NATO STANDARD

AEP-4818 Vol. VI

ROBOTICS AND AUTONOMOUS SYSTEMS – GROUND (RAS-G) INTEROPERABILITY PROFILE (IOP): COMMUNICATIONS PROFILE

Edition A Version 1
FEBRUARY 2023

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

22 February 2023

1. The enclosed Allied Engineering Publication AEP-4818 Vol. VI, Edition A, Version 1 ROBOTICS AND AUTONOMOUS SYSTEMS – GROUND (RAS-G) INTEROPERABILITY PROFILE (IOP): COMMUNICATIONS PROFILE, which has been approved by the nations in the NATO ARMY ARMAMENTS GROUP (AC225 NAAG), is promulgated herewith. The agreement of nations to use this publication is recorded in STANREC 4818.

2. AEP-4818 Vol. VI, Edition A, Version 1 is effective upon receipt.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (https://nso.nato.int/nso/) or through your national standardization authorities.

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

Dimitrios SIGOULAKIS
Lieutenant General, GRC (A)
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 Document 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 Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

CHAPTER 1 SCOPE

1.1 PURPOSE

This document defines the interfaces and attributes of the communications link to be used on Unmanned Ground Vehicles (UGVs). For the purposes of this document, communications interfaces to support multiple Operator Control Units (OCUs) and multiple platforms will be described in addition to point-to-point interface between the OCU and the platform that were addressed in previous versions of the Communications IOP. The intent of this document is to allow for a wide variety of product differentiation that can be adapted to multiple applications and usage models supporting unmanned ground systems. The end goal of this document product is to define the physical, electrical and logical interfaces of the radio systems to be plug and play to meet the need of the mission. It is not the intention of this document to provide all requirements necessary for implementation thereof but to provide a standard for on-board and off-board communications links of UGV systems.

1.2 DOCUMENT OVERVIEW

This document provides the base concepts, architecture, requirements, and overview for the communications Interoperability Profile. The document is organized into five sections:

1. Scope
2. Source documents
3. Background
4. Software Attributes
5. Hardware Attributes

This document also includes two appendices (Sections 6 and 7) which include, respectively, Acronyms/Abbreviations and technical discussions from the Communications IOP Working Groups with recommendations based on group discussions and trade studies.

The Common Communications Link (CCL) will be a term used throughout this document to describe the interoperable communications system between UGV platforms and OCUs. It is not the intent of this document to restrict the radio capability in any way outside common interface and operational mode.

1.3 CURRENT STATE OF UGV COMMUNICATIONS

The radios used on UGVs vary from platform to platform. Some of these transmit video and telemetry with separate radios and different frequency bands, while others provide a single radio to handle all wireless communications between the controller and platform. In addition, most radios are limited to a single frequency band making it difficult to use the radio in some countries to which these UGVs are deployed. These unique configurations of radios on unmanned systems make sustainment difficult and costly.

Radios must move to a standard that is interoperable so that radios can transmit and receive communications to and from any UGV and be adaptable for deployment worldwide.

UGV radio communications are largely commercial-off-the-shelf (COTS) based, closed loop, point to point links between the UGV and the controller. Generally, the UGV communications data link can be broken down to two types; the control link and video/payload sensor link. Some UGV systems keep these data links separate by employing two radios, one to handle video and the other for control and status supporting data and audio. The video link is one-way from the UGV to the controller and requires higher data rates than the control data link.

UGVs use COTS radios due to their availability at low cost in a Small Form Factor (SFF) with low weight and low power. However, the communications system hardware is largely different from one platform to another, making support expensive and difficult in the field. This issue is compounded by spectrum supportability and the lack of compatibility with radio frequency jamming systems that affect frequency bands used by COTS radios. To counter or mitigate these factors as much as possible, the UGV spectrum dependent (S-D) equipment will be required to obtain, or have, Stage 4, Equipment Spectrum Certification (ESC). Higher frequencies do not propagate as well as lower frequencies (particularly in non-Line-of-Sight (NLOS) conditions) and where low antenna heights of the controller and UGV are less than six feet above ground level. To mitigate the degradation of radio signal due to multipath while supporting high data rates, some UGV systems employ Orthogonal Frequency Division Multiplexing (OFDM) or Coded Orthogonal Frequency Division Multiplexing (COFDM) waveforms which have favorable radio performance in a multipath environment.

1.4 V1 Capabilities

The Communications IOP defines a baseline of interoperable capabilities supporting RAS-G systems. Some of the notable capabilities include Comms Lost, Off-Board Networking, Network Timing, Waveform guidance, authentication and authorization content and antenna physical connection attribute.

CHAPTER 2 SOURCE DOCUMENTS

The following documents are referenced within this IOP and shall be used to implement the requirements contained within the IOP.

2.1 GOVERNMENT DOCUMENTS

ID	Document
1011-I-2.0	NIST Special Publication, Autonomy Levels for Unmanned Systems (ALFUS) Framework Volume I: Terminology, Version 2.0, October 2008.
MIL-STD-348B	Interfaces, Radio Frequency Connector, Coaxial, Triaxial and Twinaxial
MIL-STD-461	Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment.
MIL-STD-464	ELECTROMAGNETIC ENVIRONMENTAL EFFECTS REQUIREMENTS FOR SYSTEMS
MIL-STD-810G	Environmental Engineering Considerations and laboratory test
MIL-HDBK-189	Reliability Growth Management
MIL-HDBK-338B	Electronic Reliability Design Handbook
MIL-PRF-39012	General Specification For Connectors, Coaxial, Radio Frequency
MIL-PRF-55339	General Specification For Adapters, Connectors, Coaxial, Radio Frequency, (Between Series and Within Series)

2.2 NON GOVERNMENT DOCUMENTS

ID	Version	Document
IEEE802.3-2008	1.0	Standards for Ethernet based LANs
AS5669A	Rev A	SAE Aerospace Standard, JAUS/SDP Transport Specification
AS5710A	Rev A	SAE Aerospace Standard, JAUS Core Service Set
TIA_EIA-232_485	1.0	Electronic Industries Association/Telecommunication Industry Association TIA/EIA-232/485 and ITU V.28 (generally referred to as 232).
USB-Forum	1.0	Universal Serial Bus Forum control standards
RFC791	1.0	Internet Protocol DARPA Internet Program Protocol Specification (IPv4)
RFC2460	1.0	Internet Protocol, Version 6 (IPv6) Specification
RFC2131	1.0	Dynamic Host Configuration Protocol
RFC2132	1.0	DHCP Options and BOOTP Vendor Extensions
RFC3315	1.0	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC4604	1.0	Using IGMPv3 and MLDv2 for Source-Specific Multicast
RFC4861	1.0	Neighbor Discovery for IP version 6 (IPv6)
RFC4862	1.0	IPv6 Stateless Address Auto-configuration (obsoletes RFC 2462)
RFC6144	1.0	Internet Protocol, Framework for IPv4/IPv6 Translation

CHAPTER 3 BACKGROUND

3.1 CCL ATTRIBUTE

Parent Attribute: IOP Usage

The role of the CCL is provide an open and secure communications link between the OCU and the UGV platform, with minimal latency. It is also the role of the CCL to provide network management services in support of the communications link.

The CCL systems block architecture as shown in Figure 1: CCL Systems Block Architecture below depicts the general components of the CCL and serves as a baseline for the organization and discussion of technical requirements. The router with a DHCP server is an optional component of the radio system within the CCL framework.

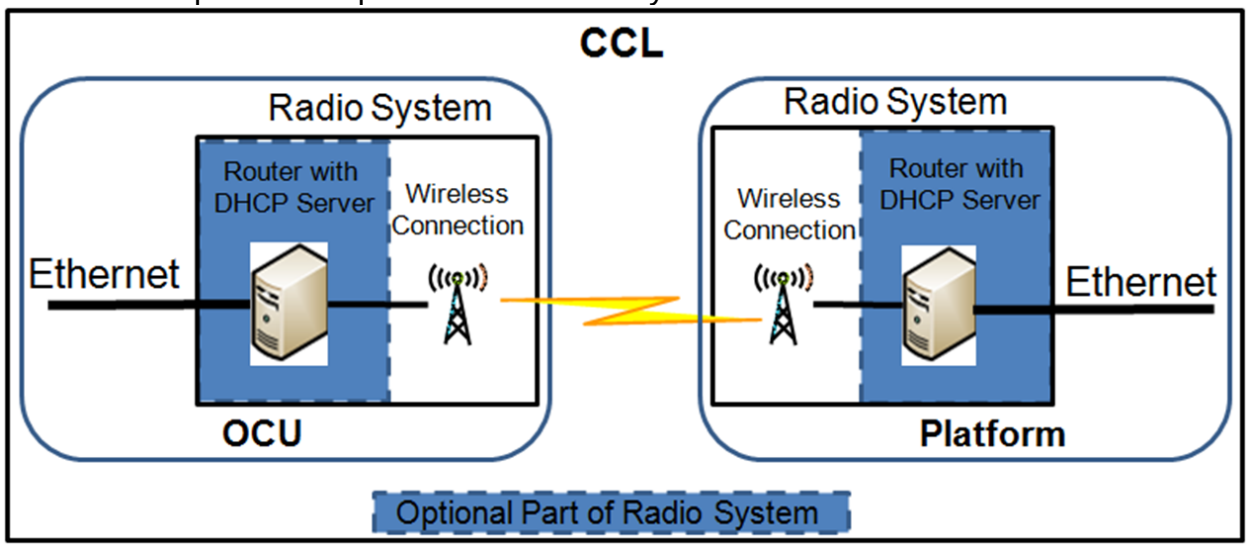


Figure 1: CCL Systems Block Architecture

The CCL architecture as shown in the diagram above will support an Ethernet interface at both the OCU and the UGV Platform, and provide on-board network services. The CCL may have Dynamic Host Configuration Protocol (DHCP) server component capable of supporting either flat or routed networking. The DHCP will be allowed to traverse the entire radio system from the UGV to the OCU. This setup is also known as a bridge network. For flat or routed networks, there will be no need for a Network Addressing Table (NAT), port forwarding, tunneling, or other techniques that would normally be required on the public/private network. The DHCP server should follow the Dynamic Host Configuration Protocol as defined in RFC 2131 and DHCP Options in RFC 2132 to avoid IP address conflicts across subnets (DHCP for IPv6 is RFC 3315).

3.1.1 CCL Power Requirement

V1.COMMS-1	*The CCL input power shall be auto-ranging supporting the voltage range of 10 to 28 VDC.*

3.2 AIR INTERFACE/WAVEFORM

For this version of the IOP, the Air Interface/ Waveform of the Communications Link will be defined by the radio vendor to meet the requirements of the system. However, it is the goal of the Communications IOP to have a common Air Interface/ Waveform for RAS-G Communications.

3.3 PRIORITIZATION OF SERVICE

Different classes of traffic have different priorities. In computer networking, this is referred to as Quality of Service (QoS). Network traffic is marked to designate the different priorities. For Ethernet frames, 802.1p is used to mark traffic. In Layer III(3), the IP layer of the OSI model, DiffServ Code Points (DCSP) is used to mark traffic. Traffic must be prioritized in two distinct places:

1. Within the platform/OCU: Higher priority traffic must leave the platform/OCU before lower priority traffic.
2. Between platforms/OCUs: Higher priority traffic from one platform/OCU must access the air interface before lower priority traffic from other platforms/OCUs.

An example of a marking and prioritization standard for wireless networks is Wi-Fi Multi-Media (WMM) 802.11e, which can be useful to the system designer in setting up a prioritization scheme to meet system objectives. The table below contains a possible priority scheme based on IEEE P802.1P.

PCP	Network Priority	Traffic
1	0 (lowest)	Background
0	1	Best Effort
2	2	Excellent effort
3	3	Video
4	4	Voice
5	5	Platform Telemetry
6	6	Platform Control
7	7 (highest)	Emergency Stop / Fire control

Table 1: Possible Priority Scheme

This is not the only way to implement packet prioritization; it can also be performed via port priority. In the port priority technique, some ports on the network have a higher prioritization than others. As an example, the JAUS port (3794) may be given the higher priority than the port that video is sent on. This might be an easier or simpler implementation for the radio payload provider.

The actual packet prioritization and schema will be left up to the system architect. Different missions may require different priority schemes. It is highly recommended that the radio payload support prioritization of service.

3.4 BOUNDARY DIAGRAM

Figure 2: Boundary Diagram below provides focus areas of the radio system toward interoperability of RAS-G communications.

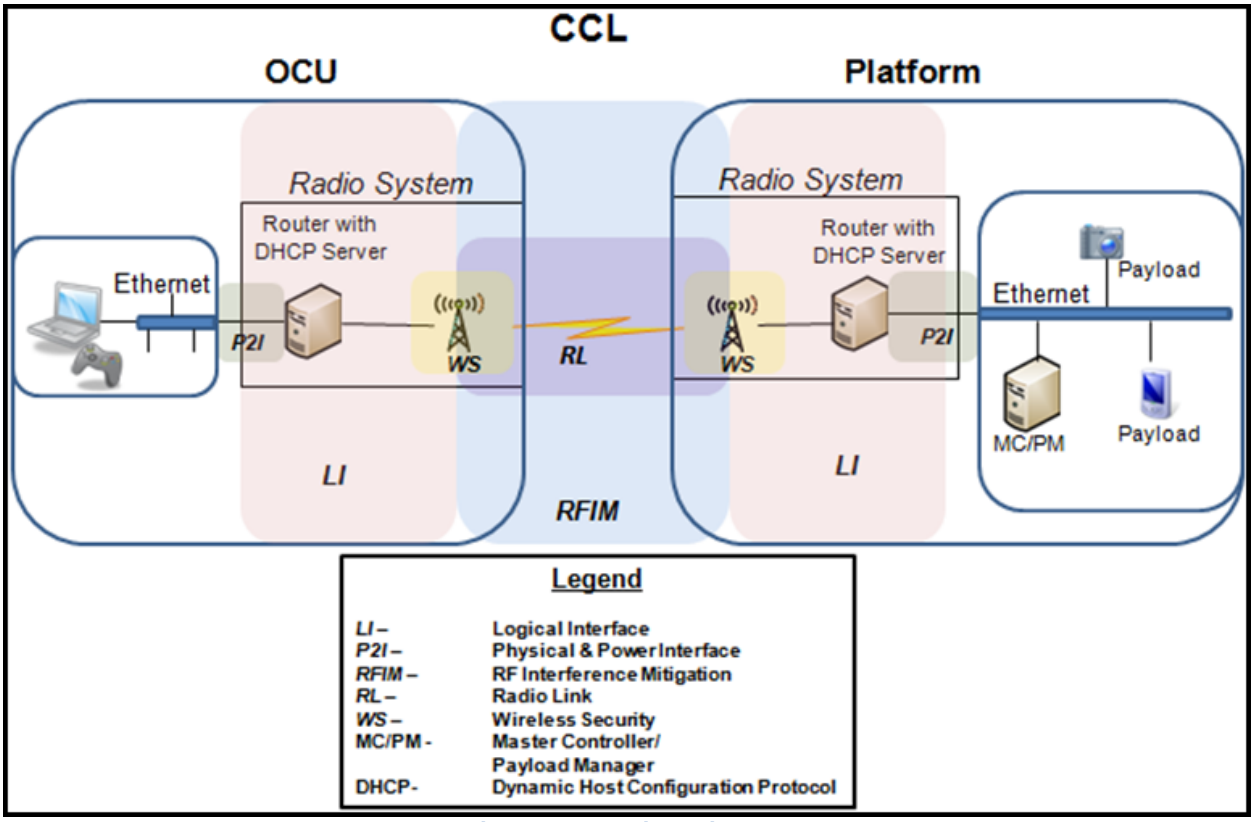


Figure 2: Boundary Diagram

The boundary areas of the CCL define specific aspects of the RAS-G communications systems as follows:

- Physical/ Power Interface - Defines the physical connection points of the CCL and input power requirements.
- Logical Interface - Defines the electrical and networking aspects of the CCL.
- Radio Link - Defines the Air Interface/ Waveform of the CCL including frequency channel selection, bandwidth and transmit power.
- Radio Frequency Interference Mitigation - Defines frequency bands and resiliency to interference.

- Wireless Security - Defines the radio encryption and tamper security of the CCL. Further discussion of Wireless Security can be found in section 4.4 and Appendix B of this document.

3.5 SECURITY (AUTHENTICATION AND ENCRYPTION)

Any new external computer device connecting to the system shall be authenticated by using an authenticating protocol, i.e. Secure Shell (SSH), Hypertext Transfer Protocol Secure (HTTPS), etc.

Encryption can be embedded in the radio or can be accomplished by an encryption module interfacing between the radio and the platform or OCU communications backbone.

Encryption is not required for a tethered link but is recommended. It is important to note that without proper user authentication (over an encrypted channel) and encryption/ authentication of the payload, an intruder may be capable of taking control of the platform. As stated above, HTTPS and SSH (when used with ciphers) provide the necessary encryption to protect user authentication. SSH can also be used to tunnel TCP traffic securely. SSH is not recommended for UDP traffic. A.2 SECURITY provides further details.

Security and Information Assurance is addressed in the following sections: 4.7 ACCESS CONTROL ATTRIBUTE defines Security and Information Assurance requirements and A.2 SECURITY provides recommendations and additional information related to Security and Information Assurance.

3.6 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) CONFIGURATION

Configuration of the DHCP server shall be open and available to the Government without the use of special tools or licenses. At minimum, the following controls shall be configurable on the server:

- Network Class
- DHCP address pool
- Subnet mask
- IP Address Lease Time

CHAPTER 4 SOFTWARE ATTRIBUTES

4.1 TRANSPORT ATTRIBUTE

Any number of the following attributes can be chosen.

Attribute	Description
Off-Board Communications Attribute	The Off-Board Communications Interoperability Attributes define capabilities to deal with communications off-board the platform.

Table 2: - Optional Select = any

4.1.1 Network Standard Requirement

V1.COMMS-2	*The primary on-board network standard shall be derived from the IEEE 802.3 standard for Ethernet communication.*
V1.COMMS-3	*The secondary standard will be for USB 2.0 or higher and/or RS232/422/485. USB standard will be derived from the USB Forum standards. The RS232/422/485 standard will be derived from EIA/TIA (232/422/485) standards.*

4.1.1.1 Parameter Listing

Parameter Name	Default Value	Allowed Values	Description
Ethernet Standard Parameter	Gigabit	*<Enumeration>*	The Ethernet speed standard met by the on-board Ethernet network.
		None	No on-board Ethernet network present
		Unspecified	Unspecified Ethernet speed
		10 Mbps	10 Mbps Ethernet
		100 Mbps	100 Mbps Ethernet
		Gigabit	Gigabit Ethernet

Table 3: - Parameter Listing for Transport Attribute

4.1.2 Addressing Standard Requirement

V1.COMMS-4	*IPv6 standard shall be used on UGV systems and will be backward compatible to support IPv4 components. See Section B.1.5.2 and B.1.5.3 for details and supporting protocols for both IPv4 and IPv6.*
V1.COMMS-5	*A CCL system with non-static addressing schema shall be capable of enacting Dynamic Host Configuration Protocol (DHCP) to enable the automatic IP address assignment of payloads and other Ethernet system components.*

4.1.3 Data Packet Handling Requirement

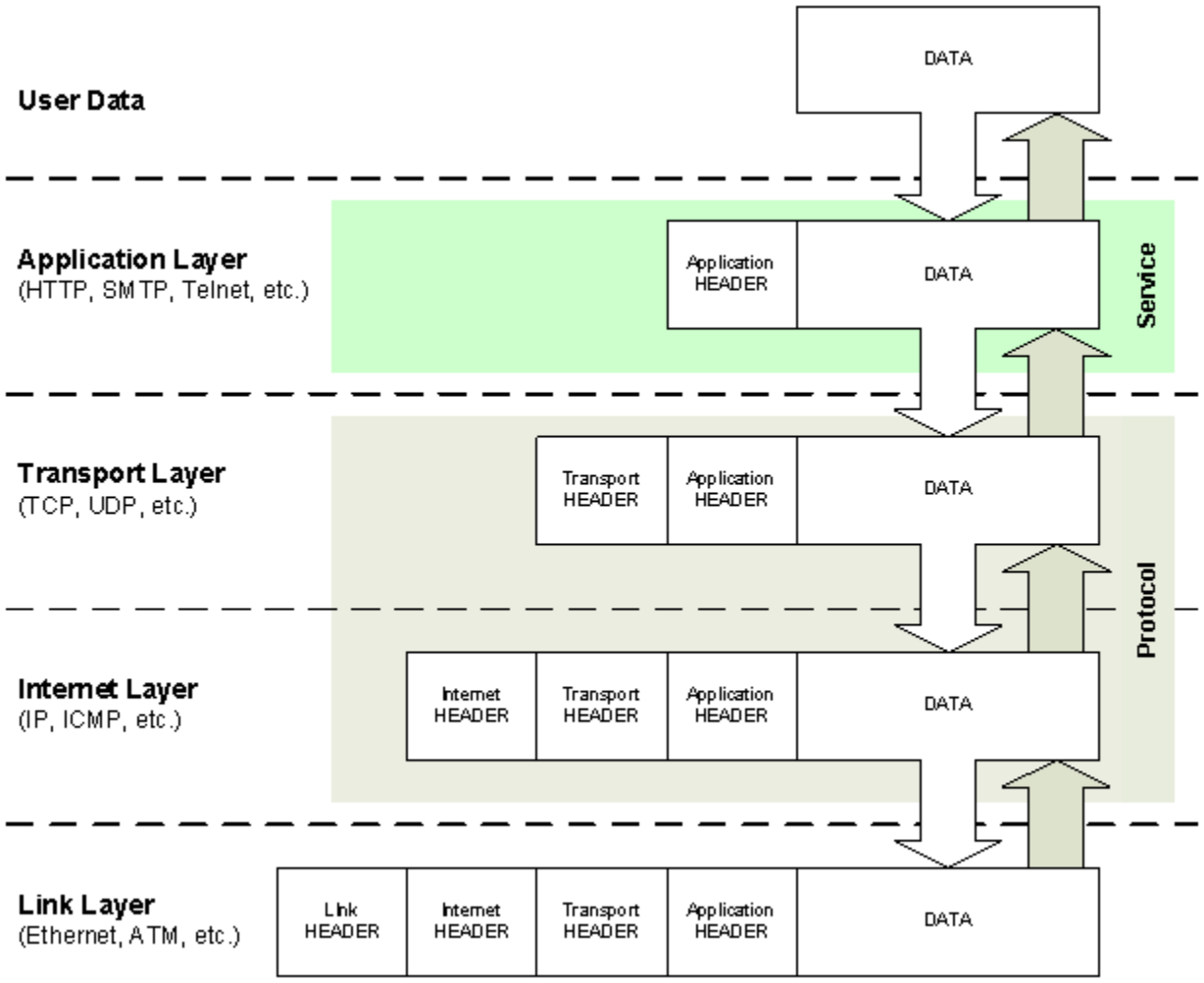


Figure 3: Network Layer Chart

V1.COMMS-6 *The CCL system shall be able to manage packets and the data contained within the IEEE 802.3 protocol standards per Figure 3.*

V1.COMMS-7 *The CCL system shall support multicast messaging.*

4.1.4 DHCP Server Configuration Requirement

V1.COMMS-8 *All DHCP servers shall have at least the following list of configuration items available and adjustable to the Government: Network Class, DHCP address pool, Subnet mask, and Address Lease time. No special tools or licenses shall be required for configuration of the server.*

4.2 OFF-BOARD COMMUNICATIONS ATTRIBUTE

Parent Attribute: Transport Attribute

For IOP V1, the off-board networking capabilities will be limited to closed networking that does not share information outside of the OCU, platform and Remote Video terminals (RVTs). However, additional interoperability attributes will be defined in future revisions to specify CCL options. These attributes will include Public / Private networking for the sharing of information on the battlefield. Eventually, the CCL will interface with the Global Information Grid (GIG) to support ubiquitous communications.

The following attributes are mandatory.

Attribute	Description
Communicator Attribute	Defines a capability to interact with a communications device, such as a radio, including configuring it.

Table 4: - Mandatory Select = all

At least one of the following attributes must be chosen.

Attribute	Description
Meshed Networks Attribute	Utilize mesh networking
Non-meshed Networks Attribute	Utilizes non-mesh or point-to-point networking
Cloud Network Attribute	Cloud networks allow OCUs and platforms to be part of a larger network without dedicated channels and are not within the scope of IOP V1.

Table 5: - Mandatory Select = any

4.3 MESHED NETWORKS ATTRIBUTE

Parent Attribute: Off-Board Communications Attribute

Mesh Networking or Mobile Ad-hoc Networking (MANET) network connections are established and broken down between compatible radios depending on the quality of the radio connections or current mission conditions. This network type is dynamic in nature and is self-forming and self-healing in terms of topology. Section B.1.2, B.1.3 and B.1.5 has more details on Mesh networking.

Messaging and service definitions will follow the SAE AS-4 JAUS standards.

Discovery of end- points (OCUs and UGVs) will follow the paradigm in SAE AS5710 JAUS Core Service Set standard. Refer to JAUS Profiling IOP and the Custom Service Messages & Transports documents on discovery service.

4.3.1 IP Addressable Requirement

V1.COMMS-9	*The CCL system using Layer II (Mesh Networking) shall be capable of routing Ethernet frames between CCL's and the system they support. See Layer II Routing section B.1.3.*
V1.COMMS-10	*The CCL radio using Layer II (Mesh Networking) shall be IP addressable for configuration purposes.*

4.3.2 Multi-node Network (Multiple OCUs <-> Multiple Platforms)

This network is commonly referred to as Mesh or Mobile Ad-Hoc Network (MANET). In this network, multiple OCUs and multiple platforms (devices) co-exists within the same networking space. The mesh radios that the OCU and Platform use are capable of linking to other mesh radios that are set up similarly. Each Device in the network can communicate to every other device as long as it is in the rage. In this network, information is passed or routed between devices on layer II (of the OSI reference model).

4.3.3 Repeater/ Relay Network (OCU <-> Relay <-> Platform)

In this network topology, the OCU cannot directly communicate to the Platform because of an obstruction or separation distance. Therefore one or more devices in must be placed in between the OCU and platform to enable their communication. The device(s) in between the OCU and platform will relay the messages from the OCU to the Platform and from the Platform to the OCU. This topology can be used to extend the communications range of the system or it can be used in NLOS missions. Mesh enabled radios would be capable of this topology. The devices that are in between the OCU and Platform may be unintelligent communication bricks that contain a mesh radio, another platform with a mesh enabled radio, or a combination of the two. It is possible to establish a Repeater / Relay net without Mesh networking radios but such specifications are not in the scope of this document.

4.4 NON-MESHED NETWORKS ATTRIBUTE

Parent Attribute: Off-Board Communications Attribute

4.4.1 IP Addressable Network Requirement

V1.COMMS-11	*The CCL system using Layer III (Non-Mesh Networking) shall be capable of enacting Routing for IP packets between CCLs and systems they support.*
V1.COMMS-12	*The CCL radio using Layer III (Non-Mesh Networking) shall be IP addressable for plug and play capability. IP shall be the standard protocol for CCL Network Layer for CCL radios with this attribute.*

4.4.2 Basic Point-to-Point Communications Network (OCU <-> Platform)

At its most basic level a network can consist of two non-meshing end-points. In this case, the two end-points are the OCU and the UGV. This point-to-point (PTP) network will be an IP-based network with the endpoints preconfigured with static IP addresses. This indicates that the OCU and the UGV are "paired".

The network will be able to use either tethered communications, or wireless communications. It is highly recommended that a common waveform be developed for UGVs like IEEE 802.11 waveform that is robust in multipath environments and supports high data rates. A standard common waveform like IEEE 802.11 would allow radios to transmit and receive data from one vendor radio to another.

The transport used for network traffic will be identical to the Interoperability Attribute Value selected for "Transport", which can be JUDP, JTCP, or Custom, as defined in the Overarching IOP and the JAUS Profiling Rules document.

As specified in the AS5669A document, implementations using JUDP will use the Internet Assigned Numbers Authority (IANA) specified port for primary contact port for JUDP messages.

Although a discovery mechanism is not specifically needed since the OCU and the UGV are "paired", a discovery mechanism for the payload components on the UGV shall be incorporated. For this case, the discovery service, and protocols should follow the SAE AS5710 JAUS Core Service Set standard.

4.4.3 Basic Point-to-Point Network 2 (OCU <-> Multiple Platforms)

As an extension to the network, a non-meshed networked OCU could be configured to select control of a UGV from multiple available UGVs. This indicates that the OCU would have the ability to choose a PTP network for a specific UGV, from a number of available PTP networks. In the realm of 802.11, the robot is the access point, and the OCU is attaching to the access point of the platform. The OCU could only control one UGV at a time. Other OCUs could be configured the same way, for the same set of UGVs. Imaging data could also be shared with RVTs capable of receiving the radio signals from the UGV.

4.5 CLOUD NETWORK ATTRIBUTE

Parent Attribute: Off-Board Communications Attribute

Cloud networks are not within the scope of IOP V4. However, following the paradigm of the World Wide Web, OCUs and UGVs can be part of a larger network without dedicated channels of communications as in previous sections. This type of network will be IP-based, and can use either statically assigned IP addresses or DHCP. It can be a combination of wired and wireless nodes that comprise the overall network. All nodes should include a standard Ethernet adaptor for testing purposes.

Both network mentioned above (mesh and non-meshed) can be connected to a larger network via a router that contains a Firewall and Network Address Translation (NAT).

4.6 COMMUNICATOR ATTRIBUTE

Parent Attribute: Off-Board Communications Attribute

4.6.1 Frequency Channel Selection Requirement

V1.COMMS-13 *The radio shall be capable of tuning across the frequency band of operation in increments of one channel bandwidth (BW) or less but not more than 5 MHz.*

4.6.2 Bandwidth Selection Requirement

V1.COMMS-14 *The radio shall be able to change the BW of the radio channel transmission through JAUS messages as defined in JAUS Profiling IOP and the Custom Service Messages & Transports document.*

4.6.3 RF Transmit On/Off Requirement

V1.COMMS-15 *The radio shall be able to turn off and on RF transmissions of the communications link through JAUS messages as defined in JAUS Profiling IOP and the Custom Service Messages & Transports document. This feature does not necessarily shut down the receive operations of the radio.*

4.6.4 Max Transmit Power Requirement

V1.COMMS-16 *The user shall be able to set the maximum RF transmit power output of the radio through JAUS messages as defined in JAUS Profiling IOP and the Custom Service Messages & Transports document.*

4.6.5 Min Transmit Power Requirement

V1.COMMS-17 *The user shall be able to set the radio minimum RF transmit power output through JAUS messages as defined in JAUS Profiling IOP and the Custom Service Messages & Transports document.*

4.6.6 Frequency Band Requirement

V1.COMMS-18 *The radio communications system shall be capable of changing the frequency band of operation either by swapping hardware or through software commands.*

V1.COMMS-19	*The primary frequency band of UGV radio systems shall be 4400 – 4940 MHz. The following frequency bands are secondary to provide spectrum agility to support worldwide operations and shall only be employed as a back-up to the primary frequency band.* *These secondary frequency bands include but are not limited to: 225 – 470 MHz, 902 – 928 MHz, 1250 – 1390 MHz, 2025 – 2110 MHz, 2200 – 2300 MHz, 2400 – 2500 MHz, 4940 – 4990 MHz and 5000 – 5875 MHz.*

4.6.7 Adjacent Channel Requirement

V1.COMMS-20	*The radio communications link shall operate without degradation of radio communications range performance in the presence of other radios tuned to second adjacent channel frequencies operating at a distance of at least 10m.*
V1.COMMS-21	*The radio communications link shall operate without degradation of radio communications range performance in the presence of other radios tuned to first adjacent channel frequencies operating at a distance of at least 150m from the area of operation.*

4.6.8 Ground to Ground Communications Waveform Requirement

The RF waveform shall be resilient in multipath environments while supporting communications data rate requirements between the OCU and platform.

4.6.9 Data Rate Requirement

V1.COMMS-22	*The radio communications video link shall support a data rate of 1.8 Mbps or better at a receive signal input level of -40 to -85 dBm throughout in a benign RF environment with a Bit Error Rate (BER) of 10^{-6}or better.*
V1.COMMS-23	*The radio communications telemetry and audio link shall support a data rate of 200 kbps or better at a receive signal input level of -40 to -85 dBm throughout in a benign RF environment with a Bit Error Rate (BER) of 10^{-6}or better.*
V1.COMMS-24	*The radio communications link that combines video, telemetry and audio products to a single link shall support a data rate of 2.0 Mbps or better at a receive signal input level of -40 to -85 dBm throughout in a benign RF environment with a Bit Error Rate (BER) of 10^{-6}or better.*

4.7 ACCESS CONTROL ATTRIBUTE

4.7.1 Authentication Requirement

V1.COMMS-25	*Any computer device connecting to the system shall be authenticated by using an authenticating protocol, i.e. Secure Shell (SSH), Hypertext Transfer Protocol Secure (HTTPS), etc.*

4.7.2 Encryption Requirement

The CCL system shall include a method of encrypting the wireless communications that meets one of the following:

V1.COMMS-26	*The radio shall be validated in accordance with the program to determine the appropriate Level of security.*

4.7.3 Key Establishment Requirement

V1.COMMS-27	*The CCL shall employ automated key establishment if needed for a program's requirements in accordance with a nation's approved Key Establishment scheme. Key establishment can be conducted manually, automated or a combination of manual and automated.*

4.7.4 Encryption Bypass Requirement

V1.COMMS-28	*When the CCL is operated in a maintenance mode, it shall allow the encryption of the communications link to toggle on and off using JAUS messages in accordance with the Custom Service Messages & Transports document.*
V1.COMMS-29	*All cryptographic keys and unprotected critical security parameters shall be zero-ized when the CCL enters into a maintenance mode.*
V4.COMMS-30	*Implementation of Encryption Bypass shall utilize two independent internal actions to activate. Timing of a two-action bypass mechanism, should be considered to ensure that the initiation does not become in an inconsistent (i.e. hung) state.*

4.7.4.1 Parameter Listing

Parameter Name	Default Value	Allowed Values	Description
Bypass Timeout			The Encryption Bypass mechanism may use a timeout function. A timeout value of TBD is recommended.
Bypass Timeout Type		*<Enumeration>*	The Encryption Bypass mechanism may use a timeout function. It can be fixed or adjustable.
		Adjustable	Adjustable timeout
		Fixed	Fixed timeout

Table 6: - Parameter Listing for Access Control Attribute

4.8 LOST COMMS MANAGEMENT ATTRIBUTE

Parent Attribute: Autonomy and Behaviors Attribute

The platform may automatically detect and attempt to recover from situations in which communications with the controller or off-board network are lost ("comms lost"). The exact conditions for a comms lost event are not specified by the IOP, as they are likely to vary per platform, per radio, and possibly per mission. For instance, teleoperation of a platform requires low latency, high throughput communication channels to support streaming video; communications might be considered lost if latency increases above some threshold or throughput drops sufficiently that real-time video is no longer supported. On the other hand, an autonomous mission may only require that a platform 'check-in' periodically with very small position and status reports; in that case, communications may not be considered lost until error rates reach 100% for hours at a time. The criteria listed below are provided for illustrative purposes only, and should be considered as examples during implementation of comms lost behavior:

- Bit Error Rate > 5%
- Packet Error Rate > 2%
- Latency > 700 ms
- Liveness::ReportHeartbeAEPulse message missed 7 out of last 10 queries

Also note that comms lost should be considered at both the physical or logical networking level. For example, a radio may be connected to other radios in a mesh-networking set-up, and all links may have acceptable throughputs and latency. From a physical networking perspective, the radio and comms links are healthy. However, if the platform is unable to send messages through the mesh-network to a controller or remote operator due to range or configuration errors, then comms could be considered lost at the logical level.

Finally, comms lost events should be considered as a matter of last resort, after other communication enhancement behaviors have been exhausted. For instance, if a radio supports automatic adjustment of the transmit/receive power, these settings should be managed first. If necessary, alternate or redundant communication systems could also be brought online; however, if such systems still do not meet the latency, throughput or other communication requirements for a platform/mission, a comms lost event might still be triggered.

Platform behavior during a comms lost event is dictated by the Comms Lost Policy Manager Service as specified in the SAE JAUS Profiling Rules and Custom Service Messages and Transports documents. Allowed behaviors are: 1) continue mission without comms; 2) stop the platform immediately; 3) retro-traverse on the previously executed path in an attempt to re-establish comms; and 4) return to a designated rally point.

The Comms Lost Policy Manager Service also requires specification of desired behavior when communications are restored after a comms lost event. For example, a system might be configured to retro-traverse along the previously executed path, then stop once comms are regained. At that point, the operator can elect to retry or restructure the mission to accommodate the communications dead-zone. Alternatively, a vehicle might be configured to return to a rendezvous/ rally point in a comms lost event, and continue to that location even after communications are reestablished. This "comms regained" behavior can also be used to handle temporary drop-outs when switching between primary and secondary communication systems. If communications are temporarily lost when a primary system goes down, the vehicle can be configured to wait for confirmation from the user via the secondary channel before continuing the mission.

4.8.1 Lost Comms Management Requirement

V1.COMMS-31	*Systems that support comms lost capabilities shall do so by implementing the Lost Comms Management Interoperability Attribute as defined by the SAE JAUS Profiling Rules and Custom Service Messages and Transports documents.*

CHAPTER 5 HARDWARE ATTRIBUTES

5.1 COMMUNICATIONS HARDWARE ATTRIBUTE

Parent Attribute: Hardware Attribute

Any number of the following attributes can be chosen.

Attribute	Description
Tethered Communications Attribute	Utilizes a tether for communication.
Antenna Attribute	Using an antenna for communications.

Table 7: - Optional Select = any

5.1.1 Data Connectors Requirement

V4.COMMS-32	*The radio or tether communication system shall employ a connector(s) defined in the Payloads IOP or provide a conversion to interface with the UGV Platform.*

5.2 TETHERED COMMUNICATIONS ATTRIBUTE

Parent Attribute: Communications Hardware Attribute

Some environments are not conducive to wireless communications due to high electromagnetic levels, obstacles that block radio communications or when radio silence is required. In these environments tethered communication can provide the communications link between the OCU and the UGV in place of radio. A tether can be a fiber optic or wired.

A fiber tether would need a fiber optic payload to convert electrical signals from the Ethernet message to light. That light would then travel through the fiber optic cable. The light would be converted back to electrical signals, which would create an Ethernet message with a similar fiber optic payload on the far end. A wired tether would physically connect the communications backbone of the two endpoints via metal wires (e.g. Ethernet).

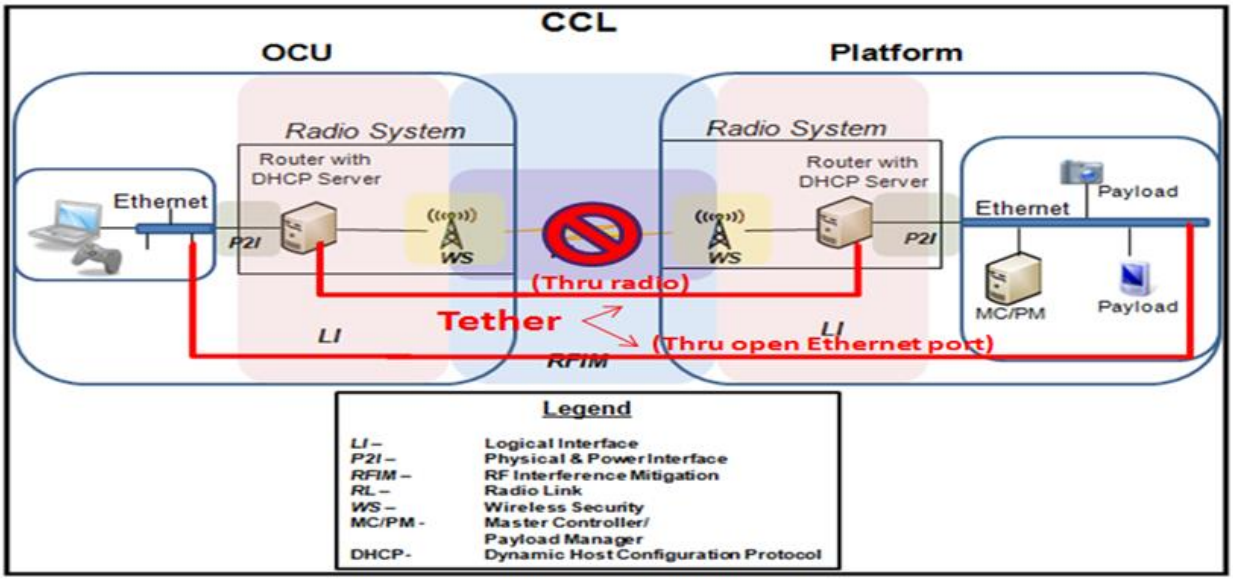


Figure 4: Tethered Operations Diagram

5.2.1 Interface Requirement

V4.COMMS-33 *The tether shall be capable of interfacing with any open payload port on the platform or through an open payload port on the radio payload. (See section 4.8.1 Data Connectors)*

5.2.2 Synchronization Requirement

V4.COMMS-34 *Once communication is established between the OCU and UGV through the tether, the OCU shall require confirmation from the user to shutdown any radio transmissions or place the radio in stand-by mode.*

5.2.3 Data Connector Requirement

V4.COMMS-35 *The tether interface shall be capable of interfacing with any open payload port on the Ethernet backbone or through an open payload port on the radio.*

5.3 ANTENNA ATTRIBUTE

Parent Attribute: Communications Hardware Attribute

5.3.1 Antenna Connectors Requirement

V4.COMMS-36 *The antenna port of the radio system shall be weatherproof, low loss with 50 Ohm impedance supporting frequency range of 200 MHz to 6000 MHz.*

V4.COMMS-37	*The external antenna connector of the radio system shall use any of the following common polarity industry connectors to interface with the antenna: SMA-female, TNC-female, N type-female, or Reverse Polarity TNC-female.*

ANNEX A COMMUNICATIONS ACRONYMS AND ABBREVIATIONS

ACM	Adaptive Code Modulation
APC	Adaptive Power Control
AEPC	Automatic Transmit Power Control
BLOS	Beyond Line of Sight
BW	Bandwidth
dB	Decibels
dBc	Decibels referenced to carrier
C2	Command and Control
CCL	Common Communications Link
CDMA	Code division multiple access
COFDM	Coded Orthogonal Frequency Division Multiplexing
COMSEC	Communications Security
CONUS	Continental US
COTS	Commercial Off-the-Shelf
CREW	Counter RCIED (Radio-Controlled Improvised Explosive Device) Electronic Warfare
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DSSS	Direct-Sequence Spread Spectrum
ESC	Equipment Spectrum Certification
FDD	Frequency Division Duplex
FEC	Forward Error Correction
GHz	Gigahertz
GIG	Global Information Grid
IA	Information Assurance
IANA	Internet Assigned Numbers Authority
IAW	In Accordance With
ICMP	Control Message Protocol
IGMP	Internet Group Management Protocol
IETF	Internet Engineering Task Force
IF	Intermediate Frequency
IOP	Interoperability Profile
IP	Internet Protocol
JAUS	Joint Architecture for Unmanned Systems
JTCP	JAUS Transmission Control Protocol
JUDP	JAUS User Datagram Protocol
kbps	Kilo-bits per second
kHz	Kilo-Hertz

LI	Logical Interface
LOS	Line of Sight
MANET	Mobile Ad-hoc Network
MBU	Mobility Base Unit
Mbps	Megabits per second
MC/PM	Master Controller/ Payload Manager
MHz	Megahertz
MIMO	Multiple Input Multiple Output
MLD	Multicast Listener Discovery
MMCX	Micro-Miniature Coaxial
ms	millisecond
NAT	Network Address Translation Table
NLOS	Non- Line of Sight
OCONUS	Outside Continental US
OCU	Operator Control Unit
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
P2I	Physical/ Power Interface
PCP	Priority Code Point
POE	Power Over Ethernet
PTP	Point-to-Point
PUI	Product Unique Identifier
QoS	Quality of Service
RCIED	Radio Controlled Improvised Explosive Device
RF	Radio Frequency
RFC	Request for Comments
RFIM	Radio Frequency Interference Mitigation
RL	Radio Link
RS	Recommended Standard
RVT	Remote Video Terminal
SDP	Session Description Protocol
SDR	Software Defined Radio
SFF	Small Form Factor
SMA	Sub-Miniature version A
SWaP	Size, Weight, and Power
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TNC	Threaded Neill-Concelman
UAV	Unmanned Air Vehicle
UDP	User Datagram Protocol
UGV	Unmanned Ground Vehicle
UMS	Unmanned Systems
USB	Universal Serial Bus

V0	Version 0
VDC	Voltage Direct Current
VGA	Video Graphics Array
VSWR	Voltage Standing Wave Ratio
WEP	Wired Equivalent Privacy
WG	Working Group
WPA	Wi-Fi Protected Access
WS	Wireless Security

INTENTIONALLY BLANK

ANNEX B DISCUSSION OF TECHNICAL TOPICS

A.1 NETWORKING CONCEPTS

A.1.1 IP Addressability (Layer III)

An IP-based network layer provides flexibility in the data link (layer II) and physical layers used for data transport whether wireless (i.e., digital radio or laser link) or hard-wire (copper or fiber-optic). In addition, IP-based systems have gained wide acceptance in many sectors and as a result, many COTS-based solutions are exploitable to reduce cost. IP-based communications put very few limits on future systems because the bandwidth capabilities of the data link and physical layers continue to increase.

A.1.2 Mobile Ad-hoc Network (MANET)

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless link. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices as it moves within the net. Each MANET radio must be capable of forwarding traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

A.1.3 Layer II Routing (for Mesh Networking)

The radio nodes of the mesh network shall use Layer II (2) for IP packet / message routing (RFC 1122 and RFC 1123). That is, routing at the Data link layer of the seven layer OSI model. In the TCP/IP reference model this is layer I (Host-to-Network Layer). One of the advantages of Layer II routing is that the radio nodes get abstracted from the devices' (OCUs' and MBUs') network configuration. The radio nodes themselves do not need a particular IP address assignment since packets from the devices are routed based on the hardware MAC addresses of the devices connected to the network. In other words, a network of radios supporting Layer II routing appears logically to the devices as a simple Ethernet switch. Each radio node behaves as an Ethernet port for this logical Ethernet switch. Naturally the radio network needs to know the MAC address of the devices and to which Ethernet port (radio) they are attached to. This is resolved by the Address Resolution Protocol (ARP) explained in RFC 1122 and RFC 826.

Example 1: let OCU and MBU be two devices on the same subnet S. If the OCU and the MBU are operable by connecting them to a common Ethernet switch then they would also be operable by connecting them to any two radios that are part of the same mesh network. No IP configurations should be necessary on the radios to reflect the subnet S.

Example 2: let OCU and MBU be two devices on the same subnet S1. Assume MBU has multiple sensors in subnet S1. In this case, the OCU may be connected to an arbitrary radio on the network and the MBU and its sensors to another arbitrary node in the network. The OCU has direct access to the sensors on the MBU via a fully flat network.

Example 3: let OCU and MBU be two devices on the same subnet S1. Assume MBU has multiple sensors in subnet S2. The MBU sensors in subnet S2 sits behind a Network Address Translation (NAT) on the MBU. In this case, the OCU may be connected to an arbitrary radio on the network and the MBU is also connected to an arbitrary radio on the network. The OCU access the sensors on the MBU via NAT.

A.1.3.1 OSI and TCP/IP Reference Models

The figure below provides a comparison of network layers for the OSI and TCP/IP reference models:

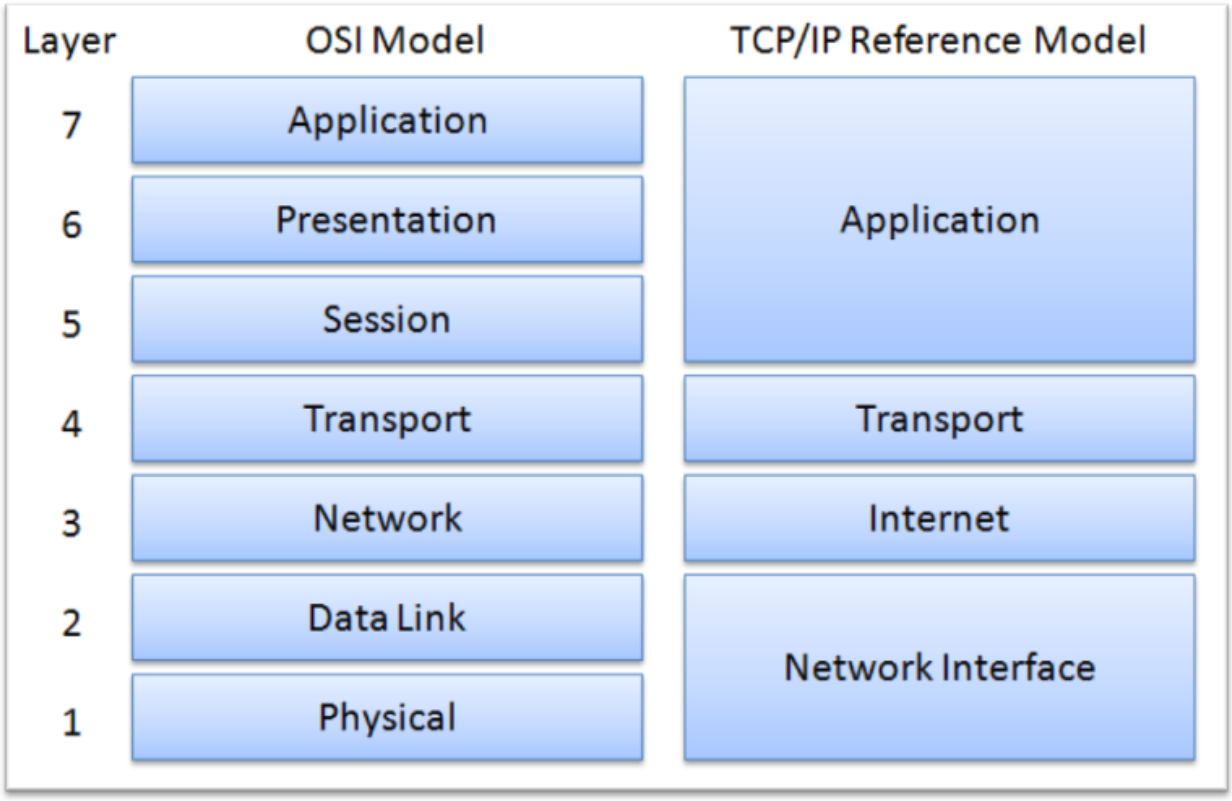


Figure 5: OSI and TCP/IP Reference Models

A.1.4 Broadcast

Broadcast addressing is the delivery of information to all connected nodes within a network simultaneously. Broadcast uses the IP network infrastructure using User Datagram Protocol (UDP) to send a packet only once.

A.1.5 Multicast

Multicast addressing is the delivery of information to a target group of destinations simultaneously. Multicast uses the IP network infrastructure using User Datagram Protocol (UDP) to send a packet only once. This means that one host can send one message to multiple receivers simultaneously. Unlike broadcast, only the nodes that join the multicast group will receive the message to limit the traffic on the network. The radio payload shall support multicast messaging. Use of Internet Group Management Protocol (IGMPv3) and/ or Multicast Listener Discovery Protocol (MLDv2) standards should be followed for multicast receivers using IPv4 or IPv6, respectively.

A.1.5.1 Multicast Configuration in a Mesh Network

IPv4 and IPv6 map the IP multicast group addresses to the underlying MAC address. To allow the underlying mesh network to optimize multicast traffic, two rules must be observed:

1. For different IP multicast groups, the system designer must select IP multicast group values that do not map to the same MAC address. The rules for IPv4 and IPv6 mappings are described below.
2. System designers shall avoid using special IP multicast group values that are designated by RFC 4541 to be treated like broadcast, as no multicast optimizations can be possible on these groups values.

A.1.5.2 IPv4 to MAC Address Mapping

Up to 32 IPv4 multicast addresses can map to the same MAC multicast address. The schema for mapping of IPv4 addresses to MAC addresses is 01-00-5e-xx-xx-xx, where xx-xx-xx is the lower 3 bytes of the IPv4 address with the most significant bit (bit 23 counting from 0) set to 0.

(http://technet.microsoft.com/en-us/library/cc957928.aspx explains this clearly).

A.1.5.3 IPv6 to MAC Address Mapping

A large number of IPv6 multicast addresses can map to the same MAC multicast address. The schema for mapping of IPv6 addresses to MAC addresses is 33-33-xx-xx-xx-xx, where xx-xx-xx-xx is the lower 4 bytes of the IPv6 address.

The following are special IPv4 and IPv6 multicast group addresses that are treated like broadcast messages based on RFC 4541 recommendations:

1. Any IPv4 address that maps to 01-00-5e-00-00-xx, where x is 0..255 is treated like a broadcast address. This specifically includes the IP addresses of the form 224.0.0.x.
2. Any IPv6 address that maps to 33-33-00-00-00-01 is treated like a broadcast. This specifically includes the All-Nodes IPv6 multicast addresses FF02::1.
3. Multicast addresses that are not of the form 01-00-5e-xx-xx-xx or 33-33-xx-xx-xx-xx (i.e., non-IP multicast) are treated as broadcast addresses.
4. MAC address 01-00-5e-00-00-fb (corresponds to mDNS IP 224.0.0.251) and 33-33-00-00-00-fb (corresponds to mDNS IP ff02::fb) are for multicast DNS (mDNS) and using them may produce undesirable side effects.

A.2 SECURITY

A.2.1 Authentication and Authorization

A.2.1.1 Data Integrity

Data integrity is a property whereby data has not been modified since it was created, transmitted or stored. Modification includes the insertion, deletion or substitution of data. Cryptographic mechanisms, such as message authentication codes or digital signatures, can be used to detect (with a high probability) both accidental modifications (e.g., modifications that sometimes occur during noisy transmissions or by hardware memory failures) and deliberate modifications by an adversary. Non-cryptographic mechanisms are also often used to detect accidental modifications, but cannot be relied upon to detect deliberate modifications.

A.2.1.2 Authentication

The use of cryptography supports two types of authentication services: integrity authentication and source authentication. An integrity authentication service verifies that data has not been modified, i.e., this service provides integrity protection, while a source authentication service verifies the identity of the user or system that created the data. Several cryptographic mechanisms are commonly used to provide authentication services, including digital signatures, message authentication codes and some key-agreement techniques.

As stated earlier, it is important to note that without proper user authentication (over an encrypted channel) and encryption/authentication of the payload, an intruder may be capable of taking control of the platform. HTTPS and SSH (when used with ciphers) provide the necessary encryption to protect user authentication. SSH can also be used to tunnel TCP traffic securely. SSH is not recommended for UDP traffic.

A good tutorial on this subject is available at the following link:
http://www.ibm.com/developerworks/aix/library/au-tunnelingssh/

Datagram Transport Layer Security (DTLS) secures UDP packets using Transport Layer Security (TLS). SSH is part of all Linux distributions. DTLS is now available as part of OpenSSL. Internet Protocol Security (IPsec) is another good alternative for securing either UDP or TCP traffic.

A.2.1.3 User Authentication

Two types of user authentication are Role-Based Authentication and Identity-Based Authentication. Role-Based Authentication requires that one or more roles either be implicitly or explicitly selected by the user without authenticating the individual identity of the user. Identity-Based Authentication requires that one or more roles either be implicitly or explicitly selected by the user, the user be individually identified and authenticated, and the authorization of the user to assume the selected role (or set of roles) be authenticated.

Examples of authorized roles for operators/users include:

- A role to perform general security services, including cryptographic operations and other approved security functions.
- A role to perform cryptographic initialization or management functions (e.g., module initialization, input/output of cryptographic keys and CSPs, and audit functions).
- A role to perform physical maintenance and/or logical maintenance services (e.g., hardware/software diagnostics).

It is recommended that the systems employ one or more authentication mechanisms to authenticate an operator accessing the module, and to verify that the operator is authorized to assume the requested role and perform the services within the role.

It is recommended that the systems employ Role-Based Authentication with, one or more of the following types of authentication data:

- Password, PIN, Cryptographic key, or equivalent;
- Physical key, token, or equivalent;
- Biometrics

Authentication data within a cryptographic module should be protected against unauthorized disclosure, modification, and substitution.

A.2.1.3.1 Services

A cryptographic module should provide various services. These services comprise all the services, operations, or functions that can be performed by the cryptographic module. Services consist of an input and an output. Service inputs shall consist of all data or control inputs to the cryptographic module that initiate or obtain specific services, operations, or functions. Service outputs shall consist of all data and status outputs that result from services, operations, or functions initiated or obtained by service inputs.

It is recommended that a cryptographic module provide the following services to operators:

- Show Status: output the status of the cryptographic module.
- Perform Self-Tests: initiate and run self-tests.
- Perform Approved Security Function: Perform at least one approved security function used in an approved mode of operation.

It is also recommended that the cryptographic module provide a capability to show status to indicate when:

1. The bypass capability is not activated, and the module is exclusively providing services with cryptographic processing (e.g., plaintext data is encrypted).
2. The bypass capability is activated and the module is exclusively providing services without cryptographic processing (e.g., plaintext data is not encrypted).
3. The bypass capability is alternately activated and deactivated and the module is providing some services with cryptographic processing and some services without cryptographic processing (e.g., for modules with multiple communication channels, plaintext data is or is not encrypted depending on each channel configuration).

A.2.1.4 Layer-2 Confidentiality & Integrity Protection

It is recommended that the advanced encryption standard is used for confidentiality (aka. encryption). It is also recommended that packet integrity protection (aka. packet authentication) be implemented using an approved algorithm. For video streams and other lossy data, packet integrity protection is optional. For command and control (C2), it is recommended that packet integrity protection always be used. This document recommends that anti-replay protection be implemented. Anti-replay protection requires packet integrity protection. It is recommended that anti-replay protection be used for all command & control traffic. For video traffic, it is not possible to achieve anti-replay protection without packet integrity protection.

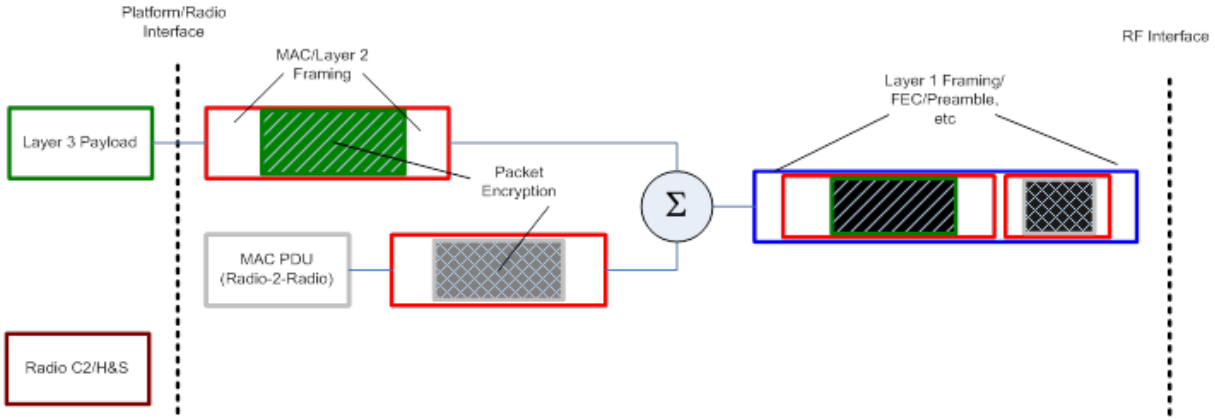


Figure 6: Nominal data flow through radio showing encrypted layer-2 packets

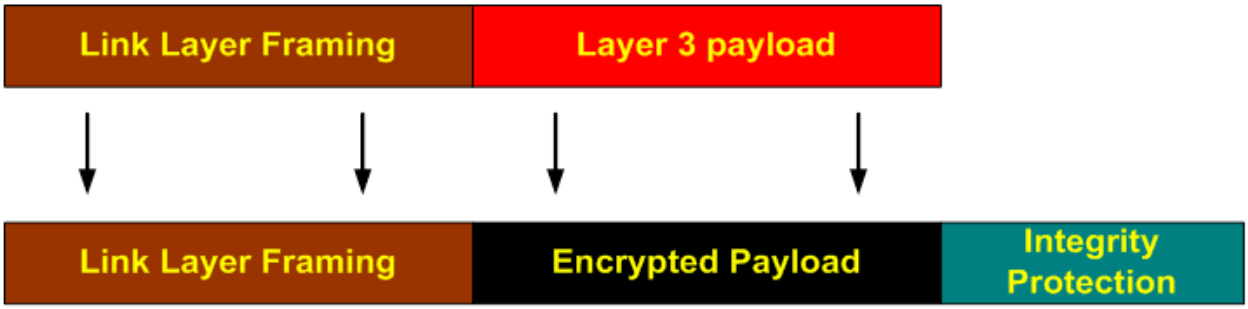


Figure 7: Details on Layer 2 Packet Structure and Encrypted Data

A.2.1.5 Key Lengths

It is recommended that both 128-bit and 256-bit key lengths be supported.

A.2.1.6 Key Establishment

Key establishment schemes can be manual, automated or a combination thereof. Automated key-establishment schemes set up keys between communicating entities. Two types of automated key-establishment schemes are: Key Agreement and Key Transport.

A.2.1.7 CONOPS and Security Requirements

It is recommended to implement a minimum set of security requirements, including encryption and authentication. It is anticipated that several operational needs will require increased security implementations. Below is an example table highlighting entries based on possible CONOPS and their security needs. Government stakeholders must determine system requirements and select radio/data links that meet their individual requirements.

CONOP	Security Certification	Minimum Key Length	Cipher Mode	Packet Authentication	Key Agreements	Key Lifetime

Table 3: Example Listing of Security Requirements Based on Operations

A.3 RF TRANSMISSION WAVEFORM

An RF waveform is largely defined by the requirements of the mission, e.g. line of sight (LOS), non-line-of-sight (NLOS), or beyond-line-of-sight (BLOS). There are many different modulation techniques available for RF transmission of digital signals. However, two attributes that drive the RF transmission waveform for ground-to-ground mobile communications used for UGVs is that is must be resilient to multipath fading and support high data rates for teleoperation.

Orthogonal Frequency Division Multiplexing (OFDM) is a multi-carrier modulation technique that reduces the rate of modulation of the sub-carriers with respect to the rate of a modulation requiring a single carrier, and therefore reduces the effect of phase errors whether equalized or not. It also provides a high level of spectral efficiency. Coded OFDM (COFDM) provides an additional layer of coding that substantially reduces the Bit Error Rate on mobile links. OFDM and COFDM have gained a significant presence in the wireless marketplace which includes wireless routers and digital television transmission. The combination of high data capacity, high spectral efficiency, and its resilience to multipath effects means that it is ideal for the high data rate applications that are becoming a common factor in today's communication devices.

Early selection of a strategy or vision for future radio control and data links will provide an emerging consensus for a robust robotics industry. Transition to interoperable waveforms as early as possible provides powerful economic advantages for Army acquisition. In the interim, interoperability should be achieved at the Interface Level IP layer as soon as possible. Interoperability at the RF/waveform level is a longer term goal for achieving better economies of scale (by competition between vendors).

There are interim choices for waveform attributes which are easy to implement. For example, provision for the use of dual RF frequency bands (back-up frequencies) is encouraged, as a method of mitigation against jamming. At least one vendor radio does this automatically already. At a minimum, two widely separated frequencies should be used. Simple spatial diversity systems (systems on a single frequency) are in common use in Police vehicles for urban environments. These can be thought of as temporary steps to the more sophisticated methods discussed above. However they are appropriate low cost solutions that can be adopted to improve performance.

A.3.1 Bandwidth

Bandwidth (BW) for purposes of this document will be defined as the emissions BW of the modulated radio signal in megahertz (MHz) bounded by the half power (-3 dB) points.

A.3.2 Data rate/Throughput

The achievable data rate for wireless links is a function of many variables including topology, error coding, transmit power and medium access control. The throughput is defined as the data rate seen by an application. The throughput is always less than the wireless link data rate because of the "overhead" associated with wireless links, such as packet size and headers. Higher throughput requirements imply more RF bandwidth needed, so throughput requirements should be minimized. The sources of these data flows are the OCU (sending commands), the platform (sending telemetry), and the payloads on the platform. The telemetry provides the status of the platform and possibly the status of the attached payloads.

Typically, one payload is a video source, with a data flow from the video source to the OCU. These video sources are a large percentage of the total data flow from the platform to OCU. To minimize the data rate produced, video signals are always compressed using an encoder. These data rates out of the encoder vary widely depending on the scene, resolution of the camera and encoder settings. Insufficient throughput can result in grainy, blocky, or high latency video at the OCU display.

The figure below depicts the transport stream data rates from the existing video standard adopted by the Motion Imagery Standard Board; however future adoption of the Advance High Definition or 3D video standard will increase the video transport throughput requirement. The MPEG-2 compression codec will yield approximately twice as high a data rate compared to the H.264 compression codec. Encoding in a video frame rate below 24 frames per second (fps) can decrease the data rate when true motion imagery is not required.

Transport Stream Data rate	4.5-12 Mb/s	1-5 Mb/s		0.75-1 Mb/s	384-768 Kb/s
Motion Imagery Standards Profile (MISP)	HD(L9H)	ED(L6H)	SD(L3H)	LD(L2.1H)	LD (L1.2H)
Resolution	1280X720P 1920X1080P	640X480P 1020X576P	640X480i 720X576i	320X480P 352X576P	320X240P 352X288P
Frame Rate (fps)	24-60 (720P) 24-30 (1080P)	24-60	24-30	24-30	24-30
Bit Depth (Nominal)	8 bits	8 bits	8 bits	8 bits	8 bits
Compression Ratio (Nominal)	110:1	110:1	83:1	83:1	83:1
Data Rate (Nominal)	6 Mb/s	2 Mb/s	2 Mb/s	1 Mb/s	512 kb/s

Table 4: Transport Stream data rate for compression with H.264 protocol

A.3.3 Scalability

Description:

(a) **Networks** have particular vulnerabilities as wireless traffic increases with more systems operating in a given area. Scaling networks to larger size can be problematic in general but is resolvable using appropriate network architectures and routing algorithms that lend themselves to be dynamically scalable according to the needs of the network.

(b) **Waveform** inefficiency consumes valuable spectrum and limits the number of platforms that can operate in a local area within a designated band. Spectrum is a scarce shared resource that is used by all services, including by UAVs. As more unmanned systems are employed in an area of operation, i.e. swarming, radio spectrum will be a critical driving factor in UxS operations while not impeding other NATO communications. Radio waveforms and technology will need to efficiently use available spectrum by adaptively scaling the RF bandwidth according to the data rate. Automatic scaling according to traffic volume will change the waveform, and this can be used in conjunction with other methods like cognitive radio technology to allow users to take advantage of the spectrum optimally.

Further work on automatic rate adjustment between nodes will permit higher numbers of platforms to co-exist. This introduces complexities for the efficient routing of network data, even if the network is infinitely scalable. This is an architectural issue for the waveform and upper layers.

It is strongly recommended that each UGV system provide its own ability to negotiate spectrum control, separate from a central spectrum allocation system. This would allow spectrum sharing and scalability that would be more robust to hostile attack.

Other Guidance: There is currently no overarching spectrum management apart from spectrum allocation prior to a mission. Cognitive radio technology provides tools to assist with survivability and improve management but has not been widely used yet.

A.3.4 Latency

Low latency is required for real-time teleoperation of UGV(s) to maneuver around obstacles and perform mechanical operations and functions. Higher latency may be acceptable for UGVs with a higher degree of autonomy.

The end-to-end latency is the sum of latencies as data travels "down" a reference model (see Figure 5) at one location, is transmitted, and then travels "up" the reference model at another location. The protocol and processing at each layer contributes to the overall latency. The packetizing and compression of data (e.g. video) is a significant latency at higher layers. And a layer's protocol can affect other layer's latency. For example, Transmission Control Protocol (TCP) employs error correction facilities for requesting the information be retransmitted. However, for streaming lossy data, User Datagram Protocol (UDP) is a better transmission method because error checking and retransmission are not required. (UDP is a standard defined in IETF Standard 6/RFC 768 and the TCP standard is in the IETF Standard 7/RFC 793).

At the physical (waveform) layer, channel coding, interleaving, and error correction incur latency. MIMO processing also adds latency.

A.3.5 Quality of Service

As stated in section 3.4 Prioritization of Service, the Internet Protocol uses a differentiated services field in the IP packet to provide a method of prioritization of network traffic for time critical delivery. The RF waveform implementing the Data Link/Physical layers (OSI model) or the Link Layer (IETF TCP/IP model) should also adhere to the differentiated services information when delivering IP packets across a wireless medium. If the RF waveform provides a much higher bandwidth than the wired link, special processing may not be required. In cases where the wireless link is run at near capacity or over capacity, or has the ability to be temporarily blocked or impeded (e.g., line of sight blockage), it is recommended that the RF waveform incorporate a queuing/ordering scheme of IP packets it receives for transmission. This will ensure that the next packets processed by the RF waveform are always the highest priority to be transferred. An example is where the RF waveform between nodes is impeded, payload data begins to queue up within the waveform, while the waveform continues to ensure that the remote control / heartbeat packets required for human safety operation of the UGV are prioritized and transferred ahead of a payload's IP packets (e.g. video packets).

A.3.6 Electronic Protection

The waveform must have the necessary characteristics to perform well in a hostile electronic warfare environment while supporting UGV communications. Some forms of electronic protection are anti-jam (AJ), low-probability-of-intercept (LPI), and low-probability-of-detection (LPD). Techniques such as spread spectrum are mature and provide jamming resistance.

A.4 FREQUENCY BANDS

The UGV communication links operate in the mobile radio communication service which is designated by the host nation spectrum authority. To complicate matters, spectrum continues to be reallocated from government to commercial allocation as demand for wireless communication grows. Spectrum is a limited resource therefore it will be necessary for the unmanned radio systems to use spectrum efficiently as demand will continue to grow.

A.4.1 Adaptive Code Modulation

The range of a radio is directly affected by many factors, including frequency; transmit power; height; and bandwidth. A recent development in radios provides the ability of radios to dynamically adjust their bandwidth and data rate to increase the reach of the radio signal. Where signal levels are good, the data rates increase to provide better video and where signal levels are low, the operator can still teleoperate the UGV with lower resolution video. This technique is called Adaptive Coding and Modulation (ACM). IEEE 802.11a standard defines a method on how to implement ACM.

A.4.2 Adaptive Power Control

Adaptive power control (APC) is widely used by cellular systems as a way to manage interference and to conserve battery power. For UGVs this well developed technology will also help with reducing detection from enemy. APC adjusts RF transmit power based on the strength and quality of the signal received to maintain the radio link. The advantages of employing APC include improved battery life, reduced interference to other systems and reduced detection from hostile forces.

In multicast operation APC may need to be shut off to ensure quality reception to other receiving stations.

In a mobile communications link, Automatic Transmit Power Control (AEPC) is implemented for the following reasons:

1. Receiver overload prevention: Receiver overload is manifested in degraded signal to noise ratio and an increase in bit errors even though the input signal level is very high.

2. Adjacent channel interference prevention: In certain types of point to multi-point networks a central receiver may be employed that uses several adjacent channels. It is possible that wideband noise from a close-in transmitter can bleed over to an adjacent channel and mask a weak on-channel signal. AEPC is very useful in preventing this near-field/far-field type of problem.
3. Weak signal range extension: When a signal drops toward the limits of intelligibility, a mechanism can be put in place to boost the TX output power, perhaps to a level that cannot be sustained long term but can be used for a short term period to temporarily extend the link distance. It is important to note that it is necessary to still be able to communicate to the transmitter that the receiver has lost or is losing the signal. This is typically done by designing the return link from OCU to UGV to have a higher system gain than the link from UGV back to the OCU. This is usually accomplished by the fact that many command links are operating on a lower frequency and narrower bandwidth than the wideband high speed data link, typically used for video and telemetry.
4. Reduce power draw from the battery.

AEPC dynamic range is typically 20 to 40 dB depending on the radio manufacturer.

Different signal quality parameters can be used to drive the AEPC, these include input signal power, signal to noise ratio, packet error rate and bit error rate either pre or post FEC, but they may also involve encryption issues. AEPC is not normally mandatory in any communications system but is a nice to have, particularly in multi-channel central receiver installations or in the case where a receiver front end is easily overloaded by the density of signals. This is obviously particularly relevant in the case of the deployment of multiple systems in close proximity.

However, the interesting case commonly occurs in current operations where multiple different missions occur nearby in an uncoordinated manner (or from different vendors). Each mission is critically important for the individuals involved, who then feel compelled to use the spectrum as best they can to accomplish a positive outcome. They are unlikely to accept a principle of limiting output power where it might jeopardize their mission or their lives. (By contrast, a cellular phone system is designed to optimize coverage for one person – the operator wishes to impose power-control usage in order to maximize the number of simultaneous calls.)

A.4.3 Security and Encryption

Wireless security of the communications link between an OCU and the UGV platform is accomplished by encrypting the radio signal. The type of encryption is dictated by the level of the information transmitted. Most UGV transmissions reside at sensitive but unclassified information.Most COTS digital radios offer an option of enabling an encryption protocol; however, some of these encryption schemes are subject to attack. For example, Wi-Fi Protected Access (WPA) (a certification program created by the Wi-Fi Alliance to secure wireless computer networks) was created in response to several

serious weaknesses that researchers had discovered in the previous system, Wired Equivalent Privacy (WEP).
However, UGV communications links are closed loop systems and the risk is relatively low on the data that is transmitted. Video transmissions are most susceptible to eavesdropping and probably the most sensitive as it could give away location from the background images transmitted or be recorded for exploitation to the media.

UGVs, by nature of their mission, have a potential to be captured, especially when operated beyond line of sight. Therefore use of any Communications Security (COMSEC) items on the remote vehicle needs to be considered carefully. The design must ensure that if the remote vehicle falls into enemy hands that they will not inherit information critical to understanding how to decrypt similar signals. Anti-tamper techniques will be used with UGV's. In addition, Data At Rest (DAR) measures will need to be implemented in robotic systems. The intent is for robot systems to be unclassified when placed in a non-operational mode, during maintenance, transport, training, or capture. COMSEC requirements for DAR on UGV platforms are outside the scope of the IOP and will be the responsibility of the program.

Encryption methods commercially available such as WPA that can provide a fairly high level of protection of data transmitted. The CCL will require the ability to select the appropriate level of security to operate by mission and should have the ability to bypass if necessary.

A policy and technical challenge exists with regard to Type 1 encryption on UGV's. Most NSA approved Type 1 solutions require the protected device to be under human control. The area of securing robotic systems does not align well with current security policies. Robotics Systems intends to work with TRADOC and Army CIO/G6 to align robotic capabilities and update security policies. In addition Army network architectures need to evolve to reflect the integration of robot sensor data into the tactical internet.

A.4.3.1 Wireless Security Recommendations for current radios

- Radios should operate with AES Encryption.
- Radios use 128-bit keys (at minimum), 256-bit keys is highly recommended.
- Latency should be less than 2 milliseconds due to the encryption/decryption process.

A.4.4 Antennas

Current frequencies used by UGVs span a wide range, requiring antenna selection specific to each radio type by frequency band. Although antennas exist that span wide range of frequencies there are tradeoffs that are made with gain and Voltage Standing Wave Ratio (VSWR). However, just like the radios there are different antennas for each radio to support the frequency band the radio transmits which again make sustainment difficult and costly. There is a need to have a common antenna that can support multiple frequency bands or range.

A.5 OFF-BOARD NETWORKING

Current UGV networks are closed networks that do not share information outside the OCU and the RCV. On the future battlefield information sharing will be a necessity to the Warfighter to be successful in their mission. Exchange of information allows the Warfighter and commanding officers to make informed decisions faster through increased situational awareness. Each network has different objectives and requirements that will determine what data is transmitted and received. With that said there must be underlying intelligence to ensure the right information is provided at the right time so not to overwhelm the system or user.

Management of two separate radios on separate networks as with the UGV and SUAS systems can be best accomplished with separate Ethernet data busses as depicted in the Figure below. Partitioning of the Ethernet data busses can also be accomplished through a router or switch with a single Ethernet connection to the computer. Separate Ethernet data busses have the added advantage that the IP address of the OCU can be different minimizing network conflicts. In this architecture all communications are controlled and managed through the OCU. There is no direct communications from the RCV to another network.

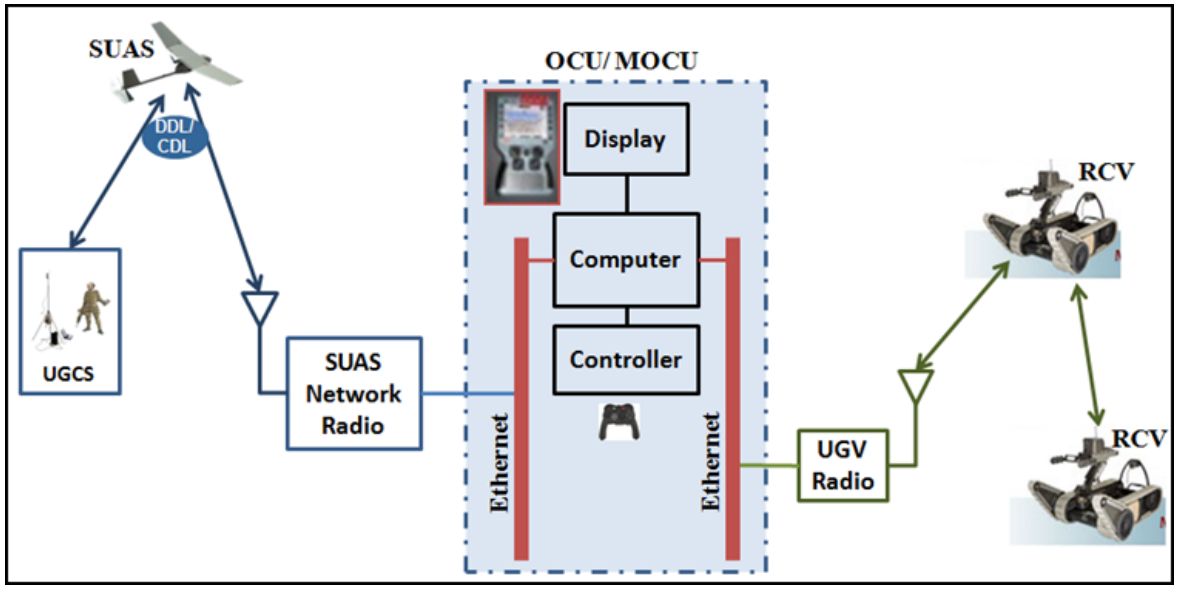


Figure 8: SUAS and UGV Network View

The operational view of the system will support tele-operation of one unmanned system at a time while allowing the viewing of a video stream from the other system for situational awareness. The capability of viewing of streaming video from the platform not being controlled may require higher end processors on the OCU/MOCU to provide adequate computational power. The system should also ensure QoS is lower on the secondary video feed so that tele-operation of the primary system is not compromised. Other text information can also be displayed from the secondary system to alert the operator of the status of the vehicle health or of a request to take control.

A.5.1 On-Board Network Interface Standards

The Table below shows the logical interfaces of currently fielded radios captured from a market survey by the Communications Working Integrated Product Team (WIPT) and radio vendors.

Interface	Format	# of Devices	Distance (meters)	Speed (Mbits/sec)
USB	Asynchronous serial	127	5	1.5/ 12/ 480/ 5000
IEEE-802.3 (Ethernet)	serial	1024	500	10/ 100/ 1000/ 10000
RS-232 (EIA/TIA-232)	Asynchronous serial	2	15 to 30	0.02 to 0.115
RS-485 (EIA/TIA-485)	Asynchronous serial	32	1000	10
I2C	Synchronous serial	40	6	3.4
IEEE-488 (GPIB)	parallel	15	20	8

Table 5: Data Interface Types

The logical interface will be comprised of one or more of the following logical interface connections: USB, Serial, and Ethernet. The following are industry standards that regulate these logical interfaces:

Ethernet - IEEE 802.3
USB - USB Forum
RS-232/485 - EIA/TIA (232/485)

A.5.1.1.1 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol is used to pass configuration parameters such as network addresses to nodes. There will be multiple DHCP servers operating on the same network. Therefore, DHCP servers must be carefully managed to avoid IP conflicts. DHCP servers must be configured so that their IP address pools do not overlap with each other.

A.5.1.1.2 Static IP support

Static IP addresses are needed for payloads that do not have a DHCP client on them. This will facilitate new payloads that were not originally part of the platform. Each system (OCU or Platform) shall have their own pool of static IP addresses. This pool shall not overlap with the IP address pool that resides in the DHCP server.

A.5.2 Network Topologies

This section depicts examples of different network topologies that could exist in an UGV system. Both Flat Networking topology and Routed Networking topology are supported in Communications IOP.

A.5.2.1 Flat Network Topology

There are two basic Flat Network topologies that will be described in this section. The figure below is the first example; here the OCU and Platform are networked together with no subnets. In this scenario, there is at least one DCHP server in the system and could be two, if the IP address pools are properly split between the DCHP servers. In this topology, the router with DHCP server could also be a switch with DHCP server.

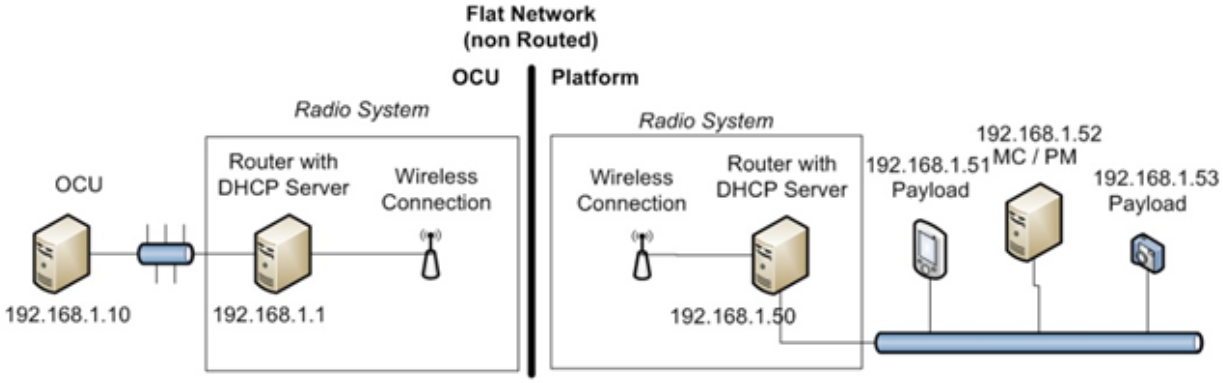


Figure 9: Flat Network

The figure below is another example of a flat network. In this network the radio system does not contain a router. The IP addresses of each component are statically assigned, so there is no need for a DHCP server.

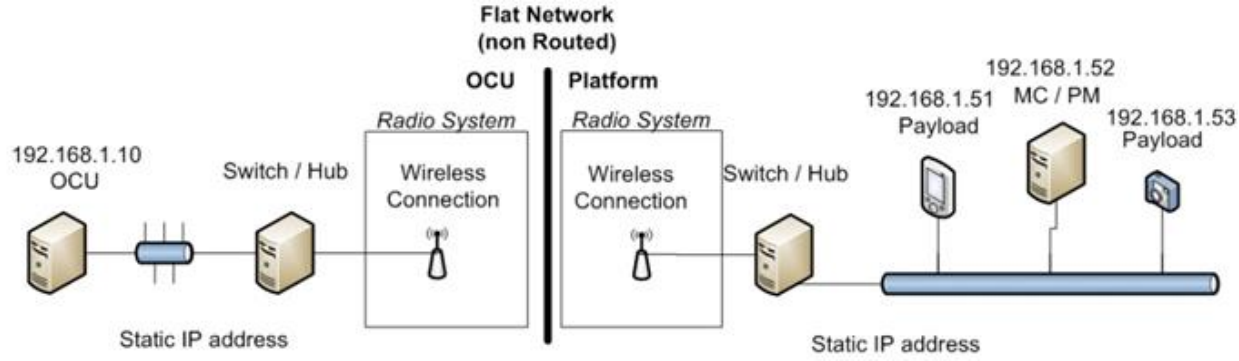


Figure 10: Flat Network (Static IP)

A.5.2.2 Routed Network Topology

There are three types of routed network configurations that will be discussed in this section. The first type of routed network is represented in the figure below. In this topology the radio IP addresses are fixed and the network is split up into subnets with no firewalls or Network Address Table (NAT). This type of network can contain multiple DHCP servers to manage IP address assignments corresponding to the appropriate subnet that the IP device is attached. To connect the subnets together a router is needed.

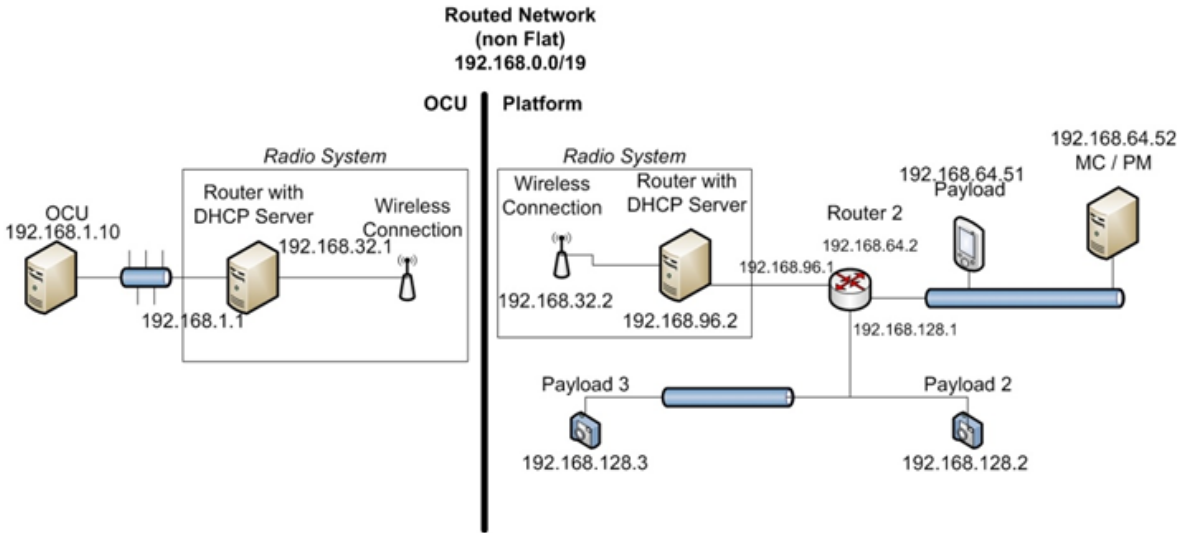


Figure 11: Routed Network Example (no firewall)

The next two types of network topologies below are here for reference only. The Communications IOP will not address the how to implement them.

The figure below is an illustration of a public/ private network. In this type of network, the communications passed between the OCU and platform is routed through larger public network. This network will contain firewalls at each point that the public (larger) and private (smaller) networks connect to each other. To effectively communicate across this network, advanced networking techniques such as port forwarding, firewall API's and the use of the demilitarized zone (DMZ) are needed.

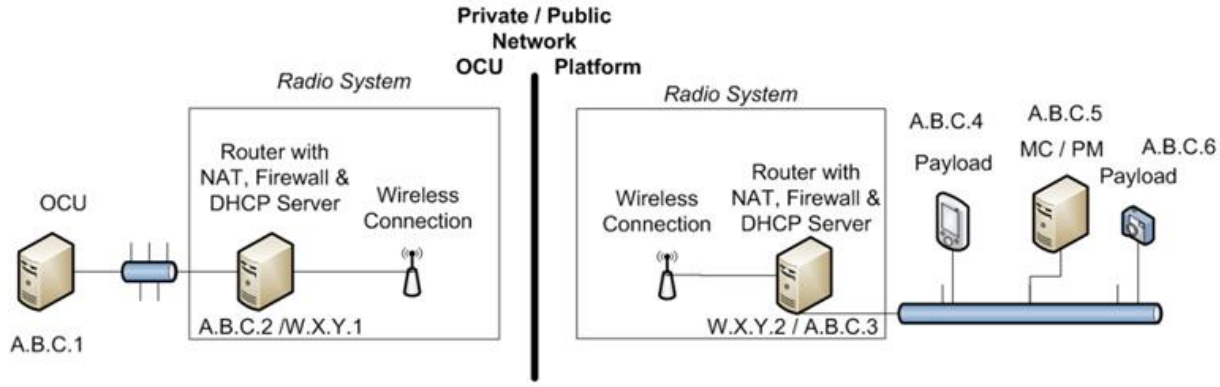


Figure 12: Public / Private, Firewalled Network Topology

The final network topology, shown in Figure 13, is a subset of the previous topology. Here the communication between the OCU and platform pass through several public networks. This architecture could contain any number of firewalls where communications can be established over popular supported ports of the public networks or through a virtual private network (VPN). These topologies are examples to provide visualization to the vernacular of this document.

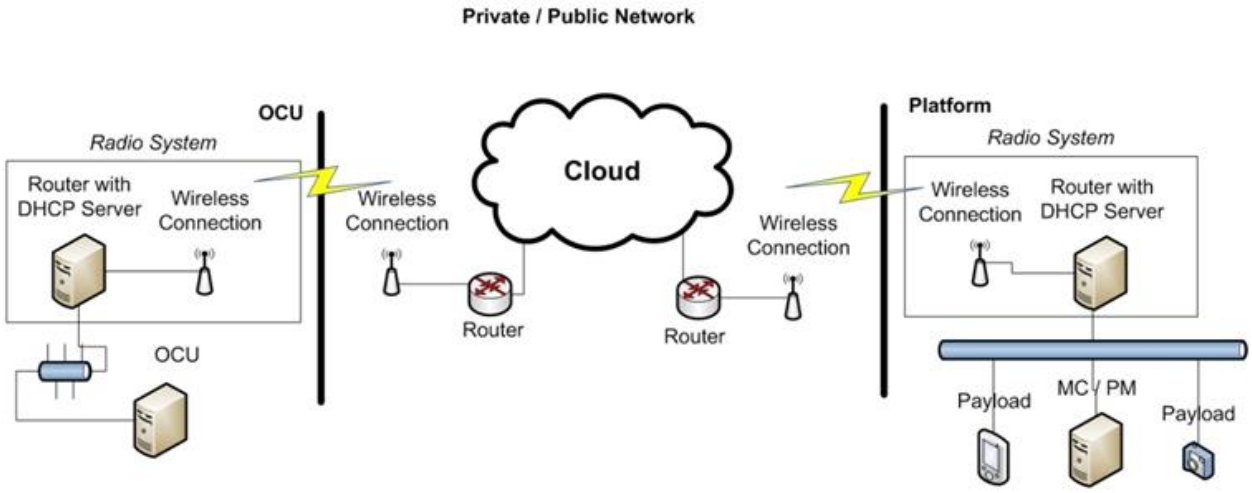


Figure 13: Cloud Networking Topology

A.5.3 Data Packet Handling Standards

A.5.3.1 Protocol Standards

A protocol is often defined as the rules governing the syntax, semantics, and synchronization of communication. This guidance addresses data communication packet types used on IP networks and identifiable by information found in IP packet headers. Several IP protocols are significant in that there are multiple subordinate packet types for the protocol with distinctive properties, identifiable through additional information in the packet headers. Internet Control Message Protocol (ICMP) packets are further distinguished by Type and Code. Packets for TCP and UDP are further identified by service (also called data service or application protocol), and port number.

A.5.3.2 Ports

Ports are a structural concept used to distinguish data services. It was designed to allow quick identification of a data service by examining the message header without any preexisting knowledge of ongoing communication or deeper packet inspection. As the use of TCP and UDP progressed, the one-to-one relationship between ports and the associated data service became weaker as there is no mechanism to enforce this relationship. As the need for interoperability between information systems grew, a central registry of port usage needed to be maintained. This function was incorporated into the Internet Assigned Numbers Authority (IANA). IANA maintains the central registry for TCP and UDP ports and their related data services. IANA divided the port address range (0 to 65535) into three ranges:

- Well Known Ports - defined as the range of assigned ports managed by the IANA with a range of 0-1023.
- IANA Registered Ports - defined as being listed by the IANA and on most system can be used by user process or programs without privilege with a range of 1024 - 49151.
- Dynamic Ports - defined as being available for private use with a range of 49152 - 65535.

Along with the Well Know Ports, Registered Ports and Dynamic Ports, there is a classification of temporarily assigned ports known as Ephemeral. Ephemeral ports are temporary ports assigned by a machine's Internet Protocol (IP) stack, and are assigned from a designated range of ports for this purpose. When the connection terminates, the ephemeral port is available for reuse, although most IP stacks won't reuse that port number until the entire pool of ephemeral ports have been used. So, if the client program reconnects, it will be assigned a different ephemeral port number for its side of the new connection.

A.5.3.2.1 Destination Port

The destination port number contained in the packet header to which a packet is sent from the originating machine that allows the identification of the service/application of the data or request is being sent to the destination machine. A process (binding) associates the service or protocol with a particular destination port number to send and receive data. On the destination machine, the process will listen for incoming packets whose destination port number and IP destination address match that port.

A.5.3.2.2 Source Port

The source port number contained in the packet header serves as analogues to the destination port and is used by the sending host to help keep track of new incoming connections and existing data streams.

A.5.3.2.3 Ephemeral Port

The Ephemeral ports are TCP or UDP ports dynamically selected by a client machine, in a client server environment, from a preconfigured port range for use in communicating with a server. The port usage is temporary and will only exist for the life of the communications session established. There are cases were the server opens a port in the ephemeral range to establish a separate connection back to the client. In these cases you can easily exhaust the ephemeral ports quickly if the port range is too small. The Ephemeral Port range was originally defined by BSD Unix as ports 1024 through 4999, however this overlaps the IANA registered port range, ports 1024 through 49151. There was a movement to change the Ephemeral Port range to 49152 through 65535 and in many communities (headed by the FreeBSD organization) have accepted this range. IANA refers to the range 49152 through 65535 as the Dynamic Range.

Recent submissions to the IETF suggest that the Ephemeral Port range should be considered all ports in the range 1024 through 65535 but there has been no formally acceptance of this.

A.5.3.2.4 Port Forwarding

Port Redirection is the method of changing the port number in route across the network (changing the routing daemon). Port redirection may be performed at the firewall or on the local server. Port redirection does not alter or hide the protocol in transit; only the port number is modified. Port redirection is not changing the coded port or port listening directly on server.

A.5.3.2.5 Protocol Tunneling (aka Port Tunneling or Nested Protocols)

Protocol Tunneling, sometimes referred to as Port Tunneling or Nested Protocols, is the method of encapsulating or wrapping or embedding a protocol through another protocol. Protocol tunneling may be unencrypted or encrypted. For example, when tunneling the TELNET protocol (port 23) through an encrypted SSH session over port 22, across the wire only the SSH protocol is visible and there is no indication that the TELNET protocol is transmitted. Popular client tools for protocol tunneling are SSH and HTTP Tunnel Client. A VPN (Virtual Private Network) is another form of tunneling (see section 1.1 Encrypted VPN Tunnels). Protocol tunneling may also be used in conjunction with Port forwarding.

For near-term systems, given the current protocol and port options there are two main potential network setups.

- A flat network (aka private network) where the DHCP is allowed to traverse the entire radio system from the UGV to the OCU. This setup is also known as a bridge network. There is no need for a NAT, port forwarding, tunneling, or other techniques that would normally be required on the public/private network. This type of network (flat) is easier to implement, but harder to maintain. May have limited future transition into more complex networks.
- A public/private network where there is a DHCP on each side of the radio system. NAT must exist on each side and port forwarding, virtual servers, demilitarized zones, tunneling, and other techniques must be used to traverse the private/public zone. This type of network is more difficult to implement, but easier to maintain. The potential for transition to more complex configurations with multiple OCU/OCU, OCU/UGV, and UGV/UGV interactions is better.

A.5.4 Time Management/ Time Reporting

In this document, Time Management refers to the act of synchronizing time between two nodes on a network. Time Reporting simply reports / request the current time to / from the targeted device. A method for time synchronization that is natively supported within the RAS-G Interoperability Profiles (IOP) is Network Time Protocol RFC5905 standard. This protocol has the ability to synchronize computers to within a few milliseconds. When established on Local Area Networks (LANs), this protocol can synchronize computers within one millisecond.

JAUS supports Time Reporting and is capable of requesting or reporting current time from and to the targeted JAUS components on the network. Both methods use UDP and Ethernet on the transport and link layer, respectively. It is also possible to implement the time service over JAUS via serial protocol.

Service	Transport	Standard
Network Time Protocol (NTP)	UDP	RFC 5905
JAUS - Time Service	UDP	SAE AS5710A
JAUS - Time Service	Serial	SAE AS5710A

Table 6: Time Management Communications Services

A.5.4.1 JAUS-Time Service

The Time Service allows clients to query and report the system time from other JAUS components. The Set Time message in the Time Service is deprecated. For more information please see SAE standard AS5710A.

A.5.4.2 Vehicle Networks

There are numerous vehicle communication networks in existence today. The Vehicle Networks Table provides an abridged list of some of the more popular architectures. In most cases, integration of a robotics system onto a vehicle will require a device that acts as a "gateway" between the networks. The "gateway device" will translate messages and signals from the existing vehicle network architecture to the JAUS robotic network. This device will also perform the translation of messages from the JAUS robotic network to the vehicle network. To not compromise the integrity of the existing vehicle network, the "gateway device" must be secure and model node Identification, protocols, messages, and signal identifiers on the native vehicle bus prior to integration.

Vehicle Network	Approx. Speed	STD	Comment
J1850	Low Data Rates	SAE J1850	
LIN	Low Data Rates	ISO 17987	
CAN	Up to 1 Mb/s	J1939, ISO 11898	
TTP	Up to 25 Mb/s	SAE AS6003	
FlexRay	Up to 10 Mb/s	ISO 17458-4	

Ethernet	100 / 1000 Mb/s	IEEE 802.3	http://articles.sae.org/12862/
DSRC	6 to 27 Mb/s	IEEE 802.11p, SAE J2735, SAE J3067, SAE J2945/1, ASTM E2213-03	

Table 7: Abridged listing of Vehicle Networks

The following standards developed by industry and academia for wireless communications of autonomous vehicle systems to exchange information between vehicles and infrastructure:

- **IEEE 802.11p:** Data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure
- **SAE J2735:** Dedicated Short Range Communications (DSRC) Message Set Dictionary
- **SAE J3067:** Candidate Improvements to Dedicated Short Range Communications (DSRC) Message Set Dictionary
- **SAE J2945/1:** On-board Minimum Performance Requirements for V2V Safety Communications
- **ASTM E2213-03:** Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems

Types of information exchanged over DSRC can include:

- Cooperative adaptive cruise control
- Intersection collision avoidance
- Approaching emergency vehicle warning
- Automatic vehicle safety inspection
- Transit or emergency vehicle signal priority
- Electronic toll collection
- Commercial vehicle clearance
- In-vehicle display of road signs and billboards
- Traffic data collection
- Rail intersection warning
- Blind spot warning
- Sudden braking ahead warning
- Rollover warning

A.6 RF INTERFERENCE MITIGATION

Wireless communications are impacted by interference whether intentional (Radio Frequency jamming) or unintentional (Electromagnetic Interference). RF Interference can originate from either friendly or unfriendly sources and is dynamically changing as technology evolves. EMI on the other hand can occur from just about anything that passes an electrical current where good design practices are not followed or because equipment is faulty and in need of repair.

To effectively maintain wireless communications the radio needs to be robust in these somewhat unpredictable harsh RF environments and adaptive so as to maintain communications link. There are four ways to minimize disruption of a wireless communications link:

1. Radio systems that lower the modulation complexity and/or channel bandwidth for a reduced data rate, aka Adaptive Code Modulation (ACM).
2. Changing frequency channel/ band. This can be done automatically or by swapping hardware that is plug and play.
3. Electrical antenna beam steering by pointing the antenna beam toward desired signal (e.g. MIMO).
4. Use another communications medium such as fiber optic tether.

The radio types in current use are listed in Table 9, along with relevant data regarding interference issues:

Type	**Purpose**	**Usage**	**RFIM features**	**Frequency Separation Requirements**
Narrowband:	Platform Control Functions (1)	Single Frequency Emission	1. Requires channel separation of at least 1 extra channel between adjacent users (practical Intermediate Frequency (IF) filter and phase noise issues). 2. Dominant interference mechanism is due to 3rd Order Intermodulation products satisfying the ±nF1±mF2 relation for all RF components in the spectrum where m+n=3. These components are generated by non-linear effects in the front end RF components of the receiver.	Vacant channel between users means center of adjacent channels used must always be > 2 x channel bandwidth, i.e. 50kHz for 25kHz V/UHF channels, or as small as 2 x 12.5kHz for APCO P25.
Narrowband: (cont.)	Platform Control Functions (2)	Frequency Agile Emitters	When hopping over large numbers of channels (>50), interference is restricted to those channels either containing an existing interferer, or with significant amplitude intermodulation components	To avoid packet collisions, GPS can be used to synchronize hops, but these techniques are not currently deployed in existing RS radios.

			satisfying the above ±nF1±mF2 relation (for all RF components in the spectrum within the input roofing filter). If the number of channels is small, then CRC or FEC techniques are used to remove those packet errors automatically. No cognitive radio techniques are employed in any of the known radios.	
Wideband:	Video downlink (1-way)	FM	Wide bandwidth requirement of FM modulation varies between 16 – 18MHz. These links are currently being phased out.	While raw step sizes of 250kHz are available, a minimum separation of > 4MHz is required between channels when a multi-system CONOPS is used.
	Video (1-way)	Digital Links	Digital links are much more efficient, and use narrower bandwidths (typically 2.5MHz)	Separation requirements depend critically on the signal processing and filtering used within the link, but typically require the same 2 x separation (i.e. 2 x 2.5MHz) when multiple systems are in use.
	Video and Control (2-way)	Digital Video with embedded control functions	They can use a separate channel integrated inside radio, use a subcarrier, or embed control data in the video data.	Ditto with 2x separation

Table 8: RF Interference Matrix

Note that all wideband links are susceptible to 2nd order intermodulation products satisfying the ±nF1±mF2 relation for all RF components in the spectrum where m+n=2. The damaging intermodulation products for wideband systems are generated by components present within the IF pass band, compared to narrowband systems where the dominant damaging products are generally outside the IF pass band (and produced by the first mixer). The narrowband interferers can be relatively easily removed, while the wideband interferers are amplified as part of the pass band and cannot.

One interesting variant of the wideband system is in current use. This system has the capability to measure the received quality of the wideband link at a designated frequency (F1), and automatically step in frequency to an alternate frequency (F2) within 0.5sec if the quality is poor. It would revert to F1 if the quality at F2 also proved poor, and try again. Only two frequencies are allocated, but this is a current concept similar to diversity that shows an explicit practical method of interference mitigation for wideband systems.

Another system samples the RF environment to detect a similar system already on that frequency. It then avoids transmitting on that channel as an interference mitigation technique.

A.6.1 Adjacent Channel Interference

RF radio links use front end and IF filtering to reduce the impact of images, ACPR, and intermodulation components in the pre-amplifiers, mixer(s), and other components such as filters. Isolation of about 40dB can be provided by commercial SAW filter technology, but these components are not available in the 4.4-4.9GHz band. Commercial technology still uses combinations of ceramic and other discrete components in this band - tunable filters can be constructed but they are large, clumsy and expensive. Industry has not been driven to invent new small filters yet in this band because there are no volume consumers (like cell phones) to drive the technology. Digitally tunable filters such as Pole-Zero components are helpful, but at a prohibitive price. Until demand has large enough volume to drive prices down, or make the R&D worthwhile, those components continue to lag availability of other components. We set performance limits by projecting receiver designs in nearby bands that have commercial volumes.

Conclusions: Interference mitigation is expected to be problematic until unwanted receiver responses can be reduced. A baseline for performance was established using SAW filter technology in designs for a radio in the 1.3GHz band. At 4.4GHz, discrete filters must be used since SAW devices are not available. An experiment was conducted to determine the degree of rejection of unwanted responses in typical receive system. Using this as a baseline, 4.4GHz receivers can be expected to match these goals only after further development of filter products to a similar level of refinement, availability, and price. The input frequency of a CW signal generator was tuned across the operating band and adjacent bands where images and other responses were known to exist. The results measured showed that:

a. Adjacent channel performance is poor in all receivers with selectivity between 15dB and 37dB. Such receivers should not be operated on adjacent channels within about 100m of each other.

b. 2nd and 4th adjacent channels provide ~50dB suppression of unwanted responses.

c. RF and IF image responses are suppressed by 52 and 61dB respectively.

d. Receiver designs have unwanted responses suppressed by >60dB for frequency offsets of >2MHz in narrowband receivers (using 230 kHz IF band pass filters).
e. Responses at offsets of 10MHz or more are generally suppressed by >70dB (except for specific RF and IF images)
f. SAW filters are available for IF filtering, but still lack the isolation to remove adjacent channel CW power. Stacking SAW filters provides a higher circuit loss that may approach 2x rejection of unwanted responses only in well designed & terminated circuits.
g. Image reject mixers would reduce significantly the effect of images on the radio link (currently between 51 and 60dB isolation) but there is a paucity of suitable devices that are not large and/or expensive.
h. Hybrid technologies could build such assemblies on ceramic or other substrates, but there is little demand as yet and low volume would make them expensive.

With the focus on this band for robotic platforms, there are compelling reasons to support new hybrid and lower cost components for RF filtering, image reduction, ACPR, and suppression of interfering signals. It is recommended that support for new components and fabrication methods be considered a part of V4 as a form of Frequency Interference Mitigation in dense environments.

Other Guidance: (a) In view of the need to operate multiple UGV systems in the same vicinity with minimum performance degradation, it is a recommendation that waveforms, power level adjustments, robust coding, and new filter components all be tailored especially for critical control links. (b) In addition, some form of frequency management should be developed to avoid operating in first or second adjacent channels when in radios are in close proximity.

A.6.2 RF Benchtop Test Methods for Adjacent Channel Performance

Figure 14: Adjacent Channel Systems below depicts the relationship between two similar radio systems, in terms of waveform and bandwidth, operating on the first or second adjacent channel of the system evaluated.

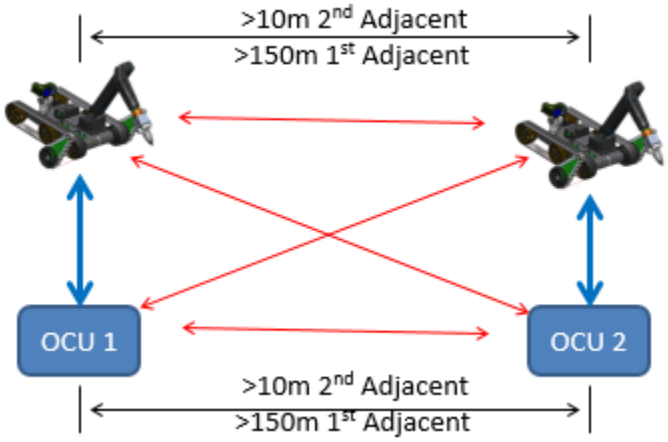


Figure 14: Adjacent Channel Systems

The test setup shown in Figure 15: RF Test Setup for Single Antenna System below employs two sets of similar radios, in terms of waveform and bandwidth, operating on different channels that could be on the first adjacent or second adjacent channel. This setup is for single antenna radio systems.

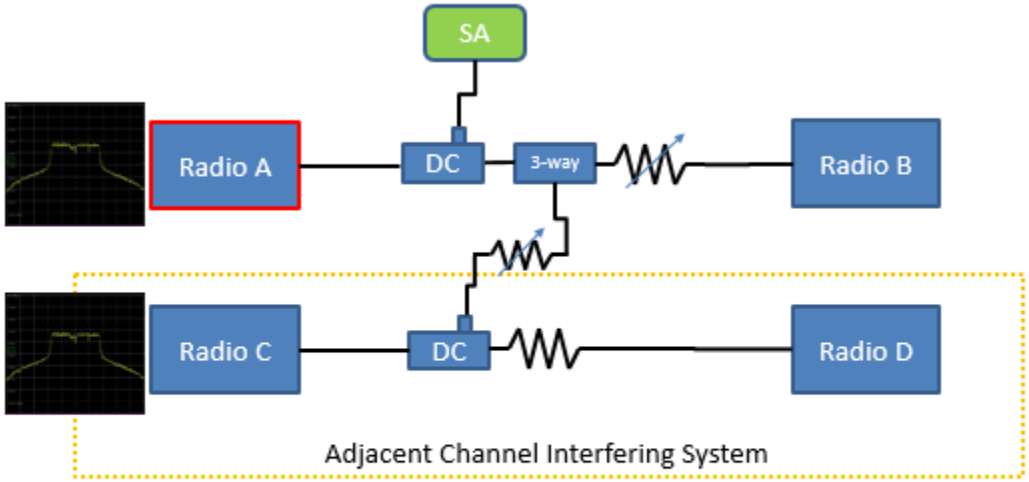
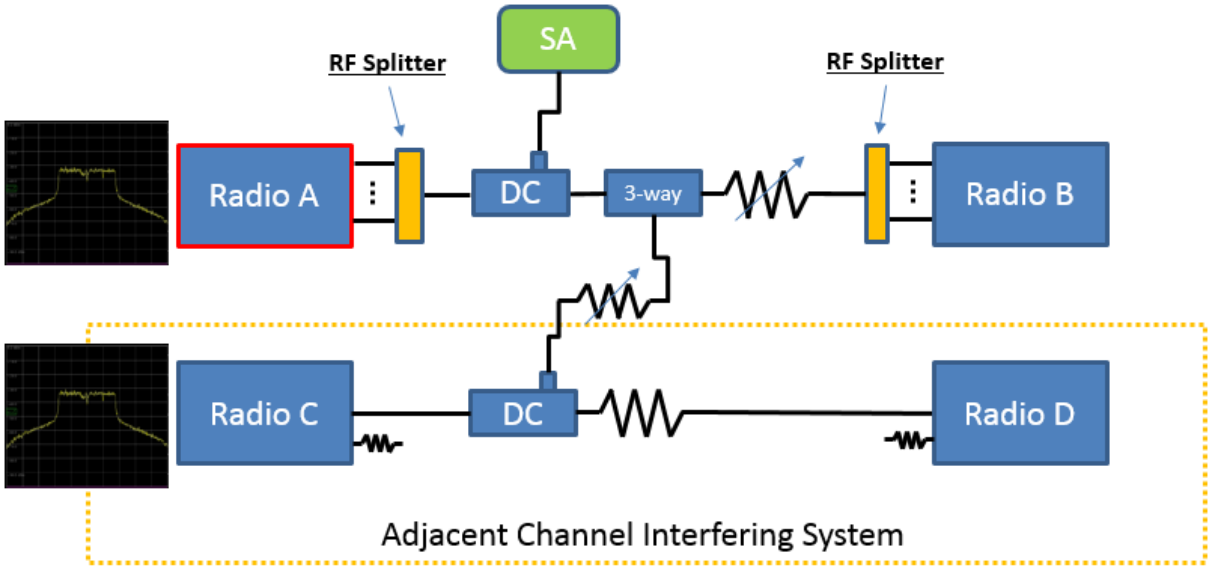


Figure 15: RF Test Setup for Single Antenna System

For MIMO type radio systems, RF attenuators placed on the extra antenna ports as a method to test however, this will negate the advantage that MIMO provides. A better test setup for MIMO type systems would be to use a RF splitter with cable leads of various lengths to simulate the antenna spatial separation of a MIMO radio as shown in Figure 16: Adjacent Channel Test Setup for MIMO below.

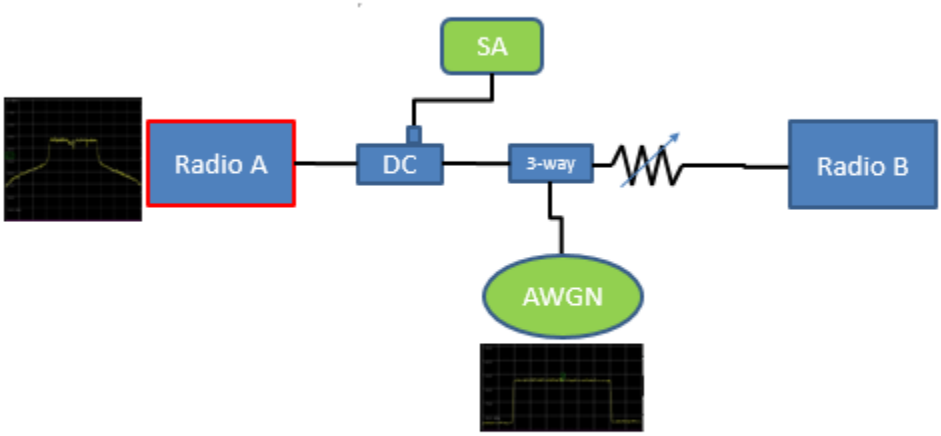


- Turn up radio A and B and reduce input to -85dBm.
- Measure error rate and data rate.
- Turn on radio C and D on 2nd adjacent channel and adjust input to 3-way at -85dBm.
- Measure error rate and data rate.
- Increase interfering signal in steps up to -35dBm and measuring at each step.
- Repeat for 1st adjacent channel to -60dBm interfering signal level.

Figure 16: Adjacent Channel Test Setup for MIMO

A.6.3 RF Benchtop Test Methods for RFI Performance

To evaluate radio performance in RF Interference (RFI) environments or co-channel interferers, such as from Electronic Warfare (EW) systems, the test setup shown in Figure 17: Co-channel or High RF Environment Test Setup below provides a straight forward test to simulate these environments.



- Turn up radio A and B and reduce input to -85dBm.
- Measure error rate and data rate.
- Turn on AWGN with leading BW edge at 2nd adjacent channel and adjust input to 3-way at -85dBm.
- Measure error rate and data rate.
- Increase interfering signal in steps up to -35dBm and measuring at each step.
- Repeat for 1st adjacent channel to -60dBm interfering signal level.

Figure 17: Co-channel or High RF Environment Test Setup

INTENTIONALLY BLANK

AEP-4818 Vol. VI (A)(1)