Development of an advanced cybersecure radio for small unmanned ground vehicles

Hoa G. Nguyen,* Narek Pezeshkian, John Yen, Abraham Hart
Space and Naval Warfare Systems Center Pacific
San Diego, CA 92152

ABSTRACT

The Space and Naval Warfare (SPAWAR) Systems Center (SSC) Pacific is developing a prototype cybersecure network radio for the Man-Transportable Robotic System (MTRS) MK2 Mod 0 explosive-ordnance-disposal (EOD) robot that will also be compatible with the Advanced EOD Robotic System (AEODRS) Increment-2 robot. Both programs of record are managed by the Naval Surface Warfare Center (NSWC) Indian Head EOD Technology Division (IHEODTD).

This paper describes SSC Pacific's solution, the MTRS/AEODRS Radio for Cybersecure Operation with Network Integration (MARCONI) system. MARCONI is a modular networking radio developed based on the Joint Communication Architecture for Unmanned Systems (JCAUS), which is being defined by the Joint Ground Robotics Enterprise (JGRE). The system architecture includes a Payload Host Module, which provides translations and interfaces to the other modules, a Communication Module based on frequency-shifted and amplified 802.11n wireless technology with ad hoc networking, and a Cybersecurity Module, which uses the latest technologies—including Tactical Key Management—to meet the unique requirements for unmanned systems.

Keywords: radio, robot, MTRS, AEODRS, cybersecure, communication, unmanned system, UGV

1. INTRODUCTION

Until recently, cybersecurity has not been an emphasis in the development and fielding of unmanned vehicles, specifically the class of small, portable or two-man-transportable ground robots. Challenges contributing to this neglect include: (1) the size, weight, and power (SWaP) of encryption devices and cross-domain solutions that cannot meet the small size and power-carrying capacity of the robots, (2) the need to keep Controlled Cryptographic Items (CCIs) under physical control at all times, which runs counter to the concept of operation of unmanned systems, and (3) the lengthy approval processes, which have often been overridden by urgent Warfighter needs.

SSC Pacific has been tasked by IHEODTD with the development of a cybersecure radio to replace the legacy communication system aboard the MTRS MK2 Mod0 (*Talon*) EOD robots, whose radio has been made obsolete by the recent sale of the 1.7-1.85 GHz frequency band by the US government. The radio being developed is based on the proven technologies of our previous series of communication systems for unmanned ground vehicles, which started with technology development under the Defense Advanced Research Projects Agency (DARPA) sponsorship in 2001 and eventually led to the fielding of radio-relay kits in Afghanistan in 2012.[1]

To ease the incorporation of cybersecurity into our communication system, we adopted JCAUS,[2] an architecture being defined by the JGRE's System Design and Integration Team (SDIT), of which SSC Pacific is a member. This architecture is being developed to provide the unmanned systems community with a standard framework to improve their communication systems' interoperability, information assurance capability, cost of ownership, ease of technology insertion, and operational and maintenance flexibility, through the use of open systems and modularity.

A high-level depiction of the JCAUS radio architecture is shown in Figure 1. A JCAUS radio contains three modules: the Payload Host Module (PHM), the Security/Cyber Module (SCM), and the Communications Module (COM). The role of the PHM is to interface with, format, and pass data to and from the other modules as well as its associated

* hoa.nguyen@navy.mil

Unmanned Systems Technology XIX, edited by Robert E. Karlsen, Douglas W. Gage, Charles M. Shoemaker, Hoa G. Nguyen, Proceedings of SPIE Vol. 10195, 101950Q · © 2017 SPIE
CCC code: 0277-786X/17/$18 · doi: 10.1117/12.2264620

endpoint, which is either the unmanned system (UxS) platform or Operator Control Unit (OCU). The SCM module is in charge of encrypting (converting plain text (PT) to ciphertext (CT)), decrypting, or routing traffic bi-directionally between its endpoint and the COM. Data and command-and-control (C2) messages meant for the platform or OCU are encrypted/decrypted by the SCM, whereas radio-control messages between an endpoint and its COM are exchanged unencrypted through the controlled bypass of the SCM. The function of the COM is to wirelessly transmit and receive encrypted messages to/from the PHM. The Certification/Key Loading interface described by JCAUS is made available to any SCM module that requires it. Under the MARCONI architecture this will be a DS-101 compliant interface, a standard currently used by the National Security Agency (NSA).

The remainder of this paper will describe the MARCONI system in detail, starting with objectives and constraints followed by system architecture and design, and it will conclude with the status of the project.

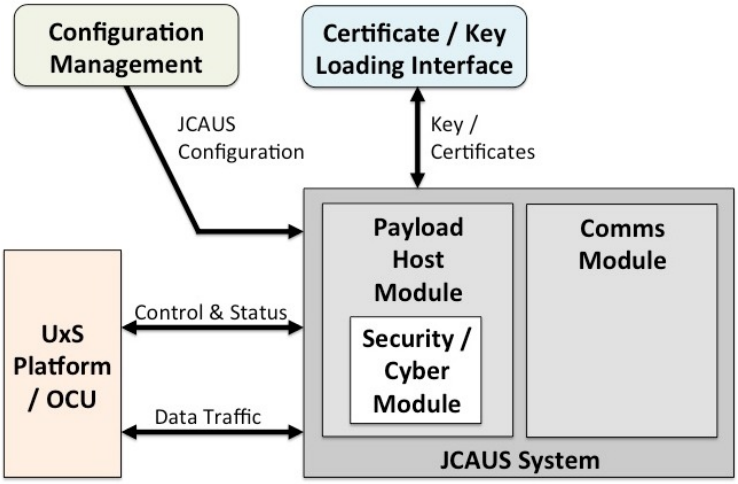

Figure 1. High-level JCAUS system view.[3]

2. OBJECTIVES AND CONSTRAINTS

Objectives for MARCONI, as outlined in the original request for proposal and initial meetings with IHEODTD, include the following:

- Easy integration into current MTRS MK 2 Mod 0 robot (or unmanned ground vehicle—UGV) and associated OCU. (The MTRS MK 2 Mod 0 is a version of the QinetiQ North America *Talon* 4, configured for EOD use.)
- Operates in an approved frequency range for continental US (CONUS).
- Compatible with AEODRS Increment 2 systems. (AEODRS Increment 2 is a robotic system being develop as the next generation EOD robot, in the same size/weight class as the MTRS MK 2.)

Most of the remaining design constraints were imposed by AEODRS requirements,[4,5] which are much stricter than those of the MTRS MK 2 Mod 0 system. A few of the high-level requirements are listed below.

Mechanical

- The maximum weight of each radio box, including all connectors, cables, antennas, and electronics, is 3 lb.[4]
- The volumetric constraint of each radio box is as shown in Figure 2.
- The UGV- and OCU-side radio boxes musts adhere to their respective mounting-hole patterns.
- Cryptographic equipment containers must meet tamper-resistance and TEMPEST requirements.

Other mechanical requirements include environmental sealing, humidity, temperature, vibration, and others.

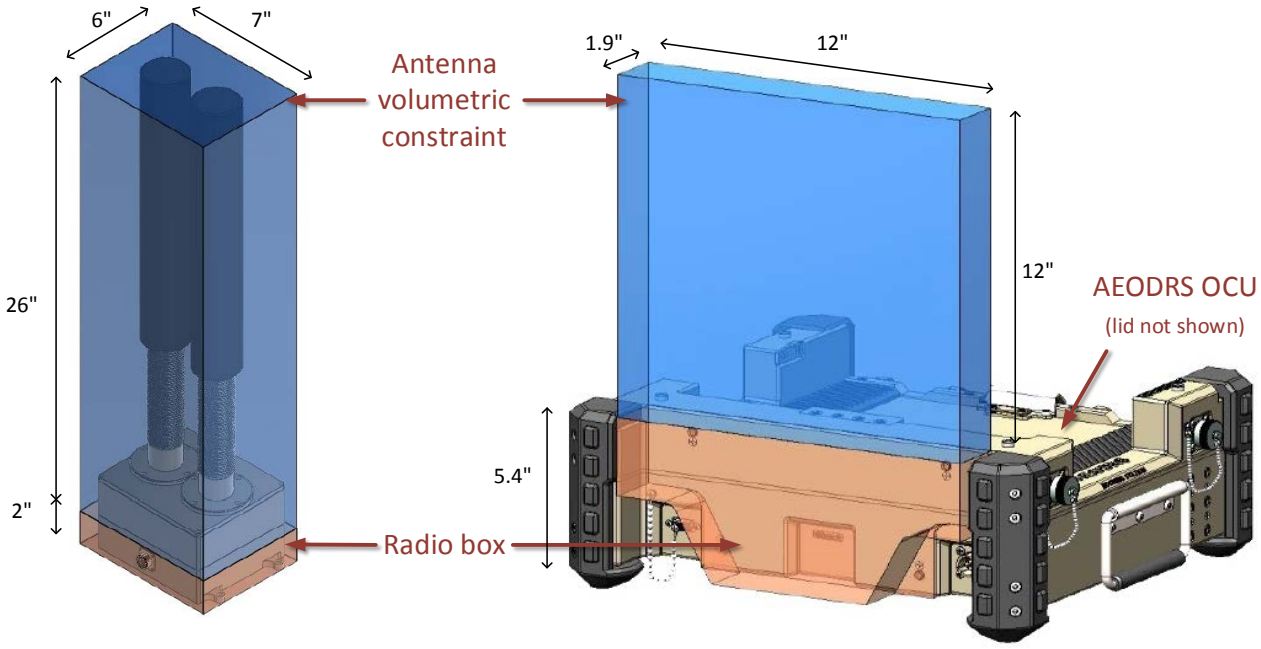

Figure 2. Volumetric constraints on the AEODRS Inc. 2 radios: UGV- (left) and OCU- (right).[5]

Electrical

- Each radio box must consume less than 48 W of power.
- The radio boxes must pass conducted emissions, conducted susceptibility, radiated emissions, and radiated susceptibility tests per the MIL-STD-461F standard.
- End-to-end system latency of the COM must be less than or equal to 5 ms.

Other requirements include meeting expected over-voltage and over-current conditions.

Cybersecurity

- All data transmitted over-the-air (OTA) must be encrypted using NSA approved cryptography at SECRET level.
- All radio-control and status messages that will not be transmitted over the air must be protected from accidental transmission. These messages cannot be encrypted; otherwise, the receiving device would not be able to interpret them. Therefore, a cross-domain solution (CDS) or controlled bypass (guard) must be used to pass them (and only them) through the cryptographic module unencrypted. Table 1 lists some sample messages that fall into this category.

Table 1. Sample control/status messages between an endpoint and its COM. These must not be encrypted.

Messages	From	To
RF received signal strength	OCU COM	OCU
Change radio channel	OCU	OCU COM
Configure SCM	OCU	OCU SCM

There are numerous other system-level requirements such as data rate, range, boot time, and so on that must also be met.

3. SYSTEM ARCHITECTURE

3.1 Architecture Overview

Figure 3 shows the MARCONI system architecture. The system supports both MTRS and AEODRS. The OCU is at the upper left of the diagram, while the UGV is at the bottom right. The Talon Adapter boxes convert signals from the Talon end units to a format compatible with AEODRS, after which the two systems are identical. Each radio box follows the JCAUS architecture that was shown in Figure 1. We will describe each system component in the following sections, and finish with a sample flow of data through the system.

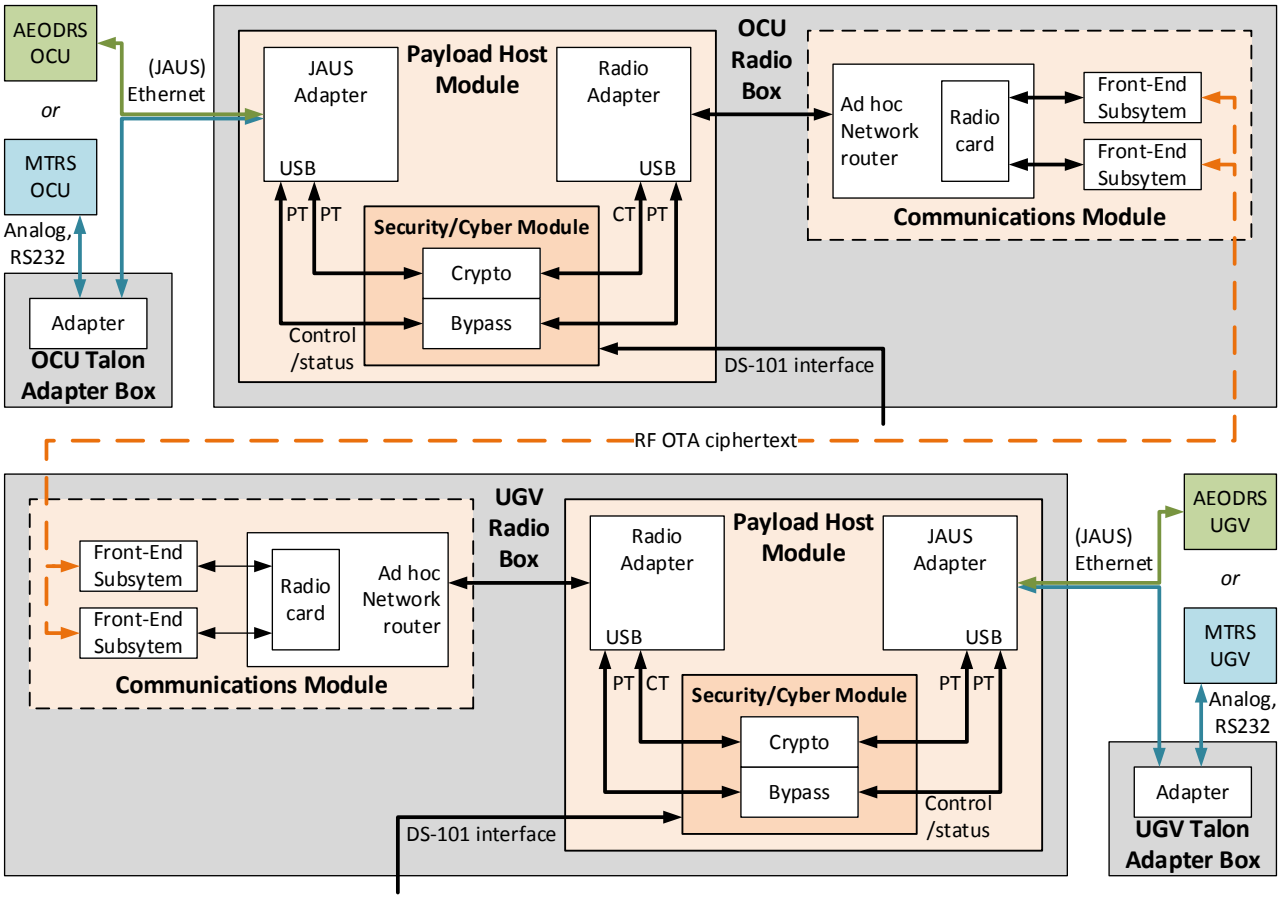

Figure 3. MARCONI system architecture.

3.2 Talon Adapter

The function of the Talon Adapter is to convert between the MTRS MK 2's analog video and RS-232 C2 signals and the Internet Protocol (IP)-based, Joint Architecture for Unmanned Systems (JAUS)[6]-compatible data as used by AEODRS. Figure 4 breaks down the functional components of the Talon Adapter, with processing performed on *Gateworks* single board computers (SBCs). A *Gateworks* GW5400 is used in the OCU Adapter Box and a GW5220 for the UGV Adapter Box. (The GW5220 is physically smaller than the GW5400 but does not support analog video out, which is not needed by the UGV-side adapter. The smaller size is a feature useful in the design of the UGV Talon Adapter Box.) The Protocol Parser converts *Talon* C2 to/from JAUS. The Video Handler converts *Talon* composite video to/from H.264 using the open-source *gstreamer* video converter plugin, and uses the JAUS library to publish the video address to JAUS. On the UGV side, the Adapter Box plugs into the fiber-optic interface port, which is meant to provide the fiber-

optic spooler of the *Talon* robot with power as well as composite video, line-level audio, and RS232-level C2 data. On the OCU side, the Adapter Box plugs into the general-purpose "Tether" port, which provides the same signals (but does not include power).

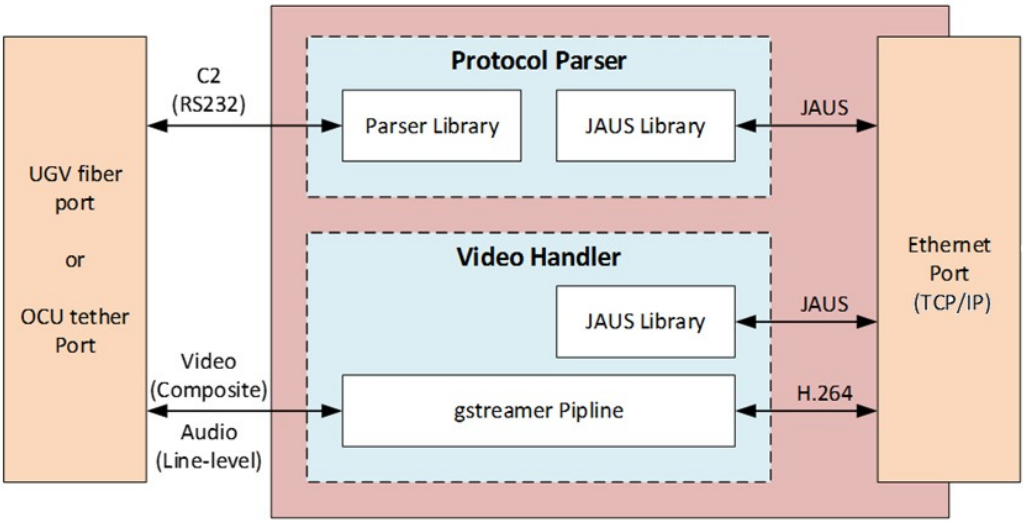

Figure 4. The Talon Adapter functional diagram.

3.3 Payload Host Module

The PHM is the "glue" module of the system. It interfaces to the endpoint (through the Talon Adapter if needed), the SCM, and the COM. It contains two main processors: a JAUS Adapter and a Radio Adapter (*Gumstix Overo IceSTORM* computer-on-modules). The JAUS Adapter serves three functions: (1) enabling the MARCONI radio system to act as a JAUS node, (2) separating incoming data from the local endpoint into data to be encrypted or bypassed and use appropriate SCM application program interface (API) calls to pass them to the SCM, and (3) recombining incoming decrypted and bypassed data from the SCM onto a single stream to forward to the endpoint through an Ethernet interface. The Radio Adapter also serves three functions: (1) translating data and radio-control/status messages that pass through the SCM between the format defined by the SCM API and the format required by the particular radio currently in use, (2) combining the radio-control/status messages and the encrypted data onto a single stream and forwarding them to the COM over an Ethernet interface, and (3) separating incoming data from the COM for either decryption or bypass and forwarding them to the SCM.

The PHM is also designed to provide regulated power to the SCM and COM. In addition, since some of the ports of the PHM are exposed to the outside world, it supports protection against electrostatic discharge (ESD) hazards.

3.4 Security/Cyber Module

The SCM provides a boundary between red (classified) data and black (unclassified) data. It serves two functions: (1) hosting an embeddable cryptographic (EC) device, which is typically a very small circuit board containing cryptographic-related hardware and software, and (2) acting as a translator between the USB interface of the PHM and the native interface of the EC device. The EC device in turn has two functional components: (1) a cryptographic module (referred to as Crypto in Figure 3), and (2) a controlled-bypass module (called Bypass in Figure 3).

The Crypto is bi-directional. It encrypts data flowing from the endpoint to the COM and decrypts data flowing in the opposite direction. For example, video in the form of classified plaintext data originating from the UGV-side JAUS Adapter is encrypted and provided as ciphertext data to the Radio Adapter.

The Bypass is similarly bi-directional. Messages that are to be bypassed are not encrypted or decrypted, and have their origin or destination at either the COM or the SCM. Such messages are used to query the health of the system or set

configuration parameters. For example, an endpoint query of the signal strength of its local COM will pass through the Bypass as plaintext to the COM via the Radio Adapter. The response from the COM to this query will pass through the same Bypass as plaintext to the endpoint via the JAUS Adapter. Table 1 lists a sample of these messages.

The Bypass incorporates a filter policy that only allows specific pre-programmed messages to pass through from the classified side to the unclassified side. Any unknown messages will be rejected. This prevents any classified data from passing through the SCM unencrypted.

3.5 Communications Module

The COM is an updated design based on our past successful unmanned-vehicle radio projects.[1] It uses a *Gateworks* GW5100 SBC that controls a radio card and executes our ad hoc networking software. The radio card being used is a *Doodle Labs* NM4965-2F 2x2 MIMO mini-PCIe form-factor 802.11n radio. This radio is accompanied by two *Prism* Front-End-Subsystem (FES) modules that provide frequency-shifting (out of the ISM band) and amplification. Currently, the range of frequencies that an FES module can be tuned to at the factory is approximately from 200 MHz to 6000 MHz.

4. SYSTEM DESIGN

4.1 Mechanical

The volumetric constraint and 3 lb. weight limit present significant design challenges to the MARCONI system, considering that the containers will have to be manufactured out of metal to provide heat dissipation and shielding against electromagnetic interference. Tamper proofing and meeting TEMPEST requirements will further impose additional burdens on these tight constraints. The volume allocated for the UGV- and OCU-side antennas and Radio Boxes were shown earlier in Figure 2. In addition, each Radio Box must conform to a specific bolt pattern in order to be compatible with an AEODRS endpoint.

Figure 5 shows the OCU-side Radio Box and Adapter Box that is required for use with the MTRS system. The Adapter Box provides the same mechanical and electrical interface to the Radio Box as the AEODRS OCU. Since the MTRS OCU cannot provide power to any external payloads, the OCU Adapter Box is designed to support a BB2557 military-style battery. It in turn provides power to the OCU Radio Box. The Adapter Box physically mounts to the fiber-spooler bracket on the side of the MTRS OCU, and interfaces to the "tether" port of the MTRS OCU via a cabled connection.

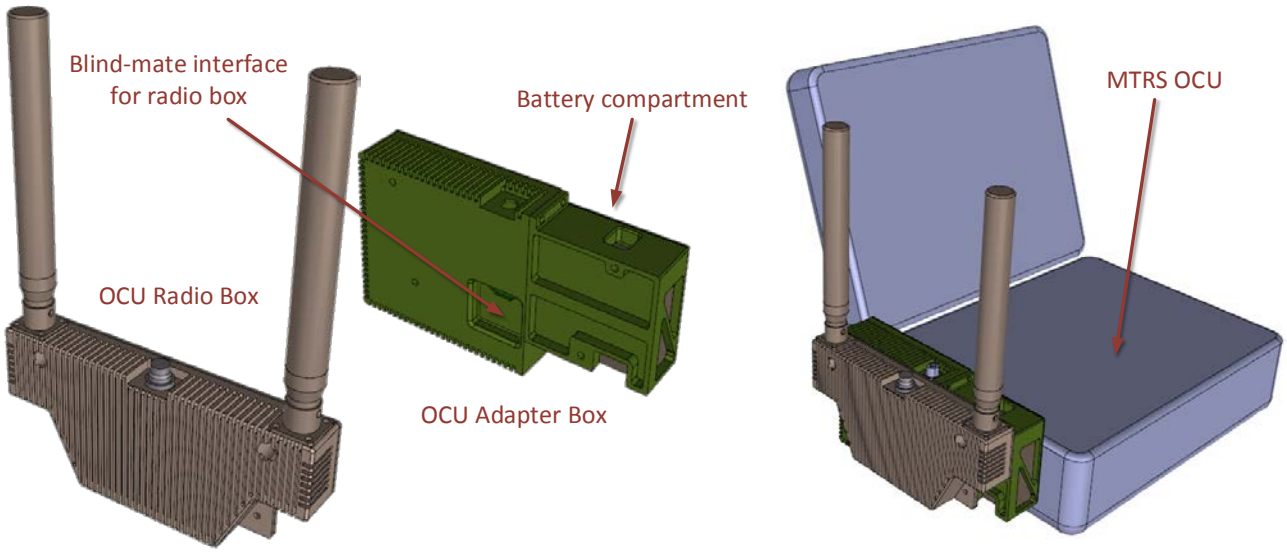

Figure 5. OCU Radio Box and Adapter Box (left) mounted on an MTRS OCU (right)

Figure 6 shows the UGV-side Radio Box and Adapter Box for use with the MTRS system. The UGV Adapter Box presents the same mechanical and electrical interface as the AEODRS UGV to the UGV Radio Box. The Adapter Box receives power from the *Talon* robot batteries and in turn provides power to the Radio Box. The UGV Adapter Box physically mounts to the "C-Box" of the *Talon* robot via two large mounting holes at its base.

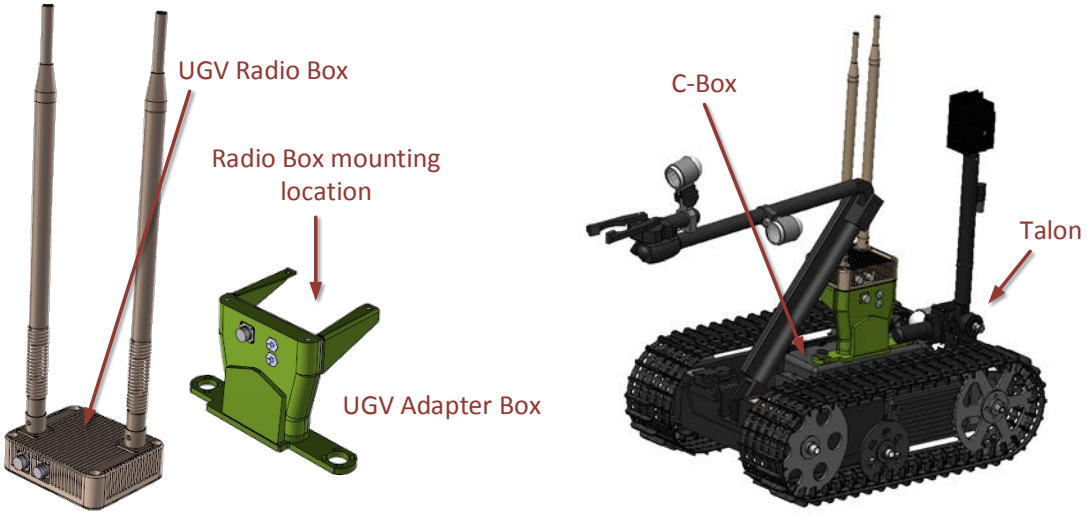

Figure 6. UGV Radio Box and Adapter Box (left) mounted on a *Talon* robot (right)

4.2 Electrical

The maximum sustained rate of the 48W power-consumption limit for each Radio Box is more than sufficient for our electronics design. The primary challenge, however, is to ensure it will pass various emissions, ESD, and TEMPEST-related testing. Proper steps are being taken to ensure that there is sufficient shielding, proper grounding, and necessary protection features designed into the electronics.

A secondary function of the Adapter Box is to provide switched power to itself and its associated Radio Box. This power-switching is necessary since both Adapter Boxes are fed with live power at all times (directly from batteries). In order to eliminate the need for the user to manually activate/deactivate the Adapter and Radio Boxes, the power-switching step is done automatically. Each Adapter Box contains a Power Board that makes use of an ultra-low-power always-on circuit that looks for a specific signal that is asserted when its associated endpoint (OCU or UGV) is turned on. The UGV-side Adapter Box looks for a 12V DC signal when the robot is activated. When detected, it switches power on to the rest of the Adapter Box and the Radio Box. The OCU-side Adapter Box looks for a bipolar ±5V signal, specifically, the RS232-level transmit signal from the tether port, and when detected, it turns power on to the rest of the Adapter Box and Radio Box. When the robot and OCU are turned off, the signals return to zero, at which point the Power Boards turn off power to the rest of the system.

In the Radio Box, most of the power is consumed by the COM module, specifically the FES modules, which are relatively high-power RF amplifiers. This is also where most of the power is dissipated as heat and must be extracted from the box. Since the boxes must be sealed in order to provide complete shielding coverage, the heat must be dissipated via passive means, for example, via heat fins on the outside. This in turn adds weight to the box. The heat dissipation, however, is highly correlated with the transmit duty cycle (data rate) of the Radio Box. With the data rate requirements of AEODRS, we expect the FES modules to generate far less heat than they would at the maximum data rate, easing the mechanical design constraints.

A more stringent AEODRS requirement is to meet the end-to-end latency of 5 ms.[4] This includes latencies caused by the PHM, SCM, and the COM.

Another design consideration of the PHM is taking into account the separation of red and black data. In general, the JAUS Adapter deals with classified data from the UGV or OCU, while the Radio Adapter only has contact with

encrypted ciphertext or unclassified radio-control commands that have been filtered by the controlled bypass. We are designing the PHM under the guidance of the NSA, to ensure ease of system approval at a later date.

4.3 Cybersecurity

We performed a cryptographic analysis-of-alternatives,[7] and determined that only two EC devices meet our SWaP and throughput requirements. One is the *Mini Crypto (MC)*, being fielded by a program-of-record under the Air Force Materiel Command (AFMC). The other is the *Nano CCM*, developed by the NSA. Currently, the SCM is being developed to host the *Mini Crypto* because it uses the new (and preferred) Tactical Key Management (TKM) technique developed by the Massachusetts Institute of Technology (MIT) Lincoln Laboratory.[8] Under TKM, classified cryptographic keys are generated for use only during an active session, and disappear when the system is powered down. This makes the system a non-cryptographic-controlled-item (non-CCI), greatly simplifying the concept-of-operation (CONOP) and logistics involved in its use on unmanned vehicles. The unmanned vehicle can operate out-of-sight without concern, and loss of an asset can be addressed simply by putting its public-key-infrastructure (PKI) certificate into a certificate revocation list. We are working with MIT Lincoln Lab in developing an SCM that hosts the *MC*. However, the MARCONI hardware enclosures are also being developed with the *Nano CCM* in mind, as a risk-reduction backup solution while we track the development of the MC.

We also found no currently available CDS or Bypass solution that meet our requirements. We are working with the MIT Lincoln Laboratory, JGRE, and AFMC to produce a certifiable MC controlled bypass. Miniature CDS solutions under development, such as the Rockwell Collins *Micro-Turnstile*, are also being tracked.

4.4 Sample data flow

In this section we will provide several data-flow examples to help solidify how the various modules of the JCAUS architecture function (see Figure 7). In Figure 7, the domain boundary indicates the separation between classified plaintext data (e.g., video and C2) and unclassified data. The unclassified data may contain encrypted ciphertext data, such as video and C2, or unencrypted plaintext data, such as radio control/status messages.

Example 1: Encrypted message over the air

This example outlines the steps taken to transmit an encrypted message over the air between the two endpoints. Assume the message here is a C2 command that is sent from the OCU to the UGV. (1) The message is generated on the OCU and forwarded to its associated PHM. (2) On the PHM, the JAUS Adapter flags the message as data to be encrypted (since it must be transmitted over the air) and forwards it to the SCM. (3) The SCM encrypts the message via the Crypto then forwards it to the Radio Adapter. (4) The Radio Adapter translates the message into a format that the COM can understand. (5) The COM then transmits the message over the air where it is received by the UGV COM. (6) The UGV COM forwards the message to the Radio Adapter of its associated PHM, where it is flagged as a message to be decrypted. (7) The SCM decrypts this message via the Crypto, and then forwards it to the JAUS Adapter. (8) The JAUS Adapter sends the message to the UGV in JAUS format.

As another example, the video data from the UGV takes the same path as above, except in reverse order. The vast majority of the messages are passed between the OCU and the UGV as outlined above. However, there are messages that circulate only between an endpoint and its associated COM or SCM. This is considered next.

Example 2: Bypassed message

This example outlines the steps taken to communicate messages between an endpoint and its associated COM. Assume the OCU requires the RF signal strength as seen by its COM. (1) A query message is generated on the OCU and forwarded to its associated PHM. (2) On the PHM, the JAUS Adapter flags the message as data to be bypassed, since the COM cannot understand encrypted messages. The message is then forwarded to the SCM in the format defined by the SCM API. (3) The SCM checks its filter policy and deems the data valid, then bypasses it without encryption and forwards it to the Radio Adapter. (4) The Radio Adapter translates the message into a format that the specific COM can understand. (5) The COM accepts the message and responds accordingly. The response is sent back to the Radio Adapter. (6) The Radio Adapter flags the response message, indicating it is to be bypassed, then forwards it to the SCM in the format defined by the SCM API. (7) The SCM checks its filter policy, deems it as valid, and then forwards it to the JAUS Adapter via the Bypass. (8) The JAUS Adapter forwards it to the OCU (or Talon Adapter) in the JAUS format.

Next, we consider the case where the OCU requires signal strength information from the UGV COM.

Example 3: Combination

This example outlines the steps taken for the OCU to obtain the RF signal strength data from the UGV-end COM. Instead of outlining all the necessary steps, here we will refer to the first two examples since this is really a combination of the two. (1) Since a status query message must be transmitted over the air, it is encrypted and transmitted from the OCU to the UGV in the same manner as in Example 1, except this message is stopped at the JAUS Adapter on the UGV-side PHM. (2) When the JAUS Adapter receives this message, it knows the destination is the UGV COM, and thus sends a request for signal strength to the COM using the SCM bypass in the same manner as in Example 2. (3) The associated response is returned from the COM to the JAUS Adapter using the same SCM bypass. (4) Finally, the UGV JAUS Adapter will transmit it to the OCU over the air encrypted, in the same manner as in Example 1.

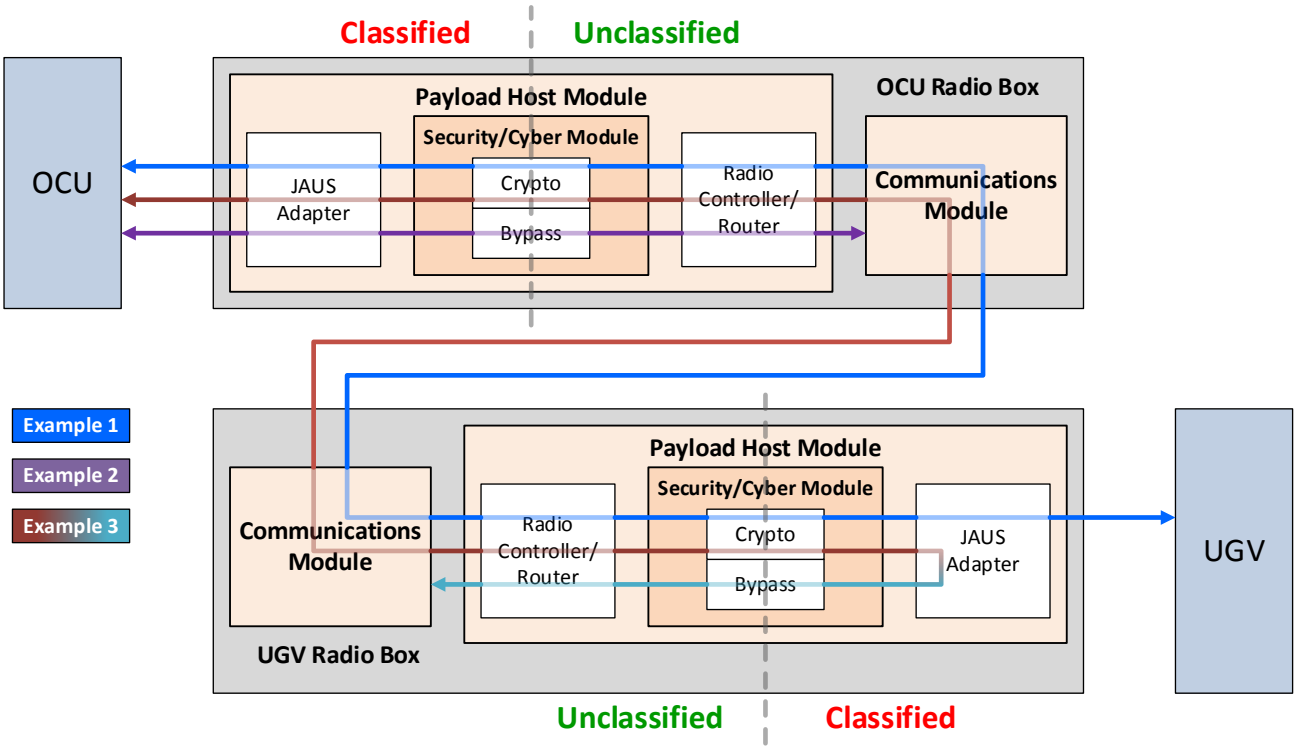

Figure 7. Sample data-flow paths between endpoints

5. CURRENT STATUS

MARCONI is currently nearing the completion of its phase 1, during which a Technology Readiness Level (TRL)-4 system is developed with preparations for integration with a cybersecurity solution. SSC Pacific is working closely with IHEODTD, JGRE, AFMC, MIT Lincoln Laboratory, and Pennsylvania State University Applied Research Laboratory in the development of the system. We are also working with the NSA to ensure timely certification upon completion. A TRL-6 system with cybersecurity is anticipated in 2018. The cybersecurity solution may or may not be certified at system completion. If it is not, a clear path must already be laid for certification and approval.

REFERENCES

[1] Nguyen, H.G., Pezeshkian, N., Hart, A., Neff, J., and Roth, L., "Evolution of a radio communication relay system", Proc. SPIE 8741: Unmanned Systems Technology XV, Baltimore, MD (2013).

[2] Reese, S., and Chang, W., "Joint communications architecture for unmanned systems (JCAUS)," Proc. SPIE 10195: Unmanned Systems Technology XIX, Anaheim, CA (2017).

[3] OUSD AT&L Joint Ground Robotics Enterprise (JGRE), "Joint Communications Architecture for Unmanned Systems (JCAUS) Interface Control Document," draft (2016).

[4] NSWC IHEODTD, "Advanced Explosive Ordnance Disposal Robotic System (AEODRS) Performance Specification for the Communications Link Suite, Tactical Operations and Base Infrastructure Operations Systems," MPS-AEODRS-INC23-COM (2016).

[5] NSWC IHEODTD, "Advanced Explosive Ordnance Disposal Robotic System (AEODRS) Interface Control Document for the Communications Link Suite, Tactical Operations and Base Infrastructure Operations Systems," ICD-AEODRS-INC23-COM (2016).

[6] Rowe, S., and Wagner, C., "An Introduction to the Joint Architecture for Unmanned Systems (JAUS)", Technical Report from Cybernet Systems Corporation (2008), available online at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.472.489&rep=rep1&type=pdf

[7] Yen, J., Smigal, J., Singh, D., Ricks, J., Brower, D., and Barlow, P., "Cybersecurity for unmanned systems," Proc. SPIE 10195: Unmanned Systems Technology XIX, Anaheim, CA (2017).

[8] Khazan, R., Nahill, B., Utin, D., Vai, M., Whelihan, D., and Wilson, D., "Seamless cryptography and key management for secure and agile UxS communication," Proc. SPIE 10195: Unmanned Systems Technology XIX, Anaheim, CA (2017).