GD200152700
Issue 4
26th October 2017

GENERAL DYNAMICS
United Kingdom Limited

Contract Number: BATCM/0263

Battlefield Management Application (BMA)

Technical Specification Competition Requirements

Author:	Approver:	Authoriser:
Tim McLeod	Marc Jones	Andy Oliver
	Marc Jones	pp Marc Jones
Applications Architect	Chief Architect	Chief Engineer
26/10/2017	26/10/2017	26/10/2017

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

GENERAL DYNAMICS
United Kingdom Limited

Revision History

Issue/Draft	Date	Comments/Reason for Change
1	19/07/2017	First formal release of this document
2	04/08/2017	Updated to incorporate MOD comments on Issue 1
3	27/09/2017	Updated to articulate TP dependencies on the BMA supplier.
4	23/10/2017	Updated to incorporate MOD comments on Issue 3

Export Marking

Confirmation is required against each marking

Export Marking	Confirmation
ITAR Data	No
EAR Data	No
Military data	No
Dual Use data	No
Export Controlled	No

ITAR Information

Subcontractor	TAA Number
Not applicable	Not applicable

External Distribution

Recipient	Company
None	

Acronyms & Abbreviations

Acronym/Abbreviation	Definition
2D	Two dimensional
3G	Third generation of mobile telephony
4G	Fourth generation of mobile telephony
AA	Principal Engineer or equivalent.
AAI	Alerts Application Interface
ADS	Adaptive Delivery Service
AOS	Application Orchestration Service
AOSI	Application Orchestration Service Interface
API	Application Programming Interface

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

Acronym/Abbreviation	Definition
ARS	Architectural Requirements Specification
ATI	ATI Technologies
BARI	Business Automation Rules Interface
BMA	Battlefield Management Application
C2	Command and Control
CATCR	Capability Acceptance Test Case Review
CCA	Circuit Card Assembly
CD-ROM	Compact Disc Read-Only-Memory
CofC	Certificate of Conformance
CoI	Community of Interest
ConX	Concept of Employment/Operation
COTS	Commercial off the Shelf
CSCI	Computer Software Configuration Item
CT1	Computer Type 1 Mk3
CT2	Computer Type 2 Mk3
DaaP	Defence as a Platform
DDR	Double Data Rate
DEFSTAN	Defence Standard
DLL	Dynamic Link Library
DSI	Directory Services Interface
DVD	Digital Versatile Disc
DVI	Digital Visual Interface
ECC	Error Correcting Code
EDR	Enhanced Data Rate
ESCoT	EvO System Coherence Team
EUD	End User Device
EvO	Evolve to Open
EvO AAcR	EvO Architecture Acceptance Review
EvO SATR	EvO System Acceptance Test Review
FMAI	Formatted Message Automation Interface

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

Acronym/Abbreviation	Definition
FMS	Formatted Message Service
FSI	Formal System Integration
FTFTRR	First of Type Field Test Readiness Review
G3	The Army Staff Branch responsible for Operations
G5	The Army Staff Branch responsible for Planning
G6	The Army Staff Branch responsible for Communications and Information Technology
GB	Gigabyte
GDDR	Graphics Double Data Rate
GDUK	General Dynamics United Kingdom Limited
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GHz	Gigahertz
GIS	Geographic Information Service
GISI	Geographical Information Service Interface
GPU	Graphics Processing Unit
GVA	Generic Vehicle Architecture
HDMI	High-Definition Multimedia Interface
HEPAR	Human Engineering Product Analysis Report
HFI	Human Factors Integration
HQ	Headquarters
HQUDT	HQ User Data Terminal
HTTP	Hypertext Transfer Protocol
ICD	Interface Control Document
IdAM	Identity and Access Management
IDD	Interface Definition Document
IER	Information Exchange Requirement
ILS	Integrated Logistics Support
JSON	Javascript Object Notation
IMAP	Internet Message Access Protocol

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

Acronym/Abbreviation	Definition
IMS	Information Management Service
IMSI	Information Management Service Interface
IPR	Intellectual Property Rights
ISS	Information Systems & Services
ITEAP	Integrated Test, Evaluation and Acceptance Plan
ITHC	Information Technology Health Check
JPO	Joint Programme Office
JSP	Joint Service Publication
KVM	Keyboard Video and Mouse
LBATRR	Lab-based Acceptance Test Readiness Review
LDAP	Lightweight Directory Access Protocol
LRU	Line-Replaceable Unit
LSI	Logging Service Interface
LTE	Long-Term Evolution
MAAcR	MORPHEUS Architecture Acceptance Review
MACA	Months After Contract Award
MCUDT	Man Carried User Data Terminal
MilCAN	Military Controller Area Network
Mk	Mark
MMSI	Multimedia Management Service Interface
MOD	Ministry of Defence
MODAF	MOD Architecture Framework
MOP	Measure of Performance
MSI	Microsoft Installer
MTRC	MORPHEUS test and Reference Centre
MTSA	MORPHEUS Target System Architecture
NCSC	National Cyber Security Centre
NFI	Network Feedback Interface
ORBAT	Order of Battle
OSPF	Open Shortest Path First

© 2017 Crown Copyright

Acronym/Abbreviation	Definition
P-BISA	Platform Battlefield Information Systems Application
PBPU	P-BISA Processor Unit Mk3
PDF	Portable Document Format
PMA	Programme/Project Manager or equivalent
PMP	Project Management Plan
POP3	Post Office Protocol 3
RFC	Request for Comment
RS	Recommend Standard
RTP	Real-time Transport Protocol
RTSP	Real-Time Streaming Protocol
SATA	Serial Advanced Technology Attachment
SBB	Solution Building Block
SDD	Software Design Document
SDK	Software Development Kit
SDP	Session Description Protocol
SEMP	System Engineering Management Plan
SI	System Integration
SI&T	System Integration & Test
SIP	Session Initiation Protocol
SMP	Security Management Plan
SMTP	Simple Mail Transfer Protocol
SPA	Single Page Application
SPR	System Problem Report
SSD	Solid State Drive
SSHD	Solid State Hybrid Drive
SSI	Symbology Service Interface
SyOps	Security Operating Procedures
SysML	Systems Modelling Language
TaskOrg	Task Organisation
TBC	To be confirmed

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

Acronym/Abbreviation	Definition
TCP	Transmission Control Protocol
TDS	Tactical Directory Services
TES	Tactical Email Service
TESI	Tactical Email Service Interface
TI	Tactical Internet
TIF	Tactical Integration Framework
TISI	Tactical Internet Service Interface
TLS	Transport Layer Security
TNA	Training Needs Analysis
TP	Transition Partner
TRS	Tactical Routing Service
UCA	Unified Communications Application
URD	User Requirement Document
USB	Universal Serial Bus
UWP	Universal Windows Platform
UX	User Experience
VCN	Virtual Core Network
VDD	Version Description Document
VGA	Video Graphics Array
VM	Virtual Machine
VPU	Vehicle Processing Unit
XGA	Extended Graphics Array
WAFFS	Web Application Framework Frontend Service
WAFFI	Web Application Framework Frontend Interface
WXGA	Wide Extended Graphics Array

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

Table of Contents

1.0 Introduction 10
1.1 Document Overview 10
1.2 Purpose 10
1.3 Scope 10
1.4 Document Structure 10

2.0 Capability Description Summary 12
2.1 General Capability Description 12
2.1.1 Staff C2 Application 12
2.1.2 Platform C2 Application 12
2.1.3 TaskOrg Editor 12
2.2 Geographic Information Service 12
2.3 Symbology Service 13

3.0 Interface Requirements 14
3.1 General 14
3.2 Internal 15
3.2.1 Geographical Information Service 15
3.2.2 Symbology Service 15
3.2.3 TaskOrg Editor 16
3.2.4 Single Page Application 16
3.2.5 Business Logic Plugins 16
3.3 External 17
3.3.1 Adaptive Delivery Service 17
3.3.2 Alerts Service 18
3.3.3 Formatted Message Service 18
3.3.4 Information Management Service 18
3.3.5 Logging Service 18
3.3.6 Multimedia Management Service 19
3.3.7 Tactical Directory Service 19
3.3.8 Tactical Email Service 20
3.3.9 Tactical Routing Service 20
3.3.10 Application Orchestration Service 20
3.3.11 Web Application Framework Frontend Service 21

4.0 Computer Resource Requirements 22
4.1 Hardware Computing Platforms 22
4.1.1 Computer Type 1 Mk3 22
4.1.2 Computer Type 2 Mk3 22
4.1.3 P-BISA Processor Unit Mk3 23
4.1.4 Vehicle Processor Unit 23
4.1.5 Man Carried User Data Terminal 23
4.1.6 HQ User Data Terminal 24
4.1.7 HQ Server 24
4.2 Software Computing Platforms 25

© 2017 Crown Copyright

4.2.1 Windows 10 Enterprise 25
4.2.2 Windows Server 2016 26
4.2.3 Application Delivery 26

5.0 Design and Implementation Constraints 27
5.1 Architectural Considerations 27
5.1.1 Tactical Element of Single Information Environment 27
5.1.2 Improved Information Superiority 27
5.1.3 Rapid Exploitation of Emergent Technology 27
5.1.4 Increased Agility/Flexibility 27
5.1.5 Reduced Delivery Times 28
5.1.6 Reduced Costs 28
5.1.7 Vendor Independence 28
5.2 Collaborative Approach to Delivery 28
5.3 Other System Level Constraints 28
5.3.1 Human Factors 28
5.3.2 Integrated Logistics Support 29
5.4 Government Furnished Information 29
5.4.1 BMA Tech Proposals, Compliance Statements and other GFI 29
5.4.2 BMA Openness Test Results 29
5.4.3 BMA Software Documentation 30
5.4.4 BMA Qualification Documentation 30

6.0 Security 31

7.0 Safety 32

8.0 Dependencies on the BMA Supplier 33

List of Tables

Table 1 – Architecture and Design Dependencies 33
Table 2 – Commercial Dependencies 34
Table 3 – BMA Definition Dependencies 36
Table 4 – Programme Dependencies 36
Table 5 – System Integration Dependencies 37
Table 6 – Product Alignment Dependencies 42
Table 7 – Customer Dependencies 42

Table of Figures

Figure 1 – BMA Architectural Context 14

© 2017 Crown Copyright

1.0 Introduction

1.1 Document Overview

The Battlefield Management Application (BMA) is Government Furnished Equipment (GFE) that will be procured by MOD as one or more third party products and integrated with the MORPHEUS Evolve to Open (EvO) system by General Dynamics United Kingdom Limited (GDUK). The BMA Technical Specification Competition Requirements document (this document) describes the system environment in which the BMA software is required to operate; it is not a specification for the function(s) of the BMA. The document will support the procurement of a BMA Commercial off the Shelf (COTS) or bespoke development or any combination of these, by identifying the EvO operating environment constraints and listing the EvO services that may be of use to the BMA and the services that the BMA shall provide.

1.2 Purpose

The purpose of this document is to support MOD procurement activity by presenting the initial requirements needed by MOD for the BMA competition.

1.3 Scope

Within the scope of this document the BMA includes the Staff C2 Application, the Platform C2 Application, the Geographic Information Service (GIS), Symbology Service and a TaskOrg Editor. Whilst the Close Combat C2 Application is outside of the scope of the EvO BMA integration, providing the same interfaces are provided and/or consumed on the appropriate dismounted computing platform, integration with the Tactical Integration Framework would follow similar lines to the Staff or Platform C2 Application. Note that Tactical Chat, which was originally considered as part of the BMA, has been excluded as this has been subsumed within the Unified Communications Application (UCA); the C2 Applications shall use the Tactical Chat capability.

1.4 Document Structure

This document is structured as follows:

- **Capability Description Summary**. Section 2.0 summarises the technical capabilities that shall be provided by the BMA. Section 2.1 describes the high level functions required of the C2 applications. Section 2.2 describes the high level function of the GIS. Section 2.3 describes the high level function of the Symbology Service.
- **Interface Requirements**. Section 3.0 lists required interfaces and includes interface requirements by Computer Software Configuration Item (CSCI). Section 3.1 provides the architectural context for the BMA; Section 3.2 lists the internal interfaces identified between Solution Building Blocks (SBBs) included within the BMA scope; *the interfaces provided by the BMA*. Section 3.3 lists the external interfaces identified between the BMA and other EvO SBBs; the *interfaces consumed by the BMA*.
- **Computer Resource Requirements**. Section 4.0 lists the hardware (Section 4.1) and software (Section 4.2) hosting platforms for the BMA. *It does not include hardware resource utilisation since it is not yet known what other applications and services will be hosted on platforms; any resource contention issues can only be determined by system performance modelling and/or during integration.*

© 2017 Crown Copyright

- **Design and Implementation Constraints**. Section 5.0 identifies design and implementation constraints that need to be considered for the BMA. Section 5.1 discusses architectural considerations. Section 5.2 considers other system level constraints, specifically Human Factors (Section 5.3.1) and Integrated Logistics Support (ILS) (Section 5.3.2). Section 5.4 lists the Government Furnished Information (GFI) that shall be provided as part of the BMA delivery.
- **Security**. Section 6.0 identifies security inputs required to support overall EvO system security design and security accreditation.
- **Safety**. Section 7.0 identifies safety inputs required to support overall EvO system safety case.
- **Dependencies on the BMA Supplier**. Section 8.0 lists the Transition Partner (TP) dependencies on the BMA supplier.

© 2017 Crown Copyright

2.0 Capability Description Summary

The BMA GFE shall deliver several EvO SBBs as follows:

- C2 applications for HQ, platform and dismounted users; this will include a TaskOrg editor (Section 2.1).
- A GIS for use by the C2 applications and other third party applications (Section 2.2).
- A Symbology Service for use by the C2 applications and other third party applications (Section 2.3).

2.1 General Capability Description

C2 applications provide commanders with a set of tools that facilitate effective planning and decision making on the battlefield. C2 applications delivered under EvO are as follows:

- Staff C2 Application (Section 2.1.1).
- Platform C2 Application (Section 2.1.2).

The MORPHEUS Dismounted C2 Application is not delivered under the EvO contract but the possibility that it is provided to MOD under the BMA contract is acknowledged.

A C2 TaskOrg Editor is expected to be delivered with the BMA (Section 2.1.3).

It is important to understand that, whilst the C2 functions are provided by two SBBs, Staff and Platform C2 Applications, the BMA software need not be delivered as two *software* applications; it could be provided as a single software application or by more than two.

2.1.1 Staff C2 Application

The Staff C2 is an application specifically required by a Staff Officer working at a HQ level. The Staff C2 application provides a tool which supports functions such as mission planning; preparation and execution; organisation management; situation awareness and target management; decision support and operational picture record and replay.

2.1.2 Platform C2 Application

The Platform C2 is an application specifically required by an operational user, likely to be a vehicle commander, which is mounted within a platform and used both on the move and at the halt. The Platform C2 application provides a tool which supports functions such as situation awareness; order management; task management; planning (suitable for company level and below); route planning and navigation; and reports, returns and requests (R3s). The Platform C2 application integrates with the platform in which it is mounted, via the information infrastructure subsystem, so that it can use the services offered by the platform, such as targeting and navigation.

2.1.3 TaskOrg Editor

TaskOrg Editor enables a user to create and maintain Establishments, ORBATs and TaskOrgs. The TaskOrg Editor supports collaborative working with other instances of itself or with other applications.

2.2 Geographic Information Service

The GIS provides a graphical multi-layered map for display, with associated user interface controls and underlying database. The GIS will be a common service simultaneously consumed by applications other than just the BMA, eg Manage and other third party software; GIS artefacts can be shared amongst GIS clients. Typically base map layers made up of geo-referenced raster and/or vector

© 2017 Crown Copyright

reference data are prepopulated within the database. The GIS provides the ability to overlay geo-referenced military and general mapping symbology onto the mapping layers using graphics and generates symbols for use on map overlays and organisation structures.

The GIS performs terrain analysis, provides a store of mapping data, and supports industry standard interfaces to allow clients to request this information in a recognised format.

2.3 Symbology Service

The Symbology Service is responsible for serving clients with symbology for use on map overlays and to identify organisations, vehicles and communications platforms during mission and system planning (eg as nodes on an ORBAT/TaskOrg tree view). The service will be a common service consumed by applications other than just the BMA, eg Manage and other third party software; symbology libraries will be provided as plugins to the service to support changing needs and/or international collaboration.

Client applications supply the interface provider with information regarding the type, orientation, size and colour of the symbol, together with any additional parameters (unit name, size etc), and the provider returns a fully rendered symbol. Symbol *type* and *size* refer to generic descriptions of function/makeup and size/command level, eg Armoured Squadron, which will allow substitution of different symbol sets.

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

3.0 Interface Requirements

3.1 General

The BMA provides an integrated solution to the users' need to view and maintain an operating picture, conduct various navigation related tasks, and to plan and execute tactical missions. These functions are executed at all echelons and by commanders at all tactical levels. The solution provides both user facing functions and some common services for use by third party applications.

The BMA shall provide several common services as part of the Tactical Integration Framework (TIF) (Section 3.2); the BMA shall consume appropriate services from the TIF (Section 3.2.4).

If the BMA requires management as a system, the supplier shall provide the necessary add-ins that allows management using the EvO Manage application (Section 3.2).

Figure 1 illustrates the architectural context for the BMA, the SBBs with a bold outline being delivered by the BMA GFE.

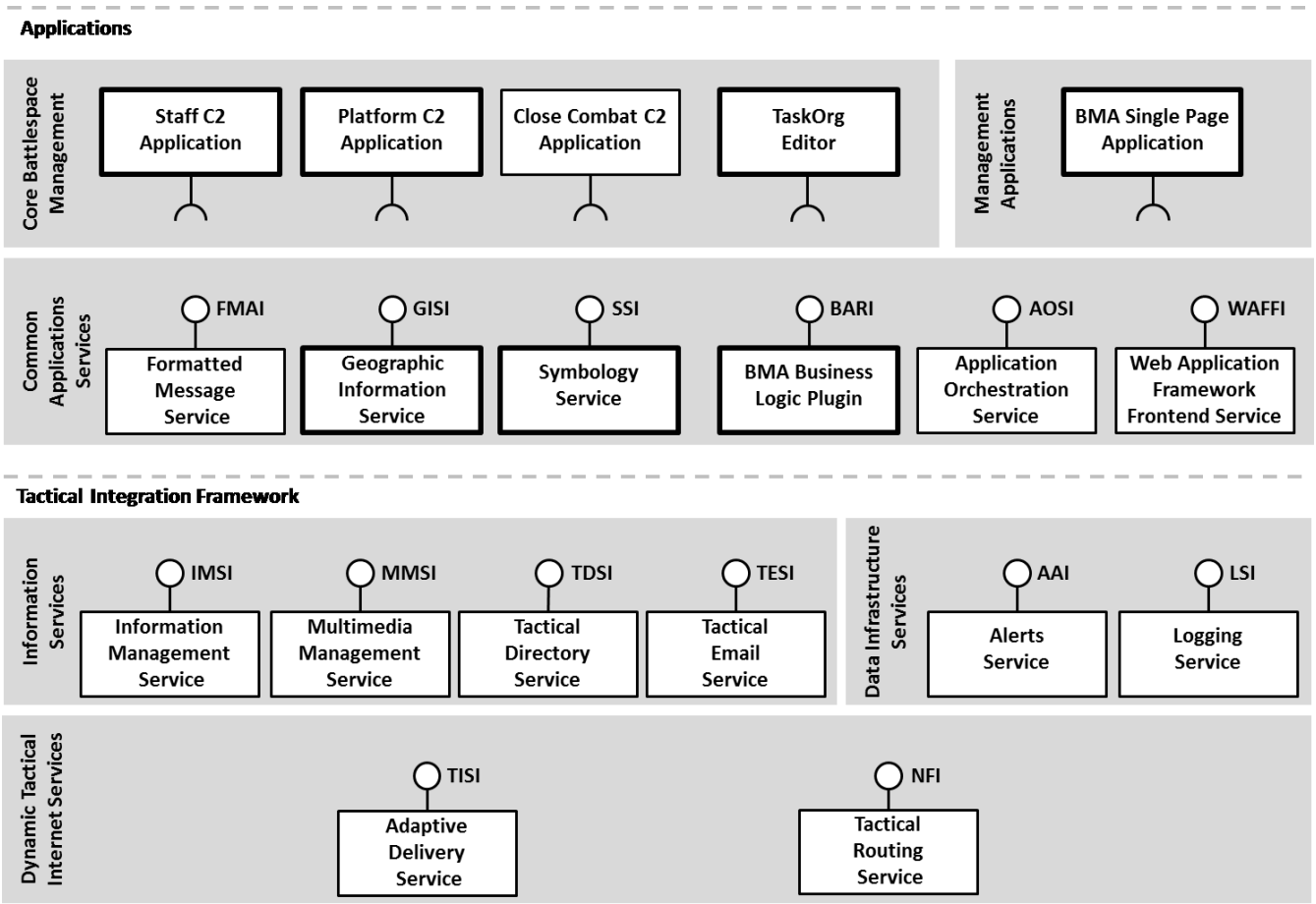

Figure 1 – BMA Architectural Context

Interface Definition Documents (IDDs) for application and service interfaces will be delivered to MOD along with two further updates to the BMA Technical Specification according the schedule outlined in the EvO contract:

© 2017 Crown Copyright

- BMA Technical Specification Assurance Release.
- BMA Technical Specification Acceptance Release.

3.2 Internal

The BMA shall provide the following services for the TIF:

- Geographical Information Service (Section 3.2.1).
- Symbology Service (Section 3.2.2).

The C2 TaskOrg Editor, using the common TIF data store, shall be provided by the BMA (Section 3.2.3).

If the BMA requires system management, it shall provide the following for the Manage application:

- Single Page Application (Section 3.2.4).
- Business Logic Plugins (Section 3.2.5).

3.2.1 Geographical Information Service

The GIS shall provide a graphical multi-layered map with associated user interface controls. The GIS could provide its own underlying database, integrate fully with the Information Management Service (IMS) (Section 3.3.4), or a combination of both. Typically base map layers made up of georeferenced raster and/or vector reference data are prepopulated within the database. The service shall also provide the ability to overlay geo-referenced military and general mapping symbology onto the mapping layers, using raster and/or vector graphics. The GIS shall expose the Geographical Information Service Interface (GISI).

The GISI shall provide the server side of an interface between the GIS and applications that need to display mapping data. The GISI shall serve up map data on request and provide a number of processing functions that cover map display, map overlays, meteorological data, terrain elevation data and spatial analysis.

The technology to be used to implement the GISI has not yet been identified. It is expected that the interface shall be provided as Microsoft .NET Core libraries.

The GISI will be defined in the MORPHEUS Geographical Information Service Interface IDD, document number GD200155034.

3.2.2 Symbology Service

The Symbology Service shall generate symbols for use on map overlays and organisation structures. Clients would supply the Symbology Service with information regarding the icon type, applicable modifier icons, version, orientation, size and colour of the symbol, together with any additional parameters (eg unit name, status affiliation and size), and in return the Symbology Service shall provide a fully rendered symbol to the client. The Symbology Service shall also support translation between different symbols sets. The service exposes the Symbology Service Interface (SSI).

The SSI shall provide clients with symbology for use on map overlays and to identify organisations (eg HQs, units, vehicles) during mission and system planning.

The technology to be used to implement the SSI has not yet been identified. It is likely that the interface shall be provided as Microsoft .NET Core libraries.

© 2017 Crown Copyright

The SSI will be defined in the MORPHEUS Symbology Service Interface IDD, document number GD200155035.

3.2.3 TaskOrg Editor

The C2 TaskOrg Editor shall enable a non-G6 staff officer (eg G3/G5) user to create and maintain Establishments, ORBATs and TaskOrgs for the purposes of mission planning and execution. This is distinct to the TaskOrgs required by the G6 user which will require additional granularity to support system management. The Editor shall be capable of automatically building an ORBAT from establishment data such as the Army's 8005 Establishment Tables, and making ORBAT and TaskOrg data available for third-party applications such as Manage. The Editor shall use the Information Management Service (IMS) (Section 3.3.4) for data storage and distribution.

The technology to be used to implement the C2 TaskOrg Editor has not yet been identified. It is expected that the Editor will be provided as a UWP App.

The C2 TaskOrg Editor Interface will be defined in the MORPHEUS Symbology Service Interface IDD, document number GD200155035.

3.2.4 Single Page Application

A Single Page Application (SPA) is a set of configuration files provided by a supplier that specify which common visual components are to be used and their layout. Visual components are bound to data sources and any business rules and processing logic are contained in the business logic plugins. The configuration files are also used by a common application orchestration services to manage interaction between presentation and business layer and business layer and data layer. The SPA is displayed to the user using a Web Browser application.

An SPA uses the Web Application Framework Frontend Interface (WAFFI) IDD (Section 10.4.2) to utilise the graphical components of the Web Application Framework Frontend Service (WAFFS) graphical components and bind application data to the components. An SPA uses the Application Orchestration Service Interface (AOSI) (Section 10.5.1) to access to business rules and processes and both system and application data.

3.2.5 Business Logic Plugins

Business Logic Plugins are software binaries, eg Dynamic Link Libraries (DLLs), which define and execute the business rules and processes necessary to support an SPA (Section 10.6). Business Logic Plugins can be written to support application presentation and business logic, including:

- Allowing IMS data to be sorted, filtered and structured appropriately to be displayed by the Single Page Application's WGCs and to be written back to the IMS.
- Auto-populating data fields based on other available data such as constructing a user's email address using their first and last names.
- Verifying user-entered data such as ensuring data is within certain ranges or constraints.
- Guiding the user through the SPA (Section 3.2.4) workflow, indicating dependencies on data, other users, and other applications, and invoking other applications as necessary.

Business Logic plugins implement the Business Automation Rules Interface (BARI).

The BARI allows the Application Orchestration Service (AOS) to apply the business rules and execute the business processes provided by a Business Logic Plugin for a SPA (Section 3.2.4).

The BARI is implemented as standard Microsoft .NET libraries.

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

The BARI will be defined in the Business Automation Rules Interface IDD, document number GD200165002.

3.3 External

The BMA shall consume the following services provided by the TIF:

- Adaptive Delivery Service (Section 3.3.1).
- Alerts Service (Section 3.3.2).
- Formatted Message Service (Section 3.3.3).
- Information Management Service (Section 3.3.4).
- Logging Service (Section 3.3.5).
- Multimedia Management Service (Section 3.3.6).
- Tactical Directory Service (Section 3.3.7).
- Tactical Email Service (Section 3.3.8).
- Tactical Routing Service (Section 3.3.9).

If the BMA requires system management, it shall consume the following for integration with the Manage application:

- Application Orchestration Service (Section 3.3.10).
- Web Application Framework Frontend Service (Section 3.3.11).

System management in this context refers to the tools and procedures delivered as part of the BMA that supports centralised setup and management of the software necessary for elements and instances of the BMA to function as a system. An example of BMA System Management might be the setting up of identifiers and IP addresses for Communities of Interest (COIs).

3.3.1 Adaptive Delivery Service

The Adaptive Delivery Service (ADS) provides a single entry point to the Tactical Internet (TI) for data exchange between communicating entities within EvO. The ADS utilises transport protocols optimised for the Tactical Environment to support its reliability requirements. The ADS has responsibilities within three layers of the Internet Protocol Suite: the Application layer, the Transport layer and the Internet layer. Only the Link layer is outside the remit of the ADS. The ADS exposes the Tactical Internet Service Interface (TISI).

The TISI provides a common approach to accessing the Tactical Internet (TI) for the functionality provided by the Adaptive Delivery Service. The TISI is used in conjunction with the Network Feedback Interface (NFI) (Section 3.3.9). The TISI provides three functions:

- Tactical messaging.
- Light-weight publish and subscribe.
- Non-real time streaming (ie TCP).

It is proposed that the interface will be implemented as a new application-layer protocol over HTTP (RFC 2616) and WebSockets (RFC 6455). Whether applications will use Microsoft's HTTP/WebSockets API calls or an EvO specific HTTP/WebSockets API is not yet known.

The TISI will be defined in the MORPHEUS Tactical Internet Service Interface IDD, document number GD200155037.

© 2017 Crown Copyright

3.3.2 Alerts Service

The Alerts Service manages Alerts within the system by creating and maintaining a list of locally active Alerts based on the occurrence of system Events and enabling client applications and software services to query and manipulate this list. The Alerts Service exposes the Alerts Application Interface (AAI).

The AAI enables client applications and software services to trigger an Alert locally, to clear Alerts, to re-sound Alerts, to enumerate a list of all currently active Alerts, and to query information relating to specific active Alerts.

It is proposed that the AAI will be implemented as WebSockets over Transport Layer Security (TLS).

The AAI will be defined in the MORPHEUS Alerts Application Interface IDD, document number GD200155038.

3.3.3 Formatted Message Service

The Formatted Message Service (FMS) supports message format translation or adaptation of messages into a specific format required for particular domains and applications. The FMS exposes the Formatted Message Automation Interface (FMAI).

The FMAI provides an automated message formatting capability that converts a message format from one type to another message format.

The FMS and FMAI will be provided by Systematic's IRIS Forms.

The FMAI will be defined in the MORPHEUS Formatted Message Automation Interface IDD, document number GD200155039.

3.3.4 Information Management Service

The Information Management Service (IMS) stores and retrieves common data and efficiently distributes/replicates this data around the EvO system; it provides consumers with a single view of the system's common persistent and transient data, irrespective of where the data is physically held. The IMS exposes the Information Management Service Interface (IMSI).

The IMSI provides point of entry to the system's common data, be it persistent or transient. The IMSI provides the following functions:

- Storage and retrieving of information items held both locally and remotely.
- Query of content by searching the distributed index of all information stored by the IMS.
- User-initiated publish and subscribe to information items or Communities of Interest (COIs), including provision of notifications to clients based on active subscriptions.

The technology used to implement the IMSI has not yet been identified. It is likely that the interface will be provided as Microsoft .NET Core libraries.

The IMSI will be defined in the MORPHEUS Information Management Service Interface IDD, document number GD200155032.

3.3.5 Logging Service

The Logging Service provides a mechanism for applications and services to log system-related events of various different types (eg standard, security related) and at different levels of severity (eg

© 2017 Crown Copyright

information, warnings, errors) to persistent storage. The Logging Service exposes the Logging Service Interface (LSI).

The LSI provides a set of functions for logging events to the system event and security logs. The interface also supports querying of the event logs and retrieval of their respective contents.

It is proposed that the LSI be based on Windows 10 Logging APIs. Whether applications will use Microsoft's API calls or an EvO specific Logging API is not yet known. It is likely that an EvO specific interface would be provided as Microsoft .NET Core libraries.

The LSI will be defined in the MORPHEUS Logging Service Interface IDD, document number GD200155040.

3.3.6 Multimedia Management Service

The Multimedia Management Service provides a mechanism for delivering multimedia services over an IP network. It provides a local point of control for all multimedia users on a platform, and allows sessions to be routed off platform if the destination user is located elsewhere. Local Unified Communications Applications[1] (UCAs) to register and can mutually authenticate with remote instances of the Multimedia Management Service for call routing purposes. The Multimedia Management Service exposes the Multimedia Management Service Interface (MMSI).

The MMSI allows multimedia client applications to communicate with each other over the Tactical Internet and across the system boundary using the appropriate gateway services. The MMSI supports the control plane (signalling) and user plane (media traffic) protocols required by Unified Communications Applications in order to communicate.

It is proposed that the MMSI be implemented as Session Initiation Protocol (SIP) (RFC 3261), Session Description Protocol (SDP) (RFC 4566), Real-time Transport Protocol (RTP) (RFC 3550), and Real-Time Streaming Protocol (RTSP) (RFC 7826). It is likely that the interface will be provided as Microsoft .NET Core libraries.

The MMSI will be defined in the MORPHEUS Multimedia Management Service Interface IDD, document number GD200155041.

3.3.7 Tactical Directory Service

The Tactical Directory Services (TDS) provides a directory of user and network accessible resources whilst being aware of the peculiarities of the TI. A directory is a set of objects with attributes organised logically in a hierarchical manner, providing a map between names and values. Information entities stored within directories can include servers, printers, users, groups, telephone numbers, and accessible devices. A directory allows the lookup of values given a name, similar to the way a dictionary is used. For example, looking up groups using a directory service might yield a list of available user groups and information relating to the members of each group. The TDS exposes the Directory Services Interface (DSI).

[1] The Unified Communications Application provides a single access point for the user to perform all of their telephony, conferencing and instant messaging activities. Examples of commercial unified communications systems include Microsoft Skype and WhatsApp.

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

The DSI provides users and applications with access to shared information infrastructure for locating, managing, administering and organising user data, network resources, and credentials. Common network resources can include, for example, users and printers.

It is proposed that the DSI will be implemented as Lightweight Directory Access Protocol (LDAP) (RFC 4511). Whether applications will use Microsoft's LDAP API calls or an EvO specific LDAP API is not yet known.

The DSI will be defined in the MORPHEUS Directory Services Interface IDD, document number GD200155042.

3.3.8 Tactical Email Service

The Tactical Email Service (TES) adapts the interfaces provided by the TIF to those required by commercial email clients. The TES exposes the Tactical Email Service Interface (TESI).

The TESI allows COTS email clients to send emails over the TI.

It is proposed that the TESI will be implemented as (SMTP) (RFC 821), (POP3) (RFC 1939) and (IMAP) (RFC 3501).

The TESI will be defined in the MORPHEUS Tactical Email Service Interface IDD, document number GD200157791.

3.3.9 Tactical Routing Service

The Tactical Routing Service (TRS) is responsible for routing within the TI. The service supports standard routing protocols, such as OSPF, as well as specialised protocols optimised for the tactical environment. One of the interfaces exposed by the TRS is the Network Feedback Interface (NFI).

The NFI provides an interface to applications enabling them to determine the quality of the path to a particular endpoint, based on information received in the last received routing update. This connectivity information would enable the System and Security Management to display network topology information indicating any connectivity issues that may exist between networks. This interface would be used in conjunction with the Tactical Internet Service Interface (TISI) (Section 3.3.1), used by client applications to send and receive network traffic.

The technology used to implement the NFI has not yet been identified. It is likely that the interface will be provided as Microsoft .NET Core libraries.

The NFI will be defined in the MORPHEUS Network Feedback Interface IDD, document number GD200157792.

3.3.10 Application Orchestration Service

The Application Orchestration Service (AOS) supports the development of applications, orchestrating the interaction between the EvO or application's data model and appropriate Business Logic Plugins (Section 3.2.5) to present data to the user through the Web Application Framework Frontend Service (WAFFS) (Section 3.3.11) graphical components. It is responsible for orchestrating the application logic, data and workflows by linking a Single Page Application to the Information Management Service (IMS) (Section 3.3.4) and the application's statically configured Business Logic Plugins (Section 3.2.5).

The AOS uses the Business Automation Rules Interface (BARI) to apply the business rules and execute the business processes provided by a Business Logic Plugin (Section 3.2.5) for an SPA (Section 3.2.4).

© 2017 Crown Copyright

The AOS exposes the Application Orchestration Service Interface (AOSI).

The AOSI provides an interface between user-facing SPAs and the AOS which, in turn allows access to business rules and processes and both system and application data.

The technology used to implement the AOSI is an open EvO-defined configuration language described using JavaScript Object Notation (JSON).

The AOSI will be defined in the Application Orchestration Service Interface IDD, document number GD200165001.

3.3.11 Web Application Framework Frontend Service

The Web App Frontend Framework (WAFFS) is a Web service that enables application user interfaces to be crafted through configuration rather than hard-coding. Each WAFFS application supports the user in performing a number of tasks, typically by providing workflows that lead them through a number of task-specific views. Views are constructed from a number of linked WAFFS graphical components. The relationships between an application's view, its data, graphical components and Business Logic Plugins (Section 3.2.5) are defined in the configuration file provided by an SPA (Section 3.2.4). An additional benefit of the WAFFS is that it supports the sharing of data, commands and workflows not only within a WAFFS application but also externally between different WAFFS applications. The WAFFS utilises HTML5, JavaScript and CSS.

The WAFFS exposes the Web App Frontend Framework Interface (WAFFI).

The WAFFI provides an interface that allows SPAs (Section 3.2.4) to utilise the graphical components of the WAFFS; these components provide different views of the structured data provided via the Application Framework's IMSI (Section 3.3.4).

The technology used to implement the WAFFI is an open EvO-defined configuration language described using JSON.

The WAFFI will be defined in the Web Application Frontend Framework Interface IDD, document number GD200164992.

© 2017 Crown Copyright

4.0 Computer Resource Requirements

This section includes hardware computing platforms (Section 4.1) and software operating systems (Section 4.2) on which the BMA will be hosted. *It does not include hardware resource utilisation since it is not yet known what other applications and services will be hosted on platforms; any resource contention issues can only be determined by system performance modelling and/or during integration.*

4.1 Hardware Computing Platforms

The BMA software will be hosted on the following physical devices:

- Computer Type 1 Mk3 (CT1) (Section 4.1.1).
- Computer Type 2 Mk3 (CT2) (Section 4.1.2).
- P-BISA Processor Unit Mk3 (PBPU) (Section 4.1.3).
- Vehicle Processor Unit (VPU) (Section 4.1.4).
- Man Carried User Data Terminal (MCUDT) (Section 4.1.5).
- HQ User Data Terminal (HQUDT) (Section 4.1.6).
- HQ Server (Section 4.1.7).

4.1.1 Computer Type 1 Mk3

Type. Rugged notebook computer.

Processor. 2.8 GHz Intel® Core i7 Dual Core (quad thread).

Volatile Memory. 2 x 8 GB DDR3/ECC (16 GB total).

Non-Volatile Memory. Removable internal 320 GB SATA hard drives; Optional DVD/CD-ROM drive.

Display. 12.1" XGA (1024 x 768); Integrated ATI Radeon high performance Graphics Processing Unit (GPU) with 128 MB GDDR3 Memory.

Multimedia. None.

Network. 10/100/1000 base-T Ethernet.

Ports. RS-232; RS-422 or RS-423; RS-422 or RS-423 or isolated RS-422.

Input Devices. Touch screen; keyboard; toggle/touchpad buttons.

4.1.2 Computer Type 2 Mk3

Type. Rugged touch-screen tablet.

Processor. 2.8 GHz Intel® Core i7 Dual Core (quad thread).

Volatile Memory. 2 x 8 GB DDR3/ECC (16 GB total).

Non-Volatile Memory. 2 removable internal 320 GB SATA hard drives or 512 GB SSHDs; Optional DVD/CD-ROM drive.

Display. 12.1" XGA (1024 x 768).

Multimedia. None.

Network. 10/100/1000 base-T Ethernet.

Ports. RS-232, RS-422 or RS-423, RS-422 or RS-423 or isolated RS-422.

Input Devices. Touch screen; remote keyboard; toggle/touchpad buttons.

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

4.1.3 P-BISA Processor Unit Mk3

Type. Rugged crew station.

Processor. 2.8 GHz Intel® Core i7 Dual Core (quad thread).

Volatile Memory. 2 x 8 GB DDR3/ECC (16 GB total).

Non-Volatile Memory. Removable internal 480 GB SSD.

Display. 12.1" Hi-resolution - VGA (640 x 480) up to SXGA (1280 x 1024 pixels) RS170 Composite - PAL/NTSC; multiple video inputs (two high resolution and two low).

Multimedia. None.

Network. 10/100/1000 base-T Ethernet.

Ports. 1 off RS170 output converted from high resolution input.

Input Devices. DEFSTAN 23-09 Generic Vehicle Architecture (GVA) or standard 20 key, all keys with variable backlight; Brightness up/down; Test; Covert Mode (dims screen & indicators). Serial or MilCAN Key presses reported; Serial or MilCAN Touch screen interface; Screen brightness and Covert.

4.1.4 Vehicle Processor Unit

The Vehicle Processor Unit (VPU) is a scalable chassis that provides processing and bulk storage capabilities for vehicle needs such as application hosting, virtual machine hosting, thin-client server hosting, advanced video encoding and processing, and other future capabilities. The exact specification is still to be confirmed during development of the EvO system, but the following information can be used as a guide:

Type. Line-Replaceable Unit (LRU).

Processor. Intel Processor; optional Intel Processor, ARM Processor, Video Processor.

Volatile Memory. At least 32 GB DDR4 RAM for hosting multiple Virtual Machines (VMs).

Non-Volatile Memory. Removable encrypted Secure SSD.

Display. 2 off Digital Visual Interface (DVI); 2 off Serial Digital Interface (SDI).

Multimedia. None.

Network. 3 off 10/100/1000 base-T Ethernet.

Ports. 2 off USB 2.0.

Input Devices. None.

Backplane. Up to 3 VPX COTS OpenVPX CCAs.

Virtual Machines. The VPU will support a variety of virtualisation solutions.

4.1.5 Man Carried User Data Terminal

The MCUDT is based on the MOD selected Panasonic FZ-M1.

Type. Rugged tablet.

Processor. 2.3GHz Intel® i5-4302Y.

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

Volatile Memory. 8 GB DDR3.

Non-Volatile Memory. 256GB SSD.

Display. 7" 1280 x 800 (WXGA); screen rotation at 0, 90, 180, 270 degrees.

Multimedia. Internal speaker; built-in microphone; built-in webcam.

Network. 10/100/1000 base-T Ethernet; Intel® Dual Band Wireless-AC 8260; Bluetooth® Version 4.1 + EDR Class 1; 4G Mobile Broadband Option (Gobi 5000), supports 3G.

Ports. RS-232; 2D Barcode Reader; USB 2.0.

Input Devices. Touch screen.

4.1.6 HQ User Data Terminal

The HQUDT is based on the MOD selected Getac S410.

Type. Semi-rugged notebook.

Processor. 2.5GHz Intel® Core™ i7-6500U.

Volatile Memory. 16 GB LPDDR3.

Non-Volatile Memory. 500GB HDD or 256GB SSD.

Display. 14" TFT, 1366 X 768.

Multimedia. Internal speaker; built-in microphone; built-in webcam.

Network. 10/100/1000 base-T Ethernet; Intel® Dual Band Wireless-AC 7260; 802.11ac; Bluetooth® Version 4.1 + EDR Class 1.

Ports. USB 3.0; USB 2.0; RS-232; VGA; HDMI; audio output; microphone.

Input Devices. Keyboard; touchpad.

4.1.7 HQ Server

4.1.7.1 Virtualisation Host

Processor. 2.2/3.2 GHz 2 x Intel® 10 Core Xeon® Processor E5-2618L.

Volatile Memory. 128 GB DDR3; 32 GB SSD Bootable Storage capacity.

Non-Volatile Memory. 8 x 512GB SSD RAID 10; Bootable Storage RAID 1.

Display. None.

Multimedia. Audio, TBC.

Network. 10/100/1000 base-T Ethernet.

Ports. RS-232; USB 2.0.

Input Devices. None.

Virtual Machines. Deployment of VMs over hosts and allocation of services to VMs is dependent on user requirements and scaling of hosts and users in HQ environments; this will be finalised during EvO integration activity.

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

4.1.7.2 Management Host

Processor. 2.3/3.3GHz Intel® i5-6500 TE.

Volatile Memory. 8 GB DDR3.

Non-Volatile Memory. 250 GB SSD.

Display. 17" IP52 LED SXGA 1280x1024.

Multimedia. Audio, TBC.

Network. 10/100/1000 base-T Ethernet.

Ports. RS-232; USB 2.0.

Input Devices. Keyboard; mouse; Two-port KVM switch switching between Virtualisation and Management hosts.

4.2 Software Computing Platforms

The BMA software will be hosted on the following operating systems:

- Windows 10 Enterprise (Section 4.2.1).
- Windows Server 2016 (Section 4.2.2).

This section also includes information on how software shall be delivered for integration and deployment (Section 4.2.3).

4.2.1 Windows 10 Enterprise

Version. The version to be delivered with the EvO baseline is not yet known; it is likely to be the latest version available from Microsoft including all updates and patches that have been made available. The operating system will be hardened appropriately; the starting point will likely be the National Cyber Security Centre's (NCSC) End User Device (EUD) security guidance for Windows 10[2].

Frameworks. .NET and support for Universal Windows Platform (UWP) will be available to hosted applications at the latest versions. .NET Core will be installed on Windows 10 platforms to support cross platform applications.

Additional APIs. DirectX and OpenGL will be available to hosted applications at the latest versions.

Containers. EvO platforms will not be providing any additional support for containerisation other than that provided by Windows 10.

AppLocker/Device Guard. Microsoft's AppLocker and Device Guard will be used on Windows 10 platforms to limit application execution to appropriate users and user groups.

Disk Encryption. Some means of disk encryption will be used to protect data at rest; it is not likely that Microsoft's BitLocker will be used for EvO.

USB Filter. Some form of USB filter will be used to restrict access to USB ports; it is not likely that Device Guard will be used for this purpose on EvO.

[2] https://www.ncsc.gov.uk/guidance/eud-security-guidance-windows-10-1.

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

4.2.2 Windows Server 2016

Version. The version to be delivered with the EvO baseline is not yet known; it is likely to be the latest version available from Microsoft including all updates and patches that have been made available. The operating system will be hardened appropriately; guidance will come from the NCSC and the starting point will likely be along similar lines to the EUD security guidance for Windows 10.

Frameworks. .NET and support for UWP will be available to hosted applications at the latest versions. .NET Core will be installed on Windows Server 2016 platforms to support cross platform applications.

Additional APIs. DirectX and OpenGL will be available to hosted applications at the latest versions.

Virtualisation. It is not yet know what virtualisation software will be provided on EvO server platforms but is likely to be VmWare at the latest version.

AppLocker/Device Guard. Microsoft's AppLocker and Device Guard will be used on Windows Server 2016 platforms to limit application execution to appropriate users and user groups.

Disk Encryption. Some means of disk encryption will be used to protect data at rest; it is not likely that Microsoft's BitLocker will be used for EvO.

USB Filter. Some form of USB filter will be used to restrict access to USB ports; it is not likely that Device Guard will be used for this purpose on EvO.

4.2.3 Application Delivery

Windows 10 Apps (UWP) shall be delivered as an appx upload package which will be uploaded to an EvO Tactical Apps Store ready for deployment.

Non-Windows 10 applications shall be delivered as Microsoft Installer (MSI) packages:

- Developed software shall be contained in a single MSI package; the installer shall allow specification of installation location in the file system.
- Each dependency, eg legacy versions of .NET, shall be contained in a single MSI package. Where dependencies are expected to be already resident on the platform, the installation shall ensure the dependency is present and alert the build system if it is not present.
- MSI packages shall support unattended installation.
- MSI packages shall support configurable parameters by provision of configuration file(s), Windows Registry entries or installer command line options.

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

5.0 Design and Implementation Constraints

5.1 Architectural Considerations

The MORPHEUS Target System Architecture (MTSA) includes a set of architectural requirements[3] that specify the architectural drivers that shall guide the development of EvO such that it is a step towards to target architecture. It is recommended that the following principles are flowed down to the BMA supplier:

- Tactical Element of Single Information Environment (Section 5.1.1).
- Improved Information Superiority (Section 5.1.2).
- Rapid Exploitation of Emergent Technology (Section 5.1.3).
- Increased Agility/Flexibility (Section 5.1.4).
- Reduced Delivery Times (Section 5.1.5).
- Reduced Costs (Section 5.1.6).
- Vendor Independence (Section 5.1.7).

5.1.1 Tactical Element of Single Information Environment

MORPHEUS will provide common and resilient services aligned to the DaaP initiative. MORPHEUS will support seamless information flow throughout the tactical battlespace to the extent that is technically feasible given capacity and latency constraints. Services will be integrated onto Land Environment platforms from formation and unit HQs down to the dismounted soldier, as well as maritime and air platforms. Appropriate use of TIF services, particularly the IMSI, will support this principle.

5.1.2 Improved Information Superiority

MORPHEUS will enable better decision making at pace through the provision and sharing of timely and accurate all-source information, including with Allies. Information superiority is achievable through collaborative decision making, shared situational awareness, information sharing, information accessibility, information prioritisation, ease of use, information coherence, information integrity and authoritative information. The Staff and Platform C2 Applications and appropriate use of TIF collaborative services, particularly the IMSI, will support this principle.

5.1.3 Rapid Exploitation of Emergent Technology

MORPHEUS will provide an open, delaminated architecture that enables the rapid insertion of emergent technologies. MORPHEUS will provide capabilities to efficiently distribute emergent technologies across a deployed system.

5.1.4 Increased Agility/Flexibility

MORPHEUS will support increased procurement agility and flexibility by supporting the principles of Evergreening. The principles of Evergreening are:

- Easy introduction of additional software services and applications.
- Straightforward bearer and device integration.
- Future-proofed external system integration.
- Design and development flexibility.

[3] GDUK-EVO-33244 MORPHEUS Architectural Requirements Specification Issue C dated 12/05/2017.

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

- Enhanced deployment flexibility.
- Manufacturing flexibility.

5.1.5 Reduced Delivery Times

MORPHEUS will increase acquisition responsiveness for delivery by identifying opportunities for rapid acquisition and insertion of mature technologies that utilise well defined interfaces that conform to open specifications or standards.

5.1.6 Reduced Costs

MORPHEUS will reduce costs by utilising open, MOD-owned, standards enabling increased competition and use of COTS technology, where appropriate, to achieve significant through-life savings whilst providing a reasonable Vendor Independence.

5.1.7 Vendor Independence

MORPHEUS will allow Information Systems & Services (ISS) to control an open supply chain that is 100% vendor independent.

5.2 Collaborative Approach to Delivery

The development of the EvO System is being done in an open and collaborative manner between the Authority, GDUK and the End User in order to optimise the EvO System. GDUK recognises and supports the Authority in its objective to become the Quasi-Prime of its own supply chain and GDUK understand that the Authority as the Quasi-Prime will develop and maintain the contractual relationship and all decision making powers on the BMA and EvO Contracts. GDUK understands that the Authority is seeking to establish collaborative partnering relationships, in line with ISO-44001, with key members of its supply chain such as the BMA provider. As the EvO Transition Partner, GDUK would seek to hold an open and collaborative relationship with the BMA Contractor to enable effective communication and information sharing during the design, development and integration of the BMA and EvO System.

5.3 Other System Level Constraints

The BMA shall be provided as GFE and delivered as a constituent part of the EvO system. As such, it is important that the BMA delivery considers system level requirements and constraints related to Human Factors (Section 5.3.1) and ILS (Section 5.3.2).

5.3.1 Human Factors

MOD shall impose the human factors requirements in DEFSTAN 00-251 Human Factors Integration for Defence Systems on the BMA supplier. Where the BMA product(s) is any combination of modified COTS and bespoke development, the BMA supplier shall be cognisant of the key Human-Computer Interaction principles defined in the MOD's Technical Guides contained within JSP 912 Human Factors Integration for Defence Systems and the EvO Style Guide. The BMA supplier shall:

- In accordance with JSP912, support joint working groups and workshops.
- Provide a Human Engineering Product Analysis Report (HEPAR) to the MOD and GDUK to assure the consistency of the system solution.
- Follow a lean User Experience (UX) methodology.
- Provide input to the progressively received and evolving user interface System Style guide.

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

5.3.2 Integrated Logistics Support

As GFE, the BMA delivery shall consider ILS requirements for a training solution (Section 5.3.2.1) and software support (Section 5.3.2.2).

5.3.2.1 Training

MOD shall impose the training requirements in JSP 822 Defence Direction and Guidance for Training and Education on the BMA supplier. To support development of the training solution for EvO, training related information shall be provided as input to the following:

- Training Needs Analysis (TNA) Report.
- EvO Role Performance Statement.

5.3.2.2 Software Support

MOD shall impose the ILS requirements in DEFSTAN 00-600 Integrated Logistic Support Requirements for MOD Projects on the BMA supplier. To support development of the EvO Support Plan a Software Support Plan for the BMA should be provided.

5.4 Government Furnished Information

The BMA is a component part of the EvO system and as such delivery of the product(s) shall be accompanied by GFI that describes its architecture, openness, operation and acceptability, and supports integration with the EvO system. The EvO contract states that the MOD will provide the following GFI to GDUK relating to the BMA procurement:

- BMA Tech Proposals, Compliance Statements and other GFI (Section 5.4.1).
- BMA Openness Test Results (Section 5.4.2).
- BMA Software Documentation (Section 5.4.3).
- BMA Qualification Documentation (Section 5.4.4).

5.4.1 BMA Tech Proposals, Compliance Statements and other GFI

Purpose. To provide information on the BMA delivery that will allow GDUK to understand the scope of the integration task and to plan integration activities.

Content. The BMA supplier's technical bid or any subset of which deemed appropriate by the Authority. This is expected to include the technical proposals, compliance statements and other GFI useful for planning integration activities such as system architecture, hardware and software operating environment requirements and development environment and tools.

Format. The information shall be delivered as documents, spreadsheets and possibly presentations in protected Portable Document Format (PDF).

5.4.2 BMA Openness Test Results

Purpose. To allow General Dynamic United Kingdom (GDUK) to understand the openness of the BMA product(s) and to include the assessment as part of the EvO openness report. This will support GDUK in meeting the EvO Architectural Principles.

Content. The results of the Authority's openness tests executed against the BMA product(s). Any test failures accepted by the Authority shall be clearly stated.

Format. The results shall be delivered as documents or spreadsheets in protected Portable Document Format (PDF).

© 2017 Crown Copyright

5.4.3 BMA Software Documentation

Purpose. To allow GDUK to install, set up, operate and conduct user maintenance of the BMA product(s) such that the BMA can be integrated with the EvO system. This information may also be used for work on the EvO Training Needs Analysis (TNA).

Content. At minimum this documentation shall include installation guides, quick start guides, user instructions and troubleshooting instructions, Software Development Kit (SDK) and Application Programming Interface (API) documentation and Interface Control Documents (ICDs). Where deemed appropriate by the Authority, additional architectural and design documentation may be provided.

Format. This documentation shall be delivered at least as protected PDF; at best all documentation will be delivered in a format allowing online intranet or Internet access by users and integration engineers.

5.4.4 BMA Qualification Documentation

Purpose. To confirm to GDUK that the BMA product(s) is acceptable to the Authority, and to allow GDUK to document the totality of the level of compliance of the EvO system.

Content. A formal Certificate of Conformance (CofC) from the supplier attesting to the level of compliance of the BMA product(s) with the Authority's requirements, as accepted by the Authority.

Format. The CofC shall be delivered as a paper hard copy accompanied by the certificate in protected PDF.

© 2017 Crown Copyright

6.0 Security

MOD shall impose security requirements on the BMA supplier that will contribute to delivery of EvO as a secure system that can be accredited. To facilitate this, the following high level requirements are mandatory:

- **Accreditation Framework**. The BMA supplier shall operate within the constraints of the EvO accreditation framework and provide a subset of accreditation and assurance evidence for the BMA.
- **Secure Configuration**. The BMA shall operate within the constraints of the EvO secure configuration baseline and shall not introduce additional security vulnerabilities.
- **Security Management**. The BMA shall operate within the constraints of the EvO security management provisions and protect the BMA configuration from unauthorised modification and tampering.
- **Availability**. The BMA shall operate to maximise service availability within the constraints of the EvO TI including backup and recovery functions.
- **Information Exchange Requirements**. The BMA shall protect the exchange of information messages internally and externally including integrity, authenticity and content checking.
- **Authentication and Access Control**. The BMA shall integrate with the EvO Identity and Access Management (IdAM) services to authenticate and determine permissions applied to authorised users and roles.
- **Classification and Labelling**. The BMA shall ensure that data held and processed by the BMA applies the correct classification and labelling information to support the EvO information handling model, access control model and information exchange requirements.

To support development of accreditation and assurance evidence for the EvO system security related information shall be provided as input to the following:

- Security Management Plan.
- Security Risk and Impact Assessment.
- Security Design and Implementation.
- Residual Risk Identification.
- Security Testing and Verification Evidence.
- Security Operating Procedures (SyOps) Recommendations.
- Information Technology Health Check (ITHC) Reports.

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

7.0 Safety

MOD shall impose the safety requirements in DEFSTAN 00-055 Requirements for Safety of Programmable Elements in Defence Systems on the BMA supplier. To support development of the EvO Safety Case BMA safety related information shall be provided by the supplier.

© 2017 Crown Copyright

8.0 Dependencies on the BMA Supplier

There are several Transition Partner (TP) dependencies on the BMA supplier; these are articulated in this section as follows:

- Architecture and Design (Table 1).
- Commercial (Table 2).
- BMA Definition (Table 3).
- Programme (Table 4).
- System Integration (Table 5).
- Product Alignment (Table 6).
- Customer Dependencies (Table 7).

Table 1 – Architecture and Design Dependencies

Title	Dependency
EvO Interfaces Conformance	For each EvO interface supported, provide a statement of conformance and any supporting evidence. This is to support statements relating to openness of the EvO system.
Non EvO Interfaces Conformance	Where the BMA exposes interfaces that are not part the EvO system, for each non EvO interface supported, provide a statement of conformance and any supporting evidence. Where required, eg proprietary interfaces, provide full interface definition. This is to support statements relating to openness of the EvO system.
Performance	Performance of the BMA within the EvO system will need be determined by TP and BMA supplier during integration of the EvO system and will be assessed against the BMA Measures of Performance (MOPs) imposed by MOD.
ILS	GD will require support from the BMA Supplier throughout the course of the delivery of the EvO Contract and requires the BMA Contractor to provide any, reasonably, requested information or response to clarification questions in an agreed form within a reasonable time period giving due regard to the complexity of the requirement. Particular instances for which GDUK view this as being necessary are: • EvO System TNA Report. • EvO System Role Performance Statement. • EvO System Support Plan.
Safety	Provision of safety related information in support of development of the EvO Safety Case. Support to collaborative Safety forum led by the Joint Programme Office (JPO).
Security	Provision of the following information at the dates specified in the TP contract: Initial Capability

© 2017 Crown Copyright

Title	Dependency
	• Security Management Plan. • Security Risk and Impact Assessment. Complete Functionality • Security Design and Implementation. • Security Operation Procedure (SyOps) recommendations. Final Drop • Residual Risk Identification. • Security Testing and Verification Evidence. • Information Technology Health Check (ITHC) report.
EvO Architecture Assurance Reviews	The BMA supplier shall provide the necessary personnel and support for the EvO Architecture Assurance Reviews from Review 3 onward (October 2018). Reviews are 1-day events occurring every 6 months. Whilst it is accepted that the BMA supplier will be best placed to determine their level of effort, GDUK typically utilise 3 personnel over 5 days in direct support of a review.
EvO Architecture Acceptance Review	The BMA supplier shall provide the necessary personnel and support for the EvO Architecture Acceptance Review taking place at the end of the EvO programme. Whilst it is accepted that the BMA supplier will be best placed to determine their level of effort, GDUK expect to utilise 3 personnel over 5 days in direct support of this review.
Support to ESCoT	The BMA supplier shall provide the necessary personnel and support for JPO and/or EvO System Coherence Team (ESCoT) requests and identification and resolution of issues relating to BMA aspects of the MORPHEUS and EvO System Architecture. ESCoT workshops are 3-day events that occur every 12 weeks. Whilst it is accepted that the BMA supplier will be best placed to determine their level of effort, GDUK typically utilise 3 personnel over 5 days in direct support of a workshop.

Table 2 – Commercial Dependencies

Title	Dependency
ITAR/Export Compliance	MOD shall be responsible for securing any export licence, authorisation(s) or other related technology transfer control required to authorise the BMA supplier to utilise any aspect of the EvO System (information and items, including software) that is subject to an export licence, authorisation(s) or other related technology transfer control.

© 2017 Crown Copyright

Title	Dependency
Intellectual Property Rights and Software Licences	Prior to MOD agreeing the Terms and Conditions of the BMA Contract with the BMA Supplier, MOD shall provide to GDUK a copy of the Terms and Conditions from the BMA Contract that govern the Intellectual Property Rights and Software Licences, to allow GDUK to review and comment upon these accordingly. In the event that GDUK believe there are deficiencies in these Terms and Conditions and that they do not align to the provisions within the EvO TP Contract, MOD and GDUK shall meet to discuss and reach a mutual agreement on the changes required to the Terms and Conditions of the BMA Contract.
Warranty	The BMA supplier shall warrant and represent to MOD, through the Terms and Conditions of the BMA Contract with MOD, that: • it has the corporate power to enter into and to exercise its rights and perform its obligations under the BMA Contract and any Sub-Contracts; • it is not subject to any claim, litigation, arbitration, proceedings or any other obligation which shall or is likely to have a material adverse effect on its to perform its obligations under the BMA Contract; • it shall not, and in entering into the BMA Contract it has not, committed any Prohibited Act as defined in the EvO TP Contract, and for this purpose only the words "or without" in the introduction of the definition of Prohibited Act shall be deleted; • so far as it is aware, there is not, nor has there been, any infringement or alleged infringement of any third party's Intellectual Property Rights in connection with the BMA Contract; • it has used and will continue to use the degree of skill, care and foresight in the performance of each of the BMA Contract Deliverables, that would reasonably be expected of a competent professional contractor experienced in carrying out activities of a similar nature, scope and complexity to those comprised in the BMA Contract Deliverables and that it shall remedy any defects in the BMA Contract Deliverables in the same manner, free of charge and as soon as reasonably possible, from notification of the relevant defect by MOD to the BMA supplier (including where GDUK have notified the BMA supplier of any defects either directly or via MOD) on or after Acceptance of the relevant BMA Contract Deliverable and on or before the date which is three (3) years after the Release Control Point under the EvO TP Contract.

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

Table 3 – BMA Definition Dependencies

Title	Dependency
Capability Description	The BMA supplier shall provide product specific information to allow GDUK to generate Capability Description Document Product Descriptors (GDUK-EVO-33611) for the following Technical Capabilities: • Mission Planning and Execution. • Shared SA/Operating Picture. • Navigation. • Geospatial Services.
Version Descriptor Document for each software release	A description to be provided for each contractual software release, covering the sections, within VDD Product descriptor 124 (GDUK-EVO-33995), applicable to a CSCI or set of CSCI's constituting an individual product
Design review slide packs	Provision of design information or Design Review Packs, to ensure that through-out its development the product conforms to the requirements within this document. Depending on the nature of the BMA development programme this may include the following types of review: – System/Product Design Review, Preliminary DR, Critical DR, Integration Readiness Review, Test Readiness Review, Acceptance Readiness Review
Certificate of Conformance	VDD for each software and firmware A statement agreed between the Authority, BMA supplier and the Authority's Security Working group that the BMA as implemented satisfies the applicable security requirements and the overall approach to security adopted for EvO. Support to GDUK to produce a product safety case for each product delivered, or equivalent statement that changes have not affected the current safety case.

Table 4 – Programme Dependencies

Title	Dependency
Delivery Schedule	Dates for BMA software to be delivered to GDUK to comply with Schedule 7 of the EvO contract.
Collaborative Working	Once contract award has been made to the product provider, it is expected that the chosen supplier will engage with the Authority and GDUK.
Exception Management	In the event of issues impacting the programme that may affect the delivery milestones identified in the schedule, the contractor is to inform the Authority and GDUK of the issue, its impact and remedial actions necessary to maintain the schedule delivery dates.

© 2017 Crown Copyright

Title	Dependency
Baseline Management	During the development programme, it would be beneficial for additional interim software drops to be made available for interim testing activities, bug identification and confirmation of bug resolution. Each software drop should be accompanied by an informal Release Note that will give details of any changes that have been included in the latest version of the product. The schedule of delivery drops will be agreed once the product provider has been chosen.

Table 5 – System Integration Dependencies

Title	Dependency

Support to System Integration	To ensure that EVO Integration Services are in a position (pragmatically, technically and commercially) to engage with the BMA Developers the following is required to be in place with the BMA provider to successfully integrate with EVO. The assumption is the BMA has a high level of product maturity and the focus is firmly on the developing, integrating and assurance of the interface between BMA and EVO.
	
	The Programmatic
	The Aim: BMA provider to achieve alignment with EVO to meet the proposed EVO delivery.
	
	Programme Alignment Meetings (PAM).
	Schedule: 2 meetings - Pre-contract and at Contract Award (CA).
	Objectives/outputs:
	• Assumes NDA in place prior to meeting
	• Address any outstanding Commercial (ITAR, GFX issues)
	• Published EVO/BMA Agreed Schedule - BMA PMP/TLMP
	  ○ Identify key EVO & BMA programme dates
	  ○ Agreement that programme schedule meets stakeholder needs
	• Initial joint EVO/BMA Risk Register compiled and published - BMA Risk Registry
	• Confirms EVO SI&T Engineering ready to engage - response to technical questions
	Inputs from BMA provider:
	• JSP 604 Data Capture Form completed and provided to EVO
	• Concept of Use and/or Concept of Employment (CONUSE, CONEMP).
	• User Requirements Document (URD).

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

Title	Dependency

	• System Requirements Document (SRD)
	• System Architecture Documents (SAD).
	• System Design Documents (SDD).
	• ITEAP (Draft)
	• Technical Standards.
	• Human Factors Integration (HFI) – BMA HFI Plan
	• Security
	  ○ Security Aspects Letter
	  ○ Security Management Plan.
	• Safety – Safety Case Part 1
	
	Architecture Alignment and production of Test Requirements (AA)
	Schedule: Two 2 day workshops to confirm Architecture Alignment. Single meeting to agree Architecture Alignment and resulting testing requirements for EVO/BMA interface.
	Objectives/outputs:
	• Produced Draft EVO/BMA Interface Control Document
	• Initial Architecture Studies completed – BMA MODAF SysML
	• Pre-condition and Input status assessment
	• Confirmation of recommendations of COTS/reuse analysis
	  ○ EVO/BMA COTS/reuse analysis complete
	• EVO/BMA Architectural Baseline ready to support test development
	  ○ Test Basis developed & frozen
	  ○ Agreement on the definition of the EVO/BMA interactions.
	  ○ Test script writing started
	• EVO/BMA Integration Test & Acceptance Plan published
	• BMA Operational Scenario available from User SME.
	
	Inputs: Updates, if applicable, to all documents already supplied
	• Application Programming Interface (API) Specifications.
	• Extracts from developed architecture models (eg UML, SysML, and MODAF) for the Interface.
	• ITEAP
	• System Perf Model - BMA Model
	• Human Factors Integration (HFI) – BMA HFI Plan
	• Safety – Safety Case Part 2 (Draft)
	
	EVO/BMA System Integration Testing (SI)
	Schedule: 3 workshops to Delivery, install, configure and commission BMA software (BMA SE & SI engineer on site at Oakdale for 3 x 1 week).

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

Title	Dependency

	Note: The testing could start to occur immediately following CA if BMA is MOTS and requires little development – either as a BMA or the "shim" with EVO. If there is BMA development then the start of EVO/BMA testing will start later and not necessary in parallel with the above architecture and test production tasks.
	One Meeting to agree EVO/BMA Interface Testing can proceed (All Stakeholders)
	One defect sentencing meeting attendance per week of 2 hours (Small and often)involving all stakeholders
	
	Objectives/outputs:
	• Confirmation of acceptable maturity of Interface Control Document
	  ○ Risk Register and Schedule updated and published
	  ○ Interface Control Document updated published
	• BMA User Guides and Training Material (if MOTS).
	• System Problem Reports (SPRs) or Technical Issues that may block the start of System Integration Testing identified
	• EVO/BMA Test Plan (including sufficient Test Scripts to commence) published
	• Stakeholders content with Planned EVO/BMA test scripts/coverage
	• Test facilities and kit in place for EVO/BMA testing
	• Appropriate releases of EVO and BMA available.
	• Operational elements of Test Plan (scenario) agreed
	• Early Expert User Evaluation conducted (if required)
	
	Inputs: Updates, if applicable, to all documents already supplied.
	• 3 BMA Software builds under configuration control with supporting documentation (such as manuals).
	
	Formal System Integration and Assurance (FSI)
	Schedule:
	One Meeting to agree EVO/BMA Interface Testing can proceed.
	One workshop to Delivery, install, configuration and commission the Final BMA software (BMA SE & SI engineer on site at Oakdale for a 1 week).
	One workshop for assurance and acceptance of the Final BMA software (BMA SE & SI engineer, User, Tech Support on site at Oakdale for a 1 week).
	One Meeting to agree EVO/BMA assured and accepted. (All Stakeholders)
	One defect sentencing meeting attendance per week of 2 hours (Small and often) involving all stakeholders.

© 2017 Crown Copyright

Title	Dependency

	Objectives/outputs:
	• Final Interface Control Document published
	  ○ Stakeholders agree Interface Control Document
	• SPRs or Technical Issues that may block Formal System Integration Testing identified
	• System Integration Test and Analysis Report published
	• FSI Test Plan published
	  ○ Stakeholders content with Planned test scripts/ coverage
	• Test facilities and kit in place
	• Final RCP/FAT release of EVO& BMA available with Keys.
	• Safety Case Part 2 and Part 3
	  ○ Safety Assessor provisional agreements.
	  ○ Safety Integrity Level (SIL) assessments / certification.
	• JSP 604 Accreditation
	• Operational elements of FSI Test Plan agreed
	• Initial Expert User Evaluation conducted (if required)
	
	Inputs: Updates, if applicable, to all documents already supplied.
	• Final BMA Software builds under configuration control with supporting documentation (such as manuals).

Support to Acceptance	BMA will need to provide support to the following 8 EVO acceptance Reviews, including documentation reviews: 30/09/2019 Capability Acceptance Test Case Review (CATCR) 30/09/2019 EvO Architecture Acceptance Review (EvO AAcR) 31/03/2020 Capability Acceptance Test Procedure Review (CATPR) 04/06/2020 Lab-based Acceptance Test Readiness Review (LBATRR) 30/07/2020 MTRC Design Document Acceptance Review 12/08/2020 MORPHEUS Architecture Acceptance Review (MAAcR) 26/10/2020 First of Type Field Test Readiness Review (FTFTRR) 30/11/2020 EvO System Acceptance Test Review (EvO SATR)

Support to Field Test	To confirm readiness to commence Field Test
	• SPRs or Technical Issues that may block Formal System Integration Testing identified
	• Test Plan published
	  ○ Stakeholders content with Planned test coverage Operational elements of Test Plan agreed
	  ○ Expert User Evaluation conducted (if required)
	• Field Test facilities, User Staff and kit in place

Uncontrolled when viewed outside of CM Repository
© 2017 Crown Copyright

Title	Dependency
	• Appropriate release of EVO and BMA available • Effort to support Field Test has not been included.
Fault assessment	BMA Developer follows EVO Defect Reporting Process for EVO/BMA ICD related defects: Includes SE & SI support to analyses and assess defect both at BMA and EVO contractors Site.
Fault Resolution	BMA Developer follows EVO Defect Reporting Process for EVO/BMA ICD related defects: Includes SE & SI support to analyses and assess defect both at BMA and EVO contractors Site. Severity and Priority Assessment.
BMA Roles and Associated Effort	**Role** / **Responsibilities** / **No (Days)** **BMA Developer Manager** / The Industry lead for the development of BMA product. / 2 x PMA, 2 AA, 5 SI, 10 FSI, 8 Reviews **BMA Lead System Engineer** / The Industry POC for the BMA architecture and SE. / 2 x PMA, 5 AA, 19 SI, 15 FSI, 4 Reviews **BMA System Integration Lead** / The Industry Lead for BMA System Integration. / 2 x PMA, 5 AA, 19 SI, 15 FSI, 4 Reviews **Customer Delivery Team (PM + Tech Support)** / The Authority lead for the development of the BMA product. Note 2 persons shared over tasks. / 4 x PMA, 6 AA, 19 SI, 15 FSI, 16 Reviews **BMA Safety & Security Representation(s)** / Industry and Authority's Security and Safety POCs. / 2 x PMA, 1 AA, 3 SI, 2 FSI, 8 Reviews

© 2017 Crown Copyright

Title	Dependency		
	BMA Configuration Manager	Industry POC for delivery of BMA artefacts (docs, builds) within a controlled manner	2 x PMA 1 AA 1 SI 1 FSI 0 Reviews
	BMA User SME	AHQ representative to provide intent, direction, guidance of the Users capability.	2 x PMA 5 AA 10 SI 7 FSI 8 Reviews

Table 6 – Product Alignment Dependencies

Title	Dependency
Integration of BMA into Manage and Conductor	Personnel support to collaborative development in the form of workshops, design meetings, response to technical questions to assist in GDUK software development and integration. Level of support is dependent on the level of compliance to the GDUK architecture and maturity of the BMA product.

Table 7 – Customer Dependencies

Title	Dependency
Support to Customer Demonstrations	Representation at end of PI demo, where appropriate (eg BMA is presented as part of a wider EvO System Demonstration).

© 2017 Crown Copyright