UGV Interoperability Profile (IOP)
Communications Profile
Version 0

Robotic Systems, Joint Project Office (RS JPO)
SFAE-GCS-UGV MS 266
6501 East 11 Mile Road
Warren, MI 48397

21 December 2011

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
21 DEC 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
UGV Interoperability Profile (IOP) Communications Profile, Version 0	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Robotic Systems, Joint Project Office (RS JPO),SFAE-GCS-UGV MS 266,6501 East 11 Mile Road,Warren,MI,48397**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**40**	

Table of Contents

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 Version 0 (V0) of this document, only the point-to-point interface between the Operator Control Unit (OCU) and the robotic platform/ UGV will be described. 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 under the control of Robotic System Joint Project Office (RS JPO). It is not the intention of this document to provide all requirements necessary, but to provide standard interfaces for the components to be designed around.

This document is developed and managed by the RS JPO, with inputs and assistance from industry and other Government organizations. This document serves as an interface agreement between the UGV provider(s) and its interfacing radio provider(s), and is maintained and controlled by the RS JPO.

1.2 Document Overview

This document provides the base concepts, architecture, requirements, and overview for the communications interoperability profile. The document is organized into seven sections:

1. Scope (this section)
2. Source documents
3. Communications Systems Architecture
4. Requirements
5. Off-Board Network Interoperability Attributes
6. Interoperability Attributes
7. Conformance and Validation Requirements

The latter part of this document addresses the conformance and validation requirements associated with the implementation of this IOP within an acquisition program.

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 for DoD. 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 to be deployed worldwide.

Current UGV radio communications are largely commercial-off-the-shelf (COTS) based, closed loop, point to point links between the UGV and the controller. For the most part, 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 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 NLOS conditions and with 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 support high data rates some UGV systems employ Orthogonal Frequency Division Multiplexing (OFDM) or Coded Orthogonal Frequency Division Multiplexing (COFDM) waveforms which have improved radio performance in a multipath environment.

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

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-DTL-17	General Specification for Flexible and Semi-rigid Cables, Radio Frequency
MIL-HDBK-189	Reliability Growth Management
MIL-HDBK-338B	Electronic Reliability Design Handbook
MIL-STD-810 G	Environmental Engineering Considerations and laboratory test
RFC 791	DOD Standard Internet Protocol (IPv4)

2.2 Non-Government Documents

IEEE 802.11	Telecommunications and information exchange between systems, - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
IEEE 802.3	Standards for Ethernet based LANs
SAE AS5669A	JAUS / SDP Transport Specification
SAE AS5710	JAUS Core Service Set standard
TIA/EIA-232/485	Electronic Industries Association/Telecommunication Industry Association TIA/EIA-232/485 and ITU V.28 (generally referred to as 232).
USB Forum	Universal Serial Bus Forum control standards
RFC 2460	Internet Protocol, Version 6 (IPv6) Specification
RFC 2131	Dynamic Host Configuration Protocol
RFC 2132	DHCP Options and BOOTP Vendor Extensions

3 Communications Systems Architecture

3.1 Notional Block Diagram

The role of the CCL is to reliably and efficiently provide a 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 for IOP V0 (i.e., point-to-point) is presented below in Figure 3-1. This architecture depicts general components integrated within the CCL and serves as a baseline for the organization and discussion of technical requirements. The primary CCL subsystems contained within the block diagram are further described below.

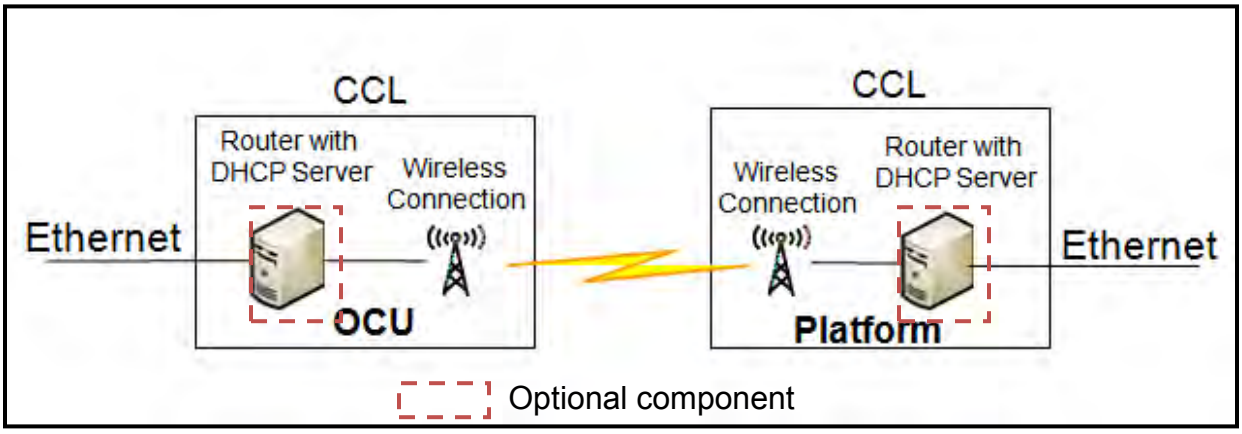

Figure 3-1 CCL Systems Block Architecture

3.2 CCL Architecture

The CCL architecture as shown in the diagram above will support an Ethernet interface at the OCU and 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 On-Board Network Interoperability Attribute has four selectable, non-mutually-exclusive values listed in the Attributes Table of Section 6 of this document. 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.

3.3 Air Interface/ Waveform

For IOP V0 the Air Interface/ Waveform of the Communications Link will be defined by the radio vendor to meet the requirements of the system.

3.4 Quality of Service

Quality of Service (QoS) requirements is not within the scope of IOP V0 as this will be handled uniquely by the acquisition program. However, standards that provide for the physical realization to perform QoS are defined in this *UGV IOP Communications Profile*.

3.5 Boundary Diagram

The Boundary Diagram of the CCL is presented in Figure 3-2 below provides focus areas of the radio system toward interoperability of UGV communications.

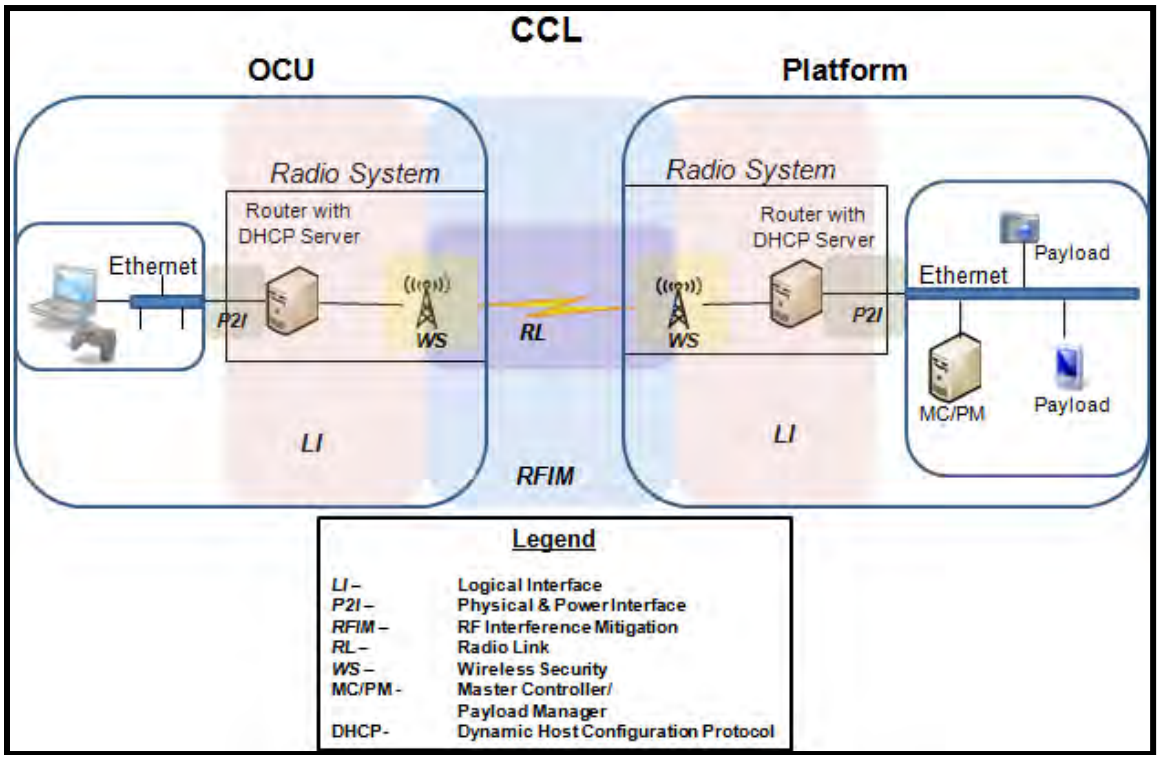

Figure 3-2 CCL Boundary Diagram

The boundary areas of the CCL define specific aspects of the UGV 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.

3.6 Tethered Communications

Tethered communications link replaces the wireless communications link with either fiber optic cable or a twisted wire pair.

4 Requirements

4.1 Physical Interface

4.1.1 Connectors

4.1.1.1 Data Connectors

[COMM 001] 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.

4.1.1.2 Antenna Connectors

[COMM 002] The 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
- MMCX type-female

[COMM 003] The antenna port of the radio system shall be weatherproof, low loss with 50 Ohm impedance.

4.1.2 Power

[COMM 004] The CCL input power shall be auto-ranging supporting a minimum voltage range of 10 to 28 VDC.

4.2 Logical Interface

4.2.1 Network Standard

[COMM 005] The primary on-board network standard shall be derived from the IEEE 802.3 standard for Ethernet communication.

[COMM 006] 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.

4.2.2 Addressing Standard

[COMM 007] The primary addressing standard for IOP V0 shall be IP version 4 (IPv4) and will accommodate for future IP version 6 (IPv6) migration per DoD guidelines.

[COMM 008] A CCL system with an On-Board Network Interoperability Attribute Value of Routed Network shall be capable of enacting Dynamic Host Configuration Protocol (DHCP) to enable the automatic IP address assignment of payloads and other Ethernet systems.

[COMM 009] The CCL system shall be capable of enacting Routing for IP packets between CCLs and system they support.

[COMM 010] The CCL system shall support routed type networks.

[COMM 011] The IP address assignment list shall be provided in accordance with JAUS transport section 4.1.4 of the *JAUS Profiling IOP*.

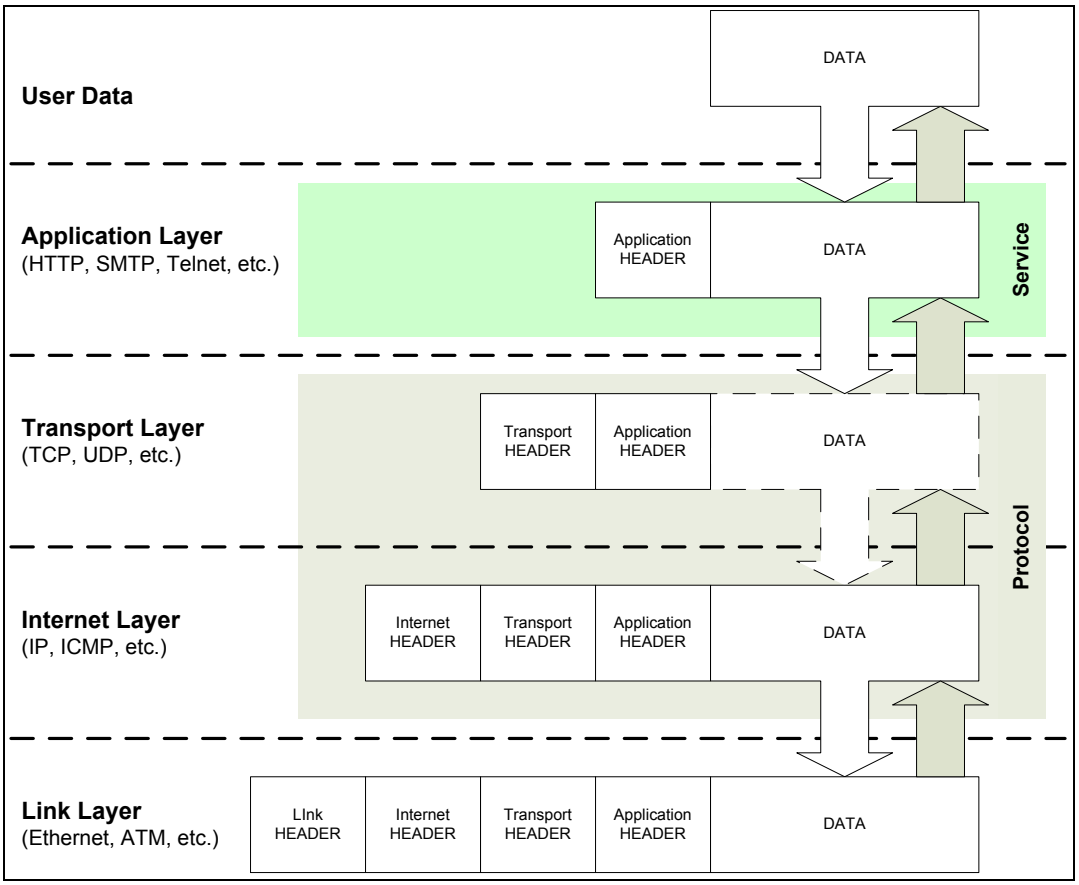

Figure 4-1 Network Layer Chart

4.2.3 Data Packet Handling

[COMM 012] The CCL system shall be able to manage packets within the IEEE 802.3 protocol standards per Figure 4-1.

4.2.4 IP Addressable

[COMM 013] The CCL radio shall be IP addressable for plug and play capability. IP shall be the standard protocol for CCL Network Layer.

4.3 Radio Link

4.3.1 Frequency Channel Selection

[COMM 014] The radio shall be capable of tuning across the frequency band of operation in increments of one channel bandwidth (BW).

4.3.2 Bandwidth Selection

[COMM 015] 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.

4.3.3 RF Transmit On/Off

[COMM 016] 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.

4.3.4 Max Transmit Power

[COMM 017] 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.

4.3.5 Min Transmit Power

[COMM 018] 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..

4.3.6 Tethered Operation

[COMM 019] The radio communications shall be capable of ceasing/ terminating RF transmissions when tether communications is employed.

4.4 Wireless Security

4.4.1 Encryption

[COMM 020] The radio shall be capable of employing Advanced Encryption Standard (AES) with a minimum 128-bit key length or similar encryption protocol that will provide the same or better protection.

4.4.2 Encryption Bypass

[COMM 021] The radio shall be able to bypass encryption using JAUS messages in accordance with the *Custom Service Messages & Transports* document.

4.5 Radio Frequency Interference Mitigation

4.5.1 Frequency Band Selection

[COMM 022] The radio communications system shall be capable of changing the frequency band of operation either by swapping hardware or through software commands.

4.5.2 Adjacent Channel

[COMM 023] The communications link shall be able to operate without degradation of radio communications range performance on second adjacent channels transmitting in the same immediate area of operation.

4.6 Waveform Requirements

4.6.1 Ground to Ground Communications Waveform

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

4.6.2 Data Rate

[COMM 024] The radio communications video link shall support a data rate of 1.8 Mbps or better.

[COMM 025] The radio communications telemetry and audio link shall support a data rate of 200 kbps or better.

[COMM 026] 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.

5 Off-Board Network Interoperability Attributes

For V0 IOP the off-board networking capabilities will be limited to closed networking that does not share information outside of the OCU and the platform. However, additional interoperability attributes will be defined in future revisions to specify CCL options. These attributes will include mobile, ad-hoc networking, mesh and repeater/ relay networking and sharing of information on the battlefield. Eventually, the CCL will tie into the Global Information Grid (GIG).

5.1 Basic Point-to-Point Communications Network (OCU ← → Platform)

At its most basic level a network can consist of two 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 suggested that IEEE 802.11 standard be used for wireless communications as a common waveform that is robust in multipath environments and supports high data rates.

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.

5.2 Basic Point-to-Point Network 2 (OCU ← → Multiple Platforms)

As an extension to the network defined in 5.1, an 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. Only one UGV could be controlled at a time. Other OCUs could be configured the same way, for the same set of UGVs. All other requirements are the same as in 5.1. Imaging data will also be shared with remote video terminals capable of receiving the radio signals from the UGV.

5.3 Repeater/ Relay Network (OCU ← → Relay ← → Platform)

While not within the scope of IOP V0, this communications network extends the range of the OCU – Platform through a relay or repeater link. The relay could be through UAV, UGV or a radio brick.

5.4 Multi-node Network (Multiple OCUs ← → Multiple Platforms)

While not within the scope of IOP V0, this network paradigm is commonly referred to as Mesh or Mobile Ad-hoc Network (MANET) in which networks are set up and broken down by finding the best path to get data from the OCU to the platform.

5.5 Cloud Network

Cloud networks are not within the scope of IOP V0 however following the paradigm of the World Wide Web, OCUs and UGVs can be part of a 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.

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. Discovery for a network such as this is more involved than in a simple PTP network. Discovery first starts with discovering a platform, and then assuming control over that platform via the OCU. Once control is established the discovery of the payload components can take place.

6 Interoperability Attributes

The following table specifies the set of Interoperability Attributes defined within this IOP. These attributes are used to specify required interoperable capabilities to be implemented within a robotic system. The specification of an Interoperability Attribute may imply additional requirements defined in other portions of the IOP.

Attribute	Paragraph	Title	Values
Waveform	3.3	Air Interface/ Waveform	OFDM, COFDM, DDL, CDL, None
OCU to Platform Communications	3.5 - 3.6	Radio & Tethered Communications	CCL, Optical Tether, Wired Tether, None
RF Connector	4.1.1.2	Antenna Connectors	SMA-female, TNC-female , N type-female, MMCX-female
Input Power	4.1.2	Power	Auto-sense 10-28 VDC
Network Interface Standard	4.2.1	Network Standard	Ethernet, USB 2.0, RS232, RS422, RS485
IP Addressing	4.2.2	Addressing Standard	IPv4, IPv6
On-board Network	4.2.3	Data Packet Handling	Flat Network with static IP assignment, Flat Network with DHCP, Routed Network, None
Channel Bandwidth Agility	4.3.2	Bandwidth Selection	Adjustable, None
Wireless Encryption	4.4.1	Encryption	AES128, None
Encryption Bypass	4.4.2	Encryption Bypass	Bypass, None
Frequency Band Selectable	4.5.1	Frequency Band Selection	Support Multiple Frequency Bands, None
Data Rate	4.6.2	Data Rate	>1.8 Mbps for video, >200 kbps for telemetry, >2.0 Mbps for video and telemetry None

Attribute	Paragraph	Title	Values
Off-Board Network Attributes	5.	Network Interoperability Attributes	OCU/Platform PTP paired, OCU/Platform PTP independent, OCU/Repeater/Platform, Mesh/MANET Network, Cloud Network

7 Conformance and Validation Requirements

The table below specifies the conformance requirements associated with this IOP. This matrix maps product unique identifiers (PUIs) to applicable IOP requirements, paragraph numbers, titles/subtitles, and planned verification methods. System Developers, Conformance and Verification Testers, and Acquisition Managers can use this matrix to help validate conformant implementations to this IOP. The following verification methods are defined:

Analysis – Analysis is an element of verification that uses established technical or mathematical models or simulations, algorithms, charts, graphs, circuit diagrams, or other scientific principles and procedures to provide evidence that stated requirements were met.

Examination – Examination is an element of verification that is generally nondestructive and typically includes the use of sight, hearing, smell, touch, and taste; simple physical manipulation; and mechanical and electrical gauging and measurement.

Demonstration – Demonstration is an element of verification that involves the actual operation of an item to provide evidence that the required functions were accomplished under specific scenarios. The items may be instrumented and performance monitored.

Test – Test is an element of verification in which scientific principles and procedures are applied to determine the properties or functional capabilities of items.

PUI	Paragraph	(U)	Title	Verification Method				
				A	E	D	T	N/A
001	4.1.1.1	U	Data Connector (Platform)	A				
002	4.1.1.2	U	Antenna Connector	A				
003	4.1.1.2	U	Antenna port	A				
004	4.1.2	U	Power	A				
005	4.2.1	U	Network Standard - Primary	A				
006	4.2.1	U	Network Standard - Secondary	A				
007	4.2.2	U	Addressing Standard	A				
008	4.2.2	U	Addressing Standard	A				
009	4.2.2	U	Addressing Standard	A				
010	4.2.2	U	Addressing Standard	A				
011	4.2.2	U	Addressing Standard	A				
012	4.2.3	U	Data Packet Handling	A				
013	4.2.4	U	IP Addressable			D		
014	4.3.1	U	Frequency Channel Selection			D		
015	4.3.2	U	Bandwidth Selection			D		
016	4.3.3	U	RF Transmit On/ Off			D		
017	4.3.4	U	Max Transmit Power			D		
018	4.3.5	U	Min Transmit Power			D		
019	4.3.6	U	Tethered Operation			D		

PUI	Paragraph	(U)	Title	Verification Method				
				A	E	D	T	N/A
020	4.4.1	U	Encryption	A				
021	4.4.2	U	Encryption Bypass	A				
022	4.5.1	U	Frequency Band Selection			D		
023	4.5.2	U	Adjacent Channel			D		
024	4.6.2	U	Data Rate			D		
025	4.6.2	U	Data Rate			D		
026	4.6.2	U	Data Rate			D		

8 Appendix A – Acronyms and Abbreviations

ACM	Adaptive Code Modulation
APC	Adaptive Power Control
ATPC	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 Remote Control Improvised Explosive Device Electronic Warfare
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DoD	Department of Defense
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	Internet Control Message Protocol
IETF	Internet Engineering Task Force
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
Mbps	Megabits per second
MC/PM	Master Controller/ Payload Manager
MHz	Megahertz
MIMO	Multiple Input Multiple Output
MMCX	Micro-Miniature Coaxial
NAT	Network Translation Table
NLOS	Non- Line of Sight
NSA	National Security Agency
OCONUS	Outside Continental US
OCU	Operator Control Unit
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
P2I	Physical/ Power Interface
POE	Power Over Ethernet
PUI	Product Unique Identifier
QoS	Quality of Service
RCIED	Remote 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

9 Appendix B - Discussion of Technical Topics

9.1 Networking Concepts

9.1.1 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.

9.1.2 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.

9.1.3 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.

9.2 IP Addressability

An IP-based network layer provides flexibility in the data link 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.

9.3 RF Transmission Waveform

There are many different forms of modulation techniques available for RF transmission of digital signals over the air. However, two attributes that drive the RF transmission waveform for ground-to-ground communications used for UGVs is that it must be resilient to multipath fading and support high data rates for teleoperation. Orthogonal Frequency Division Multiplexing or OFDM is a modulation technique that performs well with respect to these requirements and additionally provides efficiency for the transmission of high data rates over a limited bandwidth.

OFDM and COFDM have gained a significant presence in the wireless market place which includes wireless routers and digital television transmission. The combination of high data capacity, high spectral efficiency, and its resilience to interference from multi-

path effects means that it is ideal for the high data applications that are becoming a common factor in today's communications scene.

Studies on CDMA, DSSS, and ultra-fast sweeping waveforms show that spreading the information content of a system over wider bandwidths can allow robust recovery at the receiver, even in the presence of interference. These schemes may be considered inefficient with respect to bandwidth, but the schemes are still able to survive jamming signals.

9.3.1 RF Performance

RF performance is largely defined by the mission; e.g., line of sight (LOS) or non-line of sight (NLOS) or beyond line of sight (BLOS), data rate requirements, latency and environment.

9.3.2 Range

LOS requirements for UGVs are necessary to provide the Warfighter the standoff distances necessary to operate a UGV safe from threats. Mission that include building clearance, caves, sewers, foliage, etc. require NLOS communications which reduces the range due to multipath and signal blockage. Frequencies in the lower part of the spectrum (below 1 GHz) have better propagation characteristics and can propagate farther in NLOS conditions. BLOS are communications links that extend beyond the horizon and require a repeater or network link.

9.3.3 Bandwidth

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

9.3.4 Data rate/ Throughput

The data rate has a direct impact on RF bandwidth and DoD regulations require efficient use of RF spectrum. For Unmanned Systems (UMS) the communications link is for the most part comprised of a two-way telemetry data link, a two-way audio and one-way video link from the platform to the controller. The telemetry data link provides the command and control, heartbeat and status updates of the robot and its payloads as well as the status of the UGV. The video link is one-way, transmitting from the robot to the OCU. The video signal is compressed using an encoder to digitize and compress the signal to minimize the bandwidth requirement. Table 9-1 below defines nominal data rates to support Full VGA video; however high definition or 3D video will require higher data rates.

	Resolution		Color	Frames per	MPEG-2	Data Rate	H.264	Data Rate
	H	V	Depth	Second	compression	(Mbps)	Compression	(Mbps)
Full VGA	640	480	24	30	28	7.90	56	3.95
Full VGA	640	480	24	15	28	3.95	56	1.97
Full VGA	640	480	24	10	28	2.63	56	1.32

Table 9-1 Nominal Video Data Rate Requirements Chart

9.3.5 Latency

In a UGV system, latency in communications of data can be induced in various points, such as physical transmission, communication link processing, environment, payload (such as sensor or human in the loop, perceptor/effector), etc. The focus of this profile is on the latency attributed to the communications link processing.

Digital radios provide superior bandwidth efficiency over analog radios however the packetizing and compression of the video can induce significant delay/latency in the delivery of the signal. Low latency is required for real-time teleoperation of UGV(s) to maneuver around obstacles and avoid damage to or from the UGV. Most latency in the wireless communications system is attributed to the encoders, interleaving and encryption. Higher latencies may be tolerated for UGVs that have autonomous capabilities.

The way data is handled can also affect latency in Internet Protocol (IP) data streams. For example, Transmission Control Protocol (TCP) employs error correction facilities to requesting the information be retransmitted. This error correction is good where guaranteed delivery of data is required. However, for streaming video Universal Data Protocol (UDP) is a better transmission method where error checking and retransmission are not required. UDP is a standard defined in IETF Standard 6/RFC 768 and TCP standard is in IETF Standard 7/RFC 793.

9.4 Frequency Bands

The UGV communication links operate in the mobile radio communication service which is designated by the host nation spectrum authority. In April 2008, a frequency band study (Document Control No. JSC-CR-07-120) was conducted to determine if there were frequency bands that would be able to support the All-Purpose Remote Transport System (ARTS) on a worldwide basis (see Table 9-2 below). The results of the study found that no single communications system was globally accepted or designed to work on all the indicated frequency bands and will require a multiple radio solution to switch to different frequency bands. 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.

Frequency, MHz	Government Allocation Status	Usage	International Allocation Status		
			Region 1	Region 2	Region 3
225 - 230	P	G	S	P	P
230 - 235	P	G	P	P	P
235.0 - 328.6	P	G	P	P	P
335.4 - 399.9	P	G	P	P	P
1350 - 1390	P	G	P	N	N
1710 - 1755	N	NG	P	P	P
1755 - 1850	P	G	P	P	P
2200 - 2290	P	G	P	P	P
2290 - 2300	P	G	P	P	P
2300 - 2305	N	N	P	P	P
2305 - 2310	N	NG	P	P	P
2310 - 2320	S	M	P	P	P
2320 - 2345	N	N	P	P	P
2345 2360	S	M	P	P	P
2360 - 2390	P	M	P	P	P
4400 - 4500	P	G	P	P	P
4500 - 4800	P	M	P	P	P

P	-	Primary
S	-	Secondary
G	-	Federal Government
M	-	Shared Government and non-Government
N	-	Not Allocated
NG	-	Non-Federal Government

Table 9-2 DISA JSR Study - Frequency Bands

Spectrum management is key factor to robust radio communications. In general, lower frequencies (less than 1GHz) propagate farther and are better at penetrating through and around obstacles for NLOS communications. For this reason, lower frequencies are in higher demand, congested and are usually bandwidth limited. Higher frequency bands are generally more available and can accommodate higher bandwidths and data rates but do not propagate as far especially for NLOS. The current direction is to use 4400 to 5000 MHz frequency band for UGV radio communications however even this spectrum is being reallocated for other use in countries outside the CONUS. Therefore, radios will need to be adaptable to support several frequency bands with minimal or no changes to radio hardware. Software Defined Radio (SDR) technology provides the capability to dynamically change frequencies and waveforms through software.

9.4.1 Potential UGV Spectrum Utilization

225-400 MHz – Federal Spectrum- sometimes used for wideband video where extreme range and penetration is required-usually used for command and telemetry, narrowband comms.
433.05-434.79 MHz- FCC Spectrum-US and Euro ISM band, license free, narrowband telemetry, command and control.
458.5-459.5 MHz-Euro ISM license free, narrowband telemetry, command and control.
868-870 MHz- Not used in CONUS, euro ISM band, narrowband telemetry, command and control.
902-928 MHz- FCC Spectrum-US ISM band, license free, narrowband telemetry, command and control.
1350-1390 MHz – Federal Spectrum- Commonly used for command and telemetry.
1625-1725 MHz- Federal Spectrum- Wideband video and data transmission- DDL.

1755-1850 MHz- Federal Spectrum-This band is rapidly going away in CONUS due to spectrum auctions but was previously extensively used for wideband video transmission. Internationally it is often not available due to GMS cellular systems.
2200-2290 MHz- Federal Spectrum- This band is extensively used in CONUS as well as internationally, where available, for wideband video and data transmission. This band is available on a secondary basis in CONUS since it is also used for Space Communications.
2310-2390 MHz- Federal Spectrum- This band is extensively used in CONUS as well as internationally, where allowed, for wideband video and data transmission. This band is available on a secondary basis in CONUS since it is also used for aeronautical flight test telemetry.
2400-2483.5 MHz-FCC Spectrum- This band is frequently used by non-federal agencies under FCC Part 90 rules for wideband video and data transmission. Shared with license free Part 15 devices.
4400-4940 MHz-Federal Spectrum- This band is frequently used by federal agencies for wideband video and data transmissions it is also a “NATO Harmonized” band which means it is frequently available for use internationally by authorized agencies, when used internationally the band upper limit is 5000MHz.
4940-4990 MHz-FCC Spectrum- “Public Safety Band” in CONUS. Sometimes used for UGV comms but there are strict restrictions on how the band is used as well as RF output power levels.
5725-5875 MHz- FCC Spectrum- ISM band, wideband data and video, license free shared spectrum.

9.4.2 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.

9.4.3 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 (ATPC) 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. ATPC is very useful in preventing this near-field/far-field type of problem.
3. Weak signal range extension: When a signal drops towards 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 extent 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.

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

Different signal quality parameters can be used to drive the ATPC, 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. ATPC 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.)

9.4.4 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 researchers 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 need 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. DoD 5200.1-M Anti-tamper techniques will be used with UGV's. In addition, Data At Rest (DAR) measures will be implemented in Robot 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.

The National Security Agency (NSA) defines the requirements for military security for telecommunications and automated information systems for the protection of information. Type 1 products are the highest level of security and may be more than required for most UGV missions. Type 2 products cannot handle classified information but do handle Sensitive But Unclassified (SBU), which would handle most UGV mission profiles. However, there are 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.

9.4.4.1 **Wireless Security Recommendations for current radios:**

- Radios *should* operate with AES Encryption.
- Radios *should* use 128-bit keys, refraining from 256-bit keys for export/ITAR concerns

- Latency *should* be less than 2 milliseconds due to the encryption/decryption process.

9.4.5 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.

9.4.6 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 lowers the modulation complexity and/or channel bandwidth for a reduced data rate, aka Adaptive Code Modulation.
2) Changing frequency channel/ band. This can be done automatically or by swapping hardware that is Plug and Play.
3) Antenna beam steering by pointing the antenna beam toward desired signal.
4) Use another communications medium such as fiber optic tether.

The radio types in current use are listed in Table 9-4, 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 IF filter and phase noise issues). (2) Dominant interference mechanism is due to 3rd Order Intermodulation products satisfying the $\pm nF_1 \pm mF_2$ 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, ie 50kHz for 25kHz V/UHF channels, or as small as 2 x 12.5kHz for APCO P25.

	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 satisfying the above $\pm nF_1 \pm mF_2$ 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.	To avoid packet collisions, GPS can be used to synchronize hops, but these techniques are not currently deployed in existing RS 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 (ie 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 9-4 RF Interference Matrix

Note that all wideband links are susceptible to 2nd order intermodulation products satisfying the $\pm nF_1 \pm mF_2$ 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 passband, compared to narrowband systems where the dominant damaging products are generally outside the IF passband (and produced by the first mixer). The narrowband interferers can be relatively easily removed, while the wideband interferers are amplified as part of the passband 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.

9.4.6.1 Adjacent channel Interference capability of existing radios

Table 1 provides a summary of the performance attributes of both NB and WB radios. There are significant advantages to separating low bandwidth Control functions from more vulnerable wideband receiver architectures. Narrowband designs will always be able to be designed with less vulnerability than wideband receivers if they can hide their signals in amongst other signals and are not detected. More recently, frequency hopping filters provide even more evidence that practical narrowband receivers can be constructed that significantly improve survivability against RF interference from 3rd order IM products. In addition the separation of co-sited channels has been addressed for current radios in Table 1 using current radio technology. By contrast there are other technologies which involve ultra-fast sweeping modulations with sophisticated coding that can be hidden below the interference unless the code is available to coherently detect and demodulate the signal. All these techniques are not yet available in current radios. The comparative studies are deferred to V1.

Evidence of the lower vulnerability (improved resistance) of frequency hopping radios to interference is apparent in the 902-928MHz ISM band. Single frequency radios are particularly useless in this band which relies on both DSSS and FH technology to achieve any reasonable range.

9.4.7 Discovery and Handoff

UGV radios will need intelligent software for discovery of other CCL systems to support higher level requirements associated with discovery and handoff.

9.5 Networking

The CCL provides a communications link between the OCU and a UGV(s) for the exchange of data, video and payload information as shown below in Figure 9-1.

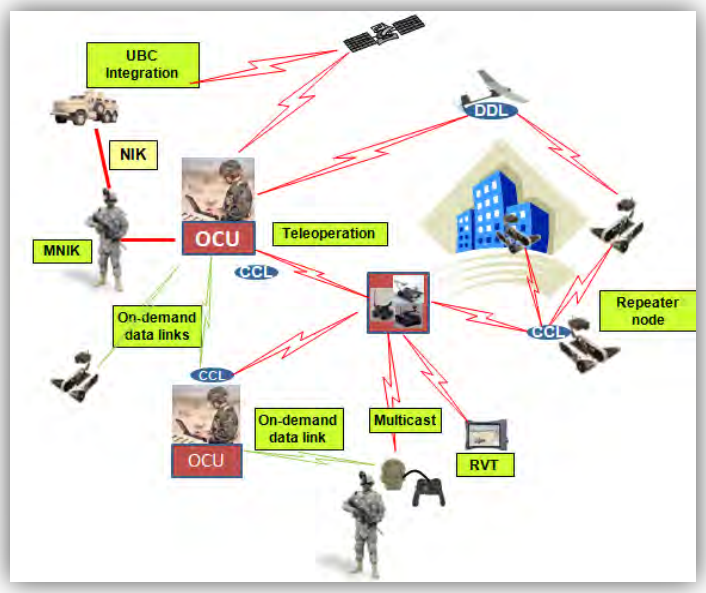

Figure 9-1 CCL Network Topology

The video and payload data may also be shared on the battlefield to provide situational awareness to Remote Video Terminals (RVT). A low data rate link between a shooter with an RVT and the OCU provides ability to have voice communication or texting. A Warfighter will also be able to have limited control of UGV payloads.

9.5.1 Network Standard:

The table below, *Table 9-5*, shows the logical interfaces of current radios that have been fielded. A request was sent to Communications WIPT members requesting feedback on the logical interface from their respective radio systems. The logical interface will be comprised of the following system connections: USB, Serial, and Ethernet. There are exceptions to the bounds for V0, but future will focus on those three connection types. The following table is the capture from the Communications WIPT members of the current connection types.

Interface	Format	# of Devices	Distance (meters)	Speed (mbits/sec)
USB	asynchronous serial	127	5	1.5/12/480
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 9-5: Data Interface Types

There are several industry standards to help regulate the logical interface standards and are as follows:

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

9.5.2 Addressing Standard:

The IPv4 has been in use for over 30 years and cannot support emerging requirements for address space, mobility, and security in peer-to-peer networking. The IPv6 is an improved version of IP, which will coexist with IPv4 and eventually replace it in most networks. The key characteristics of IPv6 are designed to increase address space, promote flexibility and functionality, and enhance security. Address space of 128-bits increases the available Internet address space from approximately 4.3 billion in IP Version 4 (IPv4) to approximately 3.4×10^{38} in IPv6. Other characteristics increase flexibility and functionality, including improved routing of data, enhanced mobility features of wireless, configuration capabilities to ease network administration, and

improved QoS. Further, IPv6 integrates IP Security (IPSec) to improve authentication and confidentiality of information being transmitted.

In IPv4, the reserved IP addresses (0.0.0.0/8 and 127.0.0.0/8), there are other addresses not used on the public Internet. These private subnets consist of private IP addresses and are usually behind a firewall or router that performs NAT (network address translation). NAT is needed because private IP addresses are non-routable on the public Internet, so they must be translated into public IP addresses before they touch the Internet.

The following blocks of IP addresses are allocated for private networks:
- 10.0.0.0/8 (10.0.0.0 to 10.255.255.255)
- 172.16.0.0/12 (172.16.0.0 to 172.31.255.255)
- 192.168.0.0/16 (192.168.0.0 to 192.168.255.255)
- 169.254.0.0/16 (169.254.0.0 to 169.254.255.255)

Note -- 169.254.0.0/16 is a block of private IP addresses used for random self IP assignment where DHCP servers are not available. 10.0.0.0/8 is normally used for larger networks, since there are approximately 16.8 million IP addresses available within that block.

Furthermore, an emergency request was sent to Communications WIPT members requesting feedback on the IP assignment, routing and dynamic host configuration protocol (DHCP) support by each of the radio system representatives. It was stated that with minimal effort, each radio system could serve as the DHCP server and router for the OCU and UGVs. The setup of the radio system will be in more detail within the Data Packet Handling Standards.

9.5.3 Network Topologies:

This section depicts examples of different network topologies that could exist in an unmanned system. Communication IOP V0 will focus on Flat Networking (fig. 9-2 and 9-3) topology and Routed Networking (fig. 9-4) topology. In the first example, fig. 9-2, the OCU and Platform are connected to each other in a network that does not contain any subnets. 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.

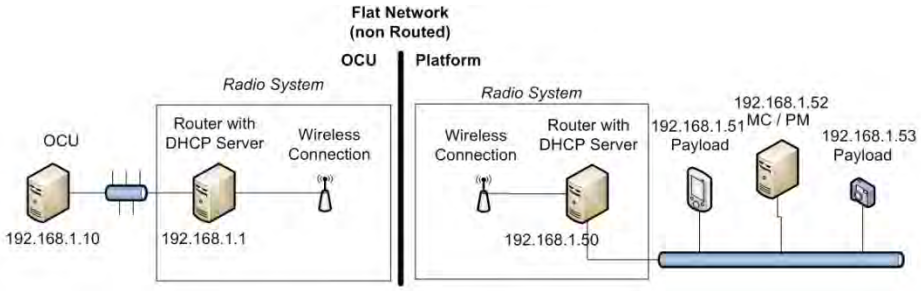

Figure 9-2: Flat Network

Fig. 9-3 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.

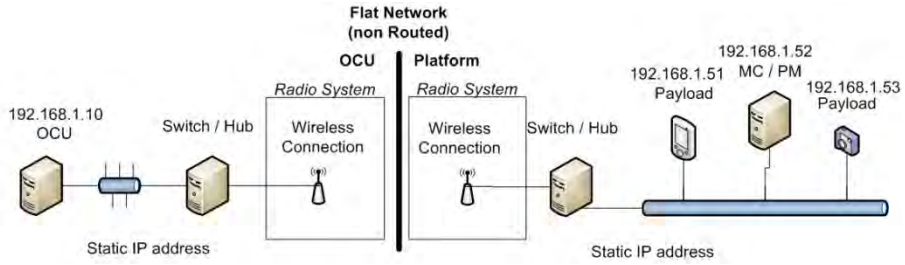

Figure 9-3: Flat Network (Static IP)

Fig. 9-4 represents a routed network. In this topology, the network is split up into subnets and there are no firewalls or NAT. That is not to say that a firewall cannot exist in a routed network, but a firewall unnecessarily complicates the communications. Accordingly, V0 will not address networks that contain firewalls or NATs. 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.

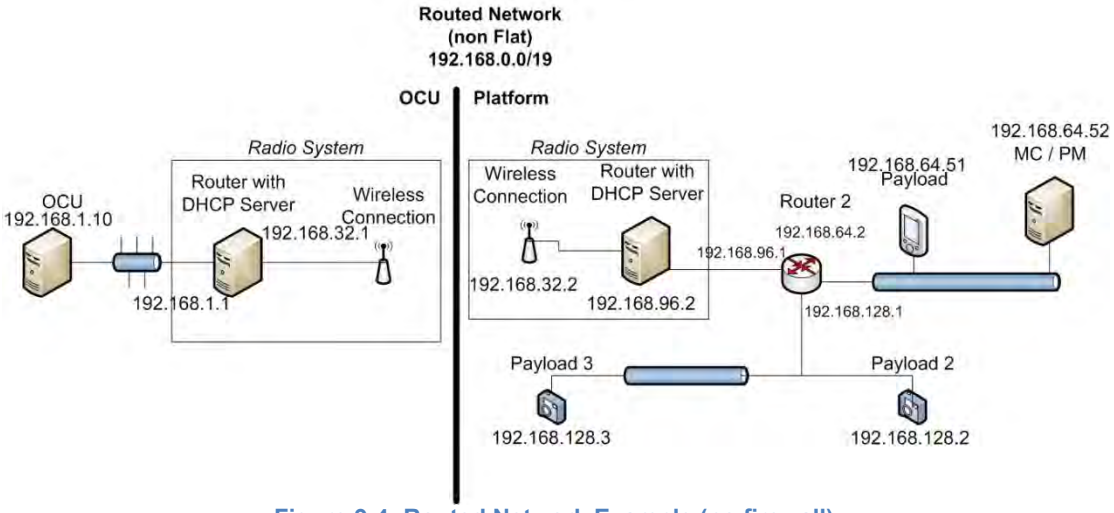

Figure 9-4: Routed Network Example (no firewall)

The next two types of network topologies below are here for reference only. V0 will not address the how to implement them. Figure 9-5, represents 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.

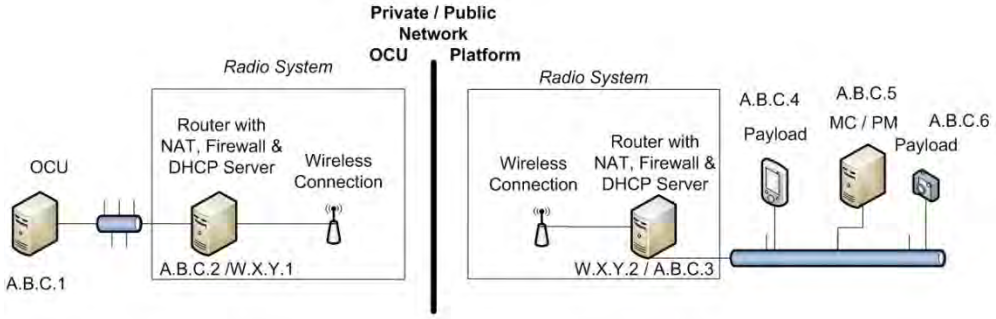

Figure 9-5: Public / Private, Firewalled Network Topology

The final network topology, shown in fig. 9-6, is a subset of the previous topology. Here the communication between the OCU and platform pass through several public networks. This architecture may contain an unknown number of firewalls. We may have the ability to communicate with the firewall that immediately separates our system to the first public network, but we do not have the ability to directly communicate to the other firewalls to obtain networking information. In this topology, traditional means of communications may not be applicable. Communication may have to be sent over popular supported ports of the public networks. The alternative to this is to create a virtual private network (VPN). Both cases are outside of the scope of V0. These examples are mainly here to provide visualization to the vernacular of this document.

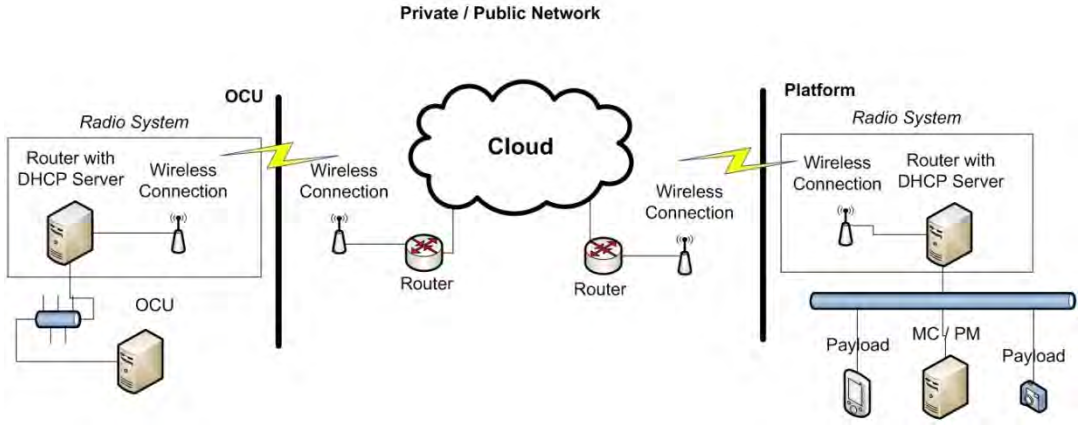

Figure 9-6: Cloud Networking Topology

9.5.4 Data Packet Handling Standards:

9.5.4.1 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. Unless explicitly stated as referring to IPv6, this refers to IPv4. 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.

9.5.4.2 **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.

9.5.4.2.1 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.

9.5.4.2.2 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.

9.5.4.2.3 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.

9.5.4.2.4 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.

9.5.4.2.5 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 is easier to implement, but harder to maintain. May have limited future transition into V1, V2, etc…

- 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 the future V1, V2, etc. with multiple OCU/OCU, OCU/UGV, and UGV/UGV interactions.