together, the opportunities and likelihood for application software to be reused and to be portable across systems are significantly increased.

However, if pre-existing PYRAMID components, developed for platforms not based on the FACE Technical Standard, are required to be redeployed on a platform that does conform to the FACE Technical Standard then some rework will likely be required to make the components conform to the FACE Technical Standard. Likewise, FACE Units of Conformance that have not been designed to adhere to the PRA are highly unlikely to be PYRAMID compliant and so may require significant rework if PYRAMID compliance is required.

CHANGE HISTORY

Date	Issue	Description of Changes
May 2024	Issue 1	First issue

List of Effective Pages

53 pages UK OFFICIAL

53 pages in total

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

ABBREVIATIONS USED IN THIS DOCUMENT

Acronym/Abbreviation	Description
ADS-B	Automatic Dependent Surveillance – Broadcast
AIRCFT	Aircraft
API	Application Programming Interface
ATC	Air Traffic Control
BALSA	Basic Avionics Lightweight Source Archetype
C2	Command and Control
CDM	Conceptual Data Model
CNTL	control
comp	component
CSP	Component State Persistence
DAIS	Defence Assurance and Information Security
DDS	Data Distribution Service
DM	Data Model
DoD	Department of Defence
DSDM	Domain Specific Data Model
EGI	Embedded GPS/INS
FACE®	Future Airborne Capability Environment – Registered Trademarked Symbol
FCAS	Future Combat Air System
FM	Fault Monitoring
GPS	Global Positioning System
HMFM	Health Monitoring and Fault Monitoring
HMI	Human Machine Interface
I/O	Input/Output
ICD	Interface Control Document
ID	Identity
IDL	Interface Data Language
IIOP	Internet Inter-ORB Protocol
IMA	Integrated Modular Avionic Architectures
INS	Inertial Navigation System
IOS	Input Output Services
IOSS	Input Output Services Segment
IP	Internet Protocol
IPR	Intellectual Property Rights
ISR	Intelligence, Surveillance and Reconnaissance
KUR	Key User Requirement
LDM	Logical Data Model
LLC	Limited Liability Company
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
OMI	Operator-Mission Interface
OpenVPX	Working Group developing open backplane standards

Acronym/Abbreviation	Description
ORB	Object Request Broker
OS	Operating System
OSS	Operating System Segment
PCS	Portable Component Segment
PDM	Platform Data Model
PIM	Platform Independent Model
PRA	PYRAMID Reference Architecture
PSCS	Platform Specific Common Services
PSM	Platform Specific Model
PSS	Platform Specific Service
PSSS	Platform Specific Services Segment
QoS	Quality of Service
Ref	Reference
RTPS	Real Time Publish Subscribe
SDM	Shared Data Model
TA	Type Abstraction
TCP	Transmission Control Protocol
TPM	Transport Protocol Module
TS	Transport Services
TSS	Transport Services Segment
UDP	User Datagram Protocol
UK	United Kingdom
UM	Unit of Portability Model
UoC	Unit of Conformance
UoP	Unit of Portability
US	United States (of America)
USM	UoP Supplied Model

REFERENCES

PYRAMID Related Document References:

Reference	Title, Document Number, Issue & Date
[1]	PYRAMID Exploiter's Pack (Crown Copyright), RCO_FUT_23_004, Issue 4.1, September 2023
[2]	PYRAMID Exploiter's Pack Annex A: PYRAMID Reference Architecture Description Document (Crown Copyright), RCO_FUT_23_005, Issue 4.1, September 2023
[3]	PYRAMID Exploiter's Pack Annex B: Deployment Guide (Crown Copyright), RCO_FUT_23_006, Issue 4.1, September 2023
[4]	PYRAMID Exploiter's Pack Annex C: Compliance Guide (Crown Copyright), RCO_FUT_23_007, Issue 4.1, September 2023
[5]	PYRAMID Exploiter's Pack Annex D: Glossary (Crown Copyright), RCO_FUT_23_008, Issue 12.1, September 2023

FACE® Related Document References:

Reference	Title, Document Number, Issue & Date
[6]	FACE® Technical Standard, Edition 3.2, ISBN: 1-957866-29-1, Document Number: C232, August 2023, The Open Group
[7]	FACE® Software Supplier Getting Started Guide, Edition 3.x, ISBN: 1-937218-94-2, Document Number: G173, March 2022, The Open Group
[8]	FACE® Software Supplier Getting Started Guide, Version 1.0, ISBN: 1-937218-94-2, Document Number: G173, August 2017, The Open Group

Other Document References:

Reference	Title, Document Number, Issue & Date
[9]	System and Software engineering – Architecture description, ISO/IEC/IEEEE42010, First Edition, 2011-12-01

1 Introduction

1.1 Overview

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.

This report documents an initial assessment of the feasibility of deploying PYRAMID components for systems conforming to the Future Airborne Capability Environment® (FACE®) Technical Standard.

In order to do so, it assesses and compares the PYRAMID Reference Architecture and the FACE Technical Standard to determine if they are compatible with each other.

1.2 Scope

This report is scoped to the assessment and comparison of the following open architectures:

- PYRAMID Reference Architecture (PRA), contained within the PYRAMID Exploiter's Pack Issue 4.1, which is owned by the UK MOD.
- FACE® Technical Standard edition 3.2, which is developed and maintained by The Open Group FACE Consortium.

1.3 Document Structure

Section 1 is an introduction and identifies the scope and detailed document structure.

Section 2 provides a basic overview of the PRA and the FACE Technical Standard.

Section 3 summarises and compares the benefits of each architecture.

Section 4 includes an assessment of the two open architectures under consideration. It identifies a common characterisation of their scope of concerns to draw high-level conclusions about their compatibility.

Section 5 provides a more detailed architectural comparison and assessment of key areas that would determine the technical compatibility of the standards. This includes:

- An overview of how PYRAMID software components fit into the FACE Technical Standard segments and an assessment of the compatibility of each PRA component with the FACE Technical Standard.
- Consideration of data exchange paradigms and the FACE Transport Service Segment (TSS).
- Consideration of other features of the PRA and FACE Technical Standard that are relevant to their compatibility.

Section 6 summarises the compatibility of the open architectures and feasibility of using them together.

It identifies:

- Areas of compatibility
- Areas of incompatibility
- Other notable considerations for ensuring compatibility and achieving key benefits

Section 7 provides the conclusions.

Appendix A supports Section 5. It provides the detailed results of the PRA component assessment against the FACE Technical Standard, and their applicability to the FACE

Technical Standard Input Output Services Segment and Transport Services Segment capabilities.

Appendix B supports Section 5. It provides an example of using PRA components within a FACE architecture.

2 Overview of the Open System Architectures

2.1 Overview of the PYRAMID Reference Architecture

The PRA defines a reference architecture for the software aspects of functionality of an air system, enabling application software components to be developed consistently and integrated into the air system. At its core is the decomposition of the software aspects into different areas of functionality. The decomposition consists of a number of standardised 'building-blocks' called components. Each PRA component definition specifies its role and responsibility, as well as other supporting information. The role and responsibilities act as the requirements and constraints for the software design of a PYRAMID component.

The PRA also provides various policies that underpin and provide guidance on the application of PRA components, as well as interaction views that give examples of how PRA components can interact to provide typical mission system functions.

Figure 1 shows the different PRA components, which for illustration and familiarisation purposes are broadly grouped by traditional sub-system functions. Note that the PRA has no actual concept of these sub-systems however.

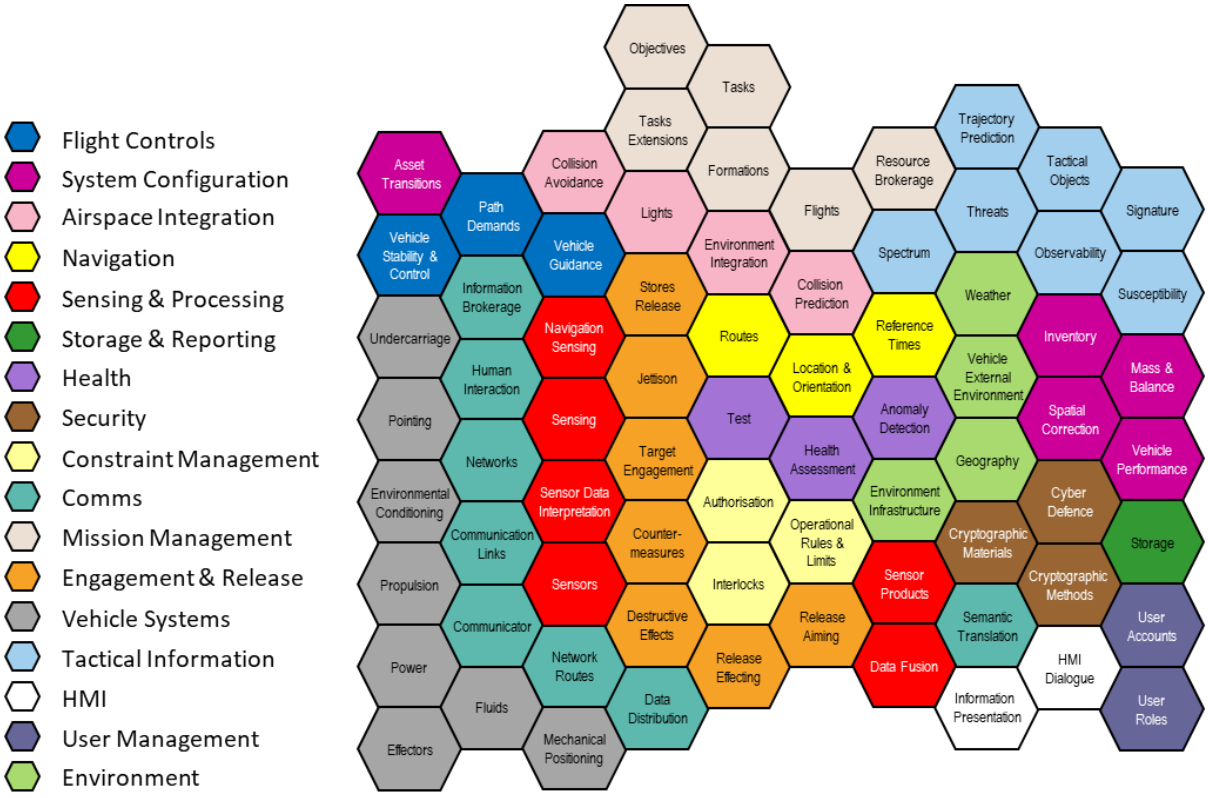

Figure 1: PRA Components

The concepts covered by the policies are wide in scope. They include the following, which are particularly relevant within this report:

- Data Driving – the concept of applying data to a PYRAMID component, either before or after the component design is compiled into executable software. This concept allows the component design to be abstracted from specific details which could vary depending upon factors such as user requirements and specific equipment details.
- Component Extensions – the concept of splitting a PRA component into a parent component and one or more extension components. This allows partitioning to

support considerations such as safety, security, interchangeability and catering for specific equipment. The concept of component extensions is in effect a special case of multiple instances or variants of PYRAMID components complying to the same PRA component.

2.2 Overview of FACE® Technical Standard

The FACE® (Future Airborne Capability Environment®) Technical Standard is a standard published by the Open Group. The FACE Technical Standard defines a reference architecture intended for the development of portable software components targeted for general purpose, safety, and/or security purposes.

It achieves this through defining five architectural segments and requirements for a data architecture and standardised interfaces.

The five segments of the FACE Reference Architecture are listed below and shown in Figure 2:

- Operating System Segment (OSS)
- Portable Components Segment (PCS)
- Transport Services Segment (TSS)
- Platform-Specific Services Segment (PSSS)
- Input/Output Services Segment (IOSS)

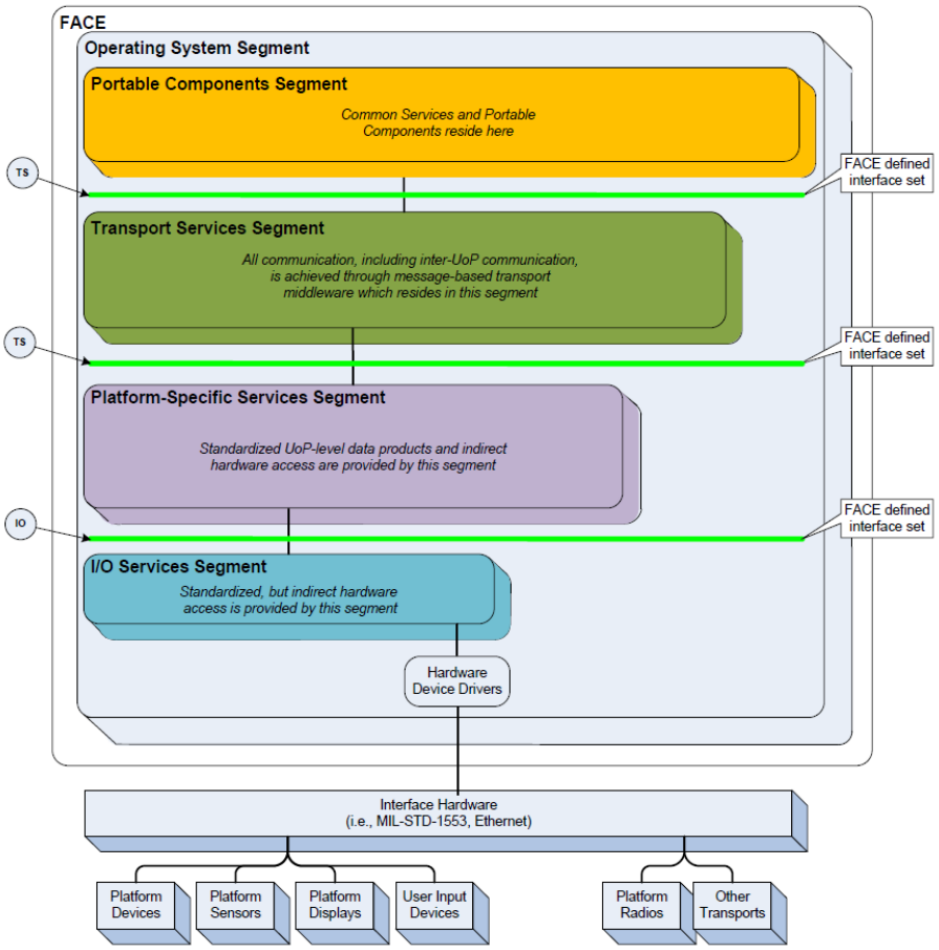

Figure 2 FACE® Architectural Segments
(figure 2 from FACE Technical Standard (Ref. [6]), © 2023 The Open Group)

3 Architecture Objectives

3.1 Introduction

This section summarises the purpose behind the PRA and the FACE® Technical Standard through identification of their principal requirements and architecture objectives.

3.2 PYRAMID

3.2.1 Architecture Objectives

The UK PYRAMID vision is to produce air mission systems that are efficiently developed, deployed and maintained to realise affordable, capable and adaptable military capability. The UK aims to develop new mission systems and transition legacy mission systems towards conformance with a comprehensive open architecture framework leveraging a library of reusable components enabled by systematic reuse processes.
This is encapsulated in the PYRAMID single statement of user need that is supported by a number of key user requirements (KURs):

> ***"To enable delivery and maintenance of Technology Advantage the User requires a core Mission System that is: inherently resilient to Obsolescence; Scalable; Exploitable; Flight Certifiable; Security Accreditable; Configurable; provides Utility across a range of mission requirements; and incorporates Future Growth potential."***

3.2.2 Principal Requirements/Approach

The purpose of the PRA is captured by the following KURs:

- **Resilient to Obsolescence** – The user shall be able to deploy the PYRAMID mission system onto a range of underlying computing platforms, and therefore it shall not be tied to the Original Equipment Manufacturer's computing solution.
- **Scalable** – The user shall be able to deploy complete (or selectable part) instances of the PYRAMID Mission System into integrated system solutions that form part of a range of families of systems that span the full range of platform system classes.
- **Exploitable** – The user shall be able to deploy the PYRAMID Mission System architecture and associated software components across multiple National, Collaborative and Export Equipment Programmes, utilising the open reference architecture to gain maximum leverage for the UK supplier base and maximum return on investment on this reusable capability.
- **Flight Certifiable** – The user shall be able to have instances of the PYRAMID Mission System certified for Flight (against Civil and Military regulations) as part of a complete system deployment.
- **Security Accreditable** – The user shall be able to have instances of the PYRAMID Mission System security accredited by Defence Assurance and Information Security (DAIS) against MOD security policy and with security risks mitigated to a level acceptable to the relevant security risk owner.
- **Configurable** – The user shall be able to configure instances of the PYRAMID Mission System such that mission capability exploits available and emerging hardware, software and data services with minimal impact on the qualified Mission System. Configurable items include - System Behaviour with varying levels of autonomy, during both planning and airborne phases, across all areas associated with

mission/flight management; sensor, weapon and defensive aids employment; data handling and appropriate vehicle system interfaces. Additionally, the user shall be able to configure necessary elements of the Operator-Mission Interface (OMI), including Human Machine Interface (HMI) aspects.

- **Utility Across a Range of Missions** – Dependent upon the core capabilities of the host air vehicle, the user shall be able to participate in a broad gamut of operations including: Intelligence, Surveillance and Reconnaissance (ISR); Command and Control (C2); Attack; and Control of the Air. The user shall also have the ability to conduct communications relay and where present operate any associated defensive aids systems.
- **Incorporate Future Growth** – The user shall be able to further develop the PYRAMID Mission System reference architecture and deployed instances of the PYRAMID Mission System through evolutionary changes in response to operational and non-operational drivers with the minimum of resource and time overhead.

One of the key approaches of the PRA, in response to this set of KURs, is the principle of the 'separation of concerns'. This drives the PRA requirement for developers to adhere to the PRA component definitions, which clearly separate subject matter, and therefore associated functionality, between PRA components. This helps to ensure that no single component is inherently dependent on the specific design of any other component.

3.3 FACE® Technical Standard

3.2.1 Architecture Objectives

The FACE Technical Standard states that:

"Ultimately, the FACE key objectives are to reduce **development costs**, **integration costs**, and **time-to-field** for avionics capabilities."

"The FACE technical approach tackles barriers to **modularity**, **portability**, and **interoperability** by defining a Reference Architecture and employing design principles to enhance software portability."

In order to achieve these overall objectives, the FACE Technical Standard objectives are stated as being to:

- "Define the FACE Reference Architecture for developing and verifying software components
- Define the FACE Reference Architecture for defining interfaces allowing communication between software components
- Enable affordability, interoperability, and time-to-field across military systems based upon fundamental software engineering principles and practical experience"

3.3.1 Principal Requirements/Approach

To meet its objectives, the FACE Technical Standard employs several software engineering practices, focusing on the following principals, as stated within the FACE Technical Standard:

- "Use published industry standards to provide normative references, allowing the use of existing software libraries and tools whenever possible
- Use profiles to define subsets of those standards when support of the entire standard would lead to safety or security certification issues, or when supporting only a defined subset would lead to a more cost effective solution; a profile can also reference a specific version of a standard in its entirety

- Use a standardized architecture describing a conceptual breakdown of functionality and the FACE Reference Architecture to promote the reuse of software components to share common functionality across military systems
- Define standardized interfaces to allow software components to be moved between systems developed by different vendors
- Use a data architecture to ensure the data communicated between the software components is fully described to facilitate the integration on new systems
- Require that hardware abstraction be used to decouple software components from specific hardware implementations, and device driver normalization be used to allow interfaces to external devices to be developed independently of the computing platform device drivers
- Use a display window management strategy to incorporate common avionics user interface standards to aid in the integration of components needing to share display areas and input devices

This technical approach enables software components to be redeployed on other platforms to achieve greater portability and interoperability when standardized FACE Interfaces are used."

3.4 Common User Objectives

From a comparison of the PRA and FACE Technical Standard architecture objectives, principal requirements, and approaches, it can be seen that the PRA and FACE Technical Standard have similar and compatible aims.

The PRA and FACE Technical Standard both aim to allow users to reduce the time taken to deploy systems and system updates.

The FACE Technical Standard objective of reducing development and integration costs, or increasing affordability, is supported by the following PYRAMID KURs:

- The 'Resilient to Obsolescence' KUR supports the FACE architecture objective of reducing costs by reducing redevelopment costs when updating the underlying computing platform.
- The 'Incorporate Future Growth' KUR supports the FACE architecture objective of reducing costs by reducing in-service development costs.

These are also supported by the PYRAMID 'Configurable' KUR, which requires mission system requalification to be minimised and therefore further supports cost reduction.

The FACE Technical Standard objective of enabling modularity, portability and interoperability is supported through the PRA separation of concerns by decomposition of the software aspects into different areas of functionality.

Furthermore, the FACE Technical Standard objective of enabling interoperability between software components is supported by the PRA 'Configurable' and 'Utility Across a Range of Missions' KURs.

4 Open System Architecture Scope Comparison

4.1 Introduction

This section includes an assessment of the two open architectures under consideration through characterisation of their scope of concern, to draw high-level conclusions about their compatibility.

4.2 Assessment Approach

The assessment approach taken identified characteristics defining the architecture scope of concerns (a term defined by ISO_IEC_IEE42010 (Ref. [9]) to describe any influence on a system). The assessment looked for alignment of these concerns in the different architectures. The concerns are characterised below and reproduced in Figure 3: Scope of Concerns Considered for Architecture Assessment:

- Operational Context

  Architectures can consider different operational contexts such as use by:
  - Sovereign military forces
  - Civilian organisations
  - Multinational military coalitions
  - Military and emergency service cooperation.
- Abstraction Levels

  Architectures can consider a single or multiple levels of abstraction such as:
  - Conceptual descriptions of observable properties
  - Logical representations and measurable properties
  - Physical data message primitives
  - Actual instances of entities.
- Deployment Platform

  Some architectures can restrict themselves to specific operational platform types such as:
  - Unmanned air vehicles
  - Control systems for unmanned vehicles
  - Manned aircraft such as fighters
  - Manned land vehicles or bases
  - Maritime vessels
  - Support systems such as planning and debrief stations
  - Sensor systems
  - All - Some architectures are agnostic of the actual operational platform.
- Engineering Concerns

  Architectures can focus on specific aspects of a system or present multiple views of the following:
  - Scenarios and use cases
  - Business processes and business logic
  - System elements
  - Software elements

- Hardware elements
- Information exchanged
- Organisation of information in the system under consideration.

- Engineering Artefacts

  Architectures can focus on describing engineering aspects such as:
  - Scope and behaviour of the system components
  - The state transitions within a system and operational state of its components
  - Specification of layers to abstract applications from the middleware and the underlying hardware.

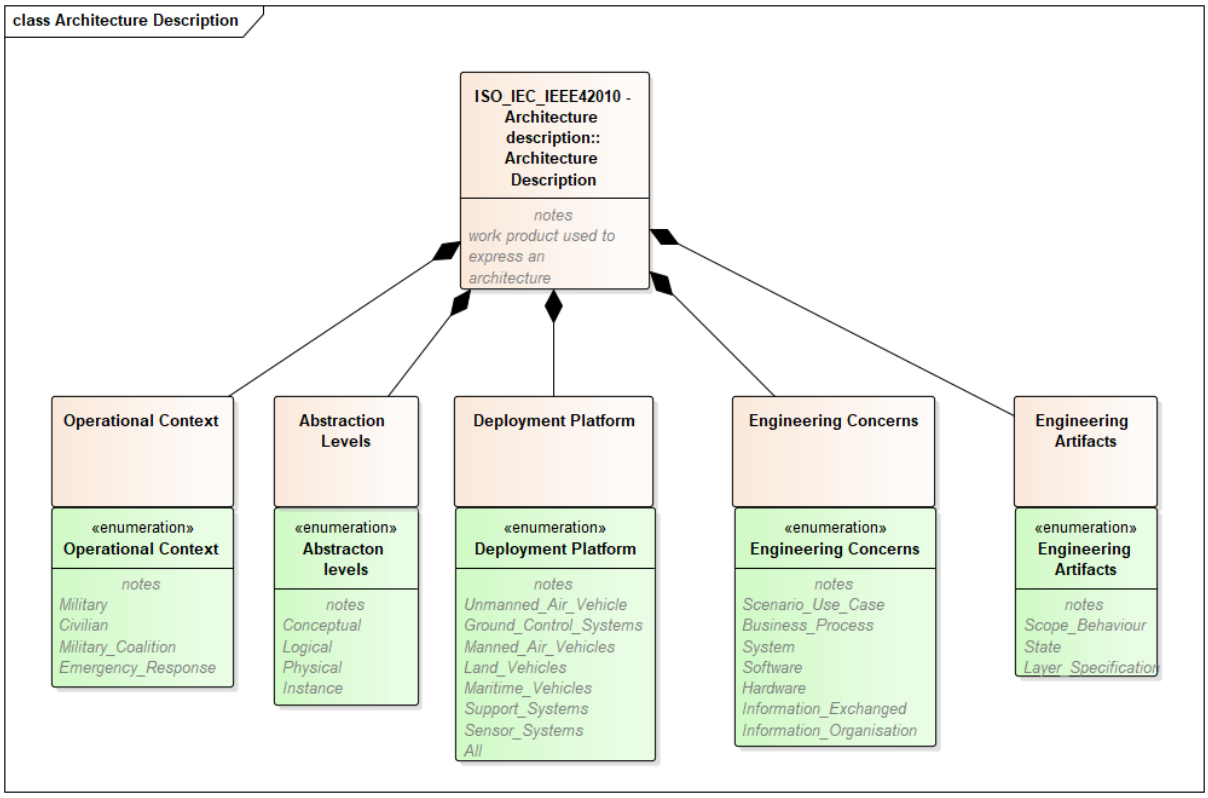

Figure 3: Scope of Concerns Considered for Architecture Assessment

4.2.1 High Level Assessment

The initial compatibility assessment of the PRA and the FACE Technical Standard is summarised in Table 1. Note the entries in the table and the column characterisations are described in Section 4.2.

Architecture	Operational Context	Deployment Platforms	Engineering Concerns	Engineering Artefact Description	Abstraction Level
PRA	Military	Agnostic	Software	Scope_Behaviour	Conceptual
FACE	Civil/ Military	Agnostic	Software	Layer_Specification	Conceptual, Logical, Physical

Table 1 Comparison of PRA and FACE® Architecture Concerns

The PRA provides the conceptual partitioning for software applications as well as their required behaviour. The FACE Technical Standard defines the software structure, data exchange and open standards that provides access to between software applications, operating systems and hardware.

At this high level of comparison it can be stated that the PRA and FACE Technical Standard appear to be compatible, have complementary purposes and are suitable for use on current and future military platforms.

5 Detailed Architecture Comparison and Assessment

5.1 Introduction

This section provides the outcome of a deeper analysis of the architectures. It focuses on the fundamental aspects of the architectures.

The topics considered are as follows:

- An overview of PRA artefacts and FACE artefacts.
- An assessment of the PRA components against the FACE Technical Standard, considering their applicability to the FACE Technical Standard segments.
- An assessment of the methods of data exchange expected by the PRA and required by the FACE Technical Standard, including consideration of:
    - PRA bridges
    - The FACE Technical Standard approach involving data models, normalised interfaces and the Transport Services Segment.
- Consideration of other features of the PRA and FACE Technical Standard that are relevant to their compatibility.
- This section is supported by Appendix A and Appendix B which provide:
    - For each PRA component, the detailed results of the PRA component assessment against the FACE Technical Standard, and their applicability to the FACE Technical Standard Input Output Services Segment and Transport Services Segment capabilities.
    - An example of the use of the PRA components the FACE Technical Standard. This is based on the example use case within the Basic Avionics Lightweight Source Archetype (BALSA) architecture described in the publicly available FACE Software Supplier Getting Started Guide (Ref. [7]).

5.2 PRA Components and FACE® Units of Conformance/Portability

A PRA component is a platform independent component that includes:

- a name
- a role
- a set of responsibilities
- a subject matter semantics definition
- a set of services
- other supporting information.

Platform independence, from the PRA perspective, means independence from the computing platform, including any associated operating system and middleware.

Although the PRA component services contain conceptual attributes, these do not define specific data definitions or data structures, and the PRA does not require adherence to any specific data structure or data definition other than the data being within a PRA component's scope.

The PRA component specifications are used by developers to develop executable software instances of these components, referred to within this document as PYRAMID components. The PYRAMID Exploiter's Pack Deployment Guide suggests different software development lifecycle stages, including a Platform Independent Model (PIM), a Platform Specific Model

(PSM) and ultimately generation of executable software. However, this is not mandated by the PYRAMID Exploiter's Pack Deployment Guide.

The PRA allows and recognises the need for multiple instances of the same PRA component to be developed and deployed on the same exploiting platform.

The FACE Technical Standard uses the term Unit of Conformance (UoC). (The term Unit of Portability (UoP) is sometimes used instead to highlight a UoCs portable and reusable attributes.) These are software artefacts developed to meet the conformance requirements of the identified FACE Operating System Segment (OSS) profile(s), a single FACE segment or FACE interface capability. The FACE Technical Standard contains individual requirements for UoCs for each FACE segment, each FACE interface and each FACE OSS Profile. The FACE Technical Standard does not define the required functional content of a UoC.

In order to aid achievement of the PYRAMID and FACE Technical Standard goals, it is generally expected that each PYRAMID component instance would be developed as a single FACE UoC. This is not mandated and deviating from this should not prevent compatibility. However, in most cases this would be desirable, since doing so standardises the capabilities provided by any UoCs within the PRA scope, thereby increasing the likelihood of different combinations of UoCs being able to work together on the same platform. This could:

- Ease integration, including integration costs and timescales.
- Increase the scope for compatibility between 'off the shelf' UoCs or UoCs being ported from one platform to another.
- Increase the opportunities to switch between alternative UoCs, such as from different vendors, that are compliant to the same PRA component. Such UoCs could provide the same general functionality, yet may provide different specialisations or optimisations to their capability.

In practice this approach, or the benefits gained from this approach, will likely be limited to UoCs for the Portable Component Segment (PCS) and Platform Specific Services Segment (PSSS), which are discussed in the next section. Nonetheless, this approach is assumed in this report unless stated otherwise.

5.3 PRA Components and FACE® Segments

FACE segments have strict and formal data definitions of the interfaces that separate the segments. In contrast, the PRA considers each of its components to exist in isolation and does not require compliance with an interface layer definition.

The FACE segments, shown in Figure 4, are:

- Portable Component Segment (PCS):
  - Consists of common services and portable services.
- Platform Specific Services Segment (PSSS):
  - Consists of services containing device specific business logic and platform specific functions.
- Input/Output Service Segment (IOSS):
  - Consists of adaptors to allow vendor-supplied drivers to support the abstracted FACE interface.
- Operating System Segment (OSS):
  - Consists of system services such as low-level health and vendor-supplied software.

- Transport Services Segment (TSS)
    - Consists of communication services to exchange data in accordance with the FACE Data Architecture

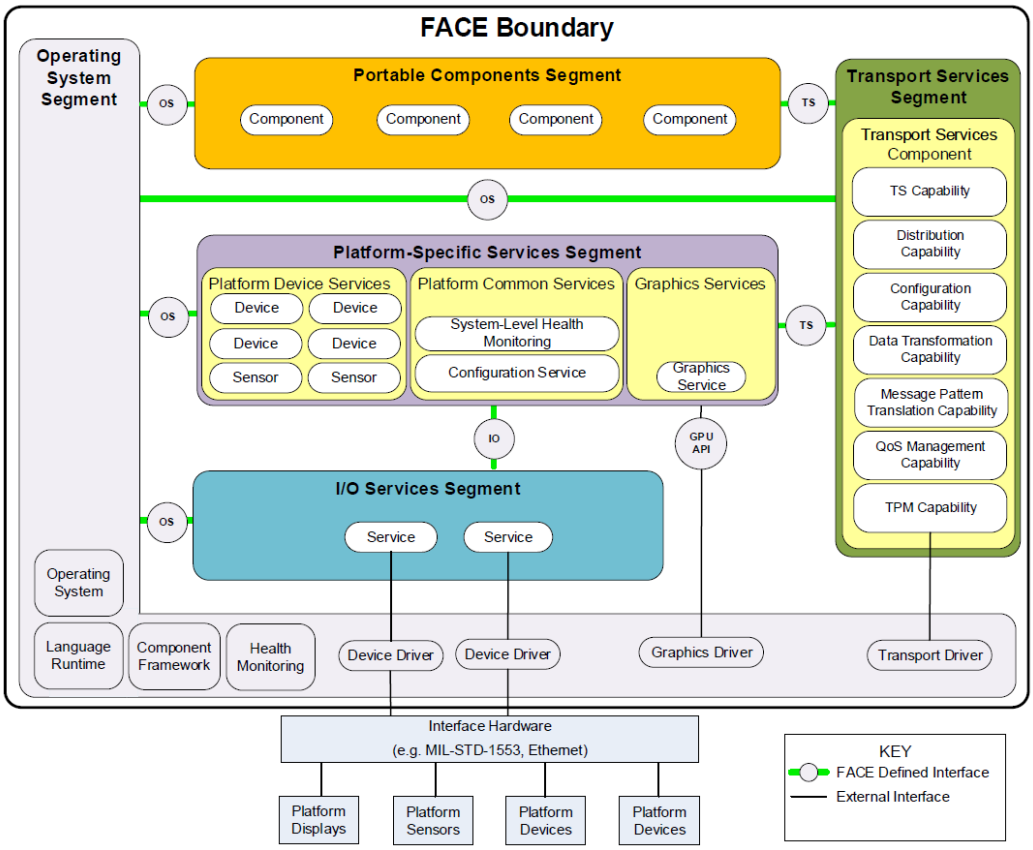

Figure 4 FACE® Segments and FACE Interfaces
(figure 10 from FACE Technical Standard (Ref. [6]), © 2023 The Open Group)

The PRA has a concept of different control architecture layers (defined by its Control Architecture policy) where each PRA component is allocated to a layer which defines its role in meeting mission objectives. The concept does not restrict how components are developed, or which components interact with each other. However, it does help to show how mission requirements can be refined into more specific requirements. The control architecture layers are:

- Objective
- Task
- Action
- Resource
- Service.

This concept is not significant to the PRA compatibility with the FACE Technical Standard; however, it does enable a general trend to be observed where PRA components in a particular layer lend themselves to being used within particular FACE segments. For example, some PRA resource components lend themselves to the FACE PSSS.

5.4 Assessment of PRA Component Compatibility with the FACE® Technical Standard

An assessment of each PRA component has been carried out to determine if there are any compatibility issues with PRA components and the FACE Technical Standard. The conclusion of the assessment determined that there are no fundamental compatibility issues.

The assessment included the determination of which FACE segment(s) is applicable for each of the PRA components. The aim of this activity was to determine whether any PRA components do not fit within any FACE segment(s), as well as to determine which PRA components fit within multiple FACE segments and if this causes any issues. This then supported the assessment of the component, by allowing a more focussed assessment against the relevant FACE segment and interface requirements, to determine if the component is likely to be non-conformant to the FACE Technical Standard.

The applicability of PRA components to FACE segments is not intended as a final or definitive categorisation for all deployments.

The results are shown within Appendix A Table 2, and no inherent non-conformance issues were identified.

Note: *In order to best achieve the benefits of PYRAMID and the FACE Technical Standard, such as reuse, it is recommended that in general each PYRAMID component is developed as a single UoC. However, some components (such as Anomaly Detection) are intended to be developed as specialised instances to sit alongside other PRA components. In such cases they could be developed either as separate UoCs or within the same UoC as the component that they support.*

All of the PRA components have been assessed as being applicable to at least one FACE segment. However, many of the PRA components do not definitively sit within a single FACE segment mainly for the following reasons:

- The most appropriate segment will often depend on the level of commitment to producing portable components that are suitably independent of specific equipment interface message structures and data definitions.
- The PRA concept of component extensions could allow for a generic core component, for example in the PCS, to have extensions in other segments, such as the PSSS if the extension incorporates equipment specific details. Alternatively, separate PYRAMID component variants could be used in different segments, instead of using extensions.
- Some PRA components, such as Anomaly Detection, are expected to have many specialised deployed instances and will therefore appear in multiple FACE segments, with the applicable segment being dependent on the type of specialisation being applied. As such different instances will naturally appear in different FACE segments without any associated problems.

  This tends to be particularly true for components relating to:

  - Communications
  - Health
  - Information Assurance.
- The PRA Effectors, Sensors and Communicator resource components are specified to be quite flexible in the level of detail that they are involved in. The consequence of this is that in some circumstances it may be necessary to split such components into two instances where one can reside in the PSSS and another in the IOSS.

The only potential concern for having PRA component extensions or instances within different FACE segments is that when reusing PYRAMID components developed for a system not based on the FACE Technical Standard for a system that is it may be necessary to perform some redevelopment to split such components to conform to the FACE Technical Standard segment requirements. In the case of separating components to enable the relevant parts to reside in a combination of the PCS and PSSS, this would be desirable, rather than a necessity, to improve future portability of PCS UOCs rather than having the whole component reside in the PSSS.

Note that when reusing PYRAMID components from a system not based on the FACE Technical Standard on a system that is based on the FACE Technical Standard other redevelopment is also likely to be needed, such as in order to ensure that the component interface conforms to the FACE data model and interface requirements.

5.5 Data Exchange and the Transport Service Segment

5.5.1 Bridges and Data Architecture

5.5.1.1 PYRAMID Bridges

PRA components are loosely coupled and do not share interface definitions. This creates a semantic gap between the information being exchanged at the interfaces of different components. Therefore, special inter-component bridges perform the semantic translation (e.g. the conversion between data types).

Note: *Whilst a deployment of PYRAMID components requires bridges, the PRA does not specify any bridges.*

Figure 5 provides examples of different bridges performing different semantic conversions.

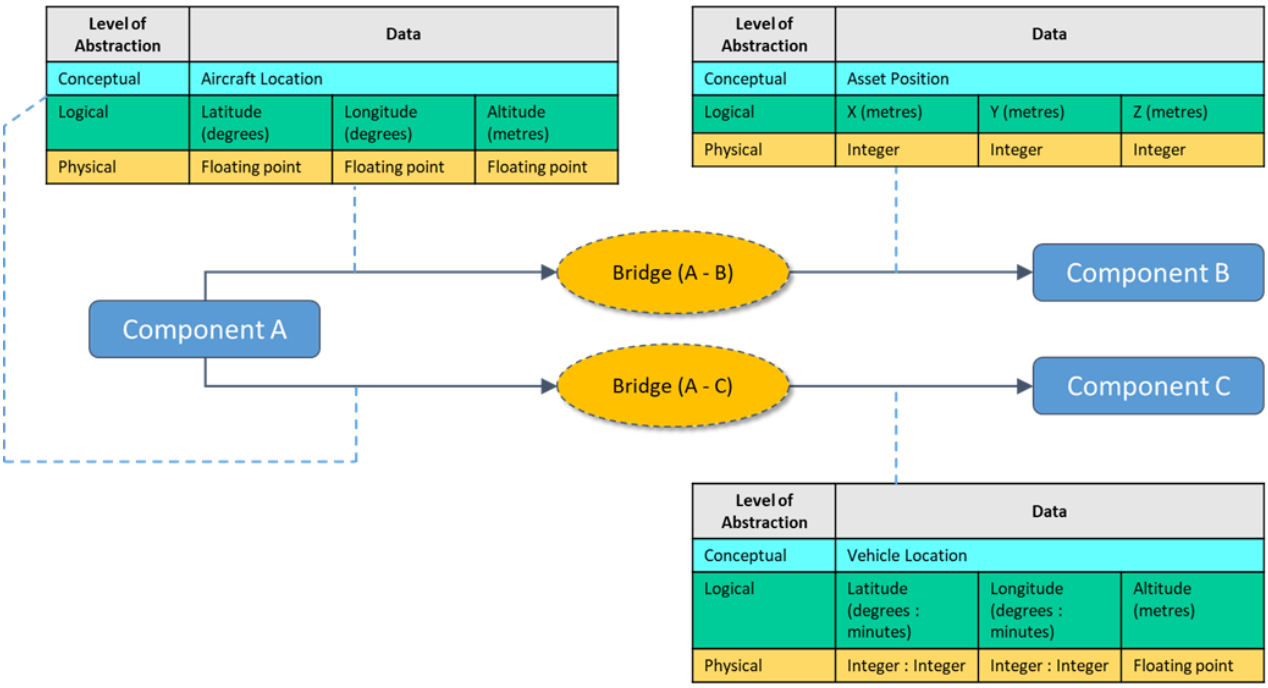

Figure 5 Examples of Bridges Performing Semantic Conversations

Bridges also have the role of logically connecting the required services of components to the provided services of components able to satisfy these.

5.5.1.2 FACE® Data Architecture

The FACE UoCs share interface definitions through conformance to the FACE Data Model Definition indicated below in the upper part of Figure 6.

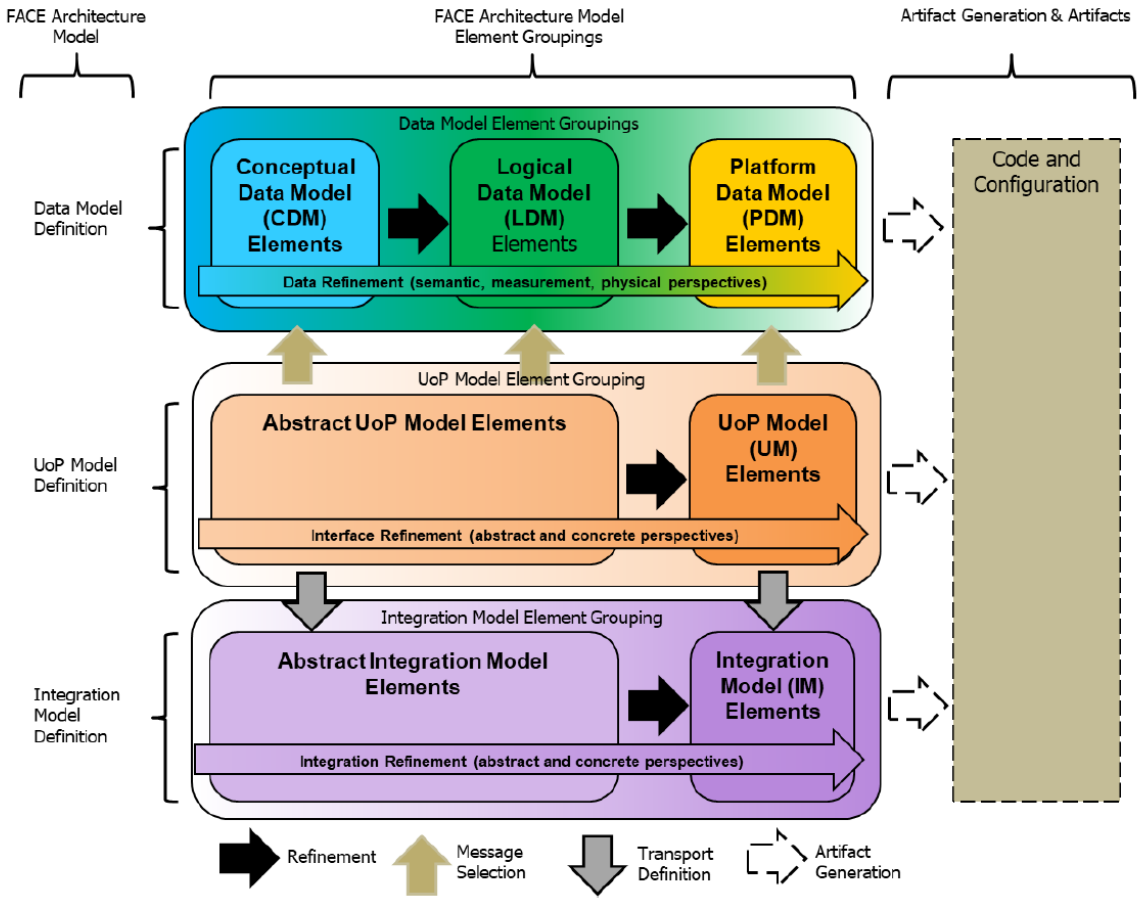

Figure 6 FACE® Model Architecture
(figure 19 in the FACE Technical Standard (Ref. [6]), © 2023 The Open Group)

Whilst the PRA does not define a data architecture, it recognises that a data architecture is needed to enable components to interact. Furthermore, the FACE Data Architecture separates the conceptual, logical and platform (physical) aspects of the data model in an equivalent way to the approach to developing PYRAMID component services suggested in the PYRAMID Exploiter's Pack Deployment Guide (Ref. [3]). (Note that the platform data model is referred to as physical instead of platform in the PYRAMID Exploiter's Pack Deployment Guide; however, the concept is the same.)

Although the PRA includes services within its component definitions, these are defined at an abstract level, which would not conflict with a FACE data model, and their data names, types and structures are not mandated by the PRA. A FACE data model should therefore build upon, by adding detail, the more abstract services defined within the PRA.

5.5.2 Transport Service Segment

The Transport Services Segment (TSS) provides capabilities related to data access and standardised interfaces for UoCs located in the PCS and PSSS, as well as other supporting capabilities, to facilitate PCS and PSSS UoC interaction and integration. These capabilities are utilised by a PCS and PSSS UoCs through the Transport Services (TS) interface and the

Component State Persistence (CSP) interface, where the CSP interface can support storage of data that is local to a PCS and PSSS UoC.

Support capabilities specified within the TSS may include distribution, routing, prioritisation, addressability, association, abstraction, and transformation of software component information. It supports transport capabilities both within the same system and across systems, using a variety of protocols.

The detailed functional components of the TSS are shown in Figure 7.

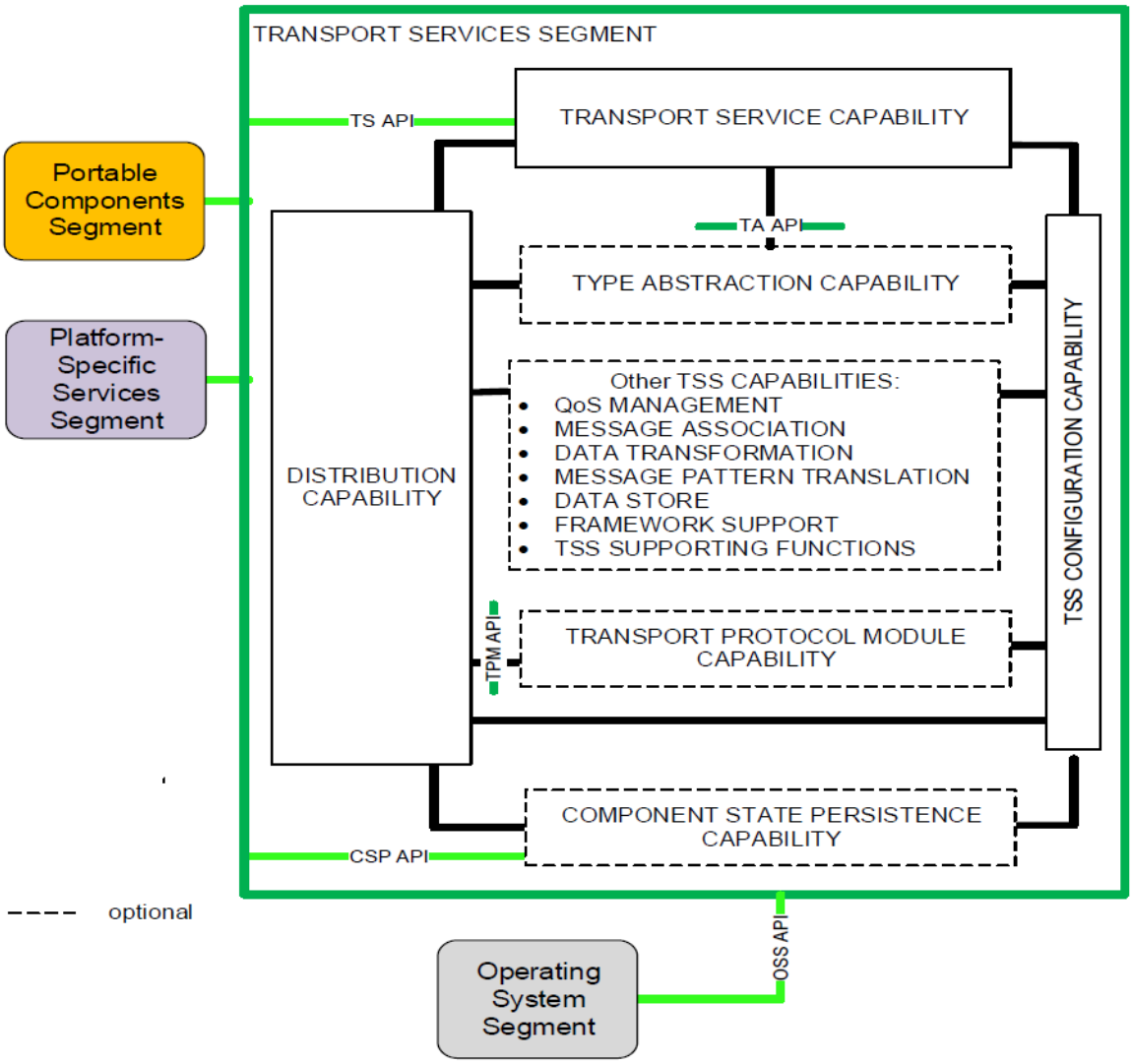

Figure 7 Detailed Structure of the TS Segment
(figure 13 from FACE® Technical Standard (Ref. [6]), © 2023 The Open Group)

The FACE TSS uses supplier provided data definitions, which conform to the FACE Shared Data Model (SDM), to generate internal data models and TSS UoC software to facilitate data exchange.

The TSS can fulfil the role of a bridges, both in terms of semantic translation and connecting PYRAMID component interfaces, for any PYRAMID components interacting with other PYRAMID components when all of the components are in the FACE PCS, PSSS or a combination of the two.

The capabilities of the TSS are far greater than those required just for bridges. The TSS fulfils many of the capabilities that can be provided by some of the PRA communications related components for specific applications. It would therefore be possible to use these PRA components in order to develop UoCs for the TSS. Appendix A Table 4 provides an initial assessment of where PRA components are likely to be applicable to the different parts of the TSS.

Likewise, TSS UoCs that are developed not using PRA components would be compatible with PYRAMID components in the PCS and PSSS.

5.5.3 PSSS to IOSS Data Exchange

The TSS does not cater for component interactions between the PSSS and the IOSS. This is done through the FACE Technical Standard Input Output Services (IOS) interfaces.

Any situation where the FACE Technical Standard forces different PRA components to interact with each other using the IOS interface is a potential concern for PRA and FACE Technical Standard compatibility. This is because directly sharing identical data between different components can imply that a component does not comply with the PRA. Therefore, the cases where the IOS may be used have been carefully assessed.

The assessment, shown within Appendix A Table 2 and Table 3, has determined that the only PRA components providing the IOS interface should be the Communicator, Sensors or Effectors components, with these potentially being augmented with the Anomaly Detection or Cryptographic Methods component (as discussed later). Most cases will be catered for by the Communicator component, whereas specific cases involving very unique equipment interfaces, may be catered for by the Sensors and Effectors components.

The interactions between the PSSS and IOSS should be either:

- Between different variants of the same PRA component (i.e. between different variants of either the Sensors, Effectors or Communicator component UoCs). Where appropriate, these may be implemented as a parent and an extension component (as described in the PRA Component Extensions policy). The PSSS component would provide the higher level equipment specific controls, whilst the IOSS component would provide the normalised to specific interface conversion for data transmission and reception.
- Between the Data Distribution component, within the PSSS, and the UoC for either the Sensors, Effectors or Communicator component, within the IOSS.

Neither of these situations should result in PYRAMID compliance issues since:

- In the first case (above) the components can share the same semantic interpretation of data and therefore conform to the same IOS interface definition.
- In the second case (above) part of the responsibilities of the Data Distribution component are to appropriately collate or disseminate, format and structure data for transfer to or from an interface. It is therefore able to adhere to the normalised IOS interface. Furthermore, the specialised versions of the Sensors, Effectors or Communicator components within the IOSS would be specifically there to provide the normalised interface and so would inherently adhere to it.

Versions of the following PRA components have been identified as potentially being incorporated into the IOSS:

- Anomaly Detection
- Cryptographic Methods
- Cyber Defence

However, these components would only ever be incorporated within the same UoC as another component (either the Communicator, Sensors or Effectors component). This is because, a standalone implementation of the Anomaly Detection, Cryptographic Methods or Cyber Defence components in an IOSS UoC would not provide an I/O service, and so would not meet the FACE Technical Standard requirement that specifies 'an IOSS UoC shall provide at least one I/O Service'.

In the case of Anomaly Detection, the component would provide only some of the information sent, from the IOSS UoC, on the IOS interface. This is not considered to be a problem for PYRAMID compliance because PYRAMID components within the PSSS, using the IOS interface, would only use the information that they require, rather than consuming all of the information in the IOS interface message. Furthermore, it is expected that where multiple components within the PSSS need to send or receive different information in the same IOS interface message, the PRA Data Distribution component will act as an intermediatory allowing the relevant data to be appropriately restructured and reformatted to or from the IOS interface message.

Whilst it is theoretically possible that the Cryptographic Methods component could directly interact with the IOS interface to encode/decode a message, it would never be aware of the meaning of the data being encoded/decoded, and so this would not cause a PYRAMID compliance problem.

5.5.4 Bridge Functions within UoCs

Where beneficial to do so, bridge data translation, including semantic conversion, could be incorporated as a dedicated data translation module within the same UOC as a PYRAMID component. This would act as a 'wrapper' or 'façade', allowing the PYRAMID component interface design to be different to that presented by the UoC for interaction, whilst still enabling conformance with the FACE Technical Standard interface and data model requirements.

Such an approach may be desirable in order to enable a PYRAMID component to be ported from, and potentially to, other computing equipment that does not conform to the FACE Technical Standard, with no change to the PYRAMID component.

5.6 Additional Features and Considerations

There are a number of features of the FACE Technical Standard that are outside the scope of the PRA, which must be observed when developing PYRAMID component UoCs and which can aid successful PYRAMID software development.

Whilst not an exhaustive list, the following in particular are worth noting:

- Injectable Interfaces – providing a standardised approach to establishing interfaces between PYRAMID component UoCs during runtime.
- Component Life Cycle Management Services – supporting PYRAMID component UoCs initialisation, configuration, connection and state.
- Health management of the computing environment and standardised interfaces for computing health information.
- Different Operating System Segment profiles to support differing levels of required component safety and security integrity.

All of these features have been determined to be complimentary to and compatible with the PRA. However, since the topic of health management required a more in depth analysis during the assessment, to determine if there are any compatibility issues, it is worth summarising.

5.6.1 Health Management

The PRA provides system wide health management related capabilities, but relies on middleware/operating systems to provide health information about the computing hardware and faults/errors with the running of software. This is predominately achieved through the following components:

- Anomaly Detection– which monitors for and detects anomalous behaviour of the system.
- Health Assessment– which diagnoses health issues when health related anomalies are detected and provides life, usage and fatigue monitoring and determination.
- Cyber Defence – which diagnoses cyber attack issues when cyber attack related anomalies are detected, and initiates protective actions.

The Health Assessment component assesses the health of:

- Aircraft structures; e.g. these may consider aspects such as life and fatigue of equipment and structures.
- Computing equipment and their interconnections – these will draw upon information provided by the computing equipment middleware/operating system.
- Other specific equipment, for example sensors and lights.

OSS Health Monitoring and Fault Management (HMFM) UoCs conforming to the FACE Technical Standard provide methods of detecting, reporting, and handling faults and failures associated with the computing hardware on which it is hosted, including any directly associated communications infrastructure. This includes runtime faults and errors at the different levels of process (i.e. thread) level, partition level and module level. The faults can arise from applications in other segments or from the OSS. Upon detection of a fault or error, the HMFM cycle, shown in Figure 8 below, is engaged to direct the computing system back to a healthy state or to some failsafe state.

The OSS HMFM are supported by standardised operating system (OS) interfaces.

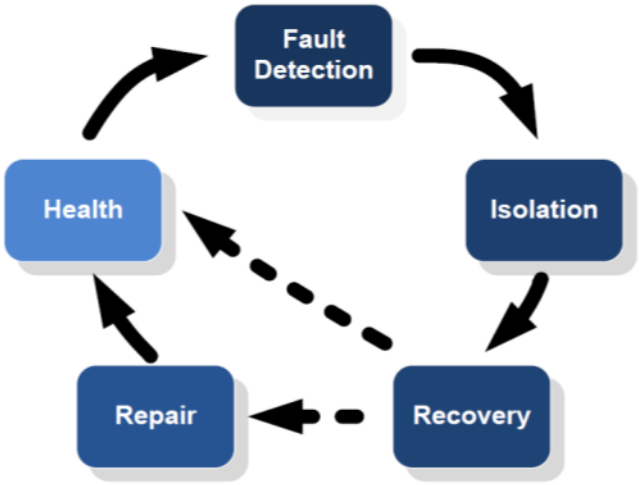

Figure 8 Fault Management Cycle State Machine
(figure 5 from FACE® Technical Standard (Ref. [6]), © 2023 The Open Group)

The role of OSS HMFM UoCs is distinct from the PRA health related components, which deal with computing infrastructure issues at a higher level of abstraction and non computing infrastructure health considerations. Furthermore, the OS HMFM interfaces enable a

standardised approach to supplying the PRA health components with input data, about the computing infrastructure, that they need to carry out their role.
Whilst the PYRAMID health related components need to cater for specifics associated with particular platforms, it is expected that their underlying definition could be common across platforms, with their specifics being data driven – probably prior to compiling the software. Therefore, whilst the executable software UoC may not be portable the underlying design and, when based on the FACE Technical Standard, their interfaces could be common, thereby providing a level of portability.

6 Summary of Compatibility and Feasibility

6.1 Introduction

This section characterises aspects of the PRA and the FACE® Technical Standard, as follows:

- Areas of compatibility – where the architectures lend themselves naturally to operate together.
- Areas of incompatibility – where the architectures are mutually exclusive such that the rules of the two architectures cannot be met at the same time. Note that no such areas have been identified.
- Other notable considerations related to achieving compatibility and key benefits.

6.2 Areas of Compatibility

6.2.1 Architecture Benefits

Section 3 identified that both the PRA and the FACE Technical Standard support:

- Reduction of development time and costs during initial development and through life maintenance cycles.
- Portable software component development.

6.2.2 Architecture Assessment

Section 4 identified that the architectures are compatible and have complementary purposes within the context of military fighter aircraft:

- The PRA provides the conceptual partitioning of software applications, abstracted away from hardware and platform implementations, as well as their required behaviour.
- The FACE Technical Standard provides definitions of the software structure, data exchange policies and open standards that define access to hardware.

6.2.3 Component Compatibility

Section 5 identified that all PRA components can be utilised within at least one FACE segment, and that all of the PRA components are compatible with the FACE Technical Standard. Furthermore, Section 5 identified that it should be possible to connect PYRAMID compliant components using the interfaces and data modelling approach required by the FACE Technical Standard.

Through the use of an independent use case, Appendix B provides further confidence that it is possible to use the PRA in conjunction with the FACE Technical Standard. The use case is based on ADS-B message generation within the BALSA example from the FACE Software Supplier Getting Started Guide (Ref. [6]).

Section 5 also identified that, where practical, by limiting the scope of UoCs to that of a single PRA component, using the PRA with the FACE Technical Standard allows the scope of UoCs to be standardised. This should provide benefits to portability and integration, potentially reducing system development time and cost.

6.3 Areas of Incompatibility

This assessment has not identified any areas of incompatibility.

6.4 Notable Considerations for Ensuring Compatibility and Achieving Benefits

In addition to following the development principles and requirements from the PRA and the FACE Technical Standard, a number of key considerations for the development of PYRAMID components and UoCs have been identified to ensure compatibility:

- Splitting PRA components across FACE segments
- Using data driving to achieve greater portability
- Porting PYRAMID components to a platform conforming to the FACE Technical Standard and redeveloping UoCs as PYRAMID compliant components
- Data exchange paradigm differences

6.4.1 Splitting PRA Components into Multiple Variants

It may be necessary to develop some PRA components as separate specialised PYRAMID components, so that they may reside in different FACE segments. These could be either implemented as independent PYRAMID components or as PYRAMID components with a parent and extensions component relationship (as described in the PRA Component Extensions policy).

For example, it is possible that the PRA Sensors, Effectors and Communicator resource layer components will require specialised variants in the PSSS and IOSS.

6.4.2 Using Data Driving to Achieve Greater Portability

The assessment of the PRA components frequently determined that the extent to which a component is potable can be significantly influenced by the extent to which data driving is implemented. This is because equipment or equipment configuration specific details can be data loaded, instead of being hard coded.

It should be recognised that data driving can be applied prior to or after compiling the executable software. Whilst both approaches significantly increase the ease by which software artefacts can be reused, only applying the data after compiling the executable software influences the portability of the UoC executable software without modification.

6.4.3 Porting Components from Platforms not Based on PYRAMID or the FACE® Technical Standard

The primary scope of this report is to determine the compatibility of PYRAMID components specifically developed to be FACE conformant UoCs. However, the following is worth noting:

- In principle, it should be feasible to redevelop PYRAMID components that were not developed for a platform conforming to the FACE Technical Standard for a platform that does conform. The extent to which redevelopment is needed will likely be dominated by:
    - The degree to which the component interfaces align to the FACE Technical Standard SDM and interfaces.
    - Whether or not it is necessary to split the component into separate variants in order to fit within the appropriate FACE segments (as discussed in Section 5.4).
    - The degree to which the original platform functional requirements or use cases for the component align with those of the new platform.
- The feasibility of redeveloping non PRA based UoCs conforming to the FACE Technical Standard into one or more PYRAMID compliant components will vary

significantly in each case. Where this is feasible the extent to which redevelopment is needed will likely be dominated by:

- The software development approach used and therefore the ease by which different elements of the software design can be decoupled.
- The degree to which the UoC happens to neatly align to one or more PYRAMID components.

6.4.4 Data Exchange Paradigm

The paradigms of data exchange differ between the PRA and the FACE Technical Standard:

- The PRA is written with the intention that the components are developed independently and linked through the use of bridges. This removes the need for components to have identical interfaces to be able to interact, thereby preventing pollution of the components and enabling them to be compliant to the PRA. This approach helps to enable benefits such as independent development and reuse.
- The FACE Technical Standard uses a combination of a data architecture, which implements a common understanding of messages through sharing data models, and standardised interfaces.

As discussed in Section 5.5, in the majority of cases the TSS can be used to provide the PRA bridge functions. Nonetheless, there will remain some cases, when interaction with PYRAMID components in the IOSS is required, where the TSS cannot be used. Nonetheless, there remain cases where interaction via the IOS interface is necessary, resulting in PYRAMID component UoCs on either side of the interface sharing the same interface definition. Due to the specific PRA components identified as needing to use this interface, this should not prevent PRA and FACE Technical Standard compatibility; however, it is an area where care should be taken to ensure that the shared interface does not result in PYRAMID component pollution.

There is also the option to incorporate bridge data translation functions within the same UoC as a PYRAMID component. This approach can be used to create a UoC interface ‘façade’ which conforms to the FACE Technical Standard interface and data model requirements when the PYRAMID component interface does not fully conform to these.

This approach may be desirable in order to help enable a PYRAMID component design to be ported from, and potentially to, other computing equipment that does not conform to the FACE Technical Standard.

7 Conclusions

This feasibility study has determined that the PRA and FACE® Technical Standard are compatible and complementary standards for use on military fighter aircraft. The PRA provides the conceptual partitioning for software applications as well as their required behaviour. The FACE Technical Standard provides the context of the software structure, data exchange and open standards that define access to hardware. The different aspects provided by the PRA and FACE Technical Standard typically relate to different layers of the computing stack and largely do not overlap. When combined these different reference architectures provide the basis for a significant portion of what is needed for military aircraft computing software to successfully operate.

Through this initial assessment it has therefore been determined that for any PRA component it should be possible to develop PYRAMID component UoCs that conform to the FACE Technical Standard.

Furthermore, the utilisation of the PRA should significantly increase the portability of UoCs, since, when used with the FACE Technical Standard, the PRA would define the scope of the PCS UoCs and many PSSS UoCs. This would significantly increase the likelihood of different combinations of UoCs being able to work together on the same platform, thereby easing integration, and increasing the scope for 'off the shelf' UoCs or UoCs being ported from one platform to another to be compatible. It would also significantly increase the ability to switch between alternative UoCs, such as from different vendors, that are compliant to the same PRA component. Such UoCs could provide the same general functionality, yet may provide different specialisations or optimisations to their capability.

Whilst not the focus of the assessment, some consideration has been given to the feasibility of redeveloping software previously developed to only be PYRAMID compliant or only conform to the FACE Technical Standard to achieve both. Assuming that the functional requirements for the components/UoCs remain the same, it appears to be the case that:

- Redeveloping PYRAMID components to conform to the FACE Technical Standard should be feasible in the majority of cases.
- The feasibility of redeveloping non PYRAMID compliant UoCs that conform to the FACE Technical Standard to be PYRAMID compliant will depend on a number of factors, such as the software development approach and the degree to which the UoC happens to align to one or more PRA component definitions.

In both cases, the benefits of such redevelopment against the time and cost of doing so should be evaluated on a case by case basis.

The study has also highlighted that two primary factors can influence how portable a PYRAMID based UoC will be:

- The extent of and approach to using data driving.
- In specific cases, the splitting of PRA components into multiple PYRAMID component variants, including the utilisation of a parent and extension component relationships, to allow the more portable elements to be separated from the less portable elements.

Appendix A – Assessment of PRA Component Applicability to FACE® Technical Standard Segments

This appendix provides the outcome of an assessment to determine which FACE® Technical Standard segments are applicable to each PRA component. It is split in to three parts:

- An assessment for each PRA component.
- A more detailed assessment of the applicability of components to the IOSS.
- A more detailed assessment of the applicability of components against the individual TSS capabilities.

A.1 PRA Component Applicability to FACE® Technical Standard Segments

The following table shows the outcome of an initial assessment that determined which FACE Technical Standard segments are applicable to each PRA component. It is not intended as a definitive statement of applicability for every system, it is intended to show the expected typical cases.

Within the table, "x" indicates the preferred allocation and optional allocations are indicated by "o". Where cells are blank it is not considered likely that the associated FACE segment will include the referenced component.

Where PRA components are identified as potentially applicable to the OSS, it is not necessarily expected that they would be used for this purpose; however, in theory they could be used as part of an OSS UoC.

PRA		FACE Segment					Comment
PRA Component	PRA Component Layer	PCS	TSS	PSSS	IOSS	OSS	
Anomaly Detection	Service	x	o	x	o		An instance may exist for each PRA component in a deployment. It is assumed that an instance of Anomaly Detection will be in the same FACE segment as the component that it supports and may be part of the same UoC. Note 1 applies. (See Table 3 for an explanation of IOSS applicability.)
Asset Transitions	Service	x		o			See Note 1.

PRA		FACE Segment					Comment
PRA Component	PRA Component Layer	PCS	TSS	PSSS	IOSS	OSS	
Authorisation	Action	x					See Note 2.
Collision Avoidance	Action	x					See Note 2.
Collision Prediction	Service	x					See Note 2.
Communication Links	Action	x		o			See Note 1.
Communicator	Resource			x	o		See Note 4. (See **Table 3** for an explanation of IOSS applicability.)
Countermeasures	Action	x					See Note 2.
Cryptographic Materials	Service	x		o			In general, this component should be agnostic of how keys are used and therefore is applicable to the PCS. However, there may be rare cases where this is not appropriate, causing the PSSS to be applicable.
Cryptographic Methods	Service	x	x	x	o	o	In general, this component should be agnostic of the exploiting platform. However, it may be necessary for an instance of this component to reside in each of the FACE segments to support the protection of data leaving the segment (allowing the data to be stored or transmitted). Where appropriate this component may be incorporated in the same UoC as another component that it is providing encryption/decryption for. This is assumed to be the case if the component is ever incorporated in the IOSS. (See **Table 3** for an explanation of IOSS applicability.)

PRA		FACE Segment					Comment
PRA Component	PRA Component Layer	PCS	TSS	PSSS	IOSS	OSS	
Cyber Defence	Service	x		o	o		This component will potentially need to work at different levels of abstraction (e.g. at assessing both the computing I/O and performance/output of other components). This may drive the need for different instances of the component to be implemented in different FACE segments (i.e. the IOSS, PSSS and PCS) in order to avoid information not normally relevant to the abstraction of a segment being provided to the segment. In some cases, such as when implemented in the IOSS, this will required the component to be incorporated into the same UoC as another component. In general, however, the component is expected to be most relevant to being applied in the PCS. (See **Table 3** for an explanation of IOSS applicability.)
Data Distribution	Resource		x	x			The Data Distribution capability is characterised in the TSS. However, data translation to external system interfaces can be associated with the PSSS. (See **Table 4** for an explanation of TSS applicability.)
Data Fusion	Service	x		o			In general, data fusion can be independent of an exploiting platform, but in special cases Note 1 applies.
Destructive Effects	Service	x					See Note 2.
Effectors	Resource			x	o		See Note 4. (See **Table 3** for an explanation of IOSS applicability.)
Environment Infrastructure	Service	x					See Note 2.

PRA		FACE Segment					Comment
PRA Component	PRA Component Layer	PCS	TSS	PSSS	IOSS	OSS	
Environment Integration	Action	x					See Note 2.
Environmental Conditioning	Action	x					See Note 2.
Flights	Service	x					See Note 2.
Fluids	Resource	x		o			See Note 1.
Formations	Action	x					See Note 2.
Geography	Service	x					See Note 2.
Health Assessment	Service	o		x			Multiple instances of this component are likely to exist in a deployment. The parts of a system that an instance caters for will influence the applicable FACE segment (PCS or PSSS).
HMI Dialogue	Service	x		o			Since this component interprets what needs to be presented to the user and what the user requires, it does not directly control the HMI graphics or equipment, generally making it applicable to the PCS. However, if complex display management is required, the component may occasionally play a small role in the Graphics Display Management Services, within the PSSS.
Human Interaction	Action	x					See Note 2.
Information Brokerage	Service	x	o				When applied to interaction between different systems this component applies to the PCS since the information needs of different systems are agnostic of the exploiting platform. However, this component could also be used to develop parts of the TSS since it knows about how and where components are distributed and bridges between segments. (See Table 4 for an explanation of TSS applicability.)

PRA		FACE Segment					Comment
PRA Component	PRA Component Layer	PCS	TSS	PSSS	IOSS	OSS	
Information Presentation	Service			x			See Note 3.
Interlocks	Resource	x		o			See Note 1.
Inventory	Service	x					See Note 2.
Jettison	Action	x					See Note 2.
Lights	Action	x					See Note 2.
Location and Orientation	Service	x					See Note 2.
Mass and Balance	Service	x					See Note 2.
Mechanical Positioning	Resource	x		o			See Note 1.
Navigation Sensing	Action	x		o			See Note 1.
Network Routes	Resource		o			x	Since this component is predominantly associated with the OSS network route requirements (e.g. the IP based network stack) it is primarily associated with the OSS. However, its quality of service congestion management capabilities can be used to support the TSS. (See Table 4 for an explanation of TSS applicability.)
Networks	Action					x	Since this component is responsible for setting-up IP network routing it is associated with the OSS.
Objectives	Objective	x					See Note 2.
Observability	Service	x					See Note 2.
Operational Rules and Limits	Service	x					See Note 2.
Path Demands	Action	x					See Note 2.

PRA		FACE Segment					Comment
PRA Component	PRA Component Layer	PCS	TSS	PSSS	IOSS	OSS	
Pointing	Action	x					See Note 2.
Power	Resource	x		o			See Note 1.
Propulsion	Resource	x		o			See Note 1.
Reference Times	Service	x		o			See Note 1.
Release Aiming	Service	x					See Note 2.
Release Effecting	Resource	x		o			See Note 1.
Resource Brokerage	Service	x		o			See Note 1.
Routes	Action	x					See Note 2.
Semantic Translation	Service		o	x			This component is predominately associated with the PSSS since it handles translated interpretations of information between different specific systems. However, it can also be applied to the TSS data transformation capability to achieve translations that go beyond data/unit type conversions. (See **Table 4** for an explanation of TSS applicability.)
Sensing	Action	x					See Note 2.
Sensor Data Interpretation	Action	x					See Note 2.
Sensor Products	Service	x		o			The types of sensor product being handled may influence the applicable FACE segment (PCS or PSSS). In some cases Note 1 will also apply.
Sensors	Resource			x	o		See Note 4. (See **Table 3** for an explanation of IOSS applicability.)
Signature	Service	x					See Note 2.
Spatial Correction	Service	x					See Note 2.

PRA		FACE Segment					Comment
PRA Component	PRA Component Layer	PCS	TSS	PSSS	IOSS	OSS	
Spectrum	Service	x					See Note 2.
Storage	Service	x		o			See Note 1
Stores Release	Action	x					See Note 2.
Susceptibility	Service	x					See Note 2.
Tactical Objects	Service	x					See Note 2.
Target Engagement	Action	x					See Note 2.
Tasks	Task	x					See Note 2.
Test	Action	x					See Note 2.
Threats	Service	x					See Note 2.
Trajectory Prediction	Service	x					See Note 2.
Undercarriage	Action	x					See Note 2.
User Accounts	Service	x					See Note 2.
User Roles	Service	x					See Note 2.
Vehicle External Environment	Service	x					See Note 2.
Vehicle Guidance	Action	x					See Note 2.
Vehicle Performance	Service	x					See Note 2.
Vehicle Stability and Control	Action	x					See Note 2.
Weather	Service	x					See Note 2.

PRA		FACE Segment					Comment
PRA Component	PRA Component Layer	PCS	TSS	PSSS	IOSS	OSS	
Note 1: The component will need to deal with details that are tailored to use with specific equipment or assets (e.g. a sensor). However, the component's interface data definition and message structure should be abstracted away from the equipment or asset interface, allowing it to be incorporated into the PCS. Nonetheless, there may be exceptional cases where greater alignment to the specific equipment or asset interface definition is sought, potentially making the PSSS applicable. Additionally, through the use of data driving with good design, equipment specific details could be defined and configured through data, allowing greater portability of the component. Alternatively, to improve portability, any aspects that are agnostic of the equipment could be incorporated into a component that has an extension catering for the aspects associated with specific equipment. **Note 2:** Through the use of good design principles, potentially using data driving, this component should almost always be applicable to the PCS. **Note 3:** The core elements of this component are specific to particular types of equipment. Whilst there may be opportunities to genericise those supported with data driving, this may be difficult to achieve in practice and so (at this time) are assumed to only be applicable to the PSSS. **Note 4:** Typically, this component is applicable to the PSSS since it covers the functionality of equipment. However the component potentially also allows for interfaces to the equipment to be catered for, making it applicable to the IOSS. This potentially drives the need for separate component instances to be incorporated into both the PSSS and the IOSS or the need for extensions in the IOSS. **Note 5:** Any PRA components identified as being applicable to the OSS or TSS are expected to form only part of a UoC. In the case of the OSS the other parts would be made up of capabilities outside the scope of the PRA, whereas for the TSS the other parts may be made up of capabilities outside the scope of the PRA.							

Table 2 PRA Components Mapped to FACE® Segments

A.2 PRA Component Applicability to the IOSS

The following table provides further explanation of the components that are applicable to the IOSS. Note that the Anomaly Detection, Cryptographic Methods and Cyber Defence components are always expected to be contained within the same UoC as another PRA component (either the Communicator, Sensors or Effectors component) when used within the IOSS.

PRA Component	Explanation of Applicability to the IOSS
Anomaly Detection	It is unlikely that Anomaly Detection would be needed in the IOSS since most device/interface error information would be available through the IOS interface, provided to the PSSS, and if necessary would be available to the PCS. However, there is a small possibility of unique cases where anomaly related information provided by the device driver, through the OS interface, to the IOSS becomes too abstracted when provided, through the IOS interface, to the PSSS. In such cases it may be necessary to incorporate the Anomaly Detection component within the IOSS, in which case it would provide abstracted anomaly information. In order to conform to the FACE Technical Standard requirement that 'an IOSS UoC shall provide at least one I/O Service', as well as being more practical, the Anomaly Detection component would need to be within the same UoC as the component providing the rest of the I/O Service Management Capability and/or the I/O Data Movement Capability for a particular device.
Communicator	Although non PRA based options may be available, the Communicator component could provide the normalised to specific interface conversion for the majority of devices. Note that the component within the IOSS would not perform the higher level device specific control reasoning, since this would be provide by a Communicator component in the PSSS.
Cryptographic Methods	It is unlikely that Cryptographic Methods would be needed in the IOSS since most information protection activities would be carried out on the information available outside the IOSS (either within the PCS, TSS or PSSS, on specific data items or blocks/packets of data, or within the device, through the encoding/decoding of signal waveforms). However, there is a small possibility of unique cases where encoding/decoding or applying additional protective data is required within an IOSS UoC, in order to fully normalise a specific device driver interface. In such cases it may be necessary to incorporate the Cryptographic Methods component within the IOSS. In order to conform to the FACE Technical Standard requirement that 'an IOSS UoC shall provide at least one I/O Service', as well as being more practical, the Cryptographic Methods component would need to be within the same UoC as the component providing the rest of the I/O Data Movement Capability for a particular device.

PRA Component	Explanation of Applicability to the IOSS
	Unless the entirety of a message on the IOS interface, or message on the interface with the device driver, requires encoding/decoding (rather than just its constituent parts being encoded/decoded) the Cryptographic Methods component will only act as a service to the other PYRAMID component within the UoC (e.g. Communicator), and so will not directly interact with the interface. If an occasion ever arises where the entirety of a message requires encoding/decoding then, since the Cryptographic Methods is agnostic of the meaning of any data that it is acting on, this would not cause pollution, regardless of what the data contains.
Cyber Defence	It is unlikely that Cyber Defence would be needed in the IOSS. However, there is a small possibility of unique cases where it would be required. In order to conform to the FACE Technical Standard requirement that 'an IOSS UoC shall provide at least one I/O Service', the Cyber Defence component would need to be within the same UoC as the component providing the I/O service.
Effectors	Although non PRA based options may be available, the Effectors component could provide the normalised to specific interface conversion for effector devices with unique interfaces that are not supported by the Communicator component, such as discrete interfaces. Note that the component within the IOSS would not perform the higher level device specific control reasoning, since this would be provide by an Effectors component in the PSSS.
Sensors	Although non PRA based options may be available, the Sensors component could provide the normalised to specific interface conversion for effector devices with unique interfaces that are not supported by the Communicator component, such as discrete interfaces. Note that the component within the IOSS would not perform the higher level device specific control reasoning, since this would be provide by a Sensors component in the PSSS.

Table 3 PRA Component Applicability to the IOSS

A.3 PRA Component Applicability to TSS Capabilities

The following table provides further detail about where TSS capabilities could be provided by PRA components.

FACE Technical Standard TSS Capability		Related PRA Components
Capability Name	**Summarised Description (Generally taken from FACE Technical Standard (Ref. 5]))**	
Transport Service Capability (Mandated by FACE)	Provides a type-specific interface, and is responsible for providing the functionality of the type-specific interface to UoCs.	Could be developed using the PRA Data Distribution component, to implement the typed interface, under the control of the PRA Information Brokerage component.
Distribution Capability (Mandated by FACE)	Controls or manages the distribution of data within a TSS and provides support functionality for data marshalling and transformations which may be used by other TSS capabilities within a TSS UoC.	Could be developed using the PRA Data Distribution component.
Configuration Capability (Mandated by FACE)	Manages configuration of TSS UoCs.	Could be developed using the PRA Data Distribution component.
Type Abstraction Capability (Optional within FACE)	Provides an Intra-segment Interface for use by the TSS UoC, where support is required for programming languages (such as C) that do not support function overloading.	Could be developed using the PRA Data Distribution component.
QoS Management Capability (Optional within FACE	Sets specific Quality of Service demands for specific information exchanges.	Could be developed using the PRA Information Brokerage component.
Message Association Capability (Optional within FACE)	Allows a TSS UoC to maintain an association between two data elements, e.g. association of security tags to data structures.	Could be developed using the PRA Information Brokerage component, to maintain the association link, and the PRA Data Distribution component to maintain the format of any associated data.

FACE Technical Standard TSS Capability		Related PRA Components
Capability Name	**Summarised Description (Generally taken from FACE Technical Standard (Ref. 5]))**	
Data Transformation Capability (Optional within FACE)	Performs transformations of data to deliver instances of message parameters defined by the consuming software component in accordance with their UoP Supplied Model's (USM) Platform View. This includes transformations for security purposes.	Could be developed using the PRA Data Distribution component to cater for messaging patterns and the protocol paradigm. Data model translations could be implemented using the PRA Semantic Translation component.
Messaging Pattern Capability (Optional within FACE)	Manages the message pattern, message communication types, transformation from one message pattern to another message and other message processing requirements.	Could be developed using the PRA Data Distribution component. Complex cases, such as where message pattern translation requires an understanding of the states of the provider/consumer, will also require the PRA Semantic Translation component.
Transport Protocol Module Capabilities (Optional within FACE)	Allows the selection between multiple protocols depending on the connectivity requirements, such as Transmission Control Protocol (TCP) and, UDP, RTPS, IIOP, Queues, Inter-Process Communication, inter-partition communication, or others as needed. Additionally, many physical transports can be supported such as Internet Protocol or Shared Memory.	Could be developed using the PRA Data Distribution component.

FACE Technical Standard TSS Capability		Related PRA Components
Capability Name	**Summarised Description (Generally taken from FACE Technical Standard (Ref. 5]))**	
Data Store Support Capability (Optional within FACE)	Access to Data Stores is usually provided by the Operating System (OS) segment. However, to maintain portability of PCS and PSSS UoCs across a wide variety of Data Store access, a common point of presence for Data Store access is required. Data Store Access Capability provides this functionality within the TSS.	None. (This is beyond the scope of the PRA.)
Component State Persistence Capability (Optional within FACE)	The Component State Persistence (CSP) Interface provides a standardised interface for PCS, PSSS, and TSS UoCs to checkpoint (back up) their internal state, or store private data.	None. (This is beyond the scope of the PRA.)
Framework Support Capability (Optional within FACE)	An abstraction that translates Component Framework interfaces to FACE Technical Standard defined interfaces.	None. (This is beyond the scope of the PRA.)
TSS Supporting Functions (Optional within FACE)	Provides serialization, primitive marshalling or buffer helper functions that can be tailored to the specific design of a data network.	The serialization elements could be developed using the PRA Data Distribution component.

Table 4 FACE® TSS Capabilities and Relevant PRA Components

Appendix B – Example of Using the PRA with FACE

B.1 BALSA Specific Use Case for ADS-B Data Transfer

Figure 9 shows example UoCs deployed in the FACE® Technical Standard architecture to implement a simple ADS-B message derived from aircraft sensors. It is a duplicate of Figure 2 in the FACE Software Supplier Getting Started Guide (Ref. [7]).

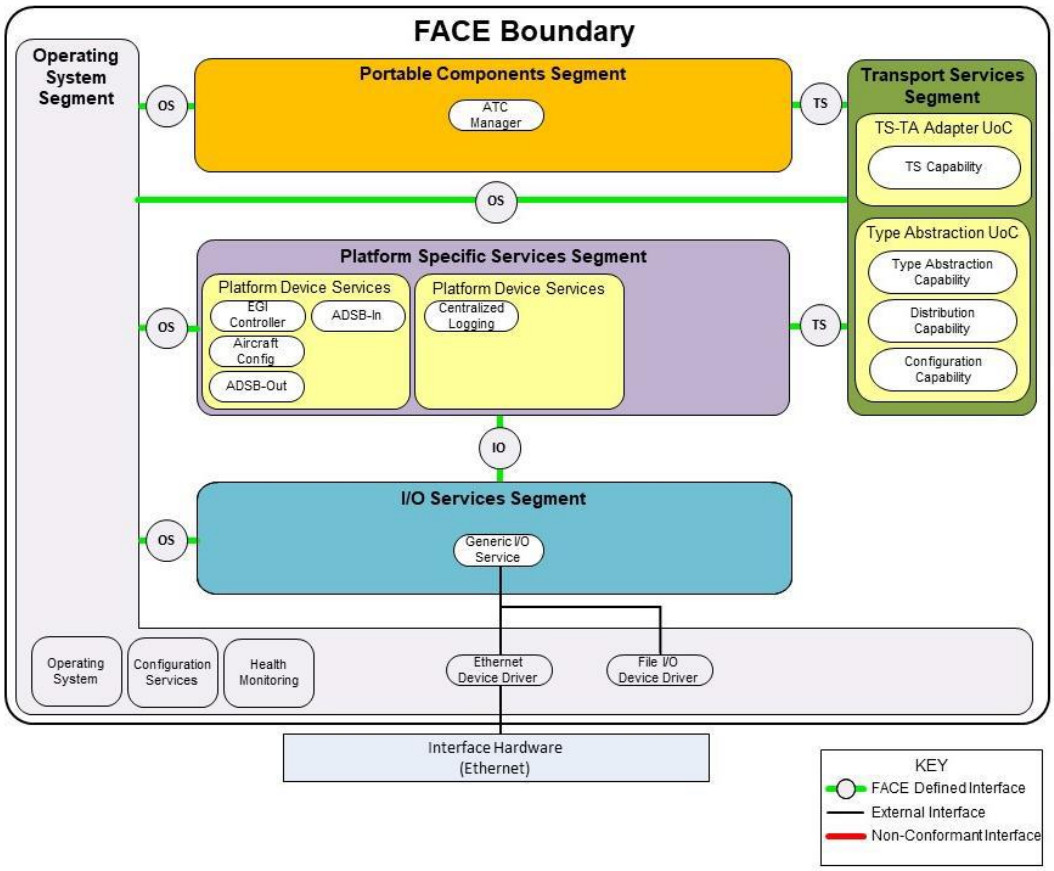

Figure 9 Data Flow in BALSA ADS-B Data Transfer Use Case (figure 1 from FACE® Software Supplier Getting Started Guide (Ref. [7]), © 2022 The Open Group)

The associated data connection summary, based on the summary provided in Section 2.3.1.5 of Ref. [8], is as follows:

- The EGI (Embedded GPS/INS) Controller component sends altitude, Latitude and Longitude data via the EGI DATA TSS connection
- The Aircraft Configuration (Aircraft Config) component sends Aircraft Tail Number to the AIRCFG DATA TSS connection
- The ATC Manager receives from the EGI DATA TSS connection
- The ATC Manager receives from the AIRCFG DATA TSS connection
- The ATC Manager sends combined data to the ATC DATA TSS connection
- The ADS-B Out receives from the ATC DATA TSS connection

- The ADS-B Out sends ADS-B formatted messages via the IOS
- The IOS writes a multicast message to the “radio”
- The ADS-B In displays the ADS-B messages for all aircraft within radio proximity.

B.2 PYRAMID Components for BALSA ADS-B Data Transfer Use Case

The PRA component mapping for UoCs in the PCS, PSSS and IOSS is shown in Table 5 below.

Original BALSA Example		**PRA Component Applicability**	
FACE Segment	**UoC**	**Applicable PRA Components**	**Rationale**
PCS	ATC Manager	Environment Integration	The Environment Integration component determines if and when ADS-B data should be transmitted by the platform. It also provides the aircraft tail ID, which will be included in the transmitted ADS-B data.
		Location and Orientation	The EGI data is provided to the Location and Orientation component which maintains the understanding of the platform position. This is subsequently supplied, by the component, for inclusion in the transmitted ADS-B data.
PSSS	ADS-B Out	Communicator	The transmitted ADS-B data is controlled by the Communicator component, but is restructured and reformatted by the Data Distribution component.
		Data Distribution	
	ADS-B IN	Communicator	The received ADS-B data reception is controlled using the Communicator component, but is restructured and reformatted by the Data Distribution component.
		Data Distribution	
	EGI Controller	Communicator	The EGI data is obtained using the Communicator component, but is restructured and reformatted by the Data Distribution component.
		Data Distribution	
	Aircraft Config	Sensors / Not applicable	If the aircraft tail ID is hardwired the Sensors component would be used to detect and report the hardwired ID. Alternatively, the aircraft tail ID could be loaded as data, in which case no PRA component is needed. Note that in both cases the aircraft tail ID is supplied to and held by the Environment Integration component.
	Centralized Logging	Not applicable	Every PRA component is responsible for requesting the appropriate logging and deletion of information within its subject matter. However, the function of actually logging the information is outside the scope of the PRA; therefore, a non PRA based UoC would be developed for the Centralized Logging.

Original BALSA Example		PRA Component Applicability	
FACE Segment	**UoC**	**Applicable PRA Components**	**Rationale**
IOSS	Generic I/O Service	Communicator	The Communicator component provides the normalised to specific interface conversion. Note that where different communication technologies are involved this may be implemented as multiple versions of a PYRAMID Communicator component, which may be component extensions.
TSS	Transport Service Capability	Data Distribution	As described in Table 4, the TSS capabilities could be provided by the Data Distribution and Information Brokerage components.
		Information Brokerage	
	Type Abstraction Capability	Data Distribution	
	Distribution Capability	Data Distribution	
	Configuration Capability	Data Distribution	

Table 5 BALSA Instances of PYRAMID Components