Cybersecurity for Unmanned Systems

John Yen, John Smigal, Daljit Singh, Jason Ricks, Don Brower, Phil Barlow
Space and Naval Warfare Systems Center Pacific
53560 Hull Street, San Diego, CA,USA 92152-5001

ABSTRACT

Unmanned Systems (UxS) present unique challenges to Cybersecurity developers due to: (1) The need to secure these systems and protect classified information in the unmanned operational environment, where the UxS are often outside the visual range and physical control of the operator. (2) They require very low Size, Weight, and Power (SWaP) consumption constraints imposed by the smaller UxS. (3) They also impose long and costly approval processes for employing Cryptographic Products, Key Management Architectures, and other High Assurance security solutions in the military operational environment. Additionally, modularizing communications architectures to take advantage of rapid technological and SWaP advancements often results in multiple classification domains, and the need to move plaintext control information between these domains, which results in a Cross Domain Solutions (CDS), requirement.

This paper details work supporting High Assurance Cybersecurity engineering for UxS that includes: (1) Investigating current approved cryptographic and CDS tactical products to assess their suitability for UxS operations. Although some current products can meet the larger UxS SWaP requirements, most approved products do not meet SWaP requirements for the smaller UxS. (2) Exploring potential new technologies that have not yet reached the operational stage but show promise for meeting the smaller UxS SWaP requirements. (3) Evaluating potential solutions that will meet the three challenges of deploying High Assurance Cybersecurity solutions onboard UxS in military operations.

Keywords: Cybersecurity, Unmanned, UxS, Cryptography, High Assurance, Cross Domain, CDS, SWaP.

1. INTRODUCTION

UxS such as Unmanned Airborne Systems (UAS), Unmanned Ground Systems (UGS), and Unmanned Undersea Systems (UUS) have the potential to reduce risks to manned forces by performing the tasks which manned systems cannot do or would put warfighters at an unnecessary risk. UxS can be the force multiplier that mitigate those human exposure risks and accomplish missions in a cost-effective way. Small UxS have been designed for Tactical Intelligence, Surveillance, and Reconnaissance applications, allowing operators to track and capture targets in great detail while remaining safe, secure and covert. A specific mission of interest is to work as explosive-ordnance-disposal (EOD) tools, keeping the EOD operators at a safe distance from the dangerous explosives that they are trying to defeat.

As UxS operations are becoming more network-centric, they become vulnerable to Cyber-attacks, such as Global Position System (GPS) spoofing/jamming, communications signal jamming, and wireless attacks on the communication links. Failure to address these threats will result in an unsecure architecture, where attacks on one component can propagate throughout the whole system and compromise the mission. Loss of the UxS and/or its information is a threat to national security.

1.1 Background

High Assurance protection of UxS can start by examining the latest threats and vulnerabilities and available countermeasures, by identifying new security policies and procedures, and also examining the currently available High Assurance security products and proposed technologies. This paper provides an overview of High Assurance protections necessary to protect UxS operations, and the information contained herein is condensed from Space and Naval Warfare Systems Center (SSC) Pacific Technical Document 3317 (TD-3317) [1].

In developing small UxS, designers must operate within tight size, weight, and power (SWaP) constraints. Adding weight to improve any given feature can reduce the operational function or equipment lifetime, so that tradeoffs must be evaluated with respect to the mission requirements.

Unmanned Systems Technology XIX, edited by Robert E. Karlsen, Douglas W. Gage, Charles M. Shoemaker, Hoa G. Nguyen, Proceedings of SPIE Vol. 10195, 101950R · © 2017 SPIE
CCC code: 0277-786X/17/$18 · doi: 10.1117/12.2265912

This paper describes an investigation based on the constraints found in the Advanced Explosive Ordnance Disposal Robotic System (AEODRS) architecture [2], which is supporting the Flexible Cyber-Secure Radio (FlexCSR) [3] and the Joint Communication Architecture for Unmanned Systems (JCAUS) [4] robotic programs. Unmanned robots are needed operationally to reduce impact of unexploded explosives to personnel safety. Figure 1 is an example of an EOD robot, Man-Transportable Robotic System (MTRS) MK2 Mod0, and its Operator Control Unit (OCU).

Figure 1. Man-Transportable Robotic System MK2 Mod0

Table 1 shows an example set of communications subsystem SWaP constraints for small platforms such as EOD robots based on the AEODRS architecture requirements [2]. In addition to the security subsystem, the communications subsystem include the radio (transceiver and antenna), microprocessors, routers, and other components, so the security subsystem SWaP allocation is only a small part of the communications subsystem SWaP allocation.

Table 1. Robot Communications Support Constraints

	Communications Subsystem Constraints	Security Subsystem Constraints
Maximum Dimensions	5” x 8” x 1.9” 76 cubic inches	2” x 5” x 1” 10 cubic inches
Maximum Weight	3 lb	1 lb
Maximum Power Consumption	48 W	5 W
Minimum Data Throughput	10 Mbps	10 Mbps
Maximum End-to-End Latency	5 ms	2 ms

1.2 Information Classification

An underlying assumption for this paper is that the UxS will process classified information that requires High Assurance protection at an identified classification level, but some of the components of the UxS will remain unclassified. For example, antennas and connected radios are typically considered unclassified.

The UxS controls and analysis functions are usually at a classified level, meaning there will be a classified enclave onboard the UxS to support those functions. Raw sensor data is usually unclassified, but processing the data generally

requires classified algorithms which can be associated with intelligence information. The UxS controller component must have connectivity with its control system, usually located at military platforms/sites and connected to other systems that are classified; therefore the UxS controller enclave will be considered classified.

The information classification determines the level of protection required, as shown in Figure 2. The Type X definitions are based on the Committee on National Security Systems (CNSS) definitions [5], where Type 1 devices are designed and certified by NSA to protect classified National Security Information (NSI). DoD information associated with operations is considered NSI and is a determinant in the decision tree shown in Figure 2.

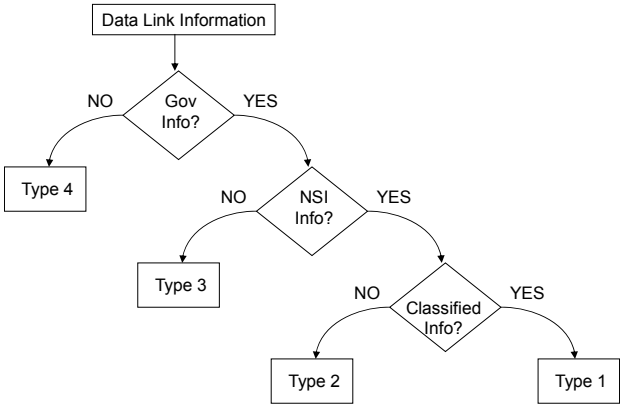

Figure 2. Information Protection Decision Tree

It is necessary for robot controllers to remotely perform EOD tasks at hazardous incident sites with high or unknown risks. The nature and classification of the video feed from the robots requires Type 1 level cryptographic protection of the communications link between controller and robot, so NSA approved cryptographic solutions are required. In addition, all military systems must be approved under the Department of Defense's Cybersecurity approval process described in Appendix C of TD-3317 [1].

2. HIGH ASSURANCE CRYPTOGRAPHY OVERVIEW

2.1 Data in Transit

Data in Transit (DIT) is data that is transported from one platform to another platform and is not stored in nonvolatile memory during or after the transmittal process. DIT cryptographic encryption protects the information that is being transported to assure the confidentiality and integrity of the information.

Examples of High Assurance DIT cryptographic devices are modern In-line Network Encryptors (INE) for network-based traffic protection and legacy radio cryptographic devices such as the KG-84C for data and the KY-57 for voice. Note that an INE is a High Assurance Internet Protocol Encryptor Interoperability Specification (HAIPE IS) compliant cryptographic product.

2.2 Data at Rest

Data at Rest (DAR) is data that is stored in nonvolatile memory anywhere within the platform. Wiping large amounts of data from storage devices in a secure manner within a very short time (capacitors last a few seconds in the case of power loss) is not practical, so effective protection of DAR must depend on another mechanism. DAR cryptographic encryption makes it easier to render DAR useless by zeroizing the cryptographic keys, which involves a very small amount of volatile memory to eliminate in comparison to the total unencrypted DAR. Emergency key zeroization involves situations where stringent time and power constraints apply. Note that wiping the stored (but encrypted) cryptographic algorithm is a secondary priority that will require overwriting non-volatile memory locations and will take more time and power.

Examples of DAR cryptographic devices are In-line Media Encryptors (IME) for use with data storage systems.

2.3 Cryptographic Considerations

High Assurance DIT and DAR cryptographic devices previously certified by the National Security Agency (NSA) were based on implicit expectations that they would be operated in controlled environments such as radio rooms, command posts, and manned aircraft where military personnel will be available to take "last-ditch" actions to eliminate keys in volatile memory.

UxS were not "anticipated" in earlier NSA cryptographic certifications, so they did not evaluate the risks involved with unmanned operations/environments. The NSA position was that unless specifically authorized in their associated operational security doctrines, operation of cryptographic devices for UxS is not permitted. Since there will not be personnel available to eliminate the keys, this issue forces UxS developers to take the necessary measures to zeroize the cryptographic keys as operational conditions require. Such zeroization design may include remote command and autonomous measures such as heartbeat zeroization and zeroization triggered by catastrophic events.

Appendix A of TD-3317 [1] includes the cryptography approval process and NSA guidance for design considerations when implementing cryptographic solutions on UxS. In addition to the typical Type 1 products, NSA has also certified products capable of protecting classified information under the Cryptographic High Value Product (CHVP) process, as described in Appendix E of TD-3317 [1].

In addition to cryptographic key zeroization, the system developer must implement security measures such as TEMPEST and tamper protection to protect the classified information as mandated by NSA and Department of Defense guidance. Such security measures may impact the UxS communications architecture, so it is highly recommended that High Assurance cryptographic solutions be designed and implemented early in the system development process to prevent large scale redesign at a later stage.

3. CLASSIFICATION SEPARATION OVERVIEW

3.1 Modularization

Modularization of various components in an UxS is intended to facilitate the technology refresh processes in the current volatile technology market, where new advances appear often and different products have different refresh timelines. It is difficult to upgrade a complicated system of systems consisting of many technologies being refreshed at different times under the paradigm of upgrading the whole system at one time. Modularization with well-defined interfaces between components should permit technology refresh at the component level without forcing upgrades of other components. A modularized architecture needs "building blocks" that are self-contained, easy-to-integrate, easy-to-operate, and can be secured [6].

3.2 Classification Boundary

One result of modularization is the need to move plaintext (PT, or human readable) information across classification boundaries, which is a CDS requirement. In an integrated communication system that includes both High Assurance cryptography and radios, the system can be designed together to support this requirement completely within the security boundary of the system. However, with the radio and cryptography as separate components, the controls for the radio and other unclassified equipment are required to move as PT messages between the controller (usually on the classified side) and the controlled equipment (on the unclassified side), as shown in Figure 3. A radio control message that is encrypted by the cryptographic device will emerge on the unclassified side as ciphertext (CT) and unreadable to the controlled equipment.

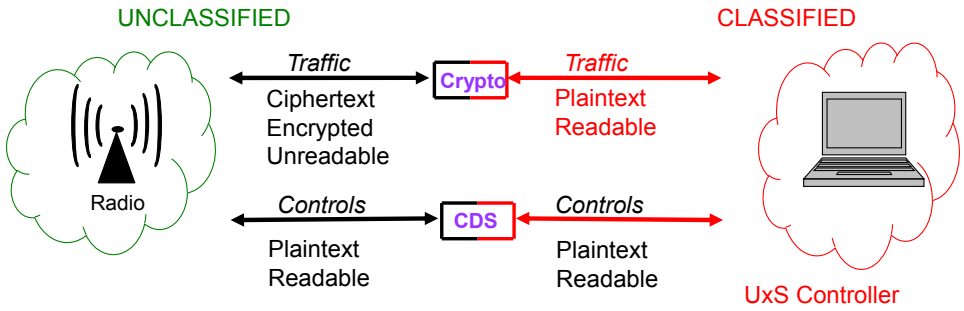

Figure 3. UxS Security Architecture

The classification of the plaintext information being moved between the domains must not exceed the classification of the lower classification domain. No plaintext information classified at the higher classification can be moved to the lower classification domain.

3.3 Cross Domain Considerations

Once a CDS requirement is recognized, the UxS program evaluates the available CDS products for one that matches their needs, or sponsor development of a new CDS. Using or tailoring an existing product will minimize the long CDS approval process and keep it to about 12-24 months. Developing a new CDS and then taking it through the CDS approval process can take 18-42 months. Table 2 summarizes the costs and schedules for taking a CDS through the approval process.

Appendix B of TD-3317 [1] describes the Unified Cross Domain Services Management Office (UCDSMO) approval process and design considerations for UxS CDS implementation.

Table 2. CDS Approval Cost/Schedule

	Contract Award, Development & Integration	Certification Test & Evaluation (CT&E)	Authorization Process	Total Timeline and Cost
Previously approved CDS on UCDSMO Baseline	6-12 Months $300K-$600K	Not needed	6-12 Months $300K	12-24 Months $600K-$900K
New CDS not on UCDSMO Baseline	6-18 Months $500K-$1200K	6-12 Months $500K	6-12 Months $450K	18-42 Months $1450K-$2150K

4. CURRENT PRODUCTS

For larger UxS such as the Littoral Combat Ship Remote Multi-Mission Vehicle, Triton UAS, Unmanned Carrier Aviation UAS, and Anti-Submarine Warfare Continuous Trail Unmanned Vessel (Sea Hunter), the existing High Assurance cryptographic solutions and CDS products can meet their SWaP and performance needs. These existing products can be inserted into the larger UxS with relatively small changes in the overall communication/network architectures, and the approval processes are known. The tradeoffs are mainly of SWaP/performance characteristics versus cost, since the schedule variation should be relatively minor.

For smaller UxS such as the EOD robots and Tactical and Small Tactical UAS [7], it will be challenging for the above High Assurance standalone products to meet their SWaP and performance needs.

4.1 DIT and DAR Encryption Products

The SSC Pacific High Assurance Unmanned Engineering Group surveyed currently available standalone cryptographic devices, including the various INE product families and non-INE DIT and DAR cryptographic devices that have been approved by NSA to protect classified information. In addition to the factors noted in Table 1, the program sponsors indicated a preference for products that are not Controlled Cryptographic Items (CCI). Non-CCI products are preferred due to the unmanned tactical operational environment, where equipment loss is common. For similar reasons, NSA prefers unmanned applications use products that are capable of supporting Suite B operations and heartbeat zeroization.

None of the standalone products can meet the SWaP, CCI, and NSA preferences for small unmanned platforms such as EOD robots, with some examples shown in Table 3 and Table 4.

Table 3. DIT Encryptors Examples [8-14]

Product	Approval	CCI?	Suite B only capable?	Heartbeat capable?	Size (cu in)	Weight (lb)	Power (W)	Throughput (Mbps)
KG-175D	Type 1	CCI	No	No	96	4	<22	200
TACLANE C100	CHVP	Non-CCI	Yes	No	96	4	<22	200
KG-250X	Type 1	CCI	Yes	Yes	54	3	14	200
IPS-250X	CHVP	Non-CCI	Yes	Yes	54	3	14	200
KG-250XS	Type 1	CCI	Yes	Yes	12	<1	<5	20
KG-245X	Type 1	CCI	No	No	248	10	34	2000
Talon 1	Type 1	CCI	No	No	<10	3		5

Table 4. DAR Encryptors Examples [15-17]

Product	Approval	CCI?	Heartbeat capable?	Size (cu in)	Weight (lb)	Power (W)
DAR-400E (ProtecDAR Embedded)	CHVP	Non-CCI	No	24.5	2	<10
KG-200R	Type 1	CCI	No	74	4	9
KG-200M (SEM6)	CHVP	Non-CCI	Yes	49	3.4	9

4.2 CDS Products

The SSC Pacific High Assurance Unmanned Engineering Group surveyed currently available standalone CDS products, including those that have not yet been approved to be on the UCDSMO Baseline to protect the transfer of plaintext information between classification domains. None of the standalone products are both (1) on the UCDSMO Baseline and (2) can meet the SWaP preferences for small unmanned platforms such as EOD robots, with some examples shown in Table 5.

Table 5. CDS Examples [18-23]

Product	UCDSMO Baseline?	Size (cu in)	Weight (lb)	Power (W)
Centurion CDS	No	10	0.5	<2
HAF-100X	No	53	2.8	14
MicroTurnstile	No	2.8	0.2	1.25
Radiant Mercury	Yes	24	1	18
Small Format Guard	No	45	0.44	5.4
Tactical CDS	Yes	48	1.75	9

5. NEW APPROACH

Investigation into the latest encryption technology led to several very small embeddable cryptographic modules that may be within the SWaP constraints after integration into the UxS. Embeddable modules are not standalone devices and will require the hosting system to implement security measures not implemented by the modules. Some of these modules are the Mini Crypto being developed by the Air Force Material Command [24], the NSA's Nano Crypto Core Module (CCM) [25], the Army's RESCUE [26], and the Secure Micro Digital Data Link (SmDDL) module [27]. RESCUE and SmDDL do not meet the throughput requirement stated in Table 1, so the following discussion is based on Mini Crypto and Nano CCM potential capabilities.

5.1 Cryptography

While these cryptographic modules will be certified by NSA, they cannot be deployed as is. Cryptographic module certifications will cover internal cryptographic functions, tamper protection, and TEMPEST protection for these modules themselves. The communications system that embeds one of these cryptographic modules will have the responsibility for the security aspects external to the cryptographic module. Therefore, the communications system will be required to meet the requirements for tamper and TEMPEST protections, zeroization design and implementation, and interfaces from the cryptographic module. Embedment of one of these cryptographic modules will likely require a NSA evaluation and approval for the communications system, which must be factored into the development and acquisition considerations because this process can be expensive and time consuming.

An alternative approach is to make the cryptographic module a standalone cryptographic product which includes requirements for the needed cryptographic protections for UxS that could then be certified by NSA. While there is a one-time cost to implement and certify the resulting product(s), there will be no anticipated recurring cost for each cryptographic module embedment and evaluation. As an example, a one-time cost for development and approval of $1M will be lower than the recurring cost of three embedments and approvals at $500K each.

5.2 Controlled Bypass

Many communication systems require control and response messages to be shared between the radio controller computer and the radio system. These control messages are consumed by the radio itself, and are transmitted over the air only as encrypted data traffic as shown in Figure 4. The data traffic flow between the OCU and the UxS (Path #1 in Figure 4) is encrypted prior to transmission over the air. The control messages are generated in the OCU and sent to the OCU Radio (Path #2) and the UxS Radio (Path #3). The control messages must pass through the cryptographic engine unencrypted in a secure and predefined manner in order for the radio to understand these messages. The control messages are sent through a Controlled Bypass, within or a part of the cryptographic function, which provides checking for messages crossing a classification boundary and verifying that everything that passed through the boundary meets the predefined "ruleset" governing the boundary crossing.

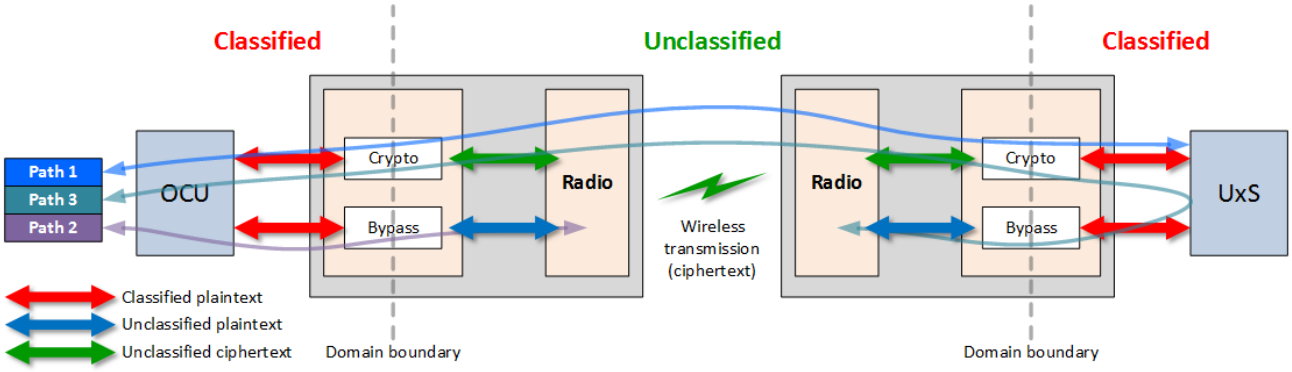

Figure 4. Data and Control Flow Paths

A Controlled Bypass function is similar to CDS, a Guard, and a Trusted Filter, whose descriptions and approval processes are described below:

- A CDS is usually a standalone product that provides checking for messages crossing a classification boundary and approved through the UCDSMO process.
- A Guard is usually a mechanism that provides checking for messages crossing a classification boundary within a cryptographic product to support cryptographic control functions and approved through the NSA cryptographic certification process.
- A Trusted Filter can be a mechanism that provides checking for messages crossing a classification boundary within a product that does not involve cryptography and usually approved under the UCDSMO process.

Each of the aforementioned embeddable cryptographic modules in Section 5 includes a Guard to support cryptographic control functions. Theoretically this Guard function can be upgraded to become a Controlled Bypass function that can

filter radio control messages supporting radio system control and management. These embeddable cryptographic modules have not been designed for this purpose, and will require modifications to achieve this capability. A Controlled Bypass implemented in a cryptographic system under NSA purview will require:

- A set of predefined messages to be bypassed.
- Strict rules for the messages in a filter policy ("ruleset") that checks for permissible values.
- A trusted "parsing engine" that ensures only permitted messages are passed through.
- NSA cryptographic certification.

6. RECOMMENDATIONS

Recommend the development and approval of a small form factor standalone protected device incorporating an embeddable cryptographic module to provide a suitable solution for use with small UxS.

Recommend the development and approval of a small form factor Controlled Bypass capability that provides a suitable radio control and response solution for use with small UxS.

REFERENCES

[1] Yen, J., Smigal, J., Singh, D., Pradhan, A., Brower, D., and Barlow, P., "Cybersecurity for Unmanned Systems," SSC Pacific Technical Document (TD-3317), March 2017.
[2] 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).
[3] Nguyen, H., Pezeshkian, N., Yen, J., and Hart, A. "Development of an Advanced Cybersecure Radio for Small Unmanned Ground Vehicles," Proc. SPIE 10195: Unmanned Systems Technology XIX, Anaheim, CA (2017).
[4] Reese, S., and Chang, W., "Joint Communications Architecture for Unmanned Systems (JCAUS)," Proc. SPIE 10195: Unmanned Systems Technology XIX, Anaheim, CA (2017).
[5] Committee on National Security Systems, "Committee on National Security Systems (CNSS) Glossary", CNSSI 4009 (6 April 2015).
[6] 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).
[7] "Unmanned Systems Integration Roadmap, FY2013-2038", DoD reference 14-S-0553.
[8] https://gdmissionsystems.com/cyber/products/taclane-network-encryption/taclane-micro-encryptor/
[9] https://gdmissionsystems.com/cyber/products/taclane-network-encryption/taclane-c100-encryptor/
[10] https://www.viasat.com/products/haipe-encryptor-kg-250x
[11] https://www.viasat.com/products/ips-250x
[12] https://www.viasat.com/products/kg-250xs
[13] http://www2.l3t.com/cs-east/what-we-do/products/encryption-products_red-eagle.htm
[14] http://www2.l3t.com/cs-east/what-we-do/products/encryption-products_talon.htm
[15] https://gdmissionsystems.com/cyber/products/data-at-rest-encryption/protecdar-embedded-encryptor/
[16] https://www.viasat.com/products/encryption-kg-200r
[17] https://www.viasat.com/products/encryption-kg-200m
[18] http://www.tacticalcds.com/CenturionCDS/CenturionCDS_Specifications.html
[19] https://www.viasat.com/sites/default/files/media/documents/haf-100x_datasheet_013_web.pdf
[20] https://www.rockwellcollins.com/-/media/Files/Unsecure/Products/Product_Brochures/Information_Assurance/Cross_Domain/MicroTurnstile_data_sheet.ashx
[21] http://www.lockheedmartin.com/us/products/cross-domain-cyber-solutions.html
[22] http://www.raytheon.com/capabilities/rtnwcm/groups/gallery/documents/digitalasset/rtn_216079.pdf
[23] http://www.tacticalcds.com/TACDS/TACDS_Specifications.html
[24] https://www.viasat.com/products/embeddable-security-system
[25] Crypto Core Modernization Family, NSA, 2016.
[26] https://www.army.mil/article/162890/Army_s_standardized_encryption_chip_comes_to_the_RESCUE

[27] Small Organic Precision Munitions (SOPM) Secure Micro Digital Data Link (SMDDL) Fact Sheet, Rev 2.0, 10 September 2013.

ACRONYMS

AEODRS	Advanced Explosive Ordnance Disposal (EOD) Robotic System
CCI	Controlled Cryptographic Item
CCM	Crypto Core Module
CDS	Cross Domain Solutions
CHVP	Cryptographic High Value Product
CT	Ciphertext
DAR	Data at Rest
DIT	Data in Transit
EOD	Explosive Ordnance Disposal
FlexCSR	Flexible Cyber-Secure Radio
GPS	Global Position System
HAIPE IS	High Assurance Internet Protocol Encryptor Interoperability Specification
IME	In-line Media Encryptor
INE	In-line Network Encryptor
JCAUS	Joint Communication Architecture for Unmanned Systems
MC	Mini Crypto
MTRS	Man-Transportable Robotic System
NSA	National Security Agency
NSI	National Security Information
NSWC	Naval Surface Warfare Center
NSWC IHEODTD	NSWC Indian Head Explosive Ordinance Disposal Technology Division
OCU	Operator Control Unit
PT	Plaintext
SmDDL	Secure Micro Digital Data Link
SSC	Space and Naval Warfare Systems Center
SWaP	Size, Weight, and Power
UAS	Unmanned Aircraft System
UCDSMO	Unified Cross Domain Services Management Office
UGS	Unmanned Ground System
UIAS	Unmanned Information Assurance Services
UUS	Unmanned Undersea System
UxS	Unmanned System, inclusive of UAS/UGS/UUS