

NATO UNCLASSIFIED

NATO STANDARD

APP-34

**TESTING AND INTEROPERABILITY
OF AREA ACCESS CONTROL
OBSTACLE SYSTEMS**

Edition A Version 1

DECEMBER 2019



NORTH ATLANTIC TREATY ORGANIZATION

ALLIED PROCEDURAL PUBLICATION

**Published by the
NATO STANDARDIZATION OFFICE (NSO)
© NATO/OTAN**

NATO UNCLASSIFIED

NATO UNCLASSIFIED

INTENTIONALLY BLANK

NATO UNCLASSIFIED

NATO UNCLASSIFIED


NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

9 December 2019

1. The enclosed Allied Procedural Publication APP-34, Edition A, Version 1 – TESTING AND INTEROPERABILITY OF AREA ACCESS CONTROL OBSTACLE SYSTEMS, which has been approved by the nations in the Military Committee Land Standardization Board, is promulgated herewith. The recommendation of nations to use this publication is recorded in STANREC 2642.
2. APP-34, 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.


for Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

NATO UNCLASSIFIED

NATO UNCLASSIFIED

INTENTIONALLY BLANK

NATO UNCLASSIFIED

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

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 Document Database for the complete list of existing reservations.

INTENTIONALLY BLANK

TABLE OF CONTENTS

CHAPTER 1 Introduction and Recommended Requirements 1-1

1.1 Introduction. 1-1

1.1.1 Aim..... 1-1

1.1.2 AAC Overview..... 1-1

1.2 Requirements..... 1-3

1.2.3 General System Requirements. 1-3

1.2.4 General Obstacle Requirements. 1-8

1.2.5 Component Requirements. 1-9

CHAPTER 2 Testing Categories, Environments and Scenarios..... 2-1

2.1 Aim..... 2-1

2.2 Definitions. 2-1

2.2.1 Categories..... 2-1

2.2.2 Environments. 2-3

2.2.3 Scenarios. 2-3

CHAPTER 3 Technical Component and System Testing. 3-1

3.1 Aim..... 3-1

3.2 Overview of Test Planning. 3-1

3.3 Developmental Test Events, Scope of Testing, and Basic Scenarios 3-1

3.3.1 Effectors..... 3-1

3.3.2 Sensors..... 3-2

3.3.3 Command and Control (C2). 3-3

3.3.4 Overall System Testing and Effectiveness Assessment. 3-3

3.4 Operational Testing..... 3-4

Annex A. AAC Employment Task List..... A-1

Annex B. Example AAC Operational and Developmental Test Matrix B-1

INTENTIONALLY BLANK

CHAPTER 1 Introduction and Recommended Requirements

1.1 Introduction.

1.1.1 Aim

The purpose of providing guidance on considerations for testing for the Area Access Control (AAC) STANREC is two-fold: to promote standardization, test planning, interoperability, and opportunities to buy common obstacle systems or components; and to increase the likelihood that any obstacle systems developed and/or procured are safe, suitable and effective for use in supporting terrain, situation and target oriented obstacles. Each nation will identify its own AAC obstacle system requirements and develop its own test plan. Providing guidance to Nations, and to industry representatives looking to sell systems or subsystems to Nations, promotes the development and fielding of robust obstacle systems that meet specific National performance requirements. All testing should be conducted under as realistic conditions as possible to support system verification.

1.1.2 AAC Overview.

1. An AAC obstacle system is a command and control (C2) system for various sensors and effectors in order to control access to or create an obstacle in a specific land-based operational area. The concept of an AAC obstacle system is first to detect and locate, then identify single or multiple threats, entering the obstacle or controlled area. Secondly, to give an overview and the status of the available lethal and non-lethal effectors to disrupt or deny those threats, and a remote-controlled way to activate and de-activate specific effectors as required, according to the commander's intent. Thirdly, to prevent or degrade further intrusion into the obstacle or controlled area, through efficient effects created by the chosen effectors, either by operator remote control or semi-autonomous (victim activated), depending on national policy and / or Rules of Engagement (ROE). Finally, to de-activate any effectors in order to provide safe passage and allow maintenance and/or recovery/reuse of the system components. The obstacle system includes three main components.

a. Sensor. The main function of sensors is to observe activity in the field and convert the activity into a standardized information format that can be evaluated by the C2 component. The sensor should be capable of converting the information into a standardized message format that C2 components can understand.

b. Effector. The main function of effectors is to react and engage the directed targets with either lethal or non-lethal effects. The effectors act on the operator's command or programmed instruction based on the information gathered from the sensors.

c. C2. Its function is to provide the operator the ability to plan, maintain, and manage the AAC obstacle systems. C2 provides the user interface required to maintain the appropriate Human In / On the Loop control and has the interfaces to interact with the sensors, effectors, and external systems (e.g. other C2). Any obstacle communication subsystem is also considered part of the C2 element.

2. AAC is a capability that will be employed to execute counter-mobility and survivability tasks. Execution of counter-mobility tasks will include emplacement of obstacles that deter aggression and deny enemy freedom of movement (FoM) by enabling the following tactical mission effects: fixing, turning, disrupting, and blocking. Survivability tasks will include enhancing force protection at base camps, facilities, and other infrastructure, while allowing access for friendly personnel or equipment. Figure 1 below shows typical examples.

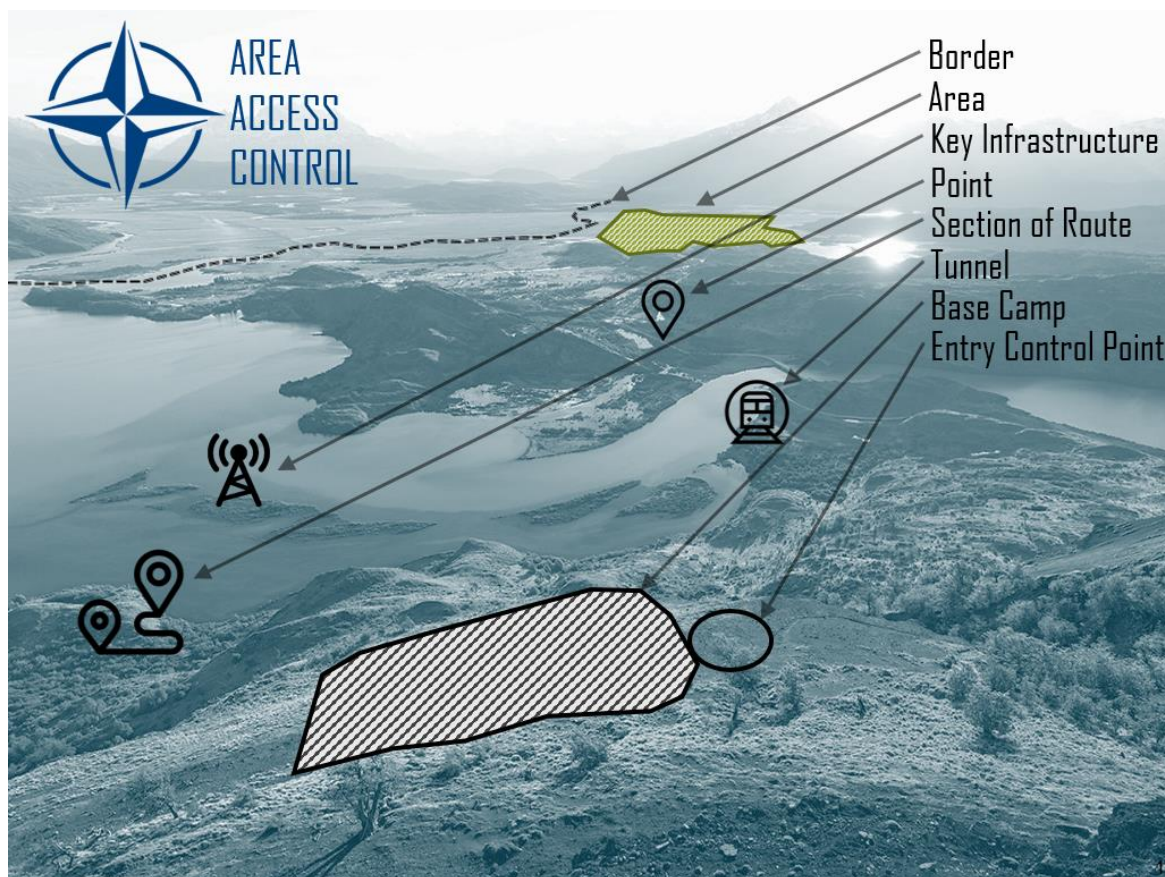


Figure 1 – AAC Operational Use Examples

3. Concept of Operations. Each Nation will differ in the operational scenarios that they will be tasked to employ an AAC obstacle system in. Below is a table completed as part of the NATO Industry Advisory Group (NIAG) study group 174, dated 30 April 2014, that provides a rough guide for potential planning considerations for different situations.

Scenario	Sub-Scenario	Emplacement Time (long period = days, medium period = hours, short period = minutes)	Employed Life* (long period > 1 year, medium period < 1 year, short period < 30 days)	Area Size (large > 1km frontage, medium = 100m to 1km frontage, small < 100m frontage)	Communication Range (long > 3km, medium = 1 to 3km, short < 1km)	Type of Effector (non-lethal, lethal)	Target Type (tracked vehicle, wheeled vehicle, commercial vehicle, personnel)
Counter-Mobility Area Denial	Area	M,S	S,M	M,L	M,L	L,NL	TV,W V,P
	Point	S,M	S,M	S	M,L	L,NL	TV,W V,CV, P
Counter-Mobility Route Denial	Border	L	L,M	L	L,	NL,L	P,CV
	Tunnel	M,L	M,S	S	M,L	NL,L	P,CV
	Section of Route	M,L	S,M	S,M	L	NL,L	P,CV
Survivability	Base Camp	M,L	L,M	L	S,M	NL,L	P,CV
	Key Infrastructure	M,L	L,M,S	M	S,M	NL,L	P,CV
	Entry Control Point	M,L	L,M	S	S	NL	CV,P

Table 1. Scenarios. The letters are in order of most relevance. Employment life does not necessarily mean armed state.

1.2 Requirements.

1.2.3 General System Requirements.

1. Overview. Each nation will determine its own unique AAC obstacle systems requirements. The paragraphs that follow cover many of the potential AAC capabilities Nations should consider as they develop their requirements. They address general, overall system requirements, obstacle subsystem requirements, and C2 subsystem requirements. Nations should consider, for requirements that are applicable to their system, what performance measures should be used to assess AAC obstacle system capabilities during testing. Additional testing guidance is contained in Chapters 2 and 3.

2. Environmental Conditions. The AAC obstacle system will need to remain safe and functional during storage, transportation, and use in the battlespace. Chapter 2 details environmental and scenario testing recommendations.
 - a. Natural Environments. Use of AECTP 230 – Climatic Conditions is the standardized documentation used for NATO to define operational environmental conditions.
 - b. Shipping / Storage, Transportation, Drop. Use AEPP-3 NATO Standard Packaging Test Procedures. Unpackaged AAC components may be exposed to a variety of logistical environments that are not addressed in the above procedures. Therefore, an assessment should be made to ensure they remain safe during and fully functional after transport.
3. Sustainability.
 - a. Maintenance. A maintenance analysis will need to be performed on the AAC obstacle system to determine maintenance man-hour requirements, spare parts requirements, components suitable for repair versus replacement, stockpile surveillance requirements, etc. AAC obstacle systems may provide a low power or battery replacement indicator on system components and offer relocation and reformation of the AAC C2 network after battery replacement.
 - b. Special Tooling. Creating a requirement for special tools should be avoided in system and requirements development. If the use of special tools is required, they should be kept to a minimum and located at the appropriate level of maintenance (e.g. operator, unit, depot).
 - c. Logistics. Logistical requirements associated with the employment of AAC obstacle systems should be identified to support realistic employment planning and training. This includes determining physical transport requirements (e.g. quantities of AAC pallets, trucks and trailers) and Materiel Handling Equipment (MHE) requirements; procedures for securing packaged and unpacked AAC components in the appropriate vehicles; and procedures for recovery, inspection, and repackaging or reuse as appropriate.
4. Availability.
 - a. Availability is the probability that a system will be able to perform its mission profile. It is measured in terms of up time and down time. After a system is developed and is in field use, the number of hours that the system is “up” (i.e., capable of performing missions) and the total number of hours that it was supposed to be up in any given timeframe can be measured. The operational availability can then be calculated by dividing the time it was up by the total time it was supposed to be up.

b. Availability is primarily a function of how often failures occur or corrective / preventive maintenance is required (reliability), and then how quickly indicated or recorded failures can be confirmed and repaired, or preventive maintenance performed (maintainability). Three performance measurements provide overall indications of field experience: mission success rates, operational availability, and operations and support costs. However, in themselves, these do not necessarily indicate the specific cause of problems. A robust data collection and analysis program, and use of forums such as Reliability, Availability and Maintainability (RAM) review boards, will help identify and prioritize specific RAM problems for resolution.

c. When the effects of design and the support system on availability are being considered, then Operational Availability is the appropriate measure. A steady-state for operational availability, calculated based on system use over long periods of time, is the goal. So when considering a short duration, such as a warfighter's three or seven day mission, then availability will most likely not achieve steady state. Therefore, it would be inappropriate to use this limited data set to calculate operational availability. Simulation should be used to calculate operational availability in this example.

d. An AAC obstacle system should have an availability requirement of 90% or greater. Sub-component availability therefore will have to have even higher availability or the employment tactics, techniques, and procedures (TTP) must provide adequate redundancy.

5. Reliability.

a. Functionality. The reliability of individual components must be very high (at least 95% or more) in order to achieve a robust system level reliability. Use of redundant control stations and / or communication networks is a potential way to increase system reliability.

b. Mission Life. Nations should be aware that there is a tradeoff between mission life and the reliability of AAC systems.

c. Self-destruct (SD) / Self De-Activate (SDA). The reliability of this function must be very high and in line with convention for Certain Conventional Weapons protocols (CCW¹).

d. Recovery and Reuse. Nations should identify how many reuses of AAC obstacle components they require and the implications for the durability of employed components.

e. Command and Control (C2). The reliability of the system hardware and software needs to be very high (ideally 95% or higher) and the control station

¹ Certain Conventional Weapons protocol. Declaration on Anti-Vehicular Mines, dated 16 Nov 2006.

software should be able to track reliability over time. Control station software should be designed for upgrades over its life cycle. Network reliability includes the ability of the AAC obstacle to receive, enact, and acknowledge commands, that typically will include on / off, change self-destruct time, command destruct, variable obstacle effect, and any obstacle-initiated messages (such as target reports). Sending and receiving commands is critical to determine the probability of AAC activity success.

6. Survivability.

a. Insensitive Munitions. The survivability and safety of AAC effectors must be maintained when exposed to events like fire, detonations, etc.

b. Sensor and C2 resilience. The AAC obstacle system should be resilient against events like fire, detonations, spoofing, and jamming.

c. Chemical, Biological, Radiological, and Nuclear (CBRN) Contamination. Selected AAC obstacle components (such as the control station) should remain safe and functional during and after exposure to CBRN contamination, and decontamination.

d. Anti-Tamper / Disturbance. Any anti-tamper / anti-disturbance feature should avoid being too sensitive, or too insensitive, as to make it more vulnerable to breaching / clearing rather than a viable deterrent to attempted dismounted breaching/clearing techniques. See Convention on Certain Conventional Weapons, Protocol II on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices, amended on May 3, 1996.

e. Countermeasures. AAC obstacle components should be resistant to / survivable against threat countermeasures like mechanical breaching, explosive line charge breaching, and electronic countermeasures like magnetic signature projectors.

f. Cryptographic Module Validation (CMV). AAC systems should possess appropriate CMV protection.

g. Cybersecurity. AAC systems should comply with host nation requirements and undergo appropriate adversarial assessment to confirm compliance.

h. Electronic Warfare (EW). The AAC system must operate in an EW threat environment. The impacts of jamming must be determined to help establish TTPs related to EW operations.

i. Directed Energy Weapons. The AAC system must be resilient against DEW effects. The impacts of DEW must be determined to help establish TTPs.

j. Electromagnetic Environmental Effects (E3). The allowable impact of natural (e.g. lightning, electro-static discharge) and manmade (e.g. radios, radars, etc.) E3 effects on AAC system components, including the potential interference between the AAC system and civilian and military communication, jamming and other systems, must be defined based on realistic distances, signal strength and frequencies.

k. Camouflage and concealment. The ability of systems to function whilst utilizing various forms of camouflage and concealment should be defined based on National requirements, and component technology constraints. TTPs can provide solutions to minimize the detectability of system components and avoid unacceptable performance degradation.

7. Safety.

a. General Safety. Early on in the program the following safety considerations should be examined:

(1) Fuzing System. The safety of the effector fuzing design.

(2) Safe and Arming Device. Use of an electronic safe and arm device is typical for effectors and its design should be assessed. After receiving a recovery command, AAC obstacle components will provide a visual indication of safe status.

(3) Environmental Safety. The materials used in AAC components should be evaluated to ensure that no undesirable environmental hazards are created through AAC employment and use.

(4) Effects Safety. Determining the surface danger zone of effectors should be part of the AAC safety assessment process. Additionally, confirmation that effects report correctly, and the remote-control station correctly displays the status of deployed components, especially any lethal deployed components, at a very high reliability is critical.

b. Personnel Safety. Soldier safety should be considered during the development of design features (e.g. safe separation time prior to effector arming, recovery and reusability), employment TTPs (e.g. obstacle command and control procedures, the use of fencing to mark obstacle boundaries with consideration of the surface danger zone for any effectors, etc.), and training (e.g. ensuring Soldier training and manuals emphasize safety points and are fully comprehensive in terms of detailing potential safety risks).

8. Human Factors Integration.

a. The initial design of an AAC obstacle system should consider how it interacts with the soldier, including the entire AAC employment concept. This will help identify potential design changes, areas of training requiring increased emphasis, or adjustments in employment methods that should be considered.

b. Training Aids. Training aides should be realistic, reliable, durable, and reusable to give accurate simulation of the tactical employment.

(1) Control Station. Control station can utilize embedded or networked training software, or both. The control station needs to simulate all tactical functions the operator may have to perform.

(2) Obstacle System. The obstacle system training aides should be the same form, fit, and function, and use the same packaging as the tactical system. Battlefield effects may be simulated using sight and sound and integrated into collective training centers. The goal of the training aides is to avoid any negative training impacts and maximize soldier proficiency and minimize skill fade. The system should include inert training devices as well.

c. Technical manuals. Conduct detailed reviews of all AAC obstacle system documentation with user representation to ensure manual sufficiency.

1.2.4 General Obstacle Requirements.

1. Field Emplacement and Recovery. Consideration should be given to a unit's ability to emplace and recover AAC obstacles with organic assets, as well as the transfer of the obstacle to another unit. The level of command that holds the obstacle control station, and the retention of packaging to support potential recovery and reuse are also considerations.

2. Geo-Location. If deployed, AAC obstacle components have an automated geo-location reporting capability, the accuracy and reliability of the reporting and recording function should be considered. If locations are manually recorded during emplacement, the AAC C2 system should be able to upload and synchronize locations with component identification numbers.

3. Obstacle Reporting. Once an AAC obstacle has been emplaced, it should be reported in accordance with either STANAG 2036 or 2430 as required. This functionality may be manually inputted or automatically generated by the system.

4. Tamper Protection / Reaction. The operator should be able to enable or disable tamper protection, and/or receive reports that inform the operator tampering is occurring with deployed AAC obstacle components.

5. Employed Life. Each nation will need to consider the mission life requirements based on likely defense scenarios including considerations of environmental conditions previously mentioned in paragraph 1.3.a. Typical and worst-case vehicle / personnel target activity and communication/message activity, should be considered in assessing the mission life requirements. Additionally, international policy may bound the maximum armed life.

6. Recover / Reseed. The AAC obstacle components should have the capability to be located, inspected, recovered, and repackaged or relocated to a new location.

1.2.5 Component Requirements.

1. Effector. Consideration should be made to ensure obstacles have a level of redundancy within the effectors so that performance will be maximized following single or multiple actions.

a. Effects.

(1) Lethality. AAC lethality is a combined function of the probability of encounter (e.g. effector density and lethal engagement area), the probability of hitting a target in a vulnerable area (e.g. sensing/targeting and firing accuracy), and the probability of kill (e.g. the impact of the effector against the target). These may vary depending on the specific AAC system component. The lethality performance may be measured using parameters such as armour penetration, blast, and fragmentation patterns.

(2) Non-Lethal. Non-lethal effectors provide several advantages over traditional lethal effects. Nations may choose to incorporate non-lethal effectors in order to address humanitarian issues. Also, non-lethal effectors can provide warning not to enter an area, and aide in the determination of intent to make an escalation of force decision. Lastly, modern technology allows non-lethal effects to provide innovative solutions to complex scenarios.

b. Effectiveness of system. AAC obstacle systems should be able to influence enemy manoeuver (e.g. encourage a bypass, or channel to engagement area) and / or serve as a force multiplier by increasing direct and indirect fire effectiveness due to the disruption to enemy manoeuver.

2. Sensor.

a. Situational Awareness. The below paragraphs describe the different levels of sensor performance potentially available for AAC obstacle systems. The sensor functions should be applicable within the boundaries of the obstacle, and on potential avenues of approach. The performance range for each sensor function will be system dependent and influenced by various environmental (e.g. wind, urban background noise, etc.) and target conditions (e.g. type vehicle, speed, etc.). Sensor performance parameters apply in both single and multi-target environments. A key trade-off to consider will be the balance between accuracy and latency of the sensor data. The operator should have the ability to ensure latency does not degrade AAC system effectiveness.

(1) Detection. The AAC sensors should be able to detect the presence of both personnel and / or vehicle movement.

(2) Tracking. The AAC sensors should be able to track personnel and / or vehicle movement and provide estimates of direction and speed.

(3) Classification. The AAC sensors should be able to classify and quantify personnel and / or vehicles (e.g. total number of people and / or tracked or wheeled vehicles, etc.).

(4) Identification. The AAC sensors should be able to identify the types of targets (e.g. T-72, BMP, etc.) in a multi-target environment.

(5) Positive Identification. The AAC sensors should be able to discriminate between enemy combatants, non-combatants, and friendly force.

(6) Target Reporting. The AAC sensors should be able to report the presence and total number of targets, report the engagement of targets, and report potential battle damage assessment (e.g. burning vehicles no longer moving, etc.).

(7) Advanced Engagement Techniques. The AAC sensors could be able to count target passes and therefore seek specific high value targets to engage (e.g. a breacher vehicle, main battle tank, etc.) or to increase disruption by attacking mid-formation.

3. C2.

a. Command and Control Station Functionality.

(1) Mission planning. Military forces operating in all types of environments, across the full spectrum of military operations

(i.e. offensive/defensive operations before, during and after hostilities), require capabilities for counter-mobility and survivability that enhance operational and tactical flexibility. AAC obstacle systems should be capable of achieving the same effects as traditional counter-mobility obstacles, while also combating emerging threats. Consequently, units should plan, site, employ and “fight” the AAC obstacle based on the principles of Combined Arms Obstacle Integration² and in accordance with (IAW) the Operations Order, Operational Plan, or ROE. The AAC obstacle should enable a unit’s ability to plan and execute counter-mobility and survivability tasks IAW the manoeuvre commander’s intent. Taking advantage of specific sensor and effector capabilities is an appropriate and effective means of terrain control and degradation of enemy combat effectiveness. Any mission planning software used in AAC obstacle systems should aid in determining the locations where AAC components should be emplaced on specific terrain, while ensuring communication connectivity within the AAC network. Mission planning requirements should promote emplacement of AAC obstacles with an effective density and breaching complexity to contribute to economy of effort and provide force multiplier effects.

(2) Reliability of Displayed State. The AAC obstacle system should display to the operator correct states / modes at a very high reliability. All operator generated commands, obstacle generated information and actions, and system displays should reflect the actual system status to the operator.

(3) Internal Interoperability. The AAC obstacle system should interoperate with other national C2 systems, ideally allowing automated timely AAC obstacle status reports to be filed across an all informed net.

(4) External Interoperability. The AAC obstacle system should be able to share information with and / or transfer data to other nations’ C2 systems. This will enable knowledge sharing within multi-national operations.

(5) Transfer Control. All AAC obstacle systems should comply with STANAG 2989, Transfer of Barriers. The ability of an emplacing unit to transfer AAC obstacle control to another unit and ideally another Nation, either physically or over a network should part of the AAC obstacle system design. The normal paradigm is that only one remote control station (RCS) can control an obstacle at any one time, however technology should allow any RCS to receive data and assume control of any AAC obstacle.

(6) Map Data. The RCS should be able to load background map data.

² Combined Arms Obstacle Integration. Planning tool to integrate direct and indirect fire, manoeuvre, engineer effort, and terrain.

(7) Establish Initial Control. Every operator will ensure control over the AAC obstacle as the first step after emplacement. Depending on the control system (e.g. wireless network, encoded initiation receiver, hardwired) military forces may need to ensure communication connectivity. This considers communication both within the AAC obstacle and to the RCS. The AAC obstacle is typically loaded with mission data and communication keys in a secure location. Once the obstacle is emplaced typical a RCS might establish a communications link with the emplaced AAC obstacle, transfer obstacle information (e.g. status and location) to a C2 system, and determine if any items did not respond during the network formation process.

(8) Recover / Reseed. The AAC RCS should have the capability to send a command to the AAC obstacle to enter state that makes it safe for recovery.

(9) System Recovery. The AAC obstacle system should have the ability to conduct system recovery following a system failure or reboot. Additionally, if the system communication is interrupted by external factors, a back-up C2 system should be considered as part of the system design.

(10) Commands, Reports, Requests, and Settings. There are two categories of messages in a typical AAC obstacle system. Messages are either operator initiated, or obstacle initiated. The following operator initiated AAC obstacle messages should be considered as part of AAC required capabilities. Every operator-initiated message should include status confirmation that the message was received and acted upon. Span of control (i.e. how many different AAC obstacles can be commanded by a single operator) should be considered in accordance with Nations' doctrine and trade-offs should be considered between functionality and financial constraints.

(a) Field / Node Configuration and Commands. Communication paths should be identifiable. Operators should be able to send commands to individual components, selected groups of components and/or entire obstacles. Example commands are:

- i. On / Off. This command will arm / disarm effectors and turn sensors on / off as directed by the operator. The Disarm function may allow safe passage of friendly forces. However, Nations may want to incorporate further design aspects that ensure friendly force safe passage.
- ii. Command neutralize / destruct.
- iii. Change self-destruct time.

- iv. Prioritization of target.
- v. Engage Target.
- vi. Anti-Tamper / Disturbance On / Off.
- vii. Change obstacle engagement effect.
- viii. Prioritization of data. In specific tactical situations the operator may both limit and prioritize alert messages from the obstacle.

(b) Obstacle Status Requests. The messages of the status request messages below are typical of what an operator would request from an AAC obstacle since the last time it was communicated with. There are potentially other status requests that Nations may desire.

- i. Obstacle Status. The status of every individual component of the obstacle should be reported back to the RCS operator.
- ii. Obstacle Diagnostics. An overall assessment of the density / health of the AAC obstacle, such as remaining battery life / time until self-destruct, and sensor surveillance and lethal coverage areas.
- iii. Built-In Test (BIT). Verification of AAC component functionality, potential identification of problems via fault codes, etc. This is more likely to occur shortly after initial obstacle employment, or turnover from another operator.

(11) Obstacle Initiated Messages. The following obstacle initiated AAC messages should be considered as part of AAC required capabilities.

- (a) Anti-Tamper / Disturbance. If capable of doing so, any AAC obstacle component should report that it is detected tampering / disturbance.
- (b) Contact Report. Personnel and vehicle movement in the vicinity. Increasing levels of sensor information may also be reported depending on sensor capabilities.
- (c) Effector has initiated.
- (d) Effector has self-destructed or dropped out of the network for an unknown reason.

- (e) Obstacle diagnostics when specific parameters are reached (e.g. battery life, field density, etc.).
- b. Network and Cyber Security.
- (1) Networking Protocols. The communication network's protocols (e.g. message formats and prioritization, communication synchronization, error recovery techniques, etc.) should be consistent with the appropriate NATO STANAGs.
 - (2) Network Status. The AAC obstacle system should have the ability to determine network status and display it to the operator at all times after emplacement.
 - (3) Connectivity and Range. The reliability, time required to connect, and communication range of the deployed AAC components, in both a benign environment and in the presence of threat countermeasures (e.g. jamming, etc.), are important requirement parameters to define early on in development. These factors will be influenced by different terrain, vegetation, and environmental conditions. The range of the network should be considered in terms of maximum reliable distances (operator to obstacle as well as between obstacle nodes) including tactical considerations like safety distances.
 - (4) Obstacle Network Size. The maximum number of components within the network should be identified early on in development. Generally, obstacle network size affects communication latency.
 - (5) Latency. The AAC network should aim to minimize latency of messages between the obstacle components and the operator. The operator's message turnaround time (the process required to send a message and get confirmation back the message was received), and obstacle-initiated message time, should be fast enough to achieve the commander's intent, in both a benign environment and in the presence of threat countermeasures (e.g. jamming, etc.).
 - (6) Bandwidth. The bandwidth to support AAC obstacle functionality should be adequate to provide required data in the network in a timely manner.
 - (7) Security and Information Assurance (Communication Security, Access Control, Computer Security). Controllable AAC obstacles will almost certainly require the identification of a person / location where a system administrative function is performed. The use and management of passwords, physical security requirements and techniques, cybersecurity

protections and techniques, etc. will fall within the responsibility of the system administrator and AAC operators.

(8) Detectability. The size and regularity of the electromagnetic (EM) signatures should be minimized with effective mitigation measures. The use of multiple frequencies and low probability of intercept techniques should be implemented to minimize EM countermeasures and signal location that may increase RCS operator vulnerability to threat fires.

INTENTIONALLY BLANK

CHAPTER 2 Testing Categories, Environments and Scenarios.

2.1 Aim.

The purpose of this chapter is to define the recommended categories, environments, and scenarios relevant to AAC obstacle system testing.

2.2 Definitions.

2.2.1 Categories.

1. The two testing categories are developmental and operational.

a. Developmental Testing. This encompasses measuring system performance in a realistic environment. It is focused on identifying technology maturity and its ability to meet individual system requirements. Successful developmental testing is normally an entry criterion for operational testing.

(1) Performance. Developmental performance testing seeks to lay out the various operational parameters that apply to measuring system effectiveness. For example, the list of target types, speeds, distances away from obstacle components, approach angles, etc. It is important to assess these variables and their impact on performance at both a component and a total system level. These component and system categories are listed below.

(a) Effectors. Measures effectiveness against defined targets. For example: penetration, or behind armour debris (BAD).

(b) Sensors. Measures ranges where sensor performance functions occur under different conditions. For example: range where detection, classification, and identification of targets takes place as a function of target type.

(c) C2. Measures network performance / communication range. For example: message turnaround time, C2 range from RCS to obstacle, reliability, latency, degradation in an E3 environment, cyber protection effectiveness, Cryptographic Module Validation Program (CMVP) (Crypto testing and integration with other systems), Information Warfare (Assurance), etc.

(d) Overall System. Measures integrated system performance that includes operation by soldiers or human-machine interactions. For example: includes all the above factors plus an assessment of dependencies that contribute to developing and fielding an effective

system. Also typically includes testing to assess the suitability of system training devices.

(2) Early User Trials with Soldiers (provides early feedback and user guidance). This is typically done during the Proof of Principle / Concept Assessment phase of a program, using mockup or prototype hardware. The focus is on influencing design decisions and maturing employment methods. It often includes the use of solder surveys and may only utilize target audience soldiers (Engineers or other soldiers that may be designated to employ AAC obstacle systems) rather than using a complete unit.

(3) Safety. Measures system safety during transport, emplacement, operation, and recovery. For example: sequential safety series; secure cargo vibration; hot / cold exposure cycle; loose cargo vibration (packaged and bare); drop test (packaged and bare), self-destruct mechanism, weapon effects, etc.

(4) Production. Measures the readiness of the production process prior to full rate production and confirms that production hardware is representative of the hardware that was taken through developmental and operational testing. For example, types of production readiness testing include Production Verification Test (PVT), First Article Test (FAT), and Quality Assurance (QA) during production.

2. Operational Testing. This encompasses early user trials and unit level testing with soldiers in a force-on-force environment. It normally includes portrayal of both friendly and threat forces. Successful operational testing is normally an entry criterion for production and fielding. Operational testing is generally categorized as follows:

a. Force Development Test and Experimentation (FDT&E) with functional, representative hardware conducted with soldiers using mission-based scenarios in a force on force environment. This is the first opportunity for realistic testing with a unit in a force on force environment.

b. Limited User Test (LUT) with functional, representative hardware conducted with a combined arms element using mission-based scenarios in a force on force environment. This is recommended instead of the operational test below for a relatively simple AAC obstacle system, and typically does not include manoeuver and fires units. However, combined arms obstacle integration with a staff element is important to include.

c. Initial Operational Test and Evaluation (IOT&E) with functional, representative hardware conducted with a combined arms element using mission-based scenarios in a force on force environment. This is typically a threat force with its equipment going against a friendly force with its equipment. The

AAC obstacle system is fully integrated with manoeuvre forces, fires, and intelligence, surveillance, and reconnaissance (ISR) assets.

2.2.2 Environments.

1. The following categories are examples of the environments that the performance of AAC obstacle systems should be assessed in. Some environments may need to be simulated as they are not regularly encountered like salt fog, ice, rain/water intrusion, etc.

a. Climate. Nations should ensure they test components in the harshest environments where they are likely to deploy / transport their AAC obstacle system. The parameters for these climatic variables are described in AECTP 230 - Climatic Conditions and this policy can be used to guide testing. The different components of the AAC obstacle system will potentially be affected to different extremes in different climatic conditions. For example, the power supply for the obstacle subsystem may be degraded in cold climates.

b. Terrain. Terrain includes both natural and manmade characteristics. Natural terrain includes mountainous, forest, open, desert, jungle, etc., and altitude should also be considered. Manmade terrain includes infrastructure, subterranean, and urban environments, host nation and military forces electromagnetic transmissions, etc

c. Transportation and Storage. AAC obstacle systems may be stored in ammunition supply points, etc., over many years, and may be stored in uncontrolled storage for months at a time before emplacement. Therefore it is important to test in accelerated storage testing both the effectiveness of the packaging and the availability of the system components over time. Transportation includes air, sea, rail, and road modes, and the forces the AAC obstacle system may be exposed to.

d. Electromagnetic Environmental Effects (E3). The effects of all sources of E3 on both packaged and unpackaged AAC obstacle systems should be assessed during testing. Examples include: External RF Electromagnetic Environment (EME); Electromagnetic Interference (EMI) / Electromagnetic Compatibility (EMC); Hazards of Electromagnetic Radiation to Ordnance (HERO); Hazards of Electromagnetic Radiation to Personnel (HERP); Near Strike Lightning (NSL); Electromagnetic Pulse (EMP); and Electrostatic Discharge (ESD).

2.2.3 Scenarios.

1. Each nation will determine which scenarios and AAC obstacle system emplacement missions are of greatest importance / most likely to occur. It is

recommended that operational testing focus on these priority missions. The following are the primary scenarios, previously identified in chapter 1, paragraph 2.c.

- a. Counter-mobility.
 - (1) Area denial.
 - (2) Route denial.
- b. Survivability.

CHAPTER 3 Technical Component and System Testing.

3.1 Aim.

The purpose of this chapter is to recommend the methods and metrics for conducting testing to assess components and AAC obstacle system performance.

3.2 Overview of Test Planning.

1. One of the first tasks in developing the test plan is to produce a matrix that assigns the requirements to specific test events. This confirms the source of data that is used to assess whether that requirement was met or not. An example of an AAC obstacle system Employment Task List for use in operational testing is found in Annex A. An example of an AAC Obstacle System Test Matrix for use in developmental test planning is found in Annex B. Once the test matrix is completed, the next step should be determining the hardware requirements needed to execute each test event.

a. Test Event Planning. Test locations, resource requirements, data collection forms, test team membership, and other test execution enablers should be identified as early as possible. Additionally, opportunities to collect data in a combined test event should be identified to reduce the cost and length of testing. For example, identification of the AAC effector safety template is important to ensure the test range location can accommodate testing.

b. Test Hardware Planning. The configuration description of the C2 system is critical to allocate hardware quantities required for performance and operational testing in relevant environments (i.e. tropic, cold, hot, and urban). For example, determining the quantities of sensors and effectors to be employed in an AAC obstacle, and need for spares if items become non-serviceable, is important to support operational test realism and avoid delays in testing.

c. Limitations. Each nation should assess the restrictions and limitations of testing imposed upon them and record them within the testing report. These limitations may impact the test design.

3.3 Developmental Test Events, Scope of Testing, and Basic Scenarios

The effectiveness for an AAC obstacle system should be demonstrated using live munitions against representative targets. Various modes of operation should be used to demonstrate the level of autonomy and soldier in the loop control.

3.3.1 Effectors.

1. AAC effectors should be tested against representative targets according to the system's requirement.

- a. **Effect on Target.** For example, effector performance against a self-protection device (e.g. mine roller) and a tracked or wheeled vehicle target should both be part of effector performance testing. The effector performance should measure both static attacks (e.g. rolled homogeneous armour (RHA) perforation testing) and dynamic attacks (e.g. against moving targets). Effector performance is a function of where it hits on the target, penetration of the target, and effects after penetration, and should also be assessed in testing. The frequency of attack locations across the target should be recorded to characterize performance. This is true for potential bottom attack, side-attack, and top attack munitions.
- b. **Effector Dependency.** For example, if the effector is initiated by a message from a sensor or the RCS, both methods should be tested to characterize effector performance.
- c. **Effector Safety Distances.** During testing hazardous distances should be assessed to establish collateral damage estimates and inform safety distances.

3.3.2 Sensors.

1. The AAC sensor testing should assess the ability to generate an accurate target report to the control station in a timely manner. An important aspect of data collection assessment is to record how well the AAC sensor discriminates targets in a complex operational environment (e.g. in the presence of battlefield noise, in a multi-target environment, in various weather conditions, etc.). If the sensor is queuing an effector to attack a target, or another sensor to provide enhanced fidelity, the sensing timelines and activation period for the effectors and additional sensors should be considered to ensure enough time exists to produce the desired outcome.
 - a. **Sensing Capability.** Stand alone and / or munition integrated sensing capability should be assessed in terms of performance at ranges for sensing functions for single and multiple targets. For each potential sensor function (Detect, Track, Classify, Identify, Positive Identification, and Battle Damage report) the ranges where those determinations occur should be recorded for each relevant operational environment. For example, sensor performance in an urban or jungle environment may be significantly degraded versus its performance in open and rolling terrain. Collecting this information will help inform obstacle planning and component spacing during emplacement.
 - b. **Sensor Reporting.** The AAC sensors ability to deliver reports to the AAC C2 system should be assessed in testing. These reports should provide real time target classification and deliver the necessary information to confidently engage the targets. The accuracy of sensor reports should also be recorded (e.g. total number of targets, target misclassifications, etc.).

3.3.3 Command and Control (C2).

1. Testing should be performed to measure the ability of the AAC operator to establish control over an emplaced AAC obstacle, send required commands and maintain control, receive obstacle reports, and perform in a reliable and timely fashion (i.e. command message completion rate and latency). The following C2 capabilities should be tested but potential capabilities are not limited to the following: network initialization, arm / disarm, on / off, command neutralize / destruct, change self-destruct time, prioritize targets, engage targets, change anti-tamper / disturbance, change obstacle engagement effect, request field/network status, transfer of control, and safe obstacle for recovery. Some of these command functions may include the ability of the user to receive a confirmation of status.

2. The following table lists the major recommended C2 functions that should be assessed during developmental testing. Both the transmission and receipt of messages should be recorded (successful or unsuccessful).

Example C2 Functions	Transmit	Receive
Establish Initial Control		
System Performance (Stand-by)		
System Performance (On / Off)		
Command Destruct		
Change Self-Destruct Time		
Command Fire / Launch Effector		
Transfer Control		
Take Control		
Commands & Settings		
Status Requests and Reports		
Operator Initiated Effects (Anti-Vehicle)		
Operator Initiated Effects (Anti-Personnel)		
Create C2 Groups Within The Same Obstacle		
Safe Obstacle For Recovery		
Reseed and Reconfigure C2 Network		
Shut Down		

Table 2. List of example C2 functions to be assessed

3.3.4 Overall System Testing and Effectiveness Assessment.

1. Effectiveness Metrics. The effectiveness of an AAC obstacle system can be measured and assessed in two ways: modeling and simulation using realistic / nationally-approved scenarios, and during force-on-force operational testing using kill assessment tools (e.g. MILES, etc.). The recommended scenario-based modeling and simulation prerequisite is to first have system effectiveness modeling completed using accurate system performance data. This data is obtained during developmental testing, including live fire testing. Both the scenario based, and system effectiveness models require inputting representative target characteristics (e.g. vehicle vulnerability maps).

2. **Battlefield Effects.** It is not enough to only examine obstacle kills as a metric for assessing AAC performance. Assessment in a combined arms environment that includes over watching fires and manoeuvre is the recommended metric to assess the battlefield impact of employing AAC obstacles. Enemy losses, friendly losses, and the outcome of the battle should be assessed compared to a scenario with no AAC obstacle systems or legacy AAC systems, in order to truly assess AAC effectiveness.
3. **Maintenance.** Maintenance tasks, the level at which they should be performed, the required time to perform the tasks, the equipment required to perform the task, the ease of performing the task, and identifying components that are suitable for repair vs. complete replacement should be assessed during AAC testing.
4. **Additional System Development Tests.** The following are further recommended considerations for testing:
 - a. **C2 Tests:** Information Security, Human Factors Engineering (HFE), Software Testing, Interoperability, etc.
 - b. **Obstacle Tests:** Mission Life Testing, Logistics Preparation Activity Testing (unpacking, munition and C2 system preparation, re-packing munitions, etc.), Air Drop Delivery (Pallet), HFE, etc.
 - c. **Exposure Tests:** Directed Energy Weapon (DEW), Electronic Warfare, Cyber Security, Chemical, Biological, Radiological, and Nuclear (CBRN), Overpressure & Noise, Toxic Fumes, etc.
 - d. **Technical manual verification.**

3.4 Operational Testing.

1. **Operational testing supports force development and materiel development processes by examining the effectiveness of existing or proposed concepts of doctrine, training, and materiel.** These tests are normally the first time that soldiers in a small unit equipped with AAC components operate the system in a tactical environment.
 - a. **Events Scopes and Scenarios.** The operational tests are intended to address the ability of the soldier to use the AAC obstacle system in a field environment with varying terrain and vegetation. Soldiers should use the system based on developed counter-mobility doctrine. The user trials should include mission preparation, pre-emplacement, emplacement, obstacle management / control, and clearance or recovery / redeployment of the system. The test events should include the emplacement and control of multiple AAC systems, either individually or connected as a larger system, of varying sizes, configurations and locations in order to test the doctrinal Mission Effects of counter-mobility (disrupt, fix, turn, and block). Nations should determine where on the spectrum of conflict

they would like to test the AAC system (Major Combat operations, stability operations, etc.) as this decision affects all aspects of obstacle planning and what threat forces / equipment and TTPs will be portrayed in the operational test event

b. Field Emplacement and Recovery. Operational testing (with Soldiers in a force-on-force environment) should address the preparation activities associated with the system (unpackaging, transport, communication establishment, etc.), system emplacement activity (effectors, sensors, fencing, etc.), and recovery (locating, inspecting, repackaging or transport to another location). Recording emplacement times during operationally testing will help inform the development of obstacle planning factors.

c. Detectability of Components. Effector and sensor detectability ranges by mounted and dismounted threat forces should be assessed during operational testing.

d. Testing Resource Requirements. Battlefield effects simulation for collective training (e.g. MILES, TES, AGDUS) could be used during this test events to enhance evidence capture.

INTENTIONALLY BLANK

Annex A. AAC Employment Task List

Service Index	Service Name	AAC System Components			Comments
		Sensor	Effector	C2	
Activity 1	Operational Deployment				
1.1	Determine system configuration	X	X	X	Conduct Terrain analysis
1.2	Determine packaging requirements/ constraints	X	X	X	Conduct Terrain analysis
1.3	Create transportation/ loading plan				Conduct Terrain analysis
1.4	Plan validation/ acceptance				Conduct Terrain analysis
1.5	Coordinate loading				Conduct Terrain analysis
1.6	Coordinate transportation				Conduct Terrain analysis
1.7	AAC system and camouflage gathering	X	X	X	
1.8	AAC system and camouflage loading	X	X	X	Air/sea/land
1.9	AAC system and camouflage transportation	X	X	X	
1.10	AAC system and camouflage unloading and unpacking	X	X	X	
Activity 2	Tactical deployment				
2.1	Determine sensor location			X	Conduct Terrain analysis
2.2	Determine effector location			X	Conduct Terrain analysis
2.3	Determine C2 Location			X	Conduct Terrain analysis
2.4	Determine communication elements location			X	Conduct Terrain analysis
2.5	Determine camouflage requirements	X	X	X	Conduct Terrain analysis
2.6	Plan validation/ acceptance				Conduct Terrain analysis
2.7	Coordinate loading				Conduct Terrain analysis
2.8	Coordinate transportation				Conduct Terrain analysis
2.9	AAC system and camouflage gathering	X	X	X	
2.10	AAC system and camouflage loading	X	X	X	Air/sea/land
2.11	AAC system and camouflage transportation	X	X	X	
2.12	AAC system and camouflage unloading and unpacking	X	X	X	
Activity 3	Deploy AAC components at Base Camp				
3.1	Visual check of component serviceability	X	X	X	By one person
3.2	Carry component to designated location	X	X	X	By one person

Service Index	Service Name	AAC System Components			Comments
		Sensor	Effector	C2	
3.3	Emplace sensors/ effectors	X	X	X	By one person
3.4	Record/ save component location on C2	X	X	X	Automatically or manually
3.5	Emplace C2 component			X	By one person
3.6	Emplace communication elements			X	By one person
3.7	Calibrate components	X	X	X	By one person
3.8	C2 configuration			X	By one person
3.9	Establish communication network			X	
3.10	Connect/integrate system components together	X	X	X	
3.11	Connect AAC system with external systems			X	
3.12	Conduct individual component Build in test	X	X	X	
3.13	Camouflage and secure AAC system	X	X	X	Use techniques to protect system against intrusion (crypto, passwords, frequency hopping) and jamming (capable of operating in friendly or enemy ECM environment)
3.14	Data exchange services with existing external systems			X	
Activity 4	AAC operator training				
4.1	Establish training environment	X	X	X	
4.2	Establish training configuration	X	X	X	On a deployed AAC components
4.3	Provide training courses/ content			X	
4.4	Conduct training activities	X	X	X	
4.5	Evaluate training results			X	
4.6	Present training results			X	
4.7	Report training results			X	
Activity 5	Test AAC system				
5.1	Turn on each component	X	X	X	By one person
5.2	Test each component	X	X	X	By one person
5.3	Turn on the AAC system			X	By one person
5.4	Communication test	X	X	X	
5.5	Configuration test	X	X	X	

Service Index	Service Name	AAC System Components			Comments
		Sensor	Effector	C2	
5.6	AAC system test			X	
5.7	Notify about faulty components			X	
5.8	Retest failed components	X	X	X	By one person
5.9	Retest AAC system			X	By one person
5.10	Report test results			X	
Activity 6	Activate AAC System				
6.1	Activate each component	X	X	X	By one person
6.2	Activate communication			X	By one person
6.3	Activate AAC system			X	By one person
6.4	Report activation status			X	
Activity 7	Data distribution and recording				
7.1	Define and distribute data	X	X	X	
7.2	Send and record data according to defined configuration rules	X	X	X	
7.3	Receive confirmation			X	
7.4	Report faults			X	
7.5	Redistribute data	X	X	X	
7.6	Report distribution status			X	
Activity 8	Defined area monitoring				
8.1	Events monitoring (continuous activity)			X	
8.2	Events validation			X	
8.3	Events notification			X	
8.4	Regular reports (events, actions)			X	
Activity 9	Detecting Target entering the area				
9.1	Sensor detects an event	X			
9.2	Sensor sends the message to C2	X		X	
9.3	C2 presents an event			X	
9.4	Sensor/ C2 validates the alert	X		X	
9.5	Sensor determines location of the target	X			
9.6	Sensor sends location data to C2	X		X	
Activity 10	Classifying the target				

Service Index	Service Name	AAC System Components			Comments
		Sensor	Effector	C2	
10.1	Sensor evaluate the target with its own logic	X			
10.2	Sensor evaluates the target with other sensors	X		X	
10.3	Sensor sends initial evaluation to C2	X		X	
10.4	C2 may initiate additional sensor to evaluate the target	X		X	
10.5	C2 provides the information to operator to conduct confirmation of target			X	
10.6	Information about target classification distributed to other C2 components.	X	X	X	
Activity 11	Identify the target				
11.1	Sensor recognizes the target	X			
11.2	Sensor provides initial target data to C2	X		X	
11.3	C2 presents information about the initial target ID			X	
11.4	C2 may initiate an additional sensor to identify the target	X		X	
11.5	Information about the target ID distributed to other C2 components	X	X	X	
Activity 12	Tracking the target				
12.1	C2 sends a message to initiate target tracking	X	X	X	
12.2	The sensor and effector tracks the target	X	X		Automatically or manually
12.3	The sensor and effector continuously provides information about the target to C2	X	X	X	
12.4	C2 initiates recording			X	
12.5	C2 may stop the tracking	X	X	X	
Activity 13	Engaging the target				
13.1	C2 decides on the method of engagement			X	
13.2	C2 decides to engage the target			X	
13.3	C2 sends the target coordinates to the effector		X	X	
13.4	C2 engage the target using its effectors		X	X	
13.5	C2 tracks the target	X	X	X	
Activity 14	Battle damage assessment				

Service Index	Service Name	AAC System Components			Comments
		Sensor	Effector	C2	
14.1	Sensors transmit the results of the engagement	X		X	
14.2	Sensors check the target	X		X	
14.3	C2 presents the results to the operator			X	
14.4	C2 registers the battle damage assessment completed by the user			X	
14.5	C2 stops recording system			X	
Activity 15	Replenishment				
15.1	C2 notifies about components that need replenishment	X	X	X	
15.2	Components are being replenished	X	X	X	By one person
15.3	Replenished components are tested	X	X	X	By one person
15.4	Replenished components are activated	X	X	X	By one person
15.5	C2 presents the status of AAC system			X	
Activity 16	AAC elements monitoring				
16.1	C2 checks AAC components status	X	X	X	Including anti-jamming/ -tampering status
16.2	C2 reports AAC components failure			X	
16.3	C2 presents AAC components status			X	
Activity 17	AAC elements replacement				
17.1	C2 detects AAC element to be replaced			X	
17.2	C2 reports AAC element to be replaced			X	
17.3	AAC element replaced	X	X	X	By one person
17.4	C2 checks AAC replaced element status	X	X	X	
17.5	C2 presents AAC replaced element status			X	
Activity 18	AAC elements repair/ calibration				
18.1	C2 detects AAC element to be repaired/ calibrated	X	X	X	
18.2	C2 reports AAC element to be repaired/ calibrated			X	
18.3	AAC elements repaired-recalibrated	X	X	X	By one person
18.4	C2 checks repaired/calibrated element status	X	X	X	
18.5	C2 presents repaired/ calibrated element status			X	
Activity 19	AAC system reconfiguration				
19.1	C2 changes status to maintenance mode			X	

Service Index	Service Name	AAC System Components			Comments
		Sensor	Effector	C2	
19.2	C2 presents current configuration			X	
19.3	C2 provides user interface to change current configuration			X	
19.4	C2 presents changed configuration			X	
19.5	C2 distributes changed configuration	X	X	X	
19.6	C2 reports reconfiguration status			X	
19.7	C2 changes status to production mode			X	
Activity 20	AAC				
20.1	C2 changes status to maintenance mode			X	
20.2	Turn off each element	X	X	X	
20.3	Disassembly of AAC components	X	X	X	By one person
20.4	Turn off C2			X	
Activity 21	Miscellaneous reporting events				
21.1	C2 provides reports about AAC events			X	Including recorded data
21.2	C2 notifies about AAC events according to defined rules			X	

Annex B. Example AAC Operational and Developmental Test Matrix

Test Type	Target #	Scenario	Vehicle Start	Vehicle Speed (kph)	Vehicle Closest Point of Approach (m)	Mode / State / Notes / Comments	Notes All times are in Zulu
C2		C2:Establish Initial Control	---	---		Standby (Default)	When prompted, send obstacle report
C2		State / Mode Change	---	---		DisArm-SenOff	
C2		State / Mode Change	---	---		Arm-Man	
Sensor	AT-1	Armoured Tank (AT)	Left to Right	30	TBD	Arm-Man	
Sensor	AT-1	Armoured Tank	Right to Left	30	TBD	Arm-Man	
C2		C2: Scenario 6B	---	---		Arm-Man	
C2		State / Mode Change	---	---		Arm-Auto	
Effector	AT-1	Armoured Tank	Left to Right	30	TBD	Arm-Auto	
Effector	AT-1	Armoured Tank	Right to Left	30	TBD	Arm-Auto	
Effector	AT-1	Armoured Tank	Left to Right	45	TBD	Arm-Auto	
Effector	AT-1	Armoured Tank	Right to Left	45	TBD	Arm-Auto	
C2		C2: Proof Field (10)	---	---		Arm-Auto	
C2		C2: Scenario 6B	---	---		Arm-Auto	
C2		State / Mode Change	---	---		DisArm-SenOff	
C2		State / Mode Change	---	---		Recover	Recover, physical checkout
C2		C2:Establish Initial Control	---	---		Standby (Default)	
C2		State / Mode Change	---	---		DisArm-SenOff	
C2		C2 Scenario	---	---		Self Protection	
						SD/SDA Timer	
						System Fail / Loss Comms	
C2		State / Mode Change	---	---		Arm-Auto	
Sensor	LW-1	Light Wheel (LW) (armoured)	Left to Right	30	TBD	Arm-Auto	

Sensor		Light Wheel (armoured)	Right to Left	30	TBD	Arm-Auto	
C2		State / Mode Change	---	---		Arm-Man	
C2		C2: Manual Effects (7)	---	---		Arm-Man	Manually fire
C2		State / Mode Change	---	---		DisArm-SenOff	
C2		State / Mode Change	---	---		Recover	Recover munition for the day
Day 2							
C2		C2:Establish Initial Control	---	---		Standby (Default)	When prompted, send obstacle report
C2		State / Mode Change	---	---		DisArm-SenOff	
C2		State / Mode Change	---	---		Arm-Man	
Sensor	LT-1	Light Track (LT) APC (Armoured)	Left to Right	45	TBD	Arm-Man	
Sensor	LT-1	Light Track APC (Armoured)	Right to Left	45	TBD	Arm-Man	
C2		C2: Scenario 6B	---	---		Arm-Man	
C2		State / Mode Change	---	---		Arm-Auto	
Effector	LT-1	Light Track APC (Armoured)	Left to Right	30	TBD	Arm-Auto	
Effector	LT-1	Light Track APC (Armoured)	Right to Left	30	TBD	Arm-Auto	
Effector	LT-1	Light Track APC (Armoured)	Left to Right	45	TBD	Arm-Auto	
Effector	LT-1	Light Track APC (Armoured)	Right to Left	45	TBD	Arm-Auto	
C2		C2: Proof Field (10)	---	---		Arm-Auto	
C2		C2: Scenario 6B	---	---		Arm-Auto	
C2		State / Mode Change	---	---		DisArm-SenOff	
C2		State / Mode Change	---	---		Recover	Recover, physical checkout
C2		C2:Establish Initial Control	---	---		Standby (Default)	
C2		State / Mode Change	---	---		DisArm-SenOff	
C2		C2 Scenario	---	---		Self Protection	
						SD/SDA Timer	
						System Fail / Loss Comms	

C2		State / Mode Change	---	---		Arm-Auto	
Sensor	LT-1	Light Track APC (Armoured)	Left to Right	30	TBD	Arm-Auto	
Sensor	LT-1	Light Track APC (Armoured)	Right to Left	30	TBD	Arm-Auto	
C2		State / Mode Change	---	---		Arm-Man	
C2		C2: Manual Effects (7)	---	---		Arm-Man	Manually fire
C2		State / Mode Change	---	---		DisArm-SenOff	
C2		State / Mode Change	---	---		Recover	Recover munition for the day
Day 3							
C2		C2:Establish Initial Control	---	---		Standby (Default)	When prompted, send obstacle report
C2		State / Mode Change	---	---		DisArm-SenOff	
C2		State / Mode Change	---	---		Arm-Man	
Sensor	LW-2	Light Wheel (LW) (armoured)	Left to Right	30	TBD	Arm-Man	
Sensor	LW-2	Light Wheel (armoured)	Right to Left	30	TBD	Arm-Man	
C2			---	---		Arm-Man	
C2			---	---		Arm-Auto	
Effector			Left to Right	15	TBD	Arm-Auto	
C2			---	---	TBD	Arm-Man	Vehicles go back
C2			---	---		Arm-Auto	
Effector			Left to Right	15		Arm-Auto	
C2			---	---	TBD	Arm-Man	Vehicles go back
C2			---	---		Arm-Auto	
Effector			Left to Right	15	TBD	Arm-Auto	
C2			---	---	TBD	Arm-Auto	
C2			---	---		Arm-Auto	

C2			---	---		DisArm-SenOff	
C2			---	---		Recover	Recover, physical checkout
C2			---	---		Standby (Default)	
C2			---	---		DisArm-SenOff	
C2			---	---		Self Protection	
					SD/SDA Timer		
					System Fail / Loss Comms		
C2			---	---		Arm-Auto	
Sensor	LT-2	Light Track APC (Armoured)	Left to Right	30	TBD	Arm-Auto	
Sensor	LT-2	Light Track APC (Armoured)	Right to Left	30	TBD	Arm-Auto	
C2			---	---		Arm-Man	
C2			---	---		Arm-Man	Manually fire
C2			---	---		DisArm-SenOff	
C2			---	---		Recover	Recover munitions for the day
C2			---	---		Standby (Default)	When prompted, send obstacle report
C2			---	---		DisArm-SenOff	
C2			---	---		Arm-Man	
Sensor	LT-2	Light Track APC (Armoured)	Left to Right	30	TBD	Arm-Man	
Sensor	LT-2	Light Track APC (Armoured)	Right to Left	30	TBD	Arm-Man	
C2			---	---		Arm-Man	
C2			---	---		Arm-Auto	
Effector	AB-1	Armoured Breacher (AB)	Left to Right	30	TBD	Arm-Auto	
Effector	AB-1	Armoured Breacher	Right to Left	30	TBD	Arm-Auto	
Effector	LT-2	Light Track APC (Armoured)	Left to Right	30	TBD	Arm-Auto	
Effector	LT-2	Light Track APC (Armoured)	Right to Left	30	TBD	Arm-Auto	
C2			---	---		Arm-Auto	
C2			---	---		Arm-Auto	

C2			---	---		DisArm-SenOff	
C2			---	---		Recover	Recover, physical checkout
C2			---	---		Standby (Default)	
C2			---	---		DisArm-SenOff	
C2			---	---		Self Protection	
					SD/SDA Timer		
					System Fail / Loss Comms		
C2			---	---		Arm-Auto	
Sensor	LW-2	Light Wheel (armoured)	Left to Right	30		Arm-Auto	
Sensor	LW-2	Light Wheel (armoured)	Right to Left	30		Arm-Auto	
C2			---	---		Arm-Man	
C2			---	---		Arm-Man	Manually fire
C2			---	---		DisArm-SenOff	
C2			---	---		Recover	
C2			---	---		Standby (Default)	
C2			---	---		DisArm-SenOff	
C2			---	---		Arm-Man	
Sensor	LW-2	Light Wheel (armoured)	Left to Right	30		Arm-Man	
Sensor	LW-2	Light Wheel (armoured)	Right to Left	30		Arm-Man	
C2			---	---		Arm-Man	
C2			---	---		Arm-Auto	

NATO UNCLASSIFIED

APP-34(A)(1)

NATO UNCLASSIFIED