Department of Homeland Security

FOR OFFICIAL USE ONLY

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS “FOR OFFICIAL USE ONLY” OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A “NEED-TO-KNOW” BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.

This page left blank intentionally

SECURITY DEVICE (CSD/ACSD) COMMUNICATIONS INTERFACE CONTROL DOCUMENT (ICD) SECURITY DEVICES-TO-NETWORK ACCESS DEVICES (NADS)

Version 8.0

U.S. Department of Homeland Security (DHS)
Science and Technology Directorate (S&T)
Cargo Security Test and Evaluation (CSTE)

Document Number CM/CS/SSC/SNL/REQ/R8.0/2010/1788

December 3, 2010

FOIA Exemption: *This document contains sensitive information exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 522(b) (2, 4, 5). Do not release without prior approval of the Department of Homeland Security Document Point of Contact*

Point of Contact:
DHS Science and Technology Cargo Security Program Manager
Kenneth Concepcion
Kenneth.Concepcion@dhs.gov
(202) 254-5351

Container Security Test and Evaluation Team
Lawrence Livermore National Laboratory
Pacific Northwest National Laboratory
Sandia National Laboratories
Space and Naval Warfare Command System Center San Diego

United States Department of Homeland Security

Science and Technology Directorate

Cargo Security Integrated Test and Evaluation Program

Technical Document Disclaimer

This document presents scientific and technical data resulting from testing and evaluation activities performed within the Science & Technology (S&T) Borders and Maritime Cargo Security Integrated Test and Evaluation Program (CSTE). Where possible, CSTE testing is performed in accordance with national or international consensus standards. When testing is performed for federal acquisition programs, test criteria are derived from systems requirements for the acquisition program. In other cases, test criteria are based on CSTE technical expertise and the U.S. Government's anticipated future mission requirements.

System performance results presented herein reflect the best efforts of the CSTE technical staff, but they neither guarantee nor endorse the suitability of the system for untested applications or other system requirements. Federal, state, local, or tribal agencies seeking to use this report as source selection criteria in an acquisition action must evaluate this report against their specific mission requirements.

This report does not constitute a federal endorsement of any tested system. Use of this report in whole or in part for commercial vendor advertising and marketing materials is strictly forbidden, and no permission for such use will be granted.

Change Summary: Security Device (CSD/ACSD) Communications Interface Control Document (ICD) Security Devices-to-Network Access Devices (NADs), Version 8.0

Note: Third column in the table below defines the ICD revision that used in the message header.

Date	Document Version	Message Header, ICD Revision Code. (0x00 not allowed)	Summary of Primary Changes
4 Apr 09	6.3 draft	1 (0x01)	1. Topology mandatory for initial implementation. IEEE 802.15.5 ad-hoc/mesh to be validated in near term revision for more persistent connectivity 2. Beacon Request deleted; use Coordinators' beacons 3. Commercial-purposed messages: Message (payload data) header: MSG Type is the only mandatory field 4. Roles of DCP in communications amplified 5. ICD Revision in message header enables variable parsing 6. Ascension number in message header for error detection 7. Secure message level ACK to Data Consolidation Point includes status 8. Secure message level ACK via command (reinstated) 9. Null Command: as ACK with no new action 10. Set UTC command (reinstated) 11. Nomenclature changes to satisfy CWG participants. 12. Removal of Zero Padding requirements for HASHing
27 Apr 09	6.3 draft	1 (0x01)	1. Arm/Change trip information: Added 3rd parameter 2. Status message: Removed Event Number and Reserved
19 May 09	6.4 draft	1 (0x01)	Incorporated Recommendations: 1. UID in message header changed from radio MAC address to a globally unique device-specific ID issued by IEEE as a EUI-64 identity http://standards.ieee.org/regauth/oui/tutorials/UseOfEUI.html 2. New concept: External CM relays to destination MAC address (internal ACSD/CSD) based on installation time pairing of EUI of internal to a non-ICD-defined MAC addr. 3. Changed date/time format from epoch to discrete bytes, UTC-referenced. 4. Added NADA message and procedure for network discovery and option for HNAD and NAD message waiting broadcast 5. Removed embedded ACK in log data records. 6. Send Log Command is now the only one without an ACK from CM. 7. Timeout for retransmission changed to 2 seconds 8. Message Type is relevant only for security-related device types in the MH 9. Added CSD device type 10. "UTC is invalid" status bit added 11. Container ID is 16 bytes; Coding of 11 byte ISO ID as a sub-type is new 12. Added section defining time as UTC and coding thereof 13. Changed format of event log records 14. Added Message Ladder Diagrams 15. Defined that Device Status is a required response to every DC/HNAD command except (1) Send Log and (2) ACK. Details given.
03 Nov 09	6.5 Draft	1 (0x01)	1. Removed Security and Encryption Discussion from Section 7 and referenced New ACSD Security and Encryption Document. 2. Removed section 8.1 Discussion on add-on sensor wired data bus. Wired

			data bus no longer allowed. 3. Added two new references in Section 2. 4. Changed Section 6.1.2.1 to allow execution of HNAD commands while in PAN or Cell coverage. 5. Added verbiage to clarify Section 6.2.2 is not referring to status message originating from DC. 6. Changed Section 6.3.2 to specify the 2 second timeout period commences following command execution to accommodate commands that take more than 2 seconds to execute. 7. Changed Section 6.3.4 to clarify last sentence indicated that when the DC/HNAD exhausts its ACK retries, it records the ACK failure in the DC/HNAD log or database. 8. Corrected Figure 6-4 to clarify the UID is of the on-container device. 9. Added verbiage to Section 6.8.1 to allow stationary ACSD/CSDs to ignore persistent NADAs for periods up to 2 seconds. 10. Added Paragraph 4.1.4.1 to clarify use of PAN IDs 11. Major re-write to old paragraph 4.1.4.1 - 4.1.4.2 (now para 4.1.4.2 to 4.1.4.3) – removed unneeded verbiage and aligned with August Demo work. 12. Added text under 4.1.6 for clarification and removed section on Beacon networks since not required by this ICD. 13. Deleted section 1.6.1.4.1.on Wired sensor bus with associated picture. 14. Rewrote old NADA broadcast para 4.1.7 and renumber to 4.1.6.1 15. Added clarification and deleted unneeded discussion in para 4.1.8 16. Para 6.6.3 set TBD value to 10 minutes 17. Corrected Ladder diagram in section 6.8.2 (added NAD to cm ACK) 18. Corrected Verbiage in section 6.8.4 19. Section 5.1.5 added verbiage and example for external CM packet. 20. Added two new device types to Table 6-1 21. Removed Vendor bytes from status message to align with Requirements doc. 22. Added table in section 7 for two new security and encryption related device types. These device types cannot be used in the MH. 23. Added sections 6.7.6 and 6.7.7 for handling garbled application layer ACKs. 24. Added comment on status transmission and retries in section 6.1
14 Jan 2010	V7.0	1 (0x01)	25. Added RF path on figure 1-4 from internal CM to Fixed Reader 26. Significant changes to Figure 4-3 for clarification 27. Deleted an unnecessary line in section 4.1.6.3 28. Inserted New Section 5.1.5.4 on External CM Rendezvous 29. Extensive re-write to Section 8 , Add-on Sensors 30. Added clarification of Section 4.1.1i. 31. Changed references to locking seals (LS) to Electronic Chain of Custody Device and added Reference [11]. 32. Changed section 1.6.2.2 to clarify that handhelds talk directly to CM whether in NAD coverage or not. 33. Section 4.1.4.1 changed to clarify comment only applies to status messages 34. Section 4.1.5.1 changed to explicitly allow all short broadcast addresses supported by ’15.4-2006. 35. Section 4.1.7 was changed to clarify response time not to exceed 2 secs in clear channel conditions. 36. Section 6.1.2.1 was changed to explicitly state that all received authorized

			commands shall be executed by ACSD/CSD/ECoC. 37. Section 6.5.4.8 was changed to clarify that UID must function as Device network address. 38. Section 6.8.1 was extensively re-written to correct timing misconception for listening and transmit duty cycles for both NADs and On-container devices. 39. Figure 6-5 and 6-6 were changed to remove unrestricted error byte section and include in error byte In restricted section of payload 40. Added section 6.6-2 to create a separate unrestricted error message using error byte as before. 41. Changed Figure 6-4 to show that UID is of sending (originating) device over the wireless portion of the link. 42. Added two device types to Table 6-1 (DC and KMF) and removed Table 7-1 43. Removed unencrypted bytes for log message and moved them into encrypted section. Removed redundant status field in Figure 6-10. 44. Figure 4-3 was changed to include DC UID and HNAD UID in NADA payload. 45. Modified Table 6-2 to reserve message type codes for key management described in Reference [9]. Removed Change key command from table 6-12. 46. Removed section on Vendor-specific data in encrypted payload. No co-mingling of commercial data allowed. 47. Noted in document figures that value 0x00 cannot be used for ICD version number or message type. 48. Added key message format figure 7-1 in section 49. Section 3.2.6 was changed to reflect the UID in the MH is always the sending device. 50. Added Clarification of NADA intervals in Section 4.1.6 51. Removed Encryption Pad Field in Figures 6-3, 6-5, 6-10 and 6-12. 52. Re-wrote Section 6.5.4.9 on message ascension numbers to align with new Reference [9]. 53. Added discussion in Section 7.3 on rekey counters (message ascension for rekey command). 54. Update sheet #1 changes implemented 55. Post-update sheet 1 changes added here
30 August 2010	V7.2	2 (0x02)	56. FY10 Deliverable Updates
19 Nov 2010	V8.0	2 (0x02)	57. FY10 Final – Document reformat and changes per meeting 16 Nov-19 Nov.

Table of Contents

List of Figures

List of Tables

1 Introduction

This Department of Homeland Security (DHS) Interface Control Document (ICD) provides the requirements for wireless communication between on-conveyance Communication Modules (CMs) in the functional sense and Network Access Devices (NADs). A CM is the communication element for several types of device, including Container Security Devices (CSDs), Advanced Container Security Devices (ACSDs), Electronic Chain of Custody (ECoC) Devices, and External Communication Modules (ECMs). In addition, this ICD provides the communications requirements for Add-on Sensors (AoSs), which communicate only with ACSDs or CSDs. For the purposes of this ICD, a *conveyance* is an ISO 668 Dry Shipping Container, motor carrier trailer, or comparable rail enclosure.

The intent of this ICD is to enable utilization of common hardware for message exchanges between all on-conveyance devices and Data Consolidation Points (DCPs), for both commercial messages and security-related messages. This document specifies in detail the communication protocols and network architecture needed to design the interfaces among all devices mentioned in the preceding paragraph. The technical specifications herein are non-proprietary and are intended to enable devices capable of global interoperation.

All devices mentioned above are components of the DHS-mandated Security Device System, which may include battery-operated, conveyance-mounted Security Devices [1], NADs [2], ECoC Devices [11], ECMs, AoSs, network data interfaces, and DHS-designated DCPs. Overviews of the Security Device System appear in Figure 3-1 and Figure 3-2. The primary purpose of the Security Device System is to monitor the doors of a conveyance for opening or removal while in transit from the Point of Stuffing (POS) through a Container Security Initiative (CSI) port to a Port of Arrival (PoA), and finally to a U.S. Point of Deconsolidation (PoDC). The Advanced CSD (ACSD) also monitors the sides, top, bottom, and doors of the conveyance for all types of intrusion, including penetration. Add-on Sensors (AoSs) allow additional functionality.

An operational *Security Device* is either a CSD or an ACSD, including Hybrid Composite Containers (HCCs), a specific ACSD implementation. Requirements in this ICD are intended to be exactly equivalent for CSDs and ACSDs. CSDs may be deployed with or without the HCC and are intended to interoperate seamlessly with ACSDs as components of a deployed Security Device System. In the remainder of this document, unless otherwise noted, the term “Security Device” is used to mean either a CSD or an ACSD.

Network Access Devices (NADs, a.k.a. “readers”) include both fixed and handheld devices. *Data Consolidation Points* (DCPs), with which Security Devices communicate, must interoperate with Security Device System elements defined herein, but the structure of networks surrounding the DCPs and how these are arranged internationally is outside the scope of this document.

Requirements for Security Devices appear in [1], which includes an overview of the Concept of Operations for the entire Security Device System and specific functional, performance, operational, environmental, and communications requirements governing the Security Device System. Interface requirements for Security Device System components are specified in two Interface Control Documents (ICDs), this document and [3], and the NAD-to-DCP ICD. Requirements for Security Device System encryption and secure operation are specified in [4]. These documents are intended to ensure global interoperability among all Security Device System components in addition to specifying the acceptable standards of performance. Table 1-1 is an overview of System interface elements and documentation.

Table 1-1, Security Device System Terms

Security Device Network Term	Addressed in this Document	Trusted Network Item	Description (in the context of this document)
ACSD	X	X	Advanced Container Security Device. Senses, logs and reports security related events per Security Device Requirements [1]
Key Management Facility		X	Entity that provides the cryptographic keys needed for Security Device System authentication and en/decryption discussed herein. Described fully in [4].
DCP		X	Data Consolidation Point. In general, DCPs are data portals that pass secure messages between Security Device System elements. At least one DCP will be designated by DHS to be the generic end-point for Security Device-originated messages and DCP responses. This DHS-designated DCP must be trusted and able to en/decrypt and authenticate.
IEEE			Institute of Electrical and Electronics Engineers (standards)
IEEE 802.15.4-2006	X		IEEE standard for MAC and PHY, without battery-powered mesh routing as in 802.15.5
IEEE 802.15.5			(2009) IEEE standard for much of a mesh network layer used with the IEEE 802.15.4-2006 MAC and PHY layer standards
LAN			Local Area Network. Typically privately owned for specific users
ECoC Device	X	X	Electronic Chain-of-Custody Device. Communicates the same as a Security Device but uses different sensors. Used for Chain of Custody applications and is not a stand-alone Security Device.
Network Topology	X		Herein, the network characteristic topology is per IEEE 802.15.5 used with 802.15.4-2006. The topology is peer to peer, no PAN coordinator, with certain nodes defined as gateways to WANs.
MAC Protocol	X		Medium Access Control (network) Layer. Herein, refers to a portion of the low-level protocols for wireless network between a Network Access Device (NAD) and a Security Device or another NAD
Mutual Authentication	X	X	Precludes rogue or stolen communicating entities. A standards-based means for network end-point entities to validate a peer entity. May use stored or derived encryption keys protected from theft and issued by a trusted third-party system. Distribution of Security Device System encryption keys is managed by a process defined in [4].
NAD (Secure)	X	X	Network Access Device. Can be fixed (FNAD) or portable hand-held (HNAD). Communicates with CMs via wireless RF and the DCP via Internet or, alternatively, Cellular or Satellite networks.
NAD (Non-secure)	X		Network Access Device. Can be fixed (FNAD) or portable hand-held (HNAD). Communicates with CMs via wireless RF and the DCP via Internet or, alternatively, Cellular or Satellite networks.
NWK	X		Network Layer Protocol, superior to MAC and PHY.
PHY	X		Physical protocol layer, i.e., modulated RF signal herein
CM	X	X	Communications Module. An element of a Security Device, an ECoC Device, and an External Communications Module. Must support IEEE 802.15.4-2006.
WAN			Wide Area Network. The Internet, Cellular network, or Satellite network.

2 Background

The Container Security Initiative (CSI), announced in January 2002, mandates that containers bound for the U.S. posing a potential risk to national security need to be examined at foreign ports. CSI consists of four key elements: (1) using intelligence and automated information to identify and target containers that pose a risk, (2) pre-screening those containers that pose a risk at the port of departure before they arrive at U.S. ports, (3) using detection technology to quickly pre-screen containers that pose a risk, and (4) using smarter, tamper-evident containers. The Department of Homeland Security (DHS) has determined that tracking and monitoring the security of intermodal container shipments are necessary to provide the required level of security information to both industry and government agencies to safeguard our borders.

The security of the global supply chain is one of the DHS's highest priorities. The ability to secure the integrity of a container as it moves through the global supply chain is vital to our nation's security. During the last ten years, private industry and government agencies have investigated ways to improve security in the global supply chain in an effort to protect against criminal activity and terrorist attacks. This has included development of improved mechanical and electronic container seal technology, sensor systems, and inspection agreements/processes to identify and monitor cargo movement at major ports and transit points throughout the world. In anticipation of new U.S. Government policies on enhanced security requirements for all U.S.-bound cargo, various government and industry teams have been investigating ways to adapt existing technologies and processes to provide monitoring of containers from the POS to the PODC. The use of Security Device Systems in the global supply chain is one component of an improved security system.

The goal of the DHS S&T cargo security program is to provide requirements and open standards for Security Device Systems and components thereof that will enable commercial competition and global interoperability for international container security. DHS recognizes that the security requirements for container shipment must take into consideration technology, people, and procedures. Any commercial vendor developing container security technologies must consider impacts to existing commercial and economic global supply chain operations in considering their design choices. This document formalizes the requirements for Security Devices consistent with DHS's security needs and operations in the context of shipping operations.

Systems currently under development by the Department of Homeland Security include the Container Security Device (CSD), the Advanced Container Security Device (ACSD), the Hybrid Composite Container (HCC), and the Marine Asset Tag Tracking System (MATTS). Among the goals of these programs are to characterize movement and status of cargo containers and to develop technologies to detect door openings and intrusions. The ACSD, CSD, HCC and MATTS programs are run by DHS Science and Technology (S&T) Directorate with the goal of deploy technologies to monitor all six sides (including both doors) of an ISO 688 Dry Shipping Container for intrusion while in storage and in transit. The Security Device System as envisioned further utilizes a layered security concept to provide maximum automated cargo security functions supporting container shipping from the Point of Stuffing (POS) through the Point of De-consolidation (POD) in the United States.

3 Scope

This ICD describes in detail the protocols necessary to satisfy the communication requirements of a Security Device System, including the functionality required within each layer and its applicability within the context of the Security Device-to-NAD interface. This document also covers requirements related to data interchanges that occur at the Application Layer, including data and message formatting and command constructs. Reference [4] addresses data security, encryption, and key management in detail. The remainder of this section discusses commingling of commercial and security data, document precedence, and applicable communication regulations, and provides a Security Device System overview.

3.1 Commercial versus Security Messaging

The intent of this ICD is to enable utilization of common hardware for message exchanges for both proprietary, commercial messages and security-related messages. Security-related messages are defined in detail in this ICD to ensure complete interoperability. Commercial message traffic may use the same hardware and lower level (MAC and PHY) protocols/firmware. When operating on the same RF channel and network ID (PAN ID), such commercial traffic may use this ICD's message header to segregate traffic in a coordinated manner. Otherwise, commercial traffic should be conducted on other channels and/or PAN IDs.

Commercial content **Shall Not** be placed into security-purposed messages defined herein during either storage or transport (See [1] for all security-purposed data requirements). Commercial message encryption and authentication **May** be proprietary. Commercial messages **May** be transported by the Security Device System to the desired commercial address. The DCP **Shall** ignore commercial messaging addressed to it. Battery power usage for commercial-purposed messaging **Shall Not** violate on-conveyance power availability requirements for security-purposed messaging (Section 7.2 of [1]).

Commercial-purposed messages are defined as any of the following:

1. **ICD-Coordinated:** *ICD-Coordinated* messages comply with Section 9.4.3, which specifies the first 16 bytes of the payload section of every ICD-compliant data packet.
2. **ICD-Uncoordinated, same network ID**: Messages outside the scope of this ICD (i.e., without the message header defined herein) **May** be transmitted by Security System Devices at the discretion of the implementer, but **Shall Not** be processed as security-purposed messages or transported by the Security Device System.
3. **ICD-Uncoordinated, different network ID**: ICD-Uncoordinated messages not processed as security-purpose messages and **May** be transmitted by an IEEE 802.15.4-2006 wireless network (e.g., the network identified by the PAN ID) not defined as security-purposed in this ICD. Commercial content and security thereof is not defined in this ICD. Such messages can be transported by elements of the Security Device System at the implementer's discretion provided such transport has no impact on security-purposed data.

3.2 Document Precedence and Nomenclature

This document addresses the requirements specific to the structure used for data and command transmittal for bi-directional communications between Security Devices and the Security Device System. In the event of conflicts between this document and other related Security Device System documents, this document has precedence with respect to the areas described in Section

3 above. IEEE 802.15.4-2006 [5] is the basis for forming the RF protocols described herein. Unless otherwise specified, [1] should be used for definitions of terms.

3.3 Regulatory Requirements

Within the United States, FCC 47 CFR Part 15.247 rules **Shall** apply and take precedence. Wireless devices utilizing interfaces defined herein (CSD, ACSD, ECM, NAD, and ECoC Device) must be approved by the host nation for operation in that locale (e.g., type-certified by the FCC under Part 15 in the United States) and likewise authorized for use in all relevant locales, worldwide.

A key consideration of this compliance is the variability of international regulations, compliance with which requires accommodating broad variations in permitted RF radiated power, antenna gain, and mandated spectral power masking. Requirements in this document are intended to meet the most restrictive regulations.

The choice of 2.4GHz addresses this regulatory issue by using internationally available unlicensed spectrum. The regulatory limits on transmitted power (inclusive of antenna gain) vary internationally by an order of magnitude. Based on the requirement to operate world-wide, transmitted power specified in this ICD is no greater than the lowest transmitted power allowed by any regulation and therefore meets all international regulations.

NOTE: To facilitate interoperability at the RF link budget level, the *minimum* effective (i.e., external to the container) radiated power is also specified in this ICD for Security Device System devices that communicate with infrastructure or peers.

3.4 Security Device System Overview

The wireless pathway from a Security Device to a DCP may include bi-directional wireless interfaces between sensors mounted inside the container, ECoC Devices, Communication Modules (CMs), Security Devices, and NADs. These pathways may also include a combination of cellular, satellite and Wireless Personal Area Networks (WPANs) based on IEEE 802.15.4-2006. The communication links for WPANs are fully described herein, including the structures of messages coming from the Security Devices and commands going to them. Communication links for cellular and satellite modes are treated as embedded WANs and are covered in [3].

The intent of this document is to establish an unambiguous specification for Security Device System message types, sequences, content, and security in such a way that interoperability is assured worldwide between any DCP and any manufacturer’s Security Device, irrespective of the end-to-end communications media. Commercial-purposed messages may be transported by this same network and **Shall** use the reserved message header code described herein. The remaining message content for non-security-related messages is outside the scope of this ICD.

The network specified herein enables communications in a variety of settings including:

1) Single and multi-lane portals (in- and out-gates)
2) Loading docks and tarmacs
3) Throughout all or portions of an intermodal container terminal
4) Among RF-linked rail cars en route
5) Container-to-tractor trucking en route
6) On-conveyance handling equipment

Figure 3-1 is a network topology-level view of facility-wide wireless coverage and connectivity with remote Data Consolidation Points.

Moving nodes include communications devices in or on conveyances and conveyance-handling devices. Fixed NADs (FNADs) are stationary nodes that may be pole- or roof-mounted, some of which are egress points that bridge data to/from other networks that reach the DCP.

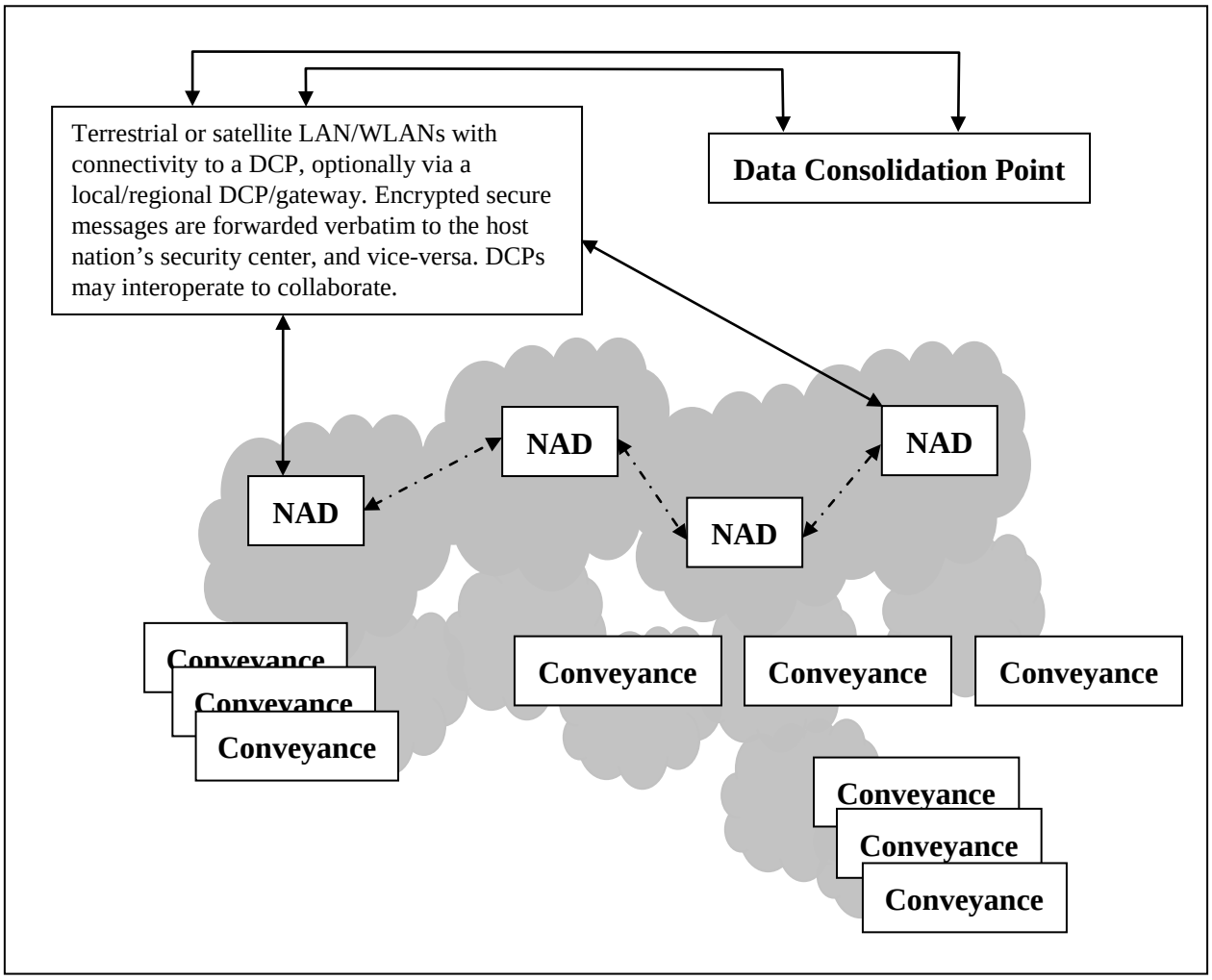


Figure 3-1, Network Topology Example: Dispersed Conveyances (at gate or in storage)

Network Access Devices (NADs) provide (1) small-area (e.g., loading dock) and (2) wide-area (e.g., storage yard) connectivity to a distant Data Consolidation Point (DCP).

This arrangement applies to access within a yard area, in a multi-lane portal, or at a loading dock, varying in scale. Some NADs may be wired bridges to a second network to begin the trip to/from a DCP. Where data wiring is impractical, other NADs may be wireless bridges and use neighboring NADs for DCP connectivity. These NADs also prevent "stranded" conveyances with no route to a DCP. The coverage radius of a given NAD will be constrained by buildings, conveyances, and antenna selection. Figure 3-2 depicts the network elements to which this ICD applies.

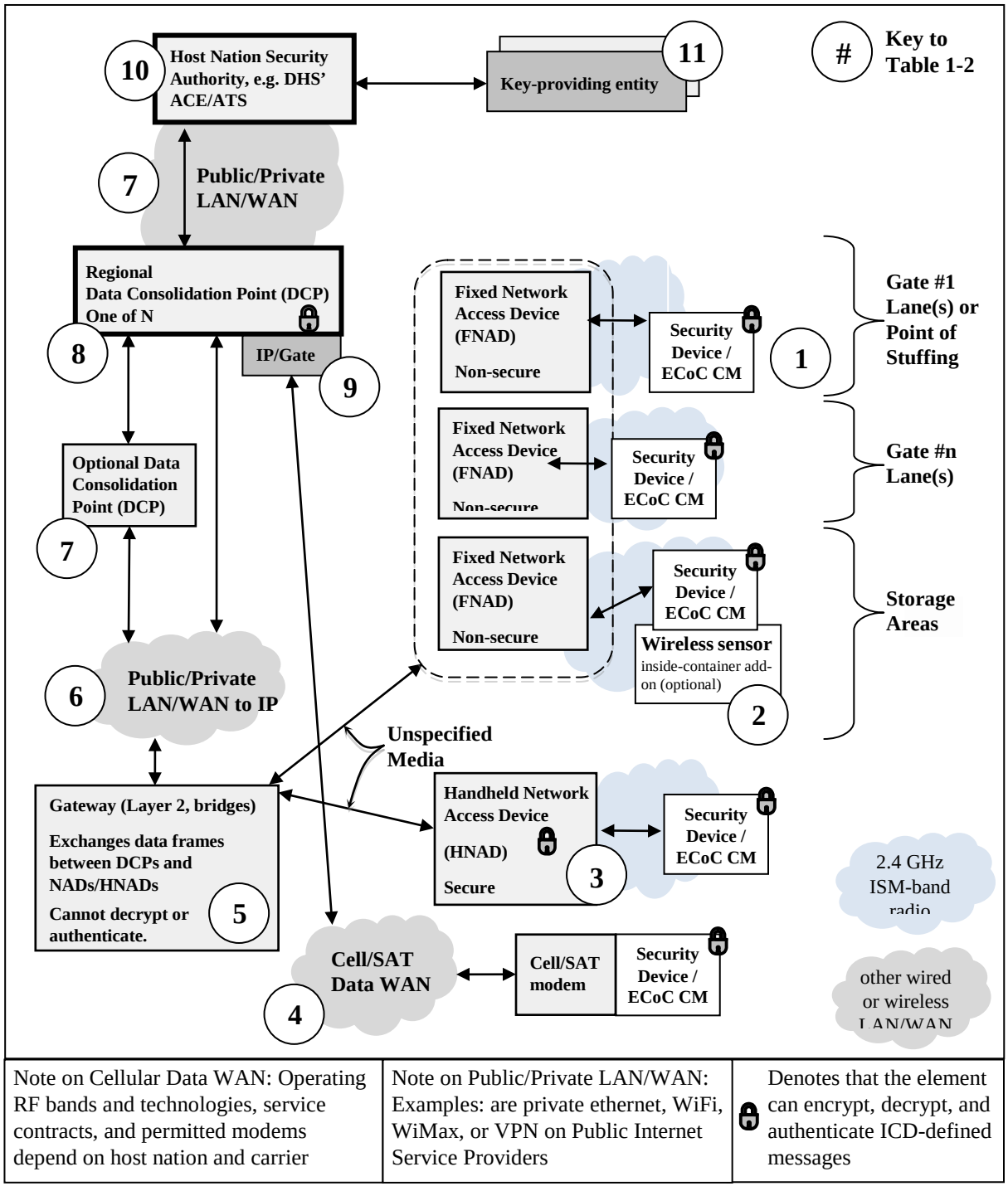


Figure 3-2, Security Device System Overview

The numbered circles in Figure 3-2 refer to Table 3-1 below. The LAN/WAN and cellular networks shown use Internet Protocol (IP) at their interface to the DCP. Security message content is the same for LAN/WAN, Cellular and 802.15.4-2006 so the nature of the many transport networks is irrelevant to the DCP message in/out processing.

Table 3-1, Network Element Descriptions

Key	Topic	Summary Description
1	**Conveyance-to-NAD Communications via Communications Module (CM)**	Low-power bi-directional unlicensed band wireless data per IEEE 802.15.4-2006. A NAD provides wireless coverage of on-conveyance devices and exchanges message data with DCPs via local and wide area networks (LAN/WAN), the message content of which is specified in this ICD. The DCPs may reformat per DCP Requirements.
2	**Wireless Sensor Inside Conveyance**	Wireless sensors are considered part of the Security Device/ECoC sensor management. The wireless sensor bus is a Security Device requirement. The protocol for the wireless sensor interface and data transfer is defined in this ICD.
3	**Secure NAD**	The secure NAD is a NAD that also emulates a subset of DCP functions. Mutual authentication between the secure NAD and the Security Device or ECoC, if required, is performed using key management procedures detailed in [4]. Some NADs can issue a subset of commands that do not require authentication as non-secure NADs; see [2] for details.
4	**Cellular/Satellite Access Network**	On-conveyance devices must use the wireless mechanism in [1] and may use cellular or other public carrier wireless as optional secondary modes. Message exchanges with the DCPs are detailed in [3]. Security is detailed in [4].
5	**Gateway**	NADs connect to gateway controllers using an unspecified medium, e.g., WiFi, LAN, Ethernet, RS232, or RS485. The gateway is intended to be transparent, copying message content verbatim between the wireless and secondary media. No security measures are required, as security is provided by the message content. This ICD defines messaging in such a way that messages can be sent using either a connectionless protocol such as UDP or simply as serial data with a fast timeout for end-of-message. The gateway controller is responsible for sending DCP (item 8) messages to the originating Security Device via the last-used NAD.
6	**Public/Private LAN/WAN**	Transport media used by the gateway (item 5) to exchange data directly with its designated DCP (item 8) or with an intermediate DCP (item 7). Refer to [13], DCP-to-NAD ICD, for specifics on the use of IP as the interface to such WANs.
7	**Optional Data Consolidation Point (DCP)**	Optional DCPs that cannot encrypt or decrypt may be utilized for commercial purposes. Such untrusted DCPs should retransmit security-purposed messages *verbatim* between Security Device System components.
8	**Trusted Data Consolidation Point (DCP)**	Encryption key possession enables communication with on-conveyance devices for security purposes. The trusted DCP consolidates security-related messages for the Security Authority (item 10). The method of this communication is not specified in this ICD.
9	**Cellular/Satellite Gateway(s)**	ICD messages exchanged with an on-conveyance device and its DHS-designated Trusted DCP (item 8) flow through a gateway determined by the cellular or satellite service provider. The transport layer protocol is not described in this ICD.
10	**Host Nation Security Authority System**	In the US, this may be DHS' Automated Commercial Environment/Automated Targeting System (ACE/ATS). The interface between the DCP and this item is not defined in this ICD. Note that only the Security Authority can provide authority to decrypt secure messages defined in this ICD. Commercial-purposed messages may be encrypted to suit by optional DCPs (item 7).
11	**Key-providing entity- Key Management Facility (KMF)**	Trusted third party issues digital encryption keys stored in and used by on-conveyance devices (item 1), secure NADs (item 3), and Trusted DCPs (item 8) for authentication, encryption/decryption, and other purposes. Key management methods are defined in [4].

3.4.1 Primary Wireless Medium, Summary

The primary wireless medium for all devices is summarized as follows and detailed in the remainder of this ICD:

1) 2.4GHz band and power per the least common denominator among regulatory domains,
2) IEEE 802.15.4 MAC/PHY strictly per the Standard,
3) Peer-to-peer topology, no PAN coordinator, no beacons, no Time Division Multiple Access (TDMA)/Guaranteed Time Slots (GTS),
4) Emphasis on assured interoperability among ICD-compliant client and access devices,
5) Data frame addresses are 64-bit IEEE MAC addresses; no network layer addresses,
6) Addresses of fixed, handheld and on-conveyance devices are discovered per this ICD,
7) Battery conservation "low power state" enabled per ICD's Message Waiting indicator,
8) Optional use of relay/repeaters,
9) End-to-end message security provided by application layer encryption and authentication,
10) End-to-end message security does *not* utilize 802.15.4 MAC layer encryption, which is disabled,
11) ICD-defined messages enable conveyance devices to passively discover fixed and handheld network access (gateway) devices' MAC addresses.

3.4.2 On-Conveyance Devices

For the purposes of this ICD, a *conveyance* is an ISO 668 Dry Shipping Container, motor carrier trailer, or comparable rail enclosure.

3.4.2.1 Container Security Device (CSD) and Advanced CSD (ACSD)

A Security Device—either a CSD or an ACSD—is an internally mounted, battery-powered security component of the Security Device System that monitors the status of conveyance doors for opening and removal. The ACSD is also required to sense intrusion through all six sides (including the doors) of an ISO 688 dry container. The Security Device is also intended to provide interfaces for add-on sensors for both security and commercial purposes and communicate with Network Access Devices (NADs) outside the conveyance. The requirements for the interfaces between Security Devices, ECoCs, ECMs, Add-on Sensors (AoS), and NADs are specified in this ICD.

Data structures for messages from and commands to the Security Device are also specified herein. For security-purposed operations, these messages and commands include encrypted information, the encryption process for which is described in [4]. The primary Security Device requirements document is [1].

Every Security Device, ECoC, ECM and AoS **Shall** incorporate an embedded Communications Module (CM), as described in the following sections. Security Devices and CMs are intended to be employed in configurations consistent with those described in the remainder of Section 3.4.2.

3.4.2.2 Embedded Communications Module (CM)

The communicating component of every Security Device, ECoC , ECM and AoS is a CM. Such integral CMs are referred to herein as *embedded CMs.* Note that the distinction between an embedded CM and the device in which it is embedded May be logical; i.e., the two devices need not be physically distinct. As shown in Figure 3-2, an embedded CM communicates with a

nearby FNAD or HNAD, which communicates in turn, via relays and intermediate WPANs, with the DHS-designated, trusted DCP. The “ends” in this end-to-end communication are the embedded CM and the DCP.

The CM is a battery-powered device that **Shall** provide wireless connectivity in the 2.4 GHz ISM-band as specified herein as its primary communication mode. In the Security Device System, a CM will always be embedded in a Security Device, ECoC, ECM or AoS.

3.4.2.3 External Communications Module (ECM)

An ECM will have one of three configurations based on its functions:

1) Relay for Paired Device Only
2) Location and Tracking Only
3) Both of the Above

Given international constraints on radiated emissions, it is likely that a Security Device mounted inside a conveyance will sometimes fail to meet range requirements in primary communication mode (i.e., IEEE 802.15.4-2006 wireless connectivity). Policies that restrict altering conveyances and the need for rapid Security Device installation and removal preclude modifying the conveyance in order to use an external antenna. An externally mounted “relay” device is an option to meet certain extended range requirements. This section defines such a device, which is referred to as the *External Communications Module (ECM).*

The ECM provides Global Positioning System (GPS) functionality and may have the means to use cellular, satellite, or other wireless alternatives. This ICD defines messaging supporting these options. If implemented, Security Device System elements using these media as a transport layer service **Shall** support verbatim exchange of messages, payload encryption, and application-layer ACK protocols defined in this ICD, [4], and [11] to simplify the Data Consolidation Point (DCP) interface with a variety of communications media.

The ECM **Shall** interoperate with all Security Devices that comply with this ICD, even if they are produced by different manufacturers. To enable this interoperation, this section defines the standards for communication between the ECM and the Security Device’s embedded CM.

The Security Device may communicate directly with a NAD if propagation conditions permit. If not, the Security Device **Shall** attempt to communicate via an ECM if one is present. The decision to use an ECM should be based on the availability of NAD connections and the Security Device power management scheme.

Per [10], the ECM is small enough to be installed on a conveyance in such a way that it does not protrude from the profile of the conveyance, which would make it vulnerable to damage. The ECM will notify the primary user of its removal from its conveyance and, if GPS-equipped, its last known location. This can be accomplished using a mechanism that activates when the device loses physical contact with the conveyance or some other unspecified means.

3.4.2.4 Electronic Chain of Custody (ECoC) Device

The ECoC, defined by [11], is a battery-powered mechanical locking device that has a minimum of two wireless communications modes - one providing connectivity in the 2.4 GHz ISM-band and the other using existing cellular networks. The ECoC **May** incorporate additional communications modes, including satellite communications, as long as they meet the requirements of [11] and do not interfere with the primary RF and secondary cellular mode.

The ECoC is designed to be mounted external to the door(s) of a conveyance, incorporate GPS functions, and provide an interactive display to enable and view the lock status (see [11] for all ECoC requirements). The ECoC is treated herein as having communication functionality identical to that of an ECM, particularly with respect to using IEEE 802.15.4-2006 protocols.

3.4.2.5 Wireless Add-on Sensor

The Security Device **Shall** accommodate wireless sensors using IEEE 802.15.4-2006 protocols as described herein for use by Add-on Sensors (AoS). All AoS except HCC panels **Shall** use only this wireless accommodation for security-purposed communication. A wired add-on sensor bus **Shall Not** be used.

AoSs can be installed and utilize the wireless IEEE 802.15.4-2006 link to provide additional security functions, such as embedded sensors for Hybrid Composite Container (HCC) Breach Security Devices (BSDs). The AoS wireless interface **May** also carry commercial-purposed information such as temperature, cargo status, or inventory management. All security-purposed data and commands passing wirelessly between an AoS and a Security Device **Shall** be encrypted per [4].

3.4.3 Network Access Device (NAD)

A Network Access Device (NAD) is any appropriate mix of hardware, software, network services, and internal interfaces that satisfies the requirements specified for the WPAN, including functionality, user interface, and error detection/correction. NADs have multiple physical configurations to support fixed installations, arming operations, backhaul communications, and mobile inspection activities.

CMs and DCPs **Shall** exchange information via intervening NADs using the messages defined in this ICD. A NAD **Shall** retransmit verbatim all wireless data traffic between CMs and DCPs. This ICD defines the message content and the application-level messaging between CMs and NADs. The wireless link between CMs and NADs is first of several network legs in the transport path. Other wireless and wired networks, which **May** be used as required to complete the eventual end-to-end path between CM and DCP, are regarded as “untrusted”. The data transport mechanism between NADs and DCPs is described in [3].

A NAD may be fixed or handheld. Handheld NADs are mobile by definition. The descriptors *FNAD* (Fixed NAD) and *HNAD* (Handheld NAD) are used herein to enable differentiation between Fixed and Handheld NADs, while the term “NAD” encompasses all potential wireless interfaces to the Security Device System consistent with [1]. The following sections describe the general properties of these devices.

3.4.3.1 Fixed Network Access Device (FNAD)

The functional requirements for FNADs appear in [2]. In this ICD revision, it is assumed that FNADs can be considered either *secure* (trusted) or *non-secure* (untrusted). FNADs are intended to be permanently installed units located near the relevant trade lanes, e.g., at the Point of Stuffing (PoS), the DHS-designated Intermediate Transit Points (ITPs), and/or the U.S. Point of Deconsolidation (PoDC). Potential FNAD installation sites include loading docks, facility in/out gates, light poles, and rooftops. An FNAD could be in the locomotive of a train, bridging to satellite. As such, the preferred implementation of an FNAD is as a non-secure network element providing IP connectivity to the DCP such that communication can occur in real time, per [1].

Security Devices, ECoC Devices, and ECMs that are within an FNAD's wireless coverage **Shall** attempt to exchange security-purposed messages with the DCP with which the FNAD is associated. The non-secure FNAD is incapable of decryption and is considered a non-secure unattended network "bridge" element. A non-secure FNAD is *not* a trusted device with respect to network security and information assurance.

Though not specified in this document, NAD-to-DCP data is merely the unmodified message packets defined herein. For non-secure FNADs, no decryption is done until message receipt at either end of the transmission path (i.e., at the DCP or at the CM). This property—encryption/decryption only at application-layer end points—permits all intervening networks used for security-purposed messaging to be untrusted. Commercial-purposed messages **May** use other policies.

3.4.3.2 Handheld Network Access Device (HNAD)

Functional requirements for the HNAD appear in [2]. In this ICD revision, it is assumed that HNADs can be *secure* (trusted), *non-secure* (untrusted) or *arming-only* (untrusted) as described in [2]. Secure HNADs Shall be capable of functionality—at a high level, issuing restricted commands and receiving secure data—enabled by access to cryptographic keys from a key-providing entity, as discussed herein (see, e.g., Figure 3-2) and defined in [4]. A non-secure HNAD **Shall** be capable of executing unrestricted message exchanges as defined in this ICD. The key-providing entity, per [4], will not provide encryption keys to a non-secure HNAD, which is therefore incapable of encrypted message exchanges per this ICD. The arming-only HNAD has a device-type that only allows limited access to execute a subset of restricted commands. All HNADs communicate with the Security Device CM directly. The secure and arming-only HNADs communicate to the DCP over an IP connection via a cradle or equivalent connection. The secure HNAD is assumed to be fully controlled by a DHS-designated Trusted Agent and **Shall** functionally support a subset of the DCP-originated messages exchanged between a Security Device and a DCP. Therefore, a secure HNAD must have the credentials to decrypt and encrypt after mutual authentication between itself and the device. The secure HNAD must implement a subset of DCP message commands, responses, authentication, encryption, and decryption.

3.4.3.3 Commercial Cellular WAN

Embedded subsystems or components providing WAN/IP connectivity to DCPs are referred to as Embedded NADs. NAD-to-DCP transport requirements for Embedded NADs are defined in [3].

An embedded secondary communications mode that Security Devices (via ECoC/ECMs) can use for backhaul and emergency notification is commercial cellular data service. Embedded cellular data service is considered herein to provide the same functionality as the cellular data service provided by a NAD, so this ICD does not separately define communication between the Security Device and the cellular subsystem. This ICD requires only that security-purposed data payloads be exchanged between Security Devices and the DCP in such a way that the use of any WAN is transparent to both end points. One option enabled by this ICD and discussed further in [3] is to use User Datagram Protocol (UDP) datagrams containing the payload data defined herein for security-purposed messages. Security for security-purposed data is defined at the application layer by this ICD and [4].

When the cellular communications mode is utilized, ECoC/ECMs **Shall** be capable of transmitting an emergency notification of an unauthorized removal, along with its location (ECoC/ECMs are required to have GPS; Security Devices are not). The device **Shall** continuously send this message out at a regular interval not to exceed 30 minutes until either the message is successfully acknowledged by an authorized user or the ECoC/ECM device power is fully depleted.

3.4.3.4 Commercial Satellite WAN

Satellite communication service **Shall** be treated as an embedded NAD, with communication functions as described above for cellular and defined in [3].

3.4.3.5 Conveyance Direct-To-WAN

ECoC/ECMs **May** have alternative, non-WPAN communication mechanisms not specified in this document (recall that Security Devices are not required to use any specific communication mechanism other than their embedded CMs—802.15.4-2006-compliant radio communication modules—as specified herein).

The following recommendations apply to ECoC/ECMs:

1. To simplify interoperability with *any* Data Consolidation Point (DCP), ECoCs **Shall** use the message formats defined in Section 9.1. These messages are independent of transport media.
2. Messages defined herein are for use with small packets, as in 802.15.4-2006, and do not require fragmentation and reassembly in the transport networks. One payload data unit (PDU) can correspond to one data packet on 802.15.4-2006, satellite-based UDP, and cellular Short Message Service (SMS) or UDP. The transport protocol for cellular and satellite are defined in [3]. Message content and format, irrespective of the means of transport, **Shall** be as defined in Section 9.1
3. Such devices should implement this document's standard for interfaces to wireless sensors to permit standardized sensors.

3.4.4 Data Consolidation Point (DCP)

Trusted Data Consolidation Points (DCPs) exchange security-purposed messages with ACSD/CSD/ECoC and ECMs. Only trusted DCPs can generate and encrypt security-related (i.e., restricted) commands or decrypt the corresponding encrypted responses and other encrypted security-purposed Security Device System traffic. The encrypt/decrypt capability requires cryptographic keys provided by an entity functionally distinct from the DCP.

4 Security Device-to-NAD Communications Overview

This section is an overview of Security Device System communication modes and protocols intended to illustrate an implementation that accomplishes the required functionality.

4.1 Communications Modes

The primary means of communication for all Security Devices **Shall** be IEEE 802.15.4-2006 radios operating at 2.4 GHz. Cellular networks, satellite communications, and other media suitable for packet data as defined herein **May** be utilized as secondary communications modes. All transport networks, including such media, **May** utilize protocols not known to be trustworthy and **Shall** be considered untrusted. All Security Device System security-purposed messages **Shall** be encrypted per this ICD for transport across untrusted networks.

In all communication modes, data formatting and message content **Shall** be consistent in detail and **Shall** comply with this document. For interoperability when using IEEE 802.15.4-2006, this document's definitions of the 802.15.4-2006 MAC/PHY **Shall** be used for messages defined herein. Cellular and satellite communications media are not defined herein but are expected to transparently transport traffic between Security Devices/ECoC/ECMs and the trusted DCP.

4.2 End-to-End Messaging Principles

4.2.1 Session-less vs. Session-based Messaging

NAD-to-DCP communication specifics are defined in [3]; this section is a derived summary.

Communication defined herein between DCPs and Security Devices/ECoC/ECMs uses datagrams (e.g., UDP via IP), and the WPAN final link, though not IP-based, is also a datagram service. Persistent connections between the trusted DCP and every locale/NAD are therefore not required for this session-less method. The type, number, and security of the networks used to transmit the Security Device System messages defined herein are outside the scope of this document.

Every Security Device System message defined herein is short enough to be a single IP packet and a single data frame on 802.15.4-2006 media. Thus, to bridge networks when transporting the messages defined herein, the packet data payloads and header information of 802.15.4-2006 frames on one network are simply copied verbatim into 802.15.4-2006 frames on the other network. This is illustrated in Figure 4-1.

An alternative to session-less messaging (UDP) is connection-based, e.g., TCP. Although TCP may be utilized, in some DCP transports, TCP may be impractical due to security policy or WAN transport methods.

The wireless messaging defined in this document enables either session-less or connection based messaging. In either case, end-to-end error correction is defined by this ICD, irrespective of the transport network(s).

4.2.2 Fragmentation and Reassembly

Fragmentation and reassembly are not required. Message formats defined herein enable, with one exception, all status and command message data to fit within a single WPAN MAC-layer data frame's payload. The exception is the Event log download described in Section 9.5.8.3.

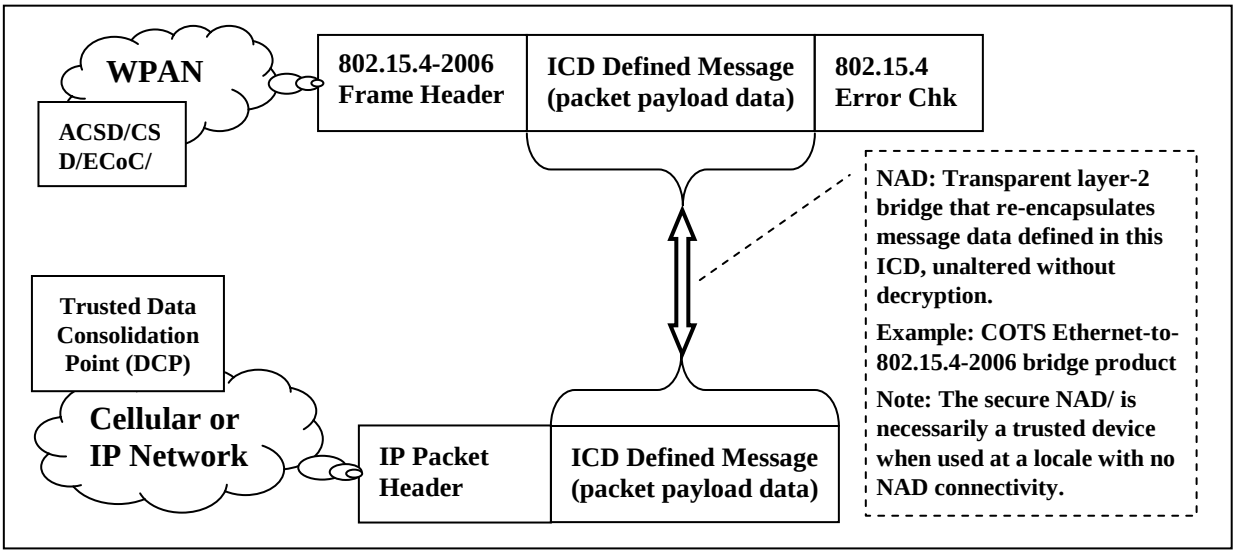


Figure 4-1, Illustration of End-to-End Message Transport

4.2.3 Error Correction

Error detection and correction processes are intended to mitigate bit errors, duplicated and lost messages, decryption faults, message integrity faults, and contextually invalid messages.

Application-layer error detection and correction is performed by the application protocol defined herein. The use of 802.15.4-2006 link-layer error correction (link-layer ACK) is also required. Link-layer ACK content and timing **Shall** be consistent with ACK content and timing described in [5]. Error correction is desired but not required in any other transport link on the end-to-end path between CM and DCP or secure NAD. This ICD defines bi-directional end-to-end application message ACK in Section 9.3

4.2.4 End-to-End Addressing and Mobility Management

The CM (within a Security Device/ECoC/ECM), for technical and practical reasons, cannot be directly assigned an IP address. The alternative, akin to that used in cell phone industry under TIA standards, is as follows.

1) A NAD forwards messages from a CM to a pre-defined DCP.
2) The DCP replies to this initial message via the same NAD, ideally before conveyance movement requires redirection to a different NAD; this is an implementation issue; e.g., local infrastructure will choose the NAD serving the destination CM. The destination CM Unique Identifier (UID) is identified from the status message header defined herein. The DCP has the capability to identify the last known serving NAD.
3) WAN/LAN devices (and non-secure NADs, in particular) can never decrypt security-purposed message content; trusted DCPS, secure NADs, and Security Devices that possess the appropriate encryption keys can.
4) The locale's infrastructure may translate network addresses to private LAN addresses, making the locale responsible for routing WAN messages to/from the correct NADs. The infrastructure in this case must comply with this ICD. This is not required if the NADs have public WAN address; the NADs can be generic devices and the infrastructure can ignore this ICD.

5) For outbound messages the DCP re-uses the last known destination locale NAD address for transmissions per methods not described in this document.

4.2.5 CM-to-DCP Addressing

NAD-to-DCP communication requirements are defined in [3]; this section is a derived summary.

The message formats in this document require the CM to pass the UID of its Security Device, ECoC or ECM in every transmitted message's data payload, in an unencrypted section. Upon arrival at a NAD, that data payload is removed from the 802.15.4-2006 payload and re-encapsulated in a protocol data unit appropriate to reach the DCP servicing the NAD.

4.2.6 DCP-to-CM Response Addressing

NAD-to-DCP communication requirements are defined in [3]; this section is a derived summary.

The message formats defined herein require that the DCP provide the UID of the destination CM to NADs en route to the CM. If the CM has moved and the DCP provides the wrong locale or NAD, the DCP will time-out waiting for message acknowledgement.

4.2.7 DCP-to-CM Unsolicited Ad-hoc Addressing

NAD-to-DCP communication requirements are defined in [3]; this section is a derived summary.

The DCP may send an unsolicited (ad-hoc) message such as status-inquiry to a Security Device or ECoC/ECM by addressing a message for a given CM to the NAD last used by that CM to contact the DCP. If the CM has moved into coverage of a different NAD in the same Personal Area Network (PAN) ID, the message will not be acknowledged by the CM and the DCP will timeout. DCP retries are discussed in [3].

4.2.8 External Relay Function

At time of installation of an ECoC/ECM, the Security Device (if present) **May** be programmed with the 802.15.4 MAC address of the ECoC/ECM (and vice-versa, i.e., the ECoC/ECM also programmed with the MAC address of the Security Device), providing network extension and additional functionality. This is referred to as *Pairing* and enables the ECoC/ECM to relay messages back and forth between the Security Device and a NAD, which also transmits the messages to and from a DCP.

The paired ECoC/ECM is likely to include GPS functionality (according to [10], ECoC/ECM Devices incorporate GPS capability) and **May** include cellular and satellite communications. Additionally the ECoC/ECM **May** be used to extend the wireless network using Ad-hoc/mesh functions described in Section 5.2.

In the paired configuration, the ECoC/ECM, as part of the Security Device System, **Shall** conduct network discovery as described in Section 5.1.6, and messages from the DCP intended for the paired Security Device **Shall** be forwarded by the ECoC/ECM to the specific paired Security Device address provided during the Pairing process. Messages forwarded to Security Devices by ECoC/ECMs, including status messages, commands and acknowledgements, **Shall Not** be altered by the ECoC/ECM.

The ECoC/ECM optionally stores and, on request, transmits Event Log Messages. Any ICD-Uncoordinated messages (described in Section 3.1) generated by the ECoC/ECM are considered commercial-purposed and are not within the scope of this ICD in content or format.

4.2.8.1 Device Network Discovery, ECoC/ECM

The ECoC/ECM **Shall** always conduct Network Discovery, whether acting as a relay or not, using the same procedure as the Security Device, i.e., by acquiring and responding to the NADA message sent by NADs. All devices in combination **Shall** meet the requirements of Section 5.1.7 for network discovery and response time.

4.2.8.2 Pairing the ECoC/ECM and the Security Device

At time of installation, the Security Device **Shall** be configured with the device UID/MAC address of the pairing ECoC/ECM (if implemented) using the method described in Section 11.1. The ECoC/ECM and the Security Device record one another's IEEE Standard 802.15.4-2006 MAC addresses using an HNAD. On completion of the Pairing command execution, the Security Device **Shall** transmit an unsolicited status message to the user's HNAD via the paired ECoC/ECM. On receipt of this message by the HNAD, successful pairing has been confirmed. Personnel or automation **Shall** confirm that the Security Device and the ECoC/ECM have established successful pair-wise communications per this ICD as the final step in the installation process.

Following pairing, the ECoC/ECM **Shall** forward all messages generated by the Security Device to the DCP via an FNAD when in coverage. The ECoC/ECM is required to respond to FNADs only when paired. The Security Device **Shall** detect ECoC/ECM-relayed NADA message(s) with a device type in the header of ECoC/ECM and from the specified MAC address for the paired ECoC/ECM. The Security Device **May** ignore FNAD NADA messages from other than the given MAC address of the paired ECoC/ECM so long as the paired devices in combination meet all network discovery requirements of Section 5.1.6 and Section 5.1.7 of this document. Throughout the remainder of the trip pairing, the ECoC/ECM **Shall** listen for incoming messages to its network address for no less than 20 milliseconds out of each second on average.

4.2.8.3 Message Bypass

The paired Security Device **Shall** periodically detect the presence of NADs per this ICD independent of an ECoC/ECM. The Security Device **May** choose to either:

1) route messages through the ECoC/ECM to FNADs as the default message path, or
2) route messages through the ECoC/ECM only when it detects no FNAD coverage.

The paired Security Device **Shall** respond to all HNAD NADAs without routing through the ECoC/ECM. If the paired ECoC/ECM is removed by accident or intent after pairing, the Security Device **Shall** be capable of detecting this within 2 minutes and **Shall** be capable of responding to and exchanging messages directly with all ICD-compliant NADs.

Receipt of the ICD-defined application layer ACK constitutes message delivery success under all paired conditions.

4.2.8.4 ECoC/ECM Relay, Messages to Data Consolidation Point

Messages from a Security Device via an ECoC/ECM to a NAD **Shall** be processed as follows.

When entering or changing NAD coverage selection:

1) All FNAD NADAs **Shall** be relayed by the ECoC/ECM as a unicast message to the paired Security Device until the initial Security Device response transmission.
2) All NADAs with Message Waiting for the paired Security Device UID **Shall** be relayed.

3) The Security Device **Shall** respond to the relayed NADA per this ICD using the MAC Address of the paired ECoC/ECM.
4) The ECoC/ECM **Shall** produce an 802.15.4 MAC layer ACK on receipt of the message.
5) The ECoC/ECM **Shall** forward the message to the coverage FNAD verbatim and take no further action.

If NAD coverage is lost during this process, the ECoC/ECM **May** attempt to send the message through alternative commercial modes such as cell or satellite if available. If no connectivity is available, the ECoC/ECM **Shall** take no further action. The Security Device will time-out waiting for an application layer ACK and take the appropriate action.

If the DCP does not receive the message, the Security Device will time-out waiting for an application layer ACK and take the appropriate action; the paired ECoC/ECM has no responsibility in error correction for relayed messages.

4.2.8.5 ECoC/ECM Relay, Messages from Data Consolidation Point

Messages from an FNAD to a Security Device via ECoC/ECM **Shall** be processed as follows:

1) For a FNAD message, the ECoC/ECM **Shall** transmit the message verbatim to the MAC address of the paired Security Device with appropriate MAC Layer acknowledgement.
2) The ECoC/ECM **Shall** take no further action beyond listening for a potential Security Device response.
3) The Security Device **Shall** process the message from the ECoC/ECM and take appropriate action in the execution of commands and response.

A paired ECoC/ECM **Shall** ignore messages from an HNAD.

4.2.8.6 Location and Tracking Function

The location and tracking functional requirements are described in [10].

5 Wireless Personal Area Network (WPAN) Description

The CM-to-NAD Wireless Personal Area Network (WPAN) is defined in this section. This includes definitions of the medium access layer (MAC), the physical/RF layer, and the required network topology support. The CM may be a stand-alone unit or a subsystem within a Security Device, ECoC or ECM.

The next sections describe the PAN topology required by this ICD version. Revisions of this ICD are identified in the Revision Code in the Control Table at the beginning of this document. The Revision Code is used in the message header illustrated in Figure 9-3. The current ICD Revision Code 2 per this document specifies Peer-to-Peer topology per IEEE 802.15.4-2006 with no requirement for PAN Coordinators or an association process. Each PAN is on a different RF channel chosen from the channels defined in this ICD.

5.1 Network Topology, Structure and Operation

5.1.1 802.15.4 Network Topology Overview

For ICD compliant communications, there is no requirement for PAN Coordinators, beacons, or beacon requests. This ICD defines a peer-to-peer topology in IEEE 802.15.4-2006 terminology. That is, on-conveyance devices learn then use the MAC address of a fixed or handheld device, or

an on-container relay device for communications. The architecture is one or more independent star topologies at a locale. No network routing is required in the 802.15.4 portion of the messages to/from remote data centers or handheld devices.

On-conveyance devices passively discover then communicate with network access devices (FNADs, HNADs), or via a relay device (ECoC/ECM) that has been specifically manually paired for such service.

Network access discovery by on-conveyance devices is done per this ICD using the NADA messages issued as broadcast packets by FNADs and HNADs. On-conveyance devices, without any transmissions, passively discover one or more ICD compliant network access “gateway” or “access point” devices. Non-ICD compliant network devices are ignored during network discovery.

Network Access Devices discover on-conveyance devices via an unsolicited message sent to a selected NAD after network discovery.

Per this ICD, on-conveyance devices cannot communicate with devices on other conveyances except as untrusted relays. No inter-conveyance encryption/decryption capacity is specified.

All packet addressing uses 64 bit IEEE-defined MAC addresses; 16 bit temporary PAN-specific addresses are **not** used.

For this *peer-to-peer topology* as applied in this ICD version:

1) The MAC **Shall** use the un-slotted CSMA (CCA) option due to low data volume. The Standard’s TDMA/Guaranteed Time Slot (GTS) option **Shall Not** be used.
2) On-conveyance CMs compliant with this ICD and may enter a low-power mode to conserve power. The Network Access Device Announcement (NADA) message (Section 5.1.6.2) **Shall** inform a CM of any waiting messages queued while the CM was not listening, and the time interval until the next NADA message.
3) NADAs are broadcast (not unicast) by NADs for use by the CMs for network discovery and Message Waiting. A paired ECoC/ECM does an addressed packet (unicast) to its paired on-conveyance device; it does not broadcast NADAs after being paired.
4) If a CM is out of RF range (coverage) of the NAD for a certain PAN ID, the CM may not discover the network. Should a CM lose coverage of its selected FFD NAD due to motion or changing RF conditions, the CM **Shall** perform network discovery, as per the above, this may be a different PAN ID and channel. Note: Application message sequence numbering, for lost/duplicate message detection, **Shall** resume as defined in this ICD’s message formats and [4], irrespective of the change.
5) When Add-on Sensors (AoS) are present, the AoS devices will simply transmit alarm messages as needed to the Security Device address provided during the pairing initialization process described in this document. The Security Device **Shall Not** transmit NADAs under any circumstances after being armed.

5.1.2 Network Protocol Stack

Figure 5-2 provides an overview of the protocol stack in any node of the wireless network, applicable to all NADs and on-conveyance devices. The PHY layer shown Figure 5-2 is largely fixed in Standard-compliant hardware and not alterable, i.e., this ICD defines the PHY as 2.4GHz, per IEEE 802.15.4-2006.

The MAC layer is firmware that is downloaded to the microprocessor(s) in commercially available or custom modules and configured per this ICD within IEEE 802.15.4-2006 defined variations.

In the topology of this ICD version, the NWK layer is absent and NWK-layer functionality is an aspect of the application layer. Except for the optional paired-relay function, there is no required message routing or forwarding within the wireless portion of the end-to-end transport in the topology ICD version.

The Application Layer, with the protocols in this ICD, is responsible for the end-to-end (i.e., between CMs and the DCP) message formats and error detection and correction across all transport networks in the path.

5.1.3 MAC Protocol Configuration

The 802.15.4-2006 MAC **Shall** be configured for full inter-operability, as follows. IEEE 802.11 coexistence as shown in Figure 5-2 is considered.

Table 5-1, IEEE 802.15.4-2006 MAC Configuration

Parameter	Value	Comment
Channel Set	IEEE 802.15.4-2006 Channel Numbers 15, 17, 21, and 23. No other channels may be used for ICD messaging.	To assure interoperability and extend battery life, no other channels are used. Band-edge channels are avoided due to spectral mask regulations in some countries. Channels above North America's ISM band edge are not used in North America, but may be permitted elsewhere. A minimum guard band of one channel for receiver selectivity is specified.
PAN ID	Only As defined herein	For messaging and network discovery as defined herein
MAC layer Encryption for NAD, HNAD	Disabled	Encryption is done in message payload data
GTS, Superframe	Disabled	
MAC ACKs	Hardware-enabled in conformance with 802.15.4 and timing	Note Application and Message ACKs are also defined herein. Lack of buffer space should not be reason for not transmitting a MAC layer ACK, as this ICD avoids need for flow control
Beacons and Coordinator Nodes	Not used for ICD-defined messaging	See Section 5.1.6.
Beacon Request MAC messages or other transmissions by the on-conveyance devices prior to passive network discovery	Restricted-use, Regulatory consideration.	Active-scan probing beacon requests when out of NAD coverage are prohibited.
CCA	Required for all transmissions	Clear Channel Assessment per the standard is required.

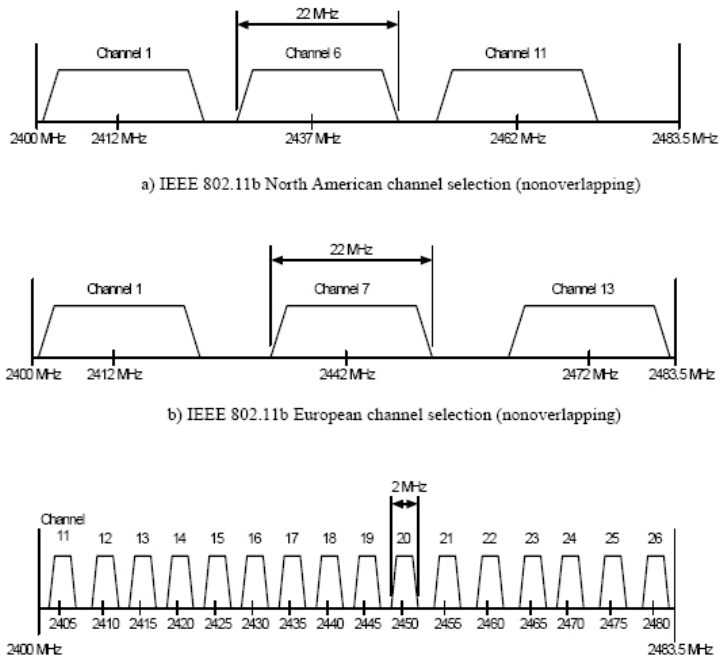


Figure 5-1, IEEE 802.11 vs. IEEE 802.15.4-2006 Coexistence

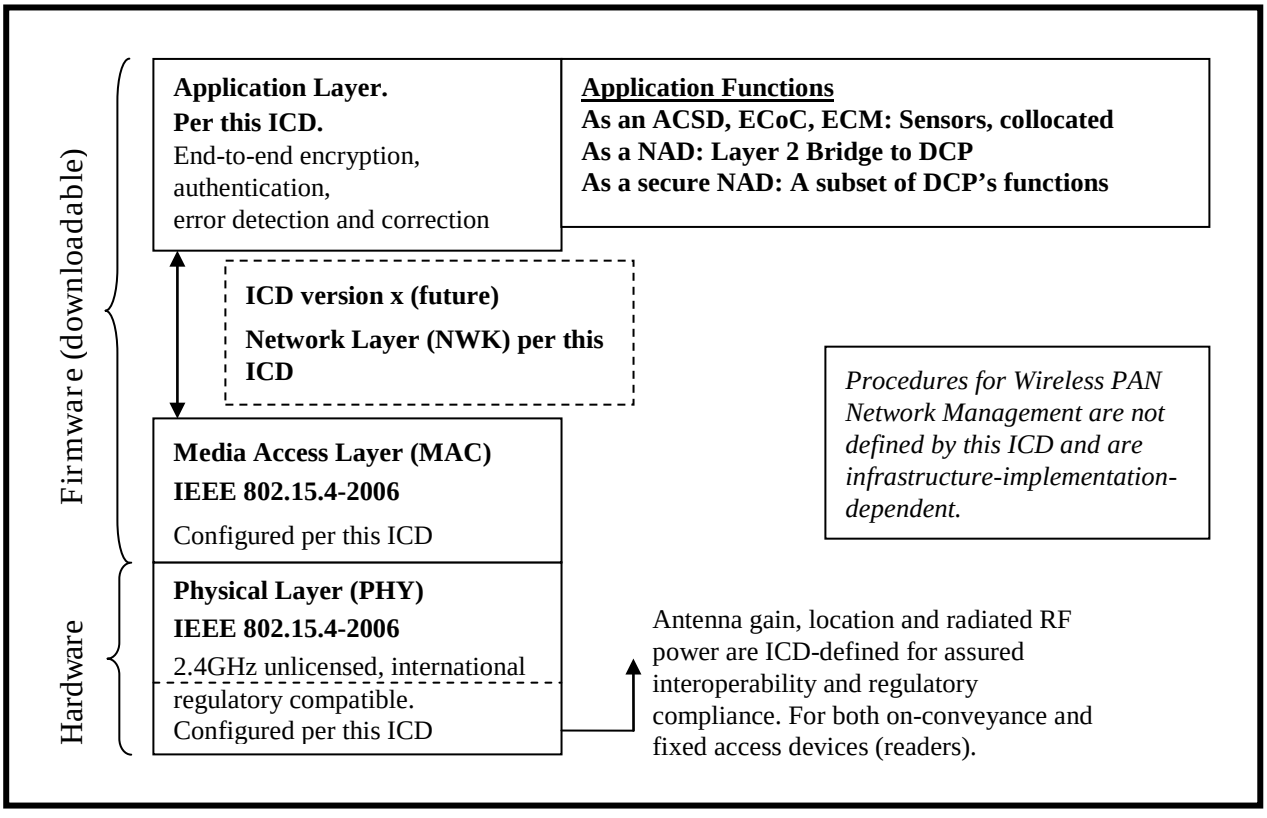


Figure 5-2, Communications Protocol Stack Architecture

5.1.4 Network PAN ID Standardization

5.1.4.1 IEEE 802.15.4b Data Frames

Every message data frame defined herein sent while using one of the PAN IDs reserved herein (see Table 5-2) **Shall** utilize 64-bit MAC addresses.

Wild-card PAN IDs are neither required nor prohibited. This ICD specifies two IEEE 802.15.4 standard 16-bit (2-byte) PAN IDs and four RF channels to minimize the network discovery power-on time for the sake of battery conservation. Other PAN IDs and channels may be used for proprietary (non-security) messaging. The PAN ID for each NAD is advertised by the NAD via the Network Access Device Announcement (NADA) message as described in Section 5.1.6. This ICD does not require or prohibit beacons. There may be multiple NADs per PAN ID and multiple NADs per ICD-defined RF channel.

In network discovery (defined in Section 5.1.6) for security-purposed messaging, the Security Device/ECoC/ECM **Shall** search for both of the PAN ID types reserved herein (see Table 5-2). A successful secure message exchange with the DCP, including application layer ACKs defined herein, confirms correct PAN ID and NAD selection.

5.1.4.2 PAN ID Codes

This ICD reserves two of 65,535 possible PAN IDs for ICD-compliant security messaging. Non-ICD messaging at a locale should not use these PAN IDs on the ICD-defined channels.

Table 5-2, Security-Reserved PAN IDs

Alternative	PAN ID, Most Significant Byte (Lowest offset in frame)	PAN ID, Least Significant Byte (Successive offset in frame)
1	0x96	0x69
2	0x69	0x96

If the PAN IDs in Table 5-2 are used for messaging other than that defined in this ICD, the expectation is that encryption and message integrity checks defined herein will reject the message with no transmitted response.

As to PAN IDs other than those reserved per Table 5-2, this ICD does not prevent use of PAN IDs for selection of message addressees. Such Proprietary use of PAN IDs is allowed by the ICD, preferably avoiding the IDs in the table (although this is not mandated) to help reduce using battery power to parse security-irrelevant commercial messages (e.g., any not defined herein). A CM may choose not to respond to broadcasts or beacons from devices using PAN IDs not listed in Table 5-2 to conform to constraints imposed by the device power budget.

5.1.4.3 Use of IEEE 802.15.4 Beacons

The use of beacons, beacon requests and network association is neither required nor prohibited by this ICD. This ICD does not require PAN coordinators or PAN coordinator association. Locale-dependent regulatory compliance may require suppression of recurring “blind” transmissions from moving devices located outside the normal area of operation. It is the intent of this ICD that Security Device System devices (excluding AoS) “listen first and transmit last” to ensure that on-conveyance transmissions occur only where NAD coverage exists.

This ICD requires that all ICD compliant transmissions of ICD messages use CCA. This ICD does not require 802.15.4-2006 beacon transmissions or beacon probe/association requests. The ICD implementer **Shall**, at a locale, select a channel and PAN ID, and change as necessary, to minimize the occurrence of non-ICD transmissions that do not use CCA, or that have recurring high rate transmissions that are likely to interfere.

5.1.4.4 PAN ID Code and Channel Re-use

Any channel or particular PAN ID code from Table 5-2 may be used by multiple NADs in a given coverage area. PAN IDs and WPAN channels should be selected prudently in the context of adjacent user systems, but neither the definition of "prudent" nor any requirements concerning PAN ID selection are in the scope of this ICD and are left to the system implementer.

5.1.5 WPAN MAC Address Interoperability Assurance

The intent of this ICD is to ensure proper coexistence and interoperability in a locale with many different manufacturers' on-conveyance devices and NADs. This includes overlapping RF coverage and WPANs with completely arbitrary WPAN data content. It is presumed that all systems comply with the IEEE 802.15.4-2006 Standard at the MAC layer following the regulatory intent of ISM-band spectrum sharing. Every Security Device **Shall** respond to its own UID as network address for purposes of wireless communications.

The WPAN radios' MAC addresses are assigned by and managed by an international authority to assure coordination among manufacturers and original equipment manufacturers (OEMs). Device UIDs defined herein **Shall** adhere to these standards and conventions.

5.1.6 Network Discovery

This ICD requires that NADA messages seen in Table 5-3 be transmitted by all NADs in such a way that interoperability is ensured among NADs and on-conveyance devices in any mix of vendors. After a CM executes network discovery, it **Shall** choose a NAD and **Shall** send the Unsolicited Device Status Message (defined in Section 9.5.6) via the chosen NAD.

5.1.6.1 Network Discovery Selection Priority

An on-conveyance device **Shall** select an HNAD in priority to all FNADs, when network discovery is undertaken and the HNAD's NADAs are detected.

An on-conveyance device that has previously selected an FNAD while dwelling in coverage **Shall** detect an HNAD's NADAs interleaved with the FNAD's NADAs. On such, the HNAD **Shall** be chosen and the FNAD use **Shall** be delayed or abandoned. When the HNAD's NADAs and unicast messages cease for 30 seconds, the use of the FNAD **Shall** resume.

When in simultaneous coverage of two or more NADs of similar types (either HNADs or FNADs), the CM **Shall** conduct NAD selection based on optimal signal strength using the Link Quality Indicator (LQI).

Per this ICD, an unsolicited *restricted status* message **Shall** be sent by the on-conveyance device to the chosen HNAD or FNAD on change of NAD coverage.

5.1.6.2 NAD Announcement (NADA) Message Broadcast

Every FNAD and HNAD **Shall** transmit a Network Access Device Announcement (NADA) message using the configured PAN ID and channel for ICD messages (commercial messages

may use the same NADA if otherwise compliant with this ICD). The NADA is essentially a brief "this NAD exists" advertisement. The NADA from FNADs and HNADs **Shall** use the broadcast address (all ones). The NADA relayed by a paired ECoC/ECM **Shall** be unicast, not broadcast.

Network Discovery, defined in the next section, references the NADA message. To avoid packet collisions, a NADA message is transmitted using CCA procedures per IEEE 802.15.4-2006.

NADA messages **Shall** be transmitted by each NAD at any of the intervals defined for NADA messages as shown in Table 5-3. The NADA interval **Shall Not** exceed one (1) second. Network discovery by CMs, while in low power mode between expected NADA messages, depends on knowledge of these intervals, based on NADAs received before entering a low-power mode.

The use of short-interval NADA messages **Shall Not** violate the least common denominator of locale-dependent regulatory limitations on transmitter duty cycle. The minimum recurring interval **Shall Not** be incompatible with the IEEE 802.15.4-2006 standard's CCA back-off (exponential) in such a way that interoperability among multiple manufacturers will be impacted by CCA faults when large but compliant exponents are used.

CMs **Shall** receive NADA broadcasts per the notional timing shown in Table 5-3. The on-conveyance device's receive duty cycle is not required to be continuous. The receive duty-cycle (listening for NADAs) of any on-conveyance device (except AoSs) **Shall Not** be less than 20 milliseconds per second on each of the four channels specified in Table 5-1. This is an equivalent of 8% listen duty cycle in total. It is the vendor's responsibility to optimize the receive duty cycle to ensure the network discovery requirements of Section 5.1.7 are met.

The NAD transmit duty cycle on any single channel **Shall** be determined by the NAD vendor and tailored to the specific implementation. This **Shall** be optimized in periodicity and duration to ensure the greatest likelihood of coverage for all possible devices moving within the FNAD coverage area. A maximum broadcast duty cycle is determined by local regulatory requirements. The broadcast duty cycle for handhelds is not required to be continuous, as shown in Figure 5-3. HNAD NADA broadcast messages are exempted from this restriction.

Multiple FNADs **May** transmit NADA messages on one or more channels using one of the PAN IDs defined herein. In the deployed case where the coverage areas of two or more FNADs overlap, it is the vendor/implementer's responsibility to ensure each channel is regulatory and IEEE compliant to preclude faults due to CCA failures in access contention.

After a Security Device is armed and it is paired with an ECM, NADA messages relayed by the ECM **Shall** be unicast to the MAC address of the paired CM, even though, in general, NADAs are broadcast. This is detailed in Section 4.2.8.

All NADs **Shall** listen continuously when not actively transmitting broadcast messages or otherwise engaged in message exchanges with devices in the NAD coverage area.

Beacon broadcasts as defined in IEEE 802.15.4-2006 **Shall Not** be used as an alternative to NADA broadcast messages. This assures interoperability of devices and NADs in mixed-vendor situations.

5.1.6.3 NADA Message Data Payload

The NADA message **Shall** be wholly contained in one MAC layer payload and consist of the following data. All fields are required. Bytes 0 and 1 are compatible with the standard ICD

message header. The Time Delay for next NADA (byte offset 2) is mandatory and must be changed if needed to enable interoperable power-conservation strategies.

An on-conveyance CM may enter power-conservation cycles no sooner than two seconds after the last (non-NADA) transmission to/from an NAD. The cycle's duration is governed by top-level system response time requirements (e.g., HNAD response time).

The ICD-defined *Set In-Trip State (SIS)* command **May** be sent by a secure NAD or DCP to assist in selection of power-conservation cycle time.

Table 5-3, NADA Message Content

Offset 0	**1**	**2**	**3**	**11**	**12**	**20**	**21**	**29**	**30**	**30 + n +1**
x0	**x1**	**x2**	**x3**	**xB**	**xC**	**x14**	**x15**	**x1D**		
Standard ICD Message Header Byte 0 Device Type	Standard ICD Message Header Byte 1, Message Type = NADA message (0xFF)	Bit 0: UTC is valid Bit 1: is 1 if MW list continues in next NADA Bits 2,3: reserved, ICD use. Bits 4-7: Time delay for next NADA; Coding: 0: 0.02 s 1: 0.04 s 2: 0.08 s 3: 0.10 s 4: 0.20 s 5: 0.40 s 6: 0.80 s 7: 1.00 s 8-15: reserved Accurate to +/- 0.01s Coding applies to next interval and may change at any time.	Date/time UTC 8 bytes per ICD format	Level 1 Facility Device Type (1 byte) DCP Device Type in Table 6-1	UID of Level 1 Facility (8 bytes) Field Usage described in [4]	Level 2 Facility Device Type (1 byte) HNAD Device Type in Table 6-1	UID of Level-2 HNAD Field usage described in [4]	Message waiting list count (1 byte) 0 if none	List of UIDs with message waiting. (n bytes) 0 is a valid count. List size limited by payload size (100 bytes). List content may rotate in successive NADA messages for an unlimited count.	NADA message checksum. One byte half-sum of NADA message (sum of the bytes modulo 256)

5.1.7 CM Network Discovery Procedure

The Network Discovery process relies on transmitted NAD Announcement (NADA) messages that recur at the time interval (variable or fixed) depicted in each NADA.

The CM **Shall** attempt network discovery at state and status-dependent time intervals constrained by battery conservation. "State" refers to the optional use of the Set In-trip State (SIS) DCP or secure NAD command.

The time interval **Shall Not** exceed the Message-Waiting list maximum age (Section 5.1.7.7). At some locales, there may be multiple NADs on different channels with the same PAN ID (e.g., an area with overlapping coverage).

The CM **Shall** tune to each ICD-defined RF channel defined herein and attempt to detect a NAD's NADA for each ICD defined PAN ID. Definitions for these are in the MAC layer configuration, Table 5-1. The scan characteristics **Shall** be determined by the vendor to enable a response time for network discovery that does not exceed 2 seconds following successful receipt and recognition of a valid NADA by the CM in the absence of channel contention (i.e., when the channel is clear).

Figure 5-3 is a timing diagram showing a CM sending status for the first time. There are two NADS on different RF channels. A CM powers up and discovers a marginal/weak-signal NAD on channel A, then retunes and finds another NAD on a channel B with an adequate signal. Note: The time synchronization of NADAs is arbitrary; an arbitrary case is shown.

When in or out of PAN coverage, the duration of low-power mode is influenced by the security condition state as shown in the DCP or secure NAD command messages in Section 9.6

After successful Network Discovery, the CM **Shall** follow Unsolicited Device Status Announcement Message procedure, as defined in Section 9.5.6.

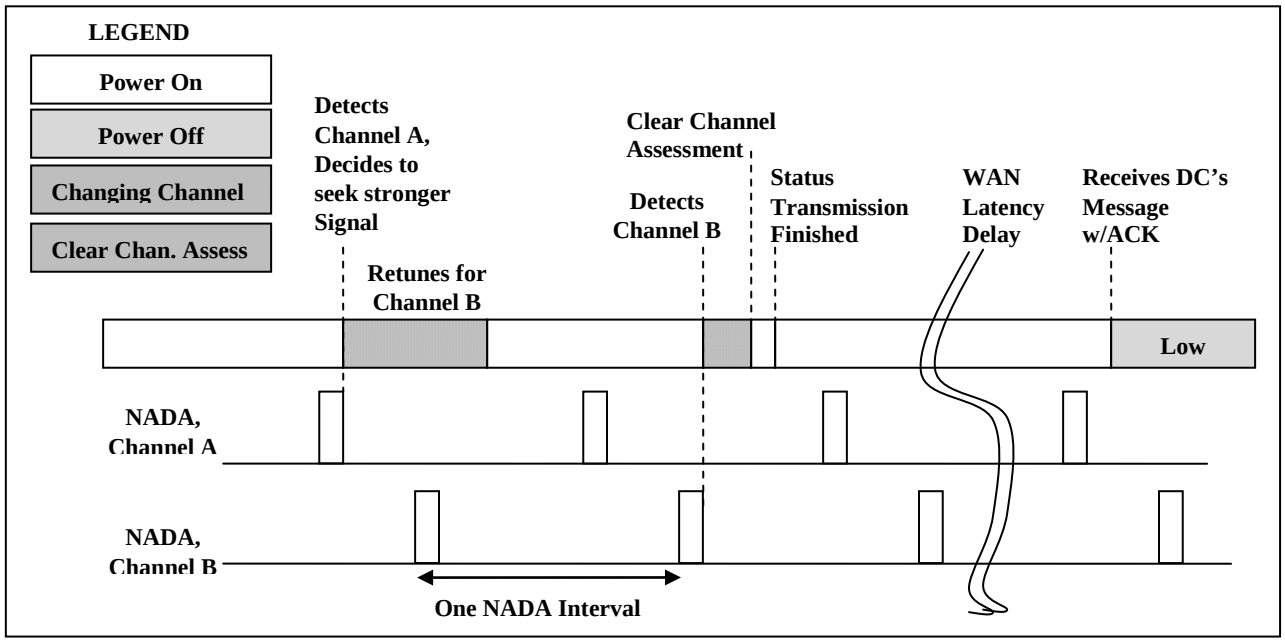


Figure 5-3, Network Discovery and Unsolicited Status Timing Example, Two NADs

5.1.7.1 Recurring Network Discovery

Due to changing RF conditions, to optimize NAD choice, and to permit an HNAD to pre-empt an FNAD, the CM **Shall** repeat Network Discovery, starting with the last-used channel/PAN ID, at time intervals not to exceed the Message-Waiting list purge timeout of 60 seconds, where the interval begins at the end of the last transaction with the DCP. The Unsolicited Device Status Announcement process (Section 9.5.6) suppresses redundant status messages where neither NAD choice nor sensor status has changed.

5.1.7.2 HNAD Network Discovery Prioritization

Secure HNADs **May** be used to conduct local short-range communication with specific CMs. For this application, the DCP will provide the HNAD a list of UID/encryption keys for identifying and conducting secure message exchange with specific devices. The HNAD will place UIDs in the message-waiting list of its NADA. A Security Device, whether paired or not, **Shall** respond to the HNAD NADA and conduct routine Message-Waiting procedure per Section 5.1.7.8. CMs that are in simultaneous FNAD and HNAD coverage **Shall** respond to the HNAD in preference to FNADs in all cases. Following completion of the HNAD message exchange, the CM **Shall** resume network discovery per Section 5.1.7.

5.1.7.3 NADA Message Waiting (MW) Overview

The purpose of Message Waiting is to enable devices with CMs (Security Devices, ECoCs, and ECMs all have embedded CMs) to extend battery life by synchronizing message delivery with power conservation cycles. The method assures interoperability among manufacturers' infrastructures and CM communications. Also, as in other protocols in this document, the method must use only the basic packet transmit/receive 802.15.4 functions.

All ICD-compliant devices **Shall** support the method defined here.

The CM **Shall** discover the network and send the initial Unsolicited Device Status Message as described in Section 9.5.6. Thereafter, e.g., while dwelling in coverage and intermittently entering a low-power state to conserve battery, the CM **Shall** use the NADA message waiting procedure described herein to passively (i.e., without transmission) detect a queued, incoming unsolicited messages from DCPs and secure NADs. The NADA message's "Message Waiting List" eliminates the need to transmit frequent polling requests. The Message-Waiting capability **Shall** be used when a transmission to a CM is to occur and:

1) The last-*received* message from the CM occurred two (2) or more seconds in the past. The age of the CM's last-*transmitted* message is not a criterion.
2) The destination device's 802.15.4-2006 MAC address, corresponding to its UID (as given by the to- CM message), is unknown to the NAD. This can occur if the NAD does not retain a history of active devices (instead using, e.g., a UID-to-MAC look-up table), if the UID/MAC has aged-out of a history due to inactivity, or if such history has been purged for other reasons, such as volatile memory or a software restart.

These criteria apply to the following situations:

1) A DCP or NAD sends an ad-hoc message long after the last from-CM message was received and the DCP is using the last-known NAD
2) A DCP or NAD retransmits a message due to a response timeout

The Message-Waiting capability **Shall Not** be used when a from-DCP message arrives at the NAD within the above-defined two-second window, such as any command/request including the restricted ACK message. The ACK would be in quick response, e.g., to unsolicited restricted status messages or log records.

5.1.7.4 NULL Message

For a specific UID in the NADA Message Waiting list, a NULL message (defined below):

1) **Shall** be sent if MW is true for Security Device's UID (Paired relay devices described in Section 4.2.8.3 are transparent but **Shall** send NULL).
2) **Shall** be ignored by the NAD if no message is waiting for that UID, e.g., if the message has already been sent.
3) **Shall** be repeated while MW is true but no more frequently than every 0.1 second.

The NULL message payload content is 9 bytes, as depicted in Figure 5-4. The purpose of the checksum byte is to reduce the probability of a non-CM's 9-byte transmission on the same channel/PAN ID being construed as an ICD-compliant NULL message. The UID byte order is the same as for the UID in the header of all other messages defined herein.

NOTE: This form of the NULL messages enables an option for some NAD types to not retain UID-to-MAC correspondence history. With correspondence history, a NAD **May** skip use of MW in many cases, such as for a DCP's quick ACK message.

Frame Payload Data, Unencrypted		
Originator's Device Type (1 byte)	Originator's UID (8 bytes)	Checksum, 1 byte (Same method as NADA checksum, Table 5-3)

Figure 5-4, NULL Message from Security Device/ECoC/ECM

5.1.7.5 NULL Message Global Response

If a UID in the MW list is an all 1's UID (0xFFFFFFFF), then each receiving non-NAD device **Shall** respond with a NULL message in the same manner and timing as if the device's specific UID was present.

5.1.7.6 Unsolicited Status Race Condition Handling

When there is a Message-Waiting indicator for a given UID *and* that UID has an Unsolicited Status Message to send in response to a real-time event, the on-conveyance device **Shall** send the Unsolicited Status Message instead of the Null message.

On receipt of the Unsolicited Status Message, the DCP **Shall** detect that the status was not the expected Solicited Status response and then presume that the prior pending message/command has been ignored and lost. The DCP **Shall** process the status message and may repeat the prior message, if relevant.

5.1.7.7 Message Waiting Method, NAD Responsibilities

A NAD asserts Message Waiting (MW), per the criteria above, as follows. The ICD-defined NADA message **Shall** contain a list of UIDs for which MW is true, i.e., for which a deferred message is queued. Successive NADAs will contain the UID in the MW list until the deferred message is transmitted by the NAD. The MW for a given UID **Shall** remain in NADA transmissions until:

1) A NULL message is received from that UID, or
2) Any other message defined herein is received by a NAD from that UID, e.g., an event's status message taking precedence over a response to a DCP command message, or
3) A period of 60 seconds elapses with no response from the target UID. The message originator (DCP) must time-out the expected response to the message that supports MW. No other indication of non-delivery is available from the message originator.

The NAD **Shall** provide an IEEE 802.15.4-compliant MAC ACK to NULL data frames, as it must to all data frames per this document.

On receipt of a NULL message from the target UID, the NAD asserting MW **Shall** transmit the deferred encrypted or unencrypted data message in less than two seconds.

After receipt of the NULL message, the NAD **May** continue sending MW via NADA until the deferred message is sent and a MAC ACK is received. A NULL message received with no MW condition for that UID, or for a UID not previously detected by a NAD, **Shall** be ignored. On

receipt of any message defined herein, the NAD **Shall** then update the UID/MAC affiliation history. The association can change due to the use of a paired device, such as an ECoC or ECM, acting as a relay.

5.1.7.8 Message Waiting Method, CM Responsibilities

On detecting of a NAD's UID in the NADA MW list, the CM **Shall** transmit the NULL message to that NAD. As for all ICD-compliant messages, the frame **Shall** be marked *MAC ACK requested*. The NULL **Shall** be repeated for every n^{th} NADA containing MW indication, where n can be 1. For NADAs at short intervals, n can be greater than 1 to reduce redundant NULL messages, as the NAD may be busy with other CM traffic. NULL messages **Shall** be suppressed for intervals less than 0.1 seconds.

The CM **Shall** inspect each NADA independently, as MW UIDs may be spread across successive NADAs when there are many UIDs pending at one NAD, not all of which will fit into a single NADA. This is referred to in this document as a *rotating MW list*.

The CM **Shall** detect and process a MW list larger than one NADA via bit 1 of the byte at offset 2 per Table 5-3.

A NAD May use this mechanism to discover in-range devices, for the chosen channel and PAN ID, e.g., when an FNAD is restarted or when an HNAD needs to discover devices.

5.1.7.9 Message Waiting Method, Relay Device Portion, NULL message frame

For a relay device such as a paired ECoC or ECM (Section 11.1.1), either of the following may occur when the UID of a non-integral sensor (e.g., a Security Device) paired to the ECoC/ECM occurs in a NADA with MW:

1) The ECoC/ECM **Shall** transmit a NULL frame to the NAD, using the UID of the paired Security Device, without Security Device involvement, or
2) The ECoC/ECM **Shall** retransmit the NADAs with MW to the paired Security Device and retransmit NULL messages sent by the Security Device. In this case, the sending unit's MAC address in the 802.15.4-2006 frame for the NULL message will be that of the ECoC/ECM. The NAD uses this in order to respond.

In either case, the NULL message **Shall** repeat while the NADA MW indication is true. As in the no-relay case, NULL messages **May** be sent for a fraction of all received NADAs with MW.

5.1.7.10 Message Waiting Method, DCP Portion

Considering power conservation, the DCP **Shall** accommodate a response delay due to MW no longer than the power conservation interval defined herein as 60 seconds, with or without Pairing.

5.2 Ad-hoc/Mesh Network Topology

Ad-Hoc/Mesh topology is not supported for trusted functions by the current version of this document for security messages. It **May** be supported for trusted functions in future versions pending validation of a routing standard such as [9]. Ad-hoc/mesh routing functions for relay devices such as ECoC/ECMs are allowed as a secondary communications path similar to cellular or satellite modes. Any current or future implementation of mesh routing functions for security messages **Shall Not** be in conflict with this document.

6 WPAN Physical Layer (PHY)

The 2.4GHz PHY is completely defined by IEEE 802.15.4-2006 with the exception of transmitter power and radiated power. The latter is essential for assured interoperability. A link budget common to all vendors is necessary for vendor A to assuredly achieve the needed signal-to-noise ratio for vendor B's device, in a bi-directional sense. This is the purpose of a link budget in any wireless system.

Also, the link budget must accommodate the expected least common denominator of regulatory restrictions in any locale in which the on-conveyance device may operate. This ICD makes no specific recommendation in this, for the sake of the common link budget, but regulatory compliance for radiated power and spectral mask compliance is a product requirement.

Table 6-1, IEEE 802.15.4-2006 PHY Configuration

Parameter	Value	Comment
Operating frequencies	See MAC layer Configuration Table 5-1	
Radiated Power	Such that the EIRP including antenna gain is no less than 10mW (10 dBm)	Least common denominator internationally; applies to fixed and on-conveyance devices; see text.
Receiver Sensitivity	Sufficient to meet Security Device and ECoC/ECM line-of-sight range requirements of [1] and [10]. Must also meet IEEE 802.15.4-2006 Packet Error Rate (PER).	Typically -85 to -90 dBm, excluding antenna gain/loss
Power consumption	Per device Functional Requirements Specification for battery life	

6.1 RF Interoperability Link Budget

The 2.4GHz specification herein addresses the requirement for internationally available unlicensed spectrum requirement. The specified IEEE 802.15.4-2006 MAC and PHY assure basic interoperability. However, inter-network-node RF signal attenuation due to obstructions and transmission path length require a common definition of assumptions.

Effective radiated transmitter (in delivered enclosure) power requirements and on-conveyance antenna location are specified herein to achieve interoperability at the received signal strength level. FNADs must be deployed in quantity and placement necessary to assure bi-directional coverage availability and adequate fade margins given the effective radiated power of on-conveyance Devices and the RF occlusion of conveyances given the system RF link budget.

The following receiver requirements apply to all CMs and AoSs per [5]:

1) Receiver sensitivity **Shall** be -85 dBm or better for a 1% packet error-rate (PER).
2) The receiver **Shall** provide 30 dB or better for alternate adjacent channel rejection.
3) Under these conditions, the receiver **Shall** conform to the packet error-rate (PER) limitations specified in [5].

6.1.1 Receiver Requirements

Security Device System WPAN receivers **Shall** comply with MAC and PHY as defined herein.

6.1.2 Transmitter Requirements

To support the common RF link budget for interoperability, the following transmitter requirements per [5] apply to all CMs, AoSs, and NADs:

1) **Shall** fully comply with the PHY as applied by this ICD
2) **Shall Not** exceed regulatory limits for in-band and out-of-band spurious and harmonic emissions
3) **Shall** comply with each regulatory domain's rules regarding maximum field strength as measured outside of the as conveyance for antennas located either inside or outside.
4) **Shall** provide the transmitter power and radiated power per the link budget listed in Section 6.1.4.

6.1.3 On-conveyance and FNAD/HNAD Bi-directional Antennas

The on-conveyance devices **Shall** support the required range when installed on conveyances per ConOps in [1], and comply with this ICD, notably the common RF link budget.

6.1.4 RF Link Budget

To assure interoperability between any manufacturer's NAD and any manufacturer's CM, at the ranges specified in [1], an example of a conventional RF engineering link budget is provided in Table 6-2. Given this, design and deployment/installation engineering can assure that the received signal strength will support the specified range and in-coverage dwell time for any mix of products. The standard link budget elements are listed, and implementation engineers should employ these standard elements in developing deployment link budgets to ensure that the range and coverage/dwell-time requirements are met for both line-of-sight and non-line-of-sight conditions due to mobility and antenna location choices.

Table 6-2, Link Budget Example

Ref	Link Budget Parameter (2.45GHz)	Security Device	FNAD	HNAD
A	Antenna Gain, minimum, (dBi), net of other losses	0dBi[1]	5dBi[2]	0dBi
B	Transmitter power[3] (EIRP), minimum (dBm)	+3dBm[4]	+10dBm[5]	+3dBm
C	Line-of-sight/clutter-free free-space path loss for exponent = 2.0 adjusted for locale-dependent clutter obstructions.	Locale-Dependent		
D	Additional path loss From RF occlusion, adjusted for factors such as Security Device/ECoC location in/on the conveyance, path to best-server reader, clutter, and obstructions.	0dB		
E	Path-loss positive adjustment for diffraction statistical mean, in non-line-of-sight	0dB		
F	Fade Margin, slow fading, (dB), for link availability	-6dB		
G	Receiver sensitivity at IEEE 802.15.4-2006 specified PER, minimum, at antenna port, (dBm), excluding antenna gain.	-85dBm		

[1] This is typical for an integral or on-PC board antenna.

[2] Typical for an antenna of practical size for the application.

[3] EIRP will be the least of those permitted under per-country regulations, which change frequently. [3] states that Japan's limit is 10mW per MHz, so for Japan the 1.5MHz occupied bandwidth (6dB points) corresponds to ~15mW, and IEEE 802.11's 20MHz bandwidth corresponds to ~30mW. Other countries' restrictions are considered in [3]. Some regulations in this band permit increased EIRP as a function of antenna beam width (directionality), although this probably doesn't apply to CMs.

[4] Typical of currently available chipsets without external power amplifier/LNA. Regulatory EIRP limits on W/MHz must be accommodated.

[5] Excludes antenna gain.

7 Media Access Control Layer (MAC)

7.1 MAC Frame Constructs

The MAC frame constructs are based on those of [5], Table 82, including:

1) All frame types identified in IEEE 802.15.4-2006 **Shall** be supported by the Security Device System.
2) Each of the four frame types **Shall** comply with 802.15.4-2006 by including:
    a. A MAC header (MHR)
    b. A MAC payload
    c. A MAC footer providing a 16-bit CRC CCITT frame-check sequence as defined by the standard.
3) Within data frames and for commands passed through the NADs, the IEEE 802.15.4-2006 MPDU **Shall** include data payload provided per this ICD.
4) The message contents transmitted by the network access device to either the DCP or a CM **Shall** be forwarded without modification.
5) The application data payload **Shall** be a maximum size defined by the IEEE Standard 802.15.4-2006.

7.1.1 MAC-layer Configuration parameters

See Sections 5.1.3 and 5.1.4.

7.1.2 MAC Layer Acknowledgement Frames

All successful communications between devices **Shall** be acknowledged. The format for the acknowledgement frame **Shall** follow exactly as provided in [5], Figure 12.

7.1.3 MAC Layer Retransmissions

Retransmissions done by the MAC layer due to MAC layer ACK timeouts **Shall** be executed per [5], and there **Shall** be at least three retransmission attempts, with each subject to the usual CCA.

8 Network Layer

Routing within the IEEE Standard 802.15.4-2006 wireless network is per this document. Addresses are full 64-bit MAC addresses. PAN Coordinators are not required.

9 Application Layer

All FNADs, HNADs and CMs **Shall** implement the IEEE 802.15.4-2006 MAC and PHY configured per this ICD.

9.1 Application Layer Messaging

Messages are created by the following network devices:

1) Data Consolidation Point (DCP) (communication between a key-providing entity and the DCP, per Figure 3-2, is outside the scope of this ICD)
2) NADs (communicating with a CM)
3) On-conveyance devices on behalf of sensors, in response to DCP commands, and during Network Discovery.

Messages are defined here so that sender and receiver end-points (e.g., Security Device and DCP) **May**:

1) Perform mutual authentication to preclude rogue devices and DCPs
2) Encrypt and decrypt at end-points, including the secure NAD with no decryption at intermediate network elements
3) Encrypt only the sensitive data elements
4) Detect lost and invalid messages
5) Provide the sender with a receipt acknowledgement, end-to-end, irrespective of the transport networks between sender and receiver
6) Easily discriminate between commercial and security-purposed messages while both message types are handled by the same end-to-end communications

The CM is required to attempt to transmit an unsolicited status message within two (2) seconds of the completion of any of the following events when in NAD coverage:

1) Initial network discovery
2) Detection of a change in the Security Device/ECoC/ECM -selected NAD or
3) Detection of a change in state (i.e. alarm, battery status, add-on sensor alarm)

The CM is required to attempt to transmit a command response message within 2 seconds of receipt of a command. Timeout periods for retries are identified in Section 9.3.

9.1.1 Date and Time Format

All times in this ICD, including messages and event records, **Shall** be in Coordinated Universal Time (UTC/GMT) as 8 bytes. The coding **Shall** be as follows:

Table 9-1, Date and Time Format

Offset 0	1	2	3	4	5	6	7
Month (1 – 12) (January = 1)	Day of month (1 – 31)	Years since 2000	Day of week (0 – 6) (Sunday = 0)	Hours since midnight (0 – 23)	Minutes after the hour (0 – 59)	(leap) Seconds after the minute (0 – 61)	Optional Fractional seconds, LSB = 1/100 sec.

9.1.2 HNAD Messages

9.1.2.1 When the CM has connectivity with the DCP

The CM, if connectivity currently exists with the DCP via the PAN, cellular or other means, **Shall** execute commands from an HNAD in preference to commands from the DCP received via the PAN or cellular communication modes. Command messages received by the CM from an HNAD **Shall** take priority for both collision mitigation and execution over messages received concurrently via alternative communications modes other than IEEE 802.15.4-2006 PAN or cellular. The CM **Shall** execute all specific addressed commands received regardless of sender priority.

9.1.2.2 When the CM has no connectivity with the DCP

CMs **Shall** communicate with the secure NAD when connectivity does not exist with the DCP. In this direct-from-NAD case, the secure NAD must emulate the DCP messages to include encryption and decryption using DCP-supplied keys. Certain command codes are required, e.g., *Disarm by HNAD.* ECMs **Shall** communicate directly with an HNAD only when not paired.

9.2 Message Addressing, End-to-End

9.2.1 Addressing, For Data Consolidation Point (DCP) Destination

The destination DCP is unknown to the CM but is known by the locale's infrastructure, which forwards every message *verbatim* to the appropriate DCP. This information is contained in the Level-2 UID of the NADA message and in the UID of the command messages sent by the DCP. See [3] for details.

9.2.2 Addressing, For On-Conveyance Device Destination

Every security-purposed message from the DHS-designated DCP contains the UID of the DCP as the UID of the message header. The message is composed by the DCP per [3] and wrapped in an IP packet (or other equivalent). This packet is sent to the IP address for the last-known NAD locale for the Security Device/ECoC/ECM. At the locale, infrastructure systems send the packet to the proper NAD, i.e., the WPAN NAD that is likely to be serving (or was most recently serving) the Security Device/ECoC/ECM with coverage.

9.3 Message ACKs, Error Detection and Correction

Independent of all wired/wireless transport media between DCP or secure NAD and CM, the following error detection and correction methods **Shall** be utilized for security-purposed messaging governed by this ICD. All other alternative communications modes such as SMS/SMPP are commercial in nature and not subject to the requirements of this section.

9.3.1 Retransmissions for Error Correction, End-to-end

Per this ICD's message formats, every transmitted and numbered message **Shall** yield a numbered acknowledgement (ACK) from the receiver (CM or DCP or secure NAD). This is at the application layer, independent of transport layer error management. In this ICD, the numbered ACK is a component of the response to requested data, to avoid sending two messages, e.g., the Send Log command from the DCP or secure NAD.

9.3.2 Acknowledgement (ACK) from the On-conveyance CM

The acknowledgement to a DCP or secure NAD command message is the matching command's ascension number stored within the response status message (or log event data message if in response to a *Send Log* command) per this ICD. For log responses, this is applicable only in the first log record. The period of the timeout **Shall** be nominally two (2) seconds. The DCP or secure NAD **Shall** retransmit up to five (5) times when in coverage.

9.3.3 Acknowledgement (ACK) from Data Consolidation Point/HNAD

The unsolicited status message sent to a DCP **Shall** yield an ACK message to the CM. This ACK message is an explicit command message, the structure of which is defined in Section 9.6.5. The period of the timeout **Shall** be nominally twenty (20) seconds after completion of the command execution (if applicable). The DCP or secure NAD **Shall** retransmit up to five (5) times when in coverage. The CM **Shall Not** transmit a status/ACK response to an ACK command message from the DCP or secure NAD.

9.3.4 Acknowledgement Failure Procedure

If a receiving CM exhausts retransmission limits without receiving an ACK message from the DCP or secure NAD, the CM **May** cease attempting to link to that NAD for a period of time not to exceed one (1) minute. The CM **Shall** respond to the next available NADA that employs a different UID immediately with its current status. When a receiving DCP or secure NAD exhausts retransmission limits, the next-higher application **Shall** be advised. The DCP **Shall** record the ACK failure in its database. The secure NAD **Shall** record the ACK failure in its secure NAD Activity Log. Duplicate messages do not require an ascension number increase (i.e. same encryption). The DCP or Secure NAD **Shall** increase the ascension number for the next message sent with new encryption.

9.4 Application Layer Message Structure

9.4.1 Applicability

Every security message **Shall** be formatted per this section. Every commercial-purposed message **Shall** be formatted per the message header (MH) definition shown in Figure 9-3.

9.4.2 Description of Application Layer Message Structure

The application layer messaging and protocol is such that the payload data may be copied verbatim from one LAN/WAN transport to another and sent on a next-transport link as an unreliable datagram. For example, the IEEE Standard 802.15.4-2006 payload data can be copied to an IP packet and sent using UDP or TCP using simple bridging, and so on, for each hop to the DCP in a routed network.

Messages should not be parsed until received at the final destination (either a CM or the DCP, depending on direction of communication) so that intermediate network elements need not meet network security (NETSEC) or information assurance (IA) requirements as trusted devices with the ability to decrypt. With this method, decrypted data will not exist at other than the DCP (or secure NAD) and secured on-conveyance device, eliminating need for physical security protection of intermediate network elements such as bridges and gateways.

Messages are conveyed wholly within the *payload data* area of a MAC layer data frame. This structure is shown in Figure 9-2.

The application message data plus the message header **Shall Not** exceed the available payload data area defined by IEEE 802.15.4-2006 with the MAC option specified in this ICD.

Note: The MIC for key management messages described in Figure 3-2 and [3] is 16 bytes. See [4] for the packet structure of key management messages.

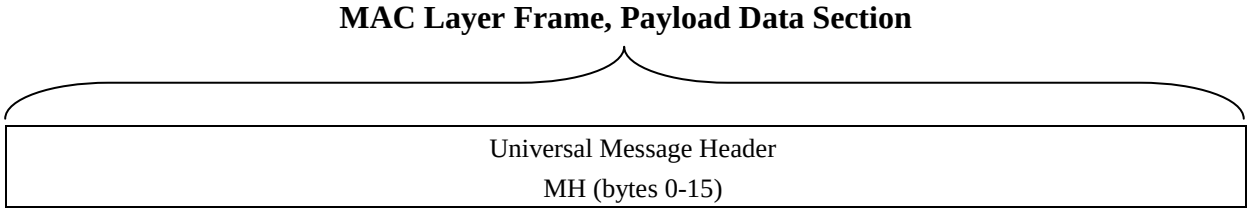


Figure 9-1, Commercial-purposed Messages from Security Devices – MAC Payload

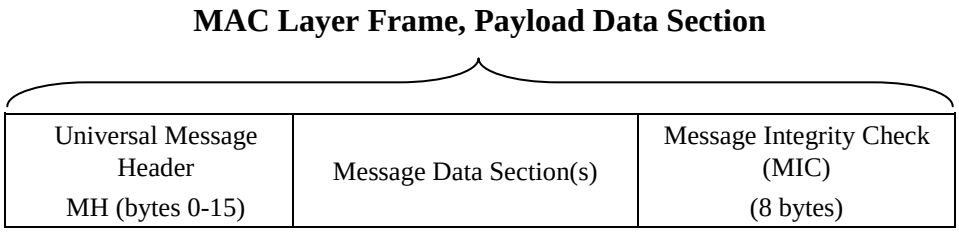


Figure 9-2, Security-purposed Messages, Message Within MAC Payload

9.4.3 Universal Message Header (MH)

The MH structure and all other message structure of messages traveling between CM and DCP in either direction **Shall Not** be altered by Security Device System transport devices. If a message arrives with Message Header contents not formatted in accordance with Figure 9-3, or is otherwise in error, the NAD application **Shall** drop the packet without processing.

9.4.3.1 MH for Commercial-purposed Messages

The MH format shown in Figure 9-1 and detailed in Figure 9-3 is required for ICD-Coordinated commercial-purposed messages, which are unrelated to security by definition, as described in Section 3.1. Other than the items shown in the message header (Figure 9-3), no content is defined by this ICD for commercial-purposed messages. Commercial messages **May** append additional fields, such as time or location codes, to the header following byte 1.

9.4.3.2 MH for Commercial-purposed Messages from a CM

The MH structure is shown in Figure 9-3. For commercial-purposed messages originating from a Security Device/ECoC/ECM:

1) The first two fields of the message header **Shall** be formatted as defined herein.
2) Device Type **Shall** be set to one of the security device types listed in Table 9-2

Message Type **Shall** be set to a value within the range allocated for commercial-purposed messages in Table 9-3.

The commercial purpose of a message sent by a Security Device **Shall** be indicated by setting the first two bytes of the header for Device Type and Message Type. Once this is done, the rest of the header and all other payload bytes are as defined by the vendor for commercial purposes.

9.4.3.3 MH for Security-purposed messages

For security-purposed messages, all fields of the message header **Shall** be formatted as defined herein. The MH length may change in future ICD revisions; this is defined by the ICD revision number in the MH. Each field of the MH is described, below.

The MH format shown in Figure 9-2 and detailed in Figure 9-3 is the same for all security related message types defined in this ICD. The MH format applies to messages sent by either CM, DCP or secure NAD. The MH within the WPAN MAC layer data frame payload is not encrypted. This enables optional bridging to/from the W-PAN and an IP network, where the Device ID in the MH may optionally be used by infrastructure devices to direct the message to one of several NADs at a locale if mobility management is needed and for unsolicited commands from a DCP.

9.4.3.4 MH Spoofing

It is understood that the MH will not be altered by message transport or transport protocols. Some Security Device System transport legs (e.g., those involving satellite and cellular networks) are outside the scope of this ICD. The MH **Shall Not** be altered by any transport mechanism or protocol defined herein. This is relevant because the MH is included in the message integrity check (MIC), and alteration of any MH or data content field will be detected by the MIC in the message content and reflected in the status message error conditions. For further discussion of this topic, see [4].

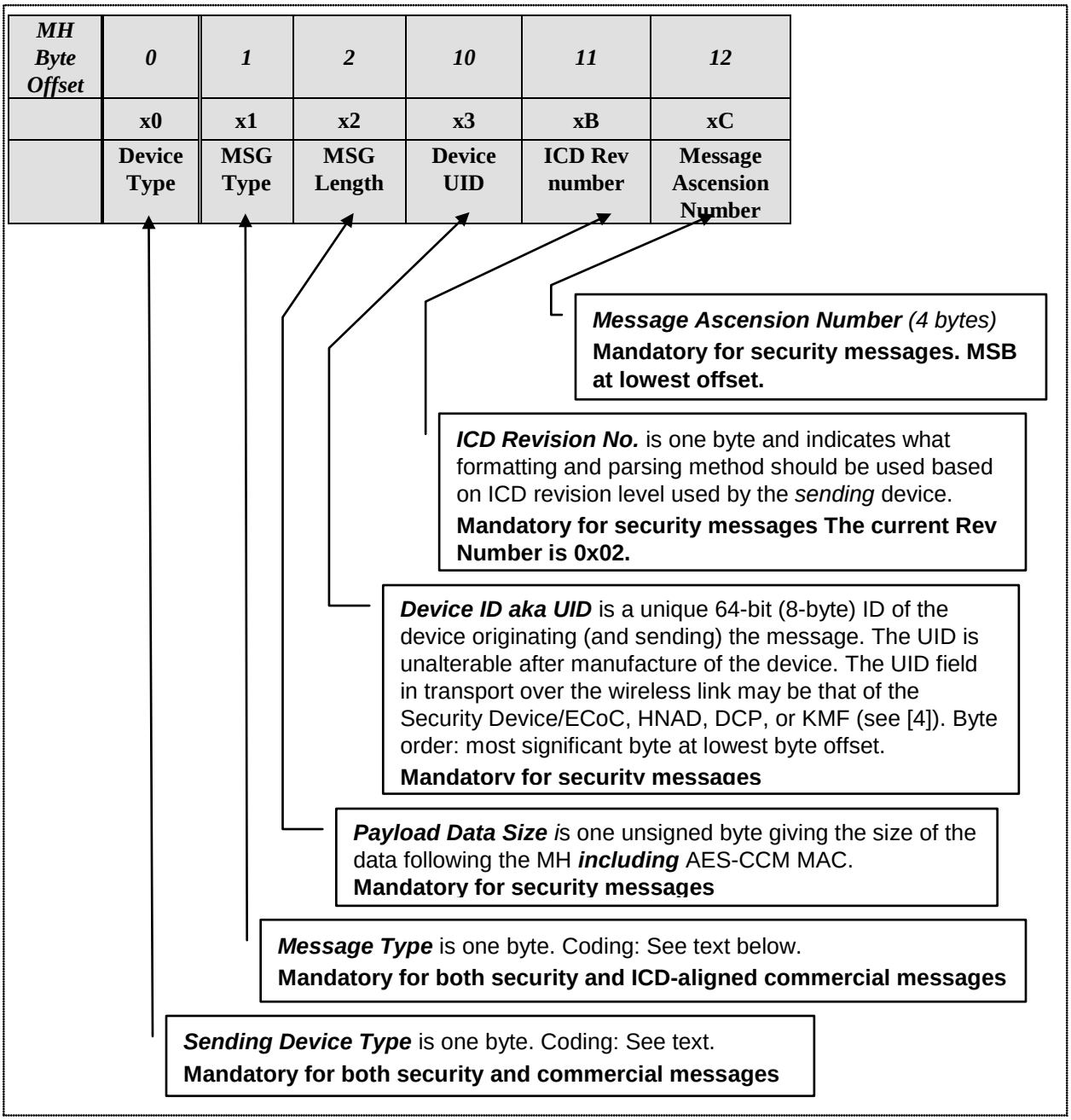


Figure 9-3, Universal Message Header Contents

9.4.3.5 MH, Device Type Codes

Table 9-2 defines Security Device System device types. Commercial device types that comply with this ICD **May** be assigned any value between 0x01 and 0x7f, as shown in the table.

Table 9-2, MH Device Type Codes

Device Type	Type Field Value
ACSD Type 0	0x80
CSD Type 0	0x81
ECoC Type 0	0x82
Wireless AoS Type 0	0x83
ECM Type 0 (not applicable to relay function)	0x84
FNAD (non-Secure) Type 0	0x85
HNAD (Secure) Type 0	0x86
FNAD (Secure) Type 0	0x87
Data Consolidation Point (DCP)	0x88
Key Management Facility (KMF; see [4])	0x89
HNAD (Non-secure) Type 0	0x90
HNAD (Arming-only) Type 0	0x91
FNAD Non-Root NAD Type 0 (future use) Type 0	0x92
Commercial (non-ICD)	0x01-0x7f

9.4.3.6 MH, *Message Type* Codes

This field is mandatory for security-related sending device types as in Table 9-2 and irrelevant for other device types.

Table 9-3, MH Message Type Codes

MSG Type		Message Data Flow
0x00	Unrestricted Status Message	From Device to DCP via NAD
0x01 – 0x7F	For ICD-compliant commercial-purposed messages, which need not conform to the MH or data content definitions herein.	Bidirectional.
0x80	Restricted Status Message From Device as defined herein	From Device to DCP via NAD
0x81	Device Event Log Record	From Device to DCP via NAD
0xA0	Sensor Discovery Broadcast (Security Device NADA)	Broadcast by Device
0xA1	Sensor Database Report	From Device to NAD
0xA2	Sensor Status Message	From AoS to Device
0xA3	AoS to Device Sensor Configuration Data Message	From AoS to Device
0xA4	Device to NAD Sensor Configuration Data Message	From Device to NAD
0xA5 – 0xAF	Reserved for AoS-related messages	
0xC0	Device Command Unrestricted as defined herein	From DCP to Device via NAD
0xC1	Device Command Restricted as defined herein	From DCP to Device via NAD
0xC2	Device to Sensor Restricted Command	Device to AoS
0xe0	Encryption Rekey	HNAD, DCP to Device via NAD or direct
0xe1 – 0xe9	Reserved for Key Management	See [4]
0xFF	NADA Message	Broadcast by NAD; unicast by ECM in relay function

9.4.3.7 MH, *Message Data Size*

Message Data Size is the byte count of the application-layer payload minus the MH byte count, as shown in Figure 9-3.

9.4.3.8 MH, Device UID

As in Figure 9-3, the Device ID (UID) is a 64-bit manufacturer-assigned unique identifier. The device must respond to this UID as its functional wireless network address. The device vendor **Shall** be responsible for obtaining address space for their organization with the ID managing authority (IEEE EUI-64). The transmission byte order is most-significant byte at the lowest MH offset. The UID **May** be the 802.15.4 radio MAC address if it is IEEE coordinated as unique.

9.4.3.9 MH, *ICD Revision Number*

The ICD Rev Number is set by the device that composed the message and in accordance with that in the Document Control Table at the beginning of this document. The Revision Number is used by receiving devices to determine how to parse the MH and how to parse/decrypt data portions of security messages.

9.4.3.10 MH, *Message Ascension Number*

Each device type **Shall** maintain separate “transmit” and “receive” Message Ascension Numbers associated with each unique device with which it communicates. For example, the Security Device/ECoC/ECM must maintain number pairs for each unique DCP or secure NAD with which it communicates. (Note: Only the MH Message Ascension Number is 4 bytes; all other Ascension Numbers in the data frame payloads are 1 byte). The initial value of all Message

Ascension Numbers **Shall** be one (1). The Security Device/ECoC/ECM must maintain number pairs for each unique secure NAD with which it communicates and vice-versa. See [4] for details.

For a non-secure NAD, the Message Ascension Numbers are managed by the DCP. For the secure NAD, the numbers are obtained from the DCP and later used for communications by that secure NAD.

A message received with a Message Ascension Number less than or equal to the number of the most recently received message **Shall** be ignored.

For a message received with a Message Ascension Number equal to the number of the most recently received message, the previous response **Shall** be transmitted in identical form. The number of response attempts **Shall Not** exceed 5.

A message received with a Message Ascension Number greater than the number of the most recently received message **Shall** be accepted with proper response.

9.5 Message Content

Security Devices and ECoC/ECMs can all send Device Status Messages, but status messages from a Security Device are different from ECoC/ECM status messages. In addition, distinctions are made between Restricted and Unrestricted status content and between Solicited and Unsolicited messages. These distinctions are explained in this section.

9.5.1 Device Restricted Status Message from Security Device

This message is sent when either of the following conditions holds:

1) A valid Status Request command from the DCP or secure NAD is received by the Security Device/ECoC/ECM. In this case, the Unsolicited Status bit is cleared in the message's status field. The ACK No. field **Shall** contain the Ascension Number from the message header of the Status Request command; The DCP or secure NAD may validate using this number.
2) The Unsolicited Device Status announcement message transmission condition is met per Section 9.5.6. In this case, the Unsolicited Status bit is set in the message's status field.

Note: The MIC for key management messages described in Figure 3-2 and [4] is 16 bytes.

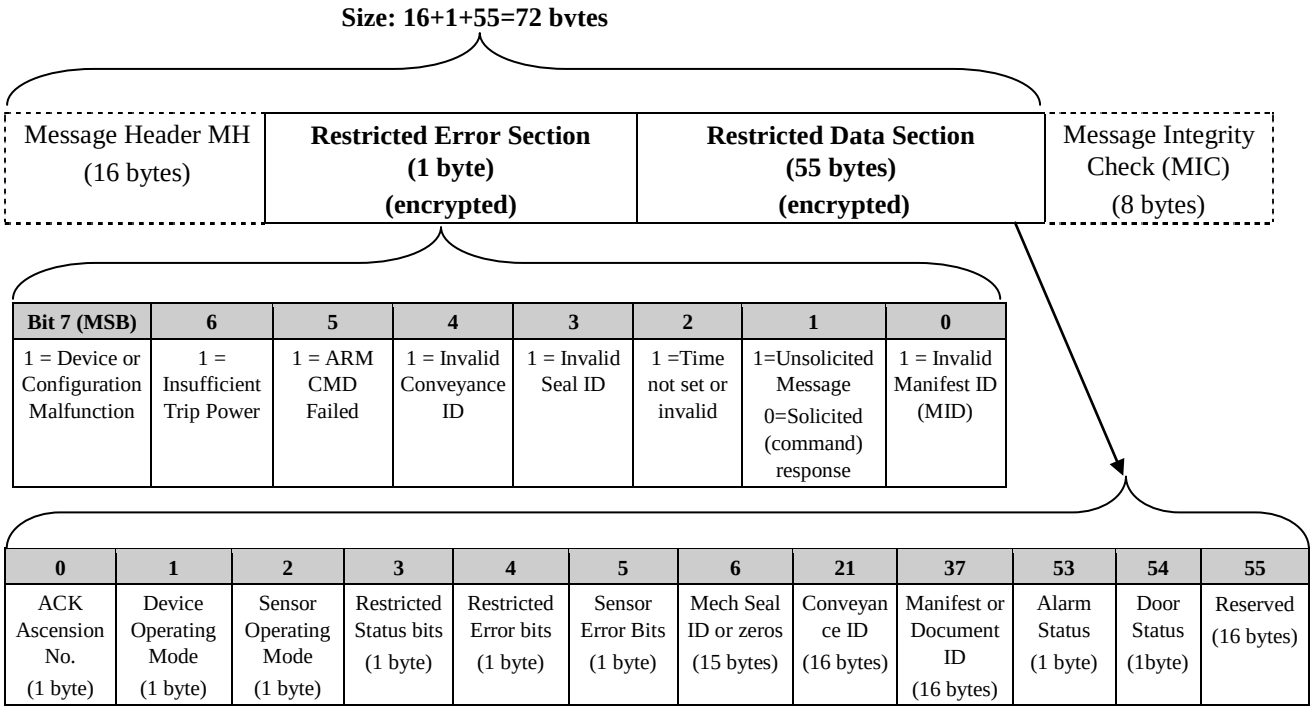


Figure 9-4, Device Status Message

Table 9-4, Device Status Message Restricted Data Section Content Definition

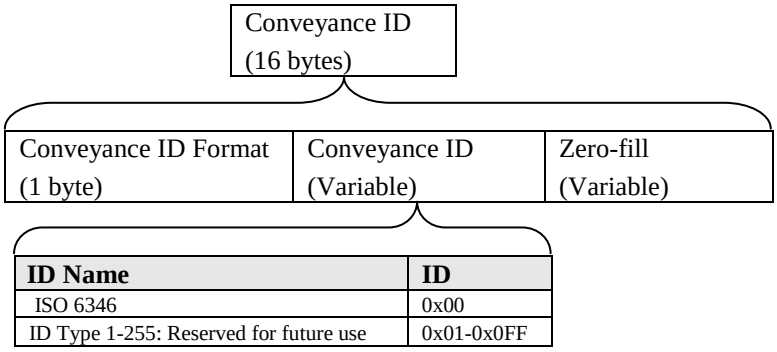
Restricted Section Content	Definition
ACK Ascension No.	Ascension Number for corresponding command. N/A for unsolicited status
Device Operating Mode	Bit 0=0: Deactivated; Bit 0=1: Armed; others: reserved
Sensor Operating Mode	Bit 0=0: Sensor 1 disabled; Bit 0=1: Sensor 1 enabled; Bit 1=0 Sensor 2 disabled; Bit 2=1 Sensor 2 enabled; etc…:
Restricted Status Bits	Bit 0 = sensor 1 alarm; bit 1 = sensor 2 alarm, etc.
Restricted Error bits	Bit 7 = Sensor malfunction; Bit 6 = decryption error; Bit 5 = invalid command; bit 4 = log overflow; Bit 3 = ACK failure; Bit 2= configuration failed; Bit 1=Sensor enable failed; Bit 0 = Reserved
Sensor Error Bits	Bit 0=1 Sensor 1 error; Bit 1=1 Sensor 2 error; Bit 2 = 1 Sensor 3 error; Bit 3 = 1 Sensor 4 error; Bit 4 =1 Sensor 5 error; others: reserved . Cause in Restricted Error Bit.
Mechanical Seal ID	ASCII characters per [6]; unused portion to be padded with spaces.
Conveyance ID and Checksum	Unique identifier for conveyance. See Section 9.5.1.2
Manifest or Document ID	ASCII characters
Alarm Status	See Section 9.5.1.3
Door Status	See Section 9.5.1.4

9.5.1.1 Mechanical Seal ID

The Mechanical Seal Identifier is not to exceed 15 alphanumeric characters consistent with the requirements of [6]. The number **Shall** be right-aligned and padded with leading spaces as required.

9.5.1.2 Conveyance ID

The Conveyance ID field is 16 bytes. The first byte codifies what form of conveyance ID is present in the remaining bytes, as follows. Unused bytes **Shall** be zero-filled.



ID Name	ID
ISO 6346	0x00
ID Type 1-255: Reserved for future use	0x01-0x0FF

Figure 9-5, Conveyance ID Field

9.5.1.3 Alarm Status

The Alarm Status is a single byte that represents the alarm state of the Security Device as defined in Table 9-5

Table 9-5, Alarm Status Parameter

Alarm Parameter	Alarm Status
0x00	Not alarmed
0x01	Alarm
0x02 through 0xFF	Reserved

9.5.1.4 Door Status

The Door Status is a single byte that represents the door state as detected by the Security Device as defined in Table 9-6**.**

Table 9-6, Door Status Parameter

Door Parameter	Door Status
0x00	Closed
0x01	Open
0x02 through 0xFF	Reserved

9.5.2 Restricted Device Status Message from ECoC/ECM

Devices mounted on the external surface of the conveyance such as an ECoC or ECM **Shall** be capable of generating a Status Message that includes the Universal Message Header and the CM integral sensor data as follows. This Status Message completely independent of the Security Device messages and is passed to the DCP via a secure NAD or non-secure NAD.

Note: The MIC for rekey commands described in [5] is 16 bytes long.

This message **Shall** be sent when:

1) The ECoC/ECM receives a valid NOP command from the DCP or secure NAD. In this case, the Unsolicited Status bit in the status field of the status message will be false. The ACK No. field **Shall** contain the ascension number from the message header of the Status Request command; the DCP or secure NAD **May** validate using this number.

2) The Unsolicited Device Status Announcement message transmission condition is met per Section 9.5.6. In this case, the Unsolicited Status bit in the status field of the status message will be true.
3) Conditions are met of pre-programmed time intervals, distance intervals, or periods of sustained loss of GPS. These intervals/periods **May** be established at the time of commissioning.

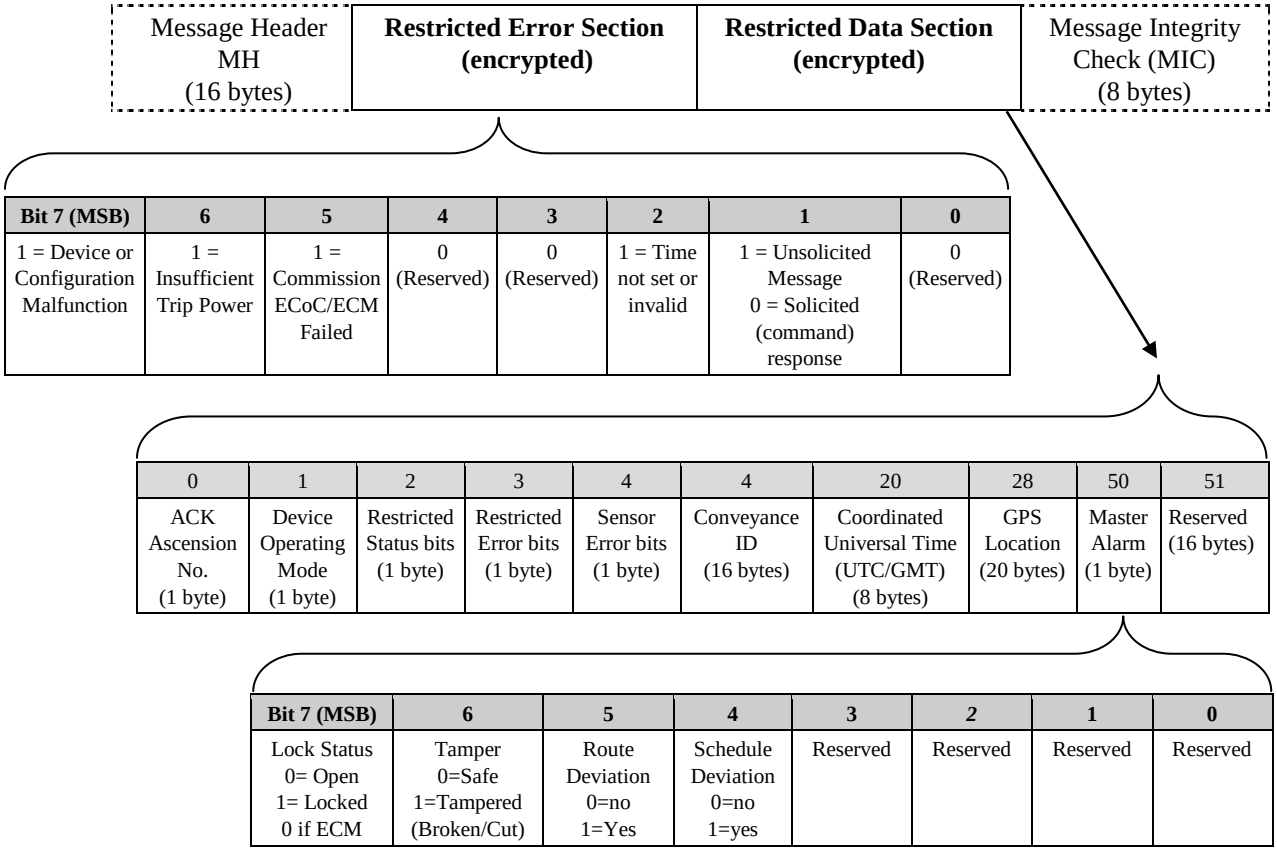


Figure 9-6, Device Status Message

Table 9-7, ECoC/ECM Restricted Data Section Detail

Restricted Section Content	Definition
ACK No.	Ascension Number for corresponding command. N/A for unsolicited status
Device Operating Mode	bit 0=0: decommissioned; bit 0=1: Commissioned; all others: reserved
Restricted Status Bits	bit 0=0: Master Alarm Off; bit 0=1: Master Alarm On; all others: reserved
Restricted Error bits	bit 7 = sensor malfunction; bit 6 = decryption error; bit 5 = invalid command; bit 4 = log overflow; bit 3 = ACK failure; bit 2= configuration failed; bit 1= sensor enable failed; bit 0 = reserved
Sensor Error Bits	bit 0=1: Lock Sensor 1 error; bit 1=1: GPS Sensor error; all others: reserved
Conveyance ID and checksum	Unique identifier for conveyance. See 0
Coordinated Universal Time	See Section 9.1.1
Alarm Status	bit 7=0: lock open; bit 7=1: lock closed; bit 6=0: hasp intact; bit 6=1: hasp broken; bit 5=0: on route; bit 5=1: off route; bit 4=0: on schedule; bit 4=1: off schedule; all others: reserved
GPS Location	see Section 0

9.5.3 Waypoint and Location Data Formats

Waypoint and location data **Shall** be in the format specified below, for all ICD use-cases. These include:

1) ECoC/ECM position reports in status and log entries
2) Waypoint/route definitions sent by the DCP

All GPS data **Shall** be directly copied from or the NMEA standard's GPRMC message, or otherwise derived. The GPRMC message is commonly provided by GPS receivers in ASCII text format, such as:

`$GPRMC,123519,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A`

For this ICD, the format is extracted as text NMEA GPRMC:

Status: One ASCII letter, with 'A' meaning the coordinates are active/valid or 'V' meaning the coordinates are void (stale) and suspect, due to lack of satellite reception/geometry. For status 'A', the time of fix is presumed to be sufficiently similar to the time of the report or log entry for this application. For status 'V', the time of fix is undefined and GPS data is the last-known location (a prior GPS solution).

Latitude:

ASCII digits, four digits, decimal point, 3 digits, and the letter N or S, as: **DDDD.DDDH**

Example: 4807.038N, meaning Latitude 48 degrees 07.038 minutes North

Longitude:

ASCII digits, five digits, decimal point, 3 digits, and the letter E or W, as: **DDDDD.DDDH**

Example: 01131.000E, meaning Longitude 11 degrees 31.000 minutes East

Radius:

Length, in meters, as four ASCII digits, with leading zeros as required.

An ICD-compliant GPS data field is the status digit followed by the latitude and longitude text, e.g.:

`A4807.038N01131.000E` i.e., exactly 20 ASCII characters for all cases.

Leading and trailing zeros **Shall** be used as needed for these fixed length fields.

9.5.4 Unrestricted Status Message from Security Device (solicited)

This message **Shall** be sent in reply to the "Send Unrestricted Status" command message.

During the process of arming the Security Device/ECoC or ECM devices, errors may occur prior to the exchange of encryption keys as detailed in [2]. These error messages may be made available to the operator in an unencrypted format. The unrestricted error message **Shall** be treated as a solicited commercial message (message type code 0x00) and be appended to the universal message header. The remaining reserved frame bytes (noted as "Reserved (n bytes)") **May** be used for vendor-specific data. This solicited status is an implicit ACK, as is the response to the restricted "NOP" command message. The message format is shown in Figure 9-7.

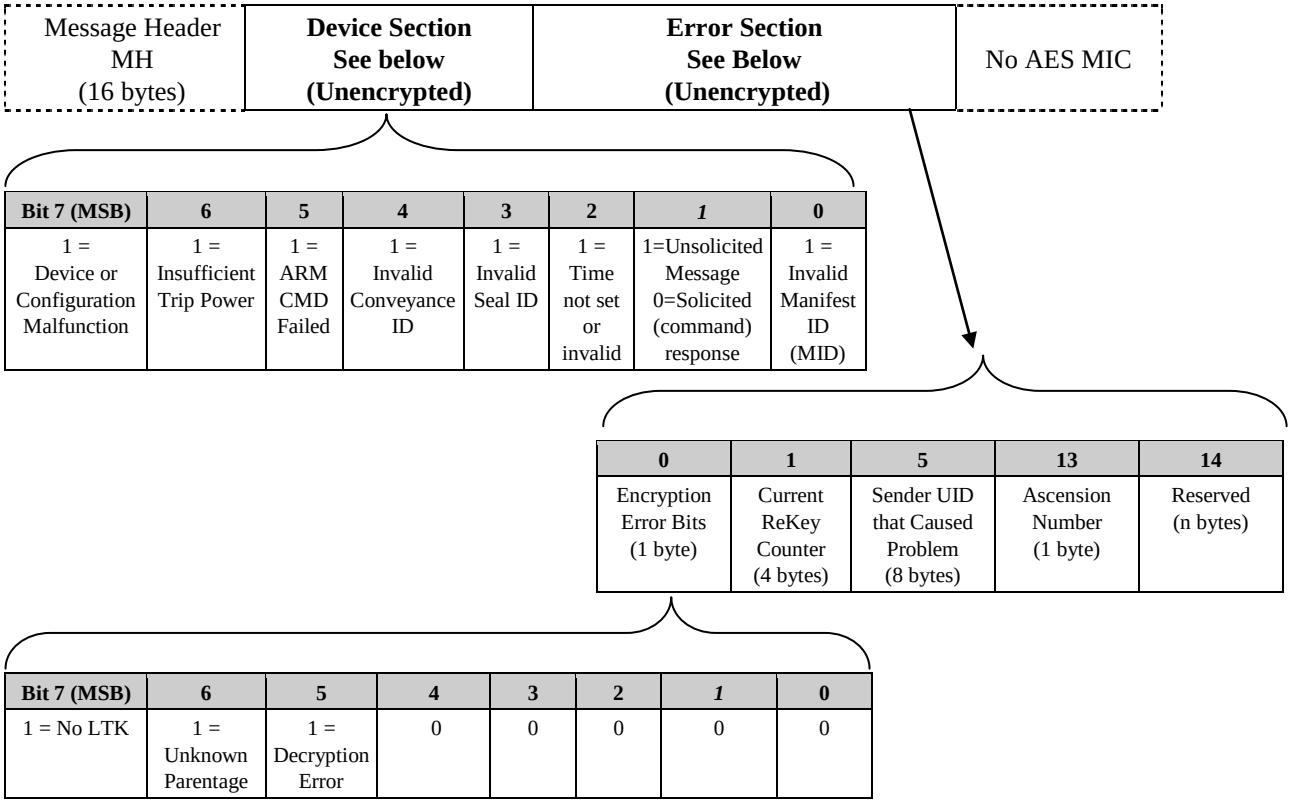


Figure 9-7, Device Status, Unrestricted Status Reply from Security Device

9.5.5 Unrestricted Status Message from ECoC/ECM (solicited)

This message **Shall** be sent in reply to the "Send Unrestricted Status" command message.

During the process of Arming the Security Device and Pairing with an ECoC/ECM, errors may occur, as detailed herein, prior to the exchange of encryption keys. These error messages may be made available to the operator unencrypted via an Unrestricted Status Message containing information about the error.

The operator must request such a message, i.e., it must be Solicited. This solicited status is an implicit ACK, analogous to the response to the restricted "NOP" command message.

The format of the Unrestricted Status Message is shown in Figure 9-8. Such an Unrestricted Status Message **Shall** incorporate the universal message header and be treated as a solicited commercial message (message type code 0x00). The remaining frame-bytes are reserved for future use. See Section 9.4.3.10 for a discussion of Ascension Numbers.

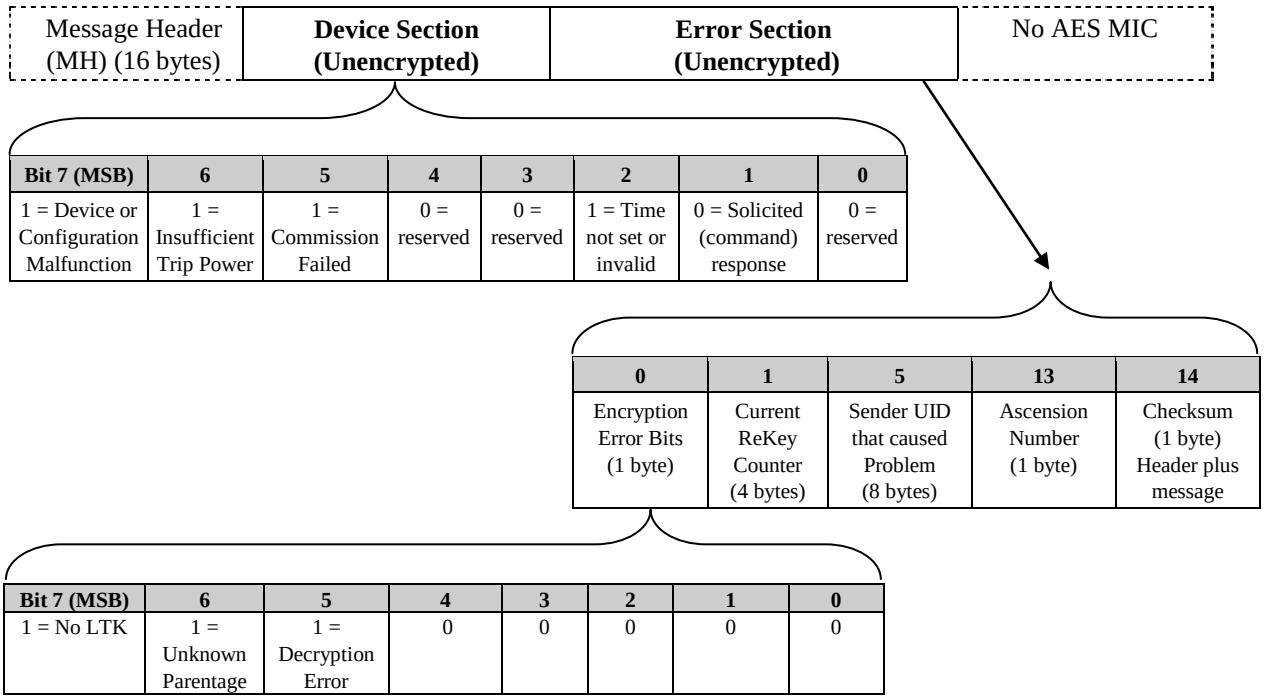


Figure 9-8, Device Status, Unrestricted Status Reply Content from ECoC/ECM

9.5.6 Unsolicited Device Status Message from Security Device

After network discovery is successful the CM **Shall** send a "presence announcement" as an unsolicited Device Status message. This message is restricted (i.e. encrypted) and is sent at the impetus of the CM. The format is described in Section 9.5.2.

This unsolicited message **Shall** be sent when communications connectivity exists (in either the primary mode or one of the secondary modes) and any of the following conditions exist:

1) An alarm or error condition exists and has not been sent with receipt-acknowledgement
2) The last Unsolicited Device Status or requested status was sent more than a nominal 10 minutes in the past, and the CM was not in secure NAD coverage during this time period.
3) The channel, PAN ID or selected NAD changed due to network discovery, since the last status message was sent.

When all of the conditions listed are false, a recurring Unsolicited Device Status message **May** be suppressed to minimize redundant messages and battery consumption in weak RF signal conditions.

9.5.7 Unsolicited Device Status Message from ECoC/ECM

If network discovery is successful, the ECoC/ECM **Shall** send an unsolicited Device Status message as a "presence announcement." This message is restricted (i.e., encrypted) and is sent at the impetus of the ECoC/ECM. The format is described in Section 9.5.2.

This unsolicited message **Shall** be sent when there is communication connectivity (in either the primary or one of the secondary modes) and any condition in Section 9.5.6.

9.5.8 Security Device/ECoC Event Log

Device event logs contain event records. Event records **Shall** be created per [1].

9.5.8.1 *Send Event Log All* Command

When a Security Device/ECoC/ECM receives a valid *Send Event Log All* command, it sends the entire contents of its event log to the requestor.

If an event record is not acknowledged by the requesting entity and the device has exhausted the retransmission limits for that message, the device **Shall** stop transmitting event records.

9.5.8.2 *Send Event Log Unsent* Command

When a Security Device/ECoC/ECM receives a valid *Send Event Log Unsent* command, it transmits all unsent event records to the requestor. An event record is considered *Unsent* if its receipt has not been acknowledged by a legitimate requestor. This includes records not sent due to transmission cessation (as in Section 9.5.8.1) and new records acquired since the last *Send Event Log (All* or *Unsent)* command.

For the purpose of responding to the *Send Event Log Unsent* command, the device **Shall** consider an event log record to be *unsent* if the event log record has either:

1) Never been sent or
2) Never been acknowledged

9.5.8.3 Event Log Records Sequence

The secure NAD or DCP sends the *Send Event Log All* or the *Send Event Log Unsent* command. When the CM receives this command, it transmits the event log as multiple messages, each containing a single event record with an ACK from the DCP or secure NAD. This command, as others, if sent more than two seconds after the last message exchange, will cause the NAD to use the NADA Message Waiting mechanism defined in this ICD for sending the command. The CM **Shall** send the message waiting response NULL message and expect the command to be sent within two seconds. The response to the command is the first log record message. The DCP or secure NAD **Shall** send a valid ACK per the ICD. A received DCP or secure NAD ACK is the indicator that the on-conveyance CM should send the next log message. Each event log that is transmitted contains, within the log record, the least significant byte ascension number of the command or subsequent ACK, for detecting lost messages. The ascension number in the message headers is used as in other messages, for detecting retransmissions or lost messages.

9.5.8.4 Event Log Message Content

In response to a Send Event Log command, the CM **Shall** respond with one or more of the event record messages, as shown below, with one event per message. If there are no logged events (empty log), the event type of the first record **Shall** indicate "End of Records".

The final (or sole) log message **Shall** be with Event Message Type = "End of Records".

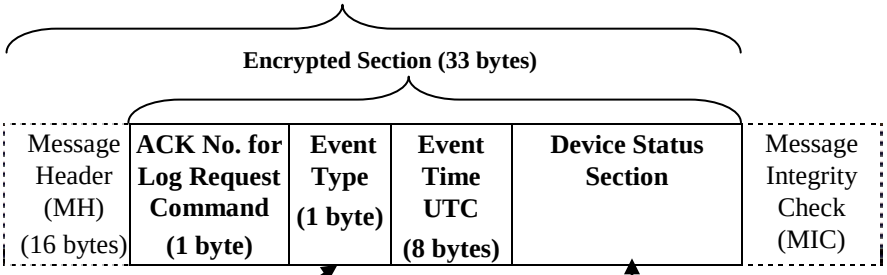
9.5.8.5 Event Log Message ACK

For each event log record message, the DCP or secure NAD **Shall** send an ICD ACK (a form of command) as shown in Section 9.6. On ACK timeout, the message **Shall** be repeated up to 5 times. On failure, the ACK FAILURE bit in the restricted status **Shall** be set true and log record transmissions **Shall** cease. The DCP or secure NAD **Shall** take appropriate action (e.g., try later, inform person, etc.).

9.5.8.6 Event Log Record Message Format for Security Devices (ACSD/CSD)

The requirements the Event Log Encryption are fully described in [4].

Device Event Log Record Message, Size (without MIC) = 16+1+1+8+22=48 bytes



Event Msg Type	Description
0xFF	End of Records or log is empty
0x00	Network Discovery Changed NAD
0x01	Change in status that was not result of a command. (Ignore Command Message Type and Command OpCode fields)
0x02	Change in status that was the result of a command. Record contains cmd OpCode
0x03	Change in alarm status (Ignore Command Message Type and Command OpCode Fields)
0x04	Fault Detection, includes Vendor Fault Code
others	Reserved

Device Status Section Bytes from Table 6-3 (22 bytes)							
Device Operating Mode (1 byte)	Restricted Status Bits (1 byte)	Restricted Error Bits (1 byte)	Alarm Status (1 byte)	Conveyance ID (16 bytes)	Door Status (1 byte)	Command Message Type (1 byte) N/A for some event record message types	Command OpCode (1 byte) N/A for some event records

Figure 9-9, Event Log Message (to DCP)

9.5.8.7 Event Type

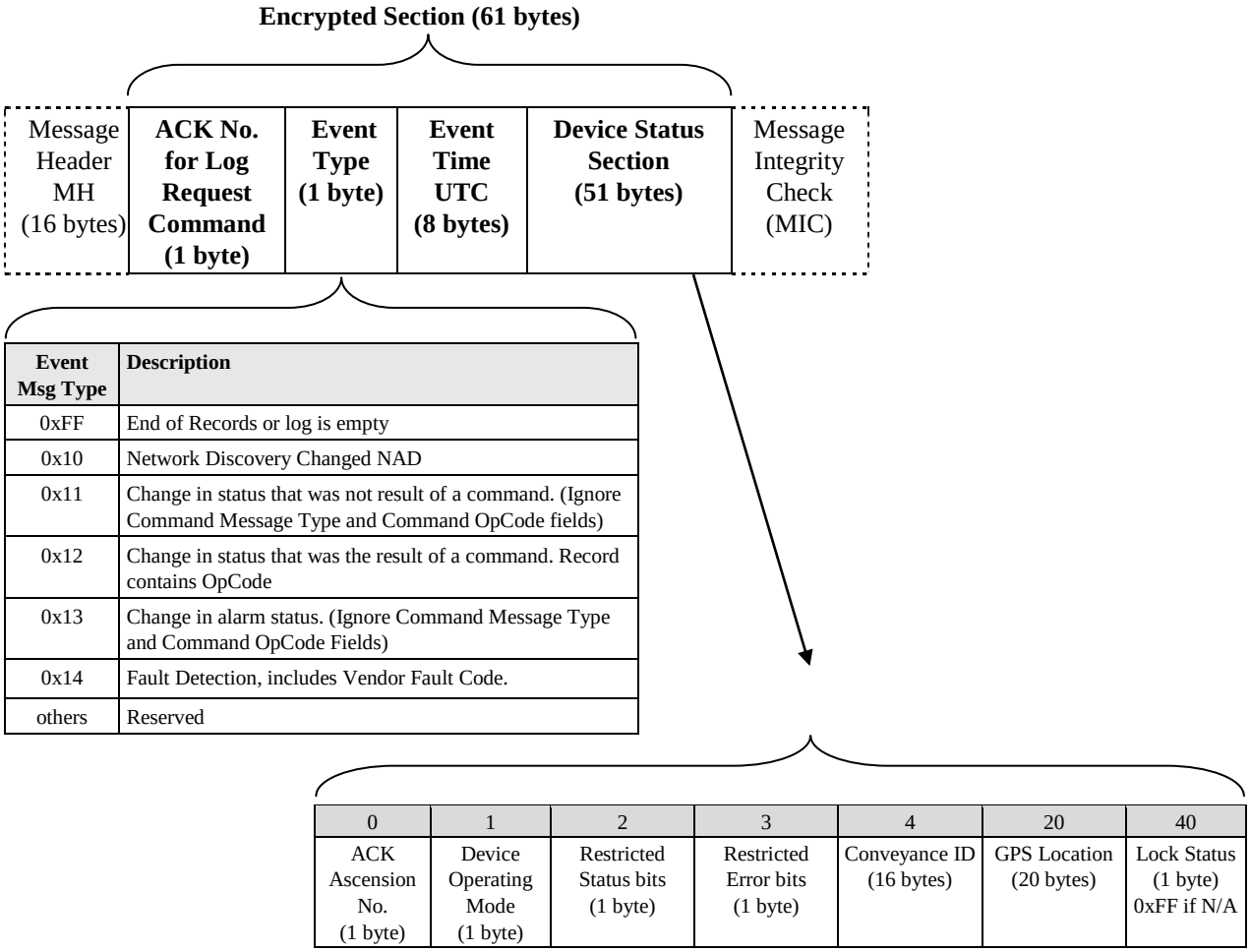
The Event Type field indicates the type of event that generated the event log message. If Event Type is equal to 0x02, the Message Type and Command OpCode fields will be populated with the appropriate values. In all other cases these two fields will be set to 0.

9.5.8.8 Restricted Section

The first three bytes of the Device Status Section are the Device Status at the time the event occurs. If the event was generated as a result of a command, the Message Type (from the MH) of the command is recorded in the Command Message Type field as well as the command OpCode.

9.5.8.9 Event Log Record Message Format for ECoC/ECM

The requirements for Event Log Encryption are declared in [4].



Event Msg Type	Description
0xFF	End of Records or log is empty
0x10	Network Discovery Changed NAD
0x11	Change in status that was not result of a command. (Ignore Command Message Type and Command OpCode fields)
0x12	Change in status that was the result of a command. Record contains OpCode
0x13	Change in alarm status. (Ignore Command Message Type and Command OpCode Fields)
0x14	Fault Detection, includes Vendor Fault Code.
others	Reserved

0	1	2	3	4	20	40
ACK Ascension No. (1 byte)	Device Operating Mode (1 byte)	Restricted Status bits (1 byte)	Restricted Error bits (1 byte)	Conveyance ID (16 bytes)	GPS Location (20 bytes)	Lock Status (1 byte) 0xFF if N/A

Figure 9-10, Event Log Message (from ECoC/ECM to DCP or secure NAD)

9.6 Command Messages from DCP or Secure NAD

Messages from the DCP or the secure NAD to the Security Device/ECoC/ECM are considered command messages. The structure of command messages is as shown below. The Message Type code shown in Table 9-3 denotes whether the command is restricted or unrestricted (not encrypted). The Security Device/ECoC/ECM **Shall** receive command messages by recognition

of its UID in the NADA Message Waiting list, and maintaining listening period not less than 2 seconds to allow receipt of the command. Once the command is received, the CM **May** resume its power conservation method.

The UID of the sending device (DCP or secure NAD) is in the message header (MH) of all command messages described in Section 9.4.3. The DCP routes the messages as a single packet to the correct locale and NAD. The structure of the command will be determined by the Message Type field in the MH.

9.6.1 Unrestricted Commands for CM

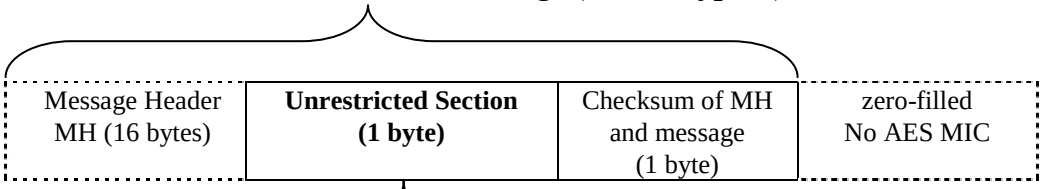
Unrestricted commands may be issued by DCP, secure NADs or non-secure NADs. The only unrestricted OpCode defined herein is *Send Unrestricted Status*, which has no parameters, and the reply for which contains only unrestricted data. Commercial-purposed ICD-Coordinated commands **Shall** use a commercial Message Type code rather than this command/response.

The message ascension number in the MH is independent of that for restricted messages.

The structure of this command message is shown in Figure 9-11. As this is a *solicited* status message, the ACK is within the response status to the command, as in the "NOP" restricted command.

The message type in the MH indicates the message is unrestricted/not encrypted.

Unrestricted Device Command Message (not encrypted)

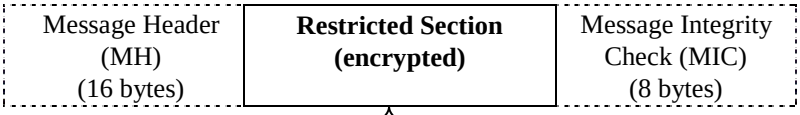


Command Name	OpCode	Required Response
Send Unrestricted Status Command	0x00	Unrestricted Status
Pair Command	0x01	CM unicasts NADA
Pairing Command Request	0x02	Unrestricted Status
Reserved	others	-

Figure 9-11, Unrestricted Command (Message Type 0xC0)

9.6.2 Restricted Security Device (ACSD/CSD) Commands

Restricted commands **May** be issued by DCPs and secure NADs to initiate a status message exchange or change the operational state of the Security Device. The message structure is shown in Figure 9-12. Every restricted command **Shall** yield a status message response, with the exception of the from-DCP ACK command from a DCP (ID=1), for which there is no response.



Security Message Command	Op Code	Required Response	Parameter 1	Parameter 2	Parameter 3	Parameter 4
NOP (no operation)	0x00	Status		(none)	(none)	
Acknowledgement (ACK)	0x01	Status	Ascension Number (1 Byte, LSB of 4-byte ascension number)	(none)	(none)	
Set In-trip State (SIS)	0x02	Status	See Table 9-9 (1 byte)	(none)	(none)	
Set Time (ST) (see also NADA msg time)	0x03	Status	8 bytes, UTC time, Format per ICD	(none)	(none)	
Arm with Trip Information (ARMT)	0x04	Status	Conveyance ID per ICD (16 bytes)	Manifest or Document ID (16 bytes)	Mechanical seal ID Right-aligned with leading spaces (15 bytes)	Sensor(s) to Enable Bit 0 = Sensor 1, etc. (1 byte)
Change Trip Information (CTI)	0x05	Status	Conveyance ID per ICD (16 bytes)	Manifest or Document ID (16 bytes)	Mechanical seal ID Right-aligned with leading spaces (15 bytes)	
Disarm From DCP (DADC)	0x80	Status	(none)	(none)	(none)	
Disarm From Secure NAD (DAHH)	0x81	Status	(none)	(none)	(none)	
Set Master Alarm = True (SMAT)	0xA1	Status	(none)	(none)	(none)	
Set Master Alarm = False (SMAF)	0xA2	Status	(none)	(none)	(none)	
Send Event Log Unsent (SLU)	0xA3					
Send Event Log All (SL)	0xA4	Status, then log records	(none)	(none)	(none)	
Erase Event Log (EL)	0xA5	Status	(none)	(none)	(none)	
NAD Enable Sensor(s) (NES)	0xA6	Status	Bit 0 = sensor 1, etc. (1 byte)	(none)	(none)	
NAD Disable Sensor(s) (NDS)	0xA7	Status	Same as above	(none)	(none)	
Configure Sensor(s) (CS)	0xA8	Status	Same as above	Size of parameter 3	Configuration Data	
Read Sensor Configuration	0xA9	Security Device-to-NAD Sensor Configuration Data Message	Sensor Number (1 byte) (0x01 = Sensor 1, 0x02 = Sensor2, etc.) Only one sensor can be queried at a time			
Sensor Pairing	0xAA	Sensor Database Report or Status (if Security Device is armed)	Sensor 1, Device Type, UID (9 Bytes)	Sensor 2, Device Type, UID (9 Bytes)	Sensor 3, Device Type, UID (9 Bytes)	Sensor N, Device Type, UID (9 Bytes) (Up to N AoSs, limited by size of 802.15.4 payload)
Sensor Database Query	0xAB	Sensor Database Report	(none)	(none)	(none)	

Figure 9-12, Restricted Command Message Structure (Message Type 0xC1)

9.6.3 Restricted ECoC/ECM Commands

Restricted commands may be issued by a DCP and some NADs to initiate a status message exchange, provision or change the operational state of an ECoC/ECM. The message structure is identical to that described in Section 9.6.2 and the ECoC/ECM commands detailed in Table 9-8.

Table 9-8, Restricted Commands for ECoC/ECMs

Security Message Command	OpCode	Required Response	Parameter 1	Parameter 2	Parameter 3	Parameter 4
NOP (no operation)	0x00	Status	(none)	(none)	(none)	(none)
Acknowledgement (ACK)	0x01	Status	Ascension Number (1 Byte, LSB of 4-byte ascension number)	(none)	(none)	(none)
Set Time (ST) (see also NADA msg time)	0x03	Status	8 bytes, UTC time, Format per ICD	(none)	(none)	(none)
Commission with Trip Information (CWT)	0x04	Status	Conveyance ID per this ICD (16 bytes)	(none)	(none)	(none)
Change Provision Information (CPI)	0x05	Status	Conveyance ID per this ICD (16 bytes)	(none)	(none)	(none)
Waypoint List New (WLN)	0x06	ACK	Last	Latitude (8-byte ASCII)	Longitude (8-byte ASCII)	Radius (meters) (4-byte ASCII)
Waypoint List Append	0x07	ACK	Last	Latitude (8-byte ASCII) Note 1	Longitude (8-byte ASCII) Note 1	Radius (meters) (4-byte ASCII) Note 1
Decommission from DCP (DADC)	0x80	Status	(none)	(none)	(none)	(none)
Decommission From secure NAD (DAHH)	0x81	Status	(none)	(none)	(none)	(none)
Set Master Alarm = True (SMAT)	0xA1	Status	(none)	(none)	(none)	(none)
Set Master Alarm = False (SMAF)	0xA2	Status	(none)	(none)	(none)	(none)
Send Event Log Unsent (SLU)	0xA3					(none)
Send Event Log All (SL)	0xA4	Status, then log records	(none)	(none)	(none)	(none)
Erase Event Log (EL)	0xA5	Status	(none)	(none)	(none)	(none)

Note 1: Waypoint coordinate formats are:

Latitude: Per section 0

Longitude: Per section 0

Radius: Per section 0

9.6.4 No Operation (NOP) Command Message from DCP or Secure NAD

Response by CM is Status (Restricted). No other action taken.

9.6.5 ACK Message from DCP or secure NAD

The DCP or secure NAD **Shall** send an ACK for the message number given in parameter 1 after error free receipt from the CM. Successful ACKs **Shall** not be logged.

9.6.6 Disarm Command Message from DCP or Secure NAD

Upon receipt of the Disarm command from a DCP or secure NAD (OpCode 0x80), the Security Device **Shall** successfully download the entire event log to the commanding DCP or secure NAD and erase the event log before executing the Disarm command.

9.6.7 Decommission Command Message from DCP or Secure NAD

Upon receipt of a Decommission command from a DCP or secure NAD (0x81), the ECoC/ECM **Shall** successfully download the entire event log to the commanding DCP or secure NAD and erase the event log before executing the Decommission command.

9.6.8 Set In-trip State

Parameter 1 of the Set In-trip State command is defined in Table 9-9. The purpose of this optional command is for DCP or secure NAD to indicate the conveyance's in-trip state to assist the device in battery conservation, e.g., reduced frequency of network discovery or suitable changes in sensor management.

Table 9-9, Set In-Trip State Parameter Values for CM Restricted Commands

Parameter 1	Low Vulnerability	Increased Vulnerability	Situation
0	-	-	Undefined situation
1	-	-	
2	**X**		No cargo present
3		**X**	
-			
10	**X**		In transit by conveyance prior to embarkation
11		**X**	
12	**X**		In storage prior to embarkation
13		**X**	
-			
20	**X**		In maritime trip or transshipment
21		**X**	
22	**X**		In over-trucking-road trip or transshipment
23		**X**	
24	**X**		In over-railway trip or transshipment
25		**X**	
26	**X**		In air trip or transshipment
27		**X**	
-			
30	**X**		In storage after debarkation
31		**X**	
-			
Add 256 to above			**Exercise, training or test**

9.6.9 Garbled Application Layer ACKs Received by On-Conveyance Devices

Application layer ACKs exchanged between DCP or secure NADs and Security Device/ECoC/ECMs may become garbled or lost. If an anticipated Application ACK is received but is unreadable or not received within the allowable the two-second timeout by an on-conveyance device, the on-conveyance device **Shall** re-send the identical message as described in Section 9.3.1, repeated no more than 5 times for a single message or until a valid ACK is received from the DCP or secure NAD.

If retries are exhausted, the on-conveyance device will cease retries for a period of time not to exceed 1 minute for that sender (DCP or secure NAD) UID. When the next network discovery succeeds, the current status of the on-conveyance device **Shall** be reported in the usual unsolicited status message.

9.6.10 Garbled Application Layer ACKs Received by DCPs or HNADs

In response to every DCP or secure NAD command, except the ACK message, the conveyance device CM, per this ICD, sends a response. The response, for most commands messages is restricted status with the “is unsolicited” bit false, meaning the response was solicited. The response to Send Log is not status, but rather is a log record. In both cases, the response contains the least significant byte of the command message’s ascension number. The DCP or secure NAD uses this for error detection, e.g., lost message detection.

If a response is received but unreadable by a DCP or secure NAD, or is not received within the allowed timeout, the DCP or secure NAD **Shall** send the Command Message as described in Section 9.6.3, repeated no more than 5 times for a single message or until a valid response is received from the addressed CM. Each re-sent message will be noted in the DCP data base or secure NAD Activity Log (this special situation is not covered in the Section 9.7 ladder diagrams). After 5 unsuccessful attempts, the DCP will store that message and forward it at the next message transmission opportunity. After 5 unsuccessful attempts, the secure NAD will record the error condition in its Activity Log and the operator will take corrective actions. These actions are the responsibility of the secure NAD operator and are beyond the scope of this ICD.

9.7 Routine Messaging Ladder Diagrams

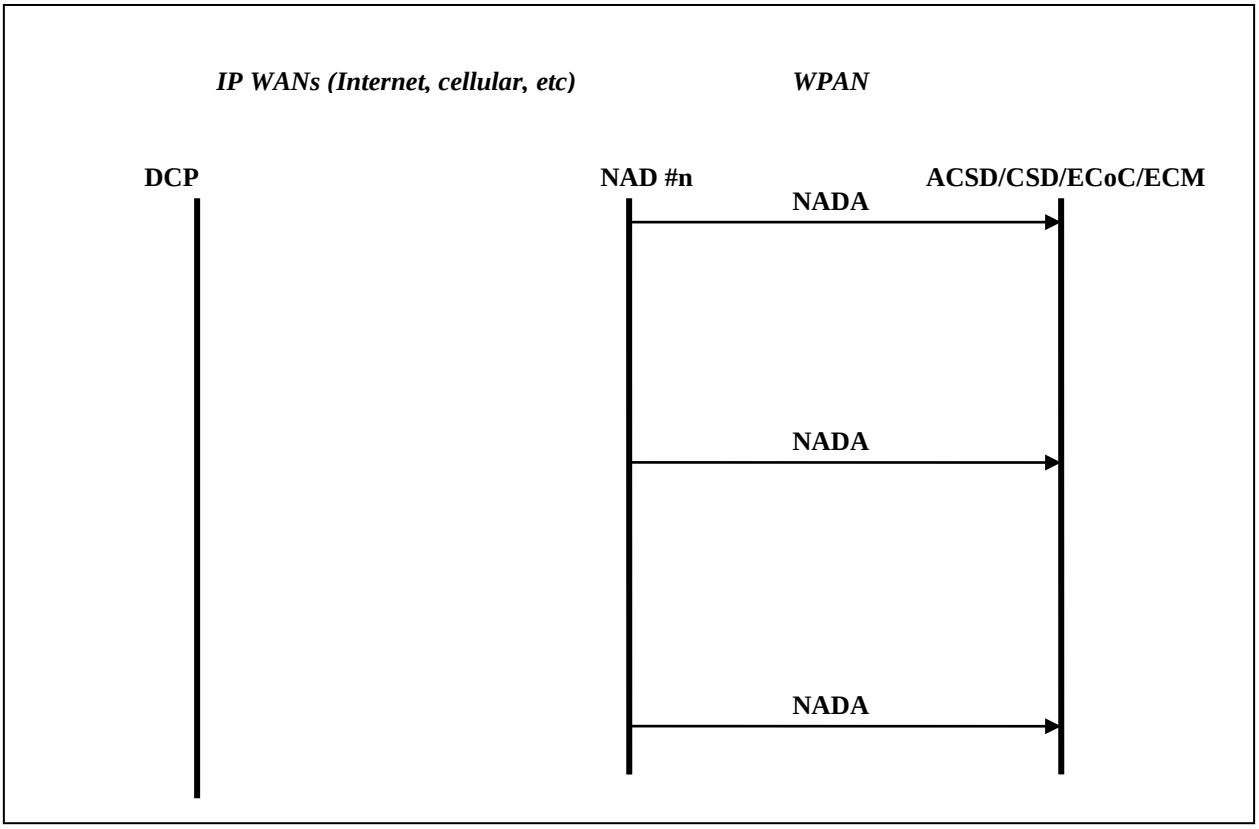
9.7.1 Broadcast Network Discovery Ladder Diagram for NAD Function

Prerequisite: None

Depicts *Passive Scan* network discovery using NADA. The CM does no transmissions.

Active Scan network discovery is not required by this ICD and is not depicted. Any Active Scan implemented for commercial-purposed network discovery **Shall** implement clear channel assessment (CCA) in some form and **Shall Not** interfere with the Passive Scan method described here. A NAD **Shall** perform CCA before transmitting a NADA (or any other) data frame.

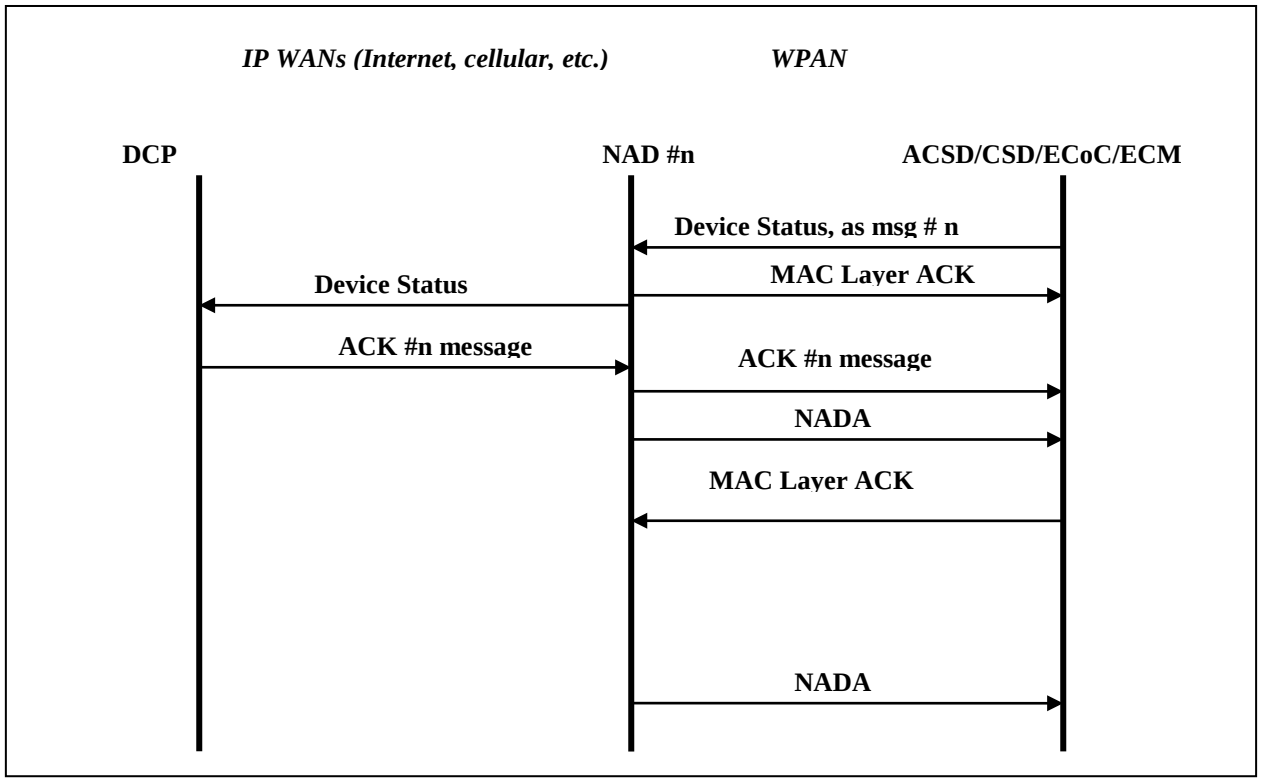
The Security Device is regarded as State Aware and may choose to not to "wake up" for every NADA message, subject to the requirements of Section 5.1.7.



9.7.2 Unsolicited Device Status Message (to DCP or secure NAD) Ladder Diagram

Prerequisite: Network Discovery Complete. Trigger criteria are given in Section 5.1.7.

CM performs clear channel assessment before transmitting.

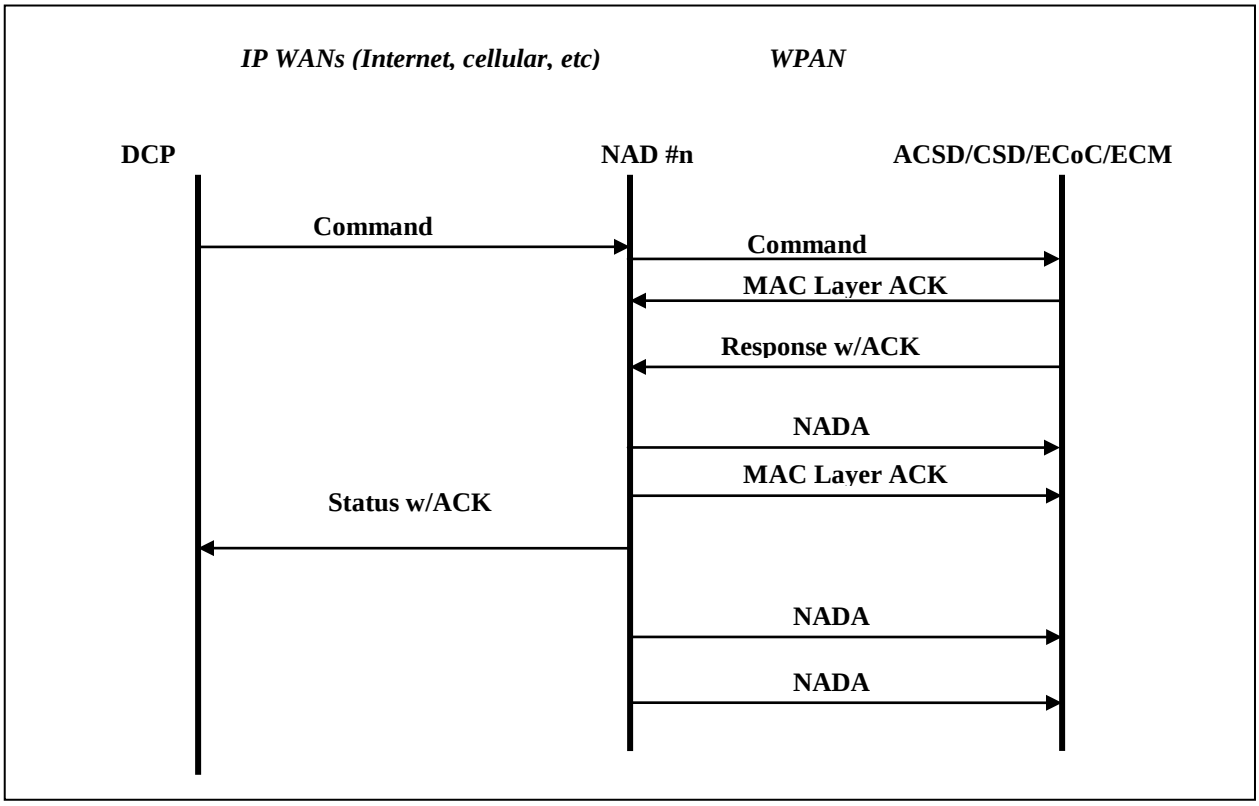


The above is not to time scale. The duration of the Device Status message transmission is small compared to the NADA message repetition interval. The MAC Layer ACK frame is sent within the time duration specified by IEEE Standard 802.15.4-2006.

The time delay for LAN/WAN messages NAD to/from DCP **Shall** be compatible with the two-second timeout for ACKs and the time window for suppressing message waiting, e.g., for successive log records.

9.7.3 DCP or Secure NAD-Originated Message Ladder Diagram

Prerequisite: Network Discovery complete. DCP knows which NAD to use based on unsolicited Device Status message sent after Network Discovery. Optionally, DCP use the last known NAD.

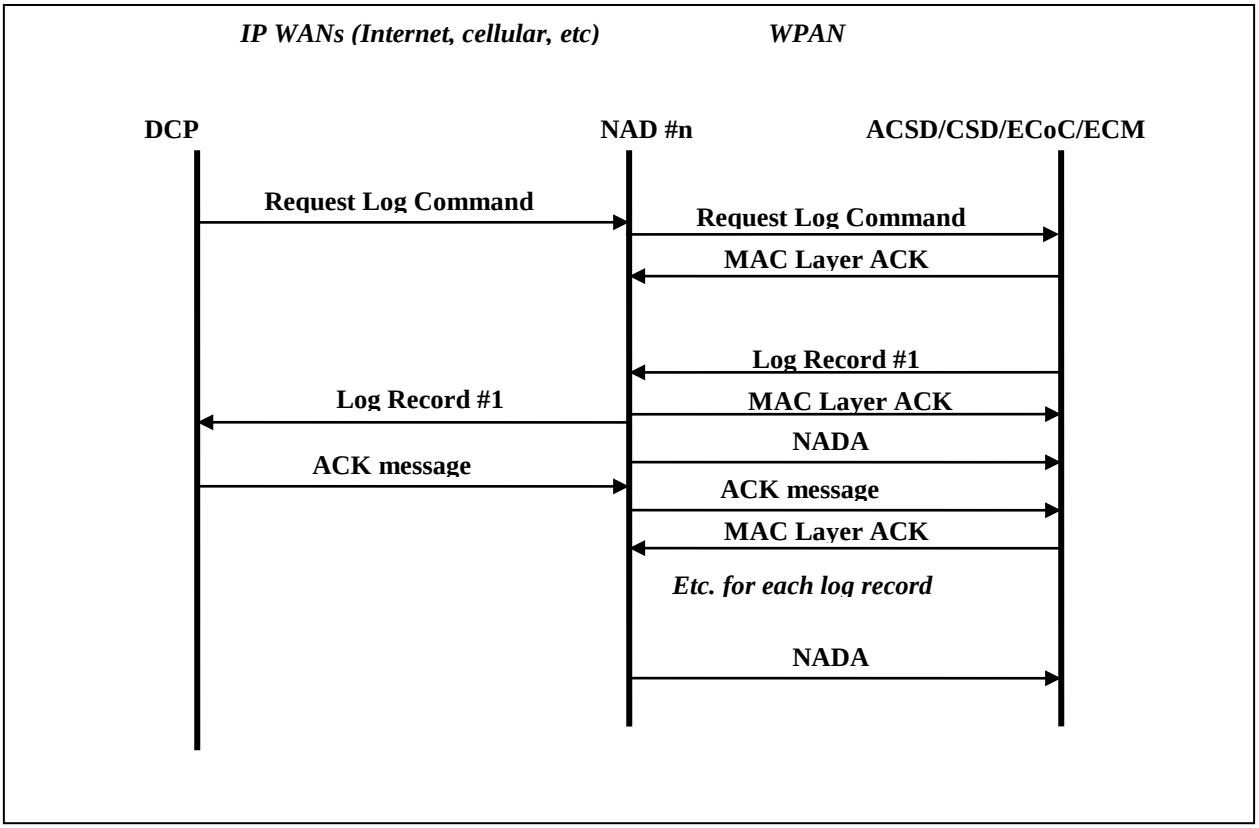


The above is not to time scale. See discussion in prior section. If the DCP does not receive the ACK #n, the DCP **Shall** timeout and repeat the command. If the command yields response data such as status, a CM to DCP message is sent by the CM after sending the ACK #n to the DCP. The procedure for this is the same as for the Device Status message shown in Section 9.7.2.

Note: MAC Layer ACKs **Shall** comply with IEEE Standard 802.15.4-2006 in both content and timing.

9.7.4 Event Log Message / Responses Ladder Diagram

Prerequisite: Network Discovery complete.



The above is not to time scale. See discussion in Section 9.5.8.

The response to Send Log Command **Shall** be one or more log records. If the log is empty, the response **Shall** be one record with record type = end of log. After a secure command to purge the log, that command will be the first entry in the log.

The DCP **Shall** send an ACK command with the proper ascension number on receipt and storage of each log record.

10 Message Information Assurance (IA) and Security

Information Assurance (IA) is performed at the application message level, thus it is not specified in the MAC and PHY sections but rather, is in this section.

Messages to and from the on-conveyance devices contain encryption, authentication, message integrity checks, and anti-spoof mechanisms that are:

1) Compliant with the most stringent information protection policies among international locales
2) Independent of all transport media between the DCP and the on-conveyance device. This may be any number of inter-working networks, WPAN, WLAN, LAN, WAN.

As shown in Figure 9-2, and elsewhere in this section, command messages from a DCP or secure NAD and replies and status messages from an on-conveyance device contain a section of payload data that is encrypted.

10.1 802.15.4 Wireless Network Interference Mitigation

10.1.1 Irrelevant Wireless PANs at Locale

The process for ignoring irrelevant but valid transmissions on “external” networks **Shall** be as follows. The CM may receive WPAN signals from adjacent or malicious networks other than the intended network. This irrelevant network may have a PAN ID that appears valid. In such a case, the CM would attempt to transmit messages as described herein.

This ICD requires that a secure (encrypted) ACK must be received by the CM from a DCP or secure NAD as the response to the first message. This first message is encrypted, and sent by a CM after network discovery. The means for encryption and mutual authentication will preclude this exchange with other than a bona fide DCP or secure NAD, irrespective of the WPAN access devices.

Commercial-purposed messages conforming to this ICD should provide an equivalent means.

10.1.2 Persistent Interference or Denial of Service (Wireless)

The implementation, irrespective of this ICD, **Shall** detect persistent interference on any of the active WPAN and automatically or manually cause correction. This correction **May** be to change NADs to an unused channel among the ICD-defined channel set or eliminate the source. The CMs **Shall** restart Network Discovery after a channel change. The mechanism for detection of persistent interference is not in the IEEE 802.15.4-2006 Standard and is to be determined by implementation authority through a method of jamming detection locally.

10.2 Counterfeit and Stolen Devices

See [4].

10.3 Mutual Authentication

See [4].

10.4 Data Security

See [4].

11 Wireless Links to Relays and Add-on Sensors

11.1 Relays (External to Conveyance)

An ECoC/ECM **May** act as a transparent relay device on behalf of a "paired" Security Device as described in Section 4.2.8. A security device **Should** communicate with a NAD in preference to a relay device when signal quality conditions permit. At any given moment, there **Shall** be only one (1) device functioning as a relay for a paired Security Device on any conveyance with the messaging relay functions described in Section 4.2.8.3. A paired ECoC/ECM **May** simultaneously provide additional functions while acting as a relay. Non-relay functions that send and receive messages **Shall** pass messages whose content is independent of the content in relayed messages. Messages for non-relay functions **Shall Not** be co-mingled with the same messages as relayed Security Device messages.

The ECoC/ECM transparent relay function **Shall Not** be capable of decrypting messages to/from the paired Security Device. The DCP or secure NAD will ensure that encryption keys will differ from those used for non-relay ECoC/ECM secure functions.

For paired devices, the following apply:

1) The ECoC/ECM paired devices **Shall** conduct network discovery via the NAD's NADA message as described in Section 5.1.6.
2) Messages relayed by a paired device **Shall** be retransmitted only to the MAC address of its paired Security Device or the NAD (i.e., unicast, not broadcast).
3) The paired device providing this relay function **Shall** forward and return without alteration all ICD messages, including status messages, commands, and acknowledgements.
4) The device providing this relay function **May** relay non-ICD data packets.
5) An ECM **Shall Not** relay HNAD NADA messages when paired with a Security Device.
6) A Security Device paired with an ECoC/ECM **Shall** be capable of determining whether the pairing has been broken (e.g., by removal or loss of the ECoC/ECM) within 2 minutes of occurrence.
7) After successful pairing, if pairing is broken, the Security Device **Shall** respond to all NADA messages from HNADs and FNADs.
8) A Security Device in the *Armed* state **Shall** ignore all Pairing Commands from HNADs and Pairing Request Commands from ECoC/ECMs.
9) If a paired device loses power, it **Shall** revert to an unpaired state.

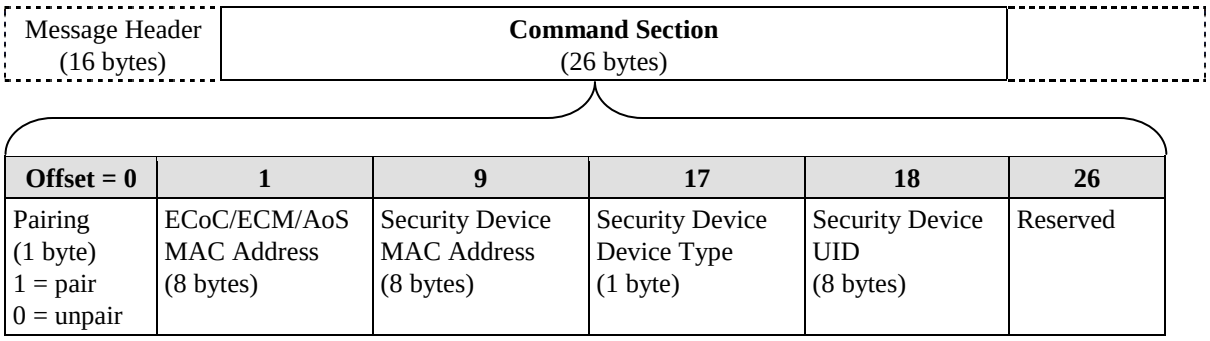
11.1.1 Method of Pairing – Security Devices and ECoC/ECMs

The Pairing process starts with an unarmed Security Device mounted in a conveyance with the doors closed. Encryption is not required to conduct Pairing. The ECoC/ECM is in an equivalent state (pre-commission, if applicable; again, encryption is not required to conduct Pairing). The ECoC/ECM is mounted on the external surface of the conveyance above the (closed) door. The HNAD used for Pairing is powered "on" and may possess valid encryption keys for the Security Device and ECoC/ECM, but the encryption key(s) are not used in Pairing. The following Pairing process description is provided with the intent of ensuring interoperability.

1) Discovery – The HNAD **Shall** send out a NADA per Section 5.1.6 containing the HNAD's UID. The Security Device responds with an unsolicited status message. The

HNAD then stores the Security Device's UID and MAC address. If the Security Device possesses an encryption key shared by the HNAD, the HNAD will acknowledge. Otherwise, the encryption error process of Section 9.3 will be executed. In either event the HNAD will have identified and stored the Security Device's UID and MAC address for use. The ECoC/ECM then responds with an Unsolicited Status Message with its MAC address in the Message Header and all zeros (0) in the body of the status message. The HNAD stores the ECoC/ECM UID and MAC address without transmitting an application layer acknowledgement. For the ECM, the UID **May** be the MAC address.

2) Command Initiation – During discovery, it is likely that multiple Security Devices and ECoC/ECMs will respond. Using the HNAD, the user selects the Security Device to be paired identifying it by the UID displayed on the HNAD screen. The user then selects the ECoC/ECM to be paired from the user interface. This could either require key-in of a known ECoC/ECM MAC address or a display field of ECoC/ECM MAC addresses generated during the discovery process above. The user then executes the Pairing Command from the user display (message type 0xC0, OpCode 0x01) which his heard by both the Security Device and the ECoC/ECM.. There is no application layer message sent back. The parameters of this command are shown in Figure 11-1.
3) Pairing Command Execution – The ECoC/ECM then responds by sending out a unicast NADA with the Security Device's UID in the message waiting list and the ECoC/ECM MAC address in the Level 2 Field of the NADA (normally HNAD, see Table 5-3). The Security Device responds with a NULL message as described in Section 5.1.7.4. If the ECoC/ECM does not hear this NULL and does not send a Pairing Request Command within two (2) seconds, the HNAD **Shall** re-send the Pairing Command. If the ECoC/ECM hears this NULL, the ECoC/ECM **Shall** send a Pairing Request Command (message type=0xC0, OpCode 0x02) to the Security Device. The ACSD/CSD response to this command **Shall** be an Unrestricted Status message per Section 9.5.4. (The ACSD/CSD must check the Message Header of the Pairing Request Command to ensure the ECoC/ECM MAC Address matches.) If successful, the ECoC/ECM **Shall** relay the Unrestricted Status Message received from the ACSD/CSD to the HNAD. If the HNAD does not receive the Unrestricted Status Message from the ACSD/CSD after two (2) seconds, the HNAD **Shall** re-send the Pairing Command.
4) Pairing Completion – the Security Device **Shall** assume it is paired at this point and accept FNAD Commands from the paired ECoC/ECM MAC address until a Pair Command is received with Pairing Byte set to zero or the Security Device is disarmed. Upon receipt of the Unsolicited Status message by the HNAD (sent from the paired ECoC/ECM), the HNAD **Shall** consider the pairing process successful. A paired ECoC/ECM **Shall Not** respond to HNAD NADAs until unpaired.



Offset = 0	1	9	17	18	26
Pairing (1 byte) 1 = pair 0 = unpair	ECoC/ECM/AoS MAC Address (8 bytes)	Security Device MAC Address (8 bytes)	Security Device Device Type (1 byte)	Security Device UID (8 bytes)	Reserved

Figure 11-1, Pairing Command

11.1.2 Method of Unpairing

A paired Security Device **Shall** become unpaired if it executes the Disarm command or if it is power cycled. The ECoC/ECM **Shall** become unpaired if it executes the Pairing command with the Pairing Byte (Byte 1) set to zero or is power cycled.

11.1.3 Pairing Keep Alive

If a paired Security Device fails to hear an FNAD NADA relayed by its paired ECoC/ECM over any 2-minute interval (while hearing an FNAD directly), the Security Device **Shall** respond to the next ICD-compliant FNAD NADA. Security Devices **Shall** respond to all ICD-compliant HNAD NADAs irrespective of pairing status.

11.1.4 Pairing Sensor CMs and Relay Devices

Non-Security Device sensors mounted inside of a conveyance **May** be similarly paired to an external relay device. For all other device pairing combinations, the pairing method is the same as above where the generic internal sensors are substituted for the Security Device and any other type of relay device is substituted for the ECoC/ECM.

11.2 Add-on Sensors (Internal to Conveyance)

An Add-on Sensor (AoS) is a device that communicates directly to a Security Device via the wireless AoS bus. There can be up to five (5) AoSs per Security Device (in addition to one (1) relay device, such as an ECoC Device or an ECM, as described in Section 11.1), which can be of multiple and mixed functions (e.g. humidity, temperature, etc.). Unless otherwise specified, messages and protocols described below refer to an AoS as an integrated unit, not to the individual sensors within a device unit. All wireless communications directly with the Security Device **Shall** adhere to this ICD.

AoSs that adhere to this ICD may play a direct or indirect role in:

1) Executing Commands: Sensor enable/disable, status inquiry, etc.
2) Status change reporting
3) Wireless interface to Security Device
4) Implementing common message formats for Security Device to AoS communications
5) Adhering to common application protocol for error detection and correction

11.2.1 ACSD to Add-on Sensor, Wired Bus Connection

The Security Device **Shall Not** accept or accommodate wired bus connections to AoSs that are not integral to the Security Device.

11.2.2 Possible Add-on Sensor Topologies

Communications between the Security Device and AoSs **Shall** adhere to this document. This ICD allows only for topologies where at least one AoS communicates directly with the Security Device.

11.2.3 Security Device to Add-on Sensor Wireless Medium

Wireless add-on sensors **Shall** use the same *ad hoc* network protocols, MAC, and PHY as the Security Device, with the following differences:

1) Routing method is optional (a battery life consideration)
2) The network discovery for sensors during the Arming Process procedure differs and is defined in Section 11.2.7.

This ICD has a message category for Sensor-to-Security Device messages, distinct from Security Device-to-NAD messages (and NAD-to-Security Device messages).

11.2.4 Wireless Medium Physical Layer

The Wireless Medium Physical Layer for AoSs **Shall** be identical to that described in Section 6.

11.2.5 Wireless Medium, Data Link Layer

The Wireless Medium Data Link Layer **Shall** be identical to that described in Section 6.1 with the exception that transmitter power **Shall Not** exceed zero (0) dBm EIRP.

11.2.6 Wireless Data Frame Content

The Wireless Data Frame Content **Shall** be as described in Section 9.5.

11.2.7 Method of Pairing Security Device and Add-on Sensors

Before a sensor can communicate with a Security Device, the two must be paired. Pairing ensures that a sensor(s) will only communicate with a desired Security Device, and that the Security Device will securely communicate with the desired sensor(s). The pairing process needs to take place every time a new sensor is added or removed from the conveyance or a new Security Device is assigned to the conveyance. Personnel **Shall** confirm that the AoS(s) and the Security Device have established successful pair-wise communications per this ICD as the final step in the process of installing a new sensor.

The Pairing process starts with an unarmed Security Device mounted in a conveyance with the door(s) closed. The Security Device **Shall** have the encryption key installed; encryption is required to conduct Pairing with an Add-on Sensor. The AoS (note: there may be multiple AoS) is not required to possess a valid encryption key when starting this process. All AoS pairing is conducted using an HNAD. The following detailed description of the pairing process is provided with the intent of ensuring interoperability for paired sensors. The Add-on Sensor pairing sequence is illustrated in Figure 11-2.

1) The pairing process for an Add-on Sensor (AoS) (Section 11.2) begins with each desired sensor's device type and UID input by the user into the HNAD or discovered by the HNAD using NADAs. Transmitting these parameters to the Security Device will ensure that the Security Device does not accidentally pair with sensors in adjacent conveyances. After having entered or discovered all required sensor information, the user will send the Sensor Pairing command from the HNAD to the Security Device with up to 5 sensor device types and UIDs. Note that space limitations of the 802.15.4-2006 protocol and previously described ICD requirements that forbid message fragmentation limit the number of Add-on Sensors that can be transmitted in a single Sensor Pairing command.
2) Discovery – The HNAD sends out a NADA per Section 5.1.6. The Security Device responds with an unsolicited status message. The HNAD then stores the Security Device's UID and MAC address. The AoS(s) respond with an Unsolicited Status Message (with the MAC Address in the Message Header) and all zeros (0) in the body of the status message. The HNAD stores the AoS MAC addresses for selection by the user. (The Security Device and the AoS(s) will derive and store fixed encryption keys for the AoSs based on the AoS UID and Serial Number as described in [2]. These keys will be shared unaltered by the Security Device and AoS for the duration of the pairing.)
3) Command Initiation – During discovery, it is likely that multiple Security Devices and AoS(s) will respond. Using the HNAD, the user selects the Security Device to be paired, identified by its UID displayed on the HNAD screen. The user then selects the AoS(s) to be paired from the user interface. This could either require key-in of one or more known AoS MAC addresses or select from a set of displayed AoS MAC addresses found during the discovery process above. The selected AoS information is then sent to the CSD UID (identified in the discovery process above) as described in Reference [2].
4) When the Security Device receives the AoS MAC Addresses and UIDs from the HNAD, it **Shall** transmit the Sensor Discovery Broadcast message to the IEEE Standard 802.15.4-2006 broadcast address.
5) Disabled sensors that receive the Sensor Discovery Broadcast message **Shall** respond with a Sensor Status message. (Enabled sensors that receive the Sensor Discovery Broadcast message are discussed below.)
6) Once the Security Device receives the Sensor Status message, it compares the sensor's UID to the list of user-inputted sensors (from Step 3). If there is a match, the Security Device **Shall** transmit the Set Gateway Security Device command from Figure 11-4 to the sensor MAC Address.
7) When the sensor receives the Set Gateway Security Device command, it **Shall** limit its communication to its gateway Security Device alone and acknowledge this message by sending an encrypted Sensor Status message. Receipt of the encrypted Sensor Status message and successful decryption by the Security Device verifies successful pairing.
8) These steps **May** be executed for up to five (5) AoS on the user inputted list simultaneously paired to a single Security Device.
9) Upon completion of the pairing process, the Security Device **Shall** transmit an encrypted Sensor Database Report (see Section 11.2.7.1) back to the commanding HNAD.

***Case: Security Device Operating Mode is* Not Armed**

Once the Security Device receives the Sensor Pairing command, it **Shall** transmit the Sensor Discovery Broadcast (Security Device NADA) message to the IEEE Standard 802.15.4-2006 broadcast address only if it is in the disarmed state. The Security Device **May** transmit several Sensor Discovery Broadcast messages in succession to ensure that all sensors in the conveyance receive the message.

***Case: Security Device Operating Mode is* Armed**

The Security Device **Shall Not** proceed with the pairing process if it is already in the Armed state and **Shall** simply respond to the HNAD with a Status message indicating its Armed state.

After the Security Device transmits the Sensor Discovery Broadcast message, it **Shall** wait no more than 3 seconds for a response. Each time the Security Device receives a new response, it will reset its timer to 3 seconds. After this timer times out, the Security Device **Shall** no longer accept responses from sensors.

Case: Sensor is disabled

Once a sensor receives the NADA message from a Security Device, it **Shall** respond immediately with a Sensor Status message if it is in the disabled state.

Case: Sensor is enabled

If the sensor is in the enabled state it will first attempt to communicate with its current gateway Security Device by sending a Sensor Status message. If the sensor receives an acknowledgement from its gateway Security Device, it will not respond to the Sensor Discovery Broadcast message. This is to prevent malicious Security Devices from being able to pair with enabled sensors.

Enabled sensors **Shall Not** be allowed to pair with alternate Security Devices.

Once the Security Device receives the Sensor Status message, it compares the sensor's source UID with the list of sensor UIDs that was selected by the user. If there is a match, the Security Device **Shall** transmit via a unicast packet a Set Gateway Security Device command in Figure 11-4 to the sensor. If the Security Device receives a Sensor Status message from a sensor that is not on the list of sensors input by the user, the Security Device **Shall Not** respond to the sensor. Once the sensor receives the Set Gateway Security Device command, the sensor **Shall** limit future communication to only its Gateway Security Device. The sensor is required to respond with a Sensor Status message that acknowledges receipt of the command. Once the Security Device receives and successfully decrypts the Sensor Status message, the pairing process for that particular sensor is complete. The only way to change the sensor's gateway Security Device is to perform the pairing process again (CSD Unarmed and Sensor unpaired/disabled).

When the Security Device has received all Sensor Status messages sent by sensors in response to the Set Gateway Security Device command, the Security Device **Shall** overwrite the Sensor Database described in Section 11.2.7.1 with the sensors it has received responses from. If the Security Device does not receive a response from a desired sensor after 5 retransmissions of the Set Gateway Security Device command, it **Shall** assume the pairing process with that sensor failed and **Shall Not** include the sensor in the Sensor Database. The Security Device will then respond to the commanding NAD with a Sensor Database Report message.

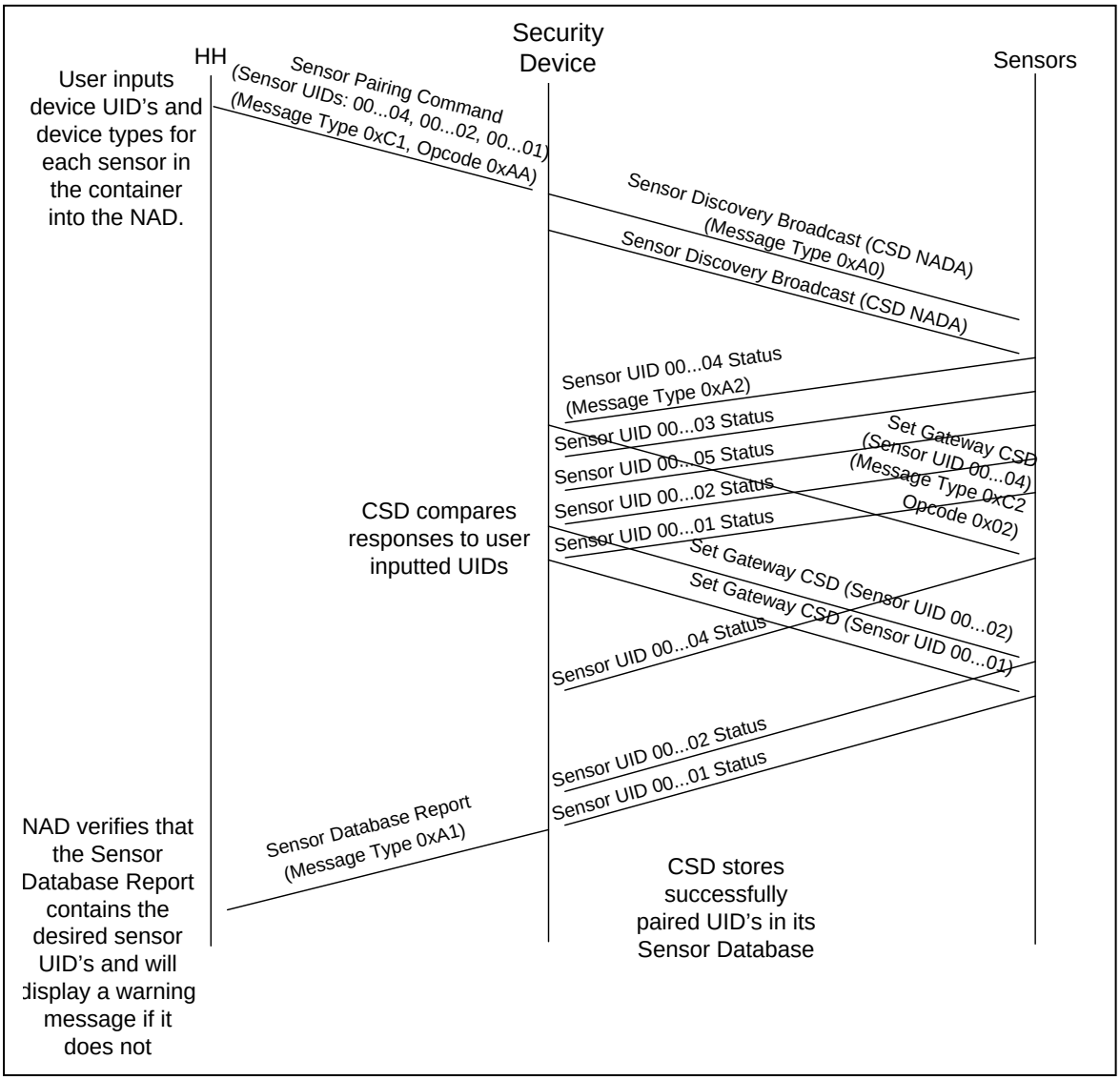


Figure 11-2, Add-on Sensor Pairing Sequence Ladder Diagram (Security Device is CSD)

11.2.7.1 Sensor Database

The Sensor Database is stored in the Security Device and contains the Device Types and UIDs of sensors that the Security Device has successfully paired with and is thus in control of. The Sensor Database is written during the last step of the pairing process described above in Section 11.2.7. The contents of the Sensor Database are queried with the Sensor Database Query command and returned in the Sensor Database Report message. The order that the sensors are returned in the Sensor Database Report message corresponds to their positions in the Security Device's Sensor Database. For example, the first sensor in the Sensor Database Report will also be the first sensor in the Sensor Database, and will be designated sensor 1. Commands such as "Disable," "Enable," and "Configure Sensor" contain a sensor number bitmap parameter that specifies the target sensor(s) by their sensor number(s).

11.2.8 Network and Application Protocol

The Network and Application Protocol for Wireless Add-on Sensors **Shall** be as described by the IEEE 802.15.4-2006 Standard and Section 6.

11.2.8.1 Retransmissions and Acknowledgements

For all communications (unless otherwise noted), it is the responsibility of the initiator of communications to ensure that a message has been received by the receiver. Upon sending a message, the sending device will wait for a response. If the sending device does not receive the expected response after 2 seconds, it will retransmit its initial message. This will be repeated up to 5 times at which point the sending device user will take action appropriate to the situation.

The receiving device of a message will not be required to retransmit multiple responses based on a timeout value. The receiving device will retransmit a response only if it receives a duplicate message from the sending device.

The Sensor/Security Device Acknowledgement command will only be sent by the Security Device in response to an unsolicited status message or alarm issued by a sensor.

11.2.8.2 Add-on Sensor (AoS) Status Message

This message is sent when:

1) A valid Status Request command from the Security Device is received by the Add-on Sensor (AoS). For this case, the Unsolicited Status bit is false in the unrestricted status field of the status message. The ACK No. field **Shall** contain the Ascension Number from the message header of the Status Request command. The Security Device may validate using this number.
2) An “alarm” event has occurred. For this case, the Unsolicited Status bit is true in the unrestricted status field of the status message.

   Note: The Sensor Alarm Status byte, byte 3 of the Add-on Sensor Status Message differs from the Alarm Status byte, byte 51 of the Device Status Message. The Sensor Alarm Status byte acts as a status bitmap for up to 8 different sensors where a set bit means that the sensor has alarmed and a cleared bit means no alarm.
3) A Status message is required in the pairing process described previously

The status message header (Figure 9-3) **Shall** include device type (0x83) for wireless Add-on Sensors (AoS). The device codes can be seen in Table 9-2.

On change of alarm status, the AoS **Shall** generate an ICD-compliant status message and send it to its Gateway Security Device set at pairing. A MAC-layer sensor/Security Device ACK will confirm receipt by the Security Device. From there the Security Device is responsible for recomposing the status and error bytes for local storage in the Security Device event log and eventual delivery to the Data Consolidation Point. The Security Device/CM will set the appropriate bit in the “Restricted Status Bits” section to identify which AoS produced the alarm.

Encryption and key management of AoS data are discussed in [4].

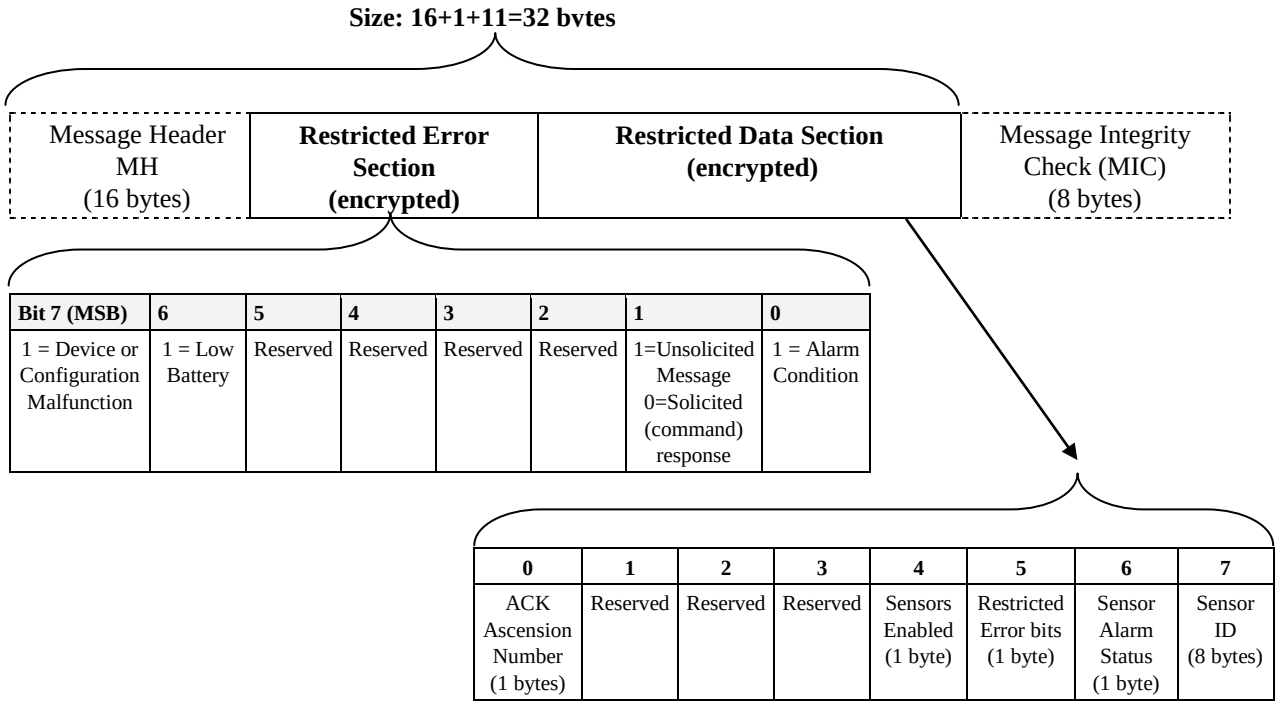


Figure 11-3, Add-on Sensor Status Message

Table 11-1, Add-on Sensor Status, Restricted Section Detail

Ref.	Restricted Section Content	Definition
A	ACK No.	Ascension Number for corresponding command. N/A for unsolicited status
B	Sensors Enabled	bit 0 = sensor 1 enabled; bit 1 = sensor 2 enabled, etc.
C	Restricted Error bits	bit 7 = sensor malfunction; bit 6 = decryption error; bit 5 = invalid command; bit 4 = log overflow; bit 3 = ACK failure; bit 2 = configuration failure; bit 1 = enable failure. Bit 0 reserved.
D	Sensor Alarm Status	bit 0 = sensor 1 alarm; bit 1 = sensor 2 alarm, etc.
E	Sensor ID	See below

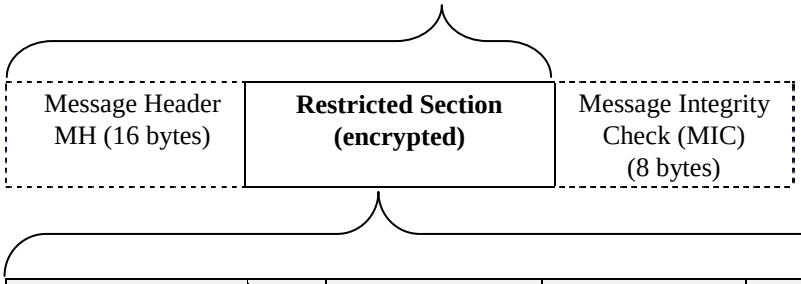
11.2.8.3 Sensor ID

The Sensor ID is equivalent to the Device UID, i.e., the 8-byte IEEE Extended Unique Identifier (EUI). This ID becomes important when the Add-on Sensors are implemented as a multi-hop network. The Security Device can use this ID to communicate with an Add-on Sensor that may be multiple hops away.

11.3 Embedded Commands for Add-on Sensors – Wireless

Embedded Commands for Add-on Sensors are commands that are sent from the Security Device to a particular sensor. Every AoS **Shall** accept and execute commands listed in the following sections. All commands from the Security Device to an AoS **Shall** have the message type 0xC2 to differentiate them from messages between the Security Device and an NAD.

Restricted (encrypted) Embedded Command Message



Security Message Command	Op code	Required Response	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Query Sensor Status	0x00	Sensor Status	(none)	(none)	(none)	(none)
Sensor/Security Device ACK	0x01	None	Ascension Number (1 byte)	(none)	(none)	(none)
Set Gateway Security Device	0x02	Sensor Status	(none)	(none)	(none)	(none)
Security Device Enable Sensor	0x03	Sensor Status	(none)	(none)	(none)	(none)
Security Device Disable Sensor	0x04	Sensor Status	(none)	(none)	(none)	(none)
Security Device Configure Sensor	0x05	Sensor Status	Size of Parameter 2	Configuration Data	(none)	(none)
Security Device Read Sensor Configuration	0x06	AoS to Security Device Sensor Configuration Data Response	(none)	(none)	(none)	(none)

Figure 11-4, Embedded Command Message Structure from Security Device to Sensor(s)

11.3.1 Security Device Configure Sensor

The Security Device Configure Sensor command seen in Figure 11-5 enables manufacturer-specific and non-ICD-defined sensor configuration parameters. Note: The input parameters shown in Figure 11-5 are only examples. The Security Device sends this command to the specified sensor after it receives the Configure Sensor command from a NAD. Note that the Security Device **May** be commanded by a NAD to configure multiple sensors via a single command with a sensor bitmap. The Security Device is responsible for transmitting individual Security Device Configure Sensor commands to the respective sensors. The configuration data can include alarm threshold conditions such as threshold value, dwell time, and sensor sampling interval. The command and configuration data plus the message header **Shall Not** exceed the available payload data area defined by IEEE 802.15.4-2006 minus bytes used by the NWK layer protocol required by this document.

The sensor's response to this message **Shall** be a Sensor Status message. If configuration fails, the sensor will send a Sensor Status message back to the Security Device with the Configuration Failed bit set to 1. The Security Device will then send a status message back to the commanding NAD with the Configuration Malfunction field set to 1 in the Restricted Error bits and the appropriate sensor number set in the Sensor Error Bits.

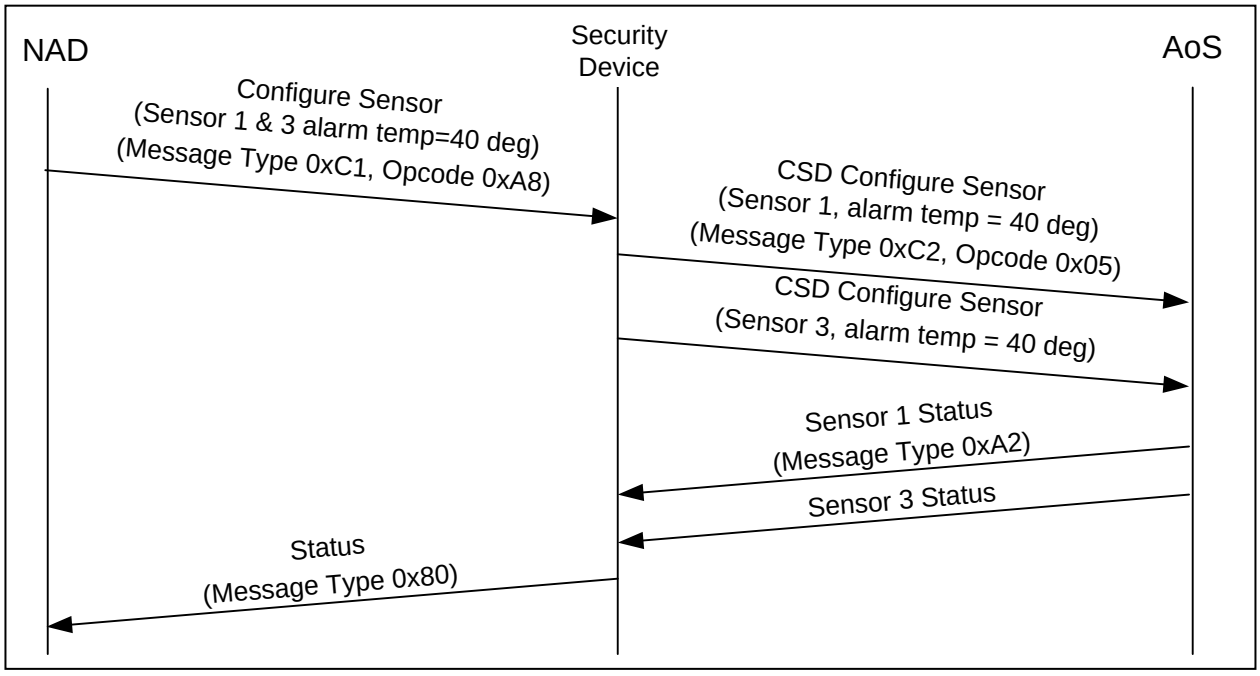


Figure 11-5, Security Device Configure Sensor Ladder Diagram (Security Device is a CSD)

11.3.2 Read Sensor Configuration (RC)

The Read Sensor Configuration command seen in Figure 11-6 enables the Security Device to read the configuration parameters from the sensor. The configuration parameters are the parameters set with the Configure Sensor command or the default parameters. The response to the Read Sensor Configuration command is depicted in Figure 11-6 below.

Note that the *Security Device-to-NAD Sensor Configuration* Message (Message Type 0xA4) and the *AoS-to-Security Device Sensor Configuration Message* (Message Type 0xA3) have the same structure.

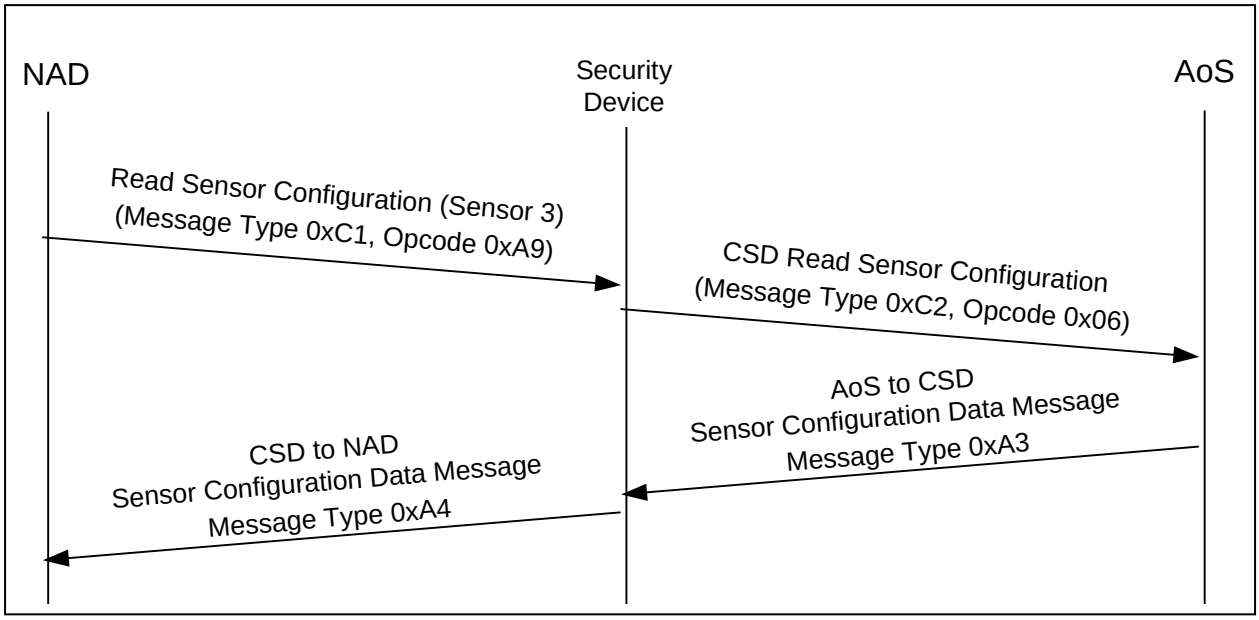
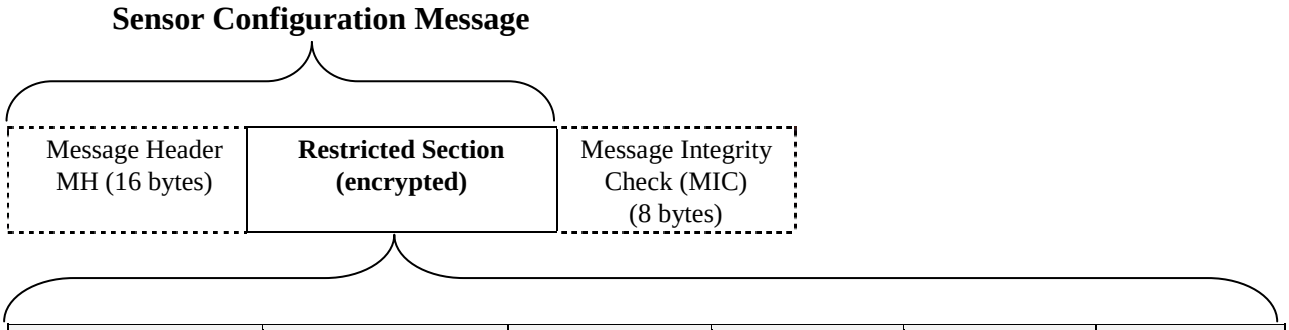


Figure 11-6, Query Sensor Configuration Ladder Diagram (Security Device is a CSD)



Security Message Command	Parameter 1	Parameter 2	Parameter 3	Parameter 4	Parameter 5
Sensor Configuration Data Message	ACK Ascension No. (1 byte)	Size of parameter 2	Configuration Data	(none)	(none)

Figure 11-7, Sensor Configuration Data Message

11.3.3 Security Device Enable Sensor

The Security Device Enable Sensor message is transmitted from the Security Device to the sensor once the Security Device has been commanded to enable a sensor (Message Type 0xC1, OpCode 0xA6) or arm the system (Message Type 0xC1, OpCode 0x04). The sensor **Shall** respond with a Sensor Status message indicating whether or not the sensor was successfully enabled. The Security Device **May** be commanded by a NAD to enable multiple sensors via a single command with a sensor bitmap. The Security Device is responsible for transmitting individual Security Device Enable Sensor commands to the respective sensors. The flow of messages is outlined below in Figure 11-8. Note: The parameter values in Figure 11-8 are only examples.

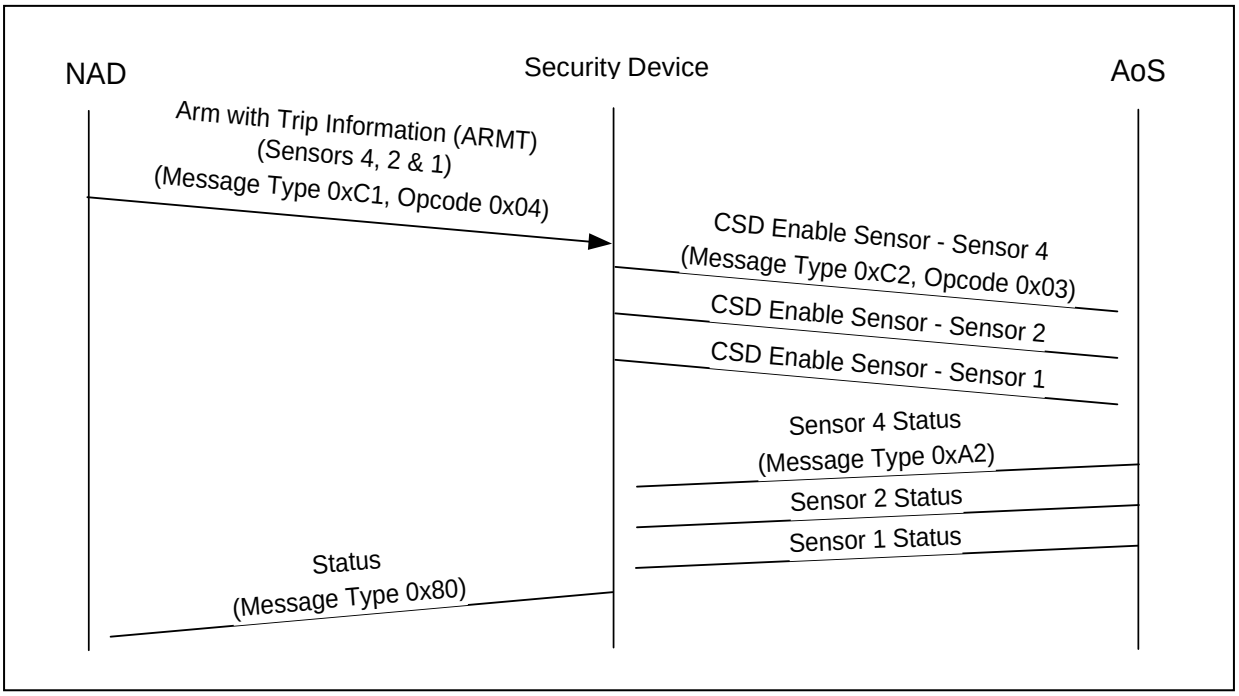


Figure 11-8, Arm System Ladder Diagram (Security Device is a CSD)

In the Security Device, this command permits certain sensors to not be enabled according to the nature of the trip or cargo characteristics, so as to lessen false alarms. The related alarm status bits are cleared when the sensor is enabled or disabled. Each sensor is disabled by default.

Enabling or disabling of sensors **Shall Not** be permitted when the Security Device is armed.

11.3.4 Security Device Disable Sensor

This message is transmitted from the Security Device to the sensor once the Security Device has been commanded to disable a sensor (Message Type 0xC1, OpCode 0xA7) or disarm the system (Message Type 0xC1, OpCode 0x80, 0x81). The sensor **Shall** respond with a Sensor Status message indicating whether or not the sensor was successfully disabled. Note the Security Device may be commanded by a NAD to disable multiple sensors via a single command with a sensor bitmap. The Security Device is responsible for transmitting individual Security Device Disable Sensor commands to the respective sensors.

Enabling or disabling of sensors **Shall Not** be permitted when the Security Device is armed.

11.3.5 Add-on Sensors (AoS) Data Formatting

Data passed from the AoSs to the controlling Security Device **Shall** be encrypted and must adhere to the requirements of [4]. The AoS event data forwarded to the controlling Security Device **Shall Not** cause the Security Device data packet size to exceed one frame, per [1].

11.3.6 Add-on Sensor Event Alarm Procedure

When an AoS is in an "alarm" state, the AoS **Shall** send a status message with the alarm bit set as "on" to the Security Device controller every 13 milliseconds until either the Security Device acknowledges receipt of the alarm message or the AoS battery is depleted. The Security Device **Shall** record the AoS event data (alarm or battery depleted condition) in the event log and forward the information as part of its status message to the DCP the next time the Security Device receives a NADA.

11.3.7 Periodic Unsolicited Status ("Health Check")

While the AoS is enabled, it **Shall** send a periodic unsolicited status message to its gateway Security Device to verify that the sensor is functioning properly and wireless connectivity has not been lost. The default time interval between "health check" messages is 1 hour, but vendors are permitted to decrease this time interval if necessary, taking into consideration the power requirements of the sensors and Security Device. If the gateway Security Device does not receive an unsolicited status message within an hour, it **Shall** assume that the sensor has malfunctioned and set the sensor's alarm status to true.

12 References

[1] *Security Device Requirements Including ACSD and CSD R1.0*; Department of Homeland Security, Science and Technology Directorate.

[2] *Network Access Device (NAD) Requirements R1.0*; Department of Homeland Security, Science and Technology Directorate.

[3] *Security Device NAD-to-DCP ICD V1.0*; Department of Homeland Security, Science and Technology Directorate.

[4] *Cargo Security Key Management and Data Security R1.0*; Department of Homeland Security, Science and Technology Directorate.

[5] *IEEE 802.15.4-2006 Standard* – Ratified January 2006.

[6] *ISO 17712:2010 Freight containers – Mechanical seals*

[7] *ISO 6346:1995 Freight Containers – Coding, identification and marking*

[8] *Federal Information Processing Standards Publication 140-2*.

[9] *IEEE 802.15.5 Standard* – Ratified March 2009.

[10] *Marine Asset Tag Tracking System (MATTS) Requirements Document R1.0*; Department of Homeland Security, Science and Technology Directorate.

[11] *Electronic Chain of Custody Device Requirements Document R1.0*; Department of Homeland Security, Science and Technology Directorate.

13 Acronyms

ACK	Acknowledge
ACSD	Advanced Container Security Device
AMH	ACSD Message Header
AMP	ACSD Message Packet
AoS	Add-on Sensors
ASH	ACSD Source Header
ARM	Arm Security Device
ARMT	Arm with Trip Information (see Figure 9-12)
BI	Beacon Interval
BO	Beacon Order
CCA	Clear Channel Assessment
CM	Communications Module
CoC	Chain of Custody
CPI	Change Provision Information (see Table 9-8)
CRC	Cyclic Redundancy Check
CS	Configure Sensor(s) (see Figure 9-12)
CSD	Container Security Device
CSI	Container Security Initiative
CTI	Change Trip Information (see Figure 9-12)
CWT	Commission with Trip Information (see Table 9-8)
DADC	Disarm from DCP (see Figure 9-12)
DAHH	Disarm from HNAD (see Figure 9-12)
DARM	De-activate
DCP	Data Consolidation Point
DHS	Department of Homeland Security
dB	Decibel
dBi	Decibel isotropic
ECM	External Communications Module
ECoC	Electronic Chain of Custody Device
EL	Erase Event Log (see Figure 9-12)
EUI	Extended Unique Identifier (per IEEE)
FFD	Full Functional Device
FNAD	Fixed Network Access Device
GTS	Guaranteed Time Slots
HMAC	Hash Message Authentication Code
HNAD	Handheld Network Access Device
IA	Information Assurance

ICD	Interface Control Document
ID	Identifier
IEEE	Institute of Electrical and Electronic and Engineers
ITP	Intermediate Transit Point
KMF	Key Management Facility (see [4])
LAN	Local Area Network
LLC	Link Layer Control
LSB	Least Significant Bit
LQI	Link Quality Indicator
MAC	Media Access Control
MCPS	MAC Common Part Sub-layer
MFR	MAC Footer
MH	Message Header
MHR	MAC Header
MIC	Message Integrity Check
MID	Manifest Identification
MLME	MAC Sub-layer Management Entity
MPDU	MAC Protocol Data Units
MPH	Miles per Hour
ms	milliseconds
MSB	Most Significant Bit
MW	Message Waiting
NAD	Network Access Device
NADA	Network Access Device Announcement
NDS	NAD Disable Sensor(s) (see Figure 9-12)
NES	NAD Enable Sensor(s) (see Figure 9-12)
NOP	No Operation
NWK	Network Layer Protocol
OSI	Open Systems Interconnect
PAN	Personal Area Network
PHR	PHY Headers
PHY	Physical Layer
PoA	Point of Arming
PoDC	Point of Deconsolidation
PPDU	PHY Protocol Data Units
PSDU	PHYS Service Data Units
RFD	Reduced Functional Device
RFID	Radio Frequency Identification
SAP	Service Access Point

SD	Security Device
SFD	Start-of-Frame Delimiter
SHA	Secure Hash Algorithm
SHR	Synchronized Header
SIS	Set in Trip State (see Figure 9-12)
SL	Send Event Log All (see Figure 9-12)
SMAF	Set Master Alarm = False (see Figure 9-12)
SMAT	Set Master Alarm = True (see Figure 9-12)
SLU	Send Event Log Unsent (see Figure 9-12)
SMS	Short Message Service
SSCL	Service Specific Convergence Layer
ST	Set Time (see Figure 9-12)
STI	Set Trip Information
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UID	Unique Identifier
WAN	Wide Area Network
WAoS	Wireless Add-on Sensor
WLN	Waypoint List New (see Table 9-8)
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

This page left blank intentionally

Department of Homeland Security

FOR OFFICIAL USE ONLY

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "FOR OFFICIAL USE ONLY" OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.