NATO STANDARD

AEP-82

UAS WEAPONS INTEGRATION

Edition A Version 1
JUNE 2017

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED ENGINEERING PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

16 June 2017

1. The enclosed Allied Engineering Publication AEP-82 Edition A, Version 1, UAS WEAPONS INTEGRATION, which has been approved by the nations in the NATO NAVAL ARMAMENTS GROUP, is promulgated herewith. The recommendation of nations to use this publication is recorded in STANAG 4737.

2. AEP-82, Edition A, Version 1, is effective upon receipt.

3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member or partner nations, or NATO commands and bodies.

4. This publication shall be handled in accordance with C-M(2002)60.

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Documents Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Documents Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1.0 INTRODUCTION

1. Weapons have been deployed by various nations and to a greater extent tested, on Unmanned Aircraft Systems (UAS) since the 2001 deployment of armed Predators in Afghanistan. While these weaponised UAS have proven to be highly effective, to date only relatively few weapons have been integrated on UAS. Five major factors limiting the broader development and production of weaponised UAS are:

a. The unique design challenges associated with these systems;

b. The size and weight of current weapons;

c. The issues of integrating the operation of unmanned systems both with manned military forces and operations in civilian airspace;

d. The high costs currently associated with armed UAS design and development; and

e. The lack of political will to introduce unmanned weaponised platforms into armed forces.

2. The most significant design challenges faced in developing armed UAS are related to ensuring system safety. While safety issues have been resolved for manned aircraft, UAS do not have the on-board crew oversight of the platform and weapon utilization. Physical safety mechanisms (crew activated hardwired switches) must be replaced with ground controller decisions which are then processed by software on the ground, relayed by data link to the UAS and again processed by software on the UAS to initiate weapon activation and deployment. Measures and equipment must be developed and certified which will enable safe operation of armed UAS.

3. Operational suitability must be managed to make armed UAS more broadly useable, exchangeable, understandable and acceptable among military forces and civilian airspace users and airworthiness authorities. Integrating the operations of manned and unmanned systems brings additional challenges to achieve the best effects in the field while minimizing investment. These challenges can be mitigated by developing common standards for UAS which ensure the interoperability of these systems with other UAS and manned platforms.

4. Costs associated with developing, integrating and certifying armed UAS is currently high in large measure due to a lack of standardisation between the various UAS. Each developer or weapon integrator generates systems with proprietary interfaces and architectures. Thus, employment of a single weapon type on different UAS platforms necessitates expensive weapon integration programs for each aircraft type. By developing

North Atlantic Treaty Organisation (NATO) standards for UAS weapon interfaces (including UAS Control Station (UCS) to Platform and Platform to Weapon) a single integration activity (for each weapon type) should demonstrate most of the integration requirements for all other UAS following, given that the standards have been satisfied. This will go a long way in reducing both the time and cost for weaponising UAS. The operational capability of armed UAS will also broaden as additional nations integrate weapons on more existing and developmental UAS.

5. The proliferation of UAS technology has increased the prospect of hostile armed UAS being used against allied forces. Defending against armed UAS may preclude the use of friendly forces UAS in the same airspace if the countermeasures cannot discriminate friendly UAS. The challenge becomes more complex if each country or UAS implements the capability differently. Integrating the deployed systems in coalition operations provides a greater challenge. Cooperation by the allies in the development of armed UAS can provide much better opportunity for operational recognition of friendly UAS from hostile ones among allied forces.

1.1 BACKGROUND

1. Cooperation for current UAS is ongoing in NATO for Intelligence, Surveillance and Reconnaissance (ISR) standards, data links, ground control stations and UAS as systems. The quest for enhanced capability in UAS is paralleled by a desire for fewer proprietary interfaces, to simplify repairs, reduce manning, share acquisition costs and promote interchangeability of parts in the field. Without continued cooperation for the development of standards, more, rather than less, proprietary designs are likely options for procurement. Many will choose independent evolutions of "off the shelf systems" as the means to lessen developmental costs and schedule risks.

2. Armed UAS standards should be aligned with existing standards for UAS and manned aircraft. Weaponising unmanned systems is an added capability, similar to equipping an attack aircraft for reconnaissance or adding surface attack weapons to a maritime patrol aircraft. The addition of weapons presents challenges. In engineering terms, the challenges can be identified and met through the definition of nodal exchanges of data.

3. Several aspects of Unmanned Aircraft (UA) require changes to the assumptions made for arming manned aircraft. The most prominent is that, although there is a “man in the loop” there is no one located on the weapon launch vehicle who can initiate or acknowledge the decision to launch the weapon. Relevant information upon which to base decisions and actions must be relayed off board to the ground control station. Then the decisions and actions themselves must be relayed back to the UAS. It is expected that, as is the case with manned aircraft, due to current operational doctrine (i.e., Law of Armed Conflict and Rules of Engagement (ROE) constraints), fully automated weapons release by UAS on identified or self-detected targets is not expected, though elements of autonomy may play a role (e.g., adjustment of a release point based on existent winds in the target area). As a minimum, the capability for “man in the loop” to intervene and prevent weapon release will need to be maintained.

Another factor that is new for aviation ordnance on UAS is that the smallest UAS are much smaller than any manned aircraft, and may drive requirements for smaller physical interfaces and smaller 'smart' weapons than have been used on manned aircraft.

4. Today's cruise missiles and precision weapons can fly extended profiles to the target and in some cases can be reprogrammed in flight for options not even considered at launch. The doctrinal and operational issues associated with the remote control of weapons in these precision strike systems demonstrate that unmanned warhead employment can be accomplished and the operational mission development process can be replicated for an object that serves as a launch platform, that is remotely operated and that can be returned to an operating base.

1.2 PURPOSE

This document:

a. Identifies the expected impacts of using armed UAS in support of the joint coalition missions in lieu of and/or in conjunction with armed manned aircraft, including impacts on current operational doctrine; and

b. Defines an armed UAS architecture, safety requirements and the associated Information Exchange Requirements (IERs) to be implemented in implementing weapons on a UAS platform.

1.3 SCOPE

Although the operational and safety issues may apply to different weapon types (e.g., directed energy, kinetic energy, etc.), the focus of this document is only Air-to-Ground Kinetic Effects weapons.

INTENTIONALLY BLANK

CHAPTER 2 ARMED UAS CONSIDERATIONS

2.1. OVERVIEW

As illustrated in Figure 2-1, the major elements (e.g., stores management system and the weapon, including their respective interface standards) are the same or similar to the manned platform. In an unmanned system however, the human operator is remotely located and his functions must be implemented in one of the UA subsystems (e.g., ground station, data link, and stores management systems).

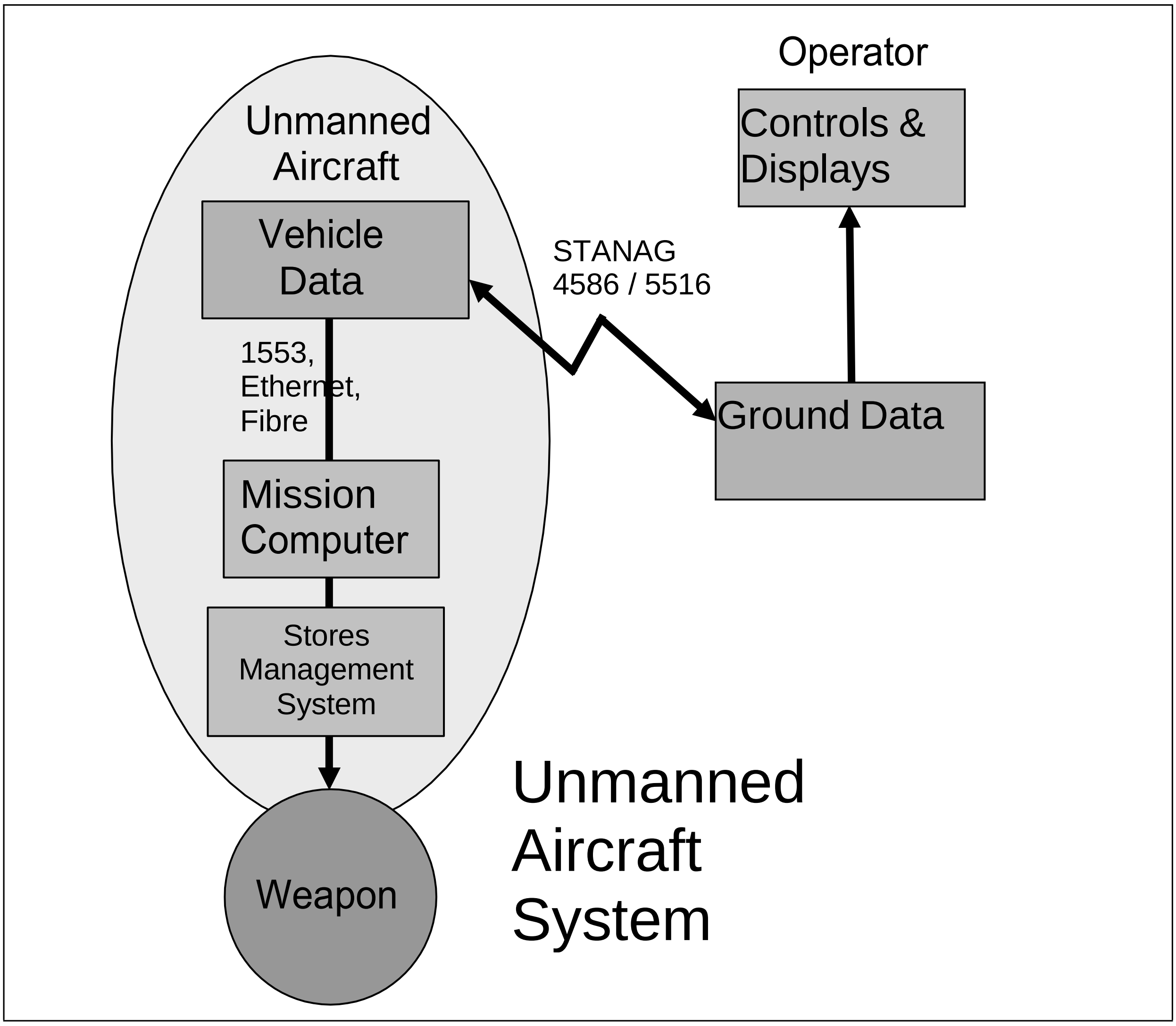


Figure 2-1: Weaponised Unmanned Platform Architecture

2.2 SYSTEM DESCRIPTION

The basic armed UAS includes the equipment required to perform a strike mission such as a Time Sensitive Target (TST) hunter-killer mission (i.e., aircraft with appropriate sensor and weapon suite, a control station, and the data link).

2.2.1 Stores Management on UA

It is assumed that the basic stores management system functions in a UAS will be the same as for manned aircraft. However, the arming/de-arming functions such as Master Arm Safety Switch (MASS), Late Arm, and Fire Button Press will be performed external to the UA by the ground crew for crew safety and/or by the Pilot/Operator at the UAS control system (UCS) and transmitted to the platform and weapon via some type of data link (Note: It is possible for the MASS to be applied by the launch crew prior to take-off). For the manned aircraft, the time interval between pressing the Fire Button and physical separation from the aircraft is system dependent and will range typically between 750 milliseconds and 4 seconds. This time interval is deemed achievable for UAS also.

2.2.2 Safety Considerations of Weapon Operation on UA

Basic manned aircraft safety considerations also apply for UAS. However, since the human is separated from the platform and weapon by data links, ground stations, and software, there is more potential for system failure within the kill chain. This creates new safety issues for which there is no strong or deep data history. These new issues are defined and addressed in Sections 3.3.3 thru 3.3.4.

2.2.3 Weapons on UA

Most, if not all, weapons utilized by manned aircraft can be utilized by UA, as a function of the payload carrying capability and release aerodynamics of the UA. It should be noted that the smaller UAS may limit their weapons (and the weapons' physical connections) to the smaller class of weapons.

2.3 JOINT CAMPAIGN/OPERATIONS STRUCTURE

UAS shall operate under the same NATO command structure and doctrine as that for manned aircraft as described in AEP-XXX, Guidelines for the Integration of Weapons on Unmanned Platforms.

2.4 JOINT TARGETING

UAS shall operate using the same Joint Targeting strategies, processes and doctrine as that for manned aircraft described in AEP-XXX, Guidelines for the Integration of Weapons on Unmanned Platforms.

2.5 WEAPON SYSTEM DOCTRINE

2.5.1 Concept of Employment

1. Armed UAS may be flown out of home bases for training as well as deployed to support forward operating locations. Modularity of the UAS may reduce the requirement to forward deploy all systems for the UAS. Control stations can be at any distance as long as beyond-line-of-sight connectivity is assured. Sorties could be launched to provide up to 24-hours/day and 7 day/week coverage of the Area of Responsibility (AOR). Loitering orbits can be anywhere in the AOR that can be supported by the effective range of the UAS in question. Regardless of the category of guided weapons, the platform must support physical, data and other technical interfaces to safely carry, initialize and release the weapon. The platform makes a critical contribution to a precision weapon’s ability to achieve design accuracy. Each type of weapon makes different demands on the UAS (aircraft, data link and control station) to support its effectiveness. Weapons commonly depend on the platform to transfer pre-launch power and initialization, coordinates for Global Positioning System (GPS) guidance, target feature data (or target class selection) for terminal seekers, and launch commands. Proper function of all munitions will depend on the platform to provide suitable initial-launch conditions. NATO’s Joint Air Power Competence Centre (JAPCC) has drafted the Strategic Concept of Employment for UAS in NATO dated 4 Jan 2010. This document details NATO’s vision for the operation, integration, and interoperability of UAS through 2025.

2. Armed UAS will have roles/missions similar to manned aircraft but will extend the role of Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) sensors from intelligence into operations, providing the ability to transition to prosecute the targets it detects when appropriate. Command and control through the Joint Theatre Forces Headquarters (JTFHQ), delegated to the Combined Air Operations Centre (CAOC) will enable armed UAS to integrate seamlessly the roles of intelligence collector, targeteer, and shooter. Long loiter times will provide extended target area coverage. As per manned aircraft, Command and Control will be exercised through the Combined Joint Forces Air Component Commander (JFACC) and the platforms will be de-conflicted using normal Air Tasking Order (ATO) and airspace control measures (ACM).

3. When acting in their role as ISTAR assets, armed UAS will detect targets from low, medium and high altitudes using highly sophisticated sensors to identify targets, and where necessary to geo-locate target coordinates accurately. When supporting strike assets are available, a UAS may perform as a scout or forward air controller (FAC), directing appropriate weapons employment using traditional FAC tactics, techniques, and procedures through digital J-Fire “9-lines,” tactical data links, secure voice, and other available links. The aircraft may be tasked to employ organic weapons when targets are time critical or of sufficient priority. To exploit the terminal guidance of Lock On Before Launch (LOBL) or autonomous weapons, armed UAS will coordinate imagery between UA ISTAR sensors and weapon seekers, to identify the proper target and aim point for the weapon, including illumination with a designating laser. With LOBL image-guided weapons, if required by TTPs, UAS downlink of weapon seeker imagery may be employed to verify proper weapon aim point (in some situations, manned aircraft could have “eyes on targets”. With UAS, this is not possible unless imagery data is accepted as equivalent to “eyes on target”).

4. The concept of employment of the armed UAS will follow the established path of tactical reconnaissance and time-critical targeting execution. When required, the mission crew may coordinate directly with airborne C2 and strike aircraft, providing verbal “talk-ons”, laser target marking and designation as required for strike support. The crew may also provide immediate or revisited post-strike assessment. Combat assessment from on-board sensors may be simultaneously broadcast to all echelons of command for further exploitation. Armed UAS may be able to provide below-the-weather support for strike aircraft operating above or vice versa. Armed UAS will also be able to independently attack UAS detected targets of opportunity within their designated engagement area. The combination of sensor and shooter in a single platform, coupled with high-speed, machine-level data links and appropriate C2, will provide for rapid capability to engage TSTs.

5. Future employment growth options include missions throughout the full spectrum of conflict. In low intensity conflicts like Military Operations in Urban Terrain (MOUT), they will leverage their long endurance loiter and sensors that provide persistent presence and intelligence collection, with weapons adding quick reaction attack capabilities in support of theatre commander objectives. These aircraft could also be employed for limited precision strikes in support of national or theatre objectives when directed as a show of force or retaliation. Finally, armed UAS will employ sensors and weapons in support of missions across the range of roles during medium- to high-intensity operations; particularly where their greater survivability and lack of on board pilot will give them greater freedom to attack heavily defended targets. Roles may also include both offensive and defensive counter-air with flights of aircraft flying in mutual support. In politically constrained conflicts, the video dissemination structure will permit timely decisions on the use of force by transmitting real time video and preliminary identification or validation of a target to appropriate levels of command with compatible signal reception equipment.

6. Regardless of the weapon type, special considerations may be given to developing procedures and mechanisms for the safe recovery of armed UAS (i.e., the automated or man-in-the-loop landing of UAS armed with live munitions).

2.6 ARCHITECTURE

1. Figure 2.6 illustrates the top level UAS architecture in terms of its components. Two primary subsystems of a UAS are the Unmanned Aircraft and the Control Station connected via a radio frequency (RF) data link. The operators control/interact systems operations via the control station. The C4I connectivity is provided via the external Command and Control Interface. The payloads including the external stores/weapons are integrated into the UA platform.

2. Weapon integration with its launch platform, controller and targeting source(s) falls into two distinct interfaces; the pre-launch interface and the post-launch interface. The pre-launch interface includes the real-time physical pre-launch connection between the weapon and its launch platform. That physical connection carries a logical connection to pass information between the weapon and its launch platform and through the launch platform to its pre-launch controller, nominally the UAS controller.

3. The physical connection must be suited to the size and weight of the weapon, the full spectrum of the UAS flight environment and weapon release environment, and must support the transfer of weapon launch signals and in most cases, pre-launch power, electrical discrete signals and digital data channels.

4. While the physical portion of the weapon interface terminates with the UA itself, the logical portion will need to be passed through the UAS control link, in order to reach the controller who makes the decision, and takes the action, to release the weapon.

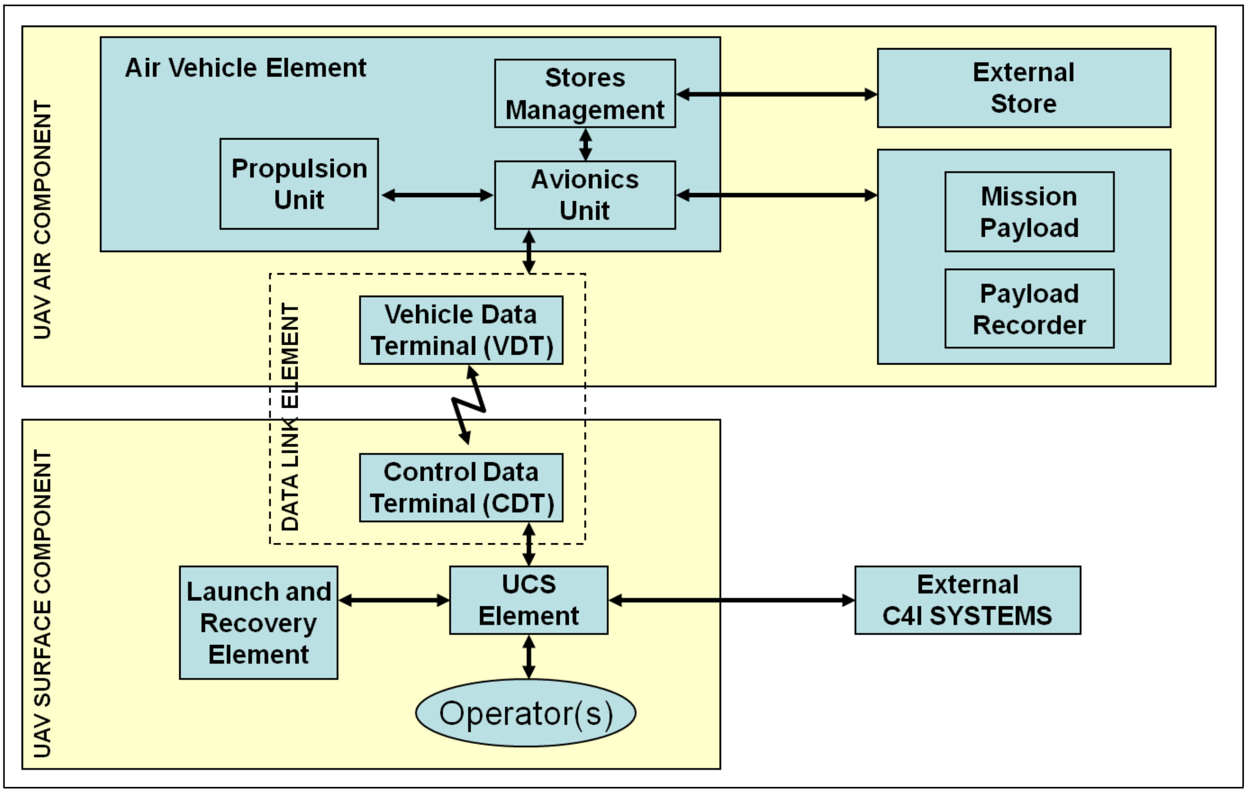


Figure 2-6: UAS Elements

5. Automated authority within the UAS to declare an object a target and employ a weapon against that object is considered beyond the scope of this initial architecture. It is assumed that, at least in the initial weaponised UAS, release of a weapon with intent to do harm will require the immediate decision and action of a human associated with the UAS mission authority. However, such a future capability would be expected to employ a subset of this architecture, simply by eliminating the UAS-to-ground station communication link and to "pre-authorize" the weapon release as part of the mission plan.

6. The pre-launch interface also includes the weapon "mission planning" interface; the pre-mission capability to use a workstation similar to that used to pre-plan the UAS mission. Some of the more advanced precision-guided munitions have sophisticated on-board systems that can be pre-loaded with mission data. This capability would most often be associated with interdiction and strike missions against fixed targets that have been committed to attack as a pre-planned element of the UAS mission. The product of mission planning is one or more digital data files that must be transferred to the weapon at some point prior to its release. Most often, this transfer is via the physical/logical interface between the weapon and its launch platform, as mentioned above. A file transfer path must be available between the weapon mission planning workstation and the weapon itself. Following the historical precedent of manned aviation, a common path would be an interface between the weapon mission planning software and the UAS mission planning software, through which weapon mission planning could be coordinated with that of the UAS, and the weapon mission file(s)

passed to the UA along with its own mission files. The UA would be programmed to pass weapon files to those weapons by means of the protocols and physical path of the weapon-to-platform interface.

7. There are at least two post-launch interfaces to weapons in use today; semi-active laser (SAL) seekers require the launch platform or a cooperative targeting source to aim a coded laser at the target. The term “semi-active” indicates that the laser designator has to emit radiation (laser) but the weapon remains passive, simply detecting the reflected energy. The reflected coded laser signal is detected by the weapon’s optical seeker, which guides the weapon to an intercept of the reflected laser signal. This capability may take advantage of a laser aboard the UA, but may also support other platforms that have laser target designators. In the latter case, coordination between the UAS and the off-board laser designator is required, to ensure that the weapon seeker is set to detect the code being used by that designator. While the code to be detected by early-generation laser-guided weapons is manually set by means of physical switches on the weapon, some later-generation weapons also have the capability to have their code and other seeker parameters updated through the logical portion of the weapon-to-platform interface. In the former case, once the UA is in the air, the weapon code is fixed. Coordination with the laser designator and the weapon, unless performed during mission planning prior to the UAS mission, requires that the weapon’s code be passed to the laser designator. In the latter case, coordination may also include the transfer of the designator’s code to the weapon at a time prior to weapon release from the UA.

8. The other form of post-launch interface is the RF data link. This typically requires that the weapon carry a transceiver by which it receives directions from its controller while in free flight toward its target, and transmits status and response messages back. There has been strong interest in this interface in recent years, with several weapon systems, launch platforms and targeting sources actively developing the capability. Collectively, this capability is known as Network Enabled Weapons (NEWs). NEWs use an existing digital data link, such as Link-16, or the Variable Message Format (VMF) of MIL-STD-6017 carried over a suitable ultra-high-frequency (UHF) radio waveform. The message set and its use have been defined in MIL-STD-6016 and STANAG 5516. NEW controllers and targeteers need the situational awareness to perform that tasking, and data link connectivity to the weapon. However, the only necessary impact of NEW capability upon the weaponisation of UAS is that the mission planning file(s) for the NEWs, and real-time update of weapon missions over the logical portion of the pre-launch interface, must include the ability to transfer the network communication parameters for the NEW itself and its correspondents, including initial or current controller, alternate controller, and third-party targeting sources.

9. Annex 2 contains a set of Information Exchange Requirements which were derived from the NIAG-125 study. These represent a top level characterisation of the type of information that passes among known nodes within the assumed architecture for armed UAS.

2.6.1 Hardware/Electrical Standard Interfaces – Weapon-to-Platform

The hardware/electrical interface between weapon and platform must be consistent with weapon hardware and electrical requirements. The interface between the weapon and platform shall be the same for manned platforms and UAS.

2.6.2 Messaging Standards – Weapon-to-Platform

The logical and messaging interface between weapon and platform must be consistent with weapon message. The interface between the weapon and platform shall be the same for manned platforms and UAS.

2.6.3 Messaging Standards – UCS-to-Platform

1. For UAS, the UCS is physically separated from the UAS platform. In most cases the UCS is located on the ground, or surface (though in some instances control can be exercised from a separate airborne asset). Because of this physical separation (as shown in Figure 2-6) all communications (command, control, status, etc.) must be transmitted via an RF data link.

2. The following standards are applicable but are not sufficient to support weapons payload integration into a UAS:

a. ADatP-3

b. CRD

c. Mil-Std 3014

d. STANAG 4586

2.6.4 Information Exchange Requirements for Weapons Integration

1. The methodology adopted for the UAS weaponisation is aimed at developing the list of IERs required to control stores carried on and released from a UAS. The UAS designer has a number of architecture options that can be considered; the actual system architecture chosen depending on factors such as:

a. UAS mission requirements;

b. Aircraft size;

c. System complexity needs;

d. Level of autonomy required.

2. A real weaponised UAS architecture would be realised by allocating each internal domain of the UAS Weaponisation Domain Model to the system nodes depicted in Figure 2-10. This means that the actual IERs needed will also depend on the

UAS architecture and the distribution of nodes within the system. The UAS weaponisation study has identified three architecture levels resulting from allocating the UAS weaponisation system domains to the nodes as follows:

a. Level 1 Capability UA: The UA Element provides Stores Control and Pre Launch Store Control functionality. All other functionality (Stores Management, Fire Control, etc.) is provided by the UCS Element;

b. Level 2 Capability UA: The same as Level 1 except the UA Element also provides Stores Management functionality instead of the UCS Element; and

c. Level 3 Capability UA: The same as Level 2 except the UA Element also provides Fire Control functionality instead of the UCS Element.

3. The three capability levels are depicted in Figures 2-7 to 2-9 with the UA elements shown in the shaded boxes. The point at which the IERs are expressed is also shown on each figure by a bold horizontal line. It is clear therefore that different IERs can exist over the Data Link Interface (DLI) between the UCS and UA. However the IERs do not change between the UAS and external systems and actors, regardless of the capability level.

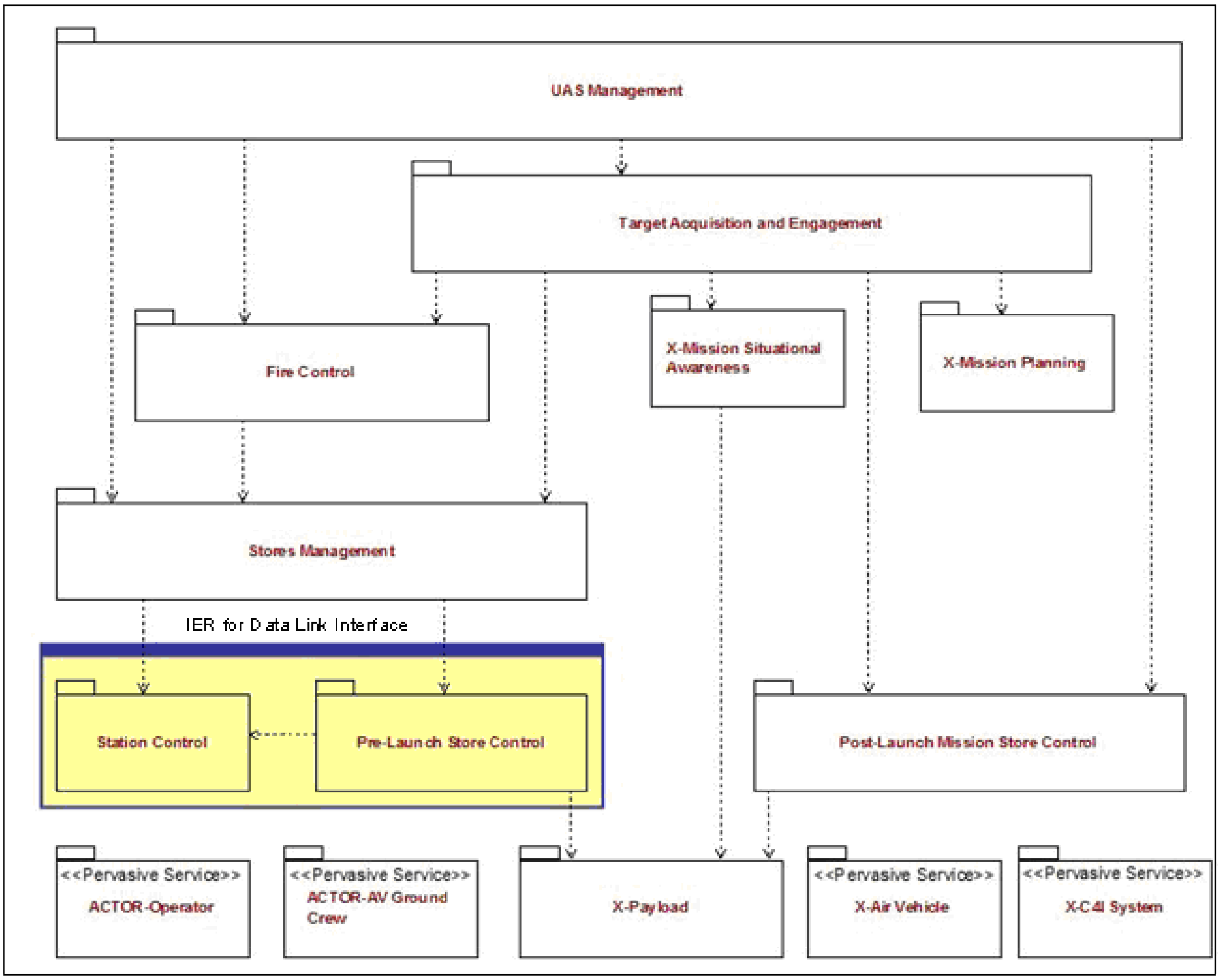


Figure 2-7: Level 1 Capability UA

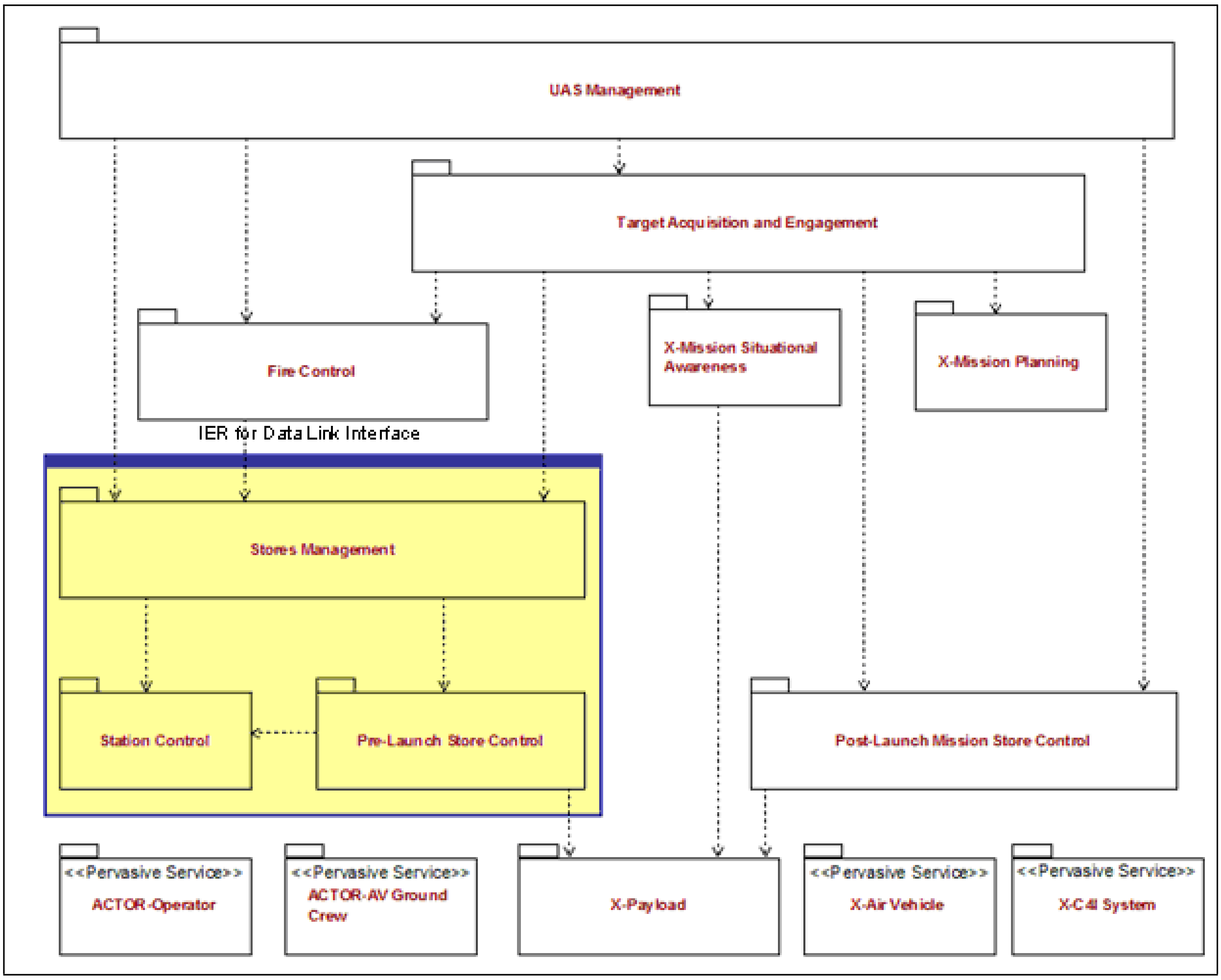


Figure 2-8: Level 2 Capability UA

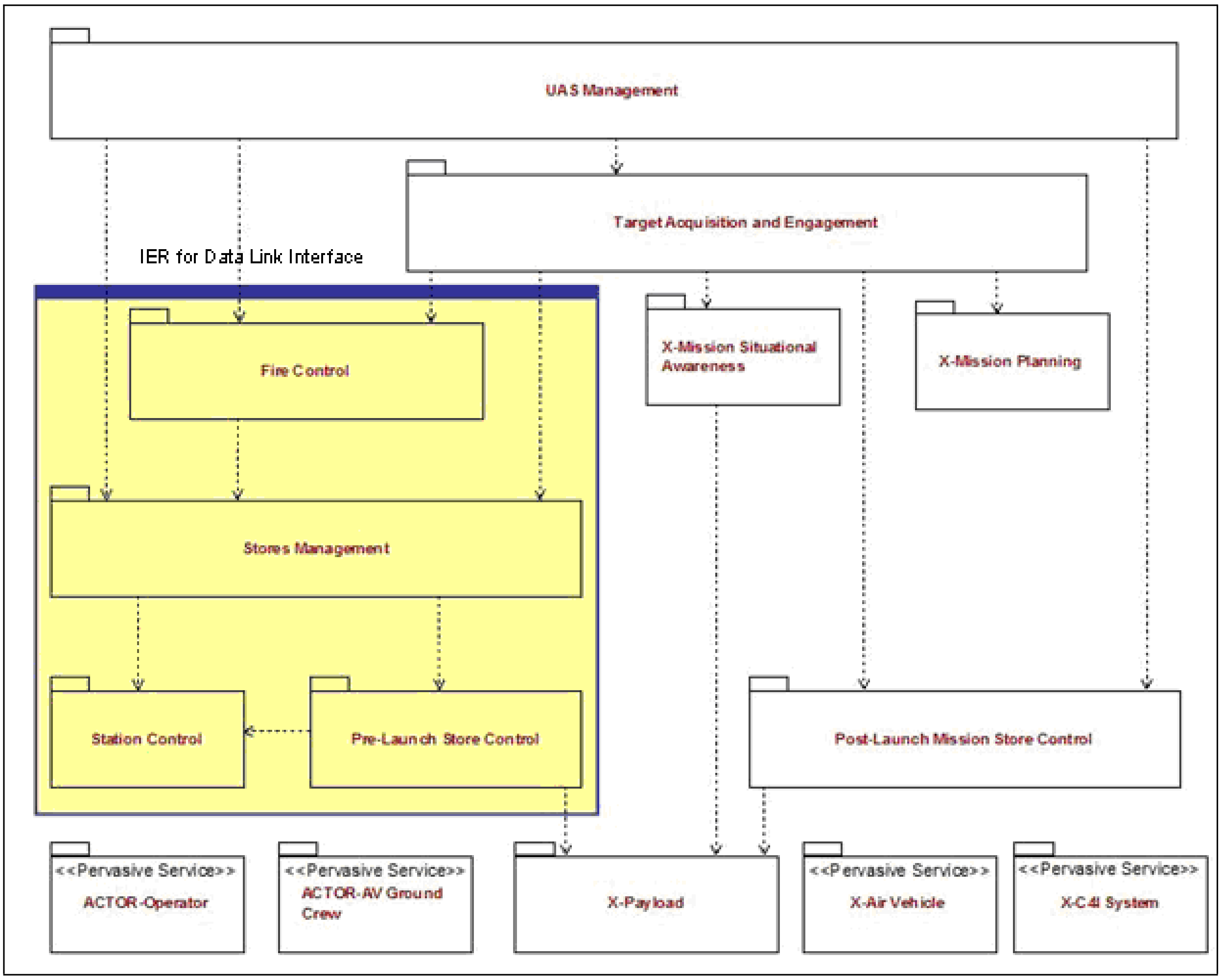


Figure 2-9: Level 3 Capability UA

2.6.4.1 Inter-Node Information Exchange Requirements

1. This section provides the IERs between the system nodes identified in Figure 2-10. The IERs apply to these interfaces:

a. The C4I Interface Element;

b. The Data Link Element;

c. The Payload Interface Element. This is included for completeness, as there should be no differences between manned and UA with respect to the payload interface.

2. Post launch mission store control is not addressed here.

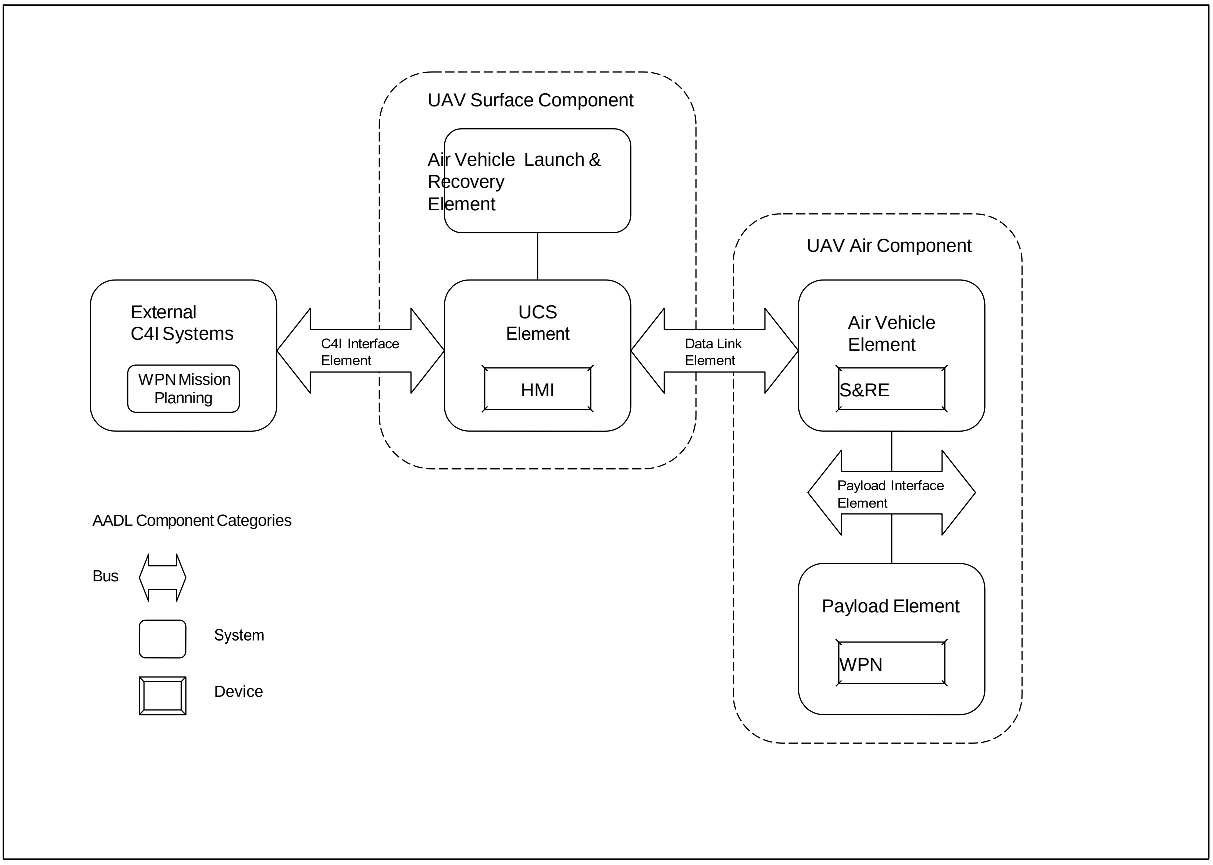


Figure 2-10: UAS Weaponisation System Nodes and Interfaces

3. The intent of these IERs is to provide a definition of the logical information that is passed between the control station and the UA over the DLI. Because these IERs are intended to be implementation independent, and therefore applicable to the widest range of systems, many traditional attributes of an IER (e.g., latency, accuracy) are not included.

Note: To understand the sequencing of these messages for specific functions, refer to the Unified Modelling Language (UML) Sequence Diagrams associated with the relevant Use Cases in the NIAG SG125 report.

2.6.4.2 C4I Interface

1. The external C4I system is responsible for the provision of the overall infrastructure in order to allow weapon mission tasking, the collection and compilation of targeting information and the evaluation, merging and dissemination of the mission report. The data is also provided to the common operational picture. The interface to this operator is defined in other standards such as ISR services (e.g., targeting data as a result of UAS sensor operation) and as defined in STANAG 4586. In the weaponised UAS architecture, the external C4I system interacts with the UAS management domain. It receives confirmation that the mission plan has been accepted by the UAS Management Domain, and after the mission receives the mission report for further action.

2. The external Mission Planning Domain generates the mission plan including route, weather, no fly zones, electronic order of battlefield, communication plan, fire control mission plan, stores management mission plan, UAS configuration information and weapon mission planning and distributes it to the UAS Management Domain. Mission planning can happen at any time before and during the mission as mission updates are also considered as mission planning.

3. Mission Planning data exchange can be considered at 3 levels:

a. Simple level: Exchange of ADatP-3 Type (ATO and/or TGT location);

b. Standardised level: Exchange of Mission Plan using the US/UK Interface specification: Common Route Definition (CRD);

c. Complete level: Reception of Full Mission Plan, specific to each UAS/ weapon.

4. Mission situational awareness captures data relevant for the representation of the mission (mission plan information such as route, no fly zones, targeting data, LAR, target position, sensor data, mission results, weather, etc.) to the operator and the local commander or other decision makers.

2.6.4.3 Data Link Interface

1. The UAS may provide different services across the DLI. The services are:

a. Fire Control and Store Management Service (Capability Level 3);

b. Stores Management Service (Capability Level 2);

c. Pre-Launch Store Control and Station Control services (Capability Level 1).

2. The IERs for each service are set out in Annex B.

2.6.4.4 Payload Interface

1. The detailed definition of the IERs between a payload and the UAS is defined in the respective weapon to platform Interface Control Document (ICD). Annex B contains a list of typical IER groups as derived from the Level 3 use cases identified in the NIAG-125 study report.

2. Although the individual IERs for any interface are often specific to aircraft-payload combination, there is an increase in the use of standardised interfaces for certain payload classes. It is anticipated that the NATO Universal Armament Interface, based on MIL-STD-1760, will be adopted by many aircraft and weapon systems.

3. For weapons and mission planning systems that use the same ICD to transfer data, the UAS shall transfer that data to the weapon over the data link without modification.

CHAPTER 3 WEAPON SAFETY CONSIDERATIONS

3.1 UAS WEAPONISATION SAFETY

1. This section addresses the system safety and airworthiness aspects of weaponising a UAS. These requirements are based on NATO, and available national system safety and airworthiness documents for manned aircraft. Analysis of these documents led to the formation of a general set of safety precepts, top level mishaps, and system safety and airworthiness objectives for weaponising a UAS. From this set of general requirements, a set of specific requirements is derived. The derived requirements address:

a. Availability (system liveness);

b. Information Assurance (IA);

c. Method of Control;

d. Human Computer Interface (HCI) Requirements;

e. Hand-Off;

f. Certification considerations.

2. Precedence is given to the latest versions of STANAG 4671, 4702 and 4703 respectively, for design considerations and for developing a basis for Air Worthiness certification. Further regulation from national authorities shall be considered as they are developed.

3. The UAS domain model, architecture and Information Exchange Requirements that are the subject of this system safety and airworthiness analysis are as above. The safety critical domains are: Stores Management, Station Control, Pre-Launch Store Control, UAS Management Domain and associated Human-Computer Interface (HCI).

3.1.1 General

The scope of this analysis is limited to system considerations and technical standards vice operational considerations. It is recognized that safety and airworthiness issues can be decomposed into both technical and operational aspects. For the purposes of this discussion, only those operational issues that have direct technical implications are considered. As such, the following are outside the scope of this document and will require separate review:

a. Training:

(1) Operator qualifications & training doctrine (e.g., STANAG 4670);

(2) Checklists and operation manual considerations;

(3) Tactics, Techniques and Procedures (TTP);

b. Rules of Engagement (ROE):

(1) Definition of operating environment;

(2) Probability of collateral damage;

c. Policies and procedures related to loss of control and mitigation;

d. Templates for different operations (e.g., Close Air Support (CAS));

e. Human Factor Interfaces;

f. Occupational Health and Safety for personnel;

g. Maintenance policies for personnel;

h. Impact that a weaponised UAS will have for Flight in Non-Segregated Airspace (FINAS).

3.1.1.1 Definitions

In addressing UAS weaponisation safety, these definitions of system safety and airworthiness apply:

a. System Safety – The application of engineering and management principles, criteria and techniques to achieve acceptable mishap risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system life cycle.

b. Airworthiness - The ability of an aircraft or other airborne equipment or system to operate without significant hazard to aircrew, ground crew, passengers (where relevant) or to the general public over which such airborne systems are flown.

3.1.2 System Safety

1. There is no agreed system safety standard across NATO, and currently each nation must use its own. As a result of its wide usage and familiarity and in order to arrive at a common lexicon and set of safety objectives for this document, MIL-STD-882D was selected as the top level standard for system safety.

2. Where applicable, MIL-STD-882 shall be supplemented by STANAG 4671, 4702 and 4703 as applicable. This includes the tolerable mishap risk for a UAS.

3. It is noted that STANAG 4671 references these non-government standards:

a. SAE ARP 4761 – Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment;

b. RTCA/DO-178B – Software Considerations in Airborne Systems and Equipment Certification, 26 March 1999;

c. RTCA/DO-254 – Design Assurance Guidance for Airborne Electronic Hardware, 19 April 2000;

d. RTCA/DO-297 – Modular Avionics (IMA) Development Guidance and Certification Considerations;

e. RTCA/DO-304 – Guidance Material and Considerations for UAS, 22 March 2007;

f. RTCA/DO-278 – Guidelines for Communications, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance, 5 March 2002.

4. STANAG 4404, Safety Design Requirements and Guidelines for Munitions Related Safety Critical Computing Systems, though not ratified, should also be considered.

3.1.2.1 Safety Related NATO Standards

1. There is no agreed system safety standard across NATO, and currently each nation must use its own. In order to arrive at a common lexicon and set of safety objectives for this document, MIL-STD-882D was selected as the top level standard for system safety, which was chosen because of its wide familiarity.

2. Compliance with specific national safety requirements and the resultant certification process is performed in accordance with each nation's policies and procedures.

3. The responsible committee in NATO for establishing a common baseline for the safety and suitability for service of munitions and explosives is AC/310. The glossary of specialized terms and definitions concerning the safety and suitability for service of munitions, explosives and related products is Allied Ordnance Publication (AOP) 38.

4. NATO safety standards for air-launched weapons and fuses are listed below (Tables 3-1 and 3-2) and shall be utilized in integrating weapons on UAS platforms. Additional more specialized standards apply to environmental safety requirements, and to the composition, transportation and exchange of energetic materials.

STANAG Number	Title	Dated	Notes/Summary of content
3786 Ed4	Safety Design Requirements for Airborne Dispenser Weapons	18/12/96	States the areas that must be taken into account in the design of Airborne Dispenser Weapons and associated sub-munitions excluding chaff and flare dispenser systems.
4297 Ed2 and AOP15 Ed2	Guidance on the Assessment of the Safety and Suitability for Service of Munitions for NATO Armed Forces	16/2/01 and 1/11/98	Provides a uniform guide to achieving a positive assessment that munitions are safe and suitable for use by NATO forces. Recommends system safety design and development criteria. Provides a methodology for assessing and documenting munitions safety.
4325 Ed1	Environmental and Safety Tests for the Appraisal of air Launched Munitions	18/5/92	Identifies what tests need to be carried out to provide evidence that air launched munitions are safe and suitable for service. The procedures and sequences for conducting the tests are given and test criteria are summarized.
4432 Ed1	Air Launched Guided Munitions, Principles for Safe Design	24/1/00	States the areas that must be taken into account in the design of air launched munitions including the explosives, propulsion systems using energetic substances, compatibility of materials fuses and safe jettison arrangements.
4439 Ed1 and AOP39 Ed1	Policy for Introduction, Assessment and Testing for Insensitive Munitions. Insensitive Munitions Requirements for Assessment Testing and Evaluation (MURAT)	18/11/98 and 18/11/98	States the NATO agreement for the introduction of Insensitive Munitions (IM) and lists the IM requirements, goals and tests. Provides guidance and direction to enable the policy and requirements specified in STANAG 4439 for the development, assessment and testing of Insensitive Munitions to be implemented.

STANAG Number	Title	Dated	Notes/Summary of content
4518 Ed1	Safe Disposal of Munitions, Design Principles and Requirements, and Safety Assessment.	8/10/01	Specifies the policies and principles to be adopted for the demilitarization and disposal of munitions in a safe, cost effective, practicable and environmentally responsible manner.
4519 Ed1	Gas Generators, Design Safety Requirements and Safety and Suitability for Service Evaluation	1/3/00	Identifies the essential safety characteristics to be included in the design of gas generators and specifies test requires to establish safety and suitability for service.

Table 3-1: General Policies for Assessment of Safety & Suitability of Service

STANAG Number	Title	Dated
4157 Ed 1	Development of Safety Test Methods and Procedures for Fuzes for Unguided Tube Launched Projectiles	Aug 1991
4187 Ed 1 with AOP16 Ed 3	Fuzing Systems - Safety Design Requirements Fuzing Systems Design Guidelines for STANAG 4187	Oct 1996 Oct 1999
4368 Ed 1	Electric and Laser Ignition System for Rockets and Guided Missile Motors: Safety Design requirements	Feb 1998

Table 3-2: Fusing Systems and Other Initiating Systems

3.2 Summary of Safety and Airworthiness Objectives

Based on the inputs assessed above, the recommended UAS weaponisation safety and airworthiness requirements are:

a. Achievement of low or, if unavoidable, medium mishap risk as defined in STANAG 4671 Section F, requirement AMC 1309-3 (Section 3.3.);

b. The principal mishaps (failure conditions) to be considered are the Top Level Mishaps (TLM) defined in the Unmanned Systems Safety Guide for DoD Acquisition, 27 June 2007 (Section 3.3.1);

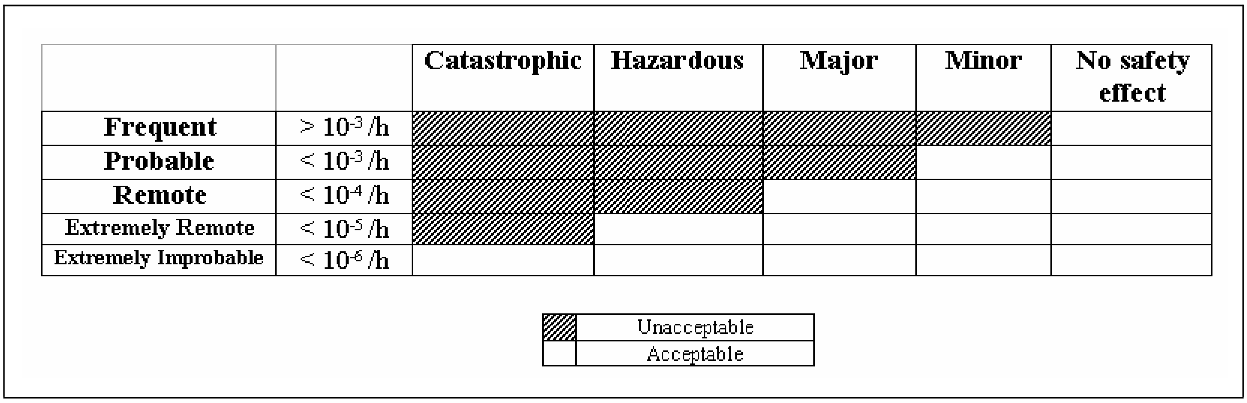
c. The UAS architecture shall support the Operational Safety Precepts and Design Safety Precepts defined in the Unmanned Systems Safety Guide for DoD Acquisition, 27 June 2007 (Section 3.3.2);

d. Compliance with latest NATO STANAGs 4671, 4702, 4703;

e. Compliance with STANAG 4404 Edition 1 Draft (Safety Design Requirements and Guidelines for Munitions Related Safety Critical Computing Systems).

3.3 Tolerable Mishap Risk

1. A weaponised UAS shall have an acceptable mishap risk as defined in STANAG 4671, 4702 and 4703 as applicable. For example in STANAG 4671 Section F, the acceptable mishap risk is presented in Table 3-3 and is based on the severity reference system detailed at the end of this section. For systems and equipment used only in certain phases of flight (e.g., weapon delivery), a probability reference of “per flight” instead of “per flight hour” may be used at the discretion of the Certifying Authority (see FAR AC23.1309-1C).



		Catastrophic	Hazardous	Major	Minor	No safety effect
Frequent	> 10^{-3} /h	▨	▨	▨	▨	
Probable	< 10^{-3} /h	▨	▨	▨		
Remote	< 10^{-4} /h	▨	▨			
Extremely Remote	< 10^{-5} /h	▨				
Extremely Improbable	< 10^{-6} /h					

▨	Unacceptable
□	Acceptable

Table 3-3: Acceptable Mishap Risk Matrix

2. This matrix applies to each individual failure condition (mishap) of each subsystem forming the UAS, such as the Stores Management System. Where, exceptionally, the current state of the art does not permit the attainment of the individual objectives stated above, it should be shown that (1) at the UAS level, the combination of all Catastrophic failure conditions is characterized by an occurrence of 10^{-5} per flight hour or less (with the calculation method subject to Certifying Authority agreement), and (2) the design and construction utilize well-proven methods.

3. Where the technology and architecture used do not permit the attainment of the objectives stated above, the UAS type certification should be dealt with on a case by case basis, subject to the Certifying Authority agreement, either through operational restrictions or through a rationale justifying lesser value (e.g., considering UA weight or/and kinetic energy at impact) based upon the risk to third parties.

4. The severity reference system applicable to Table 3-3 is as follows:

a. **Catastrophic:** Failure conditions that (1) result in a worst credible outcome of at least uncontrolled flight (including flight outside of pre-planned or contingency flight profiles/areas) and/or uncontrolled crash, which can potentially result in a fatality, or (2) could potentially result in a fatality to crew or ground staff.

b. **Hazardous:** Failure conditions that (1) either by themselves or in conjunction with increased crew workload, result in a worst credible outcome of a controlled-trajectory termination or forced landing potentially leading to the loss of the UA where it can be reasonably expected that a fatality will not occur, or (2) could potentially result in serious injury to UAS crew or ground staff.

c. **Major:** Failure conditions that (1) either by themselves or in conjunction with increased crew workload, result in a worst credible outcome of an emergency landing of the UA on a predefined site where it can be reasonably expected that a serious injury will not occur, or (2) could potentially result in injury to UAS crew or ground staff.

d. **Minor:** Failure conditions that do not significantly reduce UAS safety and involve UAS crew actions that is well within their capabilities. These conditions may include a slight reduction in safety margins or functional capabilities, and a slight increase in UAS crew workload.

e. **No Safety Effect:** Failure conditions that have no effect on safety.

3.3.1 Top Level Mishaps

1. The principal mishaps (failure conditions) to be considered for the UAS are the Top Level Mishaps (TLM) defined in the Unmanned Systems Safety Guide for DoD Acquisition, 27 June 2007. TLM provide a design safety focal point and help highlight and track major safety concerns. They are:

a. TLM-1 Unintended or abnormal system mobility operation

b. TLM-2 Inadvertent firing or release of weapons

c. TLM-3 Engagement or firing upon unintended targets

d. TLM-4 Self-damage of own system from weapon fire/release

e. TLM-5 Personnel injury

f. TLM-6 Equipment damage

g. TLM-7 Environmental damage

h. TLM-8 Aircraft loss

i. TLM-9 Aircraft collision

2. The severity of each TLM can depend on the nature of the mishap, the systems involved and the concept of employment. However, as a general rule, these TLM have

the potential of being Catastrophic.

3. The TLM are allocated to typical UAS mission phases as detailed in Table 3-4. The notional mission phases were developed and used in the study performed by NIAG Subgroup 72 (Aircraft, Launcher and Weapon Interoperability Study 2). Broadly stated, it can be seen that in the mission planning phase the primary concern is TLM-3. During the logistics handling phases and weapon loading/unloading phases the principal mishaps are TLM-2, TLM-5, TLM-6, TLM-7 and TLM-8. In the flight phases, in which the UAS Stores Management System is powered, the principal mishaps are TLM-2, TLM-3 and TLM-4, plus possibly TLM-1 and TLM-9 if the Suspension & Release Equipment (S&RE) and weapons are capable of introducing the required hazards when improperly released.

4. As a result of this, the focus for the UAS can be summarized to:

a. The integrity of mission data;

b. Adequate use of interlocks and power-down procedures during ground operations;

c. Achievement of acceptable risk for TLM-2, TLM-3 and TLM-4 during flight.

5. The relevant safety precepts identified in Table 3-5 are addressed in Section 3.3.2.

Mission Phase	Mishap Risk	Safety Precepts
ATO production	TLM-3: Engagement/firing upon unintended targets	OSP-1; DSP-1
Sortie mission planning	TLM-3: Engagement/firing upon unintended targets	OSP-1; DSP-1, 3
Weapon mission planning (deliberate targeting)	TLM-3: Engagement/firing upon unintended targets	OSP-1; DSP-1, 3
Logistics handling of energetic materials (weapon, fuse, ejection devices)	TLM-5: Personnel injury TLM-6: Equipment damage TLM-7: Environmental damage	OSP-1; DSP-1
Logistics handling of unarmed UAS	TLM-5: Personnel injury TLM-6: Equipment damage TLM-8: Aircraft loss	OSP-1; DSP-1
Weapon loading; setting system to hot	TLM-2: Inadvertent firing or release of weapons TLM-5: Personnel injury	OSP-1, 2, 3; DSP-1, 2, 3, 4, 6, 7, 8, 14
Activities leading to take-off/launch	TLM-2: Inadvertent firing or release of weapons	OSP-1, 4; DSP-1, 2, 3, 4, 6, 7, 8, 14
Transit of UAS to target area	TLM-2: Inadvertent firing or release of weapons	OSP-1, 2, 4; DSP-1, 2, 3, 4, 6, 7, 8, 14
Dynamic targeting (except engagement)	TLM-2: Inadvertent firing or release of weapons TLM-3: Engagement/firing upon unintended targets	OSP-1, 2, 4; DSP-1, 2, 3, 4, 6, 7, 8, 14
Engagement	TLM-1: Unintended/abnormal system mobility operation TLM-3: Engagement/firing upon unintended targets TLM-4: Self-damage of own system from weapon fire/release TLM-9: Aircraft collision	OSP-1, 2, 3; DSP-1, 2, 3, 4, 5, 6, 7, 8, 14, 15
Transit of UAS to landing/recovery point	TLM-2: Inadvertent firing or release of weapons	OSP-1, 2, 4; DSP-1, 2, 3, 4, 6, 7, 8, 14

Mission Phase	Mishap Risk	Safety Precepts
Landing/recovery	TLM-2: Inadvertent firing or release of weapons	OSP-1, 2, 4; DSP-1, 2, 3, 4, 6, 7, 8, 14
Safing of UAS; unloading weapons	TLM-2: Inadvertent firing or release of weapons TLM-5: Personnel injury	OSP-1, 2, 4; DSP-1, 2, 3, 4, 6, 7, 8, 14

Table 3-4: Lifecycle Mishap Identification

3.3.2 Safety Precepts

A safety precept is a basic truth, law or presumption intended to influence operational and design activities but not dictate specific solutions. The weaponised UAS shall support the Operational Safety Precepts and Design Safety Precepts defined in the Unmanned Systems Safety Guide for DoD Acquisition, 27 June 2007. These safety precepts are listed in Table 3-5. The derived requirements are addressed in Section 3.3.3.

Safety Precepts	Derived Requirements
OSP-1: The controlling entity (or entities) of the unmanned system should have adequate mission information to support safe operations;	3.3.3.4
OSP-2: The UAS shall be considered unsafe until a safe state can be verified;	3.3.3.6.3.1, 3.3.3.6.3.2
OSP-3: The authorized entity (or entities) of the unmanned system shall verify the state of the unmanned system, to ensure a safe state prior to performing any operations or tasks;	3.3.3.6.3.2, 3.3.3.6.3.3
OSP-4: The unmanned system weapons should be loaded and/or energized as late as possible in the operational sequence;	3.3.3.4.2 3.3.3.5
OSP-5: Only authorized, qualified and trained personnel with the commensurate skills and expertise, using authorized procedures, shall operate or maintain the unmanned system;	No derived requirements
DSP-1: The UAS shall be designed to minimize the mishap risk during all life cycle phases;	3.3.3
DSP-2: The UAS shall be designed to only respond to fulfill valid commands from the authorized entity (or entities);	3.3.3.2
DSP-3: The UAS shall be designed to provide information, intelligence, and method of control (I2C) to support safe operations;	3.3.3.3

Safety Precepts	Derived Requirements
DSP-4: The UAS shall be designed to isolate power until as late in the operational sequence as practical for items such as: a) weapons, b) rocket motor initiation circuits, c) bomb release racks, or d) propulsion systems;	3.3.3.3
DSP-5: The UAS shall be designed to prevent release and/or firing of weapons into the unmanned systems structure or other weapons;	3.3.3.3.1.4
DSP-6: The UAS shall be designed to prevent uncommanded fire and/or release of weapons or propagation and/or radiation of hazardous energy;	3.3.3.4.2
DSP-7: The UAS shall be designed to safely initialize in the intended state, safety and verifiably change modes and states, and preventing hazardous system mode combinations or transitions;	3.3.3.3
DSP-8: The UAS shall be designed to provide for an authorized entity (or entities) to abort operations and return the system to a safe state, if possible;	3.3.3.3
DSP-9: Safety critical software for the UAS design shall only include required and intended functionality;	3.3.5
DSP-10: The UAS shall be designed to minimize single-point, common mode or common cause failures that result in high and/or serious risks;	3.3.5
DSP-11: The UAS shall be designed to minimize the use of hazardous materials;	No derived requirements
DSP-12: The UAS shall be designed to minimize exposure of personnel, ordnance, and equipment to hazards generated by the UAS equipment;	No derived requirements
DSP-13: The UAS shall be designed to identify to the authorized entity (or entities) the weapon being released or fired, but prior to weapon release or fire;	3.3.3.6.3.3
DSP-14: In the event of unexpected loss or corruption of command link, the UAS shall transition to a pre-determined and expected state and mode;	3.3.3.3
DSP-15: The firing of weapons systems shall require a minimum of two independent and unique validated messages in the proper sequence from the authorized entity (or entities) each of which shall be generated as a consequence of separate authorized entity action. Both messages should not originate within the UAS launching platform;	3.3.3.2
DSP-16: The UAS shall be designed to provide contingencies in the event of safety critical failures or emergencies involving the UAS;	3.3.3.3.1.1 3.3.3.3.1.3
DSP-17: The UAS shall be designed to ensure safe recovery of the UAS;	3.3.3.3

Safety Precepts	Derived Requirements
DSP-18: The UAS shall ensure compatibility with the test range environment to provide safety during test and evaluation;	No derived requirements
DSP-19: The UAS shall be designed to safely operate within combined and joint operational environments;	3.3.3.2

Table 3-5: Safety Precept – Section Mapping

3.3.3 Derived Requirements

The requirements below address system availability, information assurance, method of control, the human-computer interface, hand-off, and certification. This material complements and extends the safety discussion presented in the NIAG Subgroup 125 Report, UAS Weaponisation.

3.3.3.1 Availability (System Liveness)

1. Analysis of the TLM, OSP and DSP suggests that there is no 'liveness' or continuous availability requirement for the UAS weaponisation system. That is, in all mission phases, the UAS can revert to a 'fail safe' condition. This assumes there is no 'liveness' requirement for Emergency Jettison (EJ) on the UAS as would usually be the case on manned aircraft. As a consequence of this, it is concluded that a single channel architecture is acceptable.

2. In a UAS, the term All Jettison (AJ) has sometimes been used to distinguish the function from EJ.

3.3.3.2 Information Assurance/Message Integrity

1. There is an Information Assurance (IA) requirement for the communication path between the controlling entity (or entities) and the UAS. The IA requirement is implied by the safety precepts as defined in Table 3-5.

2. In addition, the weaponised UAS design must be robust enough, but not over-engineered, to ensure that the SMS cannot be made "live" through spurious or malicious interference of the data-link controlled Late Arm/Master Arm in the presence of the following types of threats/risks:

a. External Interference

(1) Electro Magnetic Pulse (EMP)

(2) Jamming

(3) Simultaneous transmission

(4) Deliberate attempt to transmit spurious fire signal

b. Internal Interference

(1) System noise

(2) Cross-talk

c. Loss of synchronization

d. Corruption of message

3. Deliberate or malicious intervention by an aggressor to either interrupt or corrupt the signal, or attempt to transmit their own spurious fire signal, given the high degree of standardization in respect of message protocols, will merit specific consideration.

4. In the US, DoD IA controls shall be based on DoDI 8500.2, Information Assurance (IA) Implementation. It is anticipated that the objective IA level to satisfy DSP-2, DSP-15 and DSP-19 is Mission Assurance Category (MAC) 1, Classified.

5. DoD controls align with these US government unified controls:

a. NIST SP 800-53 – Recommended Security Controls for Federal Information Systems and Organizations (Revision 3)]

b. CNSSI 1253 – Security Control Catalog for National Security Systems, Oct 2009

6. Under these unified controls the objective IA level to comply with DSP-2, DSP- 15 and DSP-19 is anticipated to be:

c. Confidentially-high

d. Integrity-high

e. Availability-moderate

f. Mission criticality-high

3.3.3.3 Method of Control

1. The UAS is required to have multiple system states associated with discrete levels of control authority over weapons and S&RE. This requirement is implied by the safety precepts as defined in Table 3-3.

2. The system states and state transitions proposed for the UAS safety-critical domains are set out in the NIAG SG125 final report.

3.3.3.3.1 Stores Management Domain Safety Considerations

1. The Stores Management (SM) Domain state diagram below (Figure 3-1) shows state transitions and IER related triggers. System safety considerations require the Stores Management Domain to transition between states based on internal triggers also.

2. Internal triggers to transition from Stores Management Weapon System Live to Weapon System Active might include the following:

a. Lost Link Policy

b. Corridor/ Exclusion Zones

c. Link Recovery Manoeuver

d. Excursion From Safe Flight Envelope/ Safety Indicators

e. System Health

f. Authorized Controlling Entity

g. Data Validity

h. Take-Off and Landing

3.3.3.3.1.1 Lost Link Policy

1. In general, a lost link is considered undesirable from a safety perspective; however mission effectiveness may require the system to work through temporary lost links or to engage targets in denied communication situations. Therefore, it is recognized that each UAS may require a system or mission unique lost link policy.

2. Policy could be defined in mission planning (for mission), configured by data (e.g., UAI-type configuration data) or fixed in the code, or a combination of the above. Suppression of Enemy Air Defenses missions may result in lost link.

3.3.3.3.1.2 Corridor/Exclusion Zones

Different zones can apply. Here we could define a weapon engagement corridor/zone outside which the Stores Management cannot be live. The Launch Acceptability Region would be inside this zone. Included here are space and time constraints.

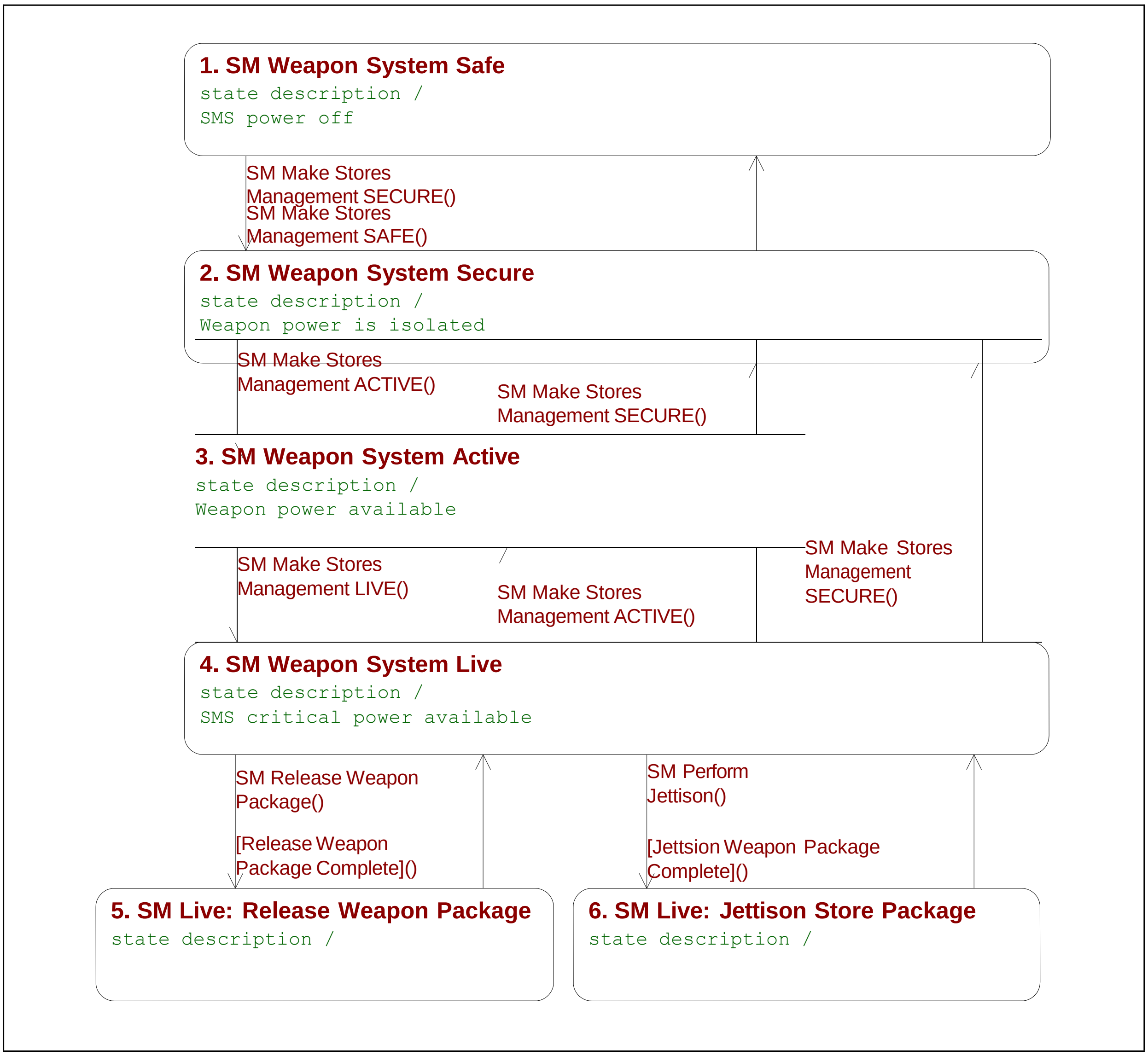

1. SM Weapon System Safe
state description /
SMS power off
SM Make Stores Management SECURE()
SM Make Stores Management SAFE()
2. SM Weapon System Secure
state description /
Weapon power is isolated
SM Make Stores Management ACTIVE()
SM Make Stores Management SECURE()
3. SM Weapon System Active
state description /
Weapon power available
SM Make Stores Management LIVE()
SM Make Stores Management ACTIVE()
SM Make Stores Management SECURE()
4. SM Weapon System Live
state description /
SMS critical power available
SM Release Weapon Package()
[Release Weapon Package Complete]()
SM Perform Jettison()
[Jettsion Weapon Package Complete]()
5. SM Live: Release Weapon Package
state description /
6. SM Live: Jettison Store Package
state description /

Figure 3-1: Stores Management States

3.3.3.3.1.3 Link Recovery Manoeuvre

In this situation, the UAS is attempting to re-establish C2 connectivity and may for example climb in spiral to find better signal strength. In this situation, target engagement is not anticipated. Subsequent signal recovery may result in re-planning.

3.3.3.3.1.4 Excursion From Safe Flight Envelope/Safety Indicators

There are situations in which weapon release would be unsafe. The basis of certification may define safety limits. Indicators include air/ground state, landing gear position, control surfaces, doors, etc. The safe flight envelope for weapon release includes limits for aircraft attitude (i.e., pitch, roll and yaw), height (AGL), speed, g-force, etc., and are defined by system design.

3.3.3.3.1.5 System Health

Various system heath indicators such as Built-In Test Equipment (BITE) and watchdog timers may trigger the Stores Manager state transition.

3.3.3.3.1.6 Authorized Controlling Entity

If the controlling entity changes, the system will drop out of Live state. As a general rule, the method of control safety precepts shall not be bypassed when the UAS is handed off to a new operator.

3.3.3.3.1.7 Data Validity (Sanity, Correct Metadata)

In this situation, inappropriate/incorrect commands are received (e.g., commands in wrong sequence or for wrong weapon load). This would suggest system fault.

3.3.3.3.1.8 Take-Off and Landing

Mishap risk during take-off and landing is mitigated by various safe flight envelope and safety indicators as noted in Section 3.3.3.3.1.4. While airborne and inside the safe flight envelope, it may be advantageous to enter the Live state if jettison availability is desired. However, emergency jettison, most often commanded just after take-off on a manned aircraft, may not be available on a UAS.

3.3.3.3.2 Station Control

1. The Station Control (SC) Domain provides station control services to the Stores Management Domain (fully described in the NIAG Subgroup 125 report). The state machine for the domain is shown in Figure 3-2. The figure indicates the external state transition triggers based on the IER of the domain.

2. The domain may transition out of the SC Live state to the SC Active state due to these internal triggers:

a. BITE;

b. Detection of unsafe S&RE release conditions including, as applicable, not fully-open bay doors, S&RE in wrong position, no store on station, safety-critical power not available.

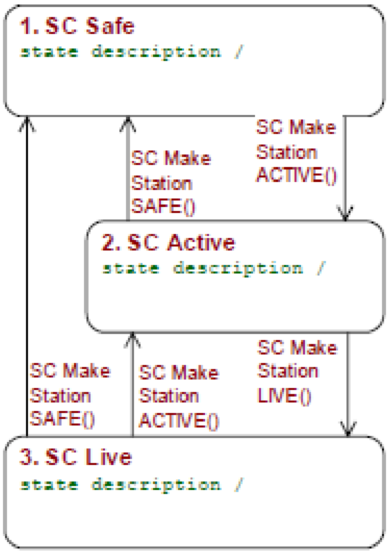


Figure 3-2: Station Control States

3.3.3.3.3 Pre-Launch Store Control

1. The Pre-Launch Store Control (PLSC) Domain provides pre-launch store control services to the Stores Management Domain, and is fully described in the NIAG Subgroup 125 report. The state machine for the domain is shown in Figure 3-3. The figure indicates the external state transition triggers based on the IERs of the domain.

2. At this time, no internal safety-critical state transition triggers have been identified.

3.3.3.4 Human Computer Interface Requirements (Safety Critical)

The Human Computer Interface (HCI) requirements were established from the operational and design safety precepts.

3.3.3.4.1 Control Station Hard Keys

Separate, single-function keys are required for setting the SM Weapon System to Live, and when Live to command weapon release and jettison. Different keys are required for the laser system.

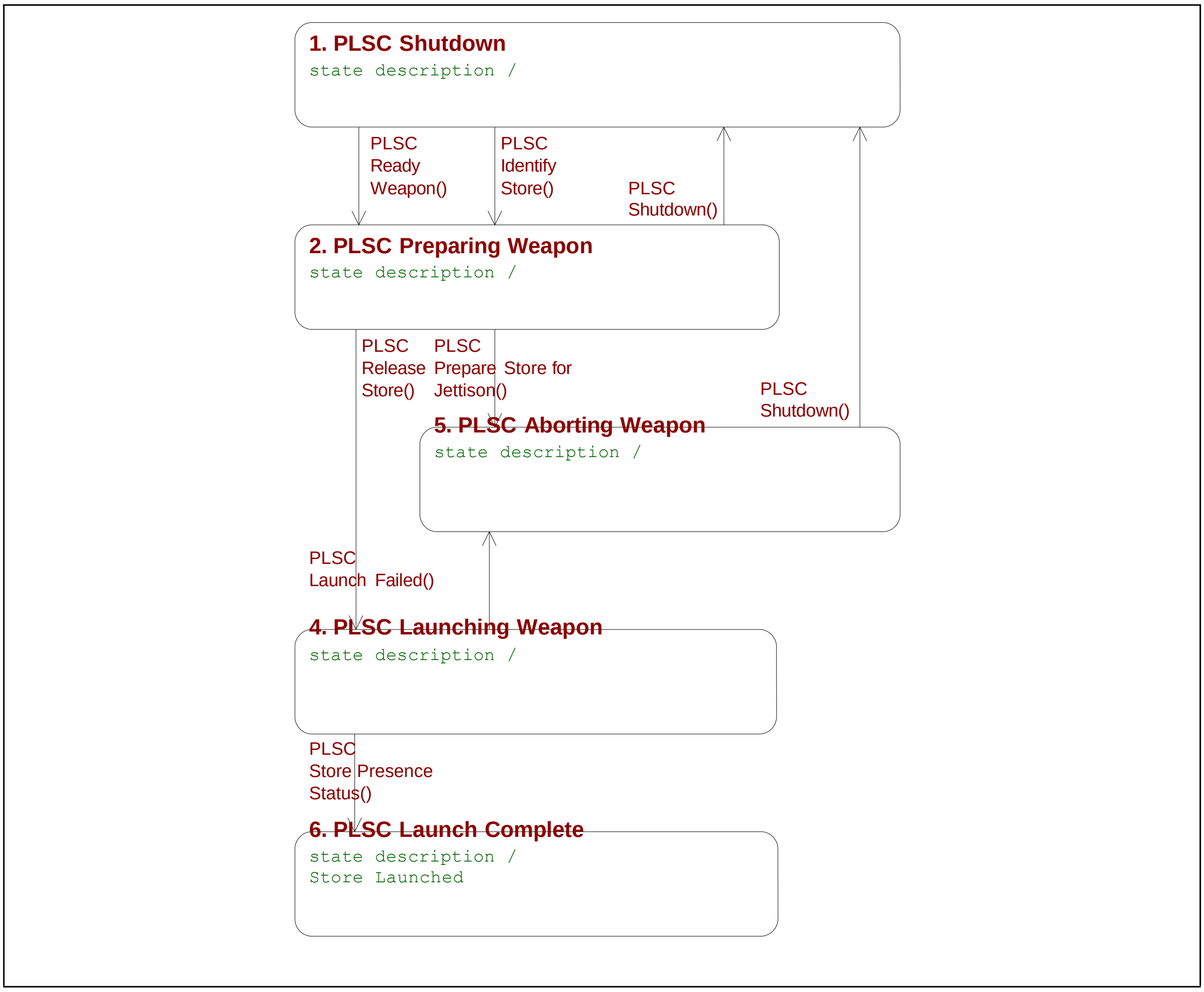


Figure 3-3: Pre-Launch Stores Control States

3.3.3.4.2 Setting Stores Management Domain to Live

Dedicated hard keys (i.e., not touch screen) for commanding the weapon system to Live state or commanding exit from the Live state are required. The position of the switch would not necessarily indicate the actual Live state of the weapon system. Therefore, the state shall be indicated by a software-actuated function via two methods (e.g., by a discrete lamp associated with the hard key and a separate indicator on the display glass).

3.3.3.4.3 Laser Designator

The laser system shall use different hard keys than the weapon system.

3.3.3.4.4 Commanding Weapon Package Release

1. There will be a dedicated hard key for commanding (triggering) weapon package release. The position of the switch would not necessarily indicate actual state of stores management; there is no ‘Boolean’ component to the switch. Therefore,

the state shall be indicated by a software actuated function (e.g., lamp and display artifact).

2. It is not a requirement that a weapon package release can be aborted once initiated.

3.3.3.4.5 Commanding Jettison Package

1. Selective Jettison Only - No Emergency Jettison (EJ). Note that weapon system state must be Live to allow jettison (thus EJ might be difficult to command during take-off and landing). There can be predefined jettison packages as well as operator defined packages.

2. There will be a dedicated hard key for commanding (triggering) jettison package release. The position of the switch would not necessarily indicate actual state of stores management; there is no ‘Boolean’ component to the switch. Therefore, the state shall be indicated by some software actuated function (e.g., light or display artifact).

3. It is not a requirement that a jettison package release can be aborted once initiated.

4. There must be a physical guard over the jettison key.

5. Generally there is no ‘liveness’ requirement for jettison. That is, failure to jettison when commanded must not be a critical hazard (resulting in critical mishap).

6. If jettison availability were a safety issue, a redundant architecture would be required with single fault tolerance.

3.3.3.5 Aircraft Ground Crew Safety Switch

1. There shall be a two-position (or multiple-position) MASS switch on the aircraft that is accessible to ground crew. One switch position shall ensure that the weapon system and all stations are in the safe state. Another position will allow the weapon system safety critical functions to be actioned from the Control Station.

2. The switch is a safety interlock when in the ‘safe’ position.

3.3.3.6 Data That Must Be Displayed (via glass, lamps, etc.)

The following requirements apply to data that must always be displayed, data to be displayed always when the Weapon System is Live, and data that must be displayable when the operator requests it.

3.3.3.6.1 Must Be Displayed At All Times (Cannot Be Covered)

Live (in state or out of state) – indicated by lamp associated with hard keys and on glass.

3.3.3.6.2 Data To Always Be Displayed When Live State Is Set

1. Live - Weapon system is releasing weapon package (and selected weapon release package).

2. Live - Weapon system is releasing jettison package (and selected jettison package).

3.3.3.6.3 Data To Always Be Displayed When 'Weapons Page' Is Selected

1. Data Link availability for weapon system must be displayed.

2. All weapon system states must be displayed.

3. For the selected weapon release package, the release readiness state must be displayed. This state is computed from individual store states, station control states, and pre-launch station control states in the package.

4. For the selected weapon release package, LAR status (go/no-go) must be displayed. This requirement addresses the mishap associated with hitting unintended objects.

5. For the jettison package, jettison readiness state must be displayed. This state is computed from the individual station control states.

6. The following Cautions, Warnings, Advisories must be displayed:

   a. Store Hung, exceptional store balance/load, exceptional interlock state;

   b. Computation of safe release condition for weapon package or jettison package. Either an inhibit or warning (or both) is to be provided. If an inhibit is provided with warning, the inhibit might be overridden if a system requirement.

7. If an operator requests the following data it shall be provided:

   a. Weapon mission plan (mitigation of risk that unintended target will be struck);

   b. Weapon status;

   c. Stores Management status and status of lower domains.

3.3.4 Hand-Off

1. It is assumed that authentication is handled by the general system. The maximum handoff state is SM Weapon System Active, which restricts any handoff occurring in a SM Live state.

2. Therefore, after a hand-off the new controller must perform the following functions to release a weapon:

a. Make weapon system live;

b. Select weapon package (weapon package definition includes select weapons and settings, plus target data);

c. Command release.

3.3.5 Certification Considerations

1. The following issues must be considered with regard to certification:

a. Partitioning of functions to isolate certification issues;

b. Dedicated hard keys for weapon safety;

c. Dedicated weapon-related messages (weapon functionality not mixed with other functionality);

d. Dedicated (partitioned) processes (or process) for stores management and lower domains;

e. Weapon-specific message validation methods (do not rely on generic network environment);

f. Architecture should be such that software safety obligations (resulting in high DO-178B DALs) are minimized;

g. Containment of safety case.

Note: Air-mechanical integration may be the same for manned and unmanned (same cables, etc.).

2. Safe separation analysis is the same for unmanned as manned.

INTENTIONALLY BLANK

ANNEX A INFORMATION EXCHANGE REQUIREMENTS (IERS)

A.1 INTRODUCTION

The information exchange requirements in this annex define the data exchanges between the services and nodes for the weaponised UAS architecture (developed by the NIAG-125 Study Group). This Study Group defined three alternative architectures (specifically location of services on the UA and UCS) which are dependent upon the inherent capabilities of the UAS. The three architectures and interfaces are shown in the following diagrams (Figures A-1 to A-3). The services provided by the UA element is highlighted in each figure. The interface requirements tables then relate to the services as shown in these architectures.

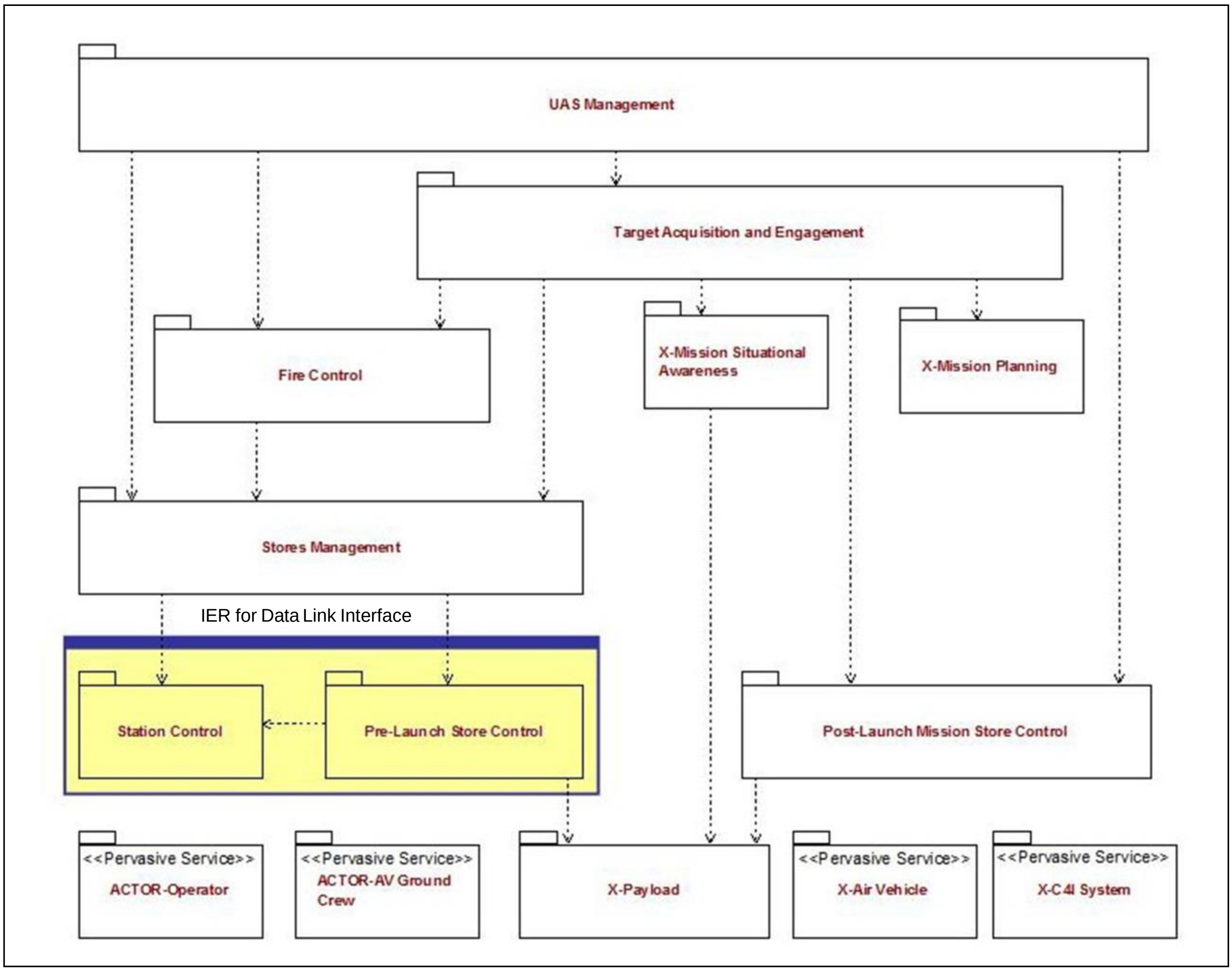


Figure A-1: Level 1 Capability UA

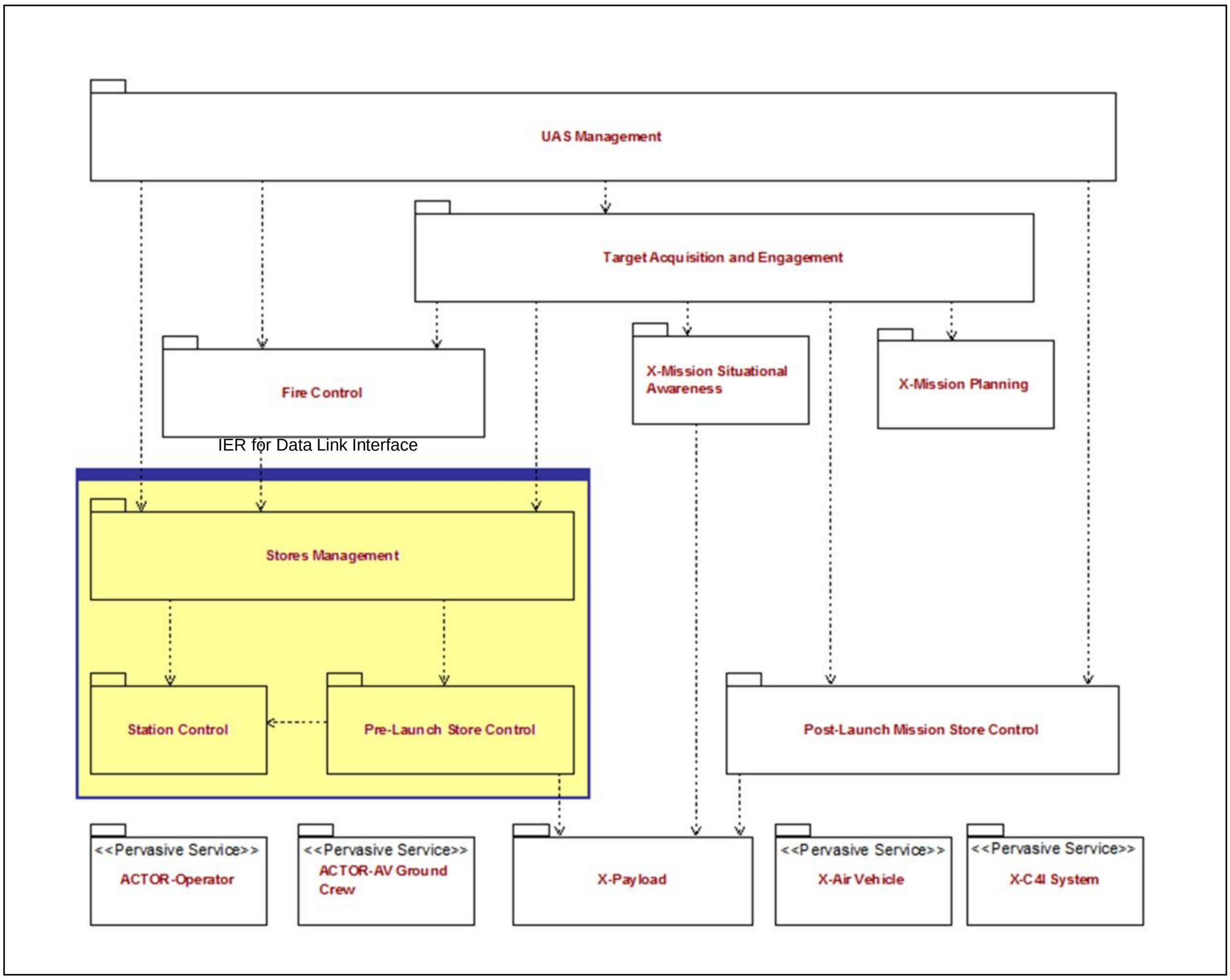


Figure A-2: Level 2 Capability UA

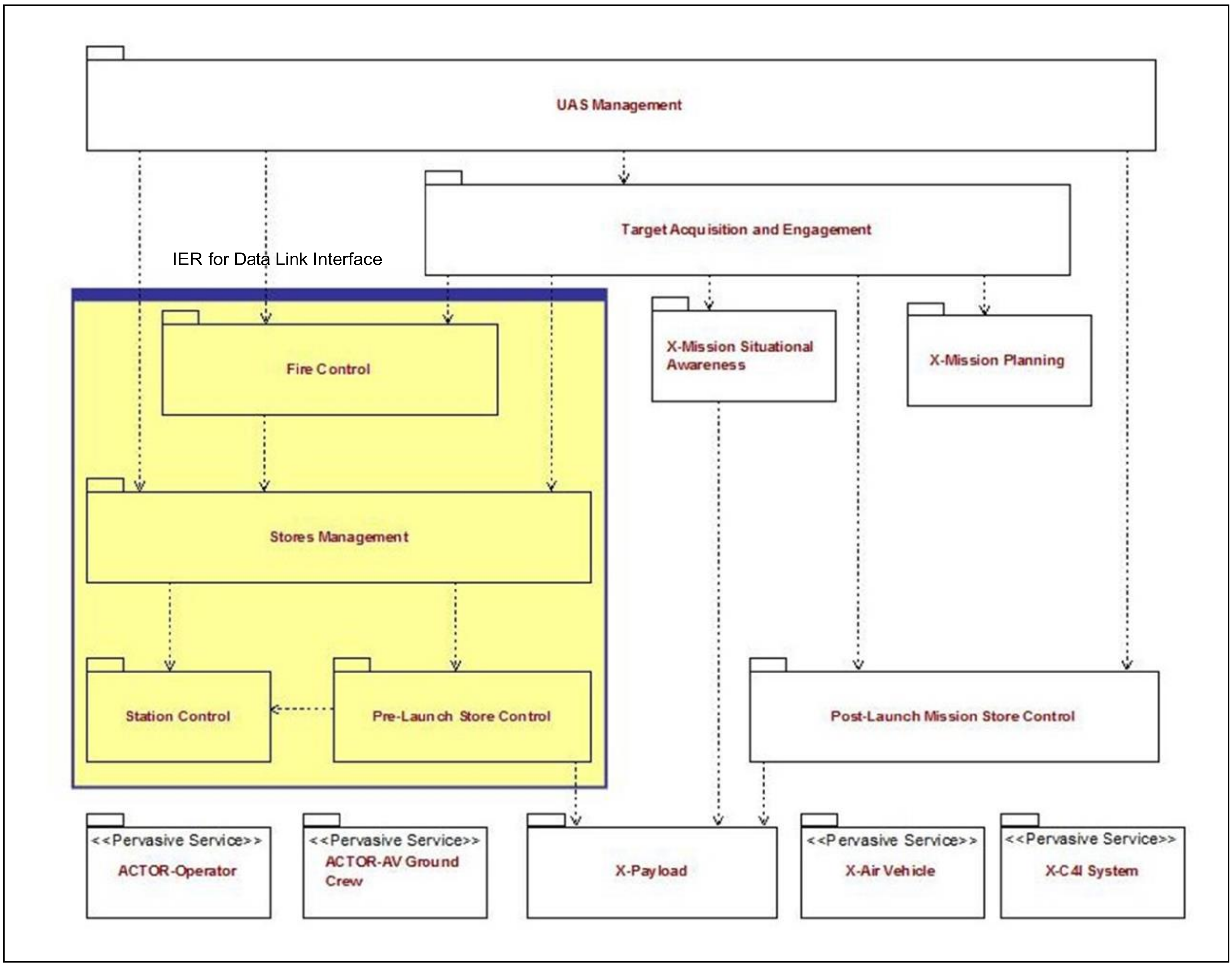

UAS Management
Target Acquisition and Engagement
IER for Data Link Interface
Fire Control
X-Mission Situational Awareness
X-Mission Planning
Stores Management
Station Control
Pre-Launch Store Control
Post-Launch Mission Store Control
<<Pervasive Service>> ACTOR-Operator
<<Pervasive Service>> ACTOR-AV Ground Crew
X-Payload
<<Pervasive Service>> X-Air Vehicle
<<Pervasive Service>> X-C4I System

Figure A-3: Level 3 Capability UA

A.2 INTER-NODE INFORMATION EXCHANGE REQUIREMENTS

1. Note that for Capability Level 3, only certain Stores Management messages are transferred across the data link. The others are private to the Fire Control Domain.

2. Table A-2 provides the IERs for the Fire Control Service.

3. Table A-3 provides the IERs for the Stores Management Service. The column C2 indicates that the message is transferred over the data link for a Capability Level 2 UAS. C3 indicates that the data is transferred over the data link for a Capability Level 3 UAS (otherwise the data is locally exchanged within the Fire Control Domain.)

4. Table A-4 provides the IERs for the Pre-Launch Store Control and Station Control Services. These interactions are transferred across the data link for a UAS with Capability Level 1.

A.2.1 IER Tables

The IER tables below (Tables A-1 to A-4) contain the following columns:

a. **Relevant Standard:** This indicates those existing standards that already define the content and/or structure of all or part of the associated message. A tilde (~) indicates that the named standard provides a partial definition of the associated message. This is not intended to indicate a recommendation to use the cited standards, but to provide a document to which the reader can refer to access additional information on the possible content of the messages.

b. **Volatility:** This indicates the degree (High – likely to change, Low – unlikely to change) to which the associated message data elements are likely to change, either from weapon type to weapon type, from platform type to platform type, or over time as CONOPS develop.

A.2.1.1 C4I Interface

These messages apply to all classes of UAS (i.e., C1, C2, and C3).

C4I Interface							
SOURCE DOMAIN	DEST NODE	DEST DOMAIN	MESSAGE NAME	NOTES	RELEVANT STANDARD	VOLATILITY	TYPICAL DATA ELEMENTS
X-Mission Planning	UCS	UAS Mgt	UAS Mission Plan	See Section C.1	MIL-STD-3014, CRD	H	Weapon Packages, Target Information, 4D Route, Fuze Settings, No Fly Zones
X-MSA	UCS	ACTOR-Operator	OP Jettison Point Reached		N/A	L	Boolean
X-MSA	UCS	TA	TA Selected Target Data	Additional targeting data not available during mission planning	~CRD, ADatP-3	H	Target Location, Target Type, Fuze Settings
X-MSA	UCS	TA	TA Target Area Information	Additional Target Area information	MIL-STD-3014, STANAG 4586, ADatP-3	H	Zones of Exclusion (fixed and dynamic (e.g., civilian traffic)
X-MSA	UCS	UAS Mgt	UAS Generate Mission Report	Control Command	N/A	L	Boolean
ACTOR-Operator	C4I	X-MSA	MSA Exploitation Of Attack Data	UAS data for external C4I Systems	N/A	L	Boolean
Fire Control	C4I	X-MSA	MSA LAR	UAS data for external C4I Systems	UAI / CLARA, STANAG 4586	L	Centre point, 3 or more 2D points

C4I Interface							
SOURCE DOMAIN	DEST NODE	DEST DOMAIN	MESSAGE NAME	NOTES	RELEVANT STANDARD	VOLATILITY	TYPICAL DATA ELEMENTS
TA	C4I	X-MSA	MSA Attack Information		MIL-STD-3014, STANAG 4586, ADatP-3	L	Attack success / fail / abort
TA	C4I	X-MSA	MSA Predicted Aim Point	UAS data for external C4I Systems Desired Aim Point	MIL-STD-3014, STANAG 4586, UAI	L	Aim Point (Lat, Long, Alt)
TA	C4I	X-MSA	MSA Target Information	UAS data for external C4I Systems	MIL-STD-3014, ADatP-3, UAI	H	Target Location, Target Type, Fuze Settings
TA	C4I	X-MSA	MSA Target Selected	UAS data for external C4I Systems	UAI	L	Boolean / Target ID
UAS Mgt	C4I	X-MSA	MSA Mission Plan Target Data	UAS data for external C4I Systems	MIL-STD-3014, ADatP-3, CRD	H	Target Location, Target Type, Fuze Settings

Table A-1: C4I Interface

A.2.1.2 Fire Control Services

These messages apply to C3 level UAS.

Fire Control Services							
SOURCE DOMAIN	DEST DOMAIN	MESSAGE NAME	SAFETY	NOTES	RELEVANT STANDARDS	VOLATILITY	DATA ELEMENTS
UAS Mgt	Fire Control	FC Erase Sensitive Data			STANAG 4586, UAI	L	Boolean
UAS Mgt	Fire Control	FC Ready Weapons			~STANAG 4586, UAI	L	Boolean
UAS Mgt	Fire Control	FC Release Weapon Package	x		STANAG 4586	L	Boolean
UAS Mgt	Fire Control	FC Select Weapon Package	x		STANAG 4586	L	Package identifier
UAS Mgt	Fire Control	FC Transfer Fire Control Mission Plan	x		MIL-STD-3014	L	SM Mission Plan + mission plan LAR, target engagement parameters (incl. SAL codes)
Fire Control	TA	TA LAR		LAR data	UAI, STANAG 4586	L	Centre point, 3 or more 2D points
Fire Control	UAS Mgt	UAS FC Weapon Package Selected	x		4568	L	Boolean, Package ID

Fire Control Services							
SOURCE DOMAIN	DEST DOMAIN	MESSAGE NAME	SAFETY	NOTES	RELEVANT STANDARDS	VOLATILITY	DATA ELEMENTS
Fire Control	UAS Mgt	UAS FC Weapon Package Status	x		STANAG 4586	H	Station Control status, Pre-Launch Store status, Weapon Status for each weapon in a package
Fire Control	UAS Mgt	UAS Fire Control Status	x		STANAG 4586	L	Boolean, Mission Plan Store Discrepancy List
Fire Control	UAS Mgt	UAS Sensitive Data Erased			STANAG 4586	L	Boolean
Fire Control	UAS Mgt	UAS Weapon Package Release Status	x		~STANAG 4586	L	Boolean, List of Weapon Id + Released / Hung / Not Released
Fire Control	UAS Mgt	UAS Weapons Initialized	x		STANAG 4586	L	Store status data (e.g., BIT result, alignment status, mission data status)

Table A-2: Fire Control Services

A.2.1.3 Stores Management Services

These messages apply to C2 and C3 level UAS as marked in the relevant columns.

Stores Management Services									
SOURCE DOMAIN	DEST DOMAIN	MESSAGE NAME	C2	C3	SAFETY	NOTES	RELEVANT STANDARDS	VOLATILITY	DATA ELEMENTS
Stores Mgt	Fire Control	FC Sensitive Data Erased	x				STANAG 4586, UAI	L	Boolean
Stores Mgt	Fire Control	FC Stores Mgt Status	x		x	Acknowledgment / Status	STANAG 4586, UAI	L	Boolean, Mission Plan Store Discrepancy List
Stores Mgt	Fire Control	FC Weapon Package Release Status	x		x	Acknowledgment / Status	~STANAG 4586, UAI	L	Boolean, List of Weapon ID + Released / Hung / Not Released
Stores Mgt	Fire Control	FC Weapons Initialized			x		N/A		
Stores Mgt	Fire Control	FC Weapons Initialized	x		x		STANAG 4586, UAI	L	Store status data (e.g., BIT result, alignment status, mission data status)
Fire Control	Stores Mgt	SM Erase Sensitive Data	x			Control Command	STANAG 4586, UAI	L	Boolean

Stores Management Services									
SOURCE DOMAIN	DEST DOMAIN	MESSAGE NAME	C2	C3	SAFETY	NOTES	RELEVANT STANDARDS	VOLATILITY	DATA ELEMENTS
Fire Control	Stores Mgt	SM Mission Plan	x			PLSC Mission Plan for all weapons, planned loadout, S&RE configuration, planned weapon release / jettison packages	MIL-STD-3014, UAI	H	Weapon Packages, Target Information, 4D Route, Fuze Settings, No Fly Zones
Fire Control	Stores Mgt	SM Query Stores Mgt Status	x		x	Control Command	N/A	L	Boolean
Fire Control	Stores Mgt	SM Ready Weapons	x			Control Command	STANAG 4586	L	Boolean
Fire Control	Stores Mgt	SM Release Weapon Package	x		x	Control Command	STANAG 4586	L	Weapon Package ID
Fire Control	Stores Mgt	SM Select Weapon Package	x		x	Control Command + package identifier	STANAG 4586	L	Weapon Package ID
UAS Mgt	Stores Mgt	SM Build Store Inventory	x	x		Control Command	N/A	L	Boolean

Stores Management Services									
SOURCE DOMAIN	DEST DOMAIN	MESSAGE NAME	C2	C3	SAFETY	NOTES	RELEVANT STANDARDS	VOLATILITY	DATA ELEMENTS
UAS Mgt	Stores Mgt	SM Make Stores Mgt ACTIVE	x	x	x	Control Command	~STANAG 4586	L	Boolean
UAS Mgt	Stores Mgt	SM Make Stores Mgt LIVE	x	x	x	Control Command	~STANAG 4586	L	Boolean
UAS Mgt	Stores Mgt	SM Make Stores Mgt SAFE	x	x	x	Control Command	~STANAG 4586	L	Boolean
UAS Mgt	Stores Mgt	SM Make Stores Mgt SECURE	x	x	x	Control Command	~STANAG 4586	L	Boolean
UAS Mgt	Stores Mgt	SM Perform Jettison	x	x	x	Control Command	STANAG 4586	L	Jettison Package ID
UAS Mgt	Stores Mgt	SM Select Jettison Package	x	x	x	Control Command + jettison package identifier	~STANAG 4586	L	Jettison Package ID
UAS Mgt	Stores Mgt	SM Transfer SMS Mission Configuration	x	x	x	Implementation Dependent	~UAI	H	SMS mission configuration data file (e.g., platform and weapon Configuration Data Sets)

Stores Management Services									
SOURCE DOMAIN	DEST DOMAIN	MESSAGE NAME	C2	C3	SAFETY	NOTES	RELEVANT STANDARDS	VOLATILITY	DATA ELEMENTS
Stores Mgt	UAS Mgt	UAS Jettison Package Status	X	X	X		~STANAG 4586	L	Boolean, List of Weapon ID + Released/Hung/Not Released
Stores Mgt	UAS Mgt	UAS Selected Jettison Package	X	X	X		~STANAG 4586	L	Jettison Package ID
Stores Mgt	UAS Mgt	UAS Stores Mgt Status	X	X	X		~STANAG 4586	L	Acknowledge Mission Plan Download/Air Vehicle Weapon Inventory/Power Status/Weapon System Status

Table A-3: Store Management Services

A.2.1.4 Pre-Launch Store Control and Station Control Services

These messages apply to C1 level UAS.

Pre-Launch Store Control and Station Control Services							
SOURCE DOMAIN	DEST DOMAIN	MESSAGE NAME	SAFETY	NOTES	RELEVANT STANDARDS	VOLATILITY	DATA ELEMENTS
Pre-Launch Store Control	Stores Mgt	SM Mission Plan Accepted			STANAG 4586	L	Boolean, Mission Plan Store Discrepancy List
Pre-Launch Store Control	Stores Mgt	SM PLSC Release Status	x		STANAG 4586	L	Boolean, List of Weapon ID + Released / Hung / Not Released
Pre-Launch Store Control	Stores Mgt	SM PLSC Status	x		~STANAG 4586	L	State (SAFE, SECURE, ACTIVE, LIVE)
Pre-Launch Store Control	Stores Mgt	SM Pre-Launch Store Control Configured			N/A	L	Boolean

Pre-Launch Store Control	Stores Mgt	SM Selected Weapon Status	x		~STANAG 4586	L	List of Weapon Id + Ready / Armed / Failed / No Comms

Pre-Launch Store Control and Station Control Services							
SOURCE DOMAIN	DEST DOMAIN	MESSAGE NAME	SAFETY	NOTES	RELEVANT STANDARDS	VOLATILITY	DATA ELEMENTS
Pre-Launch Store Control	Stores Mgt	SM Sensitive Data Erased			STANAG 4586	L	Boolean
Pre-Launch Store Control	Stores Mgt	SM Status from Weapon	x		~STANAG 4586, UAI	L	Store status data (e.g., BIT result, alignment status, mission data status)
Pre-Launch Store Control	Stores Mgt	SM Store BIT Result			UAI	L	Detailed BIT result (bit pattern)
Pre-Launch Store Control	Stores Mgt	SM Store Identity			UAI	L	Store identifier
Pre-Launch Store Control	Stores Mgt	SM Store Jettison Status	x		~STANAG 4586	L	Ready / not ready for jettison
Station Control	Stores Mgt	SM Station Control Status	x		~STANAG 4586	L	State (SAFE, ACTIVE, LIVE)
Stores Mgt	Pre-Launch Store Control	PLSC Erase Sensitive Data		Control Command	STANAG 4586	L	Boolean
Stores Mgt	Pre-Launch Store Control	PLSC Identify Store		Control Command	UAI	L	Boolean

Pre-Launch Store Control and Station Control Services							
SOURCE DOMAIN	DEST DOMAIN	MESSAGE NAME	SAFETY	NOTES	RELEVANT STANDARDS	VOLATILITY	DATA ELEMENTS
Stores Mgt	Pre-Launch Store Control	PLSC Instantiate And Configure Pre-Launch Store Control			MIL-STD-3014, UAI	L	Weapon mission configuration data (e.g., weapon configuration)
Stores Mgt	Pre-Launch Store Control	PLSC Mission Plan			MIL-STD-3014, UAI	H	Weapon mission data (in accordance with load / modify mission data use case)
Stores Mgt	Pre-Launch Store Control	PLSC Prepare Store For Jettison	x	Control Command	STANAG 4586	L	Boolean, Store ID
Stores Mgt	Pre-Launch Store Control	PLSC Ready Weapon			UAI	H	Store specific mission initialisation data (e.g., mission data)
Stores Mgt	Pre-Launch Store Control	PLSC Release Store	x	Control Command	STANAG 4586, UAI	L	Boolean, Store ID
Stores Mgt	Pre-Launch Store Control	PLSC Select Weapon	x	Control Command	STANAG 4586	L	Boolean, Store ID
Stores Mgt	Pre-Launch Store Control	PLSC Shutdown	x	Control Command	STANAG 4586	L	Boolean

Pre-Launch Store Control and Station Control Services							
SOURCE DOMAIN	DEST DOMAIN	MESSAGE NAME	SAFETY	NOTES	RELEVANT STANDARDS	VOLATILITY	DATA ELEMENTS
Stores Mgt	Station Control	SC Jettison S And RE	x	Control Command	N/A	L	Boolean, Station ID
Stores Mgt	Station Control	SC Make Station ACTIVE	x	Control Command	~STANAG 4586	L	Boolean, Station ID
Stores Mgt	Station Control	SC Make Station LIVE	x	Control Command	~STANAG 4586	L	Boolean, Station ID
Stores Mgt	Station Control	SC Make Station SAFE	x	Control Command	~STANAG 4586	L	Boolean, Station ID

Table A-4: Pre-Launch Store Control and Station Control Services

INTENTIONALLY BLANK

ANNEX B ACRONYMS

AAI	Attack-Attack Interface
AAP	Air Armaments Panel
AAR	Air-Air-Refuelling
ACC	Air Component Commander
ACCS	Aircraft Command & Control System
ACG	Air/Aerospace Capability Group
ACM	Airspace Control Measures
ACO	Airspace Control Order
ACT	Allied Command Transformation
ACU	Aircraft Control Unit
ADatP	Allied Data Publication
AEIS	Aircraft Store Electrical Interconnection Set
AGM	Attack Guidance Munitions
AH	Armed/Attack Helicopter
AI	Air Interdiction
AJ	All Jettison
AJP	Allied Joint Publication
ALARP	As Low As Reasonably Practicable
ALWI-CI	Aircraft, Launcher & Weapon Interoperability Common Interface
ALWI-TA	Aircraft, Launcher & Weapon Interoperability Technical Architecture
AMC	Airborne Mission Coordinator
AO	Area Operations
AOC	Air Operations Centre
AOCC	Air Operations Coordination Centre
AOCC(L)	Air Operations Coordination Centre (Land)
AOD	Air Operations Directive
AOO	Area Of Operations

AOP	Allied Ordnance Publication
AOR	Area Of Responsibility
AR	Armed Reconnaissance
AS	Associated Support
ASCII	American Standard Code for Information Interchange
ASFAO	Anti-Surface Force Air Operations
ASuW	Anti-Surface Warfare
ASW	Anti-Submarine Warfare
ATO	Air Tasking Order
AWACS	Airborne Warning & Control System
BCD	Battlefield Coordination Detachment
BDA	Battle Damage Assessment
C2	Command & Control
C3	Command, Control & Communications
C4I	Command, Control, Communications, Computers & Intelligence
CA	Combat Assessment
CAOC	Combined Air Operations Centre
CAS	Close Air Support
C-BIT	Continuous Built In Test
CC	Component Commander
CDA	Common Domain Architecture
CDT	Control Data Terminal
COMAO	Composite Air Operations
COP	Common Operational Picture
CR	Combat Recovery
CRD	Common Route Definition
CSAR	Combat Search & Rescue
Def-Stan	Defence Standard
DLI	Data Link Interface
DMPI	Desired Mean Point of Impact
DoD	Department of Defense

DoDAF	Department of Defense Architectural Framework
DS	Direct Support
EASA	European Aviation Safety Agency
EJ	Emergency Jettison
ELINT	Electronic Intelligence
EO	Electro Optical
ESM	Electronic Support Measures
EW	Electronic Warfare
FAA	Federal Aviation Agency
FAC	Forward Air Controller
FAC-A	Forward Air Controller (Airborne)
GASIF	Generic Aircraft Store Interface Framework
GAT	Guidance, Apportionment & Targeting
GCS	Ground Control Station
GI&S	Geospatial Information & Services
GMTI	Ground Moving Target Indicator
GPS	Global Positioning System
HALE	High Altitude Long Endurance
HCI	Human-Computer Interface
HPT	High Payoff Target
HPTL	High Payoff Target List
HUMINT	Human Intelligence
HVT	High Value Target
HVTL	High Value Target List
IA	Information Assurance
I-BIT	Initiated Built In Test
ICD	Interface Control Document
IER	Information Exchange Requirements
IMINT	Image Intelligence
IMM	Interface for Micro-Munitions
INS	Inertial Navigation System

IR	Infra Red
ISR	Intelligence, Surveillance & Reconnaissance
ISRT	Intelligence, Surveillance, Reconnaissance & Targeting
ISTAR	Intelligence, Surveillance, Target Acquisition & Reconnaissance
IT	Information Technology
JAAT	Joint Air Attack Team
JAOC	Joint Air Operations Centre
JAPCC	Joint Air Power Competency Centre
JCGUAS	Joint Capability Group Unmanned Aircraft Systems
JDAM	Joint Direct Attack Munition
JFACC	Joint Forces Air Component Commander
JFC	Joint Force Commander
JFHQ	Joint Force Headquarters
JIPTL	Joint Integrated Prioritised Target List
JMPS	Joint Mission Planning System
JOA	Joint Operational Area
JPR	Joint Personnel Recovery
JSF	Joint Strike Fighter
JSOW	Joint Stand-Off Weapon
JSTARS	Joint Surveillance & Target Acquisition Radar System
JTAC	Joint Terminal Attack Controller
JTCB	Joint Targeting Coordination Board
JTFHQ	Joint Theatre Forces Headquarters
JTL	Joint Target List
JUASP	Joint Unmanned Aircraft System Panel
LAR	Launch Acceptability Region
LCC	Land Component Commander
LOAC	Law Of Armed Conflict
LOBL	Lock-On Before Launch
LOC	Lines Of Communication
LORAN	LOng RAnge Navigation

MAAP	Master Air Attack Plan
MALE	Medium Altitude Long Endurance
MASS	Master Arm Safety Switch
MCC	Maritime Component Commander
MDA	Model Driven Architecture
MEA	Munitions Effectiveness Analysis
MiDEF	Mission Data Exchange Format
MITL	Man-In-The-Loop
MMSI	Miniature Munitions Standard Interface
MOUT	Military Operations in Urban Terrain
NAF	NATO C3 Architectural Framework
NAFAG	NATO Air Force Armaments Group
NATO	North Atlantic Treaty Organization
NC3	NATO Command, Control & Communication
NC3A	NATO Command, Control & Communications Agency
NC3TA	NATO C3 Technical Architecture
NCSP	NATO Common Standards Profile
NEW	Networked Enabled Weapon
NIAG	NATO Industrial Advisory Group
NNAG	NATO Naval Armaments Group
NNEC	NATO Networked Enabled Capability
NNWESB	Non-Nuclear Weapons & Explosives Safety Board
NRC	Nuclear Regulatory Commission
NSL	No-Strike List
NSO	NATO Standardisation Office
NSR	NATO Staff Requirement
NTRM	NATO Technical Reference Model
NUAI	NATO Universal Armament Interface
OCA	Offensive Counter Air
OMG	Object Management Group
OPCON	Operational Control

OSC	On-Scene Commander
OTC	Officer in Tactical Control
PAR	Post Attack Reconnaissance
P-BIT	Power up Built In Test
PGM	Precision Guided Munition
PLSC	Pre-Launch Store Control
RAI	Recce Attack Interface
RAM	Random Access Memory
RF	Radio Frequency
RMC	Rescue Mission Commander
RMP	Recognized Maritime Picture
ROE	Rules of Engagement
RR	Re-attack Recommendations
RSEAD	Reactive Suppression of Enemy Air Defenses
RSTA	Reconnaissance, Surveillance & Target Acquisition
RTL	Restricted Target List
RTO	Research & Technology Organisation
RVT	Remote Video Terminal
S&RE	Suspension & Release Equipment
S/G	Study Group
SAE	Society of Automotive Engineers
SAL	Semi-Active Laser
SAR	Synthetic Aperture Radar
SC	Station Control
SCAR	Strike Coordination & Reconnaissance
SDB	Small Diameter Bomb
SEAD	Suppressions of Enemy Air Defenses
SIGINT	Signals Intelligence
SM	Stores Management
SMS	Stores Management System
SOA	Service Oriented Architecture

SPINS	Special Instructions
STANAG	Standardisation Agreement
TAC	Tactical Air Controller
TACON	Tactical Control
TACP	Tactical Air Control Party
TASMO	Tactical Air Support for Maritime Operations
TLE	Target Location Error
TNL	Target Nomination List
TOO	Target Of Opportunity
TSS	Target Selection Standards
TST	Time Sensitive Targeting
TTP	Tactics, Techniques & Procedures
TUAS	Tactical UAS
UA	Unmanned Aircraft
UAI	Universal Armament Interface
UAS	Unmanned Aircraft System
UCS	UAS Control System
UHF	Ultra High Frequency
UML	Universal Modelling Language
USN	United States Navy
VDT	Vehicle Data Terminal
VMF	Variable Message Format
WEA	Weapons Effects Analysis
WF	Warfighter
WGS 84	World Geodetic System 84
WST	Weaponisation Specialist Team
XML	Extensible Mark-up Language

AEP-82(A)(1)