communications
Government Services, Inc.

3750 Centerview Drive
Chantilly, Virginia 20151
Phone: (703) 708-1400
FAX: (703) 708-5707

Tactical Automated Security System (TASS)

CM SECURITY POLICY
for the CM Device, FIPS 140-2 LEVEL 1 Validation
HARDWARE VERSION – REV B, Part no: 1550

FIRMWARE VERSION – 5.7

CDRL N/A

Contract Number: F19628-97-D-0033

L-3 GSI Document Number: **TASS-1623**

September 08, 2004

REV 1.5

Prepared by L-3 Communications

Government Services, Inc.(L-3 GSI)

For

Air Force Materiel Command Electronic Systems Center ESC/FD

5 Eglin Street, Bldg. 1624-First Floor

Hanscom, MA 01731-2308

Security Classification: UNCLASSIFIED

CM SECURITY POLICY
for the CM Device, FIPS 140-2 LEVEL 1 Certification

TASS-1623

HARDWARE VERSION – REV B, Part no: 1550

FIRMWARE VERSION – 5.7

For the

Tactical Automated Security System (TASS)

Contract Number: F19628-97-D-0033

L-3 Communications Government Services, Inc. (L-3 GSI)
3750 Centerview Drive

Chantilly, VA 20151

DOCUMENT REVISION HISTORY

Revision	Date	Description of Change	Responsible Person
	September 24, 2002	Original Write-up	Suma Shastry
	November 21, 2002	Re-organized presentation of information and removed proprietary information	Daun-Marie Curts, CEAL, CygnaCom Solutions
	December 10, 2002	Revised per CygnaCom's comments	Terry Powell
1.0	December 26, 2002	Revised document as per Cygnacom comments	Suma Shastry
1.1	April 28, 2003	Final revision as per Cygnacom comments	Suma Shastry
1.2	May 1, 2003	Added hardware version number and revised as per Cygnacom comments	Suma Shastry
1.3	Jan 05, 2004	Revised document to reflect new company name	Suma Shastry
1.4	April 27, 2004	Addressed NIST feedback in the document.	Suma Shastry
1.5	September 08, 2004	Addressed NIST comment feedback on the use of Single DES and roles. Updated firmware version.	Rory Saunders

Table of Contents

Table of Figures

Overview

The Communications Module (CM) is a component of the Tactical Automated Security System (TASS). TASS is a rapidly deployable, easily transportable and quickly relocatable integrated security system that can be tailored for a diverse variety of applications. The TASS is used to detect, monitor and assess intrusions into a secured area. TASS provides semi-permanent security to resources with little or no allied support or site preparation, and in some instances, it is used in lieu of more permanent security systems, which require substantially more installation time, effort, manpower and materials. The system also provides portable, self-contained, "fly-away" components for rapid protection of individual or small assets. Additionally, the system provides for a lightweight man portable easily emplaced and recoverable security system for small units.

To facilitate this concept, system equipment ranging from annunicators to field sensors must be simple to install, operate, recover and maintain. TASS enhances the capability for early detection and identification of an intrusion to prevent damage or destruction of mission critical assets. For example, in Air Base Defense (ABD) applications, TASS equipment will be deployed to provide an integrated security system with the capability to collect sensor data from each sector area, process the data, and display time critical information so that operators can make timely, informed decisions. In other scenarios, fewer TASS components will be employed to provide security to disperse and/or individual resources or to augment small sections of permanently secured perimeters.

TASS applications include: main operating bases (MOB), transitioning bare bases, taxiway gaps, aircraft parking and storage areas, dispersed assets, buildings (exteriors and interiors), border surveillance and drug interdiction.

The TASS consists of a number of components that are utilized to form a wireless security network. These components are:

- Communications Module (CM)
- Hand Held Module (HHM)
- Sensors
- Relocatable Battery Module (RBM)
- Desk Top/Lap Top Annunicator (DLA)
- Communications Module Converter (CMC)

The CM is a portable, battery powered packet radio. A CM can be configured via a programming unit for three types of operation:

o CM Sensor (CMS): This configuration of CM interfaces to a number of different sensor types. A CMS' primary function is to create and transmit an intrusion alarm message, over an RF (Radio Frequency) link, whenever a sensor reports an intrusion event.

o CM Annunicator (CMA): This CM configuration receives alarm messages sent by CMS and forwards them serially, via a RS485 cable, to an annunicator unit, which displays the alarm

information to an operator. A CMA can also transmit command messages from the annunicator to the CM in the network via the RF link.

o CM Repeater (CMR): This configuration of CM is used to store and forward RF packets between nodes of a network where the RF link budget is insufficient for units to communicate directly. A CMR can also be connected to sensors and report alarm events for its location.

The HHM is a hand held device that incorporates the packet radio functionality of a CM along with a keyboard and LCD display. The HHM serves as both a programming device and a portable annunicator unit. As a programming device, the HHM permits an operator to configure CMs and other HHMs with all the operational parameters needed to function in a given network. The operator sets up the operating configuration for the various units from a series of menus, using the keyboard and display. The HHM can then upload the configuration data to the CM (or HHM) serially via an RS485 cable. As an annunicator an HHM can display messages from other units received over the RF link. The HHM also incorporates cryptographic capability. The HHM is separately validated as conforming to FIPS 140-2.

The RBM provides power to the units in the field and also provides an interface to additional sensors in a given site. The RBM is not tested against FIPS 140-2.

Sensors for this system can be either active or passive. Sensor types range from simple tripwire sensors to bi static radar devices. The basic passive devices connect directly to the CMS unit and provide simple on/off indications to the CM. Active sensors are connected indirectly to a CMS via an RBM unit. In this case the status of the sensor is forwarded to the CM from the RBM using a serial protocol. The sensors are not tested against FIPS 140-2.

The DLA is a PC based computer running firmware that is used to display the status of the various nodes of a network and send a limited number of commands to the nodes via a connected CMA. The DLA is not tested against FIPS 140-2.

The CMC is a serial communications converter that converts the RS485 data from a CMA to RS232 data usable by DLA. The CMC also provides a multi-drop capability that allows a single DLA to be connected to multiple CMA in a given deployment. The CMC is not tested against FIPS 140-2.

Figure 1 depicts an example of a TASS/PEWD II deployment.

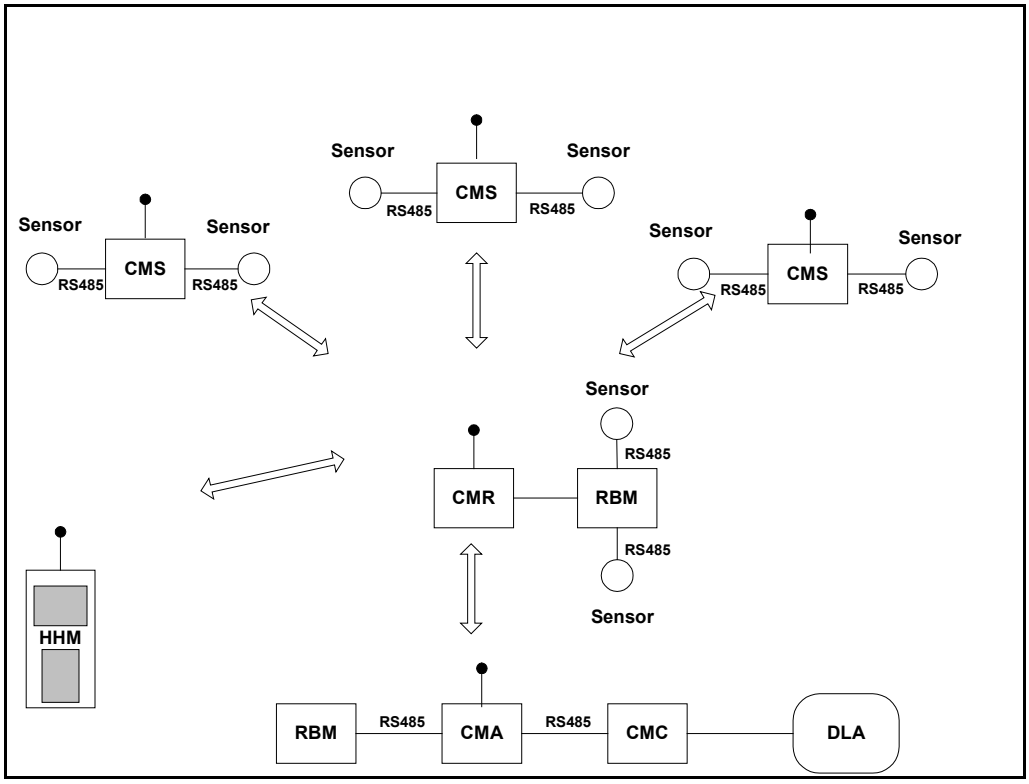

Figure 1, Typical TASS Network

1 Communications Module

Although there are many components of the TASS, this document services as the Security Policy for the Communications Module (CM) and describes how the CM meets FIPS 140-2 Level 1 Security Requirements.

1.1 Overall Functionality

1.1.1 A CM Configured as a CM Sensor (CMS)

The following paragraphs describe a typical operational scenario for a CM. A CM, to be configured as a CMS, is taken to a site along with sensors and battery. The operator sets up the CM's operational parameters from the HHMs CM configuration menus. After all of the operational parameters have been set, the configuration information is sent to CM using RS485 ports through an attached short cable from CM to HHM.

Operational parameters to be setup include:

- Unit ID
- Operating frequency
- CM operational configuration (CMS in this example)
- Type of sensors to be attached to the CMS
- State-of-health reporting period
- Encryption enabled or disabled

If the encryption option was enabled, the HHM also transfers a keyset to the CMS. The keyset consists of the Data Encryption Keys (DEKs) used for encrypting the RF network messages. The encrypted DEKs including crypto period and key name information are transferred to the CMS where they are decrypted, authenticated, and stored in the CMS' flash memory. With the exception of the DEKs all data transferred is unencrypted. The DEK's are transferred to CM from HHM or to HHM from CM in encrypted form using Triple DES. It is also possible for a CMS to upload its current set of DEKs to an HHM using the same transfer mechanism.

Once configured as a CMS the device is attached to the sensors and left at the location for standalone operation. The device is left unattended until it requires a battery change, requires a new set of DEKs, configuration parameters, or removal at the end of mission. During a mission a CMS largely remains idle, only exchanging RF packet data with the network during specific events. These events are:

- Intrusions – All intrusions are reported as intrusion alarms to CMA and HHM.
- Change of sensor state (alarm events)
- Periodic State-of-Health transmissions

- Internal alarm events (low battery, internal fault, tamper (sensor disconnect), self-test failure)
- External commands from other nodes in the network

If the unit is configured for encryption the data in the RF packets are encrypted with the exception of the link layer protocol portions. A TASS network is deployed with all devices configured for encryption or no encryption. All devices in a given network operate on the same set of DEKs (if encryption is enabled). The CM enforces the use of FIPS approved encryption services.

A TASS device, enabled for encryption, automatically discards any received packets that are not encrypted. A TASS device that does not have encryption enabled will discard any encrypted RF packets at the link layer processing stage. Additionally, TASS devices that do not have encryption enabled will be incapable of decrypting any messages since any key variables held by the device are purged from the unit's memory when configured for unencrypted operation.

1.1.2 A CM Configured as a CM Repeater (CMR)

A CM configured as a CMR performs all of the functions described for a CMS. Additionally, the CMR performs a store-and-forward function on all RF packets that are received and are not addressed to its device ID. If the device is configured for encrypted operation it must decrypt the message contained in the RF packets since the routing information is contained within the encrypted portion of the message. Once the CMR determines that the message is to be forwarded, it re-encrypts the message prior to re-transmission.

1.1.3 A CM Configured as a CM Annunicator (CMA)

A CM configured as a CMA serves as the root node of a network. Any valid messages received by a CMA are processed and then forwarded to the annunicator workstation (the DLA) via a RS485 port with a CM Converter (CMC) as an intermediary. The messages passed between the CMA, CMC, and DLA are unencrypted. A CMA also processes command messages sent to it from a DLA and then transmits them over the RF link to the intended destination in the network.

A CMA can also initiate a number of messages autonomously for transmission over the network such as time synchronization, issuing command to change key from primary to secondary. All encrypted RF messages contain a timestamp field that is used to thwart replay attacks on the system. Whenever a CMA that receives a message from a network node with an improper timestamp it will attempt to update that node's real-time-clock. Messages with bad timestamps are also processed by the CM's anti-spoofing logic to determine if the message should be accepted or rejected.

CMA communicates with other CM's like CMS and CMR's as well as HHM's. The communication between CMA and other CM/HHM is encrypted whereas only the communication with DLA is in plain text.

2 Cryptographic Module Specifications

The purpose of the CM is to provide cryptographic protection to data and keys transmitted between CMs or between a CM and a HHM. The CM falls under the "multi-chip standalone module" category of FIPS 140-2. The hardware design consists of two printed wiring boards (PWBs) contained within a metal case, which defines the boundary of the module. The PWBs are the Controller Assembly and the RF Assembly. The Controller Assembly performs all radio control and data processing functions for the device, including all cryptographic functions. The RF Assembly provides the RF physical layer functionality for the CM. Since all cryptographic functions are performed in the comptroller assembly, the RF assembly is excluded from the requirements of FIPS 140-2.

Figure 2 shows a simplified block diagram of the Controller Assembly. The Controller Assembly performs all radio control and data processing functions for the device, including all cryptographic functions.

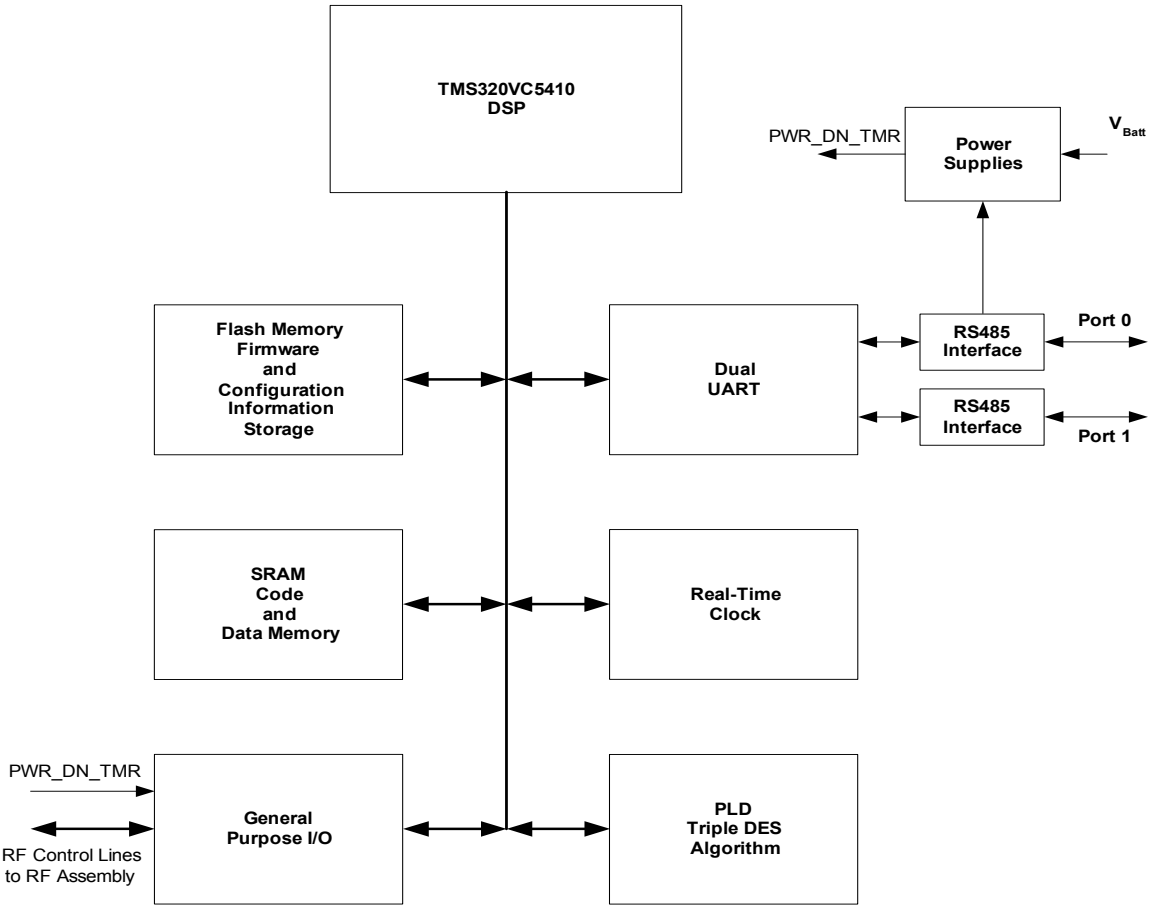

Figure 2, CM Controller Block Diagram

3 Cryptographic Module Security Policy

The cryptographic functions of the CM employ the Triple DES algorithm. All cryptographic operations of the device use Triple DES with 3 identical keys or with 3 unique keys. The use of Triple DES with 3 identical keys is equivalent to single DES and is only allowed for legacy systems. Security functions performed by the CM cryptography are:

- RF message encryption/decryption: TDES, FIPS PUB 46-3 compliant
- RF message bypass (unencrypted mode operation) – explained in section 9.8 bypass operation.)
- Message and data authentication, FIPS PUB 113 compliant
- Pseudo-random number generation. ANSI X9.31 Appendix A.2.4
- Data Encryption Keys (DEK) exchange: FIPS 171 compliant
- Key management functions, DEK storage, DEK erasure, DEK masking, crypto period enforcement

The cryptographic functions in the CM use a combination of hardware and firmware. The Triple DES algorithm is a hardware implementation, residing in a Programmable Logic Device (PLD). Logic has been added to the PLD design to implement FIPS approved CBC as well as ECB modes operation.

The cryptographic module implemented in the CM will function as follows:

1. The CM is controlled by a set of commands that are transmitted to it from the HHM.

2. The cryptographic officer may initialize a CM to function as a CMS, CMR, or CMA.

3. The CM will have the capability to encrypt plaintext data input and output the corresponding cipher. (Used in the CMS mode)

4. The CM will have the capability to decrypt input cipher text, re-encrypt the resulting plaintext under a new key and output the corresponding cipher text. (Used in the CMR mode)

5. The CM will have the capability to decrypt input cipher text and output the resulting plaintext. (Used in the CMA mode)

6. The CM will have the capability of transmitting and receiving stored keys encrypted under a Key Encryption Key.

4 Cryptographic Module Ports and Interfaces

The hardware design of the unit provides the following external physical ports:

- RF port (antenna connector): Bi-directional
- RS485 ports: serial data and external power. Bi-directional
- Battery connector: Primary power interface

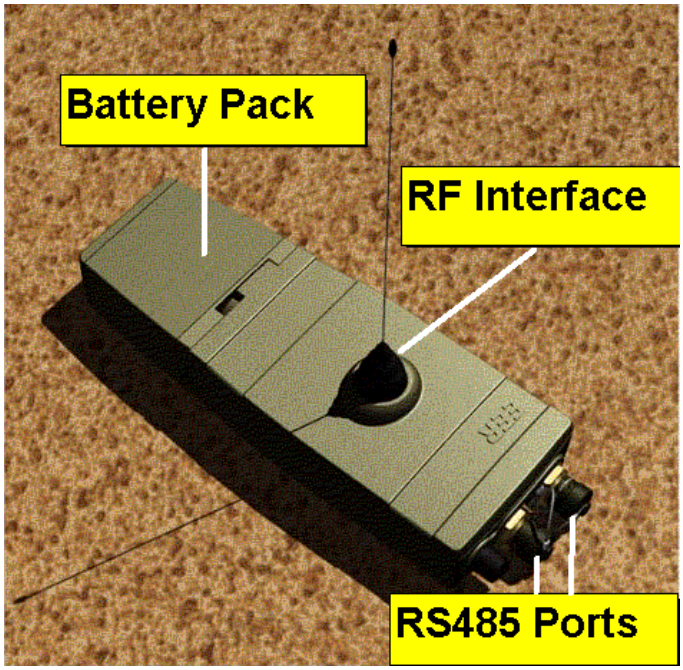

Figure 3, Communications Module

The cryptographic module boundary incorporates all circuitry within the CM case except the battery pack.

The CM device has four ports and an On/Off switch (not shown in Figure 2). The ports and interfaces are described in Table 1.

Table 1, CM Ports and Interfaces

Physical Ports	Logical Interfaces
Battery Pack	Power input
RS485 Port 0	Data Input, Data Output, Control Input, Status Output
RS485 Port 1	Data Input, Data Output, Control

Physical Ports	Logical Interfaces
	Input, Status Output
RF Antenna	Data Input, Data Output, Control Input, Status Output
Power On/off Switch	Control Input

Power (9 VDC – 15 VDC) is input to the device either through a battery pack through the power connector, or via one of the RS485 connectors.

The RF port sends and receives transmissions in the 132 to 176 MHz and 406 to 470 MHz bands. The modulation type utilized by the unit is narrow band FM and the transmit power output level is 1 watt minimum.

Each of the RS485 ports can connect to the following:

- Passive sensors
- Relocatable Battery Module (RBM)
- Active sensors (through an RBM)
- Communications Module Converter (CMC)
- Hand Held Monitor (HHM)

When connected to passive sensors the interfaces handle simple on/off signaling information.

When connected to an RBM, the ports carry DC power and unencrypted serial data. The serial data stream is bi-directional and contains RBM status and control information and information from active sensors connected to the RBM.

When connected to a CMC (in the CMA configuration only) a RS485 port carries bi-directional RS485 data between CMA and DLA. This data stream is unencrypted and carries alarm, status, and control messages for all units in a network.

When connected to an HHM an RS485 port carries bi-directional RS485 data. This data stream is also bi-directional and carries the following types of information:

- CM configuration information (frequency, type of operation (CMS, CMR, CMA), encryption on/off, unit ID, type of sensors attached, date and time, position, etc.).
- Key variables, both send and receive. The actual key variables are encrypted within these messages, the rest of the protocol is unencrypted.
- Firmware (CPU and PLD) download information (unencrypted)

5 Roles, Services, and Authentication

The CM supports two User roles and a Crypto-Officer role of operation. Switching between these roles is based upon external commands received over the RS485 port from a HHM.

The roles are defined per the FIPS140-2 standard as follows:

1. **Users - first level of access.** Can't modify encryption settings. Can configure CM devices and carry out services based on preset encryption capabilities. The User 1 is an operator who has to authenticate with a User password to access CM services through HHM, as CM itself doesn't have direct user interface. The User 2 is an HHM or another CM device that has access to the CM through authenticated messages to access CM services.

2. **Crypto-Officer – second level access.** Can access/carry all services implemented in the Module, download/upload encryption keys, firmware to/from HHM's, zeroize keys, erase firmware. The crypto officer has to authenticate with encryption password to access CM encryption services through HHM, as CM itself doesn't have direct user interface.

3. The CM does not support a **Maintenance role.**

   The CM satisfies level 1 requirement for Roles, Services, and Authentication, which do not require authentication of operators. However the CM is designed to require authentication to perform the following services:

   - DEK key establishment require authentication of the KD_KSM exchange messages before the CM accepts the new keys.
   - Operator commanded erasure of key variables from a HHM requires authentication of the command message before the command is executed.
   - Over-the-Air switching of DEKs require message authentication.
   - Firmware download operations require both authentication of individual message packets and authentication of the overall code.

5.1 User Role Commands:

Table 2 contains a list of User commands processed by the CM.

Table 2, CM User Role Commands

Command	Description
Send RF Message	Sends a message packet over the RF network in response to an alarm or control event.
Receive RF Message	Receive and process a message from the RF network.

Configure CM	CM accepts and stores operational parameters from Hand Held Monitor (HHM) device.
State-of-Health Poll	CM commanded to transmit a State-of-Health message.
Update SOH Table	CM commanded to delete a node from its State-of-Health tracking table. CMA configuration only.
DLA Offline	Processing of all received RF messages, except State-of-Health, is disabled. CMA configuration only.
DLA Online	All RF message processing enabled.
Sleep Mode Disable/Enable	Commands CM to enter or exit Sleep mode (power conservation) CMS configuration only.
GPS Position Request	CM commanded to transmit its stored GPS position.

5.2 Cryptographic Officer Role Commands

Table 3 contains a list of commands processed by a CM in the Cryptographic Officer Role.

Table 3, CM Crypto Officer Commands

Command	Description
Key Variable Download	CM accepts a new DEK keyset from an HHM over the RS485 port.
Key Variable Upload	CM sends its current DEK keyset to an HHM over the RS485 port.
Purge DEKs	Erases DEKs.
Purge Firmware	Erases all key variables and firmware.
Change Keys	The CM is commanded to switch operation from the primary to the secondary DEK. If the CM is configured as a CMA, it will forward the command to all devices in the network over the RF port.
Enable/Disable Encryption	Enables or disables encryption in the CM. If encryption is disabled any DEKs stored in the CM's memory are erased.
Reprogram Firmware	CM is reprogrammed with new firmware downloaded over the RS485 port. (The new firmware must be *validated to FIPS 140-2*.).

6 Finite State Model

Table 4 contains a summary of the Finite State Model for the Communications Module.

Table 4, CM States

State	Description
Power On/Off	Power turned on. DSP loads firmware from flash to SRAM.
System Initialization	TDES algorithm loaded into PLD, Real-Time-Operating system initialized.
Restart	CM operational parameters and key variables loaded from flash memory. Radio set to operational frequency.
SelfTest	Firmware authentication tests, key variable authentication, Known Answer Tests performed on all approved algorithms.
Send Encrypted Message	Encrypts and transmits a message over the RF network in response to an alarm or control event.
Send Plaintext Message	Same as above without encrypting the message (Transmit Bypass)
Receive Encrypted Message	Receives and decrypts an alarm or control message from the RF network.
Receive Plaintext Message	Same as above without the decryption operation (Receive Bypass)
Download Configuration Data	CM receives configuration information from the RS485 port.
Upload Configuration Data	CM sends its stored configuration over the RS485 port.
DEK Download	CM receives a new set of Data Encryption Keys (DEKs) from the RS485 port.
DEK Upload	CM sends its stored Data Encryption Keys (DEKs) from the RS485 port.
Change DEK	CM switches from the primary DEK to the secondary for encryption.
Reprogram Firmware	CM receives new firmware over RS485 port.
Purge Keys	Erases DEKs or DEKs and firmware
Recoverable Alarm State	Results if a serious fault condition occurs during operation. The CM automatically re-initializes itself.
Non-Recoverable Alarm State	Results if a serious fault is detected during initialization of the CM or during the power on SelfTest state. The CM must be manually reset.

7 Physical Security

The CM's physical security characteristics comply with those specified for Security Level 1 of FIPS PUB 140-2. The CM module is contained within a production grade chassis that has a removable cover. The circuitry on the PWBs comprising the module consists of production grade components and the PWBs have a conformal coating to protect the circuitry.

8 Operational Environment

Cryptographic control and Key Management for the module is implemented in firmware. This firmware is written in the C language, with some minor time critical exceptions written in the host platform's assembly language (Texas Instruments TMS320C5410). The application runs on a real-time operating system (RTOS); Nucleus Plus. The RTOS runs in a non pre-emptive mode thus ensuring that each task relinquishes its control of the system only at pre-defined points of its execution. All firmware that performs secure functions is logically isolated from non-cryptographic code in separate object code modules. These modules execute in system tasks separate from those in which the non-secure code executes. Access to all cryptographic and RTOS services by the non-critical tasks are limited to a well-defined set of API functions used during the development.

The CM firmware provides an application specific operational environment, responding to only to the command set that was developed for it. As manufactured the CM firmware, in flash memory, is pre-programmed into memory at the factory. The CM firmware is capable of being updated with new firmware using either a PC download program, or by an HHM with the new version of the code via serial transfer through one of it RS485 ports. Only firmware validated to FIPS 140-2 that is authenticated by a Triple DES MAC can be loaded into the module.

9 Cryptographic Key Management

The cryptographic functions of the CM employ the Triple DES algorithm. Implementation of this algorithm is either Triple DES using a key variable consisting of three identical sub-keys or Triple DES using 3 unique keys depending on operator selection. Security functions performed by the CM cryptography are:

- RF message encryption/decryption: TDES, FIPS PUB 46-3 compliant
- RF message bypass (unencrypted mode operation) – refer section 9.8 for bypass operation.
- Message and data authentication, FIPS PUB 113 compliant
- Pseudo-random number generation. ANSI X9.31 Appendix A.2.4.
- Data Encryption Keys (DEK) exchange: FIPS 171 compliant
- Key management functions, DEK storage, DEK erasure, DEK masking, crypto period enforcement

The cryptographic functions in the CM use a combination of hardware and firmware. The Triple DES algorithm is a hardware implementation, which implements FIPS approved CBC as well as ECB modes operation.

9.1 Key Management

The module implements a number of functions that are either used internally or exposed in the API to meet the FIPS140-2 Level 1 requirement for Key Management.

Key Management in the CM firmware incorporates two types of key variables. These key variables types are:

- Data Encryption Keys (DEKs)
- Internal key variables

DEKs are TDES variables used in the encryption and decryption of message data passed over the TASS RF network. The CMs have the capability to exchange DEKs over the RS485 serial ports. Each DEK has a crypto period and key name associated with it.

The internal key variables are fixed variables used by the system with no crypto period. They can only be changed by downloading the firmware with new sets of internal keys to the CM, which requires units to be returned to the factory for modification of firmware. The internal variables are:

- Key Generating Key (KGK): A Triple DES variable used in the ANSI x9.31 approved pseudo-random number generator algorithm.
- Key Encryption Key (KEK): This is the Triple DES key variable used to encrypt DEK variables during key transfers.
- Default Authentication Key (KA): This is the Triple DES key variable used for the FIPS 113 approved authentication algorithm for message and data authentication (except DEK transfers).
- Session Authentication Key (SessionKA): This is the authentication key used to authenticate all DEKs transferred over the RS485 port. The transferred DEK itself is used as authentication key.
- Fixed Masking Key: This is one component of the TDES masking key used to protect the internal key variables in memory. It is combined with the Split Key to form a Triple DES masking key.
- Split Key: This is the second component of the TDES masking key used by all key variables in the CM. It is combined with the Fixed Masking Key to form the TDES masking key used to protect the internal key variables. It is combined with a DEKs key name to form its masking key.
- Triple DES masking Key: The key formed by XORing two components of the Fixed Masking Key and the Split Key. The Triple DES masking Key is used to encrypt keys stored in CM memory.

- Electronic Codebook KAT Key (ECBKAT): This is the Triple DES key used for the Electronic Codebook mode Known Answer Test.

- Cipher Block Chaining KAT Key (CBCKAT): This is the Triple DES key used for the Cipher Block Chaining mode Known Answer Test.

- Random Number Generator KAT Key (RNGKAT): This is the Triple DES key used for the RNG KAT.

9.2 Pseudo Random Number Generators (PRNG)

The CM Pseudo Random Number generator utilizes the approved algorithm recommended in ANSI x9.31 1998, Appendix A.2.4. A 64-bit vector R that contains four 16-bit PRNs is generated.

The PRNG generates blocks of up to 128 random numbers in advance of their need and places them in a random number queue. Once the queue is filled the PRN task suspends itself until the queue falls below a threshold of 64 numbers, at which time the task is reactivated until the queue is filled once more. Each R vector generated is continuously compared to the previous R vector generated. If two consecutive R vectors are equivalent, the PRN task will force the CM into a crypto alarm state.

The CM firmware obtains the 16-bit random numbers generated by the task using the function CM_RandomNumber. Each call to CM_RandomNumber returns a single random number from the queue. In order to guard against corruption of the queue, CM_RandomNumber also performs a continuous random number check on the PRNs accessed.

9.3 Key Generation

The CM doesn't have key generation capabilities. It gets keys downloaded from HHM. The key establishment process and storage is explained in successive sections below.

9.4 Key Establishment

The CM has the capability to exchange DEKs with an HHM (key establishment) acting as a key loader device. As such it has the ability to:

- Download DEKs
- Upload DEKs.

Key establishment is performed over the RS485 port only. The CM encrypts DEK's before key establishment. This protocol is FIPS 171 compliant and includes the following command messages:

- Request for Service Initiation (RSI): Initiates all DEK transfer processes.
- Data Key_Key Service Message (KD_KSM): Message that contains a single DEK variable, its expiration date, key name. The DEK is encrypted using the KEK.
- Response Service Message (RSM): Acknowledges successful reception of a message.
- Error Service Message (ESM): Sent when a fault occurs in the processing of a message.
- Key Name Query (KNQ): Requests the key name and expiration date of a DEK.

- Key Name Response (KNR): The response to a KNQ message. Contains the key name and expiration date of the requested key. This information is plain text.

The KD_KSM, RSI, ESM, and RSM messages include 32-bit Message Authentication Codes, generated using the FIPS PUB 113 approved algorithm. The RSM, RSI, and ESM messages use the default authentication key (KA) for this process. The KD_KSM message uses the transferred DEK as the authentication key.

The Disconnect Service Message (DSM) is used to command a CM connected to the HHM to erase its DEK or all keys and firmware. This message includes a Triple DES MAC that is generated using the default authentication key.

9.5 Key Entry & Output

The internal key variables are installed as a part of the firmware, in flash memory, during the manufacturing process. The internals keys are produced during the development effort and are included in an object module linked with the rest of the firmware during the code build process. The object module containing the internal keys is compiled in a separate firmware project from the rest of the TASS code. This is done to separate the internal key variable source code from the rest of the firmware documentation. The key variables in source code are entered manually into the file. The keys are generated using the same FIPS approved algorithm (ANSI X9.31) as used to generate DEKs in the HHM and are encrypted using the masking technique described in paragraph 9.6.2. The encrypted key variables are then entered into the source file and compiled to generate the object module. The internal keys are masked in the object module to protect them from being compromised by an analysis of the contents of flash memory or during firmware download operations.

9.6 Key Storage

9.6.1 Key Variable Storage

The primary storage object for the key variable during operation of the CM is the KeyList, which resides in SRAM in the firmware's data memory area (address range 0x8000 to 0xFFFF). This object holds a record for each key variable used by the device. These records vary in size and structure, dependent upon the type of key variable stored in the record.

The key record for a DEK contains the following information:

- The masked key variable
- The DEK's key name
- The DEK's expiration date
- The DEK's current state (standby, active, stale, purged)

Standby – The state of a secondary key when the primary key is in use as the secondary is standby key.

Active – The current valid key, which is being used.

Stale – The expired primary or secondary key still being used, which has 24-hour grace period.

Purged – Key doesn't exist anymore as it has been deleted.

Expired – Keys are expired, crossed 24 hour grace period, can't be used anymore.

The key record for internal keys consists of the masked key variable only.

Because the CM does not employ any battery backup for its memory, the masked key variables and their current state (DEKs only) are also stored in flash memory in a structure named TRadioParameters. This structure resides in a separate sector of flash memory from the firmware and device configuration information (address 0x40A000 to 0x40AFFF). All key variables are loaded from flash memory to the KeyList whenever the CM is (re) booted. The records stored in flash also contain the authentication code for each key record to ensure the validity of the key load process. Whenever a DEK changes state, DEKs are transferred, or new firmware is downloaded into the CM, the key variables in flash are updated as well as the KeyList in SRAM. The firmware uses the key variables from the KeyList in SRAM for its cryptographic operations because the access time for memory in SRAM is faster than that in flash memory. Thus the key variables in flash are only accessed during boot operations of the firmware and store any changes to the keys or their state in non-volatile memory.

9.6.2 Protection of Keys

The keys are stored in flash and in SRAM (in the KeyList) are protected from analysis and inadvertent corruption by several mechanisms.

Protection from analysis is achieved through the masking of the key variables. The masking processing utilizes Triple DES encryption of each key variable in memory using a specific masking key variable. Key variables are only unmasked immediately prior to each encryption/decryption operation and all unmasked copies of the key variable is erased by calling purging routine immediately thereafter. The key variable used for masking is created only on demand, automatically, by the CM from separate components in data memory prior to the usage of any key variable and is destroyed immediately after each masking/unmasking operation. The two components are combined with an exclusive OR operation to form the masking key variable. It is realized that this is considered to be a weak protection mechanism, since all components of the masking key can be found in data memory. However, the mechanism employed requires a significant reverse engineering effort to defeat. This is considered to be beyond the semi-skilled threat level assessed by the primary customer for this system (USAF Electronic Systems Command). A different masking key combination is used for the DEKs (dependent on the unique key name of a DEK) than is used for the internal key variables.

The discretionary and automatic key purge functions discussed in the previous paragraph offer a means of key protection that can be employed in the case of an overt security threat.

The CM is protected from the inadvertent use of corrupted key variables through the use of 32-bit Data Authentication Codes stored with each key variable's record in memory. Each Triple DES DAC is generated using the FIPS 113 approved algorithm. These DACs are used to check key variable validity under the following conditions:

- During cryptographic self-test
- When loading the KeyList from flash memory

- When storing key variables or DEK state changes to flash memory
- Prior to performing any key transfer process.
- Whenever switching from primary to secondary DEK, either manually or automatically.

If a corrupted key record is detected the CM can attempt to recover the key from a backup copy, which is encrypted with TDES as original keys, also stored in flash memory. If the backup copy validates it will be used by the system, otherwise the keys are marked as purged and the CM defaults to unencrypted mode.

9.6.2.1 DEK Crypto periods and DEK Switching:

The DEKs have crypto periods assigned to them, selectable by the operator upon their creation in an HHM, which transfers the information to the CM. The available crypto periods are:

- Manual
- 30 days
- 90 days
- 180 days
- No expiration

9.7 Message and Data Authentication

The CM application firmware employs the FIPS 113 approved algorithm for it message and data authentication processes. The processes that employ authentication are:

- Firmware downloads – Only FIPS approved firmware can be downloaded.
- DEK key establishment over the RS485 port.
- Over-the-Air switching of DEKs
- Cryptographic self-test.

The algorithm employed uses Triple DES in the CBC mode. The key variable used for the producing the authentication code depends on the process that requires authentication. Most of the processes use the default authentication key (KA) stored in flash memory. Authentication of DEK transferred over the RS485 port employs the plain text DEK itself. The initialization vector used is all zeroes, as specified in FIPS PUB 113. The data to be authenticated is run through the algorithm and the most significant 32-bits of the last encryption operation becomes the authentication code.

The firmware download process uses authentication to validate each firmware packet transferred over the RS485 port. The download process also authenticates the entire downloaded firmware, after it has been stored in flash memory, to verify the authenticity of the entire load (the ROM firmware DAC is contained in the last downloaded packet).

The DEK transfer processes applies message authentication to critical messages in the key transfer protocol. This was discussed in the Key manager section.

The command issued over the RF link to force TASS devices to switch from the primary to the secondary DEK must be authenticated before the command is allowed to execute. A MAC (Message Authentication Code) field is included in the Command Key Changeover message for this purpose.

The cryptographic self-test process utilizes data authentication to validate the correctness of the runtime firmware in SRAM. This process is discussed in the Self-Test section.

9.8 Cryptographic Bypass

The CM application firmware includes a cryptographic bypass capability. This capability has been included because the device can be configured to communicated over the RF port in either encrypted or unencrypted modes of operation. The bypass facility only applies to the processing of RF messages.

Before either of the first two services can be called upon to perform the bypass CM_BypassRequest function must be called. This function determines if the Crypto Manager's state machine is in an allowable state for a bypass operation (BypassIdle, Warmboot, or SelfTest) and, if it is, the service sets the bypass event flag (RF_BYPASS_EN). If the service detects an invalid Crypto Manager state it denies the service (returns CM_BypassDenied).

The actual bypass process is accomplished by calling the appropriate bypass service function (CM_BypassRFMsgOut (), CM_BypassRFMsgIn()) with a pointer to the RF message information. Each of the services determines whether to allow the bypass based on the following rules:

- The Crypto Manager state machine must be in the BypassIdle state.
- The RF_BYPASS_EN event must be set.

Thus two independent flags must be set in order for the Bypass operation to occur. If either CM_BypassRFMsgOut() or CM_BypassRFMsgIn() are called and the RF_BYPASS_EN event is not set, the functions will return with a CM_BypassDenied error code. If RF_BYPASS_EN is set and the Crypto Manager is not in the BypassIdle state a fatal fault condition is declared resulting in the CryptoAlarm function being called and further execution of the firmware halted until the device is reset.

Before calling any of the bypass services, CM_BypassRequest must be called. This function determines if the Crypto Manager's state machine is in an allowable state for a bypass operation (BypassIdle, Warmboot, or SelfTest) and, if it is, the service sets the bypass event flag (RF_BYPASS_EN). If the service detects an improper Crypto Manager state it denies the service (returns CM_BypassDenied).

Once a bypass operation is granted the RF message is passed to the Crypto Manager task by the service routine. In the Crypto Manager task, the RF message is transferred from its input buffer to the appropriate output buffer type (Red/Black) before it is delivered to the queue of the destination task on the opposite side of the Red/Black boundary. The RF_BYPASS_EN event flag is reset after the message bypass is completed. A bypass fail-safe timer that is set during the CM_BypassRequest() service is utilized to automatically reset RF_BYPASS_EN in the unlikely event that the bypass service routine fails to reset the flag.

The CM must be configured and power cycled in order to begin unencrypted operation. Upon powering down, the keys residing in the CM are automatically purged. The CM restarts in bypass mode and obeys the BYPASS rule explained above.

9.9 Zeroization of Keys

Keys and critical security parameters (CSP) in the Module are stored in flash. The keys are loaded to SRAM during bootup and stored as keylist, which contains both primary key and secondary key. Whenever keys are purged by zeroizing, the keys in flash, SRAM as well as backup keys available in flash are purged. The module takes care of zeroizing all its internal keys and critical security parameters including total erasure of firmware on following conditions:

- Discretionary key erasure is performed when the CM receives a Disconnect Service Message (DSM) from an HHM. A DSM message can command CM to zeroize the DEKs only or zeroize all keys ***and*** erase all firmware. The later operation will render a CM totally inoperable. The DSM message contains a 32-bit Triple DES MAC that must be authenticated before the execution of the command is permitted.

- The CM erases its DEK keyset automatically when it is configured for unencrypted operation. At this point, next communication from this CM would be in Bypass mode and CM will not be able to communicate anymore with other encrypted CM / HHM devices.

- When CM is powered up without having battery connected for more than 90 seconds, the DEKs are erased.

10 EMI/EMC

This product conform to The EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Class A. The lab name is F2Labs of Damascus, MD.

11 Self-Tests

The CM firmware automatically performs a cryptographic self-test upon itself in response to specific events in its operation. These events are:

- Power-up initialization - I/O is disabled during power up self test.

- Prior to any DEK transfer process

- After a DEKs purge process

- After any configuration transfer operation.

An operator can force the module to perform self-tests by power cycling the module.

The CM cryptographic self-test process performs the following tests:

- Authentication of the runtime firmware in SRAM using a DAC – data authentication code.
- A Known Answer Test (KAT) of the Triple DES algorithm in EBC and CBC modes
- KAT on the RNG
- Authentication of all key variables in the KeyList
- Cryptographic bypass test
- Real-Time Clock and firmware timer test

The authentication of the runtime firmware uses the FIPS 113 approved algorithm to calculate a 32-bit DAC on all of CM code in SRAM (the CM executes its firmware entirely in SRAM) the result is compared to the DAC for the current version of firmware stored in flash memory. The value in flash memory is calculated prior to the formal release of the version and is included in the programming of the device. If the DACs fail to match the test fails.

The KAT tests consist of encrypting a fixed plain text data vector using a test key variable stored in the KeyList for each cryptographic mode used by the algorithm (ECB and CBC). The vectors (plaintext, ciphertext, and test keys) are taken from the example vectors in ANSI X9.52, Appendix C. The CBC mode KAT also requires an initialization vector, also taken from Appendix C of ANSI X9.52. The KAT for ECB mode involves the encryption/decryption of a block of data, while the CBC mode test is performed over two blocks. The resultant cipher text from this operation is compared to the expected value. If the cipher text matches the known answer, the cipher text is then decrypted and result is compared to the original plain text. If the expected answer is not obtained at any point in the process the test fails.

The KAT on the RNG uses a fixed RNG key, fixed date time vector, and fixed seed to generate a first random result, which is compared against the previously calculated known RNG value.

As mentioned in the Key Management section of this document all key variable records stored in the KeyList include a 32-bit DAC. During the self-test process all these records are authenticated to ensure the validity of the variables.

The cryptographic bypass test calls the cryptographic bypass functions and determines whether the bypass is correctly granted or denied.

A failure to achieve an expected result in any of the test cases results in a failure of the entire test.

The test of the RTC and firmware timer mechanisms are included in the cryptographic self-tests because their functions are critical to the proper detection of DEK expiration events. The test consists of setting the RTC hardware to a test date and time vector (after saving the current value) and setting a firmware timer to wait a specific period of time (1100 milliseconds). The timer mechanism is interrupt driven and a second non-interrupt driven timing loop is started in parallel as a part of the test. If the timer expires before the firmware-timing loop completes the firmware timer test passes and the test continues. If the timer does expire before the timing loop terminates the test fails. After the timer expires the new date and time is obtained from the RTC and examined for the expected value. The test value was chosen to cause a rollover of all fields in the RTCs date/time structure.

If any of the tests performed during cryptographic self-test fails, the CM is placed in the cryptographic alarm state.

All CM I/O is disabled during the cryptographic self-test process, with the exception of the RTC test, which requires operation of the interrupt mechanism.

The PRNG task and the CM_RandomNumber service employ continuous random number tests to detect any faults occurring in that process. A fault in the PRNG function will result in the CM being placed into a crypto alarm state. The test is discussed in more detail in the section on pseudo-random number generation.

12 Design Assurance

All CM source code, firmware release is tracked using Configuration Management. Microsoft SourceSafe is used as the CM tool for firmware development– leading to firmware release. All documents related to firmware analysis, design and developments are maintained using configuration management policy adopted by L-3 GSI through release history. The hardware components and other TASS related materials are tracked and maintained through billing materials, schematics with revision number/ date, which is again maintained by L-3 GSI configuration management system.

13 Mitigation of Other Attacks

This product is not designed to mitigate against other attacks and therefore none are specified.

14 Acronym List

ABD	Air Base Defense
CBCKAT	Cipher Block Chaining Known Answer Test
CM	Communications Module
CMA	CM Annunicator
CMC	Communications Module Converter
CMR	CM Repeater
CMS	CM Sensor
CPU	Central Processing Unit
CSP	Critical Security Parameters
DEK	Data Encryption Key
DLA	Desk Top/Lap Top Annunicator
DSM	Disconnect Service Message
DSP	Digital Signal Processor
ECBKAT	Electronic Codebook Known Answer Test
ESM	Error Service Message
HHM	Hand Held Module
IP	Intellectual Property
KA	Key Authentication
KAT	Known Answer Test
KEK	Key Encryption Key
KGK	Key Generating Key
KNQ	Key Name Query
KNR	Key Name Response

L-3 GSI	L-3 Communications Government Services, Inc.
MOB	Main Operating Bases
PEWD II	Platoon Early Warning Device II
PLD	Programmable Logic Device
PRN	Pseudo Random Number
RBM	Relocatable Battery Module
RF	Radio Frequency
RSI	Request for Service Initiation
RSM	Request Service Message
RTC	Real-Time Clock
RTOS	Real-Time Operating System
SRAM	Static Random Access Memory
SOH	State Of Health
TASS	Tactical Automated Security System
PWB	Printed Wired Board