



TECHNICAL REPORT 3168
November 2018

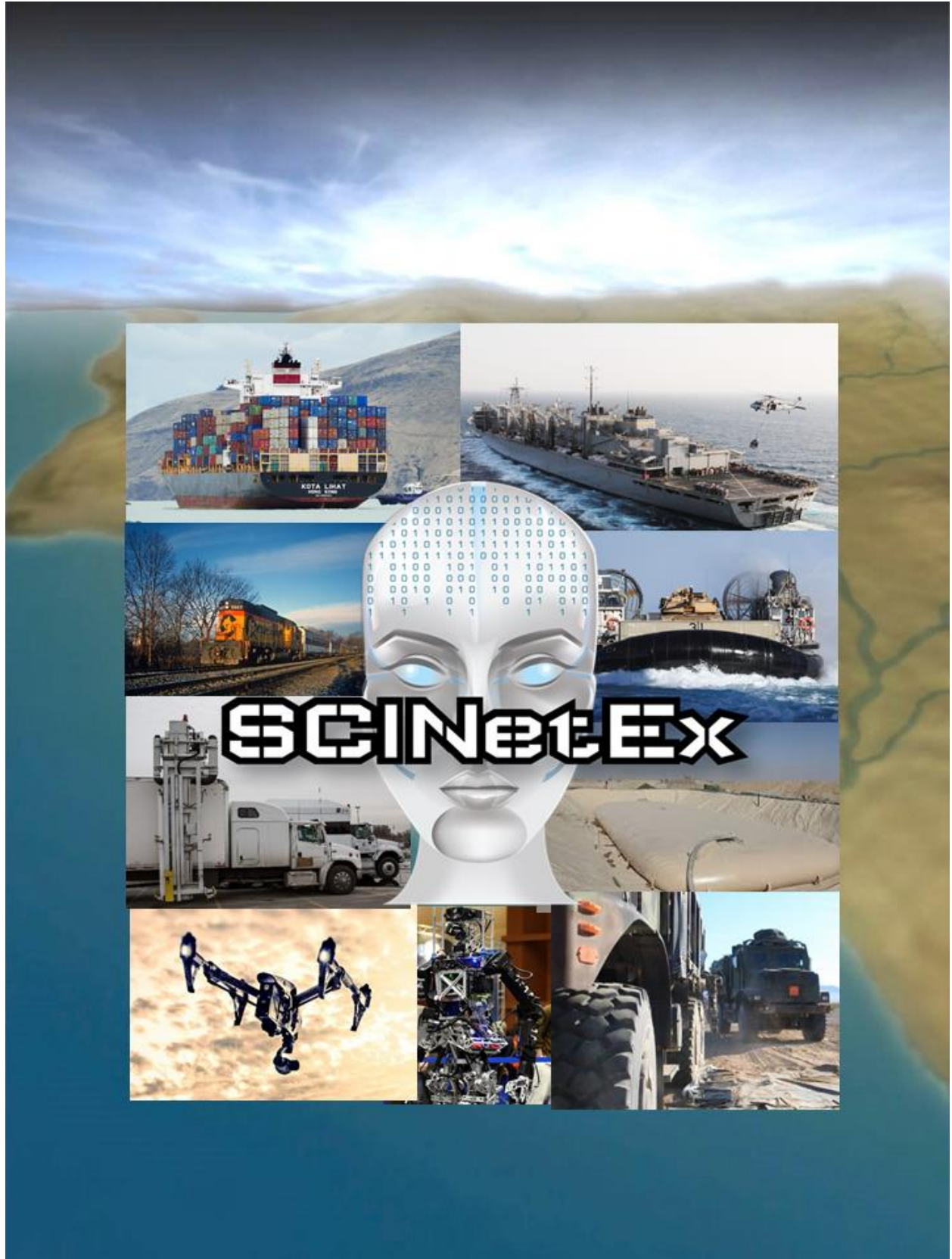
Secure Connectionless Intelligent Network Extension (SCINetEx) for Autonomic Messaging

Russ Clement
Sarah Lauff

Approved for public release.

SSC Pacific
San Diego, CA 92152-5001

This page intentionally left blank.



This page intentionally left blank.

SSC Pacific
San Diego, California 92152-5001

M. K. Yokoyama, CAPT, USN
Commanding Officer

W. R. Bonwit
Executive Director

ADMINISTRATIVE INFORMATION

The work described in this report was performed for the Marine Corps Combat Development and Integration (CD&I) Expeditionary Energy Office (E2O) by the Advanced Photonics Technologies Branch (Code 55360) of the Enterprise Communications and Networks Division (Code 55300), Space and Naval Warfare Systems Center Pacific (SSC Pacific), San Diego, CA.

Released by,
Sarah Lauff, Head
Advanced Photonics Technologies Branch

Under authority of
Clark R. Hendrickson, Head
Enterprise Communications and
Networks Division

PUBLICATION INFORMATION

Editor in Chief: Scriptatech
Publisher: *SSC Pacific*
Manuscript Editor: *Mary Clement and Robert Price*
Art Editors: *Art Armendariz*
Robert Price

The citation of trade names and names of manufacturers is not to be construed as official government endorsement or approval of commercial products or services referenced in this report.

VIC-20TM is a trademark of Commodore Business Machines

TRS-80TM is a trademark of Tandy Corporation

DOSTM is a trademark of IBM

MacintoshTM is a registered trademark of Apple Computer

DECTM is a registered trademark of Hewlett-Packard

PASCALTM is a registered trademark of Apple Computer

VAX mainframeTM is a registered trademark of Hewlett-Packard

IDARTTM is a registered trademark of Sandia National Laboratories

This page intentionally left blank.

DEDICATION AND ACKNOWLEDGMENTS

The authors would like to acknowledge the contributions of numerous people and organizations for collaborative development of the concepts and technical details included in this technical report. First and foremost is Mr. Kenneth Concepcion formerly of the Department of Homeland Security (DHS). Ken is an extraordinary person who received the Samuel J Heyman “Service to America Medal” in November 2002 for his heroic actions overseeing the seaborne evacuation of 70,000 people from Lower Manhattan Island in the immediate aftermath of 9-11. Years later, as a Program Manager for DHS, Ken led the development of autonomic detection and messaging systems for monitoring the security of cargo in the global supply chain. His understanding of international regulatory, statutory and operational requirements for maritime shipping drove many of the foundational concepts that underpin the SCINetEx protocols. These protocols were later tested, refined and used for physical security and fleet performance optimization by organizations in the US military. It has been my great honor to work with and support Ken’s efforts — he truly may be the most interesting man in the world.

In addition to Mr. Concepcion, the authors would like to acknowledge a host of scientists and engineers from the Space and Naval Warfare Systems Center Pacific (SSC PAC) and the US Department of Energy (DOE) Sandia National Labs (SNL) and Lawrence Livermore National Lab (LLNL). These highly skilled professionals comprised the foundational development team and made huge contributions to the conceptualization, design, development, testing, demonstration and documentation for the prototype systems that utilize the protocols described in this technical report. Each member of the team and their affiliations at the time of their work are listed alphabetically as follows:

Joel Baumbaugh	SSC PAC	Connie Bodmer	SNL
Steve Childress	SSC PAC (contractor)	John Dillinger	SNL
Ken Furgal	SNL	Brian Gains	SNL
Johnny Giere	SNL	John Macentee	DHS
James Meaden	SSC PAC	Melissa Mills	SNL
Aura Morris	SNL	Steve Morrison	SNL
Josh Phillips	SSC PAC	Kathy Pierce	SSC
Ayax Ramirez	SSC PAC	Mike Reaves	SSC
Karen Shanklin	SNL	Cory Sohrakoff	SSC
Mark Torgerson	SNL	Cassandra	SNL
Anton Yen	SSC PAC	Paul Zamorra	SNL

This page intentionally left blank.

EXECUTIVE SUMMARY

This technical report on Secure Connectionless Intelligent Network Extension (SCINetEx) is based on content that was created as a text book for instruction and reference in developing low-power wireless network extensions described in US Navy Patent #8855311. All commercial and government intellectual property rights for this patent are held by the US Government as part of an open architecture system. The report includes concepts and air interface protocols reviewed, tested and validated by teams from US Navy, DOE and DHS. A detailed discussion is also included that describes hierarchal messaging and network configurations supported by an encryption key management protocol for enhanced security when using untrusted Wide Area Networks (WANs). Regulatory requirements are also discussed as applied to the primary wireless medium that implements the IEEE Standard 802.15.4 waveform. Various network configurations are detailed that support autonomic terse messaging for applications such as in-transit visibility, transport and physical security, fleet optimization and management as well as sentient machine-to-machine communications. There are many topics addressed in this report specific to Network topology, data frame structures and operation including Network protocol stack set up, MAC protocol configuration set up, Network PAN ID standardization, Ad-hoc mesh network topology, Red Team testing and message encryption. There are over 40 figures included that help to make complex configurations addressed in this report easy to understand.

This page intentionally left blank.

ACRONYMS

ACK	Acknowledge
AI	Artificial Intelligence / artificially intelligent
AME	Application Management Entity
AoS	Add-on Sensor
ARM	Arm SED
BO	Beacon Order
CAN	Controller Area Network
CCA	Clear Channel Assessment
CCM	Cypher Block Chaining Message Authentication Code
CIF	Commission/Arm Information File
CM	Communications Module (common Communications Module / embedded Communications Module)
CONOPS	Concept of Operations
CPI	Change Provision Information
CRC	Cyclic Redundancy Check
CSMA	Carrier-sense Multiple Access
CWT	Commission with Use Information
DADC	Disarm from DAP
DAHH	Disarm from HNG
DAP	Data Aggregation Point
dB	Decibel
dBi	Decibel isotropic
DME	Device Management Entity
DNS	Domain Name System
ECM	External Communications Module
EL	Erase Event Log
ENG	Embedded Network Gateway
EIRP	Effective isotropic radiated power
EUI	Extended Unique Identifier (per IEEE)
FEMA	Finite Element Modeling and Analysis
FFD	Full Functional Device
FNG	Fixed Network Gateway
GTS	Guaranteed Time Slots
HitL	Human-in-the-Loop
HNG	Handheld Network Gateway
IA	Information Assurance
ICS	Industrial Control Systems
IEEE	Institute of Electrical and Electronic Engineers
IoT	Internet of Things
IP	Internet Protocols
IPsec	Internet Protocol Security

IoT	Internet of Things
IPT	Interdisciplinary Planning Team
ITV	In-transit Visibility
KIM	Key Information Manager
LAN	Local Area Network
LLC	Link Layer Control
LoPANs	Low-power Personal Area Networks
LQI	Link Quality Indicator
LSB	Least Significant Bit
LTK	Long Term Key
mA	milli-amp
M2M	machine-to-machine
MAC	Media Access Control
MH	Message Header
MHR	MAC Header
MiB	Mebibyte
MIC	Message Integrity Check
MLME	MAC Sub-layer Management Entity
MPDU	MAC Protocol Data Units
ms	milliseconds
MSB	Most Significant Bit
MT	Message Type
MW	Message Waiting
NAT	Network Address Translation
NGA	Network Gateway Announcement
NOP	No Operation
NWK	Network Layer protocol
OEM	Original Equipment Manufacturers
OSI	Open Systems Interconnect / Interconnection
PAN	Personal Area Network
PDU	Payload Data Unit
PER	Packet Error Rate
PGET	Get Sensor Parameter
PHY	Physical Layer protocol
PKI	Public Key Infrastructure
PSET	Set Sensor Parameter
RC	Reconfigure (AoS) Command
RFID	Radio Frequency Identification
RK	Rekey Key
ROC	Receiver Operating Characteristics
RSC	Read Sensor Configuration
SAP	Service Access Point
SED	Smart End Device

SEDUID	Smart End Device Unique Identifier
SHNG	Secure Handheld Network Gateway
SIS	Set In-use State
SK	Storage Key
SL	Send Event Log All
SLU	Send Event Log Unsent
SMAF	Set Master Alarm = False
SMAT	Set Master Alarm = True
SMM	Sentient Machine Messaging
SMS	Short Message Service
SNGUID	Secure Network Gateway Unique Identifier
ST	Set Time
TCK	Temporary Communication Key
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
UID	Unique Identifier / Universal Identifier
WAN	Wide Area Network
WLN	Waypoint List New
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

This page intentionally left blank.

CONTENTS

EXECUTIVE SUMMARY	ix
ACRONYMS.....	xi
1. INTRODUCTION.....	1
1.1 COMPUTERS.....	1
1.2 NETWORKS.....	3
1.3 NETWORK EXTENSION CONCEPT	5
2. INTRODUCTION AND OVERVIEW.....	9
2.1 HIERARCHICAL MESSAGING	9
2.2 PRECEDENCE AND NOMENCLATURE	10
2.3 REGULATORY REQUIREMENTS	10
2.4 SYSTEM OVERVIEW.....	10
2.4.1 Primary Wireless Medium – Summary	14
2.4.2 Smart End Device (SED).....	15
2.4.3 Network Gateway (NG)	16
2.4.4 Data Aggregation Point (DAP).....	18
3. SYSTEM EMBODIMENTS.....	19
3.1 IN-TRANSIT VISIBILITY	19
3.1.1 General Concept of Operations.....	19
3.1.2 ITV System Components	21
3.1.3 Considerations for In-Transit Visibility	23
3.2 SECURITY	23
3.2.1 General Concept of Operations	23
3.2.2 Security System Components	24
3.2.3 Chain of Custody System Components.....	25
3.2.4 Considerations Regarding Security Systems	25
3.3 FACILITY AND WAREHOUSE MANAGEMENT.....	25
3.3.1 General Concept of Operations.....	25
3.3.2 Facility and Warehouse Management System Components.....	26
3.3.3 Considerations for Facility/Warehouse Management	27
3.4 FLEET MANAGEMENT	27
3.4.1 General Concept of Operations.....	27
3.4.2 Fleet Management System Components	28
3.4.3 Considerations for Fleet Management	28
3.5 SENTIENT MACHINE MESSAGING	29
3.5.1 Concept of Operations	29
3.5.2 Sentient Machine Messaging System Components	30

3.5.3	Considerations for Sentient Machine Messaging	30
4.	SED-TO-NG COMMUNICATIONS.....	31
4.1	COMMUNICATIONS MODES	31
4.2	END-TO-END MESSAGING PRINCIPLES	31
4.2.1	Session-less vs. Session-based Messaging	31
4.2.2	Fragmentation and Reassembly	31
4.2.3	Error Correction	32
4.2.4	End-to-End Addressing and Mobility Management	32
4.2.5	SED-to-DAP Addressing	33
4.2.6	DAP-to-SED Response Addressing	33
4.2.7	DAP-to-SCINetEx Unsolicited Ad-hoc Addressing	33
4.2.8	External Relay Function	33
5.	WIRELESS PERSONAL AREA NETWORK (WPAN) DESCRIPTION.....	37
5.1	NETWORK TOPOLOGY – STRUCTURE AND OPERATION	37
5.1.1	802.15.4 Network Topology Overview.....	37
5.1.2	Network Protocol Stack.....	38
5.1.3	MAC Protocol Configuration.....	38
5.1.4	Network PAN ID Standardization	41
5.1.5	WPAN MAC Address Interoperability Assurance	42
5.1.6	Network Discovery	42
5.1.7	Communications Module Network Discovery Procedure	45
5.2	AD-HOC/MESH NETWORK TOPOLOGY	49
5.2.1	Ad-hoc/Mesh Protocol and Procedures.....	50
5.2.2	Ad-hoc/Mesh Network Layer (NWK) Management Functions Utilized	51
5.2.3	Network Discovery for Ad-hoc/Mesh.....	52
5.2.4	SCINetEx Physical Layer (PHY)	52
5.3	RF INTEROPERABILITY LINK BUDGET	53
5.3.1	Receiver Requirements.....	53
5.3.2	Transmitter Requirements	53
5.3.3	SED and FNG/HNG Bi-directional Antennas	53
5.3.4	RF Link Budget.....	53
6.	MEDIA ACCESS CONTROL LAYER (MAC).....	55
6.1	MAC FRAME CONSTRUCTS	55
6.1.1	MAC Layer Configuration Parameters.....	55
6.1.2	MAC Layer Acknowledgement Frames	55
6.1.3	MAC Layer Retransmissions	55
7.	NETWORK LAYER	57

7.1	NETWORK MEDIA CONNECTIVITY	57
7.1.1	Multi-path	57
7.1.2	Attenuation	58
7.2	SIMULATION AND MODELING OF NETWORK LAYER CONNECTIVITY	58
8.	APPLICATION LAYER	61
8.1	APPLICATION LAYER MESSAGING	61
8.1.1	Date and Time Format	61
8.1.2	HNG Messages	62
8.2	MESSAGE ADDRESSING – END-TO-END	62
8.2.1	Addressing – for Data Aggregation Point (DAP) Destination	62
8.2.2	Addressing – for SED Destination	62
8.3	MESSAGE ACKNOWLEDGEMENTS (ACKS) – ERROR DETECTION AND CORRECTION	62
8.3.1	Retransmissions for Error Correction – End-to-End	63
8.3.2	ACK from the SED CM	63
8.3.3	ACK from Data Aggregation Point/HNG	63
8.3.4	ACK Failure Procedure	63
8.4	APPLICATION LAYER MESSAGE STRUCTURE	63
8.4.1	Applicability	63
8.4.2	Description of Application Layer Message Structure	63
8.4.3	Universal Message Header (MH)	64
8.5	MESSAGE CONTENT	68
8.5.1	Device Restricted Status Message from SED	68
8.5.2	Device Restricted Status Message from SED with GPS	71
8.5.3	Waypoint and Location Data Formats	73
8.5.4	Unrestricted Status Message from SED – Solicited	74
8.5.5	Unrestricted Status Message from Tethered SED – Solicited	75
8.5.6	Device Status Message from SED – Unsolicited	76
8.5.7	Device Status Message from SED with GPS – Unsolicited	77
8.5.8	SED Event Log Records	77
8.6	COMMAND MESSAGES FROM DAP OR SECURE NG	79
8.6.1	Unrestricted Command messages for SED	80
8.6.2	Restricted Command Messages for SED – No GPS	80
8.6.3	Restricted Command Messages — for SEDs with GPS	82
8.6.4	No Operation (NOP) Command Message from DAP or Secure NG	84
8.6.5	ACK Message from DAP or Secure NG	84
8.6.6	Disarm Command Message from DAP or Secure NG	84
8.6.7	Decommission Command Message from DAP or Secure NG	84

8.6.8	Set In-use State	84
8.6.9	Garbled Application Layer ACKs Received by SED	85
8.6.10	Garbled Application Layer ACKs Received by DAPs or HNGs	86
8.7	ROUTINE MESSAGING LADDER DIAGRAMS	86
8.7.1	Broadcast Network Discovery Ladder Diagram for NG Function.....	86
8.7.2	Unsolicited Status Message (to DAP or Secure NG) Ladder Diagram	87
8.7.3	DAP or Secure NG-originated Message Ladder Diagram	87
8.7.4	Event Log Record Message and Responses Ladder Diagram	89
9.	INFORMATION ASSURANCE (IA) AND SECURITY	91
9.1	802.15.4 WIRELESS NETWORK INTERFERENCE MITIGATION.....	91
9.1.1	Irrelevant Wireless PANs at Locale	91
9.1.2	Persistent Interference or Denial of Service – Wireless.....	91
9.2	CYBER SECURITY	91
9.3	CYBER MANAGEMENT PHASED IMPLEMENTATION APPROACH.....	92
9.4	APPLICATION DATA FLOWS AND DEVICES	93
9.5	KEY TYPES	94
9.5.1	The Rekey Key (RK)	95
9.5.2	The Long Term Key (LTK).....	95
9.5.3	The Temporary Communication Key (TCK)	96
9.5.4	The Storage Key (SK)	97
9.6	DEVICES AND KEYS	97
9.6.1	The Key Information Manager (KIM).....	97
9.6.2	Level 1 Facilities.....	98
9.6.3	Level 2 Devices.....	98
9.6.4	Level 3 Devices.....	99
9.7	KEY CHANGE PERIOD	100
9.8	MULTI-USER KEY MANAGEMENT	101
9.9	IMPLEMENTATION.....	101
9.10	PACKET INFORMATION	101
9.10.1	Packet Header and MIC	102
9.10.2	Device Type.....	102
9.10.3	Key Management Message Types.....	102
9.10.4	Device UID	103
9.10.5	Message Ascension Number	103
9.11	KEY DERIVATION	104
9.11.1	The Rekey Key	104
9.11.2	Level 1 Temporary Communication Key.....	104

9.11.3	Level 2 Temporary Communication Key	105
9.11.4	The Storage Key.....	105
9.12	MESSAGE ENCRYPTION AND AUTHENTICATION	106
9.12.1	The Rekey Message.....	106
9.12.2	All Other Messages	107
9.12.3	Future Message Types	107
9.12.4	Data Storage	107
9.13	FURTHER DISCUSSIONS ON EXTENSIBILITY	107
9.14	LATER SED IMPLEMENTATION	108
9.15	TRUSTED CIRCUITS AND COMPONENTS	109
10.	HANDHELD NETWORK GATEWAYS	111
10.1	MAKING AN HNG IEEE STANDARD 802.15.4 COMPATIBLE	111
10.2	CHALLENGES WITH HNGS	112
11.	RELAYS AND ADD-ON SENSORS	115
11.1	ADD-ON SENSORS VIA WIRED BUS CONNECTION	115
11.1.1	Wired Sensor Physical Layer (PHY)	115
11.1.2	Wired Sensor Bus Physical Access	117
11.2	RELAYS – EXTERNAL TO ASSET	119
11.2.1	Method of Tethering – SEDs	120
11.2.2	Method of Untethering	121
11.2.3	Tethering Keep Alive.....	121
11.2.4	Tethering Sensor CMs and Relay Devices.....	121
11.3	ADD-ON SENSORS – NO GPS.....	121
11.3.1	SED-to-Add-on Sensor – Wired Bus Connection.....	122
11.3.2	SED-to-Add-on Sensor – Wireless Medium	122
11.3.3	Wireless Medium – Physical Layer	122
11.3.4	Wireless Medium – Data Link Layer.....	122
11.3.5	Wireless Data Frame Content.....	122
11.3.6	Method of Tethering SED and Add-on Sensors	122
11.3.7	Network and Application Protocol.....	125
11.4	EMBEDDED COMMANDS FOR ADD-ON SENSORS – WIRELESS.....	128
11.4.1	SED Configure Sensor.....	129
11.4.2	Read Sensor Configuration (RSC).....	130
11.4.3	SED Enable Sensor (Arm System)	131
11.4.4	SED Disable Sensor	132
11.4.5	Add-on Sensors (AoS) Data Formatting.....	132
11.4.6	Add-on Sensor (AoS) Event Alarm Procedure	132

11.4.7	Periodic Unsolicited Status (“Health Check”).....	133
12.	NETWORK GATEWAY TO DATA AGGREGATION POINT CONNECTIONS.....	135
12.1	DATA AGGREGATION POINTS (DAPS)	135
12.2	NETWORK GATEWAYS (NGS)	135
12.3	INTERFACE DESCRIPTION	135
12.3.1	Overall Data Flow	136
12.3.2	Network Overview	137
12.4	NETWORK GATEWAY-TO-DATA AGGREGATION POINT SECURITY	138
13.	NETWORK GATEWAY-TO-DATA AGGREGATION POINT COMMUNICATIONS ..	139
13.1	COMMUNICATIONS INTERFACE	139
13.2	DAP-TO-NG DATA CONNECTION	139
13.2.1	DAP-to-Non-secure NG Data Transfer.....	139
13.2.2	DAP-to-Secure NG Data Transfer.....	139
13.2.3	DAP-to/from-Secure NGs Network Protocol	140
13.3	DAP-TO-SECURE NG	140
13.3.1	Retrieval of SED Encryption Keys.....	140
13.3.2	Communications Data Prerequisites	140
13.3.3	Communications to Commission/Arm a SED	141
13.4	GENERAL PACKET FORMATS FOR MESSAGE-BASED INTERFACES	141
13.5	DAP-TO/FROM-NON-SECURE NGS	144
13.5.1	UDP Option	144
13.5.2	TCP Option	145
13.5.3	DAP-to/from-Non-secure NG Connect to DAP	145
13.5.4	Get Time and Date Message	145
13.5.5	DAP-to-Non-secure NG Packet Messages	145
13.5.6	Non-secure NG-to-DAP – SED Message Content	147
13.5.7	DAP-to-Non-secure NG – SED Message Content	148
13.5.8	DAP-to-Non-secure NG – Change DAP IP Address	149
13.5.9	DAP-to/from-Non-secure NG – Error Detection and Correction	155
13.6	DAP-TO/FROM-SECURE NGS MESSAGE EXCHANGE	156
13.6.1	DAP-to-Secure NG Retrieval of SED Encryption Key	156
13.6.2	DAP-provided Data Prerequisites	157
13.7	COMMUNICATIONS TO COMMISSION/ARM A SED	157
13.7.1	DAP-to-Non-secure NG – Commission/Arm Data	157
13.7.2	DAP-to-Secure NG – Commission/Arm Data	157
13.7.3	DAP Commission/Arm Information File (CIF)	157
13.7.4	Secure NG-to-DAP Data Transfer	159

13.7.5 Cellular Data Service Using Embedded NGs	160
13.7.6 Satellite Service Using Embedded NGs	160
14. TEST PLANNING	161
14.1 PROBLEM STATEMENT	161
14.1.1 Motivation	161
14.1.2 Conceptual Model	161
14.2 THE OPERATIONAL ENVELOPE	162
14.3 TEST CONDITIONS AND DEGRADATION FACTORS	163
14.4 TEST OBJECTIVES AND HYPOTHESES	164
14.5 OBJECTIVES	165
14.6 HYPOTHESES	165
14.7 EXPLORATORY DATA	166
14.8 DATA NEEDED TO TEST THE HYPOTHESES	166
14.9 ABORT CRITERIA	169
14.10 DATA ANALYSIS FRAMEWORK	170
14.11 EVALUATION CRITERIA	170
14.12 TEST DESIGN OPTIMIZATION	171
14.13 DATA TO BE COLLECTED	171
14.14 TEST PLAN EXAMPLE CROSSWALK	172
15. SCINETEX RED TEAM TEST PROCESS	177
15.1 INTRODUCTION	177
15.2 RED TEAM METHODOLOGY	177
15.2.1 Planning	177
15.2.2 Data Collection	177
15.2.3 Characterization	178
15.2.4 Analysis	178
15.2.5 Report	178
15.2.6 Demos and Experiments	178
15.3 SCINETEX DEFEAT TEST GUIDELINES	178
15.3.1 Objective	178
15.3.2 Goals of the Defeat Test Guidelines	179
15.3.3 Process	179

APPENDICES

A: COMMISSION/ARM INFORMATION FILE XML SCHEMA FORMAT	A-1
B: HYPOTHESES EXAMPLES	B-1

Figures

Figure 2-1. Network Topology Example: Dispersed Assets (fixed or mobile).	11
Figure 2-2. SCINetEx System Overview.....	12
Figure 3-1. Concept of Operations ITV.....	21
Figure 3-2. Concept of Operations Security Systems.	24
Figure 3-3. Concept of Operations Facility and Warehouse Management.....	26
Figure 3-4. Concept of Operations Fleet Management System.	28
Figure 3-5. Concept of Operations Sentient Machine Messaging.....	29
Figure 4-1. Illustration of End-to-End Message Transport.	32
Figure 5-1. IEEE Standard 802.11 vs. IEEE Standard 802.15.4-2006 Coexistence.	40
Figure 5-2. Communications Protocol Stack Architecture.....	40
Figure 5-3. Network Discovery and Unsolicited Device Status Message Timing Example – Two NGs.	46
Figure 5-4. NULL Message from SED or CM.....	48
Figure 5-5. Mesh Protocol Stacks in CMs per the IEEE Standard 802.15 References.	51
Figure 7-1. Concept Model for Latency Testing.....	59
Figure 8-1. SCINetEx Messages – Message within MAC Payload.	64
Figure 8-2. Universal Message Header Contents.....	65
Figure 8-3. Device Status Message.....	69
Figure 8-4. Tertiary ID Field.	71
Figure 8-5. Device Status Message.....	72
Figure 8-6. Device Status – Unrestricted Status Reply from SED.	75
Figure 8-7. Device Status – Unrestricted Status Reply Content from Tethered SED.....	76
Figure 8-8. Event Log Message (to DAP).	78
Figure 8-9. Event Log Message (from SED to DAP or secure NG).....	79
Figure 8-10. Unrestricted Command (Message Type 0xC0).....	80
Figure 8-11. Restricted Command Message Structure (Message Type 0xC1).....	81
Figure 8-12. Network Gateway Announcement (NGA) Ladder Diagram.....	86
Figure 8-13. Unsolicited Status Message Ladder Diagram.....	87
Figure 8-14. DAP or NG Message Ladder Diagram.	88

Figure 8-15. Event Log Record Message Diagram.....	89
Figure 9-1. Implementation Phase 3 Key Management Hierarchy.....	93
Figure 10-1. Standard HNG Configuration.	113
Figure 10-2. Scenario 1 – Issues with Integrating HNG, Notional UID.....	113
Figure 10-3. Scenario 2 – Issues with Integrating HNG, Notional UID.....	114
Figure 11-1. Wired Add-on Sensor Bus Examples.....	116
Figure 11-2. Tethering Command.	121
Figure 11-3. Add-on Sensor Tethering Sequence Ladder Diagram.....	125
Figure 11-4. Add-on Sensor Status Message.	127
Figure 11-5. Embedded Command Message Structure from SED to Sensor(s).	129
Figure 11-6. SED Configure Sensor Ladder Diagram.	130
Figure 11-7. Read Sensor Configuration Ladder Diagram.....	131
Figure 11-8. Sensor Configuration Command Message.....	131
Figure 11-9. Arm System Ladder Diagram.....	132
Figure 12-1. Top Level SCINetEx System View.	136

Tables

Table 1-1. SCINetEx System Terms.....	6
Table 2-1. Network Element Descriptions.	13
Table 5-1. IEEE Standard 802.15.4-2006 MAC Configuration.....	39
Table 5-2. Security-Reserved PAN IDs.	41
Table 5-3. Network Gateway Announcement (NGA) Message Content.	44
Table 5-4. Primary Network Layer Functions – Ad-hoc Topology.....	51
Table 5-5. IEEE Standard 802.15.4-2006 PHY Layer Configuration.	52
Table 5-6. Link Budget Example.....	54
Table 8-1. Date and Time Format.	62
Table 8-2. MH Device Type Codes.....	66
Table 8-3. MH Message Type (MT) Codes.	66
Table 8-4. Device Status Message Restricted Data Section Content Definition.	70
Table 8-5. Alarm Status Parameter.	71

Table 8-6. Condition Status Parameter.....	71
Table 8-7. SED with GPS Restricted Data Section Detail.	73
Table 8-8. Restricted Command Messages for SEDs with GPS.....	83
Table 8-9. Set In-use State Parameter Values for CM Restricted Commands.	85
Table 9-1. Device Types.....	102
Table 9-2. Key Management Message Types.....	103
Table 11-1. Wired Sensor Interface Connector.	116
Table 11-2. Frame ID Bits.	117
Table 11-3. Alive Message – Optionally Recurring at Unspecified Interval.....	118
Table 11-4. Enable Sensor – Sent by SED.....	118
Table 11-5. Disable Sensor – Sent by SED.....	118
Table 11-6. Sensor Activity.....	118
Table 11-7. Set Sensor Parameter – Sent by SED.....	118
Table 11-8. Get Sensor Parameter – Sent by SED.	118
Table 11-9. Add-on Sensor Status – Restricted Data Section Detail.	128
Table 13-1. Preamble Formats.....	142
Table 13-2. Date, Time, Heartbeat Request Packet.	146
Table 13-3. Heartbeat Response Packet.....	147
Table 13-4. Non-secure NG-to-DAP Preamble.....	148
Table 13-5. DAP-to Non-secure NG Preamble.....	148
Table 13-6. Change DAP IP Address.	149
Table 13-7. DAP Message Descriptions.....	151
Table 13-8. DAP Errors.	155
Table 14-1. Usability Hypotheses.....	172
Table 14-2. Functionality Hypotheses.	173
Table 14-3. Performance Hypotheses.....	174
Table 14-4. Rate of Failure Hypotheses.....	176
Table 14-5. Security Hypotheses.	177

1. INTRODUCTION

FORWARD

My earliest exposure to the world of computing occurred in the early 1970s. My parents came home one day with a Texas Instruments calculator that was quite exotic for its time. I don't recall the model but this marvel could be used to accurately add, subtract, multiply and divide numbers both large and small at a mind-boggling pace. In fact, I believe one number could be stored in memory to be recalled for later use so long as the device was not turned off. This calculator was very clunky by today's standards but to a pre-teen it bore a striking resemblance to technology seen in the vintage Star Trek series – other than the fact it had to be plugged in.

Calculators were initially banned from classrooms at that time since; (1) not everyone had access to one, and (2) students that became dependent on this technology would not adequately learn rudimentary mathematics. Attitudes quickly changed and teachers began to expand mathematical and scientific curricula to take advantage of the automated calculation tools. Before long, every student had access to reliable calculators that were battery-powered and capable of long term storage of constant values (such as PI) and even more complex mathematical and trigonometric functions.

Sometime prior to 1976, one of my brothers purchased an expensive Hewlett Packard (HP) handheld calculator that was programmable. It was an even greater marvel using some strange keying input method called Reverse Polish Notation (RPN). RPN is a construct invented by Jan Lucaisiewicz (1924) for optimizing computer memory access utilizing a stacking model to evaluate mathematical expressions. Programmability in these early HP calculators was similar to that of spreadsheet cell formulas that we use today. If you were a truly serious techno-geek, you had an HP.

1.1 COMPUTERS

When I graduated from high school in 1980, computers such as the Commodore VIC-20 and Tandy TRS-80 were just being introduced for home computing. The Commodore utilized a television for display and introduced the world to PC-gaming. The TRS-80 had its own built-in screen (white or green text – no graphics) and included a BASIC language interpreter to facilitate direct user programming. By 1985, Disk Operating Systems (DOS) and high performance programming language interpreters/compiler such as BASIC, COBOL and FORTRAN became available that could effectively run on desktop computers such as the International Business Machines (IBM) 8086 and Apple Macintosh.

Throughout this time, large mainframe computers such as those developed by IBM and Digital Equipment Corporation (DEC) were the domain (and jealously guarded territory) of the hardcore institutional computer scientist, engineer and programmer. I learned to program using FORTRAN on one such mainframe computer. Code was input using a card punch/reader system located in the university's student computing center. Many late nights were spent waiting in line to feed a stack of punch cards into the scanner only to find out hours later from the computing center staff that the program didn't run properly or did not successfully compile. At least in the latter event, the compiler would give you an error message and let you know where the code went bad. One of my worst adult nightmares to this date includes a flashback of dropping an enormous punch card stack on the way to the reader the night before the assignment was due. Fortunately, the next level class in PASCAL provided access to computer terminals to key-in the source code.

As personal computing power increased, the ability to network PCs to enhance processing power and facilitate data transfer became more viable and attractive. Until the mid-1980s, computing networks built around the Transmission Control Protocol Suite (commonly known as TCP) were

developed and primarily used by mainframe computing centers to connect government, academic and business clients. Over the years, the TCPs were merged with the session-less Internet Protocols (IP) to become known as TCP/IP. Related connecting technologies (wired and wireless media) also evolved for use on personal computers and that in turn led to the development of some of the distributed network concepts used by mobile personal computing today.

After graduating from college, my first job was to conduct tests on infrared satellite components for the US Navy. This work included collecting and reducing large amounts of integrated circuit performance data that traditionally utilized one or more large (room-size) VAX mainframe computers. Being youthful (and impertinent), several colleagues and I convinced our project manager to purchase a number of IBM 80286 desktop computers and rudimentary analog-to-digital (A/D) conversion boards so that we could build our own portable data reduction systems. The manager of the mainframe computing facility at the lab was incensed at our temerity and complained bitterly that such distributed computing power should not be trusted to young scientists and engineers and that we would spend all of our time doing unproductive activities such as programming (a bit ironic) or playing games.

Truth be told, the computing facility manager wasn't entirely wrong – we did play games. However, no one at the test facility fully anticipated the productivity enhancements that distributed computing provided in the laboratory setting. For example, it was no longer necessary to share computational resources (time) on the mainframe computer. Programming code changes could be executed and re-compiled without coordination between disparate users. Coding mistakes supporting one test station didn't affect operations at another test station. Portable test stations allowed us to conduct experiments at remote facilities that couldn't be executed in the laboratory where the mainframe was located. Reporting and presentation quality and quantity improved significantly with the rapid advancement of word processing, computer-aided design and publication products developed for PC and Apple platforms. But most importantly, distributed computing capability provided each experimenter greater latitude to try new things. Back then, these new things included improved visualization, information distribution (networks) and new high-level programming tools.

Thirty years later, we still have this intellectual push and pull between the preference of centralized versus distributed computing systems. Today, we usually refer to centralized systems as existing on “the cloud” and distributed systems as “mobile computing”. Cloud and mobile devices are linked by a shared digital network media. This network media can be wired or wireless with transmission control protocols that were designed during the latter part of the previous century to communicate between those big clunky mainframes. Initially, functionality of the network media for transferring the maximum amount of data quickly and reliably was the primary concern. More recently we are concerned with accessibility and security of the network media. For cloud computing, data and large applications (that turn data into useful information) reside on the cloud (read central server network) and are accessed through secure protocols. Data and smaller applications can reside on the mobile device with access to large data bases/applications through connection to the cloud.

Cloud-based networks are considered homogeneous networks in the sense that access and security strategy is that of single, uniform governance. That is to say there may be multiple domains or enclaves within the cloud, but those domains and enclaves are coordinated by a single authority. Distributed networks are different in that each network is its own domain and

may establish unique access and security strategies tailored to that network component's individual needs. Distributed networks are considered heterogeneous and may be managed by multiple authorities and implement dissimilar access and security strategies.

Proponents of cloud-based computing systems feel that homogenous systems are a more cost effective method for providing large-scale computing services and are capable of greater data and information security through uniform centralized governance. Cloud customers are encouraged to reduce their reliance on device-level data processing and ship raw data to the cloud-based servers for data reduction and conversion to useful information. The cloud-based business model is built around profits earned per byte of data shipped to and stored on the cloud servers, as well as cloud data processing time. Proponents of distributed systems that are reliant on device-level processing with minimal data transport, feel that the cost effectiveness of cloud-based computing is overstated and once breached, homogeneous cloud systems compromise all the data, information and functionality under its security governance. The benefit of a heterogeneous system is that if a single component is breached, it can be isolated more effectively from the rest of the system without affecting the overall distributed system performance. I am a proponent of heterogeneous distributed systems.

1.2 NETWORKS

A key component of both cloud and distributed systems is the network media. That media may be wired or wireless and must provide sufficient bandwidth to support packet traffic and security functions to meet the information assurance (IA) requirements of the user. IA is defined as the practice of assuring information and managing risks related to the use, processing, storage and transmission of information or data and the systems and processes used for those purposes. This includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data in both transit and at rest. IA is achieved using physical, technical and administrative controls on access to information networks and their components.

Cloud-based computing systems are generally utilized for transport, storage and analysis of large amounts of data. Thus, they are dependent on high bandwidth connections over networks that are trusted (not compromised by a malicious actor). Distributed systems, if properly designed, are less so dependent on bandwidth and trust – but not always. It should be noted that distributed systems may be connected to cloud systems but are not dependent on access to the cloud for basic operations.

Today when we think of computer networks, we are starting to equate that to autonomous systems. Autonomous data collection systems have become common as metering, monitoring and control devices are used in our vehicles, work places and homes. These devices are rather rudimentary in nature and usually take advantage of existing wired and wireless networks to send data to a central controlling location and respond to commands/queries from that controller. In the simplest form, these devices are more so designed for remote control operation rather than truly autonomous operation. Even so, when designing these systems, great care must be taken to ensure protocols that govern data exchanges between devices are sufficiently tailored to ensure that the network is not overwhelmed by message contention or compromised by malicious actors. Message contention is a function of the number of data, command and transmission control packets over the wireless or wired network at any time. Each device on a network contributes to the message contention. Denial of service hacks are an example of extreme message contention.

In some networks, one must also consider the control packet exchanges (wired and wireless) for cyber health and security and the effects on message contention. Cyber is defined as the computers, communications systems (wired and wireless) and communication services that make up the network including information contained there-in. Cyber security is therefore defined as the prevention of damage to, protection of, and restoration of computers, electronic communications systems and electronic communications services (including information contained there-in), to ensure its availability, integrity, authentication, confidentiality and non-repudiation. Cyber security activities such as periodic device scans and patch upgrades may cause significant message contention on either a wired or wireless communications system.

It is safe to assume that we will continue on our current networking arc and, with the utilization of artificial intelligence and cognitive tools, implement fully networked systems that are truly autonomous. This will include such diverse algorithmic and data-driven technologies such as machine learning and natural language processing/generation utilized for drone and robotic process automation supporting activities in our professional and personal lives. It is also safe to assume that cognitive tools supporting artificially intelligent entities, as part of fully networked systems, will need to communicate between themselves without human moderation. To maximize the positive impact of these new technologies, we need to re-think the interactions between humans and AI entities as well as between the AI entities themselves.

Collection of Industrial Control System (ICS) and telematics-type data by intelligent (smart) end devices integrated with newer cognitive technologies is rapidly increasing and is a good example of nascent pseudo-intelligent autonomous systems functioning in our day-to-day lives. This use of autonomous systems is in part being driven by the need for visibility and control for operational considerations as well as logistics, maintenance and safety. Public and private elements have started to address this need for intelligent data collection and conversion to useful information by adopting commercial metering, monitoring and networking products and services for aggregating and interpreting data that provides some level of situational awareness for intelligent decision-making.

Unfortunately, many of the design characteristics of our existing wireless networking infrastructure were conceived during the formative years of computing. The improvements we've seen to date are primarily traced to faster electronics and addition of more bandwidth. Even so, adoption of commercial products that utilize commercial cellular or Institute of Electrical and Electronic Engineers (IEEE) Standard waveforms (such as 802.11.x and 802.15.4) can rapidly overburden local network access points and available bandwidth on systems that utilize common one-size-fits-all TCP/IP Air Interface Protocols. The use of commercial metering and network products for critical government and commercial data collection systems will eventually incentivize development of an austere approach to total network packet transmission over shared wired and wireless spectra. The ideal solution for reliable, agile spectrum access for future telematics and ICS-type applications is to; (1) significantly reduce the number and rate of packet transfers from cognitive end devices (sensors/meters and monitors), and (2) minimize the network overhead for maintaining connections, routing, retries for bandwidth contention and network security.

1.3 NETWORK EXTENSION CONCEPT

One way to implement an austere packet exchange solution is by using smart (cognitive) end devices at the data collection point providing connectivity through a low-power wireless network. This low-power network acts as a local network extension allowing periodic, managed connection and exchange of aggregated information to a remote server over traditional high power and high bandwidth networks. Low-power Personal Area Networks (LoPANs) are attractive for this purpose in that the footprint of the network can be constrained to a specific locale in such a way as to not cause interference or contend for bandwidth with Wide Area Networks (WANs). Access between the former and the latter is provided through a network gateway. This gateway acts as a bridge to aggregate the information and communication packets from one or more smart or cognitive end devices and provides a portal to the user via a Wide Area Network in such a way that reduces the total bits and bytes of data and control files passing over the Wide Area Networks.

An innovative set of Air Interface Protocols (AIPs) described in US Patent # 8855311 provides one such set of solutions for a network extension to be used on existing network infrastructure supporting either distributed or centralized (cloud) computing. These patented AIPs are designed to act as a Secure Connectionless Intelligent Network Extension (SCINetEx) to any existing commercial, government, military or private (proprietary) network. The SCINetEx AIPs are wave-form agnostic, designed for open system architecture and support secure persistent machine-to-machine type information exchange that can support true artificially intelligent entities on a large scale. Overhead packet traffic for network discovery, authentication and data transfer with connection assurance functions are optimized for robust telematics and industrial control-type applications. These AIPs are designed to support smart (i.e., cognitive and intelligent) end devices as components of autonomous networks and ensure the following capabilities:

- Utilization of existing commercial, government, military and public Wide Area Networks and data repositories to the greatest extent possible.
- Enable smart sensors that protect the asset from intrusion and are capable of identifying state changes for decision making on when to send the data packets.
- Robust, local wireless communications capability to-and-from smart sensors resistant to jamming and extreme multi-path degradation.
- Employ wholistic security measures utilizing trusted circuit and device suppliers.
- Ensure availability, integrity, authentication, confidentiality and non-repudiation of data over trusted, untrusted or otherwise compromised networks.

A network extension is defined as a Local Area Network that can be implemented to meet these five objectives and minimize packet traffic on Wide Area Network connections to a remote operations facility. This technical report is intended to serve as a primer that describes to a usable detail, the protocols necessary to satisfy the communications requirement of a secure wireless communication network extension using smart end devices as described by SCINetEx. This includes the functionality within each Network Layer and its applicability within the context of the wireless end device to wired or wireless gateway interface. This technical report also addresses characteristics related to data interchanges that occur at the Application Layer,

including message formatting and command constructs. Data security, encryption and key management are also discussed in detail sufficient for basic implementation.

The SCINetEx concept enables utilization of common hardware sets for Ad-hoc message exchanges between smart end devices (mobile or fixed) and central data repositories with minimal bandwidth requirements. This technical report specifies in detail the communication protocols and network architecture needed to design the interfaces among all devices described in the following sections. The technical specifications here-in are non-proprietary and are intended to enable devices capable of global interoperability.

End devices that may be used as part of SCINetEx include battery operated, mains or vehicle-powered meters or monitors that are either located on a fixed or mobile host. This mobile host may be a vehicle, drone or any other artificially-intelligent entity capable of self-determination and locomotion. Overviews of various SCINetEx systems appear in Figure 2-1 and Figure 2-2. The primary purpose of the SCINetEx system is to provide a low-power network extension to monitor changes in the state of host device parameters as determined by the user. Table 1-1 is a compendium of the system interface elements and documentation.

Table 1-1. SCINetEx System Terms.

SCINetEx Term	Description (in the context of this technical report)
Smart End Device (SED)	Device that senses, logs, makes decisions and reports events per device application requirements. Such devices will include security monitors, fuel/energy/maintenance meters, system controllers/monitors and artificially intelligent entities.
Key Information Manager (KIM)	Entity that provides the cryptographic keys needed for SCINetEx system authentication and encryption/decryption discussed here-in. May be artificial intelligence (AI) or human-in-the-loop (HitL).
Data Aggregation Point (DAP)	In general, DAPs are data portals that pass secure messages between SCINetEx elements. At least one DAP will be designated to be the generic end-point for Smart End Device-originated messages and DAP responses. The DAP must be trusted and able to encrypt, decrypt and authenticate.
IEEE	Institute of Electrical and Electronics Engineers (Standard).
IEEE 802.15.4-2006	IEEE Standard for Media Access Control (MAC) and PHY, without battery-powered Mesh routing as in 802.15.5.
IEEE 802.15.5	(2009) IEEE Standard for Mesh network layer used with the IEEE 802.15.4-2006 MAC and PHY layer Standards.
LAN	Local Area Network (LAN). Typically privately owned for specific user.
WAN	Wide Area Network (WAN). The Internet, cellular network or satellite network. May also be other government, military or private network.

Physical Layer protocol (PHY)

Table 1-1. SCINetEx System Terms. (Continued)

SCINetEx Term	Description (in the context of this technical report)
Network Topology	Here-in, the network characteristic topology is per IEEE Standard 802.15.5 used with 802.15.4-2006. The topology is peer-to-peer, no Personal Area Network (PAN) coordinator, with certain nodes defined as gateways to Wide Area Networks (WANS).
Network Gateway (NG) Secure	Can be fixed (FNG) or portable handheld (HNG). Communicates with SEDs via wireless RF and the Data Aggregation Point (DAP) via Internet or, alternatively, cellular or satellite networks.
Network Gateway (NG) Non-secure	Can be fixed (FNG) or portable handheld (HNG). Communicates with SEDs via wireless RF and the Data Aggregation Point (DAP) via Internet or, alternatively, cellular or satellite networks.
MAC	Media Access Control (network) Layer protocol. Here-in, refers to a portion of the low-level protocol for wireless network between a Network Gateway (NG) and a Smart End Device (SED) or another Network Gateway.
PHY	Physical Layer protocol, i.e., modulated RF signal here-in.
NWK	Network Layer protocol (NWK), i.e., superior to MAC and PHY.
Mutual Authentication	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 SCINetEx system encryption keys is managed by a process defined here-in.

Physical Layer protocol (PHY)

This page intentionally left blank.

2. INTRODUCTION AND OVERVIEW

Collection and use of Industrial Control System (ICS) and telematics-type data on mobile and fixed assets is rapidly increasing. This is in part being driven by the need for visibility and control of energy distribution for operational considerations as well as logistics, maintenance, safety and training. Government and commercial organizations have started to address this need by adopting commercial metering, monitoring and networking products and services for aggregating and interpreting data that provides some level of situational awareness. Adoption of products that utilize commercial cellular or IEEE Standard waveforms (such as 802.11.x and 802.15.4) can rapidly overburden local network access points and available bandwidth on systems that utilize common TCP/IP Air Interface Protocols. The use of commercial metering and network products as part of the Internet of Things (IoT) necessitates development of an austere approach to total network packet transmission over shared spectrum. The ideal solution for reliable, agile spectrum access for telematics and ICS-type application is to; 1) significantly reduce the number and rate of packet transfers from end devices (sensors, meters and monitors), and 2) minimize the network overhead for maintaining connections, routing, retries for bandwidth contention and network security.

Smart End Devices (SEDs) are defined as any sensor, meter or monitor that collects data from an asset (mobile or fixed) and, through embedded firmware, analyzes that data for changes in state of the asset or its surroundings. A SED may be the control unit of assets such as manned vehicles, robots or drones. If a state change is detected, the SED has the capability to independently determine whether a status change message (alert or alarm etc...) must be reported via hardwire or wireless connection to a supervising system. Examples of SED inputs include maintenance sensors, fault code sensors, fuel meters, fuel-level sensors, cargo security sensors, intrusion detectors, industrial control devices, logistics trackers and any device that senses and records location or change in environment or movement for robotics or automation.

Following sections of this technical report describe in detail the protocols necessary to satisfy the communications requirements of a SCINetEx system construct, including the functionality required within each layer of the system and its applicability within the context of the Smart End Device-to-Network Gateway interface. This text also covers requirements related to data interchanges that occur at the Application Layer of each device, including data and message formatting and command constructs. Data security, encryption and key management are addressed in excruciating detail. The remainder of this section discusses co-mingling of multi-user data sets, applicable communication regulations, and, provides a basic SCINetEx system overview.

2.1 HIERARCHICAL MESSAGING

The intent of this section is to describe common hardware for message exchanges based on a general user hierarchy. The highest level message hierarchy always belongs to that user or organization that has final governance over the network. This may be the owner of the facility or where the network physically exists, or the primary user of the network in virtual space, or the governing entity that is tasked with coordination and collection of data from all parties involved. Hierarchical message types are defined in detail in a later section to ensure complete interoperability of the overall SCINetEx system. Message traffic for all user-hierarchies may use the same hardware and lower level (MAC and PHY) protocols/ firmware. When operating on the same RF channel and Personal Area Network ID (PAN ID), such traffic must use a common message header to segregate traffic in a coordinated manner. Alternatively, traffic for different user-hierarchies can be conducted on other channels and/or PAN IDs at a specific locale.

For purposes of the following discussion, the command and data messaging in support of the highest-level user hierarchy (i.e., the governing user) are referred to as security or security-purposed messages. The governing user is generally responsible for security of all aspects of the network. All lower-level hierarchy users will be referred to as non-security or non-security-purposed messages. Non-security messaging can be either proprietary or non-proprietary. Proprietary messages contain content that a user on a lower-level hierarchy wants to keep private (using encryption) from all other users. The content of non-proprietary messaging may be viewed by the highest-level (i.e., governing) user. Proprietary content should not be placed into non-proprietary-purposed messages defined here-in during either storage or transport. (See Section 8 for all data requirements.) Proprietary messages are transported by the SCINetEx system to the desired commercial network address other than that of the highest level user through a DAP. The DAP has the option to ignore proprietary messaging addressed to it (as long as the users know that). Battery power usage for proprietary-purposed messaging should not violate power availability requirements for non-proprietary-purposed messaging for battery-powered devices. The hierarchical messaging strategy is also a means to control communications between artificially intelligent entities that are linked through the SCINetEx system.

2.2 PRECEDENCE AND NOMENCLATURE

This technical report addresses the requirements specific to the structure used for data and command transmittal and bi-directional communications between end devices and the SCINetEx system. IEEE Standard 802.15.4-2006 is the basis for forming the RF protocols described here-in. Unless otherwise specified, this standard should be used for definitions of terms.

2.3 REGULATORY REQUIREMENTS

Within the United States, FCC 47 CFR Part 15.247 rules apply to all embodiments of the SCINetEx system and take precedence. Wireless devices utilizing interfaces defined here-in 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 for the SCINetEx system are intended to facilitate interoperability at the RF link budget level.

NOTE: The minimum effective (i.e., external to a shielded box or container) radiated power is also specified for SCINetEx system devices that communicate with infrastructure or peers.

2.4 SYSTEM OVERVIEW

The wireless pathway from a Smart End Device (SED) to a store-and-forward data site includes bi-directional wireless interfaces between sensors, meters, monitors and control units mounted on or in the asset being hosted. These pathways may also include a combination of cellular, satellite and Wireless Personal Area Networks (WPANs) based on IEEE Standard 802.15.4-2006. The communication links for WPANs are fully described here-in, including the structures of messages coming from the Smart End Devices and commands going to them. Communication links for cellular and satellite modes are treated as embedded Wide Area Networks (WANs) and are also covered.

What follows is an unambiguous specification for SCINetEx message types, sequences, content and security in such a way that interoperability is assured worldwide between any DAP and any manufacturer's Smart End Device, irrespective of the end-to-end communications media. Proprietary messages may be transported by this same network and use the reserved message header code described here-in.

Figure 2-1 is a network topology-level view of facility-wide wireless coverage and connectivity with remote store-and-forward data sites. Moving nodes include communications devices in or on mobile assets. Fixed Network Gateways are stationary nodes that may be pole-or structure-mounted. These are typically entrance or egress points from a specific locale that bridge data to/from other networks that reach the DAP. Mobile Network Gateways may be man-portable or mounted on vehicles, drones or any other asset with self-powered locomotion.

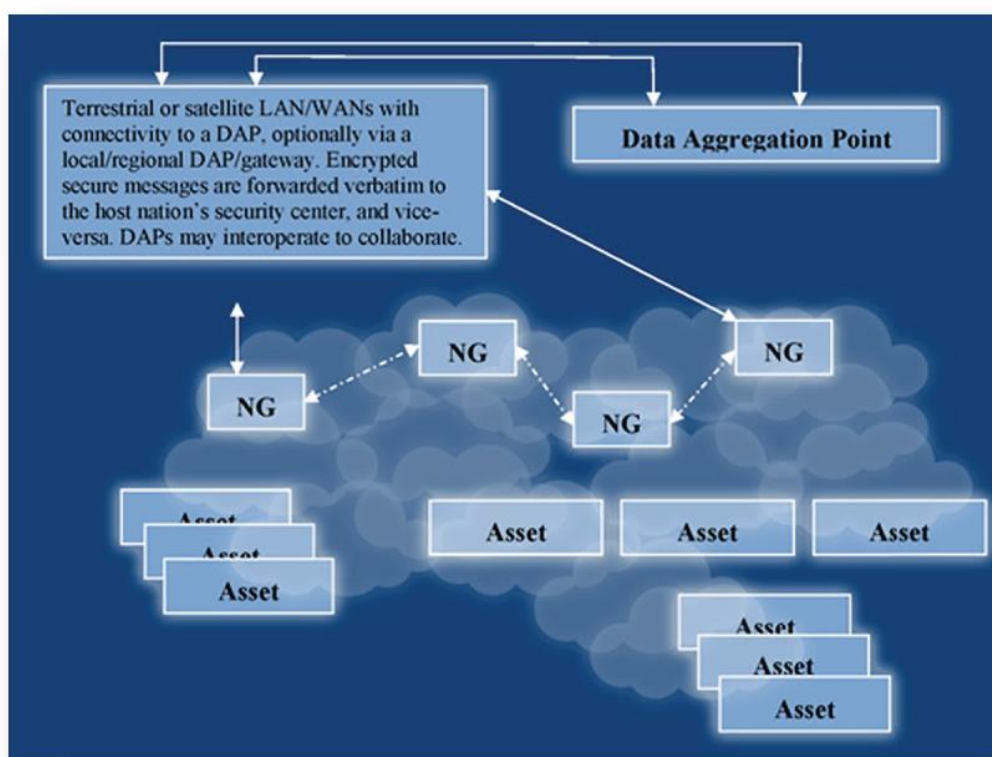


Figure 2-1. Network Topology Example: Dispersed Assets (fixed or mobile).

All Network Gateways (NGs) provide; 1) small-area, and 2) wide-area connectivity to a distant DAP. Some NGs may be wired bridges to a second network to begin the data to/from a DAP. Where data wiring is impractical, other NGs may be wireless bridges and use neighboring NGs for DAP connectivity. These NGs also prevent "stranded" metered assets with no route to a DAP. The coverage radius of any given NG will be constrained by physical structures, conveyance obstruction and antenna selection. Figure 2-2 depicts the network elements to which this text applies.

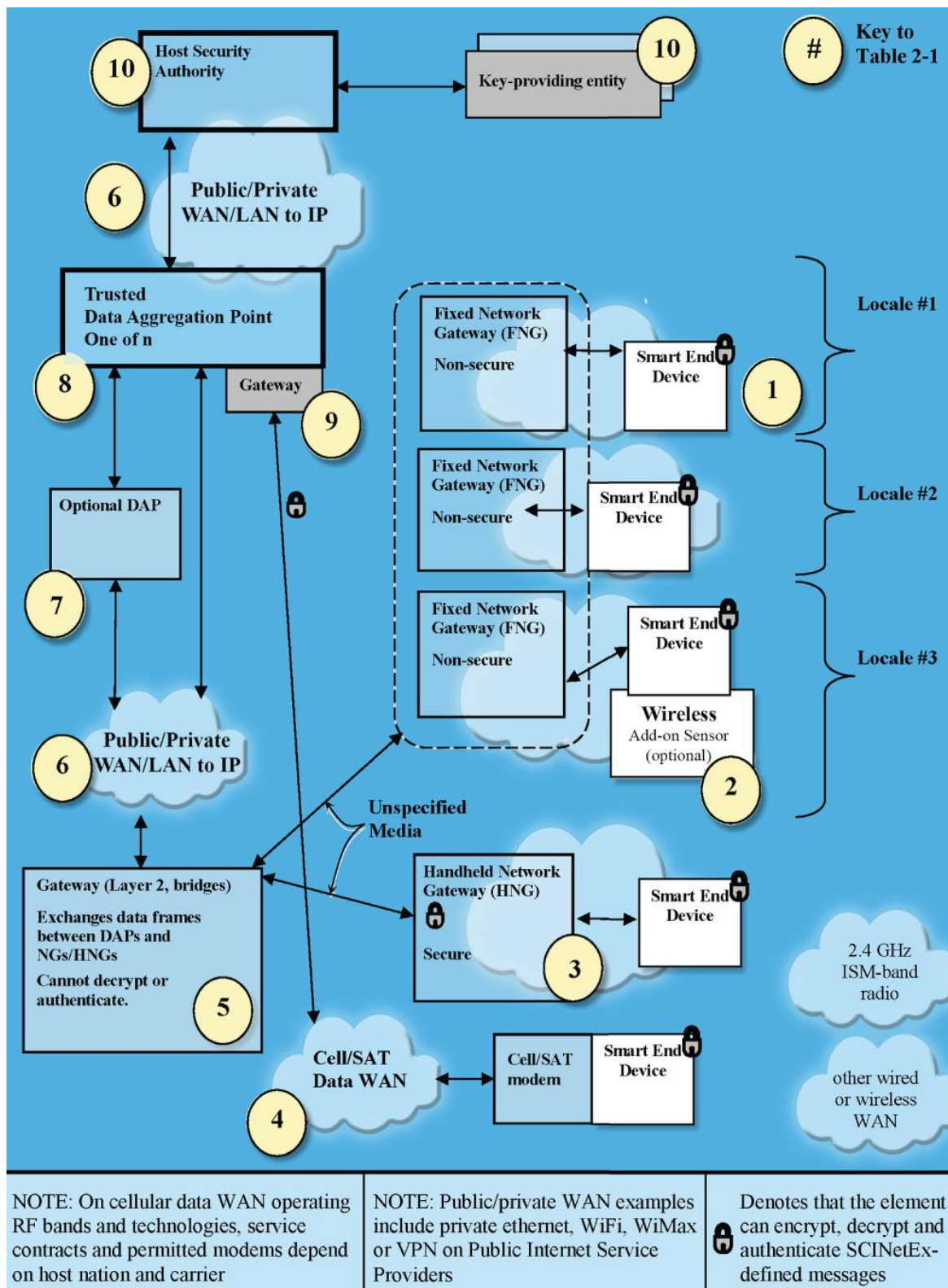


Figure 2-2. SCINetEx System Overview.

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

Table 2-1. Network Element Descriptions.

Key	Topic	Summary Description
1	SED-to-NG connectivity	Low-power, bi-directional unlicensed band wireless data per IEEE Standard 802.15.4-2006. An NG provides wireless coverage of asset-mounted SEDs and exchanges message data with DAPs via Local/Wide Area Networks (LAN/WAN), the message content of which is specified by SCINetEx.
2	Wireless Add-on Sensor inside or on asset	Wireless sensors, meters and monitors are considered part of sensor management. The protocol for the wireless sensor interface and data transfer is defined by SCINetEx.
3	Secure NG	The secure NG is a Network Gateway that also emulates a subset of DAP functions. Mutual authentication between the secure NG and the SED, if required, is performed using key management procedures detailed in Section 9. Some NGs can issue a subset of commands that do not require authentication as a non-secure NG.
4	Cellular/Satellite access network	Asset-mounted devices must use the wireless mechanism defined by SCINetEx and may use cellular or other public wireless carrier as optional secondary modes.
5	Gateway	NGs connect to the gateway controller 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. SCINetEx defines messaging in such a way that messages can be sent using either a connectionless protocol such as User Datagram Protocol (UDP) or simply as serial data with a fast time-out for end-of-message. The gateway controller is responsible for sending DAP (item 8) messages to the originating SED via the last-used NG.
6	Public/Private LAN/WAN	Transport media used by the gateway controller (item 5) to exchange data directly with its designated DAP (item 8) or with an intermediate DAP (item 7).

Yellow circled numbers correlate with defined regions in Figure 2-2.

Table 2-1. Network Element Descriptions. (Continued)

Key	Topic	Summary Description
7	Optional Data Aggregation Point (DAP)	Optional DAPs that cannot encrypt or decrypt may be utilized for lower-level user hierarchical purposes. Such untrusted DAPs should retransmit security-purposed messages verbatim between SCINetEx system components.
8	Trusted Data Aggregation Point (DAP)	Encryption key possession enables communication with asset-mounted devices for security purposes. The trusted DAP consolidates security-related messages for the Security Authority (item 10). The method of this communication is not specified by SCINetEx.
9	Cellular/Satellite Gateway(s)	SCINetEx messages exchanged with a SED and a trusted DAP (item 8) flow through a gateway determined by the cellular or satellite service provider. The transport layer protocol is not described by SCINetEx and is not trusted.
10	Key-providing entity — Key Information Manager (KIM)	Trusted third party issues digital encryption keys stored in and used by on-asset devices (item 1), secure NGs (item 3) and trusted DAPs (item 8) for authentication, encryption/decryption and other purposes. Key management methods are defined in Section 9.

Yellow circled numbers correlate with defined regions in Figure 2-2.

2.4.1 Primary Wireless Medium – Summary

The primary wireless medium for all devices is summarized as follows and detailed in the following sections.

- 2.4 GHz band and power per the least common denominator among regulatory domains.
- IEEE 802.15.4 MAC/PHY strictly per the Standard.
- Peer-to-peer topology, no PAN coordinator, no beacons, no Time Division Multiple Access (TDMA)/Guaranteed Time Slots (GTS).
- Emphasis on assured interoperability among SCINetEx-compliant client and access devices.
- Data frame addresses are 64-bit IEEE MAC addresses with no Network Layer addresses.
- Addresses of fixed, handheld and on-asset devices are discovered per SCINetEx.
- Battery conservation “low power state” enabled per Message Waiting indicator described in a later section.
- Optional use of relay/repeaters.
- End-to-end message security provided by Application Layer encryption and authentication.
- End-to-end message security does not utilize IEEE Standard 802.15.4 MAC Layer encryption, which is disabled.
- SCINetEx-defined messages enable end devices to passively discover fixed and handheld network gateway devices’ MAC addresses.

2.4.2 Smart End Device (SED)

A Smart End Device (SED) is any device that can be installed on a fixed or mobile asset to monitor change in status or provide operational parameter control. Typical examples include such things as cargo containers (open/close), fuel tanks (levels or transactions), vehicle Controller Area Network (CAN) bus data (OBD codes or engine characteristics), generators (electrical output, load), structural sensors (bridges, warehouses) and drones or robotic control units. Smart End Devices generally provide status updates when a measured parameter has changed and may provide some sort of heartbeat function to sustain periodic communications connections. The sensing phenomenology and state change analytics for any SED may be proprietary and are not described here-in. SCINetEx defines only the data structures for messages from, and, commands to the SED and are specified in later sections. For security-purposed operations and the hierarchical user strategy, these messages and commands include encrypted information. The encryption process for these messages is also defined by SCINetEx.

Every SED incorporates an embedded Communications Module (CM) as a primary subsystem. CMs are intended to be employed in many configurations including as stand-alone relays or as Radio Frequency Identification (RFID) tags to track assets for In-transit Visibility (ITV). These are referred to as External Communications Modules (ECMs).

2.4.2.1 Embedded Communications Module (CM)

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 2-2, an embedded CM communicates with a nearby Network Gateway (NG) that can be fixed or mobile or handheld. This gateway then communicates in turn via relays and intermediate WANs with the trusted DAP. The “ends” in this end-to-end communication are the embedded CM and the DAP. The CM may be either a battery or mains-powered device that provides wireless connectivity in the 2.4 GHz ISM-band as its primary communication mode. In the SCINetEx system, a CM will always be embedded in a Smart End Device.

2.4.2.2 External Communications Module (ECM)

An External Communications Module (ECM) will have one of three configurations based on its functions:

- Relay for tethered device only
- Location and tracking only
- Both of the above

Given international constraints on radiated emissions, it is likely that a Smart End Device mounted on an asset (either fixed or mobile) will sometimes fail to meet range requirements in primary communication mode (i.e., IEEE Standard 802.15.4-2006 wireless connectivity) as part of a network extension. Policies that restrict where a SED can be installed or the need for rapid SED installation and removal may also preclude modifying an asset in order to use an external antenna. An external “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 may provide Global Positioning System (GPS) functionality and may have the means to use cellular, satellite or act as a transparent bridge to other wireless alternatives. SCINetEx defines messaging supporting these options. When implemented, SCINetEx system elements using these media as a transport layer service support verbatim exchange of messages, payload encryption and

Application Layer, Acknowledge (ACK) protocols (defined in later sections) to simplify the DAP interface with a variety of communications media.

The ECM must interoperate with all devices that comply with SCINetEx constructs, even if they are produced by different manufacturers. To enable this interoperation, this section defines the standards for communication between the ECM and the SED's embedded CM.

The SED may communicate directly with an NG if propagation conditions permit. If not, the SED will attempt to communicate via an ECM if one is present. The decision to use an ECM should be based on the availability of NG connections and the SED power management scheme.

The ECM should be small enough to be installed on an asset in such a way that it does not protrude from the profile of the asset to avoid physical damage. The ECM will notify the primary hierarchical user of its removal from the asset 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 asset or some other unspecified means.

2.4.2.3 Wireless Add-on Sensor (AoS)

The SEDs may accommodate wireless sensors using IEEE Standard 802.15.4-2006 protocols as described in the following sections for use by Add-on Sensors (AoS). A wired Add-on Sensor bus for non-integral sensors is sometimes not advised for security reasons. AoSs can be installed and utilize the wireless IEEE Standard 802.15.4-2006 link to provide additional security functions, such as embedded sensors provide. The AoS wireless interface can also carry hierarchical user-purposed information such as temperature, cargo status or inventory management. All data and commands passing wirelessly between an AoS and a SED must be encrypted as described in later sections.

2.4.3 Network Gateway (NG)

A Network Gateway (NG) is any appropriate mix of hardware, software, network services and internal interfaces that satisfies the requirements specified for transport to the WAN, including functionality, user interface and error detection/correction. NGs have multiple physical configurations to support fixed installations, mobile installations, arming or commissioning operations, backhaul communications and mobile inspection activities.

CMs and DAPs exchange information via intervening NGs using the messages defined by SCINetEx. An NG retransmits verbatim all wireless data traffic between CMs and DAPs. The message content and the application-level messaging between CMs and NGs are also defined by SCINetEx. The wireless link between CMs and NGs is the 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 CMs and DAPs, are regarded as "untrusted". The data transport mechanism between NGs and DAPs are described in later sections. An NG may be fixed or handheld. Handheld NGs are mobile by definition. The descriptors FNG (fixed NG) and HNG (handheld NG) are used here-in to enable differentiation between fixed and handheld NGs, while the term "NG" encompasses all potential wireless interfaces to the SCINetEx system. The following sections describe the general properties of these devices.

2.4.3.1 Fixed Network Gateway (FNG)

Functional requirements for FNGs must be defined by the implementing organization (most likely the owner or user). It is assumed that FNGs can be considered either secure (trusted) or non-secure (untrusted). FNGs are intended to be permanently installed units physically secured where mobile assets congregate or other fixed assets are generally located. Potential FNG installation sites include loading docks, facility in/out gates, light poles and rooftops. As such, the preferred implementation of

an FNG is as a non-secure network element providing IP connectivity to the DAP such that communication can occur in real time.

SEDs that are within an FNG's wireless coverage, attempt to exchange encrypted messages with the DAP with which the FNG is associated. The non-secure FNG is incapable of decryption and is considered a non-secure unattended network "bridge" element. A non-secure FNG is not a trusted device with respect to network security and information assurance.

The FNG-to-DAP data is merely the unmodified message packets defined here-in. For non-secure FNGs, no decryption is done until message receipt at either end of the transmission path (i.e., at the DAP or at the SED). This property (encryption/decryption only at Application Layer end points) permits all intervening networks used for security-purposed messaging to be untrusted.

2.4.3.2 Handheld Network Gateway (HNG)

Functional requirements for the HNGs must be defined by the implementing organization (most likely the owner or user). It is assumed that HNGs can be secure (trusted), non-secure (untrusted) or arming-only (untrusted). Secure HNGs are 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 (i.e., the Key Information Manager), as discussed here-in (see Figure 2-2). A non-secure HNG is capable of executing unrestricted message exchanges also defined here-in. The Key Information Manager (KIM) will not provide encryption keys to a non-secure HNG, which is therefore incapable of encrypted message exchanges.

The arming-only HNG has a device-type that only allows limited access to execute a subset of restricted commands. All HNGs communicate with the SED directly. The secure and arming-only HNGs communicate to the DAP over an IP connection via a cradle, USB or equivalent connection. The secure HNG is assumed to be fully controlled by a trusted agent and functionally support a subset of the DAP-originated messages exchanged between a SED and a DAP. Therefore, a secure HNG must have the credentials to decrypt and encrypt after mutual authentication between itself and the device. The secure HNG must implement a subset of DAP message commands, responses, authentication, encryption and decryption.

2.4.3.3 Commercial Cellular WAN

Embedded subsystems or components providing WAN/IP connectivity to DAPs are referred to as Embedded Network Gateways (ENGs). ENG-to-DAP transport requirements are defined by the SCINetEx system. An embedded secondary communications mode that SEDs can use for backhaul and emergency notification is commercial cellular data service. Embedded cellular data service is considered here-in to provide the same functionality as the cellular data service provided by an NG, so this does not require separate definition of communications between the SED and the cellular subsystem. This requires only that data payloads be exchanged between SEDs and the DAP in such a way that the use of any WAN is transparent to both end points. One option enabled by this is to use User Datagram Protocol (UDP) datagrams containing the payload data defined here-in for security-purposed messages. Security for security-purposed data is defined at the Application Layer in later sections of this technical report. When the cellular communications mode is utilized, SEDs can be capable of transmitting an emergency notification of an unauthorized access or removal along with its location. The SED should 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 device power is fully depleted if battery-operated.

2.4.3.4 Commercial Satellite WAN

Satellite communication service can be treated as an Embedded Network Gateway (ENG), with communication functions as described above for cellular.

2.4.3.5 Asset Direct-To-WAN

SEDs may have alternative, non-WAN communication mechanisms not specified here-in. The following recommendations apply to SEDs:

- To simplify interoperability with any Data Aggregation Point (DAP), SEDs will use the message formats defined by SCINetEx. These messages are independent of transport media.
- Messages defined here-in are for use with small packets, as in IEEE Standard 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 IEEE Standard 802.15.4-2006, satellite-based UDP, and cellular Short Message Service (SMS) or Internet UDP. The transport protocol for cellular and satellite are defined by SCINetEx as is message content and format, irrespective of the means of transport.
- Such devices should implement this technical report's standard for interfaces to wireless sensors to permit standardized sensors.

2.4.4 Data Aggregation Point (DAP)

Trusted DAPs exchange security-purposed messages with SEDs. Only trusted DAPs can generate and encrypt security-related (i.e., restricted) commands or decrypt the corresponding encrypted responses and other encrypted security-purposed traffic. The encrypt/decrypt capability requires cryptographic keys provided by an entity functionally distinct from the DAP. Trusted DAPs are generally found in regional or national-level operations centers of the highest-level hierarchical user.

Section Summary

- End-to-end messaging principles utilized with data encrypted at the Application Layer.
- Fragmentation and reassembly of messages not required.
- Utilizes Wide Area Networks (WANs) for global data transport.
- WANs do not need to be trusted.

3. SYSTEM EMBODIMENTS

This section presents a general overview for several practical applications of the SCINetEx communications protocols and concepts. Each example is intended to provide the reader a foundational understanding of how such a system can be designed and used in real-world scenarios. The first four examples have all been demonstrated under operational conditions by the US Department of Homeland Security (DHS) and the US Department of Defense (DOD). The final example is an extension of the distributed networking concept for Smart End Devices to incorporate systems and subsystems that utilize artificial intelligence for decision making and direct intra-asset communication free of human moderation.

3.1 IN-TRANSIT VISIBILITY

In-transit Visibility, sometimes referred to as ITV, is the ability to identify, track the location and sometimes status of persons or cargo from one location to another. Tracking data is usually provided using multiple modes of communication which include commercial or private WANs that utilize private LANs that act as network extensions to the WANs. Data is collected and stored at one or more data repositories. The ITV data sets should always include a unique identifier of the item being tracked. This identifier may be a tracking device Universal Identifier (UID) or Media Access Code (MAC) address, manifest number, shipping number, container number, license number, bumper number or personal identifier (if the item being tracked is a person). In addition, ITV data sets may include contextual information such as one or more security seal numbers (if cargo container), a shipper's ID number that is registered by an over-arching authority and/or Bill of Lading (BoL) number. When tracking cargo, that cargo may be unitized (package items) or bulk materials such as fuels and agricultural products. More sophisticated ITV technologies may provide condition information such as temperatures the cargo was exposed to during transit. All ITV systems should provide the user information about where the cargo or persons originated, what is the cargo, when it left the original facility and what is the intended destination. ITV data most generally gives the user tracking information on the intended cargo or personnel that was in transit and does not include cargo that was removed or added to the asset or personnel during the transit process. Radio Frequency Identification (RFID) is commonly associated with ITV systems. These types of systems are routinely extended to use for tracking items inside warehouses. Warehouse tracking systems is addressed in Section 3.3.

3.1.1 General Concept of Operations

The essential role of an ITV tracking system is to record and report when an ITV tracking device has been detected by one or more Network Gateway devices. These Network Gateways are connected to each other through a remote Data Aggregation Point that communicates to the Network Gateway via commercial or private WAN. Tracking devices are routinely referred to as "tags". These tags are routinely commercial RFID technology that may be read-only or able to accept commands and update data stored on the tag. Gateways are usually located at critical locations in the transit route of the items or persons being tracked. These locations routinely include the facility where the

transit began, entrance and exit gates at intermediary facilities where transportation mode changes occur (i.e., truck to rail, ship or aircraft) and at entrance gates or loading docks at the product destination. The system implementer will establish the extent of the gateway deployment and details of the data flow between components of the ITV system. Generally, this system data flow will

include these basic components as seen in Figure 3-1. If the asset begins its transit at a foreign facility, the first drayage is foreign and the last drayage is domestic. If the asset begins its transit from a domestic facility, the first drayage is domestic with the last being either foreign or domestic. Drayage transports may also have WAN gateways for monitoring asset conditions and locations but are not required. All WAN gateways forward data to the Data Aggregation Point.

3.1.2 ITV System Components

All ITV system end devices must be able to communicate with the Data Aggregation Point by either wired or wireless means. The communications protocols are detailed in later sections of this technical report. ITV system components may be battery-operated or mains-powered when mounted on fixed or mobile assets. ITV end devices are components that monitor the state and location of the fixed or mobile assets they are mounted on. These end devices maintain an internal electronic log of all state change events that they are designed to detect. The event record log structure and method(s) of downloading the event record log are detailed in later sections of this technical report. The end device and the Data Aggregation Point bi-directionally communicate with each other through the WAN gateways. This connection usually includes a LAN network extension however some assets may be of sufficient value to justify putting a WAN gateway (such as a cellular modem) directly on the asset.

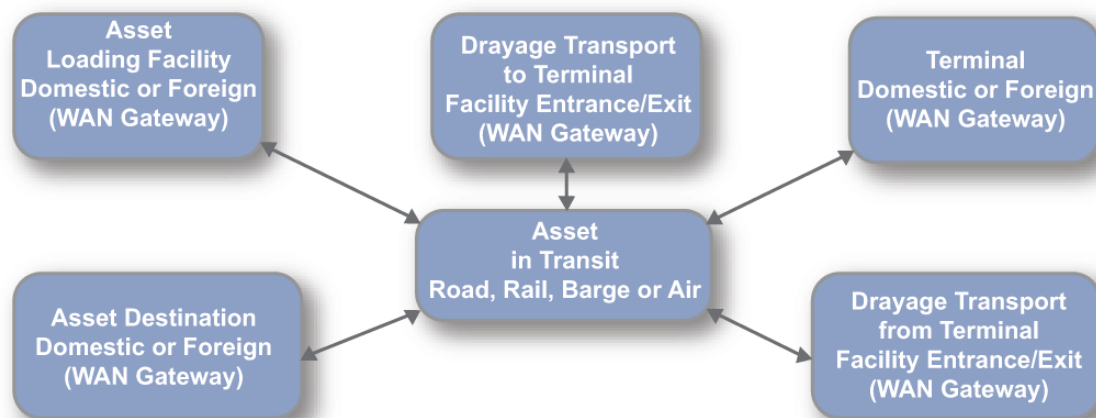


Figure 3-1. Concept of Operations ITV.

WAN gateways provide bi-directional wireless communications interface to the end devices. For LAN extensions, the waveform described in later sections is IEEE Standard 802.15.4 2006. WAN gateways support the following tasks:

- Identify end devices in their RF communication range,
- Establish a wireless network connection with the end device,
- Deliver SCINetEx commands to the end device,
- Acquire end device Status messages and event logs and
- Communicate Status messages and event logs to the Data Aggregation Point.

Data Aggregation Points receive data from the end devices forwarded by the WAN gateways. In an operational system the Data Aggregation Point will collect data from many asset-mounted end devices. From an external point of view, the Data Aggregation Point is considered a secure server that distributes ITV data to other authorized users or information systems.

3.1.3 Considerations for In-Transit Visibility

It is not the intent in this section to describe in detail the network architecture for an ITV system. Rather, to simply provide some context into how such a system has been previously developed. Each system utilizing SCINetEx-compliant communications protocols may have subtle differences including the type of WAN utilized. It is important to understand that under SCINetEx, untrusted WANs are the rule, not the exception. These WANs may be public, private, government, commercial or military. The type(s) of WANs used for ITV will determine the detailed interface requirements for each WAN gateway.

3.2 SECURITY

Security as a SCINetEx embodiment includes the capability to monitor both mobile and fixed assets and personnel in and around a secured facility. Location and state data can be collected and transmitted to data repositories located at local command centers that oversee the facility operation. As with ITV applications, status and tracking data are usually provided using multiple modes of communication which include commercial or private WANs that utilize private LANs that act as network extensions to the WANs. These private LANs may utilize the Ad-hoc Mesh network features of SCINetEx described in later sections of this technical report. The security embodiment of SCINetEx may be combined with the ITV features to provide a robust cargo security system. In both cases, data sets should always include a unique identifier of the item or person being tracked. This identifier may be a tracking device Universal Identifier (UID) or Media Access Code (MAC) address, manifest number, shipping number, container number or personal identifier (if the item being tracked is a person). In addition, security data sets may include contextual information such as one or more security seal numbers (if cargo container), a shipper's ID number that is registered by an over-arching authority and/or Bill of Lading (BoL) number. Security sensors may provide condition information such as intrusion attempts and temperatures of the space or asset being monitored. SCINetEx also supports command messages for locking or unlocking doorways or hatches and geo-fencing. When coupled with trusted agents as users, these features are very useful for Chain of custody applications. All security systems should provide the user information about who accessed the security data, where the cargo or persons are located as well as historical data.

3.2.1 General Concept of Operations

The essential role of any security system is to record and report when and where a security device has been detected by one or more Network Gateway devices. These Network Gateways are connected to each other through a remote Data Aggregation Point that communicates to the Network Gateway via commercial or private WAN. Security devices may be referred to as "tags" in some cases but more often referred to as sensors. Gateways are usually located at critical locations in the transit route of the items or persons being tracked but sometimes these gateways are mounted on autonomous security vehicles or mobile robotic systems. These locations routinely include the facility where the transit began, entrance and exit gates or in storage spaces. The system implementer will establish the extent of the gateway deployment and details of the data flow between components of the security system. Generally, this security system data flow will include these basic components as seen in the following figure.

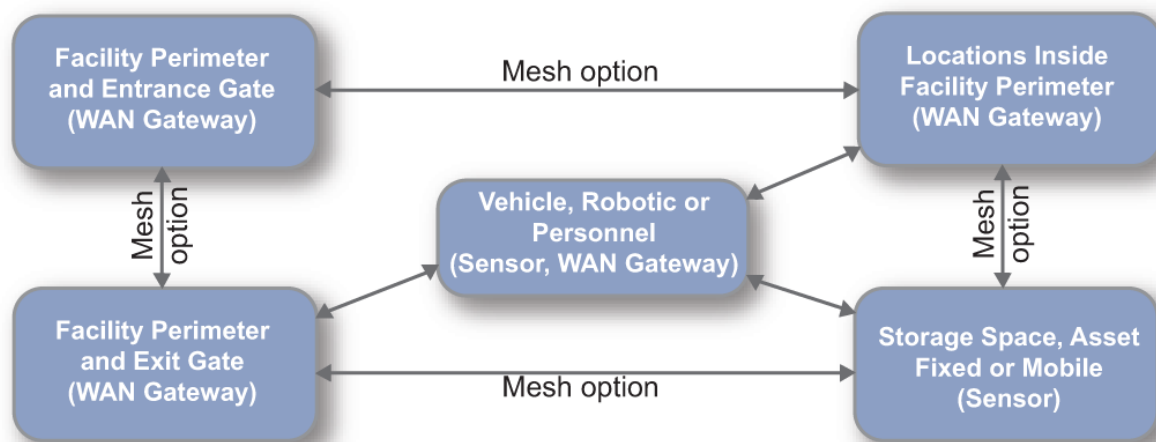


Figure 3-2. Concept of Operations Security Systems.

3.2.2 Security System Components

All security system end devices must be able to communicate with the Data Aggregation Point by either wired or wireless means. The communications protocols are detailed in later sections of this technical report. Security system components may be battery-operated or mains-powered when mounted on fixed or mobile assets. Security end devices are components that monitor the state and location of the assets or spaces where they are mounted. These end devices may detect intrusion, lock status and/or location and maintain an internal electronic log of all state change events that they are designed to detect. The event record log structure and method(s) of downloading the event record log are detailed in later sections of this technical report. The end device and the Data Aggregation Point bi-directionally communicate with each other through the WAN gateways. This connection usually includes a LAN network extension however some assets may be of sufficient value to justify putting a WAN gateway (such as a cellular modem) directly on the asset.

WAN gateways provide bi-directional wireless communications interface to the end devices. For LAN extensions, the waveform described in later sections is IEEE Standard 802.15.4 2006. WAN gateways support the following tasks:

- Identify end devices in their RF communication range,
- Establish a wireless network connection with the end device,
- Deliver SCINetEx commands to the end device,
- Acquire end device Status messages and event logs and
- Communicate Status messages and event logs to the Data Aggregation Point.

Data Aggregation Points receive data from the end devices forwarded by the WAN gateways. In an operational system the Data Aggregation Point will collect data from many space or asset-mounted end devices. From an external point of view, the Data Aggregation Point is considered a secure server that distributes security data to other authorized users or information systems.

3.2.3 Chain of Custody System Components

Chain of custody system components are identical to the security system components with the added capability of initiating an action (such as lock/unlock) by command or based on geo-location. This type of technology is generally used in conjunction with a trusted agent. This trusted agent may be human or artificially intelligent.

3.2.4 Considerations Regarding Security Systems

It is not the intent in this section to describe in detail the network architecture for a security system. Rather, to simply provide some context into how such a system has been previously developed. Each system utilizing SCINetEx-compliant communications protocols may have subtle differences including the type of WAN utilized. It is important to understand that under SCINetEx, untrusted WANs are the rule, not the exception. These WANs may be public, private, government, commercial or military. The type(s) of WANs used for security systems will determine the detailed interface requirements for each WAN gateway.

3.3 FACILITY AND WAREHOUSE MANAGEMENT

The facility and warehouse management embodiment of SCINetEx is in many ways similar to ITV. One major objective is to monitor logistical supplies or items carried by assets inside a perimeter building. If the facility is a factory or maintenance center, there may be supplemental objectives for monitoring power plant performance, machines (or robotics) operating on the facility floor and environmental conditions. Data collected in this embodiment may be utilized for monitoring equipment productivity, availability of product or supplies. Analytics and visualization tools can be used to provide predictive performance measure and visibility across the facility. Meters, monitors and gauges are used in these facilities to monitor fuel, oil and lubrication subsystems of critical equipment. Monitors can also include RFID tags for pallet or package-level tracking. Power distribution and management for environmental systems across large facilities can also be supported. Machine-to-machine (M2M) communications and Industrial Control Systems (ICS) are also common applications for the SCINetEx concept.

3.3.1 General Concept of Operations

The essential role of any facility and warehouse management system is to record and report when and where a tracking, meter, monitor or gauging device has been detected by one or more Network Gateway devices. These Network Gateways are connected to each other through a remote Data Aggregation Point that communicates to the Network Gateway via commercial or private WAN. Tracking devices may be referred to as “tags”. Gateways are usually located at critical locations in the transit route of the items or equipment being tracked but sometimes these gateways are mounted on autonomous security vehicles, mobile robotic systems or as handheld devices used by personnel. These locations routinely include the facility perimeter where the transit began, entrance and exit gates or in storage spaces. The system implementer will establish the extent of the gateway deployment and details of the data flow between components of the facility and warehouse management system. Generally, this system data flow will include these basic components as seen in the following figure.

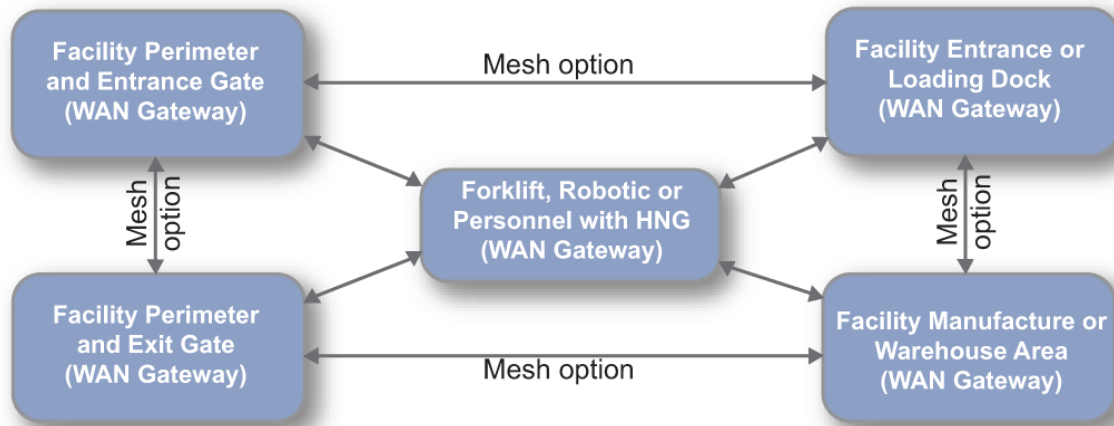


Figure 3-3. Concept of Operations Facility and Warehouse Management.

3.3.2 Facility and Warehouse Management System Components

All facility and warehouse management system end devices must be able to communicate with the Data Aggregation Point by either wired or wireless means. The communications protocols are detailed in later sections of this technical report. Facility and warehouse management system components may be battery-operated or mains-powered when mounted on fixed or mobile assets. Facility and warehouse management end devices are components that monitor the state and/or location of the assets where they are mounted. These end devices may detect equipment status, environmental conditions, plant operations and/or location of assets and maintain an internal electronic log of all state change events that they are designed to detect. The event record log structure and method(s) of downloading the event record log are detailed in later sections of this technical report. The end device and the Data Aggregation Point bi-directionally communicate with each other through the WAN gateways. This connection usually includes a LAN network extension however some assets may be of sufficient value to justify putting a WAN gateway (such as a cellular modem) directly on the asset.

WAN gateways provide bi-directional wireless communications interface to the end devices. For LAN extensions, the waveform described in later sections is IEEE Standard 802.15.4 2006. WAN gateways support the following tasks:

- Identify end devices in their RF communication range,
- Establish a wireless network connection with the end device,
- Deliver SCINetEx commands to the end device,
- Acquire end device Status messages and event logs and
- Communicate Status messages and event logs to the Data Aggregation Point.

Data Aggregation Points receive data from the end devices forwarded by the WAN gateways. In an operational system the Data Aggregation Point will collect data from many space or asset-mounted end devices. From an external point of view, the Data Aggregation Point is considered a secure server that distributes security data to other authorized users or information systems.

3.3.3 Considerations for Facility/Warehouse Management

It is not the intent in this section to describe in detail the network architecture for a facility and warehouse management system. Rather, to simply provide some context into how such a system has been previously developed. Each system utilizing SCINetEx-compliant communications protocols may have subtle differences including the type of WAN utilized. It is important to understand that under SCINetEx, untrusted WANs are the rule, not the exception. These WANs may be public, private, government, commercial or military. The type(s) of WANs used for facility and warehouse management will determine the detailed interface requirements for each WAN gateway.

3.4 FLEET MANAGEMENT

Fleet management is the ability to identify and track the location and status of mobile assets or persons from one location to another to support optimization of some aspect of the overall fleet performance. Tracking data is usually provided using multiple modes of communication which include commercial or private WANs that utilize private LANs that act as network extensions to the WANs. Data is collected and stored at one or more data repositories. The fleet management data sets can be used for many reasons including maintenance, safety, training, resource tracking and energy use optimization. In all cases, data should include a unique identifier of the asset being tracked. This identifier may be a tracking device Universal Identifier (UID) or Media Access Code (MAC) address, container number, license number, bumper number, serial number or personal identifier (if the item being tracked includes data on a person, such as the driver). In addition, fleet management data sets may include contextual information such as data from the on-board CAN bus sensors, external sensors and information about the vehicle loading. More sophisticated fleet management technologies may provide conditional information such as temperatures and terrain the asset was exposed to during transit. Fleet management data most generally gives the user tracking information on the asset or group of assets that was in transit and may not include cargo that was removed or added to the asset or personnel during the transit process. ITV and security systems can be used in conjunction with fleet management as well as metering, monitoring and gauging under the SCINetEx concept.

3.4.1 General Concept of Operations

The essential role of a fleet management system is to record and report location, condition and state change data when the asset has access to one or more Network Gateway devices. State change data may include changes in vehicle fault codes or other non-integral sensors, meters, monitors and gauges. Network Gateways are connected to each other through a remote Data Aggregation Point that communicates to the Network Gateway via commercial or private WAN. Gateways may be located at critical locations in the transit route or be integral to the asset monitoring device itself. LAN extensions are used for non-integral gateway communications. Critical locations routinely include the facility where the transit began, entrance and exit gates at intermediary facilities where transportation mode changes or maintenance events occur and at entrance gates or loading docks at the asset destination. The system implementer will establish the extent of the gateway deployment and details of the data flow between components of the fleet management system. Generally, this system data flow will include these basic components as seen in the following figure.



Figure 3-4. Concept of Operations Fleet Management System.

3.4.2 Fleet Management System Components

All fleet management system end devices must be able to communicate with the Data Aggregation Point by either wired or wireless means. The communications protocols are detailed in later sections of this technical report. Fleet management system components may be battery-operated or mains-powered when mounted on fixed or mobile assets. End devices are components that monitor the state and location of the assets they are mounted on. These end devices maintain an internal electronic log of all state change events that they are designed to detect. The event record log structure and method(s) of downloading the event record log are detailed in later sections of this technical report. The end device and the Data Aggregation Point bi-directionally communicate with each other through the WAN gateways. This connection usually includes a LAN network extension however some assets may be of sufficient value to justify putting a WAN gateway (such as a cellular modem) directly on the asset.

WAN gateways provide bi-directional wireless communications interface to the end devices. For LAN extensions, the waveform described in later sections is IEEE Standard 802.15.4 2006. WAN gateways support the following tasks:

- Identify end devices in their RF communication range,
- Establish a wireless network connection with the end device,
- Deliver SCINetEx commands to the end device,
- Acquire end device Status messages and event logs and
- Communicate Status messages and event logs to the Data Aggregation Point.

Data Aggregation Points receive data from the end devices forwarded by the WAN gateways. In an operational system the Data Aggregation Point will collect data from many asset-mounted end devices. From an external point of view, the Data Aggregation Point is considered a secure server that distributes fleet management system data to other authorized users or information systems.

3.4.3 Considerations for Fleet Management

It is not the intent in this section to describe in detail the network architecture for a fleet management system. Rather, to simply provide some context into how such a system has been previously developed. Each system utilizing SCINetEx-compliant communications protocols may have subtle differences including the type of WAN utilized. It is important to understand that under SCINetEx, untrusted WANs are the rule, not the exception. These WANs may be public, private, government, commercial or military. The type(s) of WANs used for fleet management will determine the detailed interface requirements for each WAN gateway.

3.5 SENTIENT MACHINE MESSAGING

Sentient Machine Messaging (SMM) is the ability to identify and track the location and/or status of robotic and other assets that contain an artificially intelligent (AI) subsystem and provide a method for direct communication between assets in terse (<100 byte) data packets. The AI systems, although still in their infancy, can possess various levels of artificial intelligence (AI) and maybe be either mobile or fixed machines. Sentient machine messaging data is collected using multiple modes of communication which include commercial or private WANs that utilize private LANs that act as network extensions between the sentient machines to the WANs. Data is collected and stored at one or more data repositories. The SMM data sets should always include a unique identifier of the asset being tracked. This identifier may be a communications device Universal Identifier (UID), Media Access Control (MAC) address or serial number. In addition, SMM data sets may include contextual information such as an owner's ID number that is registered by an over-arching authority. Sentient machine messaging supporting more sophisticated ITV applications may provide condition information such as temperatures the asset was exposed to and any maintenance warning or fault codes detected by the AI asset's diagnostic systems. SMM data most generally gives the user tracking information as well as where and when messages were exchanged.

3.5.1 Concept of Operations

The essential role of a sentient machine messaging system is to record and report location, condition and state change data when the AI asset has access to one or more Network Gateway devices. State change data may include changes in diagnostic system fault codes or other non-integral sensors, meters, monitors and gauges. Network Gateways are connected to each other through a remote Data Aggregation Point that communicates to the Network Gateway via commercial or private WAN. Gateways may be located at critical locations where sentient machines are located or traversing and may be integral to the asset monitoring device itself. LAN extensions are used for non-integral gateway communications and direct machine-to-machine communications where permissions allow. Machine-to-machine direct messaging may be dis-allowed or confounded using techniques described in SCINetEx at the system owner/administrator's discretion. The system implementer will establish the extent of the gateway deployment and details of the data flow between components of the SMM system. Generally, this system data flow will include these basic components as seen in the following figure.

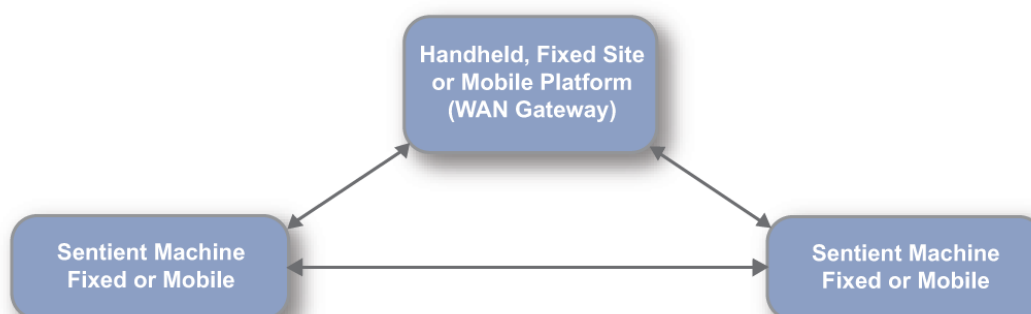


Figure 3-5. Concept of Operations Sentient Machine Messaging.

3.5.2 Sentient Machine Messaging System Components

All sentient machine messaging system end devices must be able to communicate with the Data Aggregation Point by either wired or wireless means. The communications protocols are detailed in later sections of this technical report. SMM system components may be battery-operated or mains-powered when mounted on fixed or mobile assets. SMM end devices are integral components that monitor the state and location of the assets they are mounted on. These end devices maintain an internal electronic log of all state change and communication events that they are designed to detect. The event record log structure and method(s) of downloading the event record log is detailed in later sections of this technical report. The end device and the Data Aggregation Point bi-directionally communicate with each other through the WAN gateways. This connection must include a LAN network extension. This extension is used for direct machine-to-machine messages. Some sentient machine assets may be of sufficient value to justify putting a WAN gateway (such as a cellular modem) directly on the asset. For purposes of SCINetEx, such assets are considered equivalent of a mobile WAN gateway instead of an end device.

WAN gateways provide bi-directional wireless communications interface to the end devices. For LAN extensions, the waveform described in later sections is IEEE Standard 802.15.4 2006. WAN gateways support the following tasks:

- Identify end devices in their RF communication range,
- Establish a wireless network connection with the end device,
- Deliver SCINetEx commands to the end device,
- Acquire end device Status messages and event logs and
- Communicate Status messages and event logs to the Data Aggregation Point.

Data Aggregation Points receive data from the end devices forwarded by the WAN gateways. In an operational system the Data Aggregation Point will collect data from many asset-mounted end devices. From an external point of view, the Data Aggregation Point is considered a secure server that distributes SMM data to other authorized users or information systems.

3.5.3 Considerations for Sentient Machine Messaging

It is not the intent in this section to describe in detail the network architecture for an SMM system. Rather, to simply provide some context into how such a system has been previously developed. Each system utilizing SCINetEx-compliant communications protocols may have subtle differences including the type of WAN utilized. It is important to understand that under SCINetEx, untrusted WANs are the rule, not the exception. These WANs may be public, private, government, commercial or military. The type(s) of WANs used for SMM will determine the detailed interface requirements for each WAN gateway.

Section Summary

- ITV and security embodiments can be combined to support cargo security and chain of custody applications.
- Fleet management combined with facility/warehouse management embodiments support remote facilities and activities such as military or humanitarian relief operations.

4. SED-TO-NG COMMUNICATIONS

This section is an overview of communication modes and protocols intended to illustrate an implementation that accomplishes the required functionality for the SCINetEx system.

4.1 COMMUNICATIONS MODES

The primary means of communication for all SEDs will be a network extension using LoPAN technology such as IEEE Standard 802.15.4-2006 radios operating at 2.4 GHz. Cellular networks, satellite communications and other media suitable for packet data as defined here-in can be utilized as secondary communications modes. (The SCINetEx concept however is LoPAN waveform independent.) All transport networks, including such media, can utilize protocols not known to be trustworthy and be considered untrusted. All SED security-purposed messages will be encrypted as described here-in for transport across untrusted networks. In all communication modes, data formatting and message content must be consistent in detail and comply as described here-in. Cellular and satellite communications media are not defined here but are expected to transparently transport traffic between SEDs and the trusted DAP.

4.2 END-TO-END MESSAGING PRINCIPLES

4.2.1 Session-less vs. Session-based Messaging

Communication defined here-in between DAPs and SEDs use datagrams (e.g., UDP via IP). The WPAN final link, though not IP-based, is also a datagram service. Persistent connections between the trusted DAP and every locale and NG are not required for this session-less method. Every SCINetEx system message defined here-in is short enough to be a single IP packet and a single data frame on IEEE Standard 802.15.4-2006 media. Thus, to bridge networks when transporting the messages defined here-in, 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 DAP transports, TCP may be impractical due to security policy or WAN transport methods. The wireless messaging defined in this technical report enables either session-less or session-based messaging. In either case, end-to-end error correction is defined here-in, irrespective of the transport network(s).

4.2.2 Fragmentation and Reassembly

Fragmentation and reassembly are not required in SCINetEx. Message formats defined here-in 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 as described later.

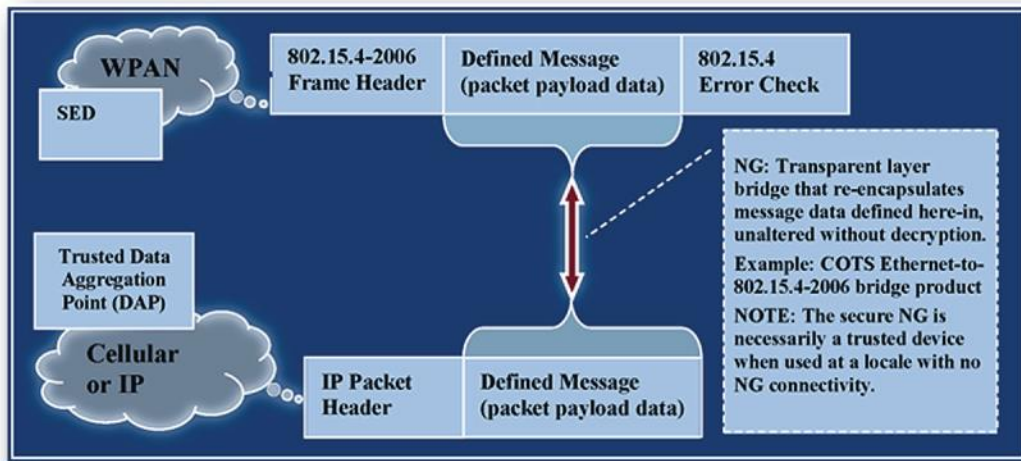


Figure 4-1. Illustration of End-to-End Message Transport.

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 here-in. The use of IEEE Standard 802.15.4-2006 link-layer error correction (link-layer ACK) is also required. Link-layer ACK content and timing must be consistent with ACK content and timing described by SCINetEx. Error correction is desired but not required in any other transport link on the end-to-end path between SED and DAP or secure NG. A bi-directional end-to-end application message ACK is defined by SCINetEx.

4.2.4 End-to-End Addressing and Mobility Management

The SED, for technical and practical reasons, in most cases cannot be directly assigned an IP address. The alternative, akin to that used in the cell phone industry under TIA standards, is as follows:

- 1 An NG forwards messages from a SED to a pre-defined DAP.
- 2 The DAP replies to this initial message via the same NG, ideally before mobile asset movement requires redirection to a different NG; this is an implementation issue; e.g., local infrastructure will choose the NG serving the destination SED. The destination SED Unique Identifier (UID) is identified from the status message header defined here-in. The DAP has the capability to identify the last known serving NG.
- 3 WAN/LAN devices (and non-secure NGs, in particular) can never decrypt security-purposed message content; trusted DAPS, secure NGs and SEDs that possess the appropriate encryption keys can decrypt security-purposed message content.
- 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 NGs. The infrastructure in this case must comply as defined here-in. This is not required if the NGs have public WAN addresses; the NGs can be generic devices and the infrastructure can ignore this construct.
- 5 For outbound messages the DAP re-uses the last known destination locale NG address for transmissions per methods not described in this technical report.

4.2.5 SED-to-DAP Addressing

NG-to-DAP communication requirements are defined by SCINetEx; this section is a derived summary. The message formats here-in require the SED to pass its UID, Smart End Device Unique Identifier (SEDUID) in every transmitted message's data payload, in an unencrypted section. Upon arrival at an NG, that data payload is removed from the IEEE Standard 802.15.4-2006 payload and re-encapsulated in a protocol data unit appropriate to reach the DAP servicing the NG.

4.2.6 DAP-to-SED Response Addressing

NG-to-DAP communication requirements are defined by SCINetEx; this section is a derived summary. The message formats defined here-in require that the DAP provide the UID of the destination SED to NGs. If the SED has moved and the DAP provides the wrong locale or NG, the DAP will time-out waiting for message acknowledgement.

4.2.7 DAP-to-SCINetEx Unsolicited Ad-hoc Addressing

NG-to-DAP communication requirements are defined by SCINetEx; this section is a derived summary. The DAP may send an unsolicited (Ad-hoc) message such as a status inquiry to a SED by addressing a message to the NG last used by that SED to contact the DAP. If the SED has moved into coverage of a different NG in the same Personal Area Network (PAN) ID, the message will not be acknowledged by the SED and the DAP will time-out. DAP retries are discussed here-in.

4.2.8 External Relay Function

At time of installation, the SED may be programmed with the IEEE Standard 802.15.4 MAC address of a second SED (and vice-versa), providing network extension and additional functionality. This is referred to as tethering and enables the SED to relay messages back and forth between the second SED and the NG, which also transmits the messages to and from a DAP.

The tethered device is likely to include GPS functionality and include cellular and satellite communications. Additionally the tethered relay may be used to extend the wireless network using Ad-hoc/Mesh functions described in Section 5.2.

In the tethered configuration, the SED will conduct Network Discovery as described in Section 5.1.6, and messages from the DAP will be forwarded by the SED to the specific tethered device address provided during the tethering process. Messages forwarded to SEDs including Status messages, Command messages and acknowledgements, are not to be altered by the tethered device.

The SED optionally stores and, on request, transmits event log messages.

4.2.8.1 Device Network Discovery

SEDs always conduct Network Discovery, whether acting as a relay or not by acquiring and responding to the Network Gateway Announcement (NGA) message sent by NGs. All devices in combination must meet the requirements of Section 5.1.1 for Network Discovery and response time.

4.2.8.2 Tethering the SEDs

At time of installation, the SED may be configured with the device UID/MAC address of the tethering SED (if implemented) using the method described in Section 10.2. The tethered SEDs record one another's IEEE Standard 802.15.4-2006 MAC addresses using an HNG. On completion of the tethering command execution, the SED will transmit an unsolicited Status message to the user's HNG via the tethered SED. On receipt of this message by the HNG, successful tethering has been confirmed. Personnel or automation must confirm that the tethered SEDs have established successful pair-wise communications as the final step in the installation process.

Following tethering, the tethered SED forwards all messages generated by either SED to the DAP via an FNG when in coverage. The tethered SED is required to respond to FNGs only when tethered. The SED will detect the tethered SED-relayed NGA message(s). The message header of the tethered SED NGA message will include the SED device type and the specified MAC address will be that of the tethered SED that sent the message. The SED may ignore FNG NGA messages from other than the given MAC address of the tethered SED relay so long as the tethered devices in combination meet all Network Discovery requirements of Section 5.1.6. All relaying SEDs must listen for incoming messages to its network address of no less than 20 milliseconds out of each second on average while tethered.

4.2.8.3 Message Bypass

The tethered SED must periodically detect the presence of NGAs independently. The SED may choose to either:

- 1 Route messages through the tethered SED to FNGs as the default message path or
- 2 Route messages through the tethered SED only when it detects no FNG coverage.

The tethered SED must respond to all HNG NGAs without routing through the other SED. If the tethered SED is removed by accident or intent after tethering, the other SED must be capable of detecting this within two (2) minutes and be capable of responding to and exchanging messages directly with all other NGs. Receipt of the defined Application Layer ACK constitutes message delivery success under all tethered conditions.

4.2.8.4 SED Relay – Messages to DAP

Messages from a SED via a tethered SED to an NG are processed as follows.

When entering or changing NG coverage selection:

- All FNG NGAs are relayed by the tethered SED as a unicast message until the initial SED response transmission.
- All NGAs with Message Waiting for the tethered SED UID must be relayed.
- The SED responds to the relayed NGA using the MAC address of the tethered SED.
- The tethered SED produces an IEEE Standard 802.15.4 MAC Layer ACK on receipt of the message.
- The relaying SED forwards the message to the coverage FNG verbatim and takes no further action.

If NG coverage is lost during this process, the relaying SED may attempt to send the message through alternative commercial modes such as cellular or satellite if available. If no connectivity is available, the relay takes no further action. The tethered SED will time-out waiting for an Application Layer ACK and take the appropriate action. If the DAP does not receive the message, the tethered SED will time-out waiting for an Application Layer ACK and take the appropriate action; the relaying SED has no responsibility in error correction for relayed messages.

4.2.8.5 SED Relay – Messages from DAP

Messages from an FNG to a tethered SED via a relay SED is processed as follows:

- 1 For an FNG message, the relay SED transmits the message verbatim to the MAC address of the tethered SED with appropriate MAC Layer acknowledgement.
- 2 The relay SED takes no further action beyond listening for a potential tethered SED response.
- 3 The tethered SED processes the message from the relay SED and takes appropriate action in the execution of commands and response.

A relay SED ignores messages from an HNG.

4.2.8.6 Location and Tracking Function

The location and tracking functional requirements are defined by the implementing organization.

Section Summary

- SCINetEx uses session-less messaging principles and User Datagram Protocol (UDP).
- Message addressing to each device utilizes a 64-bit UID.
- Although SCINetEx protocols are waveform independent, IEEE Standard 802.15.4 is utilized for demonstration purposes.

This page intentionally left blank.

5. WIRELESS PERSONAL AREA NETWORK (WPAN) DESCRIPTION

The SED-to-NG Wireless Personal Area Network (WPAN) is defined in this section. This includes definitions of the Media Access Layer (MAC), the Physical/Rf Layer and the required network topology to support a common Communications Module (CM). The CM may be a stand-alone unit or a subsystem within a SED.

The next sections describe the SCINetEx system PAN topology. Revisions of this topology are identified in the Revision Code in the Control Table maintained for any implementation of this system. The Revision Code is used in the message header illustrated in Figure 8-2. The current Revision Code 2 per this edition specifies peer-to-peer topology per IEEE Standard 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 here-in.

5.1 NETWORK TOPOLOGY – STRUCTURE AND OPERATION

5.1.1 802.15.4 Network Topology Overview

For this edition of the SCINetEx topology, there is no requirement for PAN coordinators, beacons or beacon requests utilizing peer-to-peer topology in IEEE Standard 802.15.4-2006 terminology. That is, SEDs learn then use the MAC address of a fixed or handheld device, or a SED relay device for communications. The architecture is one or more independent Star topologies at a locale. No network routing is required in the IEEE Standard 802.15.4 portion of the messages to/from remote DAPs or handheld devices. SEDs passively discover then communicate with Network Gateways (FNGs or HNGs) or via a relay device that has been specifically manually tethered for such service.

Network access discovery by SEDs is done via NGA messages issued as broadcast packets by FNGs and HNGs. SEDs, without any transmissions, passively discover one or more compliant NGs. Non-compliant emissions from access devices are ignored during Network Discovery. NGs discover SEDs via an unsolicited message sent to the NG by the SED after Network Discovery. SEDs cannot communicate with other SEDs except as untrusted relays. No inter-SED 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 the SCINetEx system peer-to-peer topology:

- The MAC Layer uses the un-slotted Carrier-sense Multiple Access (CSMA) Clear Channel Assessment (CCA) option due to low data volume. The Standard's TDMA/GTS option is not used.
- SED CMs may enter a low-power mode to conserve power. The NGA message (Section 5.1.6.2) informs a CM of any waiting messages queued while the CM was not listening, and the time interval until the next NGA message.
- NGAs are broadcast (not unicast) by NGs for use by the CMs for Network Discovery and notification of a Message Waiting (MW). A tethered SED sends an addressed packet (unicast) to its tethered SED; it does not broadcast NGAs after being tethered.

- If a CM is out of RF range (coverage) of the NG for a certain PAN ID, the CM may not discover the network. Should a CM lose coverage of its selected NG due to motion or changing RF conditions, the CM performs Network Discovery, as per the above; this may be a different PAN ID and channel. The channels are defined in Figure 5-1.

NOTE: Application message sequence numbering, for lost/duplicate message detection, will resume as defined in the SCINetEx system's message formats, irrespective of the change.

- When Add-on Sensors (AoS) are present, the AoS devices will simply transmit alarm messages as needed to the SED address provided during the tethering initialization process described in this technical report. The SED does not transmit NGAs 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 NGAs and SEDs. The PHY Layer shown in Figure 5-2 is largely fixed in Standard-compliant hardware and not alterable, and the PHY is defined as 2.4 GHz, per IEEE Standard 802.15.4-2006. The MAC Layer is firmware that is downloaded to the microprocessor(s) in commercially available or custom modules and configured within IEEE Standard 802.15.4-2006 defined variations.

In the topology of the SCINetEx system, the NWK Layer is absent and NWK Layer functionality is an aspect of the Application Layer. Except for the optional tethered-relay function, there is no required message routing or forwarding within the wireless portion of the end-to-end transport in the topology for this version. The Application Layer, with the protocols defined here-in, is responsible for the end-to-end (i.e., between CMs and the DAP) message formats and error detection and correction across all transport networks in the path.

5.1.3 MAC Protocol Configuration

The IEEE Standard 802.15.4-2006 MAC protocol configuration is configured for full interoperability, as follows. IEEE Standard 802.11 coexistence as shown in Figure 5-2 is considered. The MAC configuration is shown in Table 5-1.

Table 5-1. IEEE Standard 802.15.4-2006 MAC Configuration.

Parameter	Value	Comment
Channel Set	IEEE Standard 802.15.4-2006 channel numbers 15, 17, 21 and 23. No other channels may be used for messaging unless otherwise designated by the implementing organization.	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 here-in.	For messaging and Network Discovery as defined here-in.
MAC Layer Encryption for NG	Disabled.	Encryption is done in message payload data.
GTS, Superframe	Disabled.	
MAC ACKs	Hardware-enabled in conformance with IEEE Standard 802.15.4 and timing.	Application and Message ACKs are also defined here-in. Lack of buffer space should not be reason for not transmitting a MAC Layer ACK. This avoids need for flow control.
Beacons and Coordinator Nodes	Not used for here-in defined messaging.	See Section 5.1.4.3.
Beacon Request MAC messages or other transmissions by the on-asset devices prior to passive Network Discovery	Restricted-use, regulatory consideration.	Active-scan probing beacon requests when out of NG coverage are prohibited.
CCA	Required for all transmissions.	Clear Channel Assessment per the Standard is required.

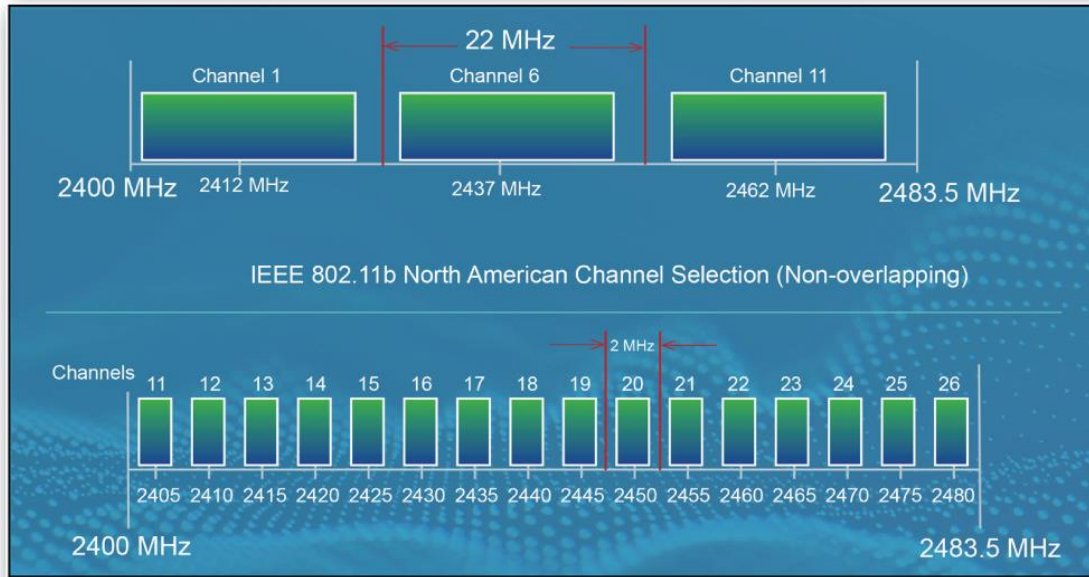


Figure 5-1. IEEE Standard 802.11 vs. IEEE Standard 802.15.4-2006 Coexistence.

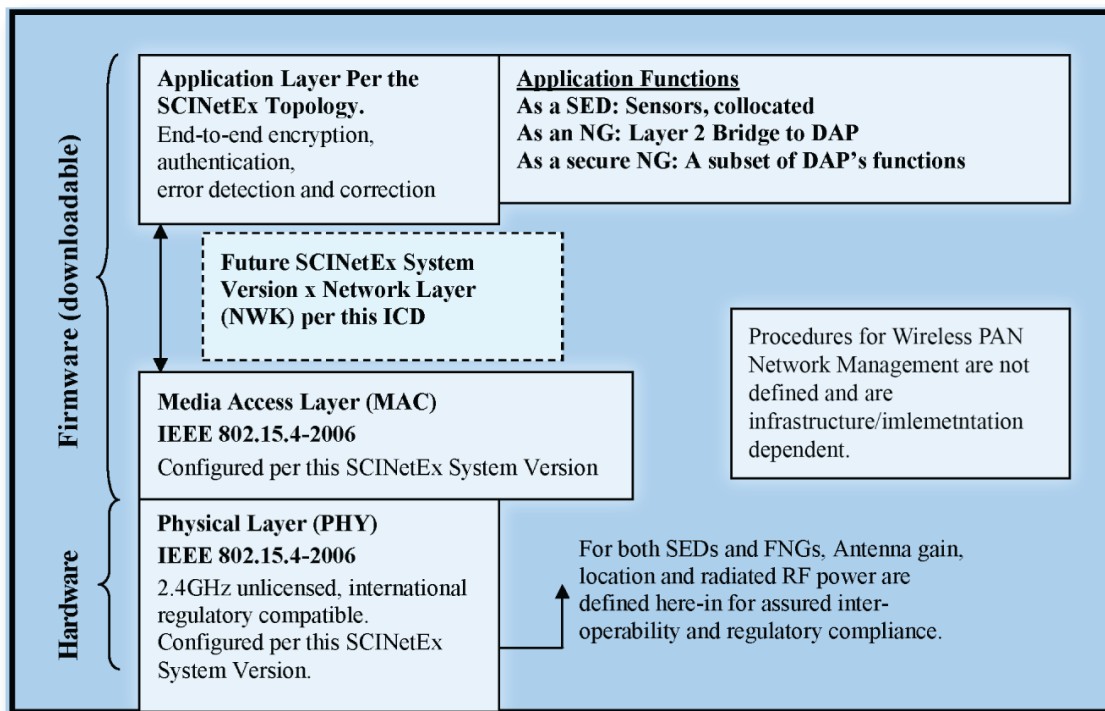


Figure 5-2. Communications Protocol Stack Architecture.

5.1.4 Network PAN ID Standardization

5.1.4.1 IEEE Standard 802.15.4b Data Frames

Every message data frame defined here-in sent while using one of the PAN IDs reserved here-in (see Table 5-2) utilizes 64-bit MAC addresses. Wild-card PAN IDs are neither required nor prohibited. This version of SCINetEx specifies two IEEE Standard 802.15.4-2006 16-bit (2-byte) PAN IDs and four RF channels to minimize the Network Discovery power-on time for the sake of battery conservation. The PAN ID for each NG is advertised by the NG via the Network Gateway Announcement (NGA) message as described in Section 5.1.6. The SCINetEx system does not require or prohibit beacons. There may be multiple NGs per PAN ID and multiple NGs per RF channel.

In Network Discovery (defined in Section 5.1.6) for security-purposed messaging, the SED searches for both of the PAN ID types reserved here-in (see Table 5-2). A successful secure message exchange with the DAP, including Application Layer ACKs defined here-in, confirms correct PAN ID and NG selection.

5.1.4.2 PAN ID Codes

This SCINetEx system version reserves two of 65,535 possible PAN IDs for compliant messaging. Non-compliant messaging at any locale should not use these PAN IDs on the SCINetEx system 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 here-in, the expectation is that encryption and message integrity checks also defined here-in will reject the message with no transmitted response. As to PAN IDs other than those reserved per Table 5-2, the SCINetEx system does not prevent use of PAN IDs for selection of message addresses. Such proprietary use of PAN IDs is, 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 here-in). 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 Standard 802.15.4 Beacons

The use of beacons, beacon requests and network association is neither required nor prohibited by the SCINetEx system. SCINetEx 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 that SEDs (excluding AoS) “listen first and transmit last” to ensure that SED transmissions occur only where NG coverage exists.

SCINetEx requires that all transmissions of compliant messages use CCA. SCINetEx does not require IEEE Standard 802.15.4-2006 beacon transmissions or beacon probe/association requests. The SCINetEx implementer at a locale will select a channel and PAN ID, and change as necessary, to minimize the occurrence of non-compliant 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 Reuse

Any channel or particular PAN ID code from Table 5-2 may be used by multiple NGs 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 described here-in and are left to the system implementer.

5.1.5 WPAN MAC Address Interoperability Assurance

The intent is to ensure proper coexistence and interoperability in a locale with many different manufacturers’ SEDs and NGs. This includes overlapping RF coverage and PANs with completely arbitrary PAN data content. It is presumed that all systems comply with the IEEE Standard 802.15.4-2006 at the MAC Layer following the regulatory intent of ISM-band spectrum sharing. Every SED must respond with its own UID as network address for purposes of wireless communications. The SCINetEx 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 here-in adhere to these standards and conventions.

5.1.6 Network Discovery

SCINetEx requires that NGA messages seen in Table 5-3 be transmitted by all NGs in such a way that interoperability is ensured among NGs and SEDs in any mix of vendors. After a CM executes Network Discovery, it will choose an NG and send the unsolicited device Status message (defined in Section 8.5) via the chosen NG.

5.1.6.1 Network Discovery Selection Priority

A SED selects an HNG in priority to all FNGs, when Network Discovery is undertaken and the HNG’s NGAs are detected. A SED that has previously selected a Fixed Network Gateway (FNG) while dwelling in coverage must detect an HNG’s NGAs interleaved with the FNG’s NGAs. On such, the HNG will be chosen and the FNG use will be delayed or abandoned. When the HNG’s NGAs and unicast messages cease for 30 seconds, the use of the FNG resumes.

When in simultaneous coverage of two or more NGs of similar types (either HNGs or FNGs), the CM conducts NG selection based on optimal signal strength using the Link Quality Indicator (LQI). Per this SCINetEx version, an unsolicited restricted Status message is sent by the SED to the chosen HNG or FNG on change of NG coverage.

5.1.6.2 Network Gateway Announcement (NGA) Message Broadcast

Every FNG and HNG transmits a Network Gateway Announcement (NGA) message using the configured PAN ID and channel for compliant messages. The NGA is essentially a brief “this NG exists” advertisement. The NGA from FNGs and HNGs uses the broadcast address (all ones). The NGA relayed by a tethered SED is unicast, not broadcast. Network Discovery, defined in Section 5.1, references the NGA message. To avoid packet collisions, an NGA message is transmitted using CCA procedures per IEEE Standard 802.15.4-2006.

NGA messages are transmitted by each NG at any of the intervals defined for NGA messages as shown in Table 5-3. The NGA interval does not exceed one (1) second. Network Discovery by CMs, while in low-power mode between expected NGA messages, depends on knowledge of these intervals, based on NGAs received before entering a low-power mode.

The use of short-interval NGA messages should not violate the least common denominator of locale-dependent regulatory limitations on transmitter duty cycle. The minimum recurring interval should not be incompatible with the IEEE Standard 802.15.4-2006’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 receive NGA broadcasts per the notional timing shown in Table 5-3. The SED’s receive duty cycle is not required to be continuous. The receive duty cycle (listening for NGAs) of any SED (except AoSs) cannot be less than 20 milliseconds per second on each of the four channels specified here-in.

This is an equivalent of 8% listen duty cycle in total. It is the developer’s responsibility to optimize the receive duty cycle to ensure the Network Discovery requirements of Section 5.1.1 are met.

The NG transmit duty cycle on any single channel is determined by the NG developer and tailored to the specific implementation. This is optimized in periodicity and duration to ensure the greatest likelihood of coverage for all possible devices moving within the FNG 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. HNG NGA broadcast messages are exempted from this restriction.

Multiple FNGs can transmit NGA messages on one or more channels using one of the PAN IDs defined here-in. In the deployed case where the coverage areas of two or more FNGs 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 SED is armed and it is tethered with another SED, NGA messages relayed by the relay SED are unicast to the MAC address of the tethered CM, even though, in general, NGAs are broadcast. This is detailed in Section 4.2.8.

All NGs listen continuously when not actively transmitting broadcast messages or otherwise engaged in message exchanges with devices in the NG coverage area. Beacon broadcasts as defined in IEEE Standard 802.15.4-2006 are not used as an alternative to NGA broadcast messages. This assures interoperability of devices and NGs in mixed-developer situations.

5.1.6.3 Network Gateway Announcement (NGA) Message Data Payload

The NGA message is wholly contained in one MAC Layer payload and consists of the following data. All fields are required. Bytes 0 and 1 are compatible with the standard message header. The Time Delay for next NGA (byte offset 2) is mandatory and must be changed if needed to enable interoperable power-conservation strategies. A SED CM may enter power-conservation cycles no sooner than two (2) seconds after the last (non-NGA) transmission to/from an NG. The cycle's duration is governed by top-level system response time requirements (e.g., HNG response time).

The SCINetEx Set Interval State (SIS) command is sent by a secure NG or DAP to assist in selection of power-conservation cycle time.

Table 5-3. Network Gateway Announcement (NGA) Message Content.

Offset 0	1	2	3	11	12
x0	x1	x2	x3	xB	xC
Standard message header Byte 0 Device Type	Standard message header Byte 1 Message Type = NGA message (0xFF)	Bit 0: UTC is valid. Bit 1 = 1 if MW list continues in next NGA. Bits 2 and 3: Reserved for future use. Bits 4-7: Time delay for next NGA; 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 Bits 8-15: Reserved. Accurate to +/- 0.01s. Coding applies to next interval and may change at any time.	Date/ Time UTC (8 bytes) See Table 8-1 for format.	Level 1 Facility Device Type (1 byte) See Table 8-2 For DAP Device Types.	UID of Level 1 Facility (8 bytes)

Message Waiting (MW)

Table 5-3. Network Gateway Announcement (NGA) Message Content. (Continued)

Offset 0	20	21	29	30	30+ n + 1
x0	x14	x15	x1D		
	Level 2 Facility Device Type (1 byte) See Table 8-2 for HNG Device Types.	UID of Level 2 HNG	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 NGA messages for an unlimited count.	NGA message checksum 1-byte half-sum of NGA message (sum of the bytes modulo 256)

5.1.7 Communications Module Network Discovery Procedure

The Network Discovery process relies on transmitted Network Gateway Announcement (NGA) messages that recur at the time interval (variable or fixed) depicted in each NGA. The CM attempts Network Discovery at state and status-dependent time intervals constrained by battery conservation. “State” refers to the optional use of the Set Interval State (SIS) DAP or secure NG command. The time interval does not exceed the Message Waiting list maximum age identified in Section At some locales, there may be multiple NGs on different channels with the same PAN ID (e.g., an area with overlapping coverage).

The CM tunes to each RF channel defined here-in and attempts to detect an NG’s NGA for each PAN ID. Definitions for these are in the MAC Layer configuration in Table 5-1. The scan characteristics are determined by the developer to enable a response time for Network Discovery that does not exceed two seconds following successful receipt and recognition of a valid NGA 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 NGs on different RF channels. A CM powers up and discovers a marginal/weak-signal NG on channel A, then retunes and finds another NG on channel B with an adequate signal.

NOTE: The time synchronization of NGAs 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 DAP or secure NG command messages in Section 8.5.

After successful Network Discovery, the CM follows the unsolicited device Status message procedure, as defined in Section 8.5.

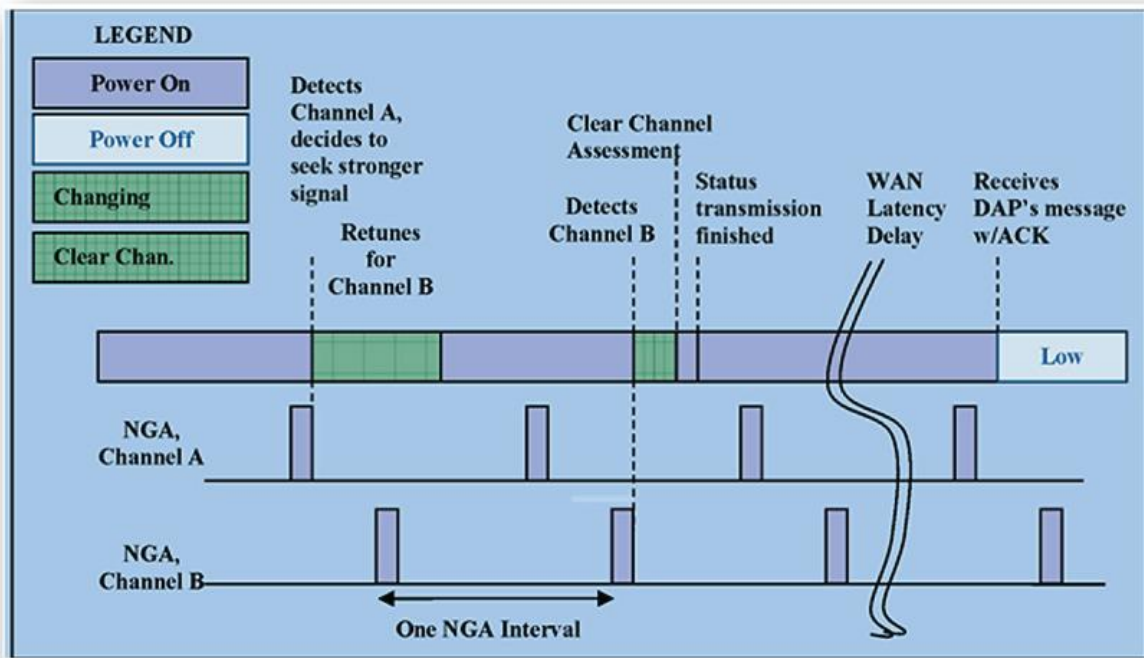


Figure 5-3. Network Discovery and Unsolicited Device Status Message Timing Example – Two NGs.

5.1.7.1 Recurring Network Discovery

Due to changing RF conditions, to optimize NG choice and to permit an HNG to pre-empt an FNG, the CM repeats Network Discovery, starting with the last-used channel/PAN ID, at time intervals not to exceed the Message Waiting list purge time-out of 60 seconds, where the interval begins at the end of the last transaction with the DAP. The unsolicited device Status message process suppresses redundant Status messages where neither NG choice nor sensor status has changed.

5.1.7.2 HNG Network Discovery Prioritization

Secure HNGs are used to conduct local short-range communication with specific CMs. For this application, the DAP will provide the HNG a list of UID/encryption keys for identifying and conducting secure message exchange with specific devices. The HNG will place UIDs in the Message Waiting list of its NGA. A SED, whether tethered or not, responds to the HNG NGA and conducts routine Message Waiting process. CMs that are in simultaneous FNG and HNG coverage respond to the HNG in preference to FNGs in all cases. Following completion of the HNG message exchange, the CM resumes Network Discovery.

5.1.7.3 Network Gateway Announcement (NGA) Message Waiting (MW) Overview

The purpose of Message Waiting is to enable devices 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 technical report, the method must use only the basic packet transmit/receive IEEE Standard 802.15.4 functions. All SCINetEx-compliant devices support the method defined here-in.

The CM discovers the Network Gateway and sends the initial unsolicited device Status message. Thereafter, e.g., while dwelling in coverage and intermittently entering a low-power state to conserve battery, the CM uses the NGA Message Waiting procedure described here-in to passively (i.e., without transmission) detect queued, incoming unsolicited messages from DAPs and secure NGs. The NGA message's Message Waiting list eliminates the need to transmit frequent polling requests. The Message Waiting capability is used when a transmission to a CM is to occur and:

- The last-received message from the CM occurred two or more seconds in the past. The age of the CM's last-transmitted message is not a criterion.
- The destination device's IEEE Standard 802.15.4-2006 MAC address, corresponding to its UID (as given by the to-CM message), is unknown to the NG. This can occur if the NG 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 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:

- A DAP or NG sends an Ad-hoc message long after the last from-CM message was received and the DAP is using the last-known NG.
- A DAP or NG retransmits a message due to a response time-out.

The Message Waiting capability is used when a from-DAP message arrives at the NG 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 NGA Message Waiting (MW) list, a NULL message (defined below) is:

- Sent if MW is true for the security device's UID (tethered relay devices described in Section 4.2.8.3 are transparent but still send NULL).
- Ignored by the NG if no message is waiting for the security device's UID, e.g., if the message has already been sent.
- 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 a compliant NULL message. The UID byte order is the same as for the UID in the header of all other messages defined here-in.

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

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

Figure 5-4. NULL Message from SED or CM.

5.1.7.5 NULL Message Global Response

If a UID in the MW list consists of an all 1's UID (0xFFFFFFFF), then each receiving non-NG device responds 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 SED sends the unsolicited Status message instead of the NULL message. On receipt of the unsolicited Status message, the DAP detects that the status was not the expected solicited status response and then presumes that the prior pending message/command has been ignored and lost. The DAP processes the Status message and may repeat the prior message, if relevant.

5.1.7.7 Message Waiting Method – NG Responsibilities

An NG asserts Message Waiting, per the criteria above, as follows. The SCINetEx-defined NGA message contains a list of UIDs for which MW is true, i.e., for which a deferred message is queued. Successive NGAs will contain the UID in the MW list until the deferred message is transmitted by the NG. The MW for a given UID remains in NGA transmissions until:

- A NULL message is received from that UID, or
- Any other message defined here-in is received by an NG from that UID, e.g., an event's status message taking precedence over a response to a DAP command message, or
- A period of 60 seconds elapses with no response from the target UID. The message originator (DAP) 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 NG provides an IEEE Standard 802.15.4-compliant MAC ACK to NULL data frames, as it must to all data frames per this technical report.

On receipt of a NULL message from the target UID, the NG asserting MW transmits the deferred encrypted or unencrypted data message in less than two seconds. After receipt of the NULL message, the NG continues sending MW via NGA 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 an NG, is ignored. On receipt of any message defined here-in, the NG updates the UID/MAC affiliation history. The association can change due to the use of a tethered device acting as a relay.

5.1.7.8 Message Waiting Method – CM Responsibilities

On detection of an NG's UID in the NGA MW list, the CM transmits the NULL message to that NG. As for all SCINetEx-compliant messages, the frame is marked as MAC ACK requested. The NULL will be repeated for every nth NGA containing MW indication, where n can be 1. For NGAs at short intervals, n can be greater than 1 to reduce redundant NULL messages, as the NG may be busy with other CM traffic. NULL messages are suppressed for intervals less than 0.1 seconds.

The CM inspects each NGA independently, as MW UIDs may be spread across successive NGAs when there are many UIDs pending at one NG, not all of which will fit into a single NGA. This is referred to as a rotating MW list. The CM detects and processes a MW list larger than one NGA via bit 1 of the byte at offset 2 per Table 5-3. An NG may use this mechanism to discover in-range devices for the chosen channel and PAN ID, e.g., when an FNG is restarted or when an HNG needs to discover devices.

5.1.7.9 Message Waiting Method – Relay Device Portion – NULL Message Frame

For a relay device such as a tethered SED (Section 11.2.1), either of the following may occur when the UID of a non-integral sensor (e.g., a SED) tethered to the relay SED occurs in an NGA with MW:

- 1 The relay SED transmits a NULL frame to the NG, using the UID of the tethered SED, without tethered SED involvement, or
- 2 The relay SED retransmits the NGAs with MW to the tethered SED and re-transmits NULL messages sent by the tethered SED. In this case, the sending unit's MAC address in the IEEE Standard 802.15.4-2006 frame for the NULL message will be that of the relay SED. The NG uses this in order to respond.

In either case, the NULL message repeats while the NGA MW indication is true. As in the no-relay case, NULL messages may be sent for a fraction of all received NGAs with MW.

5.1.7.10 Message Waiting Method – DAP Portion

Considering power conservation, the DAP is able to accommodate a response delay due to MW no longer than the power conservation interval defined here-in as 60 seconds, with or without tethering.

5.2 AD-HOC/MESH NETWORK TOPOLOGY

Ad-hoc/Mesh topology is supported for untrusted functions by the current version of the SCINetEx system for security messages. Mesh routing functions for relay devices such as relay SEDs or NGs are allowed as a secondary communications path similar to cellular or satellite modes. An Ad-hoc/Mesh network has the following characteristics:

- Every Mesh network node is a Full Functional Device (FFD) per the IEEE Standard 802.15.4-2006 and may route (forward neighbor's frames if needed), including NGs and SEDs.
- Mesh node neighbor associations are self-forming based on dynamically changing RF propagation conditions (blockages, movements, etc.).
- The RF path lengths in the network are on average far shorter than with a Star topology as described in the IEEE Standard 802.15.4-2006.
- Route diversity exists and improves fault tolerance.
- Infrastructure nodes (NGs) may peer amongst themselves in a logically independent Ad-hoc/Mesh network.

- These neighbor associations reform as needed due to changing conditions (self-healing).
- Nodes collaborate with neighbor nodes irrespective of manufacture/vintage, based on procedures as described in the separate governing Mesh network Standard document.
- Security-purposed messages are encrypted such that unauthorized nodes are not a security risk.
- Hierarchical messages are encrypted such that information is protected as seen fit by the node's owner.

The IEEE Standard 802.15.5b for Mesh networks enables single-or multi-hop dynamic routing among network nodes. Those nodes could be SEDs and infrastructure. SCINetEx does not constrain a user to this Mesh network standard. These nodes communicate with distant data aggregation centers. The IEEE Standard 802.15.5b for example defines both fixed single-hop and multi-hop dynamic routing among peer nodes to reach the best network egress node, and vice-versa. For nodes that can communicate directly with a Network Gateway, the topology is a single-hop Star. A principal difference in Star and Mesh topologies are procedures for Network Discovery and access device affiliation. In Mesh, the most reliable (or only) network access may be a nearby peer. Once joined to the network, the messaging protocol itself is the same as with Star topology.

5.2.1 Ad-hoc/Mesh Protocol and Procedures

Figure 5-5, below, depicts the data, network management and device management protocols and interfaces. All but the lower part of the PHY Layer is downloadable firmware code. The MAC and PHY Layers are commonly available from many suppliers, as a single low-cost chip, or as a part of an OEM module or end-user product that is certified for use by regional regulatory authorities. Some products may use a single chip for IEEE Standard 802.15.4-2006 MAC, PHY and Application Layers while others may have two chips for added memory and CPU resources. All NGs are FFDs in IEEE Standard 802.15.4-2006 terminology (some SEDs may be). As defined later, many of the options in the figure's functional boxes are not required. The Application Management Entity (AME) and DME from the figure are mere frameworks and are left to the implementer to define, being unrelated to interoperability.

Here-in, the IEEE Standard 802.15.5 term Service Access Point (SAP) is synonymous with the Applications Program Interface (API) (is not a physical device "AP"). The IEEE Standard 802.15.4-2006 defines a standard API for controlling the MAC and PHY Layers. The IEEE Standard 802.15.5 defines the Network (NWK) API used with the IEEE Standard 802.15.4-2006 MAC and PHY API. The messages defined in Section 8 are input and output to this layer by the application.

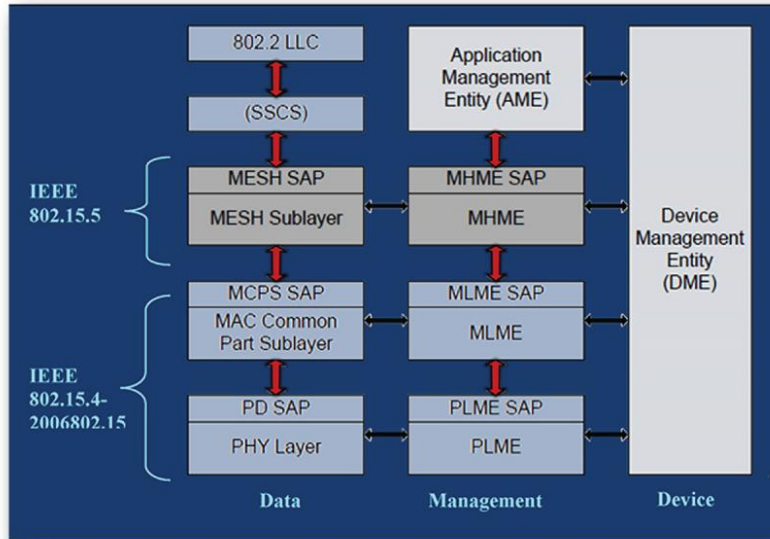


Figure 5-5. Mesh Protocol Stacks in CMs per the IEEE Standard 802.15 References.

5.2.2 Ad-hoc/Mesh Network Layer (NWK) Management Functions Utilized

From IEEE Standard 802.15.5, the following network management functions as listed in Table 5-4 are required. Refer to the Standard for specifics. These functions in turn invoke the necessary IEEE Standard 802.15.4-2006 functions, so that 802.15.5 may utilize any compliant IEEE Standard 802.15.4b stack and hardware. Below, non-essential network management functions are omitted. The procedures for applying these functions are given in the IEEE Standard 802.15.5. Inter-node commands are used within the IEEE Standard 802.15.5 Network Layer of peer nodes and the coordinator. These are listed in Table 35 of the IEEE Standard 802.15.4-2006. Notably, the “hello” command and “probe” response, used to discover neighbor-nodes, is detailed for maintaining link state information used for route selection.

Table 5-4. Primary Network Layer Functions – Ad-hoc Topology.

IEEE Standard 802.15.5 Network Layer Function (SAP)	Used By
MHME-START-NETWORK	Coordinator – to commence WPAN
MHME-DISCOVER	Nodes – to scan channels to find WPAN(s)
MHME-START-DEVICE	Node – to participate in network
MHME-JOIN	Node – to join/rejoin network
MHME-LEAVE	Node – to exit network
MHME-START-SYNC	Coordinator, then each node – to enable time synchronized neighbor-node rendezvous
MHME-TRACE-ROUTE-REPLY	Node – to optimize routing
MHME-MULTICAST-JOIN	Node – to join a multicast group
MHME-MULTICAST-LEAVE	Node – to exit a multicast group
other TBD	other TBD

5.2.3 Network Discovery for Ad-hoc/Mesh

The Network Discovery procedure is defined by IEEE Standard 802.15.5 for beaconless, asynchronous CSMA-based low data volume WPANs. Precision latency management is not assumed to be required; message delays of seconds are adequate and avoids the high complexity and battery life impact of TDMA (GTS/EGTS)-based protocols. Certain parameters are needed for efficient Network Discovery, e.g., channel subset to scan and a constant for the NWK Layer rendezvous interval and dwell time. The meshed device selects the best route to an NG (where best route is per the IEEE Standard 802.15.5).

- A single-hop to an NG is to be chosen if a channel is found with an adequate LQI.
- A peer SED (CM) shall be chosen as an alternative, per IEEE Standard 802.15.5 procedures.
- Subject to battery life limitations, Network Discovery is repeated if the LQI for the selected route diminishes unacceptably or on receipt of network management direction to do so.

5.2.4 SCINetEx Physical Layer (PHY)

The 2.4 GHz PHY Layer is completely defined by IEEE Standard 802.15.4-2006 with the exception of transmitter power and radiated power. The latter is essential for assured interoperability as per the example in Table 5-5. A link budget common to all developers is necessary for developer A to assuredly achieve the needed signal-to-noise ratio for developer 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 SED may operate. SCINetEx 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 5-5. IEEE Standard 802.15.4-2006 PHY Layer Configuration.

Parameter	Value	Comment
Operating Frequencies	See MAC Layer Configuration.	
Radiated Power	Such that the Effective isotropic radiated power (EIRP) including antenna gain is no less than 10mW (10 dBm).	Least common denominator internationally; applies to fixed and on-asset devices; see Section 5.3.
Receiver Sensitivity	Sufficient to meet SED line-of-sight range requirements of the implementer. Must also meet IEEE Standard 802.15.4-2006 Packet Error Rate (PER).	Typically -85 to -90 dBm, excluding antenna gain/loss.
Power Consumption	Per device requirements of the system owner/user.	

5.3 RF INTEROPERABILITY LINK BUDGET

The 2.4 GHz specification here-in addresses the requirement for internationally available unlicensed spectrum. The specified IEEE Standard 802.15.4-2006 MAC and PHY Layers 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 SED antenna location are specified here-in to achieve interoperability at the received signal strength level. FNGs must be deployed in quantity and placement necessary to assure bi-directional coverage availability and adequate fade margins given the effective radiated power of SEDs and RF occlusion given the system RF link budget. The following receiver characteristics must apply to all CMs and AoSs:

- Receiver sensitivity is -85 dBm or better for a 1% Packet Error Rate (PER).
- The receiver provides 30 Decibel (dB) or better for alternate adjacent channel rejection.
- The receiver conforms to the PER limitations specified by implementer requirements.

5.3.1 Receiver Requirements

All SCINetEx-compliant receivers comply with MAC and PHY Layers as defined here-in.

5.3.2 Transmitter Requirements

To support the common RF link budget for interoperability, the following transmitter requirements apply to all CMs, AoSs and NGs:

- Fully complies with the PHY Layer as applied by SCINetEx.
- Does not exceed regulatory limits for in-band and out-of-band spurious and harmonic emissions.
- Complies with each regulatory domain's rules regarding maximum field strength as measured outside of the on-asset device for antennas located either inside or outside.
- Provides the transmitter power and radiated power per the link budget listed in Section 5.3.4.

5.3.3 SED and FNG/HNG Bi-directional Antennas

The communication subsystems of all SEDs and CM devices support the required range when installed and comply with SCINetEx, notably the common RF link budget.

5.3.4 RF Link Budget

To assure interoperability between any manufacturer's NG and any manufacturer's CM, at the ranges specified by the implementer's requirements, an example of a conventional RF engineering link budget is provided in Table 5-6. 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 common 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 5-6. Link Budget Example.

Link Budget Parameter (2.45GHz)	Security Device	FNG	HNG
Antenna Gain – minimum, [Decibel isotropic (dBi)], net of other losses.	0dBi	5dBi	0dBi
Transmitter Power (EIRP) – minimum (dBm).	+3dBm	+10dBm	+3dBm
Line-of-sight/clutter-free free-space path loss for exponent = 2.0 adjusted for locale-dependent clutter obstructions.	Locale-dependent		
Additional path loss from RF occlusion, adjusted for factors such as SED location, path to best-server NG, clutter and obstructions.	0dB		
Path loss positive adjustment for diffraction statistical mean, in non-line-of-sight.	0dB		
Fade margin – slow fading, (dB), for link availability.	-6dB		
Receiver sensitivity at IEEE Standard 802.15.4-2006 specified PER, minimum, at antenna port, (dBm), excluding antenna gain.	-85dBm		

Section Summary

- SCINetEx uses a hybrid network topology incorporating Star and Mesh capabilities.
- SCINetEx defines a unique Network Discovery protocol with single-frame message exchange.
- RF link budget is defined for device interoperability and operations in the global unlicensed bands.

6. MEDIA ACCESS CONTROL LAYER (MAC)

6.1 MAC FRAME CONSTRUCTS

The MAC frame constructs are based on those of the IEEE Standard 802.15.4 – 2006, including:

- All frame types identified in IEEE Standard 802.15.4-2006 are supported by the SED.
- Each of the four frame types in SCINetEx comply with IEEE Standard 802.15.4-2006 by including:
 - A MAC Header
 - A MAC Payload
 - A MAC Footer providing a 16-bit Cyclic Redundancy Check (CRC) CCITT frame-check sequence as defined by the Standard.
- Within data frames and for commands passed through the NGs, the IEEE Standard 802.15.4-2006 MAC Protocol Data Units (MPDU) includes the data payload provided per SCINetEx characteristics.
- The message contents transmitted by the NG to either the DAP or a CM is forwarded without modification.
- The application data payload is the maximum size defined by the IEEE Standard 802.15.4-2006.

6.1.1 MAC Layer Configuration Parameters

See Section 5.1.3 and Section 5.1.4.

6.1.2 MAC Layer Acknowledgement Frames

All successful communications between devices is acknowledged. The format for the acknowledgement frame follows exactly as provided in IEEE Standard 802.15.4 - 2006, Figure 12.

6.1.3 MAC Layer Retransmissions

Retransmissions done by the MAC Layer due to MAC Layer ACK time-outs is executed per IEEE Standard 802.15.4 - 2006 and there are at least three retransmission attempts, with each subject to the usual CCA.

Section Summary

- Basic SCINetEx topology is Star with Network Layer functions defined by SCINetEx.
- Network Gateways may support Mesh routing.
- The Network Discovery procedure is beaconless, asynchronous CSMA-based that may be broadcast or unicast dependent on device type.

This page intentionally left blank.

7. NETWORK LAYER

The Network Layer provides switching and routing functions for transmitting data from one node to another as well as addressing, error handling and retries for congestion and interference among other things. All routing within the IEEE Standard 802.15.4-2006 wireless network is per SCINetEx parameters. Addresses are full 64-bit MAC addresses. PAN coordinators are not required. The effectiveness of the Network Layer protocols is strongly dependent on the choices made for the MAC and PHY Layers as described in the Open Systems Interconnection (OSI) model for network communications. What follows is a brief discussion of the rationale behind some of the foundational characteristics of the SCINetEx system.

7.1 NETWORK MEDIA CONNECTIVITY

In the context of wireless network extensions such as SCINetEx, the wireless network media performance is subject to the effects of the laws-of-physics constraints on RF propagation in the physical settings representative of where the owner/user implements the system. It cannot be assumed that simple line-of-sight transmission characteristics for digital wave forms will apply in most, if any, implementations. In the SCINetEx construct presented here, it is assumed that RF communications supporting sophisticated reporting devices must operate in physical settings typical of industrial control systems (ICS) that include impairments that cause extreme multi-path propagation and attenuation issues.

7.1.1 Multi-path

Multi-path is caused by reflection of RF signal from surrounding structures and materials. These conditions can vary widely from locale to locale and may include reflective effects of impairments not located in the line-of-sight of the RF transmission. A good example of multi-path is on-screen TV “ghosts” caused by reception of over-the-air transmissions that includes reflections from large buildings or mountains. The main impact of this kind of impairment is in the uncorrectable Packet Error Rate which limits network capacity and makes it difficult for two nodes to communicate in certain locations. In data transmission, reflected signals can significantly degrade air link bit rates. The primary means for mitigating multi-path is to reduce the transmission spectral efficiency (information bits per unit of bandwidth) of the individual transceiver system. IEEE Standard 802.15.4-2006 radios were designed for ICS-type applications and operate at lower bit rates than standard 802.11.x radios used for WiFi. Thus systems that utilize IEEE Standard 802.15.4 radios, as described in this embodiment of SCINetEx, handle multi-path much better than alternate systems that use WiFi. One may implement SCINetEx air interface protocols using IEEE Standard 802.11.x waveform (it would no longer be called WiFi), however it would not handle an extreme multi-path as well.

Multi-path is measured by determining how much energy arrives at a receiver via a “direct” propagation path as compared to a time-delayed path (reflected). The amount of power versus the time delay statistics is called the delay spread. Multi-path that arrives at (nearly) the same time as the direct path signal simply sums. This can decrease the desired non-reflected signal’s strength if the delayed signal’s instantaneous phase is in opposition. An analogy comes from noise-cancelling headphones: here the undesired outside noise is, via a microphone and electronics, made opposite-phase and sent to the headphone’s speakers; at the ear, the outside plus the synthetic out-of-phase sounds sum and tend to cancel. Short duration RF multi-path has this kind of effect, however, the phasing is almost random for extreme impairment paths.

Conversely, multi-path arriving later than the period of the desired signal causes difficult-to-mitigate interference. Many digital data systems transmit data as symbols (as does IEEE Standard 802.15.4-2006) where a symbol depicts one, two, four or more data bits. The more bits per symbol, the more complex the transmitted digital signal must be to encode the symbol. IEEE Standard 802.15.4-2006 uses 4-bit symbols. Complex symbol codes require a large ratio of signal-to-noise-plus-interference to operate effectively. As mentioned before, the mitigation for multi-path is to slow down the rate at which data bits are transferred. An analogy for this effect would be two people at either end of a canyon trying to understand each other through the echoes. In order to do so, they should speak more loudly (high signal-to-noise) and more slowly (lower data rate).

7.1.2 Attenuation

In the context of SCINetEx, signal attenuation refers to reduction in available, measurable signal due to RF-obstructing and absorbing materials as compared to clear line-of-sight conditions for wireless data transmissions. In the real world, complicating effects include knife-edge-type diffraction by the obstruction and surrounding terrain. Many commercial radios provide a signal strength indicator, however simple received power does not capture the effects of multi-path and diffraction for degrading data error rates. As useable signal is degraded, signal-to-noise-to-interference decreases and complex symbol codes become less effective. Modeling can be used to predict attenuation in complex obstructed environments.

7.2 SIMULATION AND MODELING OF NETWORK LAYER CONNECTIVITY

Modeling and simulation can be an effective tool to assess anticipated network connectivity for wireless data systems. The cell phone industry has invested heavily in modeling and simulation tools in the presence of typical impairments and obstructions. Most SCINetEx implementers will not have the resources to develop dedicated tools for their locale, however there are some commercially-available tools (such as OpNet and QualNet) to optimize the implementation of a particular system by identifying factors that will affect the assured and timely operation of the deployed network extension. Such tools can be used to assess the departure and arrival times for each communication packet as it traverses the various network nodes of the integrated system. Environmental effects on propagation loss for implementation architecture can be assessed. Reporting, acknowledgement and Network Discovery times can be assessed for mobility purposes and node placement studies. Numerous studies have demonstrated that commercially-available network simulation tools can be used to accurately predict Network Layer and overall system performance for various SCINetEx hardware and protocol implementations. These simulations should always however, be corroborated using field tests and other demonstrations. One such recommended field test is for latency. Packet latency is defined as the amount of time it takes for a packet to traverse the networked system. Figure 7-1 is a notional configuration for a packet latency testing using a modeling and simulation tool.

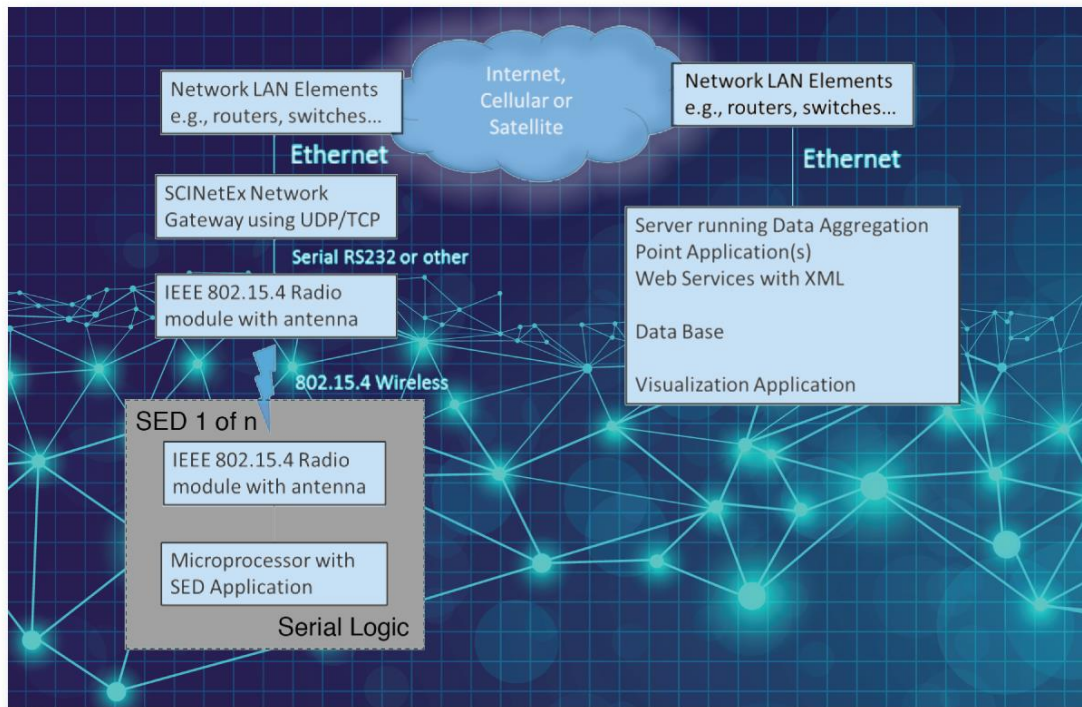


Figure 7-1. Concept Model for Latency Testing.

Section Summary

- IEEE Standard 802.15.4 handles multi-path signal interference exceptionally well.

This page intentionally left blank.

8. APPLICATION LAYER

All FNGs, HNGs and CMs implement the IEEE Standard 802.15.4-2006 MAC and PHY Layers configured per SCINetEx parameters.

8.1 APPLICATION LAYER MESSAGING

Messages are created by the following network component types:

- Data Aggregation Point (DAP).
- Network Gateway (NG).
- Communications Module, a sub-system of the Smart End Device on behalf of sensors in response to DAP commands and during Network Discovery.

Messages are defined here-in so that sender and receiver (e.g., SED and DAP) messages may:

- Perform mutual authentication to preclude rogue devices and DAPs.
- Encrypt and decrypt at the SED, DAP and secure NG with no decryption at intermediate network elements.
- Encrypt only the sensitive data elements.
- Detect lost and invalid messages.
- Provide the sender with a receipt acknowledgement, end-to-end, irrespective of the transport networks between sender and receiver.
- Easily discriminate between proprietary 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 NG coverage:

- 1 Initial Network Discovery,
- 2 Detection of a change in the SED-selected NG or
- 3 Detection of a change in state (i.e., intrusion alarm, fuel level, battery status, Add-on Sensor alarm, etc.).

The CM is required to attempt to transmit a command response message within two (2) seconds of receipt of a command. Time-out periods for retries are identified in Section 8.3.

8.1.1 Date and Time Format

All times, including messages and event records, are in Coordinated Universal Time (UTC/GMT) as 8 bytes. The coding is as shown in the Table 8-1.

Table 8-1. Date and Time Format.

Offset 0	1	2	3	4	5	6	7
Month (1–12) Jan.: 1	Day of month (01–31)	Years since 2000	Day of week (0–6) Sun.: 0	Hours since midnight (0–23)	Minutes after the hour (0–59)	(leap) Seconds after the minute (0–61)	<u>Optional</u> Fractional seconds LSB = 1/100 sec.

Least Significant Bit (LSB)

8.1.2 HNG Messages

8.1.2.1 When the CM has Connectivity with the DAP

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

8.1.2.2 When the CM has No Connectivity with the DAP

CMs communicate with the secure NG when connectivity does not exist with the DAP. In this direct-from-NG case, the secure NG must emulate the DAP messages to include encryption and decryption using DAP-supplied keys. Certain command codes are required, e.g., Disarm by HNG. In this case, the SED communicates directly with an HNG only when not tethered.

8.2 MESSAGE ADDRESSING – END-TO-END

8.2.1 Addressing – for Data Aggregation Point (DAP) Destination

The destination DAP is unknown to the CM but is known by the locale's infrastructure, which forwards every message verbatim to the appropriate DAP. This information is contained in the Level-2 UID of the NGA message and in the UID of the command messages sent by the DAP.

8.2.2 Addressing – for SED Destination

Every security-purposed message from the DAP contains the UID of the DAP as the UID of the message header. The message is composed by the DAP and wrapped in an IP packet (or other equivalent). This packet is sent to the IP address for the last-known NG locale for the SED. At the locale, infrastructure systems send the packet to the proper NG, i.e., NG is likely to be serving (or was most recently serving) the SED with coverage.

8.3 MESSAGE ACKNOWLEDGEMENTS (ACKS) – ERROR DETECTION AND CORRECTION

Independent of all wired/wireless transport media between DAP or secure NG and CM, the following error detection and correction methods are utilized for messaging. Alternative communications modes such as SMS/SMPP are commercial in nature and not subject to the requirements of this section.

8.3.1 Retransmissions for Error Correction – End-to-End

Every transmitted and numbered message yields a numbered acknowledgement (ACK) from the receiver (CM, DAP or secure NG). This is at the Application Layer, independent of Transport Layer error management. 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 DAP or secure NG.

8.3.2 ACK from the SED CM

The acknowledgement (ACK) to a DAP or secure NG command message is the matching command's ascension number stored within the response Status message (or event record Log message if in response to a Send Log command). For log responses, this is applicable only in the first log record. The time-out period is nominally two seconds. The DAP or secure NG retransmits up to five times when in coverage.

8.3.3 ACK from Data Aggregation Point/HNG

The unsolicited Status message sent to a DAP yields an ACK message to the CM. This ACK message is an explicit command message, the structure of which is defined in Section 8.6.5. The time-out period is nominally 20 seconds after completion of the command execution (if applicable). The DAP or secure NG retransmits up to five times when in coverage. The CM does not transmit a status/ACK response to an ACK command message from the DAP or secure NG.

8.3.4 ACK Failure Procedure

If a receiving CM exhausts retransmission limits without receiving an ACK message from the DAP or secure NG, the CM stops attempting to link to that NG for a period of time not to exceed one minute. The CM responds to the next available NGA that employs a different UID immediately with its current status. When a receiving DAP or secure NG exhausts retransmission limits, the next-higher application is advised. The DAP records the ACK failure in its database. The secure NG records the ACK failure in its secure NG Activity Log. Duplicate messages do not require an ascension number increase (i.e., same encryption). The DAP or secure NG increases the ascension number for the next message sent with new encryption.

8.4 APPLICATION LAYER MESSAGE STRUCTURE

8.4.1 Applicability

Every security-purposed message is formatted per this section. The message header (MH) definition is shown in Figure 8-2.

8.4.2 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 DAP in a routed network. Messages should not be parsed until received at the final destination 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 DAP (or secure NG) and SED, 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 8-1.

The application message data plus the message header does not exceed the available payload data area defined by IEEE Standard 802.15.4-2006 with the MAC Layer option described here.

NOTE: The MIC for key management messages is 16 bytes. See Section 9 for the packet structure and protocols of key management messages.

MAC Layer Data Frame, Payload Data Section

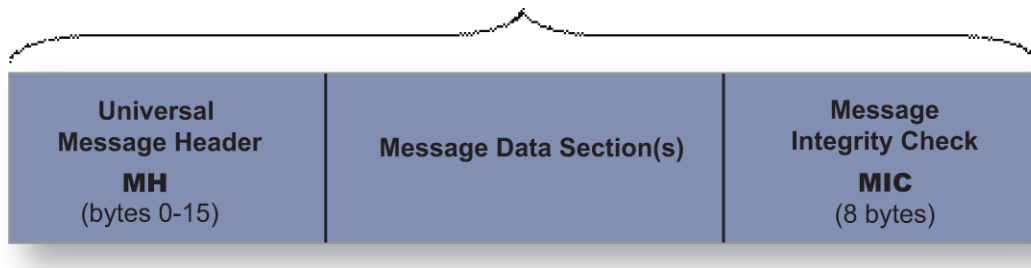


Figure 8-1. SCINetEx Messages – Message within MAC Payload.

8.4.3 Universal Message Header (MH)

The message header (MH) structure and all other message structure of messages traveling between a CM and DAP in either direction is not altered by SCINetEx transport devices. If a message arrives with message header contents not formatted in accordance with Figure 8-2, or is otherwise in error, the NG application drops the packet without processing.

8.4.3.1 MH for SCINetEx Messages

For security-purposed messages, all fields of the message header are formatted as defined here-in. The MH length may change in future SCINetEx revisions; this is defined by the revision number in the MH. Each field of the MH is described below. The MH format shown in Figure 8-1 and detailed in Figure 8-2 is the same for all security-related message types. The MH format applies to messages sent by either CM, DAP or secure NG. The MH within the WPAN MAC Layer data frame payload is not encrypted. This enables optional bridging to/from the WPAN 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 NGs at a locale if mobility management is needed and for unsolicited commands from a DAP.

8.4.3.2 MH Spoofing

It is understood that the MH will not be altered by message transport or transport protocols. Some SCINetEx system transport legs (e.g., those involving satellite and cellular networks) are outside the scope of this technical report. The MH is not intended to be altered by any transport mechanism or protocol defined here-in. 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.

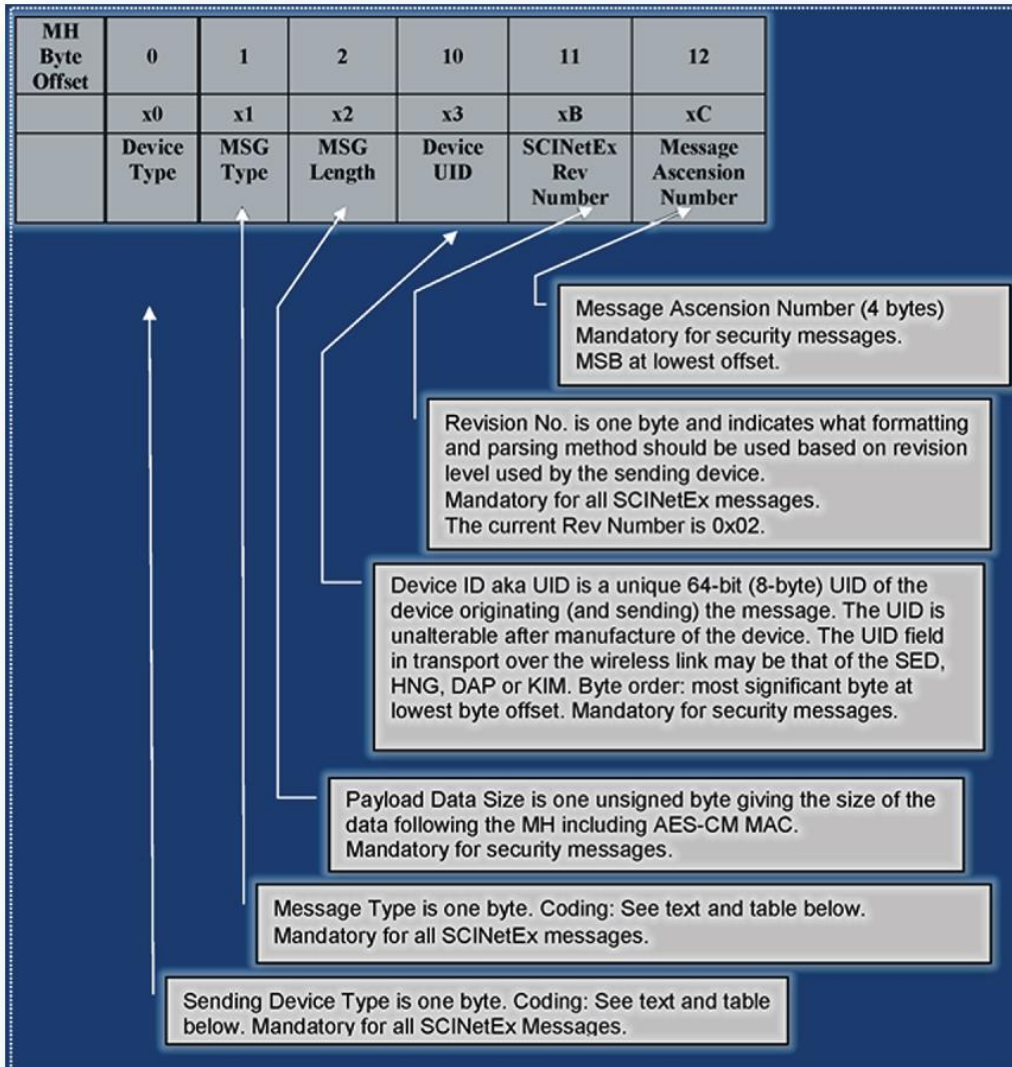


Figure 8-2. Universal Message Header Contents.

8.4.3.3 MH – Device Type Codes

The table below defines SCINetEx device types and corresponding codes for the Device Type Field in the message header.

Table 8-2. MH Device Type Codes.

Device Type	Device Type Field Code
SED – Type 0	0x80
SED – Type 1	0x81
SED – Type 2	0x82
SED – Type 3	0x83
Wireless AoS – Type 0 (not applicable to relay function)	0x84
FNG (non-secure) – Type 0	0x85
HNG (secure) – Type 0	0x86
FNG (secure) – Type 0	0x87
Data Aggregation Point (DAP)	0x88
Key Information Manager (KIM)	0x89
HNG (non-secure) – Type 0	0x90
HNG (non-secure) – Type 1	0x91
FNG Non-Root NG – Type 0 (future use)	0x92
Reserved for future SCINetEx versions	0x01-0x7f

8.4.3.4 MH – Message Type Codes

This field is mandatory for SCINetEx sending device types as in Table 8-2 and irrelevant for other device types.

Table 8-3. MH Message Type (MT) Codes.

Code	Message Type	Message Data Flow
0x00	Unrestricted Status message	from SED to DAP via NG
0x01-0x7F	Reserved for compliant messages for future use	Bi-directional
0x80	Restricted Status message from device as defined here-in	from SED to DAP via NG
0x81	Device event record Log message	from SED to DAP via NG

Table 8-3. MH Message Type (MT) Codes. (Continued)

Code	Message Type	Message Data Flow
0xA0	Sensor Discovery broadcast message (security device NGA)	Broadcast by device
0xA1	Sensor database report message	from SED to NG
0xA2	Add-on Sensor Status message	from AoS to SED
0xA3	Sensor configuration data message from AoS to device	from AoS to SED
0xA4	Configuration data message from device to gateway sensor	from SED to NG
0xA5 - 0xAF	Reserved for additional AoS-related messages	
0xC0	Device unrestricted command message as defined here-in	from DAP to SED via NG
0xC1	Device restricted command message as defined here-in	from DAP to SED via NG
0xC2	Device to sensor restricted command message	Device to AoS (direct)
0xe0	Encryption Rekey	HNG, DAP to SED via NG or direct
0xe1- 0xe9	Reserved for Key Management	See Section 9
0xFF	NGA message	Broadcast by NG; unicast by SED in relay function

8.4.3.5 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 8-2.

8.4.3.6 MH – Device UID

As in Figure 8-2, 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 developer is responsible for obtaining address space for their organization with the ID managing authority (IEEE Extended Unique Identifier (EUI)-64). The transmission byte order is most-significant byte at the lowest MH offset. The UID may be the IEEE Standard 802.15.4-2006 radio MAC address if it is IEEE coordinated as unique.

8.4.3.7 MH – ICD Revision Number

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.

8.4.3.8 MH – Message Ascension Number

Each device type maintains separate “transmit” and “receive” message ascension numbers associated with each unique device with which it communicates. For example, the SED must maintain number pairs for each unique DAP or secure NG 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 is one (1). For a non-secure NG, the message ascension numbers are managed by the DAP. For a secure NG, the numbers are obtained from the DAP and later used for communications by that secure NG.

A message received with a message ascension number less than or equal to the number of the most recently received message is ignored. For a message received with a message ascension number equal to the number of the most recently received message, the previous response is transmitted in identical form. The number of response attempts does not exceed five.

A message received with a message ascension number greater than the number of the most recently received message is accepted with proper response.

8.5 MESSAGE CONTENT

SEDs can all send device Status messages, but each device type has their own distinct Status message. In addition, distinctions are made between restricted and unrestricted status content and between solicited and unsolicited messages. These distinctions are explained in Table 8-4.

8.5.1 Device Restricted Status Message from SED

The device restricted Status message as seen in Figure 8-3 is sent when either of the following conditions holds:

- 1 A valid Status Request command message from the DAP or secure NG is received by the SED. In this case, the Unsolicited Status bit is cleared (0) in the message's Status field. The ACK ascension number field contains the ascension number from the message header of the Status Request command message; The DAP or secure NG may validate using this number.
- 2 The device unsolicited Status message transmission condition is met. In this case, the Unsolicited Status bit is set (1) in the message's Status field.

NOTE: The MIC for key management messages described in Section 9.10.1 is 16 bytes.

Size: $16 + 1 + 55 = 72$ bytes

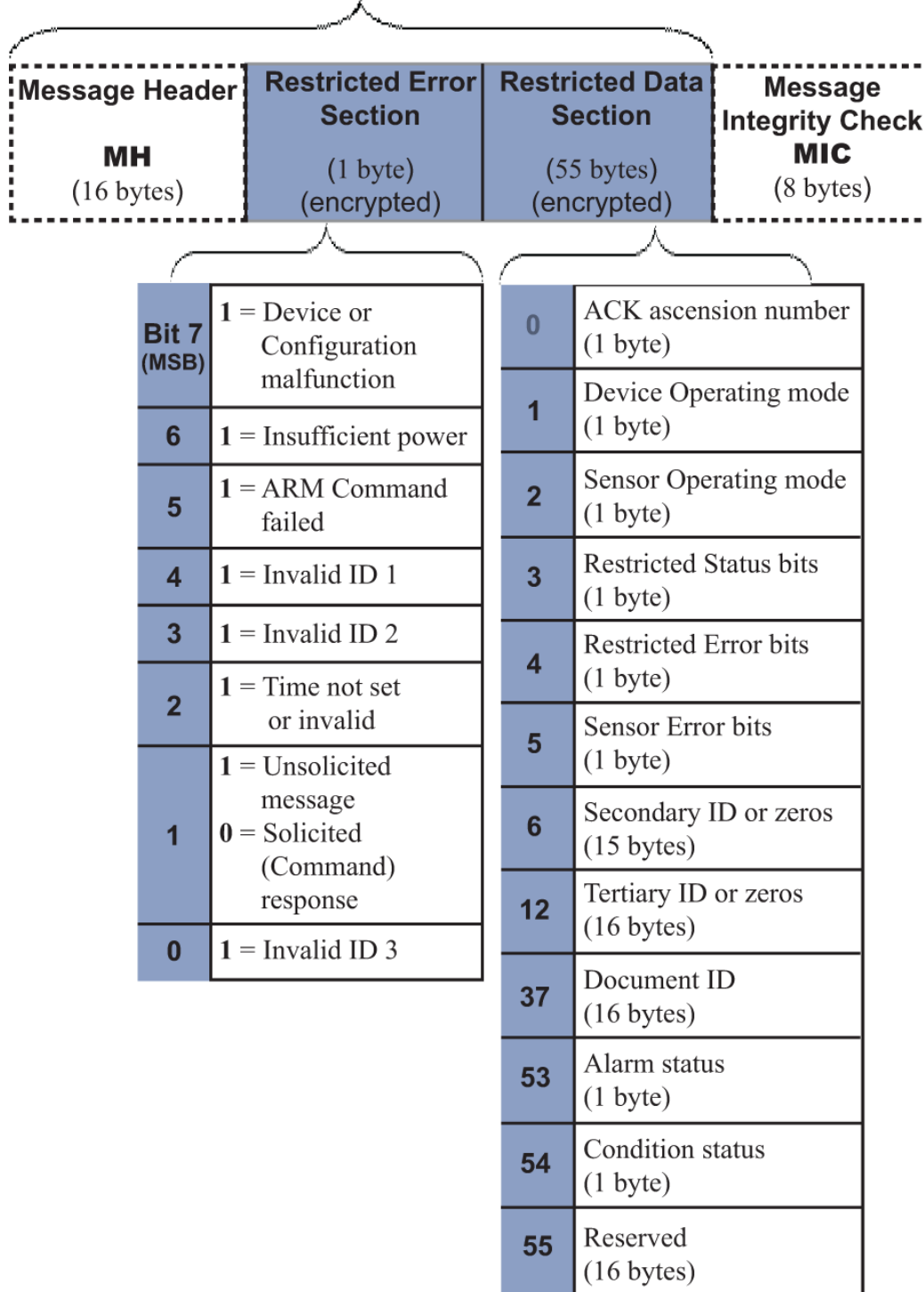


Figure 8-3. Device Status Message.

Table 8-4. Device Status Message Restricted Data Section Content Definition.

Restricted Section Content	Definition
ACK ascension number	Ascension number for corresponding command. N/A for unsolicited Status message.
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 = 1: Sensor 1 Alarm Bit 1 = 1: Sensor 2 Alarm, etc.
Restricted Error bits	Bit 7 = 1: Sensor malfunction Bit 6 = 1: Decryption error Bit 5 = 1: Invalid command Bit 4 = 1: Log overflow Bit 3 = 1: ACK failure Bit 2 = 1: Configuration failed Bit 1 = 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 bits.
Secondary ID	ASCII characters; unused portion to be padded with zeros. See Section 8.5.1.1
Tertiary ID and Checksum	Unique identifier for asset. See Section 8.5.1.2
Document ID	ASCII characters.
Alarm status	See Section 8.5.1.3
Condition status	See Section 8.5.1.4

8.5.1.1 Secondary ID

This identifier is not to exceed 15 alphanumeric characters consistent with the requirements of the implementer. The number is right-aligned and padded with leading zeros as required. The Secondary ID may be any ID unspecified by SCINetEx and incorporated by the implementer.

8.5.1.2 Tertiary ID

The Tertiary ID field is 16 bytes. The first byte codifies what form of mobile or fixed asset ID is present in the remaining bytes, as follows. Unused bytes are zero-filled.

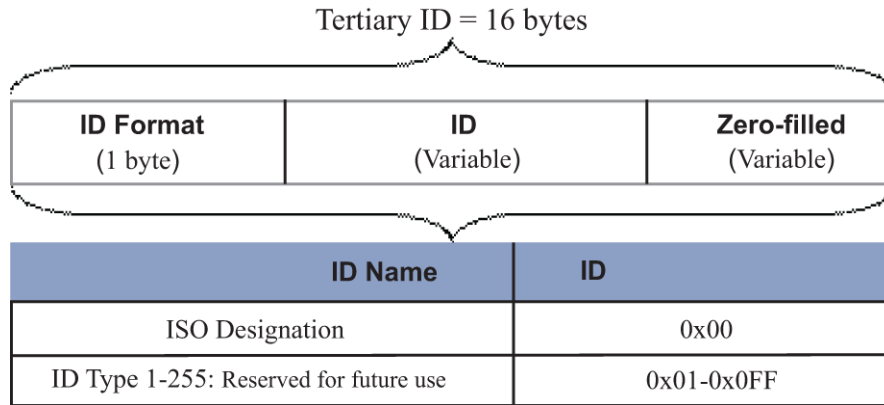


Figure 8-4. Tertiary ID Field.

8.5.1.3 Alarm Status

The Alarm status is a single byte that represents the alarm state of the SED as defined in the table below.

Table 8-5. Alarm Status Parameter.

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

8.5.1.4 Condition Status

The Condition status is a single byte that represents the asset state as detected by the SED as defined in the table below.

Table 8-6. Condition Status Parameter.

Door Parameter	Door Status
0x00	Normal
0x01	Exception
0x02 through 0xFF	Reserved

8.5.2 Device Restricted Status Message from SED with GPS

Devices that are GPS-enabled are capable of generating a Status message that includes the universal message header and CM integral sensor data as follows. This Status message is completely independent of the SED Type 1 messages and is passed to the DAP via a secure NG or non-secure NG.

NOTE: The MIC for Rekey command messages in Section 9.10.1 is 16 bytes long.

The device restricted Status message is sent when:

- The SED receives a valid No Operation (NOP) command message from the DAP or secure NG. In this case, the Unsolicited Status bit in the Status field of the Status message will be false (0). The ACK ascension number field contains the ascension number from the message header of the Status Request command message; the DAP or secure NG validate using this number.
- The device unsolicited Status message transmission condition is met. In this case, the Unsolicited Status bit in the Status field of the Status message will be true (1).
- Conditions are met of pre-programmed time intervals, distance intervals or periods of sustained loss of GPS. These intervals/periods are established at the time of commissioning.

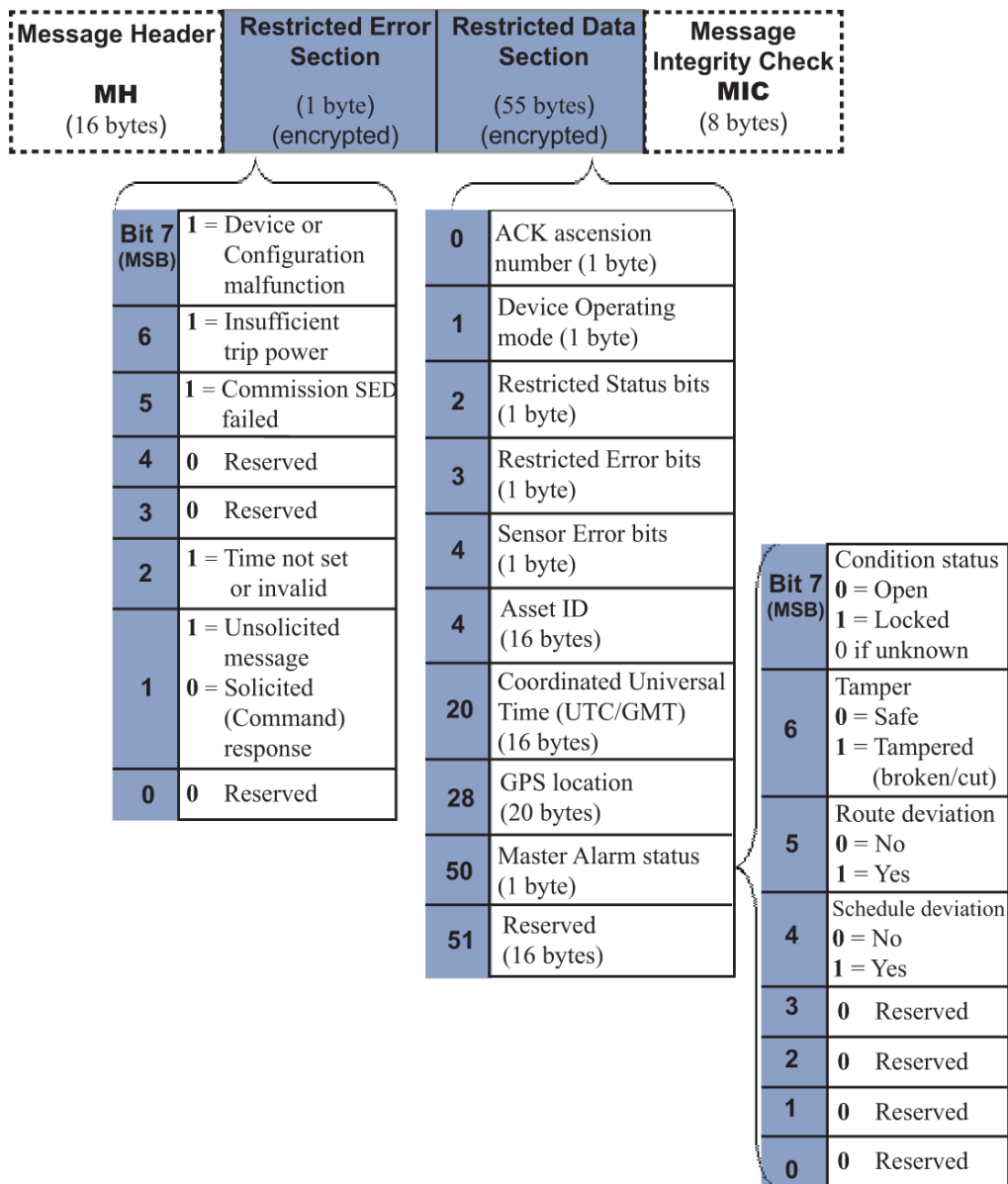


Figure 8-5. Device Status Message.

Table 8-7. SED with GPS Restricted Data Section Detail.

Restricted Section	Definition
ACK ascension number	Ascension number for corresponding command. N/A for unsolicited Status message.
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 = 1: Sensor malfunction Bit 6 = 1: Decryption error Bit 5 = 1: Invalid command Bit 4 = 1: Log overflow Bit 3 = 1: ACK failure Bit 2 = 1: Configuration failed Bit 1 = 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
Asset ID and checksum	Unique identifier for asset.
Coordinated Universal Time	See Section 8.1.1
GPS location	See Section 8.5.3
Master 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

8.5.3 Waypoint and Location Data Formats

Waypoint and location data are in the format specified below, for all mobile asset use-cases. These include:

- CMpositionreportsinstatusandlogentries.
- Waypoint/routedefinitionssentbytheDAP.

All GPS data is directly copied from the National Marine Electronic Association (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 SCINetEx compliance, 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, such as:

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

Leading and trailing zeros are used as needed for these fixed length fields.

8.5.4 Unrestricted Status Message from SED – Solicited

The device unrestricted Status message is sent in reply to the Send Unrestricted Status command message.

During the process of arming the SED, errors may occur prior to the exchange of encryption keys as detailed in Section 9. These error messages may be made available to the operator in an unencrypted format via an unrestricted Status message containing information about the error. The unrestricted Status message is treated as a solicited non-conforming message (message type code 0x00) and appended to the universal message header. The remaining reserved frame bytes (noted as “Reserved (n bytes)”) may be used for developer-specific data. This solicited status is an implicit ACK, analogous to the response to the restricted NOP command message. The message format is shown in the Figure 8-6.

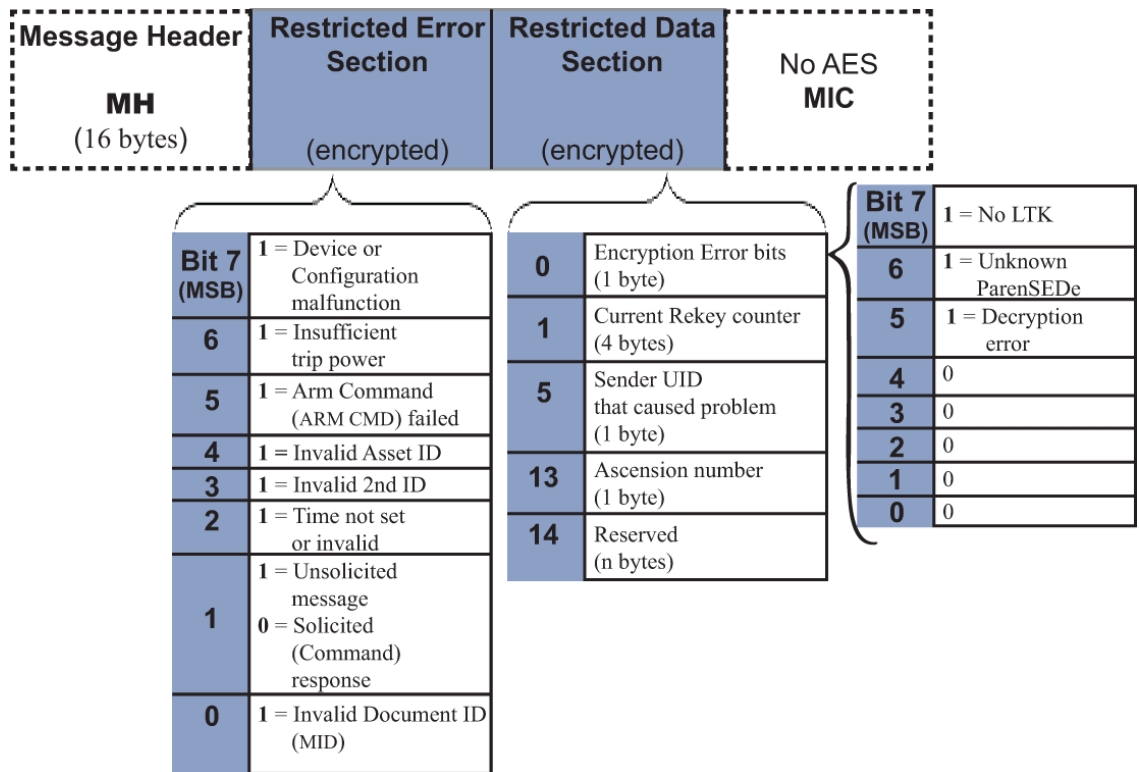


Figure 8-6. Device Status – Unrestricted Status Reply from SED.

8.5.5 Unrestricted Status Message from Tethered SED – Solicited

The unrestricted Status message is sent in reply to the Send Unrestricted Status command message.

During the process of arming the SED and tethering with a relay SED errors may occur, as detailed here-in, 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 the figure below. Such an unrestricted Status message incorporates the universal message header and is treated as a solicited non-conforming message (message type code 0x00). The remaining frame-bytes are reserved for future use. See Section 8.4.3.8 for a discussion of ascension numbers.

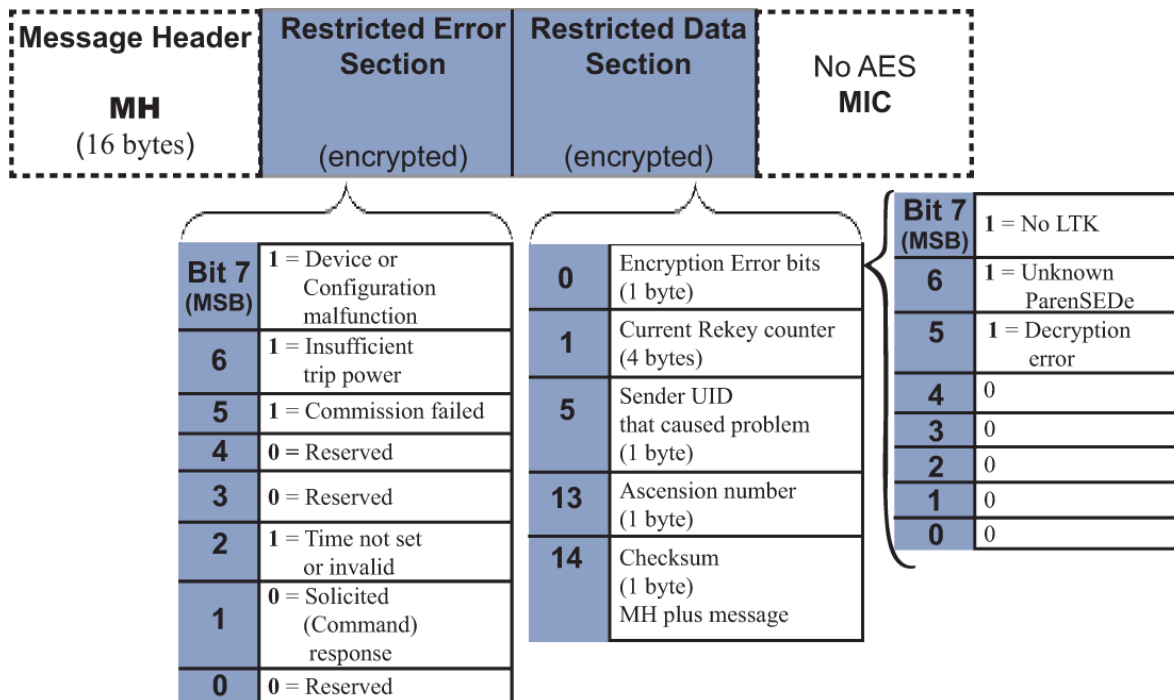


Figure 8-7. Device Status – Unrestricted Status Reply Content from Tethered SED.

8.5.6 Device Status Message from SED – Unsolicited

After Network Discovery is successful, the SED sends an unsolicited Status message as a presence announcement. This message is restricted (i.e., encrypted) and is sent at the impetus of the SED. The format is described in Section 8.5.2.

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

- An alarm or exception condition exists and has not been sent with receipt-acknowledgement.
- The last unsolicited Status message or Status Request command was sent more than a nominal ten minutes in the past, and the SED was not in secure NG coverage during this time period.
- The channel, PANID or selected NG changed due to Network Discovery, since the last Status message was sent.

When all of the conditions listed above are false, all recurring unsolicited Status messages are suppressed to minimize redundant messages and battery consumption in weak RF signal conditions.

8.5.7 Device Status Message from SED with GPS – Unsolicited

After Network Discovery is successful, the SED sends an unsolicited Status message as a presence announcement. This message is restricted (i.e., encrypted) and is sent at the impetus of the SED. The format is described in Section 8.5.2.

This unsolicited message is sent when there is communications connectivity (in either the primary or one of the secondary modes) and any condition in Section 8.5.6 is true.

8.5.8 SED Event Log Records

Device event logs contain event records. Event records are created per the implementer's requirements but are fully supported by SCINetEx.

8.5.8.1 Send Event Log All Command

When a SED receives a valid Send Event Log All command message, it sends the entire contents of its event log records to the requestor. If an event log record is not acknowledged by the requesting entity and the device has exhausted the retransmission limits for that message, the device stops transmitting event log record messages.

8.5.8.2 Send Event Log Unsent Command

When a SED receives a valid Send Event Log Unsent command message, it transmits all unsent event log records to the requestor. An event log 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 8.5.8.1) and new records acquired since the last Send Event Log (All or Unsent) command message. For the purpose of responding to the Send Event Log Unsent command, the device considers an event log record to be unsent if:

- 1 The event log record has never been sent or
- 2 The event log record message has never been acknowledged.

8.5.8.3 Event Log Records Sequence

The secure NG or DAP sends the Send Event Log All or the Send Event Log Unsent command message. When the SED receives this command message, it transmits the event log records as multiple messages, each containing a single event log record with an ACK from the DAP or secure NG. This command, as others, if sent more than two seconds after the last message exchange, will cause the NG to use the NGA Message Waiting mechanism for sending the command. The SED sends the Message Waiting response NULL message and expects the command to be sent within two seconds. The response to the command is the first event log record message. The DAP or secure NG sends a valid ACK as defined by SCINetEx. A received DAP or secure NG ACK is the indicator that the on-asset SED should send the next event log record message.

Each event log record message that is transmitted contains the least significant byte ascension number of the command or subsequent ACK, for detecting lost messages. The ascension number in the message header is used as in other messages, for detecting retransmissions or lost messages.

8.5.8.4 Event Log Records Message Content

In response to a Send Event Log command message, the SED responds with one or more event log record messages, as shown in Figure 8-8 and Figure 8-9, with one event log record per message. If there are no logged events (empty log), the Event Message Type of the event log record indicates "End of Records" (0xFF). The final (or sole) event log record message is sent with Event Message Type = 0xFF.

8.5.8.5 Event Log Records Message ACK

For each event log record message, the DAP or secure NG sends an ACK (a form of command) as shown in Section 8.7. On ACK time-out, the message is repeated up to five times. On failure, the ACK failure bit in the Restricted Status is set true (1) and event log record transmissions cease. The DAP or secure NG takes appropriate action (e.g., try later, inform person, etc.).

8.5.8.6 Event Log Record Message Format for SEDs without GPS

The requirements for the event log record encryption are determined by the implementer.

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

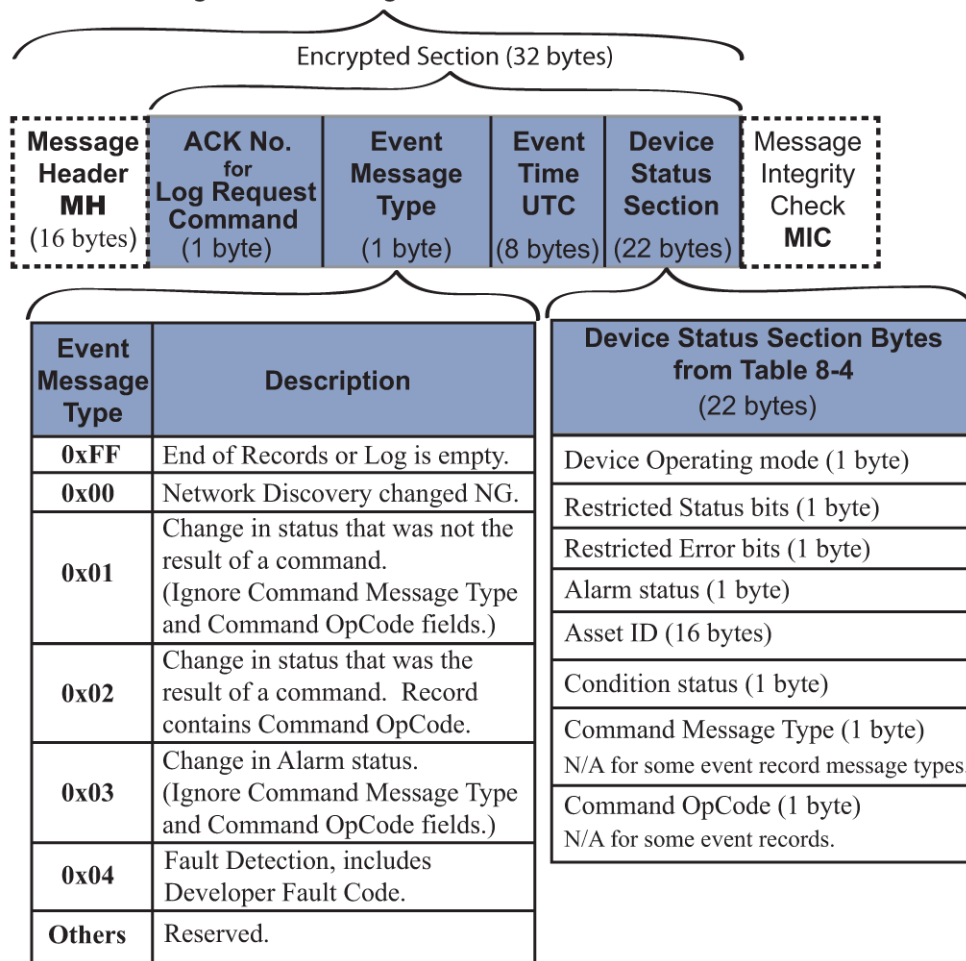


Figure 8-8. Event Log Message (to DAP).

8.5.8.7 Event Message Type

The Event Message type field indicates the type of event that generated the Send Event Log command message. If Event Message Type is equal to 0x02, the Command 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.

8.5.8.8 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 Event Message Type (from the MH) of the command is recorded in the Command Message Type field as well as the command OpCode.

8.5.8.9 Event Log Record Message Format for SED with GPS

The requirements for event log record encryption are determined by the implementer.

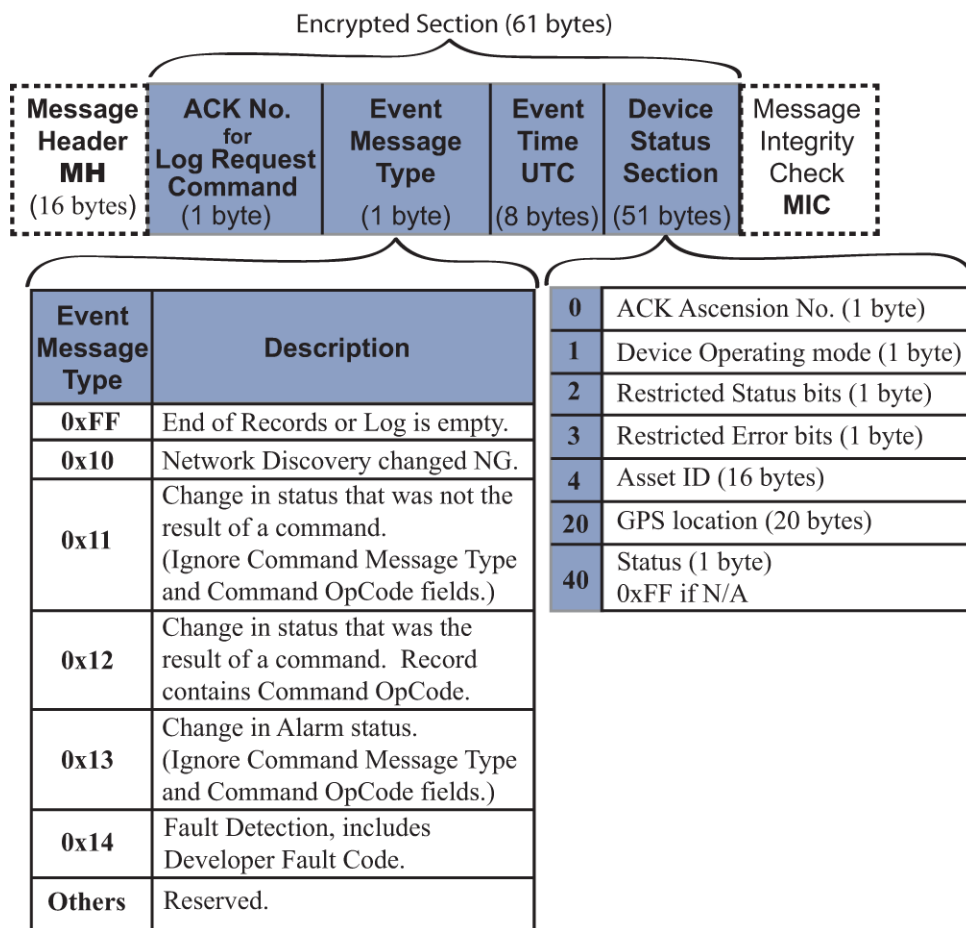


Figure 8-9. Event Log Message (from SED to DAP or secure NG).

8.6 COMMAND MESSAGES FROM DAP OR SECURE NG

Messages from the DAP or secure NG to the SED are considered command messages. The structure of command messages is as shown below. The Message Type code shown in Table 8-3 denotes whether the command is restricted (encrypted) or unrestricted (not encrypted). The SED receives command messages by recognition of its UID in the NGA Message Waiting list, and maintaining listening period not less than two seconds to allow receipt of the command. Once the command is received, the SED may resume its power conservation method.

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

8.6.1 Unrestricted Command messages for SED

Unrestricted commands may be issued by DAP, secure NGs or non-secure NGs. The only unrestricted OpCode defined here-in is Send Unrestricted Status, which has no parameters, and the reply for which contains only unrestricted data. Non-conforming commands use a designated 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 8-10. 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.

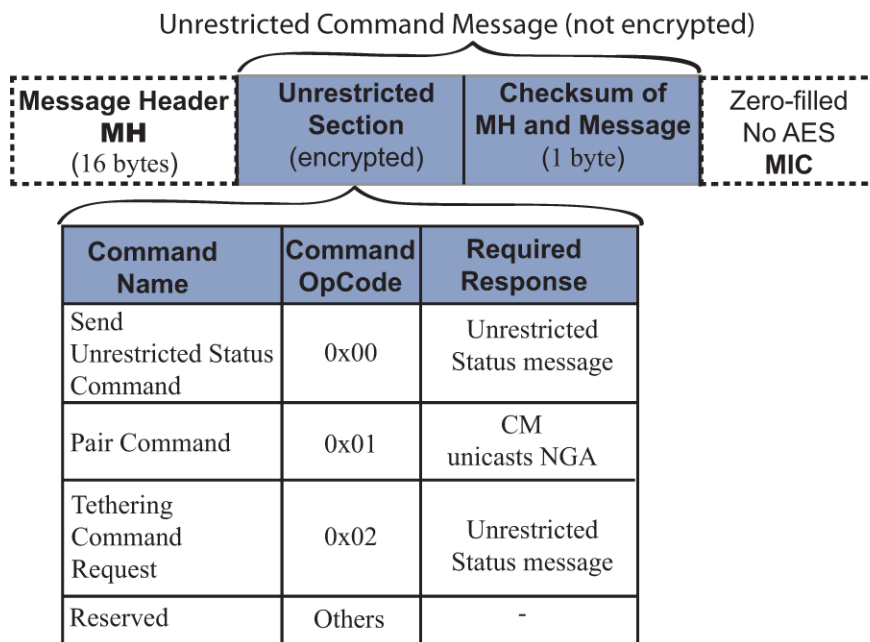


Figure 8-10. Unrestricted Command (Message Type 0xC0).

8.6.2 Restricted Command Messages for SED No GPS

Restricted command messages are issued by DAPs and secure NGs to initiate a status message exchange or change the operational state of the SED. The message structure is shown in Figure 8-11. Every restricted command message yields a Status message response, with the exception of the from-DAP ACK command from a DAP (ID = 1), for which there is no response.

Message Header MH (16 bytes)		Restricted Section (encrypted)		Message Integrity Check MIC (8 bytes)		
Security Message Command	Cmd OpCode	Required Response	Parameter 1	Parameter 2	Parameter 3	Parameter 4
NOP (no operation)	0x00	Status		(none)	(none)	
Acknowledgement (ACK)	0x01	Status	Ascension No. (1 byte, LSB of 4 byte ascension number)	(none)	(none)	
Set In-use State (SIS)	0x02	Status	See Table 8-9 (1 byte)	(none)	(none)	
Set Time (ST) (see also NGA message time)	0x03	Status	8 bytes, UTC time, format per SCINetEx	(none)	(none)	
Arm with Use Information (ARMT)	0x04	Status	Asset ID per SCINetEx (16 bytes)	Document ID (16 bytes)	Seal ID right-aligned with leading spaces(15 bytes)	Sensor(s) to Enable Bit 0 = Sensor 1, etc. (1 byte)
Change Use Information (CTI)	0x05	Status	Asset ID per SCINetEx (16 bytes)	Document ID (16 bytes)	Seal ID right-aligned with leading spaces(15 bytes)	
Disarm from DAP (DADC)	0x80	Status	(none)	(none)	(none)	
Disarm from secure NG	0x81	Status	(none)	(none)	(none)	
Set Master Alarm = True	0xA1	Status	(none)	(none)	(none)	
Set Master Alarm = False	0xA2	Status	(none)	(none)	(none)	
Send Event Log Unsent (SLU)	0xA3	Status, then unsent log records				
Send Event Log All (SL)	0xA4	Status, then log records	(none)	(none)	(none)	
Erase Event Log (EL)	0xA5	Status	(none)	(none)	(none)	

Figure 8-11. Restricted Command Message Structure (Message Type 0xC1).

Message Header MH (16 bytes)	Restricted Section (encrypted)		Message Integrity Check MIC (8 bytes)			
Security Message Command	Cmd OpCode	Required Response	Parameter 1	Parameter 2	Parameter 3	Parameter 4
NG Enable Sensor(s) (NES)	0xA6	Status	Bit 0 = Sensor 1 Bit 1 = Sensor 2 etc.	(none)	(none)	
NG Disable Sensor(s) (NDS)	0xA7	Status	Bit 0 = Sensor 1 Bit 1 = Sensor 2 etc.	(none)	(none)	
Configure Sensor(s) (CS)	0xA8	Status	Bit 0 = Sensor 1 Bit 1 = Sensor 2 etc.	Size of payload	Configuration	
Read Sensor Configuration	0xA9	SED-to-NG Sensor Configuration Data Message	Sensor Number (1 byte) (0x01 = Sensor 1, 0x02 = Sensor 2, etc.) Only one sensor can be queried at a time			
Sensor Tethering	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 8-11. Restricted Command Message Structure. (Continued).

8.6.3 Restricted Command Messages – for SEDs with GPS

Restricted command messages may be issued by a DAP and some NGs to initiate a status message exchange, provision or change the operational state of a SED. The message structure is identical to that described in Section 8.4 and the SED commands detailed in Table 8-8.

Table 8-8. Restricted Command Messages for SEDs with GPS.

Security Message Command	OpCode	Required Response	Parameter 1	Parameter 2	Parameter 3	Parameter 4
No operation (NOP)	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 NGA message time)	0x03	Status	8 bytes, UTC time, Format per SCINetEx	(none)	(none)	(none)
Commission with use Information (CWT)	0x04	Status	Asset ID per SCINetEx (16 bytes)	(none)	(none)	(none)
Change use information (CPI)	0x05	Status	Asset ID per SCINetEx (16 bytes)	(none)	(none)	(none)
Waypoint List New (WLN)	0x06	ACK	Last waypoint	Latitude (8 byte ASCII)	Longitude (8 byte ASCII)	Radius (meters) (4 byte ASCII)
Waypoint List Append (WLA)	0x07	ACK	Last waypoint	Latitude (8 byte ASCII) See Note 1	Longitude (8 byte ASCII) See Note 1	Radius (meters) (4 byte ASCII) See Note 1
Decommission from DAP (DADC)	0x80	Status	(none)	(none)	(none)	(none)
Decommission from Secure NG (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)

Table 8-8. Restricted Command Messages for SEDs with GPS. (Continued)

Security Message Command	OpCode	Required Response	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Send Event Log Unsent (SLU)	0xA3	Status, then unsent log records				(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)

Send Event Log All (SLU)
Send Event Log Unsent (SL)

NOTE 1: Waypoint coordinate formats are:

Latitude: Per Section 7.5.7

Longitude Per Section 7.5.7

Radius: Per Section 7.5.7

8.6.4 No Operation (NOP) Command Message from DAP or Secure NG

Response by CM is a restricted Status message. No other action is taken.

8.6.5 ACK Message from DAP or Secure NG

The DAP or secure NG sends an ACK for the message number given in parameter 1 after error-free receipt from the CM. Successful ACKs are not logged.

8.6.6 Disarm Command Message from DAP or Secure NG

Upon receipt of the Disarm command message from a DAP (OpCode 0x80 Figure 8-11) or secure NG (OpCode 0x81 Figure 8-11), the SED successfully downloads the entire event log record to the commanding DAP or secure NG and erases the event log record before executing the Disarm command.

8.6.7 Decommission Command Message from DAP or Secure NG

Upon receipt of a Decommission command message from a DAP (OpCode 0x80 Table 8-8) or secure NG (OpCode 0x81 Table 8-8), the SED successfully downloads the entire event log record to the commanding DAP or secure NG and erases the event log record before executing the Decommission command.

8.6.8 Set In-use State

Parameter 1 of the Set In-use State command is defined in Table 8-9. The purpose of this optional command is for the DAP or secure NG to indicate the asset's in-use state to assist the device in battery conservation, e.g., reduced frequency of Network Discovery or suitable changes in sensor management.

Table 8-9. Set In-use 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
11		X	
12	X		In storage
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

8.6.9 Garbled Application Layer ACKs Received by SED

Application Layer ACKs exchanged between DAP or secure NGs and SEDs may become garbled or lost. If an anticipated Application Layer ACK is received but is unreadable or not received within the allowable the two second time-out by an on-asset device, the SED resends the identical message as described in Section 8.3.1, repeated no more than five times for a single message or until a valid ACK is received from the DAP or secure NG.

If retries are exhausted, the SED will cease retries for a period of time not to exceed one minute to that sender (DAP or secure NG) UID. When the next Network Discovery succeeds, the current status of the on-asset device is reported in the usual unsolicited Status message.

8.6.10 Garbled Application Layer ACKs Received by DAPs or HNGs

In response to every DAP or secure NG command message, except the ACK message, the SED sends a response. The response, for most command messages is a restricted Status message with the “is unsolicited” bit false, meaning the response was solicited. The response to the Send Event Log command message is not a Status message, but rather is an event log record message. In both cases, the response contains the least significant byte of the command message’s ascension number. The DAP or secure NG uses this for error detection, e.g., lost message detection.

If a response is received but unreadable by the DAP or secure NG, or is not received within the allowed time out, the DAP or secure NG resends the command message, repeated no more than five times for a single command message or until a valid response is received from the addressed CM. Each resent command message will be noted in the DAP database or secure NG Activity log (this special situation is not covered in the Section 8.7 ladder diagrams). After five unsuccessful attempts, the DAP will store that command message and forward it at the next message transmission opportunity. After five unsuccessful attempts, the secure NG will record the error condition in its Activity log and the operator will take corrective actions. These actions are the responsibility of the secure NG operator and are beyond the scope of this technical report.

8.7 ROUTINE MESSAGING LADDER DIAGRAMS

8.7.1 Broadcast Network Discovery Ladder Diagram for NG Function

Prerequisite: None

Depicts Passive Scan Network Discovery using NGA. The CM does no transmissions.

Active scan Network Discovery is not required and is not depicted. Any active scan implemented for proprietary Network Discovery implements clear channel assessment (CCA) in some form and does not interfere with the passive scan method described here-in. An NG performs CCA before transmitting an NGA (or any other) data frame, see Figure 8-12. The SED is regarded as State Aware and may choose not to “wake up” for every NGA message, subject to the requirements of Section 5.1.1.

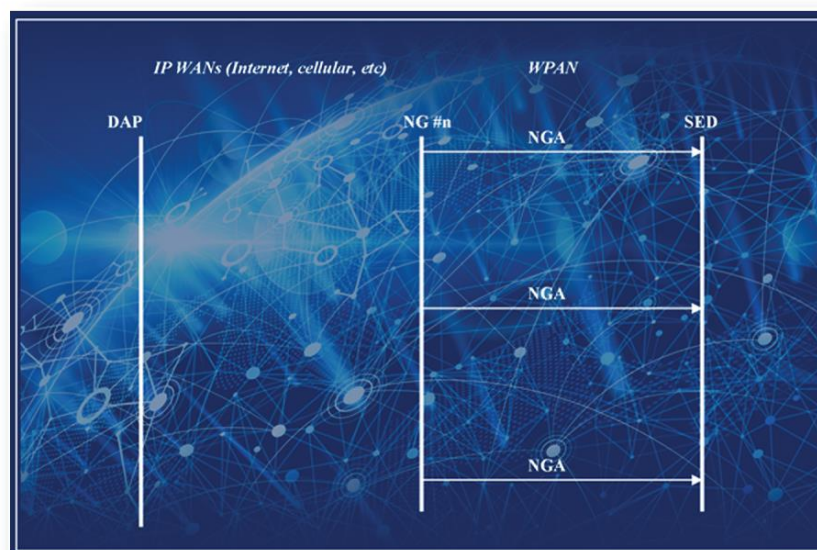


Figure 8-12. Network Gateway Announcement (NGA) Ladder Diagram.

8.7.2 Unsolicited Status Message (to DAP or Secure NG) Ladder Diagram

Prerequisite: Network Discovery is complete. Trigger criteria are given in Section 5.1.6. CM performs clear channel assessment before transmitting, see Figure 8-13.

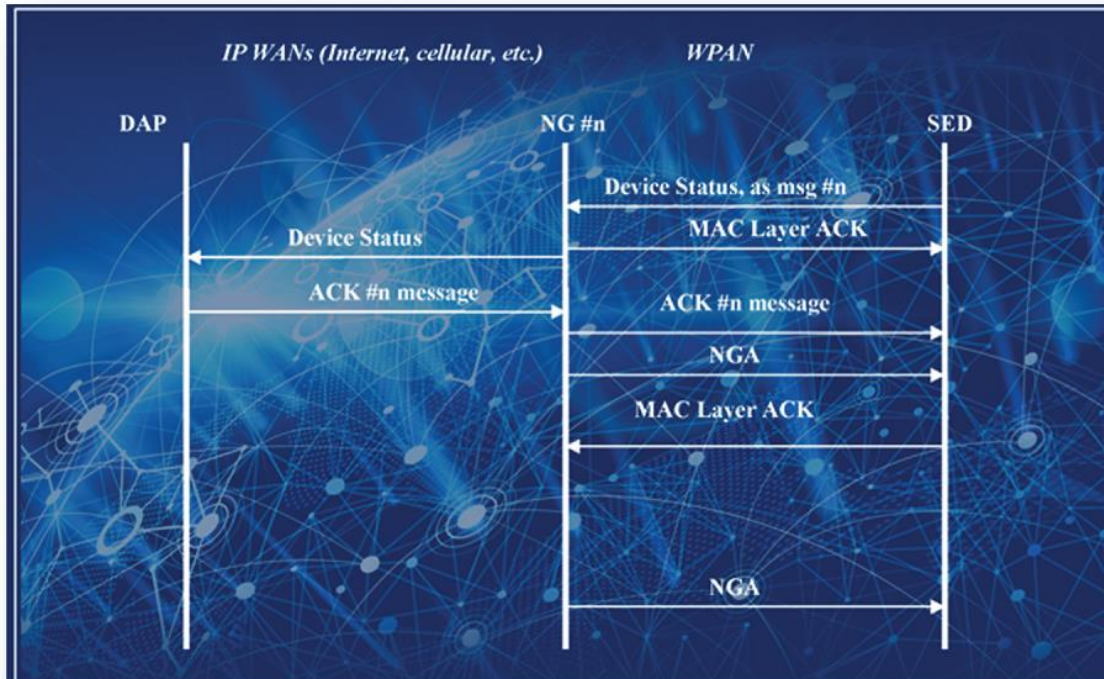


Figure 8-13. Unsolicited Status Message Ladder Diagram.

The above figure is not to time scale. The duration of the device Status message transmission is small compared to the NGA 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 NG-to/from-DAP is compatible with the two second time-out for ACKs and the time window for suppressing Message Waiting, e.g., for successive event log records.

8.7.3 DAP or Secure NG-originated Message Ladder Diagram

Prerequisite: Network Discovery complete. DAP knows which NG to use based on the unsolicited Status message sent after Network Discovery. Optionally, the DAP uses the last known NG, see Figure 8-14.

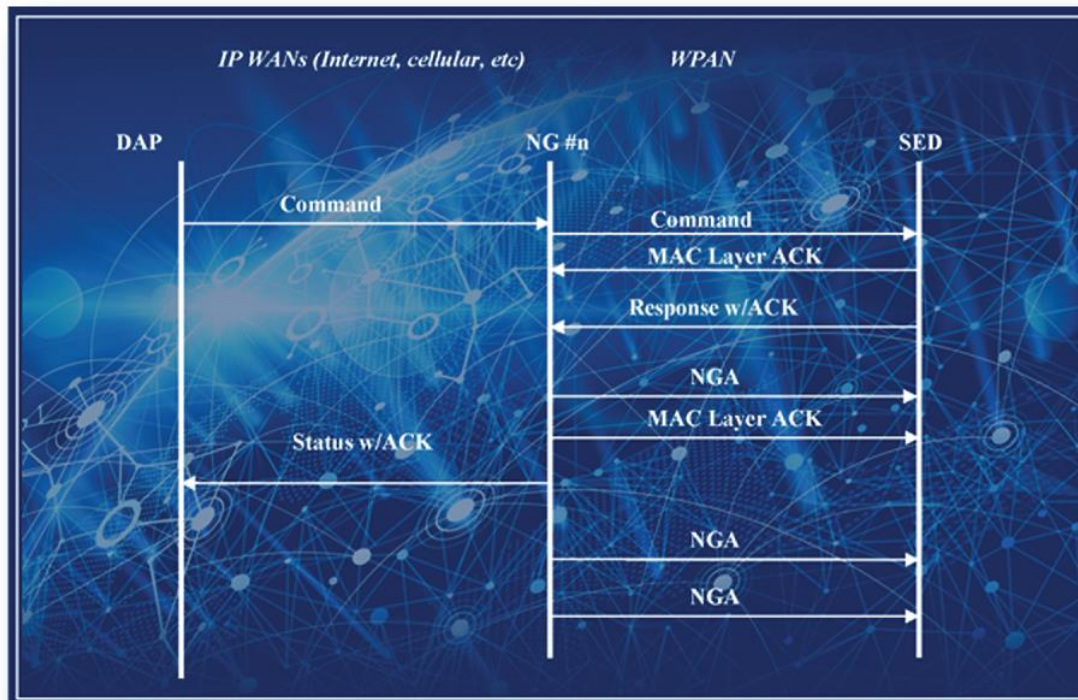


Figure 8-14. DAP or NG Message Ladder Diagram.

The above is not to time scale. See discussion in the prior section. If the DAP does not receive the ACK #n, the DAP times out and repeats the command message. If the command message yields response data such as status, a CM-to-DAP message is sent by the CM after sending the ACK #n to the DAP. The procedure for this is the same as for the device Status message shown in Section 8.7.2.

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

8.7.4 Event Log Record Message and Responses Ladder Diagram

Prerequisite: Network Discovery complete, see Figure 8-15.

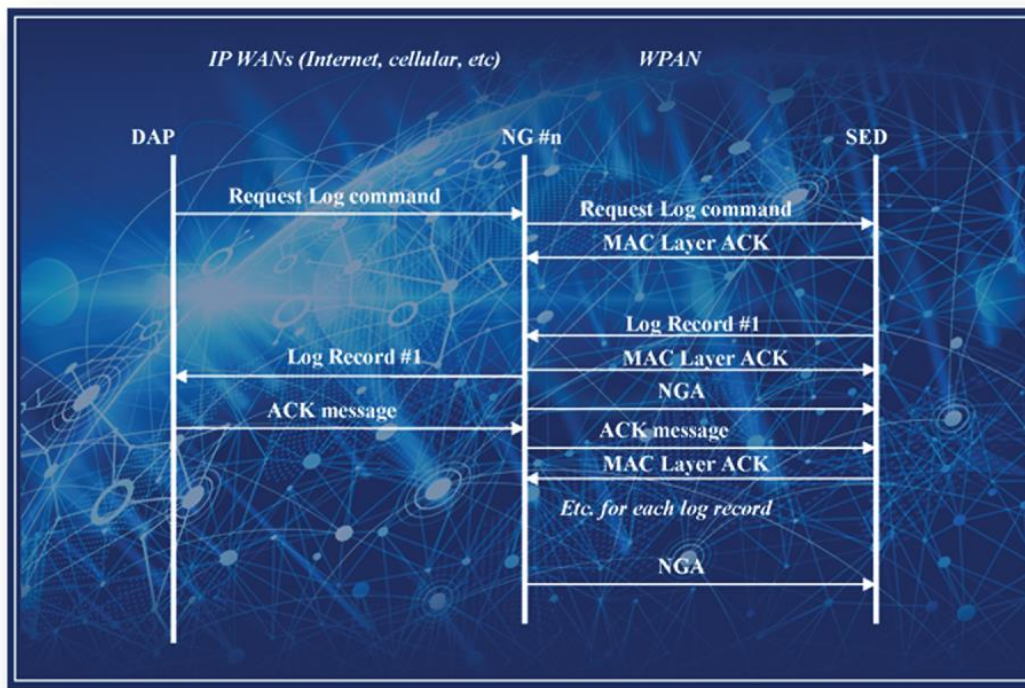


Figure 8-15. Event Log Record Message Diagram.

Section Summary

- All data and command packets are defined by SCINetEx.
- All routing protocols are defined by SCINetEx.

This page intentionally left blank.

9. 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-asset devices contain encryption, authentication, message integrity checks and anti-spoof mechanisms that are:

- Compliant with the most stringent information protection policies among international locales.
- Independent of all transport media between the DAP and the SED. This may be any number of inter-working networks.

As shown in Figure 8-1, and elsewhere in this section, command messages from a DAP or secure NG and reply and Status messages from a SED contain a section of payload data that is encrypted.

9.1 802.15.4 WIRELESS NETWORK INTERFERENCE MITIGATION

9.1.1 Irrelevant Wireless PANs at Locale

The process for ignoring irrelevant but valid transmissions on “external” networks is 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 here-in. SCINetEx requires that a secure (encrypted) ACK must be received by the CM from a DAP or secure NG 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 DAP or secure NG, irrespective of the WPAN access devices. Proprietary messages conforming to SCINetEx provide an equivalent means.

9.1.2 Persistent Interference or Denial of Service – Wireless

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

9.2 CYBER SECURITY

The intent for SCINetEx messages is that the security of these messages be controlled at the Application Layer. The view of having Application Layer security allows Application Layer packets/messages to be essentially independent of the delivery mechanisms. This simplifies the overall mandated portions of the system and allows the message to have a great deal of flexibility in delivery. Other security mechanisms may be applied as a message passes through the system including cypher text monitoring as long as they don’t interfere with the security protocols described here-in.

For the SCINetEx system to be secure, cryptographic keys must be utilized. The method of key management is important for overall network and data security. The key management system must account for all aspects of key lifecycle, which is commonly broken up into the following twelve activities: Generation, Distribution, Installation, Key Exchange, Use, Update, Revocation, Destruction, Storage, Backup/Recovery, Archiving and Audit.

In this technical report a hierarchy is described with four security layers and entities that reside within those layers. Those layers (and the following discussion) are pictorially described in Figure 9-1.

- The Key Information Manager (KIM) will be a single entity at Level 0. The KIM controls all key change operations. The KIM does not process network data and must not communicate directly with any network device other than the Level 1 entities.
- The physically secure Data Aggregation Points (DAPs) are at Level 1. These facilities may be either mobile or fixed and are the intended recipients of most of the network data. They must have the resources to control and manage, potentially on the order of thousands of SEDs. In reality these facilities manage the network and make decisions concerning its operations.
- Fixed Network Gateways (FNGs), Secure Handheld Network Gateways (SHNGs), handheld Network Gateways (HNGs) and like devices or facilities with limited authority (as dictated by Level 1 facilities) are at Level 2. As lessons are learned and commercial support is realized, products and services will be introduced into the cargo security market. We cannot predict all future functionality, but Level 2 is designed to support a wide range of eventual functionality.
- On-asset devices such as SEDs are at Level 3. These may be battery powered and have limited computational and communication resources.

The cryptographic primitives and the implementation phases are designed so that little change is needed to be made in the network or its devices in order to support transition to later implementation phases. More precisely, there should be no negative impact to fielded SEDs when new functionality is introduced into the SCINetEx system. It is expected that changes will be made at the Level 1 facilities in order to support changes in functionality. However, the design here-in will require minimal changes in the key management system.

9.3 CYBER MANAGEMENT PHASED IMPLEMENTATION APPROACH

The intent of the cyber management system described in this technical report is to provide a reasonable path toward optimal SCINetEx security. It is recommended this be done in implementable phases where lessons may be learned and the phases modified as needed.

Phased Implementation

Phase 1 and Phase 2 implementation of the SCINetEx system assume a single entity will take ownership and responsibility for all data and see that the first implementation phases are complete and functional. Global SCINetEx security may in some cases be a multi-national challenge and the security architecture must scale accordingly. Even within a single country, the security architecture must include a mechanism to support data sharing between multiple agencies or organizations. They will need access to data and need to have fielded devices to support security operations. To facilitate this eventuality, Phase 3 includes multiple Level 1 facilities. The intent is that the Level 1 facilities exercise significant control in the network. It is assumed for Phase 3 that every Level 1 facility is able to cooperate fully with every other Level 1 facility and do so in a trusted fashion.

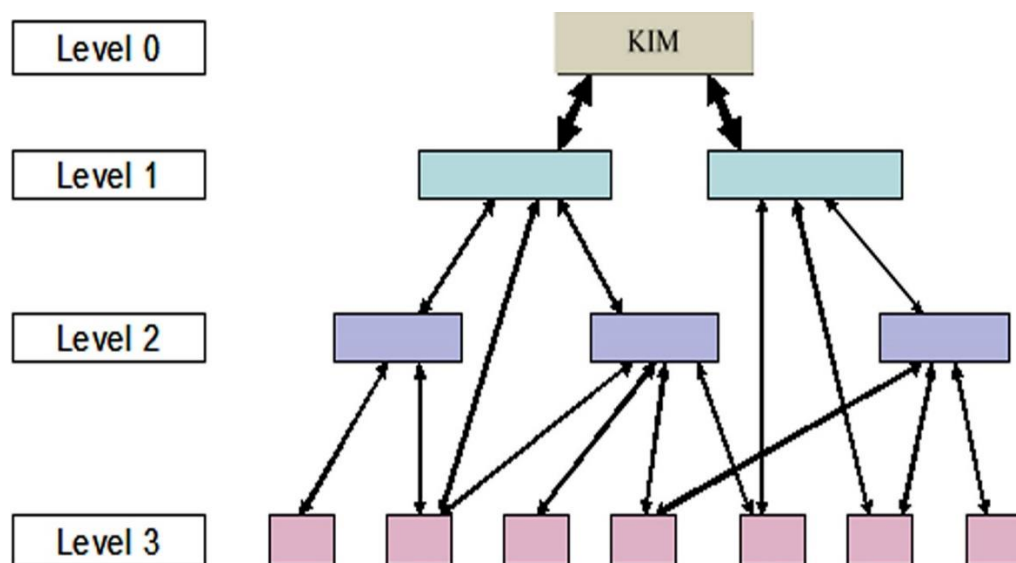


Figure 9-1. Implementation Phase 3 Key Management Hierarchy.

From a key management perspective, the adoption of Phase 2 completes the various key types needed in the SCINetEx system. The inclusion of multiple Level 1 facilities adds a complexity to the use cases of the system and changes the threat model. A great deal of trust and cooperation is needed to make things run smoothly. A few technical measures will be put in place to help, but the largest hurdle is beyond the scope of the technical measures. But rather, the political and human factors tend to be the most difficult to manage.

Just as Phase 1 is really a precursor to Phase 2, Phase 3 is a precursor to later implementation phases. The technology in place at the end of Phase 3 should support a wide range of future phases including multi-agency or control. These agencies may be multi-national. It is realized that the coordination and human aspects will be the biggest challenge for Phase 3. More will be said later on the possible directions that can be taken with Phase 4 and beyond.

9.4 APPLICATION DATA FLOWS AND DEVICES

The application data will always flow to and from different levels. Same-level devices will never communicate Application Layer data with each other within the SCINetEx system. Same-level devices may, of course, store and/or forward secured or unsecured data from same-level devices as needed for delivery, but will never process that data. The Level 1 facilities may share data as they see fit, but the means of doing so will be considered out of band for SCINetEx. Again, the protocols and methods designed here are for supporting resource constrained SEDs. Other methods and means are available for high functioning devices and are out of scope for this technical report, or will be included in later versions.

Similarly, KIM-to-Level 1 facility communications are not specified in this technical report. No SCINetEx application data will be communicated to the KIM. Rather, its sole purpose is to provide keys for communication. There is no need for any Level 2 or Level 3 devices to communicate with the KIM, even for key management functions. Those will be handled through a Level 1 intermediary, which makes all key management decisions. As such, the details of the inter-Level 1-to-KIM communications are out of scope for this technical report. However, this text does specify the details of the message formats that need to be delivered to the Level 1 facilities so they may forward key management data into the network.

For this technical report, we introduce the notion of an “extended ID”. For security to be meaningful each network device must have its own, unique ID. However, this is not sufficient, as other devices must be able to understand what type of device they are communicating with. So in addition to a globally unique ID field (UID) each UID must be augmented with device type. Together the following information makes up the extended ID of a device.

- DeviceType(1 byte)
- UID(8 bytes)

From the extended ID perspective one may view this extra information as part of the device’s ID. However, it need not be a contiguous set of bits in the device ID as found within a network message. The receiving device just needs to be able to glean the information from the message in a standardized fashion.

9.5 KEY TYPES

In this key management system there are four types of keys:

- RekeyKey(RK)
- LongTermKey(LTK)
- Temporary Communication Key (TCK)
- StorageKey(SK)

Associated with each of the first three keys is a pair of ascension numbers, which are to account for the number of times that a key has been used. In order to simplify the key management as much as possible, we assume each Level 2 and Level 3 device must be given one key upon manufacture: a RK. The Level 1 facilities do not need their own RKs (or LTKs) as specified here. When a Level 2 or Level 3 device is made:

- The manufacturer must insert the RK into the device. That key must be randomly chosen with the highest quality generation system. This process and the storage and archival of all keys must be protected, at the highest levels. The ascension number for the RK must be set to zero (0).
- The manufacturer must securely communicate the RK together with the extended device ID to the KIM. The manufacturer should delete their record of the RK after reception at the KIM has been confirmed.
- The manufacturer must NOT communicate the RK to any entity other than the KIM.

The Temporary Communication Keys are special keys derived from the LTK and given to the Level 1 and Level 2 devices to communicate with Level 3 devices. In the case of Level 2 to Level 3 communication, the TCKs are designed to help control the scope of a compromise.

9.5.1 The Rekey Key (RK)

The RK is intended to facilitate the delivery of the LTK, to assist in the recovery from compromise and assist in general maintenance of the LTK. Its use in the system is completely restricted and is used to derive a key, which is used only to change the LTK. Only the KIM and the device will have access to the device's RK. The device must not be able to communicate the RK. The RK is essentially hardcoded into the trusted hardware in the device. Any changes to the RK must require physical possession of the device and requires a depot-level effort to change. Because this key has the ability to change the LTK, it is imperative that the RK be tightly controlled.

To be viable in the system, Level 2 and Level 3 devices must support a number of key management messages, including the ability to use the RK to process the replacement of the LTK.

9.5.2 The Long Term Key (LTK)

The LTKs are known only by the KIM and the individual device and are changeable using the RK. When a Level 2 or Level 3 device comes from the factory it shall receive a new LTK before (or as) it enters service. Even if the device comes from the factory with a pre-installed LTK, this key must not be used as part of the SCINetEx system and must be changed first. To prevent replay of the LTK update messages, the LTK must also have a four-byte counter indicating the number of times it has been changed. The factory preset counter will be zero (0). The device must not be allowed to process secure data until the LTK has been changed. The device receiving a Rekey message will inspect the four-byte rekey counter in the message and compare with its internal counter; if the counter in the message received is not greater than the internal count value, the message will be ignored.

Details of the Rekey messages are given below. If the rekey counter reaches its maximum value, the device will not accept a new key via the electronic rekey mechanism. It should continue to function, but it will take a depot-level refurbishment to change the RK, reset the counter and be able to change the LTK. There are a couple of options for a change of the LTK, in particular the initial rekey.

- The network device does not come under the physical control of the governing entity before operation.
- The network device does come under the physical control of the governing entity before operation.

If the device does not come under the physical control of the network governing entity, (i.e., government or oversight agency) there is no way to eliminate all risk associated with the LTK update. It is a root of trust issue. The factory must know the RK that they installed in the device and must communicate that key to the KIM. Even though the factory should delete the record of the RK, it cannot be guaranteed that they will. Policies and procedures outside the scope of this technical report must be implemented to reduce this risk to an acceptable level.

The security of the LTK is determined by access to the LTK update messages and knowledge of the RK. If the update message flow is not accessible or the RK is not known, the update of the LTK will be secure. If the factory (or other entity that has acquired the RK by some means) is able to capture the update messages, it will be able to divine the new LTK. Having physical control of the device and

updating the LTK in a secure location is the only way to ensure the new LTK cannot be divined by an outsider.

On the other hand, expecting one entity to physically handle every network device before it goes into operation is not reasonable. Similarly, having the device removed from service and sent to a trusted facility to update the LTK upon every suspected compromise may also be unreasonable. Such would incur tremendous expense for both vendor and user of the device.

Once the keys are created and installed, the vendor must securely transfer the two keys and the extended device ID to the KIM. It is expected that as part of fielding the device, the final commercial owner of the device will initiate an exchange between the Level 1 facility and the device.

The Level 1 facility will initiate the rekey mechanism with the KIM. No fielded device will communicate directly with the KIM. The KIM will electronically update the LTK by forwarding a Rekey message through the Level 1 facility. Again, there is some residual risk but the alternative is to have all network devices be physically funneled through a single facility.

It may be that certain high-value Level 2 devices may warrant the expense of depot-level update of the LTK, while other less valuable devices do not.

9.5.3 The Temporary Communication Key (TCK)

Each pair of communicating devices must have a key unique to that pair of devices with which that pair of devices may communicate. The Temporary Communication Key (TCK) is a key derived from an LTK. There are three types of TCKs. The three types are derived in a slightly different fashion.

- Level 0 TCKs are derived from the RK and used only to rekey Level 2 and Level 3 devices. These come in two varieties: TCK_0_2 (Level 2 rekey events) and TCK_0_3 (Level 3 rekey events).
- Level 1 TCKs come in two varieties: TCK_1_2 (Level 1-to-Level 2 communications) and TCK_1_3 (Level 1-to-Level 3 communications).
- Level 2 TCKs come in only one variety: TCK_2_3 (Level 2-to-Level 3 communications).

The method of derivation is different for the three types and is explained below. When a Level 1 facility needs to communicate with a Level 2 or Level 3 device for the first time, the Level 1 facility will communicate with the KIM to receive the appropriate Level 1 TCK, which is a function of the Level 1 extended ID and the LTK of the device. When a Level 2 device needs to communicate with a Level 3 device, the Level 2 device receives the appropriate Level 2 TCK from the Level 1 facility. That key is a function of a number of things including the extended ID of the Level 2 device, the extended ID of the parent Level 1 facility and the LTK of the Level 3 device.

The Level 1 facilities are not given the LTK of any device and thus cannot compute Level 1 TCKs. They must be supplied by the KIM. However, given the appropriate identification information, the Level 2 or Level 3 devices are able to derive the Level 1 TCK they will use with the Level 1 facility. This derivation removes the need for a key exchange with the SEDs. The Level 1 TCKs act as seeds for the Level 2 TCKs and so a Level 1 facility is able to derive the Level 2 TCKs without having to communicate with the KIM. The Level 2 device is not able to derive the Level 2 TCK, it must receive it from its parent Level 1 facility. As with the Level 1 TCKs the SEDs are able to derive the Level 2 TCKs, removing the need for a key exchange with the resource constrained device.

9.5.4 The Storage Key (SK)

There are requirements that stored data be protected. In the case of Level 3 and Level 2 devices that protection includes encryption and authentication of the stored data. The complete list of protection mechanisms that must be in place are architecture-dependent and cannot be spelled out in every detail, up front. This technical report provides a key generation method a vendor may use to protect the data in storage. The Storage Key (SK) is derived from the LTK as are the Level 1 TCKs. It may be viewed, for instance, as a Level 3 TCK.

Since the protection of stored data is not an interoperability issue, there is some flexibility in how the data may be protected. For instance, if a Level 3 device intends to send a Status message to a Level 1 facility, the Level 3 device may secure the Status message with the TCK it shares with that facility and store the entire message as it would be sent to the Level 1 facility. If properly done, the Level 3 device would not necessarily need to encrypt and authenticate the message again with the Storage Key. Another option may be something akin to whole disk encryption, where a key independent of all other keys is installed at manufacture; this protected key is persistent and used for the sole purpose of managing and securing the data at rest.

It is important that keys be used in the way intended and that mixed usages not take place. The RK, LTK and the TCKs described thus far shall not be used for the general storage of data. Those keys have a predefined purpose and usage. The only exception is that noted above, when a message is properly secured with the proper key and placed in storage for future delivery. In that case, the key is being used as it was intended. Conversely, the SK shall not be used to protect any transmitted data. In all cases, it is up to the device vendor to show that their method of protection does indeed protect the stored data in the context of their architecture.

9.6 DEVICES AND KEYS

This section is a look at each level in the system as depicted in Figure 9-1 and the keys each device will use for its communication and the types of messages that will be secured using those keys.

9.6.1 The Key Information Manager (KIM)

The KIM is a single entity that contains all of the keys in the SCINetEx system. If it is compromised, the entire network will be compromised. Recovery will be difficult and costly. To help limit the possibility of a compromise, the communications with the KIM must be tightly restricted and controlled. The KIM will communicate only with Level 1 governing entity facilities via a secured communications network.

- The KIM will hold all of the RKs for every device.
- The KIM will hold all of the current LTKs and the rekey counters for every device.
- The KIM may be fully autonomous utilizing artificial intelligence.

During an LTK update, the KIM communicates directly only with Level 1 devices.

- If a Level 2 or Level 3 device requires its LTK changed, the KIM will randomly select a new LTK for the device and secure the update messages with the Level 0 TCK associated with the device. Embedded in this Rekey message will be the rekey counter. In the device, the rekey counter is set to zero (0) at manufacture time. The first Rekey message created by the KIM will have a counter value set to one (1) and increment each time a new Rekey message is created.

- The Level 2 or Level 3 device must not communicate directly with the KIM, so the update messages must involve a Level 1 device. The update LTK message will be securely passed to the Level 1 facility who forwards that message to the Level 3 device.

It is assumed that changing an LTK is a significant event in the life of a device and will not happen as a daily occurrence. The trigger for LTK update is TBD and will be defined by a user-coordinated policy. For Level 3 devices, it is likely that most rekey events will be in conjunction with installation, in response to the action of an adversary or with battery change. Even though it is assumed that LTKs will be changed minimally a few times a year, this management scheme will support more frequent changes, to a maximum of 232 rekey events before a depot-level refurbishment is required. Rekey events do impose a burden on the system. Sufficient infrastructure must be in place to handle whatever key change frequency is decided upon.

9.6.2 Level 1 Facilities

The Level 1 facility serves as the central repository for data and information and, in a sense, initiates all the command and control in the SCINetEx system. These facilities exercise global control over all of the SEDs within their purview. They also control a certain collection of Level 2 facilities/devices. If a Level 1 facility is compromised, this constitutes a major violation of the network. So, the Level 1 entities must be highly fortified. The derivation process for the Level 1 TCKs is such that there is key separation between Level 1 facilities.

- The Level 1 facilities will NOT possess the RK or LTK of any device.
- The Level 1 facilities may communicate with the KIM as described above.
- The Level 1 facilities may possess the Level 1 TCK of any Level 2 or Level 3 device it needs to communicate with. These are obtained via a request to the KIM.
- The Level 1 facilities may derive and send Level 2 TCKs to the Level 2 devices so that the Level 2 device may communicate with the Level 3 devices.
- The Level 1 facilities must not give a TCK belonging to one Level 2 device to another Level 2 device.
- The Level 1 facilities may communicate directly with Level 2 and Level 3 devices to exchange Application Layer data and/or issue commands.

9.6.3 Level 2 Devices

As mentioned previously, Level 2 devices may actually be facilities rather than a single device. It may be that at a particular location there is a collection of devices that operate together to facilitate security. In that case, a facility at that location may operate as a single unit and exercise significant control over the SEDs within that location, but may not need to have global privileges. In any event, we call these facilities devices, for convenience. It is intended that Level 2 devices be tied to a particular Level 1 facility. As mentioned above, a Level 2 device may store a number of Level 2 TCKs in order to communicate with the various Level 3 devices it must communicate with. The less-than-secure environments in which these devices must operate necessitate more care when deriving keys. Thus each key is not created by the Level 2 devices.

Using its RK:

- Level 2 devices will receive and decode LTK Rekey messages from the KIM through a Level 1 facility as described above.
- Level 2 devices will never have the RK or LTK of any other device.

Using its Level 1 TCK:

- Level 2 devices may communicate with the Level 1 facilities to request and receive Level 2 TCKs.
- Level 2 devices may communicate with the Level 1 facilities to exchange Application Layer data and/or receive commands.
- Level 2 devices may communicate with the Level 1 facilities to forward Application Layer data from the Level 3 devices.

The Level 2 device must communicate its extended ID to the Level 3 devices it wishes to communicate with. It must also communicate its parent Level 1 extended ID to the Level 3 device.

Using a Level 2 TCK:

- Level 2 devices may communicate with the Level 3 devices to exchange Application Layer data and/or issue commands as allowed by Level 2 device type.

9.6.4 Level 3 Devices

The Level 3 devices are envisioned to be SEDs, possibly battery powered and resource constrained. The only keys that they should have are their own RK and LTK. The key management scheme designed here is such that, except for a rekey event, keys do not need to be pushed down to the Level 3 devices. As there will likely be tens of millions of SEDs, it was decided that doing traditional key exchanges would not be reasonable or possible. Thus this system removes the need for key exchange. Keys are derived from identification information that may be broadcast to the Level 3 devices. As mentioned above, for efficiency sake, a Level 3 device may compute and store a TCK that is required to communicate with a Level 1 or Level 2 device. At some point, Level 3 devices must acquire the extended IDs of the devices to which they are going to send messages.

Using its RK:

- Level 3 devices will process the Rekey message from the KIM through a Level 1 facility as described above only to receive a new LTK.
- Level 3 devices will never have the RK or LTK of any other device.

Using a Level 1 TCK:

- Level 3 devices may communicate with the Level 1 facilities to exchange Application Layer data and/or receive commands.

Using a Level 2 TCK:

- Level 3 devices may communicate with the Level 2 devices to exchange Application Layer data and/or receive commands as allowed by Level 2 device type.

9.7 KEY CHANGE PERIOD

If two entities share a 128-bit or greater key, which is used properly with strong cryptographic functions and parameters, then that key should be sufficient from a data protection stand point for the lifetime of the device. The described system should have a relatively low data rate and a single device will not ever transmit enough messages to any other single device to pose a cryptographic threat to any particular key. There are opposing requirements for the length of the crypto-period; each time there is a key change there is an opening into the key management system that does not otherwise exist. The key change mechanism may be exposed. Also there are risks and requirements with auditing and archiving old keys, and keeping the system synchronized. From a purely functional point-of-view, getting the system into a state where all entities know which keys to use may be difficult if the crypto-period is too small or if the key change happens when the devices are not all connected.

If the RK is used only between the KIM and the end device and is used only to update the LTK, then the RK may serve for the lifetime of the device, provided no known compromise has occurred and its use is properly accounted for. As mentioned in Section 9.2, Level 3 devices may be battery powered, that those batteries will deplete, and will be changed as the asset mounted SED is being prepared for use. The keys and ascension numbers may or may not be stored in non-volatile memory, depending on the device.

The RK and the rekey counter MUST be placed in non-volatile memory or otherwise hard-coded into the device. These must survive loss of power or any other fault that may cause normal memory functions to be lost. If the RK is lost, the device cannot be rekeyed outside of a depot-level environment.

There is a security threat associated with the reuse of ascension numbers. Since the TCKs are derived from the LTK, they may be derived independent of previous use. If any key or its ascension number is placed in volatile memory, then a security concern opens up if it is derived anew after loss of power and the ascension number is reused. It is not enough to store the LTK in non-volatile memory, but not the TCKs and ascension numbers. If a device is designed such that its ascension numbers and/or associated keys are stored in volatile memory, then a rekey of the LTK is required after power is restored and the device is brought back into service.

The SK is derived from the LTK and thus should be at least as volatile as the LTK. So if the SK is used to protect the data at rest and the LTK is changed, it is assumed that the stored data would be flushed and a new SK derived. In the low data rate environments for which this system is designed, one should never expect to see enough encrypted traffic to pose a cryptographic threat to the data and means of security. So, if the keys and ascension numbers are properly accounted for during usage and after battery changes, there is no cryptographic threat due to data overuse of a particular key requiring an LTK change. The primary concern and direction of threats come from repeat of ascension numbers with a particular key.

Given proper accounting of keys and ascension numbers, the crypto-period is set as a matter of policy. Policy should be set in a way that is convenient for the operation of the network. Too frequent changes would place a burden on the infrastructure. Whereas insisting that the crypto-period be longer than battery lifetime (if battery powered) would put an undue burden on the vendors to create devices able to hold significant amounts of state information during the process of power loss. (This does not preclude them from doing so.) In either case, the infrastructure must be able to support the decided upon crypto-period.

9.8 MULTI-USER KEY MANAGEMENT

This section focuses primarily on the requirements for communication from a single entity/owner perspective. However, the reality is that there may be two types of data: owner-purposed and guest-purposed. An owner of the device may well desire to have the device, if it is capable, relay commercially valuable data to the owner. This owner's data may be secured as the data owner sees fit. However, for security reasons the guest data and owner data, especially the secure data, any keys and secure computations must not comeingle. Any device that processes both owner and guest data must be split into two halves: an owner and a guest half. Ideally each half will be both physically and logically separate. However, the various devices must be commercially viable and so true separation of all things owner and guest may not be possible.

The locations in memory where the keys and sensitive owner data are stored should be physically separate. In the case of logical separations of computations and other data processing and the like, the device should not comeingle owner and guest data.

After the outbound data has been parsed and secured as needed in the appropriate half, it must proceed into more common physical ground and be shipped out through a potentially common interface. Upon reception, the common interface must be able to distinguish between the owner and guest data and present said data to the appropriate hardware. A field in the message header will be sufficient. This also means that when a device is created it may be installed with keys in addition to the owner RK and LTK. When a guest entity purchases a device, the vendor will supply that device's pre-installed commercial-side keys to the guest entity. Those keys are managed and used as the guest owner chooses, provided the commingling constraints mentioned above are observed.

If it chooses to secure its communications, the guest owner of the device may construct and manage its own key management system as it so chooses. The guest owner is free to mimic the key management system described here-in. Vendors may provide the same key management operations and security options on the guest side for use by the guest entities that are available for the owner's use on the owner's side. Vendors must ensure that there are no correlations between any of the owner-side keys and the guest-side keys.

9.9 IMPLEMENTATION

Information assurance is performed at the Application Layer. The intent is that the information assurance be independent of the delivery so as to increase the flexibility in the delivery of the SCINetEx system messages. System devices contain encryption, authentication, message integrity checks and anti-spoof mechanisms that are:

- Compliant with the most stringent information protection policies among international locales.
- Independent of all delivery media between the devices. This may include any number of inter-working data transport networks.

9.10 PACKET INFORMATION

All SCINetEx network packets destined to or originated from a SED have a maximum size of 100 bytes in length. This size is to fit within a single IEEE Standard 802.15.4-2006 data frame. The cryptographic methods described here are not limited by that size, though a different packet header would have to be chosen and details refined.

9.10.1 Packet Header and MIC

The following values and sizes comprise the message header of an Application Layer packet.

- Devicetype(1 byte)
- Message type(1 byte)
- Message length, including MIC(1 byte)
- Device UID(8 bytes)
- SCINetEx rev number(1 byte)
- Message ascension number (4 bytes)

Device type, Device UID and SCINetEx rev, must all be of the sender. The message integrity check (MIC) is appended to every secured packet. Normal messages have a MIC of 8 bytes. The Rekey messages have a MIC of 16 bytes.

NOTE: The use of “MIC” is non-standard as cryptographic terminology; rather message authentication code (MAC) is more common. However, other sections of this technical report that discuss media access control uses MAC for that purpose and so use MIC to avoid naming confusion.

9.10.2 Device Type

The following device types, listed in Table 9-1 are to be used for the KIM and Level 1 facilities.

Table 9-1. Device Types.

Description	Device Type
0x89	KIM
0x88	Level 1

9.10.3 Key Management Message Types

The following is a minimal set of message types that are needed to support key management for the various implementation phases described. For each of the messages a message type must be reserved. Key management message types are outlined in Table 9-2.

KIM to Level 2 or Level 3 device:

- KIM rekey of LTK of Level 2 or Level 3 device messages will be secured by Level 0 TCK of the target device and given to the Level 1 facility for delivery. Message type value is given below.

Level 2:

- Level 2 to Level 1, request for Level 2 TCK_2_3. Message type value is to be determined by the system implementer.
- Level 2 to Level 3, Point-to-Point/Introduction message containing Level 2 device type, UID and Parent Level 1 facility extended ID information (unsecured). Message type value and format is to be determined by the system implementer.

- Level 2 to Level 3, Broadcast Introduction message containing Level 2 device type, UID and Parent Level 1 facility extended ID information (unsecured). For SCINetEx this is the NGA message type 0xFF.

Table 9-2. Key Management Message Types.

Message Type	Description
0xE0	Rekey message
0xE1-0xE9	Reserved for Key Management

9.10.4 Device UID

The KIM UID is to be determined by the system implementer; that is to say before any SCINetEx network becomes viable operationally, this UID will need to be chosen appropriately. When the KIM UID is chosen, all devices in the network need to know that UID. Similarly, the Level 1 facilities are not really devices and the process of obtaining a UID may be different from the process a Level 2 or Level 3 device might go through. However, the UID need not/probably should not be hardcoded in a Level 2 or Level 3 device. If a Level 1 facility UID is hardcoded in the device, then in later implementation phases, there should be an option for the device accepting another UID for another Level 1 facility.

9.10.5 Message Ascension Number

The message ascension numbers are tied tightly to a key. Each device must maintain a send and receive ascension number. Each time a message is sent to a destination using a particular key, the sending device must increment its send ascension number. Each time a message is received and authenticated with an ascension number greater than the receive ascension number for a particular key, the receive ascension number shall be set to the received value. When a packet is received with an ascension number lower than or equal to the current stored (receive) number, the packet is not cryptographically processed and should be discarded. If a packet is received, but the message does not pass the authentication test, the receive ascension number must not be changed. Similarly, if a device is able to receive valid, but unsecured messages from a particular device, the receive ascension number should not be incremented. For instance, one device broadcasts a message that has not been encrypted nor does it have an authentication value. The receiver may view the message as valid, but must not increment the receive ascension number.

When an ascension number reaches the largest value, the LTK must be changed, or communications with the given TCK must be ceased. Repeat of an ascension number with the same key with a different message is a security violation and is not allowed. Of course, if done within specification, repeat or retransmission of the exact same secured message with the same key and ascension number as required for delivery (such as for error correction) is not a security violation, but shall not increment the send ascension number. If the LTK is changed, all old TCKs should be discarded along with their ascension numbers. (This does not mean that if an old key is re-derived its ascension number should be reset. On the contrary, care must be had to ensure that re-derivation of the same key does not include resetting of previous ascension numbers; they must continue to increment.)

The exception to these rules is the ascension number associated with RK. A SED must never transmit with the RK. It should maintain only a receive ascension number. For clarity we call this the rekey counter. Initially this value is set to zero (0). The KIM maintains the RK rekey counter as the number of Rekey message keys sent including the current message, thus the first time a rekey event occurs the value should be one (1) and so on. The discussion in this section has focused on the treatment of the ascension numbers. Actual communication protocols will certainly be more complicated than that described here. This discussion is not meant to limit the possibility of various responses that might be required for delivery and functionality, such as retries, error correction, etc. Rather, each device should follow functional requirements levied upon it, subject to the usage of the ascension numbers described here-in.

9.11 KEY DERIVATION

Key derivation will use one or more blocks depending on encryption algorithm. In the following examples, using cypher text message in 128 AES Standard codebook form, this would be $C = \text{AES}(K, M)$ indicating block M encrypted with key K. There is no restriction in SCINetEx on the type or level of encryption used.

9.11.1 The Rekey Key

The Long Term Key (LTK) Rekey message is secured slightly differently than all other messages in SCINetEx. The key used to secure the Rekey message is the Temporary Communication Key (TCK) derived from the RK.

- Let H_{RM} be the entire 16-byte header of the Rekey message. That is,

$H_{RM} = (\text{KIM device type, Rekey message type, Rekey message length, KIM UID, version number, rekey counter}) = (0x89, 0xE0, 0x20, \text{KIM_UID, version number, rekey counter})$

- Let RK_2 and RK_3 be the Rekey key of Level 2 and Level 3 device, respectively.

For the Level 0 TCKs, the RKs respectively are:

$TCK_{0_2} = \text{AES}(RK_2, H_{RM})$

$TCK_{0_3} = \text{AES}(RK_3, H_{RM})$

These are used solely for updating the LTK. Because of its special role, a special name is given to it.

NOTE: that only the KIM and the intended Level 2 or Level 3 device can compute this value.

9.11.2 Level 1 Temporary Communication Key

The Level 1 Temporary Communication Key (Level 1 TCK) is used to secure communications between a Level 1 device and a Level 2 or Level 3 device and is derived from the Long Term Key (LTK) and certain identification information.

NOTE: The target Level 2 or Level 3 device can derive this value. However, the Level 1 facility cannot. Rather, the Level 1 facility must receive the Level 1 TCK from the KIM.

- Let n_ZB be a sequence of n bytes containing the value zero.
- Let $P1 = (\text{Device type of Level 1 facility, } 2_ZB, \text{Level 1 facility UID, } 5_ZB)$.
- Let LTK_2, LTK_3 be the LTK for the Level 2 or Level 3 device, respectively.

The derived Level 1 TCK between a Level 1 facility and a Level 2 and Level 3 device, respectively are:

$$\text{TCK}_{1_2} = \text{AES}(\text{LTK}_{2}, \text{P1})$$

$$\text{TCK}_{1_3} = \text{AES}(\text{LTK}_{3}, \text{P1})$$

NOTE: P1 is 16 bytes in length. It is equivalent to the message header from a Level 1 facility with all but device type and UID set to zero (0). This allows the Level 1 TCK to be derived by the target device without any prior communications. Recall that the Level 1 facility must receive these keys from the KIM.

9.11.3 Level 2 Temporary Communication Key

The Level 2 Temporary Communication Key (Level 2 TCK) used to secure communications between a Level 2 device and a Level 3 device is derived by a Level 1 facility and given to a Level 2 device. The intent is that the Level 2 devices answer to a Level 1 facility and their privileges in the network are tied to that facility.

- Let n_ZB be a sequence of n bytes containing the value zero (0).
- Let TCK_{1_3} be the Level 1 TCK between the Level 1 and the Level 3 device.
- Let K be the bitwise complement of TCK_{1_3} .
- Let $\text{P2} = (\text{Device type of Level 2 device}, 2_ZB, \text{Level 2 device UID}, 5_ZB)$.

The derived TCK between a Level 2 device and a Level 3 device:

$$\text{TCK}_{2_3} = \text{AES}(K, \text{P2})$$

NOTE: P2 is 16 bytes in length. It is equivalent to the message header from a Level 2 facility with all but device type and UID set to zero (0).

The Level 3 device can derive this key provided it is given the correct Level 1 and Level 2 identification information. If the Level 3 device has previously computed the TCK_{1_3} then this requires a single encryption. If the Level 3 device will communicate with several Level 2 devices associated with a single parent Level 1 facility, the same TCK_{1_3} is used to derive the various TCK_{2_3} s.

9.11.4 The Storage Key

The derivation process for the Storage Key (SK) is the same process used to derive the Level 1 Temporary Communication Keys discussed in Section 9.11.2. The SK is used solely for protecting stored data and shall not be used to protect transmitted messages. As the SK is intended to protect the data within a particular Level 2 or Level 3 device:

- Let LTK be the LTK of the given Level 2 or Level 3 device.
- Let Device_Type be the device type of the given Level 2 or Level 3 device.
- Let Device_UID be the UID of the given Level 2 or Level 3 device.
- Let n_ZB be n zero bytes.
- Let $\text{P3} = (\text{Device_Type}, 2_ZB, \text{Device_UID}, 5_ZB)$.

The derived Storage Key is then:

$$\text{SK} = \text{AES}(\text{LTK}, \text{P3})$$

NOTE: P3 is 16 bytes in length. It is derived in the same fashion as the Level 1 TCKs. So, given that the device has an LTK, it will always be able to derive its own SK.

9.12 MESSAGE ENCRYPTION AND AUTHENTICATION

Depending on what type of device a message is sent from and intended for, one of the three key types, the Level 0 TCK, the Level 1 TCK or the Level 2 TCK, is used to secure a message. All encryption and authentication of messages in the SCINetEx system will be via the authenticated encryption scheme and encryption module. There are two types of secured messages: the Rekey message and all others. The two types have a similar nonce description. However, the Rekey message has a 160-byte authentication value whereas all other messages have an 8-byte authentication value. The requirements are such that there is to be no co-mingling of owner data and guest data and that keys and data will be protected at all times. IEEE Standard 802.15.4 devices have a built-in mechanism to do encryption. Unless special precautions are made, having the IEEE Standard 802.15.4 device provide the security for both the owner and guest data would be a violation of one or the other of these requirements.

9.12.1 The Rekey Message

- The 8-byte nonce for encryption is the Rekey message header with the 8-byte KIM UID removed.
 - KIM Device type = 0x89
 - Rekey message type = 0xE0
 - Message length, including MIC = 0x20
 - SCINetEx rev number (1 byte)
 - Message ascension number (rekey counter) (4 bytes)
- The encryption key will be the Level 0 TCK defined in Section 9.11.1.
- Cypher Block Chaining Message Authentication Code (CCM) starting with the first byte after the 16-byte message header and applied to a message 16 bytes long (one AES block).
- The 16-byte payload shall be the new 16-byte LTK randomly chosen by the KIM.
- The authentication SED will be 16 bytes in length.
- All fields have specific specified values. Each of those must be checked for consistency before the CCM message nonce is created or the message processed.

A valid Rekey message initializes/replaces the LTK. When the LTK is changed, any TCK derived from the previous LTK must not be used again. Thus the previously derived TCKs should be purged along with their send and receive ascension numbers. The ID information stored in the device may be retained to streamline exchanges needed to get communicating devices synchronized again.

9.12.2 All Other Messages

- The 8-byte nonce for all other non-secure (see Section 9.2) messages is the message header with the UID removed.
 - Device type (1 byte)
 - Message type (1 byte)
 - Message length, including MIC (1 byte)
 - SCINetEx rev number (1 byte)
 - Message ascension number (4 bytes)
- The encryption key will be the Level 1 or Level 2 TCK defined in Section 9.11.
- CCM will be applied starting with the first byte after the 16-byte message header.
- CCM authentication tag will be 8 bytes in length.

9.12.3 Future Message Types

The message and header structures given in this technical report are geared toward supporting messages to or from SEDs. As of the writing of the current version of SCINetEx, the requirements documents and Concept of Operations (CONOPS) for KIM or Level 1 facilities were not available. Similarly, there is active ongoing discussion concerning function and form of Level 2 entities. Level 3 devices are more mature, the message structures are defined and products are being developed. The key derivation described above is sufficient to support a wide range of eventualities. The message types will naturally change and expand as the SCINetEx construct evolves. In particular the changes in the header definitions and development of the nonce for encryption will likely expand as the Level 1↔Level 2 communications are refined.

Level 1 and Level 2 facilities are less resource constrained. As such, different methods of cryptography are available for securing those devices and communications. The definitions and technologies introduced in this technical report are not intended to limit or restrict technologies more appropriate to the communication types available to more functional devices. Rather the intent is that it will expand and change as different portions of the SCINetEx construct develops.

9.12.4 Data Storage

As described previously, vendors may define to a large degree the methods for which they protect stored data. This section is not intended to limit device architectures or insist on protection methods that must be dependent on the architecture. However, it provides for a key derivation and insists that proper key usages be strictly enforced. Again, the burden of proof to show a storage method (and architecture) to protect the secure owner data is on the burden of the vendor.

9.13 FURTHER DISCUSSIONS ON EXTENSIBILITY

In the first four implementation phases of this encryption management scheme, there is one KIM for all users in the global hierarchy. It has also been implicitly assumed that one entity will build and manage the KIM, and that all key management functions (generation, distribution, revocation, etc.) are controlled by that entity. Although a likely tractable solution for the near term as a first step, it is not viable in the long term taking into account the multi-national nature of the global operations. Here we discuss in more detail the reasoning behind the phased approach to implementation.

With cryptographic security measures, security is defined in a large part by control of keys. The more limited their use and the more tightly they are controlled the more likely a system may be secure. On the other hand, the more entities with control of the keys the more chances that there will be violations in the security policies surrounding the keys. This is especially true if the controlling entities have equal say in what should be done, but have differing opinion about what should be done.

In the end, this is the biggest challenge in thinking about multi-organizational or multi-national control of any one SCINetEx system network. Understandably, participating users will desire to do things their own way, which may be different than any other and may not match up from a security perspective. This problem is age old and has no known purely technical solution. Rather a regulatory or governance solution is required.

9.14 LATER SED IMPLEMENTATION

Phases 1, 2 and 3 are intended to provide a solid operational footing so that bugs can be worked out, products produced and experience gained. Later phases include multi-organizational or multi-national control. Phase 2 includes Level 2 devices that may be on foreign soil, but are under the control of the single Level 1 facility. The Phase 3 design includes multiple Level 1 facilities, each having significant control within the network. These are assumed to be fully trusted and work in complete cooperation with the initial controlling entity, or that the facilities represent independent agencies within a single entity. Phase 4 loosens these assumptions to assume that a transition has occurred to allow a Level 1 facility that may be owned and operated by an entity that may do or see things differently than the governing entity envisions. However, the deviation is assumed to still be manageable.

The Level 1 facilities exercise significant control in the network. If they do not cooperate fully, then the network's usefulness may be questionable. Thus, for Phase 4 to be viable there may need to be a significant level of trust between the controlling entity and the owner of a Level 1 facility. Likely treaties and agreements would need to be put in place to ensure smooth and seamless operations of the network. Level 1 facilities are able to commission Level 2 facilities and devices. They are able to act essentially in an autonomous fashion. Thus that assumes that their actions must be acceptable within the overall network.

With true multi-organizational control, SEDs potentially travel the globe. They may move from country X to country Y and back again. Each country may not exactly trust each other to behave properly. Here, if full cooperation between Level 1 facilities is not possible we introduce the notion of a destination authority.

When a SED is brought into service, it is rekeyed. The Rekey event is tied to a particular Level 1 facility or destination authority. The destination authority is then solely responsible for the operation of the SED, until the device reaches its destination and is released for use. Agreement is made to make sure the KIM does not distribute keys to other Level 1 facilities, unless permission is granted by the destination authority. The destination authority may grant whatever access it deems necessary for operation. When use is completed, the destination authority releases hold of the SED so that some other country or Level 1 facility may become the next destination authority and rekey the device.

The Level 1 design is that once a Level 1 facility receives a Level 1 TCK it need not communicate with the KIM until some serious event has occurred. So, the workload may be manageable for the single entity-controlled KIM. There may also be a case where entity X may not completely trust the entity Y KIM. Later phases for key implementation may be a significant departure from the previous phases in that the notion of the KIM would change. It is unclear at this point what would be best. Two

possible choices include moving control KIM to super-entity control or to allow another entity to stand up its own KIM. The former would likely necessitate use of artificial intelligence.

For the second option to be viable, the RKs and the LTKs of the various devices in the network (or some portion of them) would need to be transferred to potentially a super-KIM. This would need to be carefully considered. Once the RKs and LTK are given to another entity, control of the network is lost. The super-KIM would have to be a partner in every sense of the word and communications about key management operations would have to flow between the two entities as is needed to manage the SCINetEx system.

The current models of security rely on very tightly controlled trust. In a truly global paradigm trust is always an issue. Full-fledged partners may not be possible, nor may single entity multi-national control of the KIM be possible. The current design paradigm is constrained by the resources available to the SEDs. For instance, at the time of writing this version of SCINetEx, public key technologies are simply not an option for battery-powered devices. Sometime in the future, this may change. Similarly, future communications protocols refinements may have the bandwidth to support key exchanges and the like.

Public key paradigm solves many issues associated with symmetric key management, but it does require a Public Key Infrastructure (PKI) to be implemented. There are attempts at making a viable PKI, but those have been at a very large cost in time and money. Even after implementation, a PKI is not trivial to maintain. Because of the flexibility of the public key paradigm, more odd situations can occur and so more policies and procedures must be in place to manage the eventualities. In the end, trust is moved to a new place and must be more actively managed. This is a technological effort to address the lack of trust between organizations, but it cannot really solve such a problem.

The technology changes that need to take place in order for a public key transition to take place may be disruptive or at least incompatible to rudimentary devices such as those described in this technical report. At this point, the way forward with PKI in the SCINetEx system can be planned for to some extent. For instance, the communications protocols should account for the eventual messaging needed to support PKI. This means that there must be some reserved fields and room in the protocol to support changes. In any event, evolution in the resources available to SEDs would allow a shift of the key management technologies available and so on.

9.15 TRUSTED CIRCUITS AND COMPONENTS

No discussion of information assurance and cyber security would be complete without a discussion of the hardware itself. All components of the SCINetEx system are built from integrated circuits. Since the 1990s nearly all of the commercial integrated circuit fabrication has transitioned to facilities owned and operated by foreign entities at overseas locations for cost reasons. Over time, these facilities have refined their methods to maximize IC circuit wafer yields at low cost and minimal feature size. It has been suspected by US agencies that foreign adversaries at these locations have been actively involved in developing the means and methods to install malicious circuitry and code directly on integrated circuit components during the fabrication process. This code and circuitry may do many things including providing access to a presumed secure device by an unauthorized user or otherwise provide the means to disrupt operation of critical infrastructure reliant on these devices for strategic or criminal purposes. Malicious actors could use this capability as a man-in-the-middle, denial of service or insider attack.

The US government and affiliated commercial interests have invested large amounts of capital to develop tools that interrogate circuitry and code nascent to ICs and packaged components to detect the presence of malevolent activities. Utilization of these tools on a large scale for commercial

products is costly and impractical. These tools are most useful to protect critical infrastructure and systems managed by government agencies. Numerous examples can be cited where counterfeit devices such as routers were detected by cyber defense staff before installation.

Methods have also been developed to mitigate the risk of malicious code or circuitry from foreign-owned fabrication facilities through split manufacture of ICs. This promises to be more cost effective for establishing IC circuit security on a large scale. The details of IC fabrication are beyond the scope of this technical report, however split manufacturing for ICs is basically a process for having the Front End Layers (FELs) of an IC wafer processed at a foreign commercial fab to maximize producibility and minimize cost, then, developing the critically sensitive Back End Layers (BELs) at a trusted facility at another location. Since most of the critical design characteristics of any integrated circuit reside on the BELs, this approach has the added benefit of protecting the intellectual property of the designer from theft at the overseas foundry.

The challenge with this approach is that it is more expensive to fabricate the Back End Layers outside the foreign-owned commercial foundry system and then transport the IC wafers to a trusted facility for completion. Unfortunately, the threat does not end there. Malicious code and circuitry can be installed anytime during the IC fabrication, packaging and component integration processes. Since IC fab, packaging and integration do not normally occur at the same location, a carefully planned secure chain of custody must also be established for transferring ICs and components between FEL/BEL foundries, trusted packaging and trusted component integration sites.

This threat is real. In 2018, the US Army removed surveillance systems manufactured by a company owned by a foreign adversary from a training installation because of the risks associated with malicious code and circuitry. About the same time, it was discovered and reported that new high speed commercial processors designed by a trusted US company and manufactured at foreign-owned foundries were shown to include hardware-level flaws that allowed malicious actors to bypass traditional software security features and access all data stored in the affected system memory. The designers of the circuitry maintain the designs are sound and the flaws were introduced during manufacture. The hardware vulnerabilities were shown to be mitigated by software patches in some cases, however the patching solution significantly slowed processor performance. These processors are widely used in cloud-computing servers which makes cloud-based systems particularly vulnerable. The only comprehensive solution is to replace those widely-used, compromised processors – a very expensive proposition. Either by accident or intent, these examples demonstrate the importance of trusted manufacture.

Section Summary

- Information assurance and cyber security for data in transit and at rest are provided by Application Layer encryption with over-the-air rekeying.
- Malicious circuitry and code are threats that can be installed at the fabrication, packaging and device integration facilities.

10. HANDHELD NETWORK GATEWAYS

This technical report has already discussed in great detail the communication protocols and formatting for messages sent and received from HNGs. However, securely integrating HNGs into any system such as SCINetEx is a complicated subject, worthy of a separate section. HNGs are generally any rechargeable handheld device such as a smart phone, tablet or otherwise ruggedized device that provides as its primary function, connectivity to SCINetEx-compliant components. The HNG is capable of providing a reduced set of Data Aggregation Point functionality to meet the requirements of the governing entity for the overall system. The HNG has a unique UID and provides periodic connectivity to a SCINetEx DAP. The HNG may incorporate some level of web service functions as desired by the device owner as long as they do not conflict with the SCINetEx protocols. The HNG communicates with the DAP via cellular service or Internet by either wireless or wired connection. Usually the wired IP connection is programmable for one or more Domain Name System (DNS) addresses of the associated DAP upon integration to the system.

The wireless communications interface of the HNG must be IEEE Standard 802.15.4 – 2006 compliant in the 2.4 GHz band to communicate with systems as described in this technical report. The radiated power output of the wireless antenna may be specified by the system owner but is usually 10 milliwatts (omni-directional) to establish a useful line-of-sight range. If the power is too low, the system owner runs the risk of being able to see the device, but cannot communicate with it. If the power is too high, the system owner runs the risk of not adequately viewing the device they intend to monitor. HNGs do not alter in any way message headers or payloads passed through it from another SCINetEx device that is intended for the DAP. The HNG can use web services to generate IP packet headers appended to SCINetEx data packets in acting as the RF/IP network bridge. The HNG generates, transmits and receives its own messages for authentication, timing, status, error reporting and maintenance purposes.

Since the HNG is capable of some of the functions of a DAP, physical security of the device and the data stored on the device is of great importance. For that reason, multi-factor authentication of the user is advised. Use of smart ID cards, user name/passwords and biometrics are effective to ensure the person using the HNG is a trusted agent. Furthermore, the system owner should specify how long encryption keys should be resident on the device, how often the device should be re-authenticated and provide a mechanism to rapidly and securely revoke certifications if needed. All encryption key management details for HNGs are discussed in Section 9.

10.1 MAKING AN HNG IEEE STANDARD 802.15.4 COMPATIBLE

A handheld Network Gateway (HNG) can be any device that is able to reach back on the network and access the DAP. However, most smart devices do not have the built-in ability to communicate via IEEE Standard 802.15.4. Because of this, it is recommended to buy or create a communications adapter that will allow you to switch from the built-in communications protocol to IEEE Standard 802.15.4.

If using a smartphone, the transition to IEEE 802.15.4 can be done in multiple ways. First, you can create a Bluetooth-to-IEEE Standard 802.15.4 adaptor. Creating this Bluetooth transparent bridge would allow the user to pass data from the phone, to the bridge, to the SED. The benefit of a Bluetooth bridge is that it can be powered by a separate battery and does not affect the phone's battery drainage rate. One of the biggest drawbacks to a Bluetooth bridge is that the user would now have to keep track of a second piece of equipment. Another option would be to have a bridge that plugs directly into the phone's micro-USB port (or other port). Unlike the Bluetooth bridge, the micro-USB bridge would have to be directly connected to the phone in order to be used. It would be very difficult to misplace it

while out in the field. The micro-USB bridge would also not be prone to wireless attacks since it connects directly to the phone. One of the biggest cons to the micro-USB bridge is that it would need to be powered by the phone, thus draining the battery on the phone significantly faster than expected. During testing, it was found that the battery life on the phone was reduced to half when using the micro-USB bridge configuration. Another con to the micro-USB bridge was that the micro-USB connector was often the main point of failure. The micro-USB bridge would often get hit/knocked during a daily routine and would have bent/broken connectors.

Using IEEE Standard 802.11 is not recommended since it can potentially be the protocol used to reach back to the Data Aggregation Point.

10.2 CHALLENGES WITH HNGS

Since HNGs are routinely used outside, environmental requirements should be considered. Temperature and humidity are usually tolerable by most smart phones but mechanical shock from drop and precipitation are always an issue. One option would be to purchase rugged smart phones or rugged cases. Another issue that often comes into play is the ability to see the screen while out in the midday sun. The cellular connection for smart phones can be a particularly useful feature for remote communications but the user should take care to ensure SCINetEx data and data from other smart phone functions are not co-mingled. It is recommended that the phone be locked from basic access to websites and apps to remove any possibility of virus accessing the device.

One of the most difficult design aspects of the HNG is ensuring that the store-and-forward capabilities do not affect the overall security. For example, let's say a SED triggers an alarm and the HNG is the first to receive the notification. The most ideal situation is that the HNG has a direct and continual link to the DAP and is able to immediately relay the alarm. However, if the HNG is set up with store-and-forward capabilities, there is a significant risk of the DAP receiving the alarm too late to provide effective security.

Another issue that causes difficulty for using HNGs is keeping track of the ascension numbering as messages are transmitted and received. In a normal scenario, the DAP, NG and SED would all keep track of the ascension numbering as messages are transmitted and received as depicted in Figure 10-1.



Figure 10-1. Standard HNG Configuration.

Issues may occur when a SED is within range or was recently within range of an FNG. In the figure below, the HNG is communicating with the SED. Both the SED and HNG will increment their counter. However, if the FNG tries to communicate before the HNG transmits an update to the DAP, both the FNG and DAP will be off in the ascension numbers as seen in Figure 10-2.

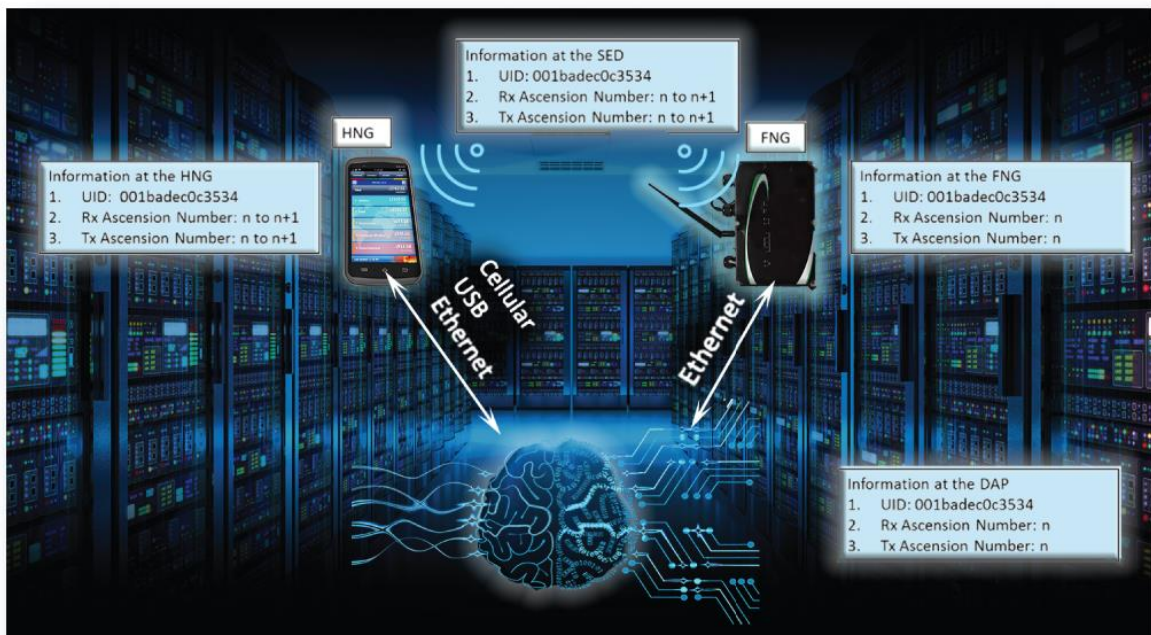


Figure 10-2. Scenario 1 – Issues with Integrating HNG, Notional UID.

Figure 10-3 is the opposite case of Figure 10-2. In Figure 10-3, the user downloads the information onto the HNG, but an FNG develops a connection to the SED before the HNG. This means that the SED, FNG and DAP would increase their ascension numbers without the HNG's knowledge. In this configuration, the smart phone is acting as an HNG with a cellular gateway – all previous considerations stated in Section 9 apply.

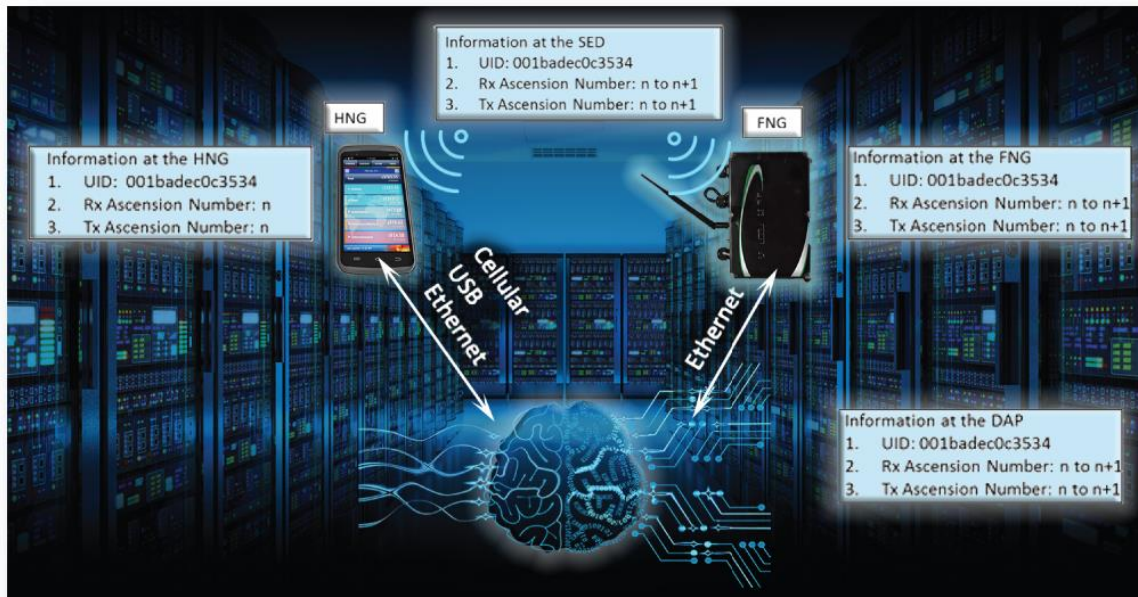


Figure 10-3. Scenario 2 – Issues with Integrating HNG, Notional UID.

Section Summary

- HNGs can be either secure or non-secure devices.
- Non-secure HNGs may be used to execute non-secure commands.
- Secure HNGs may be capable of a reduced set of DAP functions.
- When secure HNGs are connected to, or made integral to, a mobile asset, they are sometimes referred to as mobile gateways.

11. RELAYS AND ADD-ON SENSORS

Add-on Sensors (AoSs) are supported by the SCINetEx construct and may include a direct or indirect role in:

- Commands: Sensor enable/disable, arm/disarm, status inquiry
- Status change reporting
- Wired interface to a SED or CM
- Wireless interface to a SED
- Common message formats for direct-to-DAP as well as via SED/CM communications
- Common application protocol for error detection and correction

11.1 ADD-ON SENSORS VIA WIRED BUS CONNECTION

The intent here is to specify simple bi-directional wired bus message formats to best enable the use of an 8-bit microprocessor with very small code and data memory sizes. Also, the majority of the bus protocol is to be done by on-chip peripheral support. The specified bus has been used in hundreds of millions of nodes, making it robust and low cost. Therefore, Protocol Data Unit oriented protocols such as CAN Open and SAE J1939 are not specified here but can be utilized in a similar context.

11.1.1 Wired Sensor Physical Layer (PHY)

The wired sensor bus allows for use of a mature, low power, industry standard contention-based access method with collision avoidance. This is similar to CSMA/CA in other systems. The specification of the wired bus standard, below, enables low cost bus MAC Layer processing that is commonly available in contemporary low cost, low power 8-bit microprocessors. The electrical interface with the bus is expected to be via bus transceiver chips designed for power-down modes in battery-powered systems. This is necessary and practical for both shared-use and sensor-internal batteries.

The wired bus interface(s) shall comply with ISO 11898-2 with the 250Kbps maximum speed option (ISO 11519) and Controller Area Network CAN 2.0A messaging. Power for the Add-on Sensor is optionally obtained via this interface, within the limits defined below.

As shown in Figure 11-1, repeated sensors may be each independently interfaced to the wireless bus, or sensors may be subordinated to a system controller which is the sole interface to the SED for that sensor suite. The distinction may be in how modularity, redundancy and wiring is best accomplished for that sensor.

Fault Tolerance: The low speed bus operation defined here permits operation with one of the two data lines severed. Wiring may be advantageously arranged based on this.

Noise Immunity: Because the SED environment is likely to be electrically noisy, standard CAN bus information is carried on the bus as a voltage difference between the two lines. If both lines are at the same voltage, the signal is a recessive bit. If the CAN_H line is higher than the CAN_L line by 0.9V, the signal line is a dominant bit. There is no independent ground reference point for these two lines. The bus is therefore immune to any ground loop noise. Because of this, the bus better tolerates electromagnetic interference.

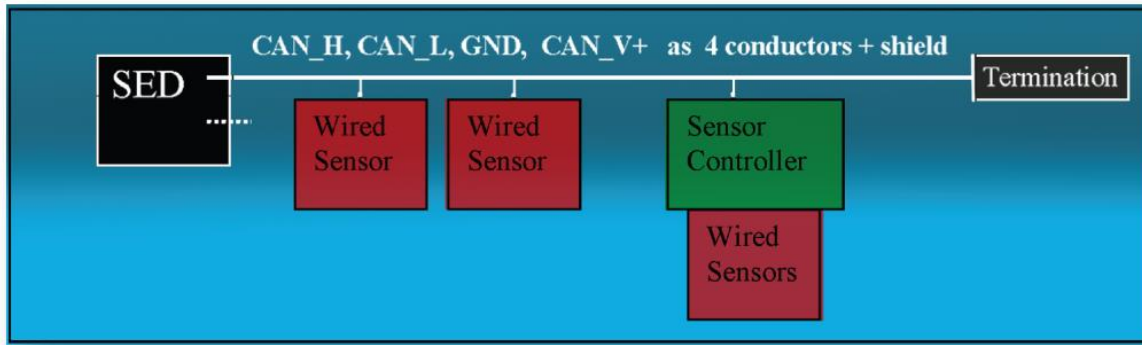


Figure 11-1. Wired Add-on Sensor Bus Examples.

Figure 11-1 is a logical bus connection based on the defined standard. However, the secured physical routing of the bus may daisy-chain, e.g., in/out and through mechanically interlocked panels or other arrangement.

11.1.1.1 Bus Bit Rate and Timing Error

A single uniform bus data (bit) rate of 64,000 bps shall be used in all transmissions by all nodes. The bit time duration error versus environmental conditions should not exceed 1.5%.

11.1.1.2 Bus Connector and Signals

The SED internal (inside enclosure), DB9 female, with the industry standard pin-out is as follows in Table 11-1:

Table 11-1. Wired Sensor Interface Connector.

DB9-F Pin	CAN Signal	Description
2	CAN_L	Dominant Low
7	CAN_H	Dominant High
5	Shield	Shield
9	CAN_V+	Power; mandatory here; optional in standard
6	GND	Signal ground, common

11.1.1.3 Wired Sensor Bus Power Characteristics

CAN_V+ is defined as follows:

- To be determined by implementer 5.0VDC +/-15%.
- To be determined by implementer 100 milli-amp (mA) maximum, sum all connected devices, short-circuit protected.
- To be determined by implementer 10 mA average maximum consumption by all connected devices.

11.1.1.4 Encryption

Encryption is not required. Bus message content is terse, e.g., 16 bits.

11.1.2 Wired Sensor Bus Physical Access

Each SED wired sensor bus shall provide a connection inside the SED enclosure. No external connectors exist. The method for cable entry to the SED is not specified here-in.

11.1.2.1 Wired Sensor Link Layer Control (LLC) and MAC

The Link Layer protocol for media access, arbitration, error detection, acknowledgements, low-powered modes, etc., are defined by the CAN bus standard and are not repeated here.

11.1.2.2 Frame ID Bits

Frame ID option: the CAN bus standard 11-bit wide identifier field is mandatory. The extended option is not permitted. ID bit definitions are as follows:

Table 11-2. Frame ID Bits.

ID Bit	10	9	8	7	6	5	4	3	2	1	0
Use	A	A	H	R	D	D	D	D	D	D	D

Where:

A is reserved for SED use.

H is reserved for use by a sensor with high priority data.

R is reserved for use by a sensor with routine priority data.

D is a don't care for filtering and is reserved for future use.

11.1.2.3 Frame ID Reservations

Sensor ID numbers are conveyed via the frame ID field and shall not conflict with the SED ID assignments. There are no specified sensor ID numbers; the SED will accept any ID with valid data content. ID assignments are an implementation configuration item.

11.1.2.4 Frame Bit Streaming

All datum shall be a multiple of 8-bits.

11.1.2.5 Wired Bus Message Data

The following message data is passed using the data length and data content fields in the standard. In the tables below:

- Ascension number is incremented by the transmitting node prior to transmitting each message, modulo 256. The ascension number is 0 at power up and after an Enable or Disable Sensor command message is received.
- Sensor ID codifies the controller, sensor or sub-sensor related to the message. Sensor ID numbers are assigned at time of installation.
- Authentication is a shared secret assigned at time of installation.

Table 11-3. Alive Message – Optionally Recurring at Unspecified Interval.

Mnemonic	Byte 0	Byte 1	Byte 2	Byte 2
ALIVE	1	Sensor ID	Ascension number	0: No faults present Otherwise, a fault code not defined here

Table 11-4. Enable Sensor – Sent by SED.

Mnemonic	Byte 0	Byte 1	Byte 2	Byte 2	Byte 3
ENA	2	Sensor ID	Ascension number	Authentication MSB	Authentication LSB

Most Significant Bit (MSB)

Table 11-5. Disable Sensor – Sent by SED.

Mnemonic	Byte 0	Byte 1	Byte 2	Byte 2	Byte 3
DIS	3	Sensor ID	Ascension number	Authentication MSB	Authentication LSB

Table 11-6. Sensor Activity.

Mnemonic	Byte 0	Byte 1	Byte 2	Bytes 3-12
ALARM	4	Sensor ID	Ascension number	1: Event Detection, New 2: Event Detection, Repeat Other: Reserved

Table 11-7. Set Sensor Parameter – Sent by SED.

Mnemonic	Byte 0	Byte 1	Byte 2	Bytes 3-12
PSET	5	Sensor ID	Ascension number	Unspecified

Set Sensor Parameter (PSET)

Table 11-8. Get Sensor Parameter – Sent by SED.

Mnemonic	Byte 0	Byte 1	Byte 2	Bytes 3-12
PGET	6	Sensor ID	Ascension number	Unspecified

Get Sensor Parameter (PGET)

11.2 RELAYS – EXTERNAL TO ASSET

A SED may act as a transparent relay device on behalf of a tethered SED as described in Section 4.2.8. A SED communicates with an NG in preference to a relay device when signal quality conditions permit. At any given moment, there can be only one device functioning as a relay for a tethered SED on any asset with the messaging relay functions described in Section 4.2.8.3. A tethered SED with GPS may simultaneously provide additional functions while acting as a relay. Non-relay functions that send and receive messages pass messages whose content is independent of the content in relayed messages.

Messages for non-relay functions are not co-mingled with the same messages as relayed SED messages. The SED transparent relay function is not capable of decrypting messages to/from the tethered SED. The DAP or secure NG will ensure that encryption keys will differ from those used for non-relay SED with GPS secure functions. For tethered devices, the following apply:

- The SED with GPS tethered device conducts Network Discovery via the NG's NGA message as described in Section 5.1.6.
- Messages relayed by a tethered device are retransmitted only to the MAC address of its tethered SED or the NG (i.e., unicast, not broadcast).
- The tethered device providing this relay function forwards and returns without alteration all SCINetEx messages, including Status messages, commands and acknowledgements.
- The device providing this relay function may relay proprietary data packets.
- A SED does relay HNG NGA messages when tethered with another SED.
- A SED tethered with a relay SED is capable of determining whether the tethering has been broken (e.g., by removal or loss of the relay SED) within two (2) minutes of occurrence.
- After successful tethering, if tethering is broken, the SED responds to all NGA messages from HNGs and FNGs.
- A SED in the Armed state ignores all tethering commands from HNGs and Tethering commands from other SEDs.
- If a tethered device loses power, it reverts to an untethered state.

11.2.1 Method of Tethering – SEDs

The tethering process starts with an unarmed SED mounted on an asset. Encryption is not required to conduct tethering. The relay SED is in an equivalent state (pre-commission, if applicable; again, encryption is not required to conduct tethering). The relay SED is mounted on the external surface of the asset usually in a location to collect GPS information. The HNG used for tethering is powered on and may possess valid encryption keys for both SEDs, but the encryption key(s) are not used in tethering. The following tethering process description is provided with the intent of ensuring interoperability.

- 1 **Discovery:** The HNG sends out an NGA message per Section 5.1.6 containing the HNG's UID.
 - The SED responds with an unsolicited Status message. The HNG then stores the SED's UID and MAC address. If the SED possesses an encryption key shared by the HNG, the HNG will acknowledge. Otherwise, the encryption error process of Section 8.3 will be executed. In either event, the HNG will have identified and stored the SED's UID and MAC address for use.
 - The relay SED 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 HNG stores the relay SED's UID and MAC address without transmitting an Application Layer acknowledgement. The UID may be the MAC address.
- 2 **Command Initiation:** During discovery, it is likely that multiple SEDs will respond. Using the HNG, the user selects the SED to be tethered identifying it by the UID displayed on the HNG screen. The user then selects the relay SED to be tethered from the user interface. This could either require key-in of a known relay SED MAC address or selection from a display field of relay SED MAC addresses generated during the discovery process above. The user then executes the Tethering command from the user display (message type 0xC0, OpCode 0x01) which is heard by both SEDs. There is no Application Layer message sent back. The parameters of this command are shown in Figure 11-2.
- 3 **Tethering Command Execution:** The relay SED then responds by sending out a unicast NGA message with the first SED's UID in the Message Waiting list and the relay SED MAC address in the Level 2 field of the NGA (normally HNG, see Table 5-3). The SED responds with a NULL message as described in Section 5.1.1.4. If the relay SED does not hear this NULL message and does not send a Tethering command within two (2) seconds, the HNG resends the Tethering command. If the relay SED hears this NULL message, it sends a Tethering command (message type 0xC0, OpCode 0x02) to the tethered SED. The tethered SED response to this command is an unrestricted Status message per Section 8.5.4. (The tethered SED must check the message header of the Tethering command to ensure the relay SED address matches.) If successful, the relay SED relays the unrestricted Status message received from the tethered SED to the HNG. If the HNG does not receive the unrestricted Status message from the tethered SED after two (2) seconds, the HNG resends the Tethering command.
- 4 **Tethering Completion:** The tethered SED assumes it is tethered at this point and accepts FNG commands from the relay SED address until a Pair command is received with Tethering byte set to zero (0) or the tethered SED is disarmed. Upon receipt of the unsolicited Status message by the HNG (sent from the relay SED), the HNG considers the tethering process successful. A relay SED does not respond to HNG NGAs until untethered.

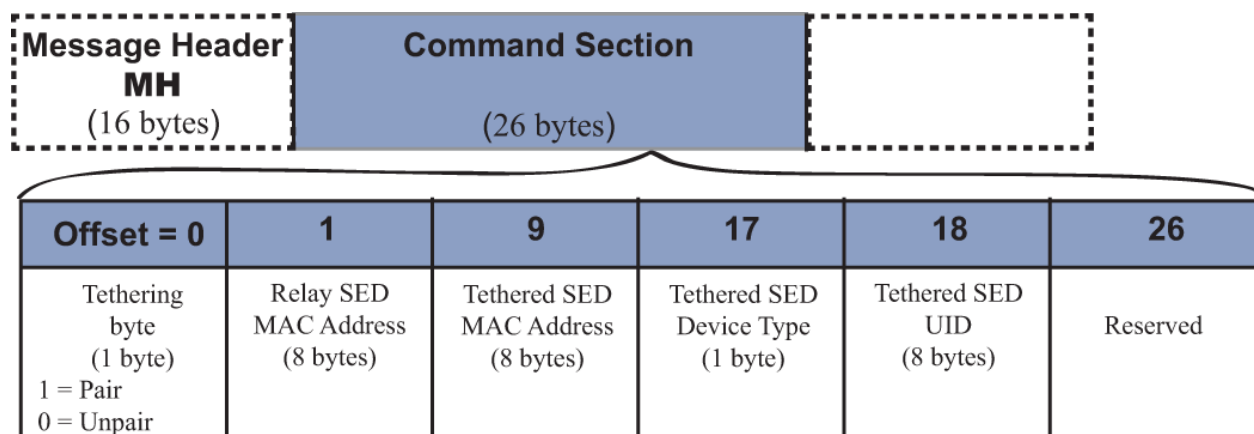


Figure 11-2. Tethering Command.

11.2.2 Method of Untethering

A tethered SED becomes untethered if it executes the Disarm command or if it is power cycled. The relay SED becomes untethered if it executes the Tethering command with the Tethering byte (byte 1) set to zero (0) or is power cycled.

11.2.3 Tethering Keep Alive

If a tethered SED fails to hear an FNG NGA message relayed by its relay SED over any two-minute interval (while hearing an FNG directly), the tethered SED responds to the next compliant FNG NGA message. SEDs respond to all compliant FNG NGAs irrespective of tethering status.

11.2.4 Tethering Sensor CMs and Relay Devices

Supplemental sensors may be similarly tethered to a GPS-enabled SED. For all other device tethering combinations, the tethering method is the same as above where the generic internal sensors are substituted for the tethered SED and any other type of relay device is substituted for the relay SED.

11.3 ADD-ON SENSORS – NO GPS

An Add-on Sensor (AoS) is a device that communicates directly with a SED via the wireless AoS bus. There can be up to five AoSs per SED (in addition to one relay device, as described in Section 11.2) 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.

AoSs that adhere to SCINetEx protocols may play a direct or indirect role in:

- Executing commands: Sensor enable/disable, status inquiry, etc.
- Status change reporting.
- Wireless interface to a SED.
- Implementing common message formats for SED-to-AoS communications.
- Adhering to common application protocol for error detection and correction.

11.3.1 SED-to-Add-on Sensor – Wired Bus Connection

The SED may accommodate wired bus connections to AoSs that are not integral to the SED as described in Section 11.1.

11.3.2 SED-to-Add-on Sensor – Wireless Medium

Wireless Add-on Sensors use the same Ad-hoc network protocols, MAC and PHY, as the Smart End Device (SED) with the following differences:

- Routing method is optional (a battery life consideration).
- The Network Discovery for sensors during the arming process procedure differs and is defined in Section 11.3.6.

The message category for sensor-to-SED messages are distinct from SED-to-NG messages (and NG-to-SED messages).

11.3.3 Wireless Medium – Physical Layer

The wireless medium Physical Layer for AoSs must be identical to that described in Section 5.2.3.

11.3.4 Wireless Medium – Data Link Layer

The wireless medium Data Link Layer must be identical to that described in Section 5.3 with the exception that transmitter power must not exceed zero (0) dBm EIRP.

11.3.5 Wireless Data Frame Content

The wireless Data Frame content is as described for SCINetEx in Section 11.4.4.

11.3.6 Method of Tethering SED and Add-on Sensors

Before a sensor can communicate with a SED, the two must be tethered. Tethering ensures that a sensor(s) will only communicate with a desired SED, and that the SED will securely communicate with the desired sensor(s). The tethering process needs to take place every time a new sensor is added or removed from the asset or a new SED is assigned to the asset.

The tethering process starts with an unarmed SED mounted on an asset. The SED has the encryption key installed; encryption is required to conduct tethering with an Add-on Sensor. The AoS is not required to possess a valid encryption key when starting this process. All AoS tethering is conducted using an HNG. The following detailed description of the tethering process is provided with the intent of ensuring interoperability for tethered sensors. The Add-on Sensor tethering sequence is illustrated in Figure 11-3.

NOTE: There may be multiple AoSs.

- 1 **The tethering process** for an Add-on Sensor (AoS) (Section 11.3) begins with each desired sensor's device type and UID input by the user into the HNG or discovered by the HNG using NGA messages. Transmitting these parameters to the SED will ensure that the SED does not accidentally pair with sensors in adjacent assets. After having entered or discovered all required sensor information, the user will send the sensor Tethering command from the HNG to the SED with up to five (5) sensor device types and UIDs.

NOTE: Space limitations of the IEEE Standard 802.15.4-2006 protocol forbid message fragmentation therefore limit the number of Add-on Sensors that can be transmitted in a single sensor Tethering command.

- 2 **Discovery:** The HNG sends out an NGA per Section 5.1.6. The SED responds with an unsolicited Status message. The HNG then stores the SED's UID and MAC address. Each AoS 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 HNG stores all AoS MAC addresses for selection by the user.

NOTE: The SED and the AoS(s) will derive and store fixed encryption keys for the AoSs based on the AoS UID and serial number. These keys will be shared unaltered by the SED and AoS for the duration of the tethering.

- 3 **Command Initiation:** During discovery, it is likely that multiple SEDs and AoSs will respond. Using the HNG, the user selects the SED to be tethered, identified by its UID displayed on the HNG screen. The user then selects the AoS(s) to be tethered from the user interface. This could either require key-in of one or more known AoS MAC addresses or selection from a set of displayed AoS MAC addresses found during the discovery process above. The selected AoS information is then sent to the SED UID (identified in the discovery process above).
- 4 When the SED receives the AoS MAC addresses and UIDs from the HNG, it transmits 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 respond with a sensor Status message. (Enabled sensors that receive the sensor Discovery broadcast message are discussed below.)
- 6 Once the SED receives a 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 SED transmits the Set Gateway SED command from Figure 11-5 to the sensor MAC address.
- 7 When the sensor receives the Set Gateway SED command, it limits its communication to its gateway SED alone and acknowledges this message by sending an encrypted sensor Status message. Receipt of the encrypted sensor Status message and successful decryption by the SED verifies successful tethering.
- 8 These steps can be executed for up to five (5) AoSs on the user inputted list simultaneously tethered to a single SED.
- 9 Upon completion of the tethering process, the SED transmits an encrypted Sensor Database report message (see Section 8.5) back to the commanding HNG.

Case: **SED operating mode is not armed**

Once the SED receives the sensor Tethering command, it transmits the sensor Discovery broadcast (SED NGA) message to the IEEE Standard 802.15.4-2006 broadcast address only if it is in the disarmed state. The SED transmits several sensor Discovery broadcast messages in succession to ensure that all sensors in the asset receive the message. After the SED transmits the sensor Discovery broadcast message, it waits no more than three (3) seconds for a response. Each time the SED receives a new response, it will reset its timer to 3 seconds. After this timer times out, the SED no longer accepts responses from sensors.

Case: **SED operating mode is armed**

The SED does not proceed with the tethering process if it is already in the armed state and simply responds to the HNG with a Status message indicating its armed state.

Case: **Sensor is disabled**

Once a sensor receives the NGA message from a SED, it responds 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 SED by sending a sensor Status message. If the sensor receives an acknowledgement from its gateway SED, it will not respond to the sensor Discovery broadcast message. This is to prevent malicious SEDs from being able to pair with enabled sensors. Enabled sensors are not allowed to pair with alternate SEDs. Once the SED 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 SED transmits via a unicast packet a Set Gateway SED command (Figure 11-5) to the sensor.

If the SED receives a sensor Status message from a sensor that is not on the list of sensors input by the user, the SED does not respond to the sensor. Once the sensor receives the Set Gateway SED command, the sensor limits future communication to only its gateway SED. The sensor is required to respond with an encrypted sensor Status message that acknowledges receipt of the command. Once the SED receives and successfully decrypts the sensor Status message, the tethering process for that particular sensor is complete. The only way to change the sensor's gateway SED is to perform the tethering process again (SED unarmed and Sensor untethered/disabled).

When the SED has received all sensor Status messages sent by sensors in response to the Set Gateway SED command, the SED overwrites its Sensor Database with the sensors it has received responses from. If the SED does not receive a response from a desired sensor after five retransmissions of the Set Gateway SED command, it assumes the tethering process with that sensor failed and does not include the sensor in the Sensor Database. The SED will then respond to the commanding NG with a Sensor Database report message.

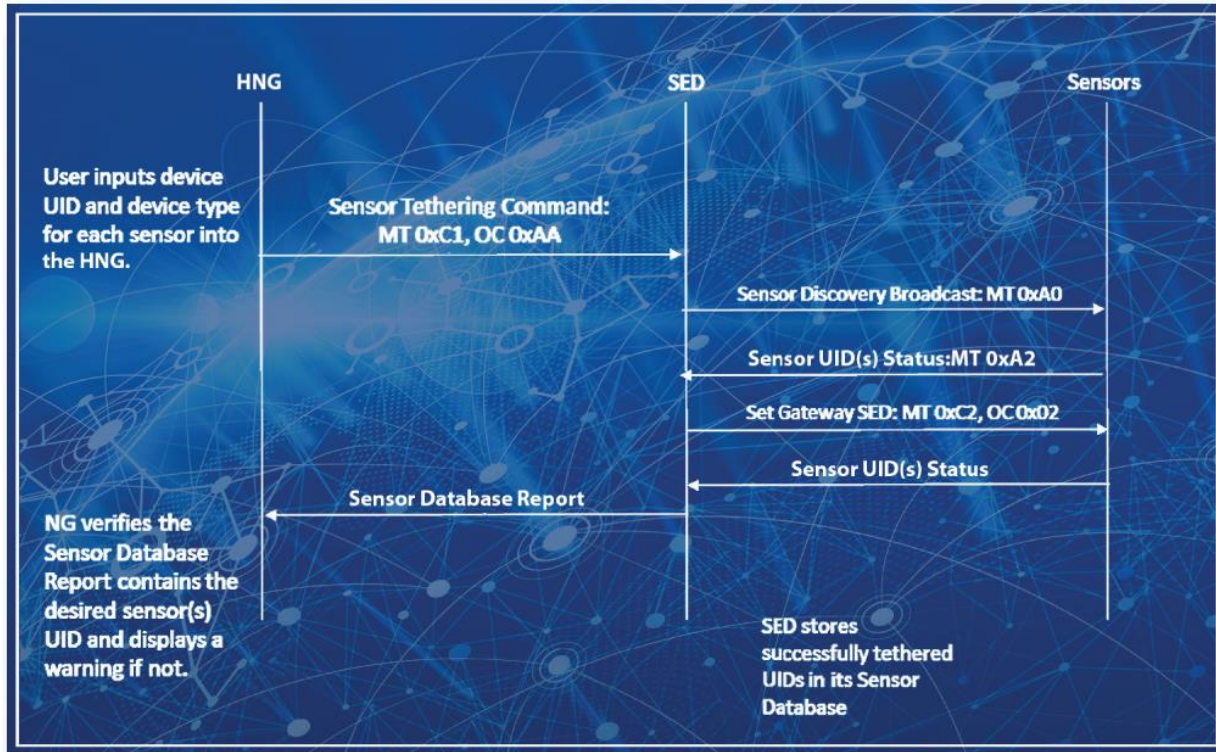


Figure 11-3. Add-on Sensor Tethering Sequence Ladder Diagram.

11.3.6.1 Sensor Database

The Sensor Database is stored in the SED and contains the device types and UIDs of sensors that the SED has successfully tethered with and is thus in control of. The Sensor Database is written during the last step of the tethering process described above in Section 11.3.6. 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).

11.3.7 Network and Application Protocol

The Network and Application protocol for Wireless Add-on Sensors are as described by the IEEE Standard 802.15.4-2006 and Section 5.

11.3.7.1 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 two seconds, it will retransmit its initial message. This will be repeated up to five 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 time-out value. The receiving device will retransmit a response only if it receives a duplicate message from the sending device. The SED Acknowledgement message will only be sent by the SED in response to an unsolicited Status message or alarm issued by a sensor.

11.3.7.2 Add-on Sensor (AoS) Status Message

The Add-on Sensor Status message is sent when:

- A valid Status Request command from the SED 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 field contains the ascension number from the message header of the Status Request command. The SED may validate using this number.
- 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.

- A Status message is required in the tethering process described previously.

The message header of the Status message (Figure 8-2) includes device type for wireless Add-on Sensors (AoSs). The device codes can be seen in Table 8-2.

On change of alarm status, the AoS generates a compliant Status message and sends it to its gateway SED set at tethering. A MAC Layer sensor/SED ACK will confirm receipt by the SED. From there the SED is responsible for recomposing the status and error bytes for local storage in the SED event record log and eventual delivery to the DAP. The SED will set the appropriate bit in the Restricted Status bits section to identify which AoS produced the alarm, see Figure 11-4 and Table 11-9.

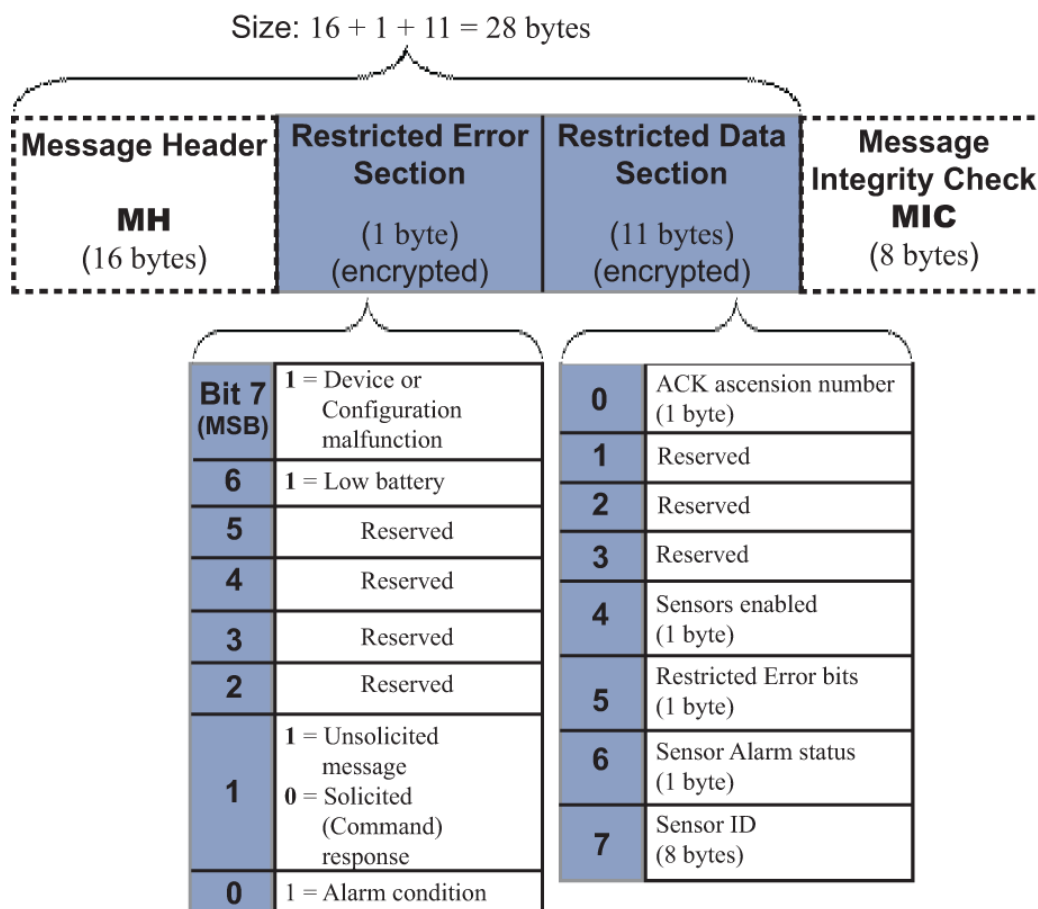


Figure 11-4. Add-on Sensor Status Message.

Table 11-9. Add-on Sensor Status – Restricted Data Section Detail.

Restricted Section Content	Definition
ACK ascension number	Ascension number for corresponding command. N/A for unsolicited Status message
Sensors Enabled	Bit 0: Sensor 1 Enabled Bit 1: Sensor 2 Enabled, 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 failure Bit 1: Enable failure Bit 0: Reserved
Sensor Alarm Status	Bit 0: Sensor 1 alarm Bit 1: Sensor 2 alarm, etc.
Sensor ID	The device UID. See Section 11.3.7.3 below.

11.3.7.3 Sensor ID

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

11.4 EMBEDDED COMMANDS FOR ADD-ON SENSORS – WIRELESS

Embedded commands for Add-on Sensors are commands that are sent from the SED to a particular sensor. Every AoS accepts and executes the commands listed in the following sections. All commands from the SED to an AoS have the Message Type 0xC2 to differentiate them from messages between the SED and an NG.

Restricted (encrypted) Embedded Command Message

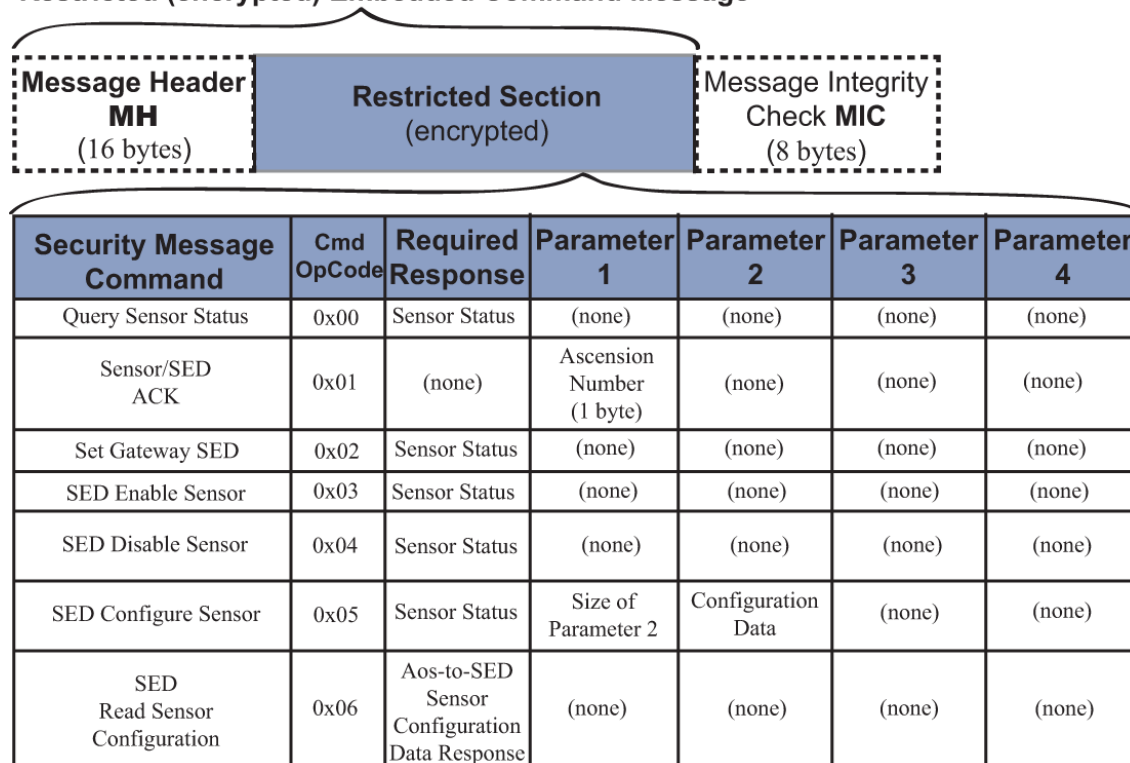


Figure 11-5. Embedded Command Message Structure from SED to Sensor(s).

11.4.1 SED Configure Sensor

The SED Configure Sensor command message seen in Figure 11-6 enables manufacturer-specific or otherwise undefined sensor configuration parameters.

NOTE: The input parameters shown in Figure 11-6 are only examples.

The SED sends the Configure Sensor command message to the specified sensor after it receives the Configure Sensor command message from an NG.

NOTE: The SED may be commanded by an NG to configure multiple sensors via a single command with a sensor bitmap.

The SED is responsible for transmitting individual SED 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 does not exceed the available payload data area defined by IEEE Standard 802.15.4-2006 minus bytes used by the NWK Layer protocol required by SCINetEx.

The sensor's response to the Configure Sensor command message is a sensor Status message. If configuration fails, the sensor will send a sensor Status message back to the SED with the Configuration failure bit set to 1. The SED will then send a Status message back to the commanding NG with the Configuration malfunction field set to 1 in the Restricted Error bits and the appropriate sensor number set in the Sensor Error bits.

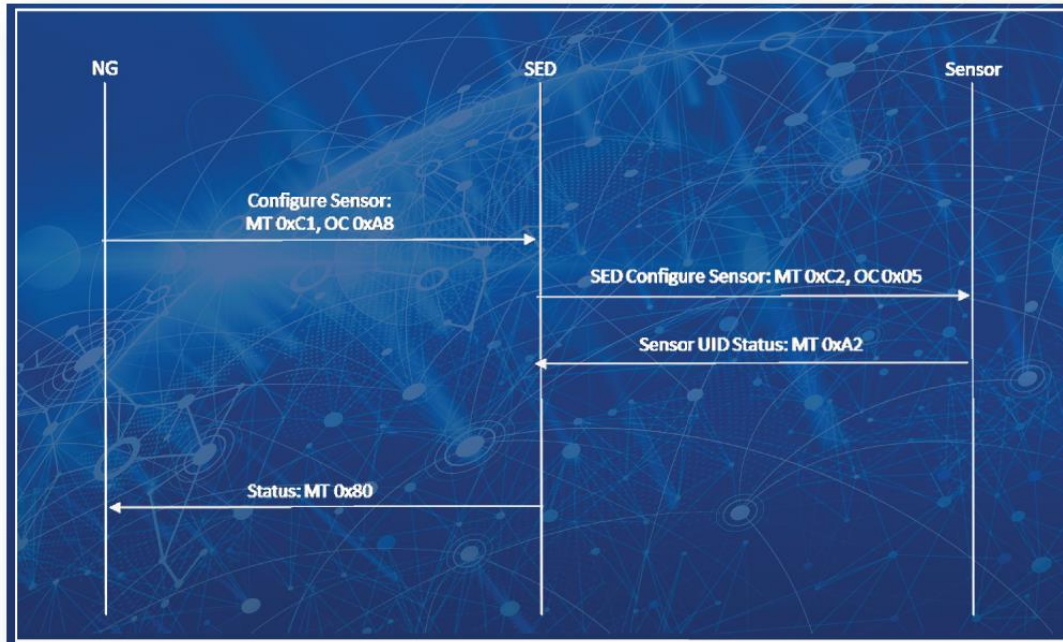


Figure 11-6. SED Configure Sensor Ladder Diagram.

11.4.2 Read Sensor Configuration (RSC)

The Read Sensor Configuration command seen in Figure 11-7 enables the SED 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 message is depicted in Figure 11-8.

NOTE: The SED-to-NG Sensor Configuration message (Message Type 0xA4) and the AoS-to-SED Sensor Configuration message (Message Type 0xA3) have the same structure.

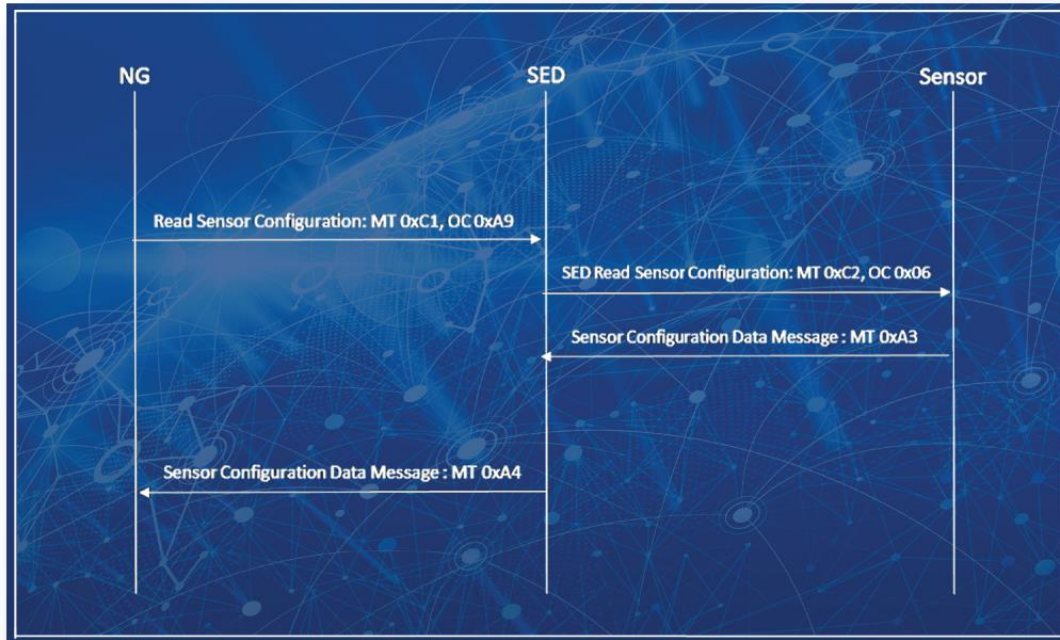


Figure 11-7. Read Sensor Configuration Ladder Diagram.

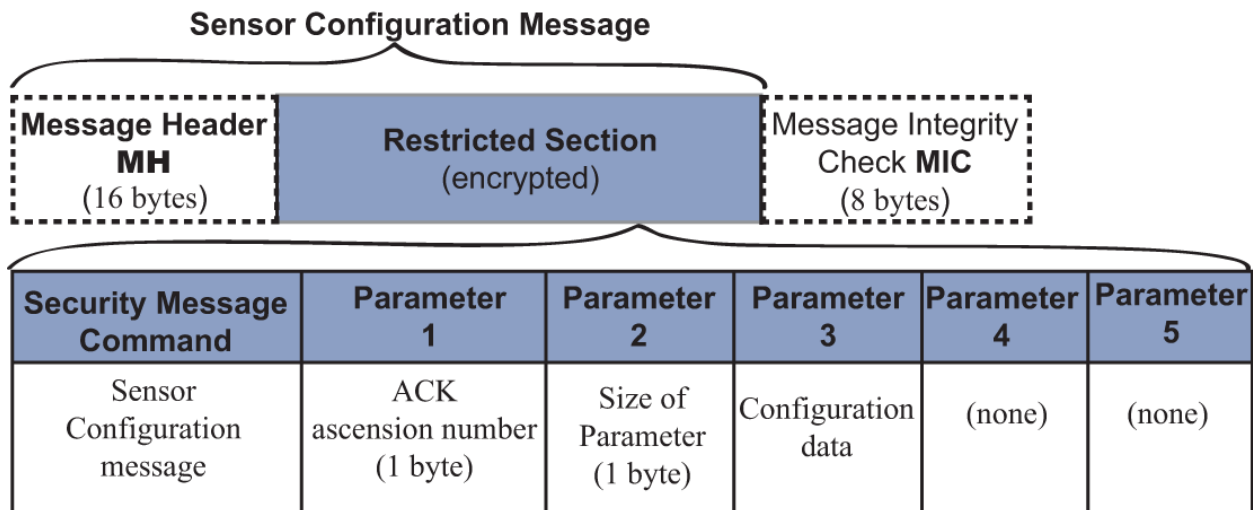


Figure 11-8. Sensor Configuration Command Message.

11.4.3 SED Enable Sensor (Arm System)

The SED Enable Sensor command message is transmitted from the SED to the sensor once the SED has been commanded to enable a sensor (Message Type 0xC1, OpCode 0xA6) or arm the system (Message Type 0xC1, OpCode 0x04). The sensor responds with a sensor Status message indicating whether or not the sensor was successfully enabled. The SED may be commanded by an NG to enable multiple sensors via a single command with a sensor bitmap. The SED is responsible for transmitting individual SED Enable Sensor command messages to the respective sensors. The flow of messages is outlined below in Figure 11-9.

NOTE: The parameter values in Figure 11-9 are only examples.

In the SED, the Enable Sensor command message 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 is not permitted when the SED is armed.

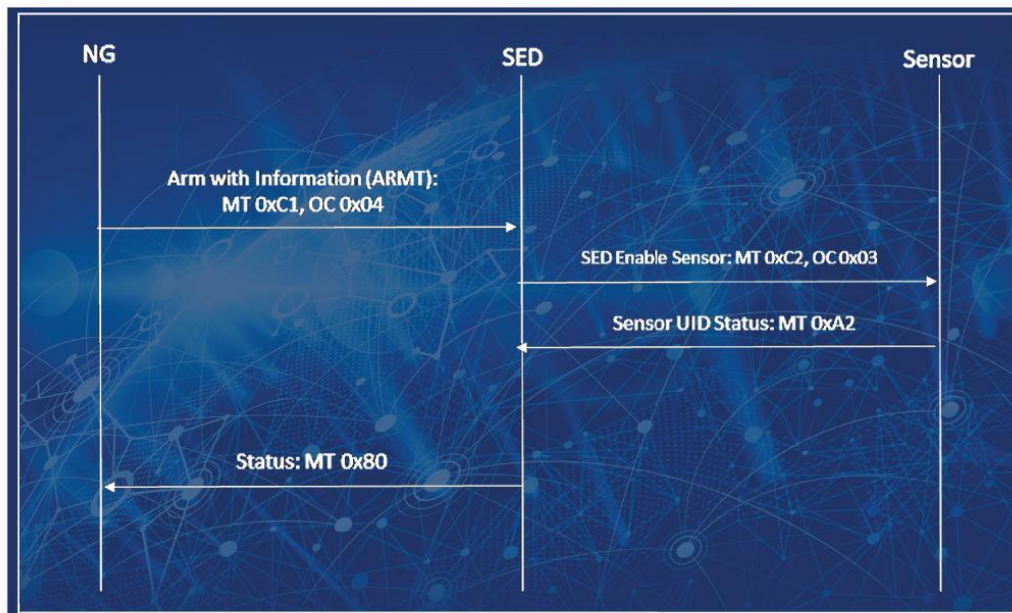


Figure 11-9. Arm System Ladder Diagram.

11.4.4 SED Disable Sensor

The Disable Sensor command message is transmitted from the SED to the sensor once the SED has been commanded to disable a sensor (Message Type 0xC1, OpCode 0xA7) or disarm the system (Message Type 0xC1, OpCode 0x80, 0x81). The sensor responds with a sensor Status message indicating whether or not the sensor was successfully disabled.

NOTE: The SED may be commanded by an NG to disable multiple sensors via a single command with a sensor bitmap.

The SED is responsible for transmitting individual SED Disable Sensor command messages to the respective sensors. Enabling or disabling of sensors is not permitted when the SED is armed.

11.4.5 Add-on Sensors (AoS) Data Formatting

Data passed from the AoSs to the SED is encrypted and must adhere to the requirements of SCINetEx. The AoS event data forwarded to the controlling SED does not cause the SED data packet size to exceed one frame.

11.4.6 Add-on Sensor (AoS) Event Alarm Procedure

When an AoS is in an alarm state, the AoS sends a Status message with the Alarm bit set to 1 (true) to the SED controller every 13 milliseconds until either the SED acknowledges receipt of the alarm message or the AoS battery is depleted. The SED records the AoS event data (alarm or battery depleted condition) in the event record log and forwards the information as part of its Status message to the DAP the next time the SED receives an NGA.

11.4.7 Periodic Unsolicited Status (“Health Check”)

While the AoS is enabled, it sends a periodic unsolicited Status message to its gateway SED to verify that the sensor is functioning properly and wireless connectivity has not been lost. The default time interval between health check messages is one hour, but developers are permitted to decrease this time interval if necessary, taking into consideration the power requirements of the sensors and SED. If the gateway SED does not receive an unsolicited Status message within an hour, it assumes that the sensor has malfunctioned and sets the sensor’s alarm status to true.

Chapter Summary

- Relays and Add-on Sensors may be wired or wireless.
- Add-on Sensors may be reconfigured over-the-air.
- All data and messaging formats are defined by SCINetEx.

This page intentionally left blank.

12. NETWORK GATEWAY TO DATA AGGREGATION POINT CONNECTIONS

This section provides a description of the communication interface between Network Gateways (NGs) and one or more Data Aggregation Points (DAPs). There are two forms of NGs; secure and non-secure as described here-in. Although it is fully understood that more than one DAP may exist, this section only describes communications to support one DAP and its connections to one or more NGs. Inter-DAP connections are not described.

12.1 DATA AGGREGATION POINTS (DAPS)

A DAP is a data portal for secure messaging between SCINetEx system elements described previously and provides control for the network. The initial DAP designated by the network ownership is the end-point for the Smart End Device (SED)-oriented messages and DAP command/responses. This designated DAP must be a physically and electronically secure facility (operations center) able to process millions of secure messages from various SEDs daily. It must also be able to securely communicate with the Key Information Manager (KIM) and other DAPs if not integral to those facilities.

12.2 NETWORK GATEWAYS (NGS)

NGs act as the communications bridge to/from SEDs whose embedded Communications Modules' function is the primary wireless communications interface. All of the requirements for wireless communication between the SED Communications Modules and NGs are previously described in this technical report. A top-level system view is provided in Figure 12-1.

12.3 INTERFACE DESCRIPTION

A DAP exchanges message-based data with SEDs via NGs in either real time or time deferred batch data transfers. Restricted commands are sent by the DAP to the SED via NGs. Secure messages are received by the DAP from the SED and NGs and are protected from unauthorized access, modification and spoofing by use of encryption. The DAPs have the ability to:

- Decrypt secure data from the SEDs.
- Generate restricted commands.
- Transfer encryption keys.
- Process security device event record logs.
- Process Status messages from NGs.
- Organize/control the SCINetEx network via automated tools, artificial intelligence and human operators.

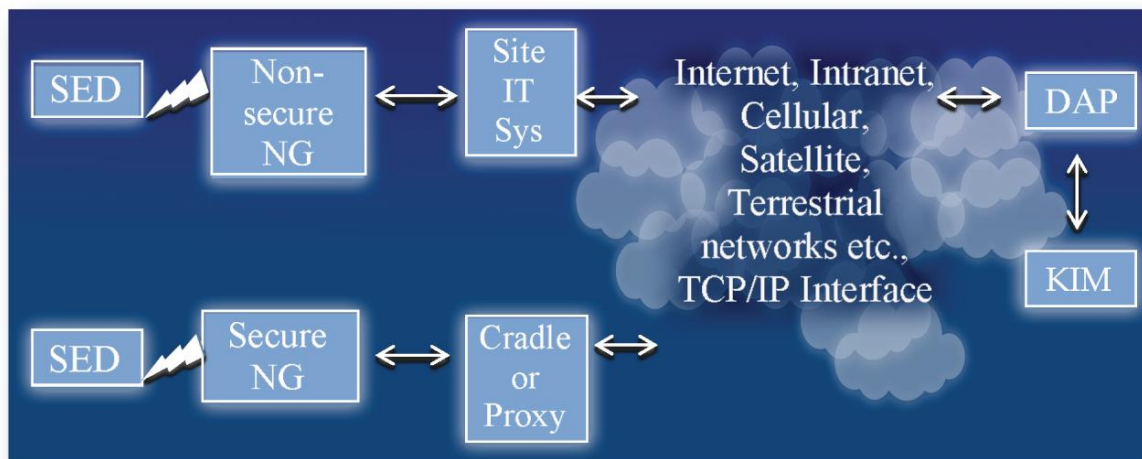


Figure 12-1. Top Level SCINetEx System View.

The terminology in Figure 12-1 is as follows:

Data Aggregation Point (DAP): The system end-point that communicates bi-directionally with designated NGs per this section, with the KIM and/or a higher level organization by means not defined here-in.

Non-secure NG: A device installed at a location such as intermodal terminals, refueling areas, mobile units or otherwise centralized locations. These devices are generally assumed to be unattended and are not given credentials to decrypt SCINetEx encrypted data.

Secure NG: A device that supports a subset of DAP functionality from SEDs' perspective. Secure NGs are generally assumed to be in the possession of a trusted user or agent. As such they have the capability to utilize temporary credentials to encrypt/decrypt SCINetEx messages. The credentials must be provided by the DAP. Connectivity to the DAP may be intermittent.

SED: Smart End Device that reports asset status to the DAP via wireless communications path utilizing messaging protocols defined earlier in this technical report.

12.3.1 Overall Data Flow

The bi-directional data flow of the SCINetEx system is as follows:

- The DAP communicates securely with the SEDs via non-secure NGs in real time.
- The DAP communicates securely with secure NGs in batch/non-real time or in real time as defined by that particular device. SEDs are given security credentials to communicate with the DAP.
- Secure NGs are given security credentials to communicate with the SEDs designated by the DAP.
- Non-secure NGs, unattended, have no security credentials and act as transparent bridges between message transport media.
- The DAP may communicate with managing organizations.
- SEDs communicate per the secure wireless methods described earlier.

12.3.2 Network Overview

DAP Operation: The purpose of the DAP is to present human operators with the information they need to determine if the various SED types are functioning properly and securely. The information presented should allow operators to make judgements about the health and security posture of the assets on the SCINetEx system network up to a global perspective, usually down to a specific locale and specific assets. The full set of the operational requirements for any DAP must be determined by the owner or manager of the DAP. The following is a short list of functions that must be performed by any DAP from an operational perspective:

- Enforce a policy to protect data stored or retransmitted after receipt by methods defined for SCINetEx system compliance.
- Securely communicate with NGs per the protocol and formats defined by SCINetEx.
- Securely communicate with the KIM.
- Maintain and present to operators the connectivity status and history for all communications interfaces defined by SCINetEx. This includes both real time connectivity and scheduled connectivity with NGs.
- Accept from all compliant NGs status and event record log history information produced by SEDs and retain such data in a database, indexed by device UID.
- Form data packages for NGs to execute arm/disarm and commission/decommission commands defined by SCINetEx and related actions, allocating tasks to specific secure NGs via secure data packets.
- Provide secure NG-specific encryption information to the correct NG at or before the required time, via methods defined by SCINetEx.
- Be able to aggregate the information received to present a useful asset status and security picture of targeted aspects of the SCINetEx system network to DAP operators.

Types of NGs and Interfaces: The DAP must support communications with the various forms of NGs over various available interfaces. These interfaces include wired interfaces connecting DAPs to fixed NGs and handheld NG cradles over IP, as well as embedded WAN interfaces such as cellular or satellite data services. It is envisioned that future products and services may define other types of NGs but for our purposes, we will assume there are at least two categories of NGs: non-secure NGs and secure NGs.

Non-secure NGs act as functionally transparent wireless-to-IP bridges that cannot encrypt or decrypt security-purposed Application Layer messages passing between the DAP and SEDs. Non-secure NGs must do the following:

- Pass messages to and from a DAP without payload modification.
- Use various public/private WANs to connect to the DAP.
- Act as elements of an untrusted network, of the same security role as routers and switches.
- Assume to be installed in locations that are not controlled for physical access.

The non-secure NG may have other security features associated with the network backend. For instance, a non-secure NG may or may not use IPSec as part of the networking protocols for delivering its data.

At the other functional extreme are secure NGs that temporarily possess authorizing credentials (i.e., encryption keys) that allow them to issue restricted commands, access encrypted messages and event record log files in the same manner as a DAP. These devices are intended to always be in a fully secure area or in possession and complete control of the designated/trusted agent. In the latter case, secure NGs are most likely portable. All forms of secure NGs must do the following:

- Securely communicate with a DAP.
- Authenticate to the DAP for download of temporary encryption keys.
- Provide the user capability to view the secure data SEDs.
- Aggregate and package NG sensitive data in order to ship securely to the controlling DAP.
- Aggregate and package data secured by the SEDs as bound to the DAP.

Secure and non-secure NGs provide the capabilities to support both ends of the security and functional spectrum. As other types of NGs become developed, they may have different levels of access to security data provided by the SEDs and different levels of control in the SCINetEx system network.

12.4 NETWORK GATEWAY-TO-DATA AGGREGATION POINT SECURITY

The SED Communication Modules each have a unique security code (UID), a value that uniquely defines them. This value is used in security applications to allow authentication of data and ensure communications with intended devices are supported. Similarly, the DAP must have a unique identification (UID) that the SEDs are aware of. The DAP's UID is bound into the key derivation functions that allows SEDs to communicate with secure NGs.

- Every DAP is assigned a unique 64-bit (8 byte) DAP UID.
- The DAP UID must be communicated directly to the SEDs for secure communication.
- All NGs must be able to communicate the UID of their parent DAP to communicate securely with the SEDs.

To communicate secure messages to/from a SED, the DAP must store certain sensitive information. This includes keys obtained from the KIM and decrypted data obtained from SEDs. The DAP's stored data obtained from the KIM or from the SED is protected from unauthorized access or transmission on any media, in accordance with the DAP security plan policy. This policy is beyond the scope of this technical report.

Section Summary

- The DAP's UID is needed for key derivation functions.
- All NGs communicate the UID of their parent DAP to each SED in coverage.

13. NETWORK GATEWAY-TO-DATA AGGREGATION POINT COMMUNICATIONS

13.1 COMMUNICATIONS INTERFACE

- The DAP implements IPv4-compatible network interface or higher for data exchanges with non-secure NGs that bridge messages to/from IEEE Standard 802.15.4 – 2006 wireless links to SEDs. Message security is independent of WAN transport service provider.
- The DAP implements IPv4-compatible network interface or higher for data exchanges with non-secure NGs and SEDs that communicate (secondary path) on a WAN via cellular data and satellite. The DAP also supports IPv4 interfaces to such public carrier WAN services. Message security is independent of WAN transport service provider.
- The DAP implements an IPv4-compatible network interface or higher for data exchanges with secure NGs and utilize previously batch transferred data to later securely exchange data with SEDs. The specifics of the batch transfers are provided in a later section of this section. Message security is independent of the WAN transport service provider.
- The DAP securely exchanges data with a distant or co-located KIM. Message security is independent of the WAN transport service provider.

The characteristics of the interface to the KIM database are to be determined by the governing entity of the database. This section defines methods to enable a DAP interoperable interface to each category of NG, irrespective of the manufacturer of the NG and independent of the characteristics of the varying DAPs.

13.2 DAP-TO-NG DATA CONNECTION

The DAP accepts both session-based and session-less connections from NGs on their on-site proxy. The security and transport protocols for both connection types are applicable for data packet exchange with the DAP at any point in time.

13.2.1 DAP-to-Non-secure NG Data Transfer

If the SED is in the coverage of a non-secure NG, the DAP may pass commands through the non-secure NG using the encryption keys held by the DAP. The same is true for status queries, log retrieval or deactivation/decommission of a SED by a DAP.

13.2.2 DAP-to-Secure NG Data Transfer

The secure NG, when in communications with the DAP, directly or via an on-site proxy, exchanges all trip information and SED data through encrypted batch file transfers. This can include the data needed for all of the commands and encryption credentials. This information can also be used by personnel or automated processes on-site to plan tasks for secure NGs. A secure NG obtains the encryption keys for transactions with assigned SED UIDs during either the commissioning process for FNGs or by secure File Transfer Protocol (FTP) for HNGs. This done, the secure NG is then able to undertake the tasking as directed by the DAP or trusted agent.

13.2.3 DAP-to/from-Secure NGs Network Protocol

All DAP IP to secure NG data traffic is compatible with IPv4 or higher standards. DAP-to-secure NG data transfers can be accomplished per the following in an unattended manner when devices are not in use by personnel. This condition provides secure NGs with IP connectivity with DAP(s) directly (cradle) or indirectly through an on-site proxy. In the case of a proxy or terminal server, the data flow from proxy to the NG conforms to the DAP information assurance (IA) policy.

13.3 DAP-TO-SECURE NG

13.3.1 Retrieval of SED Encryption Keys

The secure NG (or its proxy) obtains the encryption keys for SEDs to which the operator/NG is tasked. The messaging may vary, but the means to obtain keys given here applies to all. The DAP has the option to securely commission/arm SEDs via a direct connection through an on-site non-secure FNG if available. This section however applies to the use of a secure NG. Encryption keys are transferred from the DAP to the secure NG as follows:

- 1 A secure NG, having received a list of SED UUIDs and related data with instructions must now obtain the encryption key to conduct secure data transactions for each SED. This is needed to authenticate and autonomously communicate with the SED.
- 2 The DAP accepts secure File Transfer Protocol (FTP) connections with the secure NG. The DAP authenticates by username/password and logs all connections. The username and password strength is governed by local IA policies.
- 3 The DAP provides a data file on the FTP server for the particular secure NG (or its proxy) that has connected. This is the only file in the login directory. The content of this file is a list of UUID-correlated encryption key pairs matching the assignments made by the user in the preceding section.
- 4 The secure NG (or its proxy) downloads this file via secure FTP connection process and is described as follows:
 - a The SED UUIDs in the file are compared to the work assigned list of the SED UUIDs previously obtained by the secure NG.
 - b The FTP session now terminates.
 - c The DAP logs this event.
 - d If the list is deemed inaccurate by the secure NG (or its proxy), an exception will be alerted to on-site staff for disposition and the secure NG will become idle until re-tasked.

With the downloaded list of UUID-correlated encryption keys, the secure NG is able to accomplish the tasking that involves secure data and command transactions for these SED UUIDs. Local policy defines the encryption key security while stored in the secure NG and how/when this information is to be destroyed.

13.3.2 Communications Data Prerequisites

The following sections describe the prerequisites for communications between an NG and a DAP.

Secure NG Every secure NG and/or its on-site proxy is provided the following information:

- The UID of each DAP with which the secure NG (or its proxy) will perform message exchanges.
- The Public network address that corresponds to each DAP UID, this being an edge router/firewall or other IT-defined mechanism for remote access to the DAP server.
- An IP address and server login/password/home file directory. These may be used by automation on the secure NG (or its proxy) rather than by a person. For each secure NG (or its proxy) supported by a given DAP UID, that is, for each secure NG UID, there is a login account for a specific DAP UID. The server function may be isolated/outside of firewalls at a DAP, etc. to meet IA policy.

13.3.3 Communications to Commission/Arm a SED

If a SED is in the coverage of a non-secure FNG with a real-time connection to the DAP, the DAP may pass baseline information and commission/arm a SED. Alternatively, a policy/practice compliant procedure may be used by a secure NG without real-time connection to a DAP to commission/arm a SED.

13.3.3.1 Commission/Arm SED Prerequisites

A specific SED on an asset that is selected by the user is made known to the DAP. The DAP data correlates asset ID and any additional information needed for commission/arming. This combined with the secure NG UID and the SED encryption key (previously provided to the DAP) enables the commission/arm task to be undertaken with secure commands that require data entry plus security credentials.

13.3.3.2 DAP-to-Secure NG Commission/Arm Data

The following steps must be completed prior to securely communicating with a SED for a commission/arm action by a secure NG:

- 1 The DAP obtains the asset ID (plus any subfield IDs) from the user.
- 2 The DAP obtains a list of asset IDs, and associated with each asset ID, a list of one or more secure NG UIDs that is planned to communicate with the SED UID on that asset.
- 3 The DAP obtains from the KIM the Long Term Key (LTK) for each SED UID obtained in step 2, above. There may be multiple NG UIDs for one SED UID if the user needs such, e.g., the first available secure NG is used for the task.

13.4 GENERAL PACKET FORMATS FOR MESSAGE-BASED INTERFACES

The DAP-to-NG messaging is bi-directional and packet-based as defined for the following interfaces:

- Non-secure NGs.
- KIM.
- SEDs when using public carrier (cellular/satellite) for security-purposed messaging.

NOTE: This packet message interface is not used for secure (handheld) to/from NGs. The secure HNG is described in Section 10. The DAP does not need prior knowledge of the IP address of the remote site gateways used by non-secure NGs. Each packet has a general preamble followed by content, as defined in this section. Each packet has a response for flow control and error correction. Packets are sent via either connectionless UDP or via TCP/IP connections per the conventions specified here-in.

The message rates are assumed low and infrequent for a given NG, thus the implementer may find at large scale (NG counts) that UDP is more reliable as compared to the need for persistent or recurring connections in TCP. Thus SEDs that include a public (cellular/satellite) may use either UDP or TCP. The use of Network Address Translations (NAT) is assumed the norm, i.e., public addresses for NGs are not needed.

NOTE: Data sent/received by DAPs may be via a relay. This may be the norm for NGs and SEDs that communicate via WANs. In the SCINetEx system, sensitive data is encrypted by the secure NG, SED or DAP. For such, the relay is akin to switches and routers in the public carrier/Internet WAN and are untrusted. Non-secure NGs also do not encrypt/decrypt in their bridging function. The SCINetEx security mechanisms enable the message integrity and authentication of the message originator by the destination system. Table 13-1 depicts the general packet preamble for all packets exchanged via the DAP interfaces listed here-in.

Table 13-1. Preamble Formats.

General Packet Preamble Format		
Size	Data Content	Notes
UDP: 8 bytes TCP: 0 bytes	UDP: UDP header per Request for Commands (RFC) in IPv4 TCP: Not present See note to right.	The operating system, if any, may remove these UDP header bytes and pass the packet size and source IP address via an API. However, as transmitted, the UDP RFC requires these 8 bytes be transmitted.
1 byte	Packet format, revision letter (V), as a null-terminated one-character string, as: \0 For DAP-originated messages, per current version of SCINetEx, the revision letter is A.	\0 depicts an ASCII NULL byte.

Table 13-1. Preamble Formats. (Continued)

General Packet Preamble Format		
Size	Data Content	Notes
3 bytes	Function code A number, 000-999, as three 1-byte ASCII numeric digits, formatted as: ddd\0 Codes 000-499 are reserved for exclusive use per this version of SCINetEx. For codes 500-999, all bytes subsequent to the Function code are not defined by this version of SCINetEx.	Codes by function are listed in subsequent sections. \0 depicts an ASCII NULL byte.
8 bytes	The numeric ID of the entity producing this message as 16 1-byte ASCII hexadecimal digits, with leading zeros as: dddddddddddddddd\0 Byte order: left-most digits depict byte at lowest offset in array-bytes, as in the message header. The number is inserted by the message originator.	For messages sent from the DAP, the ID is the UID of the DAP. For messages sent to the DAP, the ID is the UID of the sending NG, to include the non-secure NGs UID (i.e., UID not used for encryption) or the UID of the sending KIM. Valid for the reserved Function codes. \0 depicts an ASCII NULL byte.
0 or n bytes	Zero or more additional text or binary data bytes, according to the Function code above. Formatted per the specific packet Function code shown above. Content per Function code is wholly contained in one standard IP packet.	The size and format of additional bytes is given in the definition of the particular added comment.

13.4.1.1 DAP UID and IP Address

Every DAP has one associated UID. This UID is used by non-secure NGs to inform the DAPs identity and is included in the Network Gateway Announcement (NGA). This permits the SED to use the proper security credentials for that UID. A SED may retain the credentials for multiple DAPs according to mobility needs. A KIM for a given DAP has security credential information based on the unchanging UID for a DAP and for SEDs subordinated to that and other DAPs.

The UID of a DAP does not have a fixed association with the DAP's IP address. This UID cannot change though the IP address may change. For the DAP's purposes, the LAN IP address of an NG is assumed to be a non-public address, assigned by the local IT authorities as static, DHCP or DHCP reservation. The DAP does not need knowledge of these LAN IP values.

Security sensitive data is encrypted at the application message level. Thus the DAP does not require secure message Transport Layer. This is to avoid TLS/SSL, digital certificates, etc. when using non-secure NGs.

13.5 DAP-TO/FROM-NON-SECURE NGs

The DAP communicates with non-secure NGs via IPv4 or higher UDP or TCP with the general packet preamble in Table 13-1.

13.5.1 UDP Option

Each UDP-based NG communicating with a DAP is provided the following at the time of installation/activation:

- Primary DAPUID
- IP Address
- UDP port number
- WAN Gateway/subnet mask

An NG may have a list of alternative/back-up DAP IP addresses and port numbers. The DAP should not assume this is the case. The DAP accepts incoming UDP packets on the designated port from a valid gateway IP address for the sites affiliated with the DAP. The DAP may block/ignore others according to the firewall configurations for multiple services. Each packet will have the NG's UID in the general packet preamble of Table 13-1. As non-secure NGs are relay/bridges and do not encrypt or decrypt, the non-secure NG UID may not exist in the KIM database.

The DAP sends response UDP packets on the same port number as received, and to the IP address of the corresponding incoming packet's originator. The LAN/WAN gateway administrator will assure that packets on the chosen port are not blocked for incoming or outgoing packets. For policy reasons, the remote site administrator may elect to configure the firewall/gateway to route UDP for an NG with a static LAN address solely to/from that IP address for a chosen port number. This assures that packets on a selected port (or port range), irrespective of the packet source on the WAN, go only to NGs and not to other servers on the LAN.

The DAP has the discretion to discard incoming packets for security or system loading reasons. The SCINetEx protocols will detect such discards and retry later. SCINetEx messages provide a means for an authenticated DAP to alter the primary DAP interface values should the need arise to change the DAP interface port number, a single DAP's IP address or the IP address of the local WAN gateway router/firewall.

13.5.2 TCP Option

Each TCP-based NG communicating with a DAP is provided the following at the time of installation/activation:

- Primary DAPUID
- IP address
- TCP port number
- WANgateway/subnetmask.

An NG may have a list of alternative/back-up DAP IP addresses and port numbers. The DAP should not assume this is the case. The DAP accepts incoming TCP connections on the designated port from a valid NG IP address for the sites affiliated with that DAP. The DAP has the discretion to block/ignore other connections according to the firewall configurations for multiple services.

The TCP-based NG is responsible for initiating the TCP connection as needed. The DAP supports concurrent TCP connections from NGs where the total is chosen by the DAP administrator. When this number is exceeded, the DAP rejects the TCP connection attempt. The DAP may forcibly terminate a TCP connection for security reasons such as abusive or unexpectedly high connection rates. The DAP also has the discretion to discard incoming packets for security or system loading reasons. The SCINetEx protocols provide a means to detect such discards and retry later.

SCINetEx messages provide a means for an authenticated DAP to alter the primary DAP interface values should the need arise to change the DAP interface port number, a single DAP's IP address or the IP address of the local WAN gateway router/firewall. Security data is encrypted at the application message level. Thus, the DAP does not require a secure message Transport Layer. This is to avoid TLS/SSL, digital certificates, etc. when using non-secure NGs.

13.5.3 DAP-to/from-Non-secure NG Connect to DAP

For both TCP and UDP connections, the host DAP gets notification of an incoming packet to the address provided to the NG during installation/activation. Therefore, no introductory connection message/response is required.

13.5.4 Get Time and Date Message

See Section 13.6.5.1.

13.5.5 DAP-to-Non-secure NG Packet Messages

This section defines the IP packets exchanged bi-directionally by a DAP and non-secure NG via either UDP or TCP. Each message is a single packet. A DAP accepts from-NG packets only in the format shown in Section 13.6.5.2. Every packet must conform to the SCINetEx general packet preamble format described in this section.

13.5.5.1 DAP-to-Non-secure NG Heartbeat Request Packet

Every DAP sends the Heartbeat Request packet to every DAP-subordinate non-secure NG, at an interval in the range of 30 to 300 seconds. Because the Heartbeat packet contains date/time (UTC), the receiving NG may set its internal clock and use that in the NGA wireless broadcasts. SEDs may extract the date/time from the NGA message for their own use. The DAP produces the Heartbeat Request packet in the format shown in the Table 13-2.

Table 13-2. Date, Time, Heartbeat Request Packet.

DAP-to-Non-secure NG Heartbeat Request Packet, Function Code 000 (in packet preamble)		
Size	To-DAP Data Content	Notes
Variable	General Packet Preamble	See Table 13-1
3 bytes	Maintenance Code, two 1-byte ASCII numeric digits followed by an ASCII NULL, is as: 00\0	00-49 are reserved 50-99 are manufacturer specific
15 bytes	Date/Time (UTC) as one-byte ASCII characters, of the form: YYYYMMDDhhmmss\0	\0 depicts the ASCII NULL byte January = 1

13.5.5.2 Non-secure NG-to-DAP Heartbeat Response Packet

A non-secure NG responds to the Heartbeat Request packet sent only by the designated DAP, based on both the source IP address and the preamble's DAP UID being that for which the NG is configured. Non-secure NGs send the Heartbeat Response packet in response to not less than 90% of the received Heartbeat Request packets. A DAP accepts this packet only from NGs that show a UID in the preamble that is among those designated as subordinate to that DAP. On receipt of a valid Heartbeat Response packet, the DAP updates health status for that NG. On receipt of an invalid packet, the DAP updates the non-secure NG configuration error status for the reporting NG (e.g., NG failed to change DAP affiliation as commanded by message or locally reconfigured without authorization). The DAP only accepts Heartbeat Response packets in the format shown in Table 13-3.

Table 13-3. Heartbeat Response Packet.

Non-secure NG-to-DAP Heartbeat Response Packet, Function Code 000 (in packet preamble)		
Size	To-DAP Data Content	Notes
Variable	General Packet Preamble	See Table 13-1
3 bytes	Maintenance Code, as two 1-byte ASCII numeric digits followed by an ASCII NULL, is as: 00/0	00: Normal condition 01: Maintenance attention required 02: IEEE Standard 802.15.4 network hardware fault 03: IEEE Standard 802.15.4 network CCA failures or MAC/ACK time-outs are excessive due to persistent interference 04-49 Reserved 50-99 Manufacturer specific

13.5.6 Non-secure NG-to-DAP – SED Message Content

Here, SED message content means any message defined for the SED literally and unchanged in its binary form. A non-secure NG produces the packet defined in Table 13-4. This content will have been created and encrypted by a SED communicating with the non-secure NG. The DAP accepts such content and processes the information provided per the DAP functional requirements. The DAP provides a response to each received message in the prescribed format, and transmitted to the NG whose UID is invalid for this DAP (not affiliated). The NG UID is in the preamble. The DAP processes valid packets of this type which defines which messages are themselves a response and which yield a response. Unsolicited messages to a DAP must have a response.

Table 13-4. Non-secure NG-to-DAP Preamble.

Non-secure NG-to-DAP Packet Type: SED message content, Function Code 010		
Size in bytes	To-DAP Data Content	Notes
Variable	General Packet	See Table 13-1
Variable	Binary byte-oriented data content. Includes message header, content and Message Integrity Check (MIC) bytes for restricted messages.	Size is located in the header content, where the header size is fixed and the message size plus variable MIC size is inclusive.

13.5.7 DAP-to-Non-secure NG – SED Message Content

Here, SED message content means any message defined by SCINetEx, literally and unchanged in its binary form. The DAP produces the packet defined in Table 13-5 below. The non-secure NG accepts the packet and forwards to the SED. This content is encrypted by the DAP depending on the message type. A response will be sent by the SED via the NG if it is a DAP's command to the SED, with the exception of the DAP's ACK message. The response is formatted as in Table 13-4.

Table 13-5. DAP-to Non-secure NG Preamble.

DAP-to-Non-secure NG SED Message Content, Function Code 011		
Size in bytes	To-DAP Data Content	Notes
Variable	General Packet Preamble	See Table 13-1
Variable	Binary byte-oriented data content. Includes message header, content and Message Integrity Check (MIC) bytes for restricted messages.	Size is located in the header content, where the header size is fixed and the message size plus variable MIC size is inclusive.

13.5.8 DAP-to-Non-secure NG – Change DAP IP Address

This function enables, with authentication, a DAP to alter the following configuration items retained by an NG in non-volatile storage:

- DAP IP address, protocol (TCP or UDP), port number
- LAN Gateway IP address, subnet mask
- NG ID number

NOTE: Non-secure NGs do not have a UID as used for encryption purposes.

The NG ID number in this message is for the DAP indexing to a place name database, irrespective of the non-secure NG's private NAT-ed IP address. This is to reduce the need for physical access to the device for a change. The change may be caused by a shift in DAP roles or an IP address management change at a DAP.

The command's success is observable by the DAP, now using the changed DAP IP address, issuing Heartbeat Request packets and receiving a response. The NG ignores the packet if either:

- Four-byte authentication code in the DAP message does not agree with that retained in the NG's non-volatile memory.
- The DAP UID in the general packet preamble is that for which the NG is currently assigned.

The NG ignores the packet if the 4-byte authentication code does not match that expected, or if the parameters are invalid. The NG retains the new 4-byte authentication code, if they differ, for future use. The DAP retains the current 4-byte authentication code used for some or for all NGs. The DAP assigns DAP IP addresses, protocol and port numbers. If the configuration change is ignored by the NG, it may be necessary to locally access the NG to correct the settings. The DAP produces the message format shown in Table 13-6.

Table 13-6. Change DAP IP Address.

DAP-to-Non-secure NG Change DAP IP Address, Function 002		
Size	To-DAP Data Content	Notes
9 bytes	Authentication code as 8 hexadecimal digits in 1-byte per character ASCII form, with terminating NULL byte as: ABC12345\0	The NG will ignore this command if the authentication code does not match that stored in non-volatile memory. Where \0 denotes an ASCII NULL
9 bytes	Replacement authentication code formatted as shown above. If 8 zeros, replacement is not performed.	The NG will replace the value stored in non-volatile memory if the code is not zeros and differs from the current authentication code.

Table 13-6. Change DAP IP Address. (Continued)

DAP-to-Non-secure NG Change DAP IP Address, Function 002		
Size	To-DAP Data Content	Notes
variable	Protocol and port selection as a 1-byte ASCII character depicting the protocol to use, followed by one or more ASCII numeric digits depicting the port number to use, followed by an ASCII NULL, as: N\0 for no change. U12345\0 for UDP T54321\0 for TCP	Where \0 denotes an ASCII NULL
variable	New DAP IPv4 address as 1-byte per character ASCII form, with terminating NULL byte in dot form, as: 111.222.333.13\0	Where \0 denotes an ASCII NULL NOTE: A non-public IP address may be used if the DAP and all NGs are in the same private network or virtual private network (VPN) irrespective of the carrier used for the WAN.
variable	New LAN Gateway IPv4 address formatted as shown above, or if no change, place a zero in all octets.	
variable	New LAN subnet mask Formatted as shown above, or if no change, place a zero in all octets.	
variable	New NG ID number	Non-secure NGs do not have a UID used for encryption purposes. The ID number in this message is for indexing to a place name database.

13.5.8.1 SED UID Message Exchange

Examples and guidelines for SED UID message exchange are shown in Table 13.7.

Table 13-7. DAP Message Descriptions.

Example DAP Message Exchange Description		
Activity	Data Content	DAP Action
Incoming Unsolicited Message	Per SCINetEx Protocols. The only unsolicited message received by the DAP is a restricted Status message with the “is unsolicited” bit flag set to true. NOTE: An unsolicited message may arrive at any time due to real-time events in the SED. For example, the DAP may receive an unsolicited message though the DAP last sent a command and expects and ACK. In this case the unsolicited message takes precedence.	Extract originating SED UID from message header. Validate the revision number given in the header and adjust message handling accordingly. If the LTK for the UID at this DAP is not known, use KIM messaging to obtain the LTK and proper message ascension number for transmit and receive. If the UID is already known, retrieve from DAP cache the LTK and ascension numbers. An incoming message to the DAP with an ascension number (originator’s transmit ascension number) that is identical to that last received; the DAP will consider the message as a duplicate. If the message is a duplicate, skip to “send response ACK” below. Decrypt the message. If failure, discard message and send no response. Optionally log locally for diagnosis. Take appropriate database add/modify actions using the decrypted data. Update the Registry data for the device UID, for all relevant Registry data record items.

Table 13-7. DAP Message Descriptions. (Continued)

Example DAP Message Exchange Description		
Activity	Data Content	DAP Action
Incoming Unsolicited Message	The SED ignores the DAP messages except the ACK for the unsolicited message. That is, the DAP's time-coincident command is ignored or lost. The DAP will retry the command if still applicable, using the same transmit ascension number succeeding the DAP's ACK to the unsolicited Status message.	SEND RESPONSE ACK: Prepare an ACK message with the proper transmit ascension number and encryption. Prepare a UDP or TCP packet with the UID of the destination device pre-pended as shown in this section. Transmit the message to the IP address from which the incoming UDP or TCP packet came. The originating SED will retry n times if the DAP's ACK is lost or indecipherable. If retries are exhausted, the originating device will log the error. The DAP itself cannot otherwise determine if the ACK was undeliverable. The DAP will increment the DAP's transmit ascension number and expected receive ascension numbers for the UID in question after the first ACK transmission. All subsequent retransmissions due to duplicate incoming messages will use the same message as the first attempt, including the original ACK's transmit ascension number. The Registry update done by the DAP will have the ascension numbers associated with a successful message exchange, regardless of retransmissions due to duplicate incoming messages.

Table 13-7. DAP Message Descriptions. (Continued)

Example DAP Message Exchange Description		
Activity	Data Content	DAP Action
Incoming Unsolicited Message	DAP command message per Section 4. Commands are restricted (i.e., encrypted) or unrestricted (non-encrypted). Most are restricted. The DAP ACK message is sent as the response to a valid incoming unsolicited message. Every DAP message to a SED has one or more specific response messages. Each incoming (to the DAP) response message is of the same restricted/unrestricted type as the command.	DAP has reason to send an Ad-hoc command to a SED given its UID. DAP retrieves from the Registry the last known IP address for the subject UID. If this is unknown, the command cannot be sent and the process or person is so notified and faults the action. Otherwise, the DAP obtains the LTK and ascension numbers for the subject UID from the DAP's local cache. If that is absent in the cache, the DAP takes either of two courses: 1) The DAP faults the attempt notifying the process or person; or 2) The DAP messages the KIM to obtain a new LTK for the subject UID, performs over-the-air rekeying and ascension number initialization. On success, the DAP updates the Registry data record for that UID, noting the date/time and UID of the DAP doing the rekeying. With proper LTK and ascension numbers for the target UID, the DAP composes a command message and transmits that to the IP address obtained from the DAP's cache or from the Registry. The DAP now times-out the proper response from the target UID. Most often, this is a Status message marked "solicited". The time-out period is 30 seconds. On each time-out, the DAP retransmits the identical message, up to 10 times. When retries are exhausted, the DAP notifies the process or person affected and logs such for diagnostic purposes. The DAP then updates the Registry with the next in sequence transmit and receive ascension numbers, as if the message had been successful. On receipt of a response to the command message, the DAP validates that the UID in the message header is expected and takes appropriate action based on the version number in the header. Next, the DAP compares the ascension number in the message header to the DAP's expected number. If the received number is less than the expected number, message is to be ignored as a duplicate of an irrelevant prior message exchange.

Table 13-7. DAP Message Descriptions. (Continued)

Example DAP Message Exchange Description		
Activity	Data Content	DAP Action
Incoming Unsolicited Message	Timing: The response to a DAP outgoing message may be delayed according to the power conservation characteristics of the target SED. A response may be immediate if the device has sent a prior message within the last two (2) seconds. The worst-case response time is 30 seconds. Longer times indicate a device or network error condition or loss of wireless coverage.	If the received number is greater than the expected number, the DAP logs "lost message" detection for diagnostic purposes and proceeds to decrypt and process the message. The expected ascension number will be adjusted to reflect the lost message(s). If the received or adjusted (for lost message) number is the expected number, the DAP proceeds to decrypt the message. If decryption (which includes a MIC validation) fails, the DAP retransmits the identical command and begins a new response time-out. After 5 re-transmissions, the DAP notifies the process/person affected and logs the error for diagnosis. The DAP compares the one-byte message ACK number in the solicited response to the transmitted command's ascension number's least significant byte. If these differ, the DAP takes the same action as for an encryption error. (The one-byte ascension number for solicited status and for the first solicited event record log.) On successful validation and decryption, the DAP updates the database as appropriate. The DAP then updates the relevant Registry data for the UID. The DAP, for a failed (retransmissions exhausted) or successful message, increments the DAP transmit ascension number for the subject UID. The UID's expected receive ascension number, at this point, is to be one greater than the actual or expected receive ascension number. These numbers will be saved to the DAP's cache.

Table 13-7. DAP Message Descriptions. (Continued)

Example DAP Message Exchange Description		
Activity	Data Content	DAP Action
DAP command yields multiple responses	The DAP command messages that may yield more than one response message are: • Send Log All • Send Log Unsent • AoS Inventory Discovery	DAP determines that the last response of the series has been received. A time-out on receipt of the last response, constitutes a partial loss of data and the appropriate recovery will be taken by the DAP. This may be a retry of the entire message sent or notification of the affected process/person, plus diagnostic logging.

13.5.9 DAP-to/from-Non-secure NG – Error Detection and Correction

Every DAP conforms to the following protocol and parameters in Table 13-8 for error detection and correction.

Table 13-8. DAP Errors.

#	DAP Error Condition	DAP Action
1	When the TCP connection option is used rather than UDP, a connection-closed even if TCP keep-alive fault is detected at the DAP for a given NG.	None. NG (or its proxy) is responsible for error recovery.
2	A DAP-transmitted message has no response.	The DAP enforces a response packet time-out of 30 seconds. The DAP retransmits up to 5 times for error correction. Unsuccessful delivery triggers an automated or manual intervention. The cause may be transport LAN/WAN error, loss of wireless coverage, decryption error or ascension number mismatch. Locally, log the anomaly for diagnostic purposes.
3	A DAP-received security message is invalid. This includes encryption errors, ascension number sequencing, message type versus context and other causes.	Send no response. Locally, log the anomaly for diagnostic purposes.
4	Message ascension number handling (ascension numbers are unique for each SED).	Initial value for transmit and receive numbers after Rekey is 1. See also the effect of rekeying on the ascension number. See Section 9.7.

13.6 DAP-TO/FROM-SECURE NGS MESSAGE EXCHANGE

DAP-to-secure NG data transfers can be accomplished per the following in an unattended manner when the devices are not in use by personnel. This condition provides secure NGs with IP connectivity to DAP(s) directly (cradle) or indirectly via an on-site proxy. In the case of a proxy or terminal server, the data flow from proxy to NG conforms to the DAP IA policy.

13.6.1 DAP-to-Secure NG Retrieval of SED Encryption Key

The secure NG (or its proxy) will obtain the encryption keys for SEDs to which the operator/NG is tasked. The messaging may vary but the means to obtain keys given here applies to all. The DAP has the option to securely commission/arm SEDs via a direct connection through an on-site non-secure FNG if available. This section, however, applies to the use of a secure NG as follows:

- 1 A secure NG, having received a list of SED UIDs and related data/instructions obtains the encryption key to conduct secure data transactions for each SED. This is needed to authenticate and autonomously communicate with the SED.
- 2 The DAP accepts secure File Transfer Protocol (FTP) connections from the secure NG. The DAP authenticates by username/password and logs all connections. The username and password strength is governed by local IA policies.
- 3 The DAP provides a data file on the FTP server for the particular secure NG (or its proxy) that has connected. This is the only file in the login directory. The content of this file is a list of UID-correlated encryption key pairs matching the assignments made by the user in step 1.
- 4 The secure NG (or its proxy) downloads this file via secure FTP connection process and is described as follows:
 - a The SED UIDs in the file are compared to the work assigned list of the SED UIDs previously obtained by the secure NG.
 - b The FTP session now terminates.
 - c The DAP logs this event.
 - d If the list is deemed inaccurate by the secure NG (or its proxy), an exception is alerted to on-site staff for disposition and the secure NG will become idle until re-tasked.

With the downloaded list of UID-correlated encryption keys, the secure NG is able to accomplish the tasking that involves secure data and command transactions for the SED UIDs. SCINetEx defines how the encryption key is stored in the secure NG and how/when this information should be destroyed.

13.6.2 DAP-provided Data Prerequisites

Every secure NG and/or its on-site proxy is provided the following information:

- The UID of each DAP with which the secure NG (or its proxy) performs message exchanges.
- Public network address that corresponds to each DAP UID, this being an edge router/firewall or other IT-defined mechanism for remote access to the DAP server.
- An IP address and server login/password/home file directory. These may be used by automation on the secure NG (or a proxy) rather than by persons. For each secure NG (or its proxy) supported by a given DAP UID, there are login accounts for each specific DAP UID. (The server function may be isolated/outside of the firewalls at a DAP to meet IA policy.)

13.7 COMMUNICATIONS TO COMMISSION/ARM A SED

If a SED is in the coverage of a non-secure FNG with a real-time connection to the DAP, the DAP may use SCINetEx messaging to set baseline information as part of the commission/arm process for a SED after personnel or systemic approvals to do so. Alternatively, a policy/practice-compliant procedure can be used by a secure NG without a real-time connection to a DAP to commission/arm a SED. The balance of this section details the communications for the secure NG alternative. A specific SED is on or in an asset that is selected by the user then made known to the DAP. Therefore, the DAP data includes any baseline information used as part of the commission/arm process. This combined with the secure NG UID and the SED encryption key previously provided by the DAP, enables the commission/arm task to be undertaken with secure commands by the secure NG that require security credentials.

13.7.1 DAP-to-Non-secure NG – Commission/Arm Data

Since the non-secure NG acts as a transparent bridge, the DAP uses the messaging described by SCINetEx to conduct the SED commission/arm sequence using a non-secure NG.

13.7.2 DAP-to-Secure NG – Commission/Arm Data

The following steps are completed prior to securely communicating with a SED for commission/arm action by a secure NG.

- 1 The DAP obtains any asset data fields (such as asset ID numbers, etc...) from the user.
- 2 The DAP obtains a list of asset IDs, and associated with each, a list of one or more secure NG UIDs that is planned to communicate with the SED UID in that asset.
- 3 The DAP obtains from the KIM the LTK for each secure NG UID and SED UID obtained in step 2 above. There may be multiple NG UIDs for one SED UID if the user needs such, e.g., first available secure NG performs the task.

13.7.3 DAP Commission/Arm Information File (CIF)

The DAP uses the data from the steps in Section 13.8.2 to generate one or more Commission/Arm Information File(s) (CIF). The CIF contents include all relevant asset IDs and SED UIDs which secure NGs at a given site will utilize in a restricted time period. The length of this time period is determined by the DAP and local site administrators. The format of a CIF file, given below, enables one file to have the data for one secure NG UID, listing all the assigned SEDs for that secure NG. A different secure NG may also be given the same SED data so that either secure NG may perform the task. A single CIF file can include multiple secure NGs and their SEDs. This may be used by a proxy

to retrieve all data for all secure NGs in one file and de-collate off-line. The choice of CIF file content is a decision coordinated by the DAP and site administrators.

13.7.3.1 Commission/Arm Information File (CIF) Encryption

The DAP formats all CIF file contents for compatibility with agreed upon encryption tools. An example would be the AES-256 FIPS-197 encryption option of the WinZip file compressor software utility. The encryption key/password is referred to as the secure CIF passkey. This passkey is provided and changed by the DAP administrator as needed per local DAP policy, for use by manual and automated processes at sites where secure NGs can be used. The method of this exchange is not defined here-in.

13.7.3.2 Commission/Arm Information File (CIF) Naming

The CIF's validity period commencement is given by the file's name and contents on the line of the file. The file's validity expiration is within the file. The file contains information for one, many or all secure NGs, as agreed to by the DAP and secure NG site administrators.

The file name convention is as follows:

`XXXXXXXXXXXXXXXXXXXX-YYYYMMDDhhmmss.zip`

Where: the character X is X if the file contains XML and T if the file contains TAG-value, for the formats in the next section.

U's are the file-producing DAP's UID as 16 hexadecimal digits.

YYYYMMDDhhmmss is the UTC date/time after which the file is valid (Jan is 01).

13.7.3.3 Commission/Arm Information File (CIF) Contents

The DAP produces two CIF file formats for use by one or a group of secure NGs (or its/their proxy), where the information in each is the same. The secure NG (or its proxy) can choose the file format that is most prudent based on data processing resources.

13.7.3.4 Commission/Arm Information File (CIF) XML Format

The unencrypted content of the CIF is textual XML, the schema is defined in Appendix A.

13.7.3.5 Commission/Arm Information File (CIF) TAG-value Format

This format has the same information as the XML file, but in TAG-value format, with one set of data per line. Each line ends with ASCII CR/LF. If "=" appears in a TAG's value, it shall be escaped with an ASCII backslash.

NOTE: Secure Network Gateway Unique Identifier (SNGUID)

Line 1 is as follows:

DELIM=character, DAPUID=string, EFFECTIVEUTC=string, EXPIRESUTC=string

where the one character to the right of DELIM is the value-TAG delimiter for the file, followed by the character as the first actual delimiter. The DELIM must be a printable ASCII character, e.g., a comma, semi-colon, etc. but shall not be a backslash. An example line 1 is:

```
DELIM=,, DAPUID=0x0102030405060708, EFFECTIVEUTC=20101231000000,  
EXPIRESUTC=20101231235900
```

Line 2 is:

```
SNGUID=value
```

Line 3 is:

```
SEDUID=value,... for the TAG/values in the XML format for a particular SEDUID.
```

For additional SED UUIDs for the same SNGUID, Line 3 is repeated. For a different SNGUID, the content of Line 2 now is given in the file, followed by one or more SEDUID lines (Line 3) for all SNGUIDs and SEDUIDs provided in this file. The secure NG uses the record data which matches both its UUID and the SED UUID in order to be able to conduct secure data and command transactions.

13.7.4 Secure NG-to-DAP Data Transfer

At any time, a secure NG may receive information from SEDs via the SCINetEx protocols. This section defines how that data is communicated, non-real time, to the DAP, when the secure NG is in a condition to communicate with the DAP, e.g., in a cradle or wireless LAN coverage, etc.

13.7.4.1 Secure NG-to-DAP – SED Payload Data

The SED status and/or log data records are conveyed non-real time to the DAP as follows. The secure NG (or its proxy) receives and stores binary data messages as received from the SEDs. All pertinent binary messages are concatenated with no added bytes into one file. The content of each message is decrypted/plain-text form, using credentials for the secure NG-to-SED keying.

This file is encrypted by the secure NG (or its proxy) for the secure NG-to-DAP data file. The file name is the same as for the encrypted file, with the UTC in the file name being the UTC of the final SED communications. The secure NG (or its proxy) transfers the file to the DAP using the same file transfer method in reverse for the DAP-to-secure NG data file. The DAP logs this incoming file and processes its contents according to DAP procedures.

13.7.4.2 Secure NG-to-DAP – NG Activity Log

The secure NG activity log is accepted for upload by the DAP. The file content and format is TAG-value textual as follows:

Line 1: SNGUID=UUUUUUUUUUUUUUUU, UTC=YYYYMMDDhhmmss

Where U's are the secure NG's UUID and UTC is the time/date of the file.

Line 2: SEDUID=UUUUUUUUUUUUUUUU, UID=YYYYMMDDhhmmss

Where U's are the SED's UUID and UTC is the time/date of the last communication.

Line 3: +COMPLETION=x for the SED UUID

Where x is a textual task completion status code, with x=OK if no anomalies.

Line 4: +NOTES:

Operator notes for the SED UID, if any.

Line 5: If present, is another SED UID as in Line 2, followed by the same Line 3 and Line 4.

This file is encrypted by the secure NG (or its proxy) for the DAP-to-secure NG data file. The file name is the same with the UTC in the file being the UTC of the final SED communications.

The file name is as follows:

TUUUUUUUUUUUUUUUUUUYYYYMMDDhhmmss.zip

where `u`'s are the secure NG's UID and `YYYYMMDDhhmmss` is the UTC as in the file's Line 1 content. The secure NG (or its proxy) transfers the file to the DAP using the same file transfer method, in reverse for the DAP-to-secure NG data file. The DAP logs this incoming file and processes its contents according to procedures.

13.7.5 Cellular Data Service Using Embedded NGs

The DAP interface is IPv4-compatible or higher for cellular data service, and able to transport the UDP and/or TCP methods. All messaging protocols and formats are per this section. Cellular providers frequently change the IP address assigned to the mobile device as it does hand-offs between service areas or regulatory domains. The DAP is transparent to this.

NOTE: When TCP is elected for use in DAP messaging, it is common for the carrier to drop the TCP connection due to such cross-domain mobility, as these are not usually tunneled for session continuity, nor may allow the use of mobile IP for IP address persistence. TCP connections can fail frequently with cellular data systems due to RF propagation conditions, hand-off failures and hand-off rejections due to roaming agreements.

The DAP responds to each incoming packet to the source address, though it could change mid-transaction. When UDP is used, these TCP issues are not present. Per SCINetEx protocols, the DAP does not initiate outward connections for TCP. For UDP, the DAP can use the incoming packet's source IP address.

13.7.6 Satellite Service Using Embedded NGs

The DAP interface for satellite communications is IPv4-compatible or higher, and able to transport the UDP and/or TCP methods previously defined by SCINetEx. All messaging protocols and formats are per SCINetEx protocols. The round trip delay in geosynchronous orbit satellite services may reach 0.8 seconds, however this is compatible with SCINetEx principles. For low Earth orbit satellite services, the delay is less.

Section Summary

- Network Gateways may be either secure or non-secure.
- Network Gateways are wireless bridges to WANs.
- All Network Gateways must be commissioned and assigned to a DAP.

14. TEST PLANNING

Testing is an integral part in development of any SCINetEx-compliant system. The primary emphasis of the testing strategy presented here is on assuring the communications link (connectivity) and physical security of data from SCINetEx devices mounted on mobile and fixed assets is passed through the entire SCINetEx system. The SCINetEx devices must also be capable of surviving the environmental rigors specified by the system owner or user requirements.

14.1 PROBLEM STATEMENT

14.1.1 Motivation

The intent of this test planning section is to provide a notional construct for evaluating SCINetEx devices and integrated systems under laboratory, field and operational conditions, to characterize security efficacy, performance characteristics, reliability, vulnerability, interoperability and operational concepts. Testing will be conducted to determine if the selected SCINetEx components and sub-systems perform consistent with the technical requirements of the system users and governing entity under operational conditions. Each system component should be evaluated on its effectiveness in addressing the requirements, inclusive of the following categories:

- Bi-directional communications
- GPS location (required for devices mounted on mobile assets)
- Physical interfaces (installation and operation on fixed or mobile assets)
- Operating considerations (including environmental conditions and power supply)
- Security

It is recommended that testing be conducted in at least three phases, with each phase building upon the previous one, focusing on a different aspect of the attributes to be tested, and being conducted under more realistic conditions as the effort progresses.

14.1.2 Conceptual Model

In order to understand the environmental influences on the function of SCINetEx devices, it is important to understand the environment in which SCINetEx will exist. SCINetEx components must be designed to endure the conditions of the owner/user-defined environment as well as perform its primary function of reliably monitoring asset state changes, providing wireless communications and GPS location as required. It is recommended that the system developer/implementer adopt a “build a little, test a little” approach to testing to ensure that small design issues are not propagated into larger design issues.

The core elements of the requirements for a SCINetEx system are defined by the system owner/user. A fully developed SCINetEx device should integrate into the current owner/user infrastructure without impacting on-going operations to the greatest extent possible. Development of a conceptual model (usually in graphical or pictorial form) is useful to present a general overview of system desired end-state architecture. It is important to realize that this high-level overview does not

need to include all of the factors that will influence the functions of the SCINetEx system, but is provided to list examples of factors that will be considered during testing. These factors commonly include such things as:

- Shock and vibration
- Shearing forces and container racking
- Weather
- Climate changes

The SCINetEx device must be able to endure these forces while being able to reliably provide wireless connectivity. While an asset is in use, SCINetEx will also interact with several types of personnel with close proximity to the asset. These personnel include:

- Asset owners and operators
- Supplier personnel and factory personnel
- Transport crews
- Trade, law enforcement and international authorities
- Malevolent individuals (such as criminals or terrorists)

The roles of these actors vary widely as will their intended interactions. Some of these actors will need limited access to SCINetEx bi-directional communications features, such as the ability to pass arm commands to the asset-mounted devices or gather statistics. Other users will need access to a wider feature set. The personnel listed above may have access to SCINetEx devices including:

- Smart End Devices
- Network data interfaces
- Owner/user Data Aggregation Points
- Key Information Managers
- Other systems that personnel have access to may be able to influence or interact with SCINetEx. These systems may include:
 - Database management systems
 - Cryptographic key systems
 - Accounting systems
 - Vendor software suites
 - Other management systems

Again, this list of factors is not meant to be exhaustive, but is provided to highlight some of the factors that will be considered during testing.

14.2 THE OPERATIONAL ENVELOPE

Due to the risk of malevolent cyber activities, it is very important to increase the security of critical network components including network extenders. The communications and tracking solution that is described in SCINetEx should be the correct tool for the job and should be deployable in all conceivable operational environments. Before SCINetEx devices are tested as a communications solution for any application, it must be shown that SCINetEx is suitable for the task. To be so,

SCINetEx must be deployable and operable to ensure that SEDs forward data to Data Aggregation Points appropriately. The following addresses each of these issues:

Correct tool for the job: A communications system supporting a sensor that can reliably detect state changes in fixed or mobile assets as well as help detect and alert cognizant authorities to address metering, monitoring and control issues in autonomous systems.

Deployable in operations environment: SCINetEx devices must be robust enough to do what they were designed for in the anticipated asset environment.

Limits of communications technology: SCINetEx devices are intended to provide wireless connectivity between SEDs and public information networks. It may be possible (through some inherent characteristic of the communication system in some environments) for a cyber-threat to be perpetrated by an unauthorized user. The communication systems limitations should be assessed to determine if it can provide sufficient security and accomplish its intended task in spite of its limitations.

14.3 TEST CONDITIONS AND DEGRADATION FACTORS

Test conditions will encompass situations from laboratory to the operational field environment. The first phase of testing (Phase I) will be conducted in a controlled laboratory environment, including initial documentation and device reviews, bench testing, functional testing and environmental testing in laboratory equipment, use-case evaluations, trial installations, security evaluation, defeat testing and red teaming. The suite of tests conducted on SCINetEx technology will cover the range of likely conditions the device(s) would experience in its anticipated application, whether they are environmental conditions, usage conditions or even attacks. These early tests are meant to determine the likelihood of a device performing as expected under actual operating conditions. Later tests, in Phases II and III, will place the devices in actual use conditions, subjecting them to a subset or range of actual operating conditions. These later tests are intended to determine if the device can function as intended within the established infrastructure without negatively impacting owner/user operations, as well as endure real world conditions and extreme operating conditions likely to cause performance degradation of the device. Such conditions are known as degradation factors.

Degradation factors are conditions or procedures that will exist in operational conditions that could render the performance of the communications system to be less than owner/user specifications. These factors can be related to elements such as installation, environment (fog, wind, darkness, etc.), procedures (failing to test after maintenance, etc.) or anything else that could degrade the performance of the system. At the discretion of the test team, additional testing of proposed degradation factors can be performed to determine how significant the factor is or how sensitive a particular make/model is to the degradation factor.

Degradation factors may also affect the ability to defeat a device. For example, a SCINetEx device may operate abnormally when subject to temperatures approaching the extremes of the required operating range. Defeat testing may exploit vulnerabilities exposed by degradation factors. Defeat testing may attempt to qualitatively compare defeat methods and degradation factors. Not all degradation factors are useful to an adversary for all defeat methods. An attempt may be made to capture the relationship between degradation factors and defeat methods, that is, which degradation factors will help an adversary with which defeat methods. Some degradation factors may have broader impact on the system, device and/or communications performance than others. Testing that includes degradation factors may be conducted during functionality and performance tests as well as during defeat testing and red teaming. In general, if testing is performed under ideal conditions, this should

be noted. All test results should clearly explain the conditions under which those tests were performed.

14.4 TEST OBJECTIVES AND HYPOTHESES

Test plan construct:

This can be used to test SCINetEx technology as a three-phase testing effort. For testing, the phases are:

Phase I: Initial device overview, Laboratory testing and Vulnerability testing.

Phase II: System level performance/Demonstration testing in domestic trade lanes, at least in representative operational conditions.

Phase III: System level performance testing under actual operational conditions.

Goal of these tests:

The goal will be to test all hypotheses and objectives listed in this section. The following is an overview of the objectives of each phase:

Phase I: is basic sensor characterization, bench testing of both functional and performance characteristics, (potentially destructive) environmental survivability testing, defeat testing and execution of vulnerability scenarios (red teaming), using at least ten (10) devices per developer.

Phase II: is system (sensor and communications) testing in representative operational environment observing not less than one hundred (100) monitored asset state changes and other criteria developed by the test organization.

Phase III: is system (sensor and communications) testing in the actual operational environment of the owner/user observing not less than one thousand (1,000) monitored asset state changes and other criteria developed by the test organization.

Decision points are built into the process to eliminate unqualified devices and reduce testing expenses. Assessments of device usability, device functionality, device performance, susceptibility to defeat and suitability for the owner/user-defined environment, along with recommendations on the data gathered during testing, will be provided in a report at the end of each phase. The owner/user will then determine which devices will continue on to the next phase of testing. Each assessment will identify operational and functional deficiencies, failures and device vulnerabilities that could eliminate the need for further testing. The first decision point is built into the initial overview with other decision points at specific locations in Phase I, Phase II and Phase III. In all cases, a decision point occurs at the end of each phase or sub-phase.

14.5 OBJECTIVES

Usability: How practical the device is to install and use; fitness or readiness for use or service.

- Is the device realistically usable (based on its physical configuration, general construction, installation and operational requirements) in the owner/user-defined environment?
- Are the communications offered practical for use in the owner/user-defined environment?

Functionality: The utilities or behaviors that are offered to the user; the functions that the device should provide.

- Does the device perform the basic required functions for communications?
- Does the device perform location and tracking using GPS?
- Does the device have basic security functionality?

Performance: How well a device performs its required functions; the accomplishment of a task to a preset standard of completeness and accuracy.

- Does the device meet the data recording, communication mode selection, GPS location and power management needed to operate in the owner/user-defined environment?
- Can the device survive the environment to which it will be subjected (forces, environment and interference)?

Security: Measures taken as a precaution against theft, espionage or sabotage; ensuring the integrity, confidentiality and availability of the system and its associated data.

- Does the device adequately protect data against a malevolent threat from a program-specified level of adversary?
- Does the device provide an effective security solution (assessed through defeat testing, red teaming and risk assessment when testing in an operational environment)?

14.6 HYPOTHESES

For each phase of testing, the focus is on a variety of hypotheses, dictated by the objectives of that phase. The tests themselves are characterized according to the type of test (physical, functional, performance, security), which map directly to the evaluation criteria (usability, functionality, performance, rate of failure, security). The hypotheses are listed as pairs which cover all possible outcomes. The first is called the null hypothesis (denoted as H_0) and the second is called the alternate hypothesis (denoted as H_A). The null hypothesis is the desired hypothesis and testing must be performed to determine which of the two hypotheses is true. The hypotheses are intended to be thorough, but they may vary based on the design of the device being tested. Example hypotheses are detailed in Appendix B. Hypotheses in Appendix B are grouped according to which aspect of the overall SCINetEx test program they address.

The hypotheses are addressed in Appendix B are as follows:

Phase I

- Usability hypotheses

Hypothesis 1 for qualitative and quantitative evaluation

Hypotheses 2 and 3 for qualitative evaluation

- Functionality hypotheses for qualitative and quantitative evaluation
- Performance hypotheses for qualitative and quantitative evaluation
- Rate of Failure hypotheses for qualitative and quantitative evaluation
- Security hypotheses for qualitative and quantitative evaluation

Phase II

- Usability hypotheses for qualitative evaluation
- Functionality hypotheses for qualitative evaluation
- Performance hypotheses for qualitative evaluation
- Rate of failure hypotheses for qualitative evaluation
- Security hypotheses for qualitative evaluation

14.7 EXPLORATORY DATA

Data that needs to be obtained includes a determination of security requirements and (as close to complete as possible) characterization of the forces, environmental conditions and interference SCINetEx devices may experience in the owner/user-defined application. In order to be certain that the ranges of conditions to which the devices are tested are reflective of those actually experienced in the owner/user-defined application, separate endeavors which include the gathering of that data should be undertaken in advance. The basic measurements that should be included are temperature, shock, vibration and humidity. In addition, Finite Element Modeling and Analysis (FEMA) can be performed for shock drop conditions on containers with results confirmed by conditions observed in the field and actual drop tests performed, respectively. These conditions then apply to SCINetEx components that are installed on any mobile or fixed asset. The owner or governing entity should refine these conditions to reflect the application.

14.8 DATA NEEDED TO TEST THE HYPOTHESES

In order to test the hypotheses, numerous types of data must be gathered. The data will be used to test the hypotheses and determine which hypothesis from each pair is the correct one. Below are examples of data that may be used to prove or disprove the hypotheses from each of the four (4) categories.

Data needed to test usability hypotheses include:

- Physical attributes of device (size, shape, material, etc.)
- Installation requirements (including location) of device
 - Form and fit for use
 - Mounting/retrofit requirements
 - Interference with normal asset functions
 - Interference with other relevant infrastructure
- Suitability for application
 - Interference with shipping/handling process
 - Usage requirements of system (including communications)
 - General construction (obvious defects or shortcomings)
 - Environmental survivability (general evaluation)

Data needed to test functionality hypotheses include:

- Communications (to IEEE Standard 802.15.4-2006; data and command packet message structure and data formats; Network Gateway communications pathways, communications mode selection, protocols and configurations; data transfer protocols and packet configurations; data configuration, encryption, protocols and command structures and execution)
- Passing status, commands and response to commands
- Data and message encryption capability
- Ability to log GPS and location information
 - Basic acquisition technique
 - Functional measurement of impairments

Data needed to test performance hypotheses include:

- Characteristics of communications (stationary and in-motion, between SCINetEx device and Network Gateway)
 - RF characteristics: i.e., frequency, power, spectrum
 - Read/communicate characteristics: i.e., range, orientation, pattern, speed
 - Compliance/compatibility with existing international treaties and national laws on frequency usage
 - Licensing requirements
 - Human safety review
- Operational environment effects
 - Environmental conditions
 - In-situ communications evaluation and effects
 - System duration

- Resistance to environmental factors
 - Temperature and humidity
 - Shock and vibration
 - Precipitation
 - RF
 - Radiation
- Clock and GPS accuracy (particularly with respect to processing latency and alarm detection)
- Performance of communications (stationary and in-motion) including speed, reliability, security, interference and multi-path
- Component stability
- Quantitative system characteristics, which include distance to read, download speed and multiple SCINetEx device effects
- System reliability and durability
- Power requirements
 - Power consumption during hibernation (idle)
 - Power consumption during use
- Failure modes
- Operational considerations
 - Multiple SCINetEx device interference
 - Multiple impairment interference

Data needed to test security hypotheses include:

- Conceptual defeat scenarios (examples of how an owner/user-specified level of adversary could defeat the device)
- Defeat demonstration and/or testing of conceptualized scenarios
- Red Team assessment of device
- Resistance to system spoofing
- Resistance to message overload
- Resistance to device reset or re-programmability
- Protection from diminished availability, modification of data or viewing of data by an owner/user-specified level of adversary
- Existence of communications/cyber vulnerabilities

14.9 ABORT CRITERIA

Abort criteria may cause testing to be discontinued for a particular device at the discretion of the test team or program manager. Abort criteria are considered at key decision points during testing, which occur at the end of each phase or sub-phase. At the end of each phase, a decision must be made by the test team about whether or not to move on to the next phase of testing. In rare cases, abort criteria may cause testing to halt before the end of a phase. Existence of any of the following abort conditions will not necessarily cause a device to be excluded from further consideration, but their existence will be taken into account, along with results of the tests performed during each phase, when deciding whether or not to move on to further testing. The following are some abort criteria for each of the different categories of tests:

Usability

- Cannot fit on the asset without great interference with asset operation.
- Use of device may cause damage to asset.
- Device size and/or weight constitutes dangerous installation conditions.
- Device is wide open to the environment (is still in the “bread-board” prototype phase of development).
- Installation in fixed location causes substantial interference with operations at that locale.

Functionality

- Cannot reliably communicate with handheld or fixed Network Gateways.
- Allows no method of getting device status or communicating with the SED for arming/disarming.
- Device power insufficient for intended use.
- Cannot provide GPS location data.

Performance

- Cannot operate in owner/user-defined application environment.
- Cannot withstand the shock, vibration, temperature extremes, corrosion and handling impacts involved.
- Major vulnerability in communications technology implementation.

Security

- Can be defeated by a program-specified level of adversary.
- Does not protect data from unauthorized access or modification.
- Does not protect device availability from being diminished by an owner/user-specified level of adversary.

14.10 DATA ANALYSIS FRAMEWORK

This section gives details on how analysis of the data may be conducted. As an alternative to actual physical tests, modeling or analysis can be used if it proves to be in the governing entity's interest (for example, if it is more cost effective to do so than conduct actual tests). Potential methods for computing values and mathematical modeling are described below.

Mathematical models

- Reliability analysis, including component-level modeling, may be used as part of the analysis of the devices. This type of analysis will play a critical role in developing justifiable conclusions, and recommendation for future system improvements, from field tests.

Statistical methods

- ROC (Receiver Operating Characteristic) curves

Parameters of interest (for each device/system)

- Meantime to message latency
- Mean battery life
- Probability of critical failures
- Usage and maintenance impact
- Non-numeric/qualitative
 - Any impact on existing shipping infrastructure
 - Any impact on or amendment required to user-defined CONOPS
 - Defeat-resistance and tamper-resistance

All data obtained will be compared to existing standards and to any data obtained as to conditions experienced in the operational environment under adjacent efforts in gathering of data on the operational environment.

14.11 EVALUATION CRITERIA

After a phase has been completed for a device and a decision point has been reached, an evaluation will be made regarding its suitability for use. This evaluation may include a recommendation from the test team regarding whether or not the device should be considered for deployment. The evaluation of the device will be based on the following criteria:

- Critical factors (summation of results of a phase of testing with particular emphasis on the key areas listed for abort criteria)
- CONOPS (verifies that the owner/user implementation is consistent with security needs and that the system use will fit within the application)
- Configuration control
- Testing history
- Maturity of technology and quality of design (mechanical, electrical and functional aspects of the design)
- System design and characteristics relative to CONOPS and operational scenarios

- Adequacy of documentation
- Ability of devices and procedures to perform in the manner intended
- Human factors
- Overall security effectiveness

14.12 TEST DESIGN OPTIMIZATION

The test and evaluation effort will be optimized by conducting multiple phases (Phases I and II, nominally) carefully designed to maximize data output and minimize redundancy, while constructively contributing to the decision points built into each phase. This approach should include, but is not required to include, the data collection and testing described in this section, as applicable to the particular device and technology being evaluated. The decision points, utilized along these phases, are built into the plan to eliminate unqualified devices. Optimization with flexibility provides the opportunity to adjust the testing order yet still acquire sufficient data to reach an informed decision. For this testing, the owner/user will review the documentation, may request additional data, and will conduct testing to verify compliance with requirements.

14.13 DATA TO BE COLLECTED

Phase I No less than ten (10) asset-mounted SCINetEx devices of each type and no less than three (3) NGs of each type (handheld and fixed) per vendor to be reviewed.

- Vulnerability assessment synopsis.
- Measurements of dimensions and weight of main components of the system.
- Inspection and assessment of main system components for form and fit, within or on the exterior of the container and the general shipping industry environment and practices.
- Inspection and assessment of the main system components for general construction for consistency with good engineering practices.
- Inspection and assessment (based on knowledge of the expected operating environment) of the main component's general environmental survivability.
- Inspection and evaluation of the system's capabilities in the following key areas:
 - Location data storage and retrieval
 - System commands/response structure and implementation
 - Communications (RF and read characteristics, compliance/compatibility with frequency laws, licensing requirements, human safety, speed, reliability, security, interference, multi-path)
 - Failure modes
 - Security features (encryption, tamper-evidence)
 - Power requirements
 - Environmental resistance and performance
 - ◆ Temperature – simulated extreme hot and cold (thermal shock) as well as cyclical
 - ◆ Humidity – simulated marine environment/conditions
 - ◆ Shock – simulating handling drops, container drops and asset shocks

- ♦ Vibration – representative of transportation modes
- ♦ Salt mist – simulated marine weather environment/conditions
- ♦ Rain – simulated marine environment/conditions
- ♦ Impacting water – simulated waves or washing
- ♦ Frost and ice – simulated cold weather conditions
- ♦ Corrosion
- ♦ Sand and dust
- ♦ Fungus
- ♦ Electromagnetic emissions
- ♦ Electromagnetic susceptibility – interference from external sources
- ♦ Static electricity – simulated electric contact discharge
- ♦ Lightning – simulated lightning strike nearby
- ♦ Radiation – simulated conditions representative of current inspection technologies

Phase II One hundred (100) moves in operational field test environments, with the number of devices to be used determined on a vendor-by-vendor basis.

14.14 TEST PLAN EXAMPLE CROSSWALK

The outcome of each phase will depend upon the aggregation of all of the hypotheses evaluated during that phase. For each hypothesis, there is a subset of tests and evaluations that generally address the outcome. The evaluation of each hypothesis will have a conclusion, stemming from the outcome of the tests and evaluations conducted to verify the hypothesis, and those conclusions will feed into the aggregate for the phase. The test and evaluation team will use all of the previously mentioned data and conclusions, in conjunction with each team member's technical experience, to make an informed engineering decision as to the results of that phase. Crosswalks are useful tools for organizing this information. An example crosswalk developed by the Department of Energy for testing the SCINetEx system and components is as shown in Table 14-1 to Table 14-5.

Table 14-1. Usability Hypotheses.

Usability Hypothesis	Evaluation	Documentation
Item 1 Physically workable (device size, weight and shape)	Phase I – Physical Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Physical Qualitative	
Item 2 Installation	Phase I – Physical Qualitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Physical Qualitative	
Item 3 Communications workable	Phase I – Physical Qualitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Physical Qualitative	

Table 14-2. Functionality Hypotheses.

Functionality Hypothesis	Evaluation	Documentation
Item 1 Radio Frequency (RF) general technical requirements	Phase I – Functional Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Functional Qualitative	
Item 2 Cellular Communications general technical requirements	Phase I – Functional Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Functional Qualitative	
Item 3 GPS general technical requirements	Phase I – Functional Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Functional Qualitative	
Item 4 Tracking and Geo-fencing system general technical requirements	Phase I – Functional Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Functional Qualitative	
Item 5 Satellite Communications general technical requirements	Phase I – Functional Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Functional Qualitative	
Item 6 MLS general technical requirements (e.g., asset monitoring)	Phase I – Functional Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Functional Qualitative	
Item 7 Receives and forwards status, commands and responses	Phase I – Functional Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Functional Qualitative	

Table 14-2. Functionality Hypotheses. (Continued)

Functionality Hypothesis	Evaluation	Documentation
Item 8 NGs provide required functions	Phase I – Functional Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Functional Qualitative	
Item 9 Required security and encryption	Phase I – Functional Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Functional Qualitative	

Table 14-3. Performance Hypotheses.

Performance Hypothesis	Evaluation	Documentation
Item 1 Minimum NG communication range for specified mounting heights	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 2 Minimum communication range to HNG of 0-10 feet (3.05m)	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 3 Minimum cellular communication connectivity requirement	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 4 Minimum overall communication requirement for mode selection and prioritization	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 5 GPS location accuracy; no less than 40ft while on a stationary asset	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 6 TGPS location and accuracy and geo-fencing; no less than 40ft while on a moving asset	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	

Table 14-3. Performance Hypotheses. (Continued)

Performance Hypothesis	Evaluation	Documentation
Item 7 Cellular communication connectivity while on an asset moving at TBD	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 8 MLS provides sufficient physical security for bonded cargo	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 9 Operates in / survives the environmental conditions in the Trade Lanes	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 10 Operates in / withstands the temperature and humidity conditions in the Trade Lanes	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 11 Operates in / withstands shock and vibration conditions in the Trade Lanes	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 12 Operates in / withstands precipitation conditions in the Trade Lanes	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 13 Operates in / withstands RF conditions in the Trade Lanes	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 14 Operates in / withstands potential radiation that may be in the Trade Lanes	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 15 Meets SOLAS 11-2/19.3.2 requirements	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	

Table 14-3. Performance Hypotheses. (Continued)

Performance Hypothesis	Evaluation	Documentation
Item 16 Power requirements threshold and/or goal	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 17 Rate of Failure threshold and/or goals	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 18 Cost requirement threshold and/or goal	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	

Table 14-4. Rate of Failure Hypotheses.

Rate of Failure Hypothesis	Evaluation	Documentation
Item 1 Threshold of 1 RtF per 1,000 attempts to associate	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	
Item 2 Goal of 1 RtF per 1,000 attempts to take GPS read	Phase I – Performance Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Performance Qualitative	

Table 14-5. Security Hypotheses.

Security Hypothesis	Evaluation	Documentation
Item 1 Reliable and robust technology	Phase I – Security Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Security Qualitative	
Item 2 Program code cannot be modified, replaced or deleted, other than by the manufacturer	Phase I – Security Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Security Qualitative	
Item 3 Tamper-evident mechanisms	Phase I – Security Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Security Qualitative	
Item 4 Component interfaces security requirements	Phase I – Security Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Security Qualitative	
Item 5 Defeat by a specified level of adversary	Phase I – Security Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Security Qualitative	
Item 6 Data stored in or passed through SCINetEx cannot be accessed by a specified level of adversary	Phase I – Security Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Security Qualitative	
Item 7 Device availability cannot be diminished by a specified level of adversary	Phase I – Security Qualitative and Quantitative	• Test Plan • Identify Requirement • Identify item
	Phase II – Security Qualitative	

Section Summary

- Testing is an integral part of developing SCINetEx system components.
- The areas of testing are Usability, Functionality, Performance, Rate of Failure and Security.

This page intentionally left blank.

15. SCINETEX RED TEAM TEST PROCESS

15.1 INTRODUCTION

Red teaming is the process of aggressively testing the security posture of networks and systems using benevolent adversaries as a form of “ethical hacking”. Red Teams ideally represent the capabilities of the most likely or worst case malicious adversary that may attempt to disrupt or undermine the effectiveness of the deployed system. The key to effective red teaming any system is to clearly define what tools, information and resources the malicious adversary will have at their disposal and replicating those capabilities during the red teaming process. For a system like SCINetEx, the Red Team should routinely perform assessments during the development and early integration of the SCINetEx devices and subsystems using a “build a little, test a little” strategy. A Red Team assessment is an evaluation that makes use of consequences, adversarial level and successful exploitation of identified vulnerabilities. Red Team testing is performed from the perspective of an attacker with malevolent intentions. There are at least six (6) steps in the standard red teaming process that are described in more detail below. There should also be at least two (2) decision points in this process where it must be determined whether to continue to the next step in testing or not.

An in-depth Red Team test can build on an initial defeat test, which takes place during the first two steps of red teaming. Defeat testing is usually restricted to one vulnerability or consequence path with the highest probability of success. An in-depth Red Team, which pursues multiple attack paths, is allowed a greater amount of time and resources. Although the specific tests performed during red teaming are not predetermined and are based upon the technologies used, there are defined processes for selection and validation of these tests. Some of the goals of red teaming are to identify multiple attack paths graded by level of adversary, identify critical points of failure and identify the strengths and weaknesses of a system. The results of these tests allow for a better understanding of the risk associated with the corresponding device or system. Results of Red Team tests can also be used by the owner or governing entity to better understand the posture of SCINetEx system security as well as provide feedback to industry for improvement of the system design.

15.2 RED TEAM METHODOLOGY

According to the Information Design Assurance Red Team (IDART)[™] methodology developed/utilized by the US Department of Energy (DOE), red teaming consists of six (6) steps: Planning, Data collection, Characterization, Analysis, Reporting and Demos and Experiments. More detail on each of these steps, much of which was taken from the IDART[™] website, is described below.

15.2.1 Planning

During the planning phase, the Red Team seeks to bound the assessment problem, understand the threat space of concern and understand the significant mission of the information system in order to understand what adversary goals might be attempted.

15.2.2 Data Collection

The data collection phase is typically done in cooperation with the owner/user of the SCINetEx system to reduce the time spent in discovery and to enhance the effort spent on analysis of the system architecture. Open-source information and owner/user-provided information are used to gain a better system understanding. When directed by the owner/user, social engineering techniques may be used to collect data. Defeat testing will be done during this step as well.

Defeat testing is a subset of red teaming and usually occurs during the first two phases of an in-depth Red Team evaluation. The purpose of defeat testing is to identify high consequence, easily exploitable vulnerabilities. It is designed to find a simple attack that will circumvent a critical component or function of the system.

Defeat testing is performed using limited time and resources that are expected for the malicious adversary, a defined number of staff and a limited amount of development time. It provides data collection, introductory views and system understanding for the in-depth red teaming. Upon discovery of one defeat, defeat testing could be considered successful; however, the defeat test guidelines specify formal repetition of tests to provide a more comprehensive understanding of the limits of the vulnerability. At the conclusion of a defeat test, a decision must be made about whether or not to proceed with the rest of the Red Team investigation.

15.2.3 Characterization

The SCINetEx system under study is characterized according to several viewpoints in an effort to identify and understand single points of failure or high value nodes, or by passable security controls. Views may include physical views, logical views, functional views, network views, device views, lifecycle views, data flow views, protocol views and temporal views.

15.2.4 Analysis

The Red Team analyzes the viewpoints and the system for weaknesses or vulnerabilities that, when exploited by an adversary, would permit them to achieve malevolent adversary goals. This analysis is performed to the depth and breadth specified by the owner/user. This phase includes an attack brainstorm and attack graph generation. After this graph is generated, a decision must be made about whether or not to continue testing by validating any of these attacks.

15.2.5 Report

The analysis results are recorded in a report that is delivered to the owner/user of the SCINetEx system and includes detail on the techniques used against the system. This includes the contents of the attack graph. If further testing is recommended, one or more attacks may be implemented to verify their effectiveness, and the results of these tests will be added to the report as well.

15.2.6 Demos and Experiments

If required, additional analysis and demonstration of attacks can be performed under controlled conditions or experiments can be developed to test hypotheses about system performance under adversarial conditions. If further testing is recommended after the attack graph is generated, this step can be used to validating potential attacks.

15.3 SCINETEX DEFEAT TEST GUIDELINES

15.3.1 Objective

The purpose of a defeat test is to determine if a SCINetEx device can be defeated by an adversary within a minimal budget. The information obtained will be helpful in identifying how difficult it is to defeat SCINetEx devices, the necessary capabilities of an adversary to complete the defeat and the amount of time and effort required to accomplish the defeat. Defeat testing is the primary focus in the Red Team process and provides a decision point on whether to pursue additional red teaming which would consider a more sophisticated adversary as well as additional consequences of concern, such as an undetected alarm or tampered log record files. Defeat testing is designed to:

- Explore potential vulnerabilities.

- Determine if a SED can be defeated by an adversary within a minimal budget.
- Identify a high consequence vulnerability that can be exploited by a low to medium level adversary.
- Identify attributes of the attack such as the amount of time and effort required to accomplish the task.

15.3.2 Goals of the Defeat Test Guidelines

The defeat test guidelines provide a process that will:

- Give a description of the resources necessary for an adversary to accomplish the defeat test.
- Create consistency in defeat test preparation, formal testing and documentation.

15.3.3 Process

The major steps in the defeat testing process are:

1. Phase IA Screening

- Attended by members of the Interdisciplinary Planning Team (IPT).
- Obtains recommendation to continue with Phase IA/B defeat test and suggestions for direction of testing.

2. Defeat Mechanism Brainstorm

- Kick-start from Phase IA screening discussion and published results.
- Develop postulated defeat methods.

3. Develop a Defeat Test Determination Matrix

(a tool used to determine which attack(s) to pursue)

4. Defeat Mechanism Development

- Develop a test plan.
 - Identify and record goal of defeat test.
 - Determine which defeat(s) will be developed.
 - Determine and acquire necessary resources.
 - Use tools that can be constructed or purchased by the chosen level of adversary.
 - Execute preliminary tests to prove concept (develop attack).
 - Refine process and tools.

5. Execute a Formal Test

- Independent observation (honest broker).
- Stop watch timing.
- Use of data sheets to record results.

6. Videotape the Final Defeat Method

- This may be done as the formal testing, but may be done at another time to mitigate the impact of the camera's presence on defeat tests results.

7. Complete Report

- A detailed technical report is generated that documents the methodology and the results obtained by the Red Team during testing.

15.3.3.1 Guidelines

Each SCINetEx device test should adhere to a set of guidelines and procedures as determined by the Interdisciplinary Planning Team (IPT). In the event this is not possible, any exceptions will be documented and explained. The adversary role being represented should have at most a moderate capability for defeat development and low to moderate capability for defeat execution.

15.3.3.2 Constraints

The bounds of the defeat test are primarily driven by overall budget limits on resources for the attack and level of adversary. Other boundary conditions are:

- Threat can represent either an insider or outsider.
 - Successful outsider attacks are usually considered a more serious vulnerability.
- Partially destructive tests will be avoided.
 - If a postulated destructive attack/vulnerability is considered serious, it will be reported as such.
- Modification of a device and/or asset to which it is mounted are within bounds (see second bullet).
- A set attack target price is the theoretical cost to duplicate the resources (tools, materials and services such as machine shop time) that an adversary would require to execute the defeat attack.

15.3.3.3 Documentation

To meet tight schedules and budget constraints, documentation can be done in parallel with the defeat test phases, expediting availability of test results.

15.3.3.4 Testing and Learning Period

Each defeat test team will be given approximately one week to perfect the defeat mechanism process. Variability is expected based on availability of resources. After this characterization and development period, a formal defeat test will be executed for data collection.

15.3.3.5 Test Execution Guidelines

Each test will be performed multiple times. The team lead is expected to minimize variability to a reasonable extent, trying to maintain consistency in level of adversary and resources between defeat tests. This is helpful for drawing conclusions about the overall success rate of a defeat.

Once the formal defeat test has been started:

- The following information will be recorded for each test:
 - Discrepancies or events that influence the outcome of the test sequence.
 - Time it takes for each attack.
 - Success or failure for each attack.
 - Serial number (or unique IDs) of device(s) used for testing.
 - Serial number (or unique ID) of the asset used for testing.
 - Person(s) who performed test.
 - List of tools used.
- Test will not be interrupted or restarted due to lack of success on the part of the adversary.
 - In the event of equipment failure, extreme weather or other catastrophic events, the test may be rescheduled and started over.
- Each test will be done thirty (30) times.
 - Exceptions for time intensive tests will be documented and explained.
- Videotape of the final defeat method.
 - This may be done at the formal testing, but may be done at another time to mitigate the impact of the camera's presence on defeat tests results.

Section Summary

- Red Team using DOE IDART™ methods are recommended.
- An Interdisciplinary Planning Team (IPT) is utilized to screen Red Team strategy.
- SCINetEx system owner/user defines the level of adversary.

This page intentionally left blank.

APPENDIX A

COMMISSION/ARM INFORMATION FILE

XML SCHEMA FORMAT

A.1 OVERVIEW

Appendix A has the unencrypted content of the CIF in textual XML schema. The secure NG UID is always unique within one CIF where XML data elements are detailed in this Appendix.

A.2 XML DATA ELEMENTS

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs=http://www.w3.org/2001/XMLSchema>
  <xs:element name="DAPUID" type="xs:string" />
  <xs:element name="VALIDITY">
    <xs:complexType>
      <xs:element name="EFFECTIVEUTC" type="xs:string" />
      <xs:element name="EXPIRESUTC" type="xs:string" />
    </xs:complexType>
  </xs:element>
  <xs:element name="SNGUID">
    <xs:sequence>
      <xs:element name="SEDUID" type="xs:string" />
      <xs:element name="AssetIDTypeCode" type="xs:string" />
      <xs:element name="AssetID" type="xs:string" />
      <xs:element name="SecondaryID" type="xs:string" />
      <xs:element name="TertiaryID" type="xs:string" />
      <xs:element name="LTK" type="xs:string" />
      <xs:element name="RKK" type="xs:string" />
      <xs:element name="RKC" type="xs:string" />
      <xs:element name="AUX" type="xs:string" />
    </xs:sequence>
  </xs:element>
</xs:schema>
```

A.2.1 XML Data Elements Parameters

From the XML data, the parameters are as follows:

DAPUID: conveys the UID of the DAP producing this data.

EFFECTIVEUTC and **EXPIRESUTC:** are strings as: YYYYMMDDhhmmss in UTC date/time (Jan is 01), depicting the validity time period for the file's contents.

SNGUID: conveys 16 hexadecimal digits being the 8 byte UID of the secure NG (NG UID) to which this record applies.

AssetIDTypeCode: conveys two hexadecimal digits being the asset ID and check characters.

SecondaryID: conveys the alphanumeric second ID.

TertiaryID: conveys the alphanumeric third ID.

LTK: is the 16 hexadecimal digits depicting the Long Term Key as 8 bytes.

RKK: is the 16 hexadecimal digits depicting the Rekey key as 8 bytes.

RKC: is the 16 hexadecimal digits depicting the Rekey count as 8 bytes.

AUX: is zero or more alphanumeric data character strings, separated by commas.

The DAP provides the encrypted CIF to secure NGs (or their proxy) via a means not defined in this technical report, e.g., FTP, email, HTTP server, etc. On receipt, the secure NGs (or their proxy) decrypt and place in secure storage, the XML or TAG-value records. The secure NG (or its proxy) then extracts that data and ensures that each secure NG has the records pertinent to the secure NG. The secure NG will use the record data which matches both its UID and the SED UID in order to be able to conduct secure data and command transactions.

APPENDIX B

HYPOTHESES EXAMPLES

B.1 OVERVIEW

Hypotheses examples are provided in this appendix for five areas: usability, functionality, performance, rate of failure, and security, see Sections B2.2.1–B2.2.5.

B.2 HYPOTHESES TEST STRATEGY OBJECTIVES BREAKDOWN

The main objective of testing is to evaluate the subject technology for system efficacy and suitability for use in the owner/user-defined environment. In order to assess the overall system efficacy of a SCINetEx device, a determination needs to be made if it meets five (5) broad criteria listed in Section B.1.

B.2.1 OVERALL HYPOTHESIS ADDRESSED BY TEST PLAN

Overall hypothesis that the test plan addresses, and from which all following hypotheses are generated, detailed in this appendix are:

H₀: This SCINetEx technology meets the requirements for use in the owner/user-defined application.

H_A: This SCINetEx technology does not meet the requirements for use in the owner/user-defined application.

B.2.2 HYPOTHESES BREAKDOWN

B.2.2.1 Usability

Usability Hypotheses

- 1 **H₀:** The SCINetEx device meets the size, weight and shape requirements for use in the owner/user-defined application.

H_A: The SCINetEx device does not meet the size, weight and shape requirements for use in the owner/user-defined application.

- 2 **H₀:** Installation of the SCINetEx components can be accomplished in the owner/user-defined application.

H_A: Installation of the SCINetEx components cannot be accomplished in the owner/user-defined application.

- 3 **H₀:** Communications is workable in the owner/user-defined application.

H_A: Communications is not workable in the owner/user-defined application.

B.2.2.2 Functionality

Functionality Hypotheses

- 1 H_0 : The SCINetEx radio frequency (RF) communications meets the general technical requirements.
 H_A : The SCINetEx radio frequency (RF) communications does not meet the general technical requirements.
- 2 H_0 : The SCINetEx cellular communications meets the general technical requirements.
 H_A : The SCINetEx cellular communications does not meet the general technical requirements.
- 3 H_0 : The SCINetEx Global Positioning System (GPS) meets the general technical requirements.
 H_A : The SCINetEx Global Positioning System (GPS) does not meet the general technical requirements.
- 4 H_0 : The SCINetEx Tracking and Geo-Fencing System (TGPS) meets the general technical requirements.
 H_A : The SCINetEx Tracking and Geo-Fencing System (TGPS) does not meet the general technical requirements.
- 5 H_0 : The SCINetEx satellite communications meets the general technical requirements.
 H_A : The SCINetEx satellite communications does not meet the general technical requirements.
- 6 H_0 : The SCINetEx asset monitoring capability meets the general technical requirements.
 H_A : The SCINetEx asset monitoring capability does not meet the general technical requirements.
- 7 H_0 : The SCINetEx device receives and forwards the status, commands and response to commands as required.
 H_A : The SCINetEx device does not receive and forward the status, commands and response to commands as required.
- 8 H_0 : The SCINetEx system gateways provide the functionality as required.
 H_A : The SCINetEx system gateways do not provide the functionality as required.
- 9 H_0 : The SCINetEx system has security measures and encryption as required.
 H_A : The SCINetEx system does not have security measures and encryption as required.

B.2.2.3 Performance

Performance Hypotheses

- 1 H_0 : The SCINetEx device can meet the requirement for the minimum communications range to a fixed NG at height(s) and range(s) determined by the owner/user-defined requirement.
 H_A : The SCINetEx device cannot meet the requirement for the minimum communications range to a fixed NG at height(s) and range(s) determined by the owner/user-defined requirement.
- 2 H_0 : The SCINetEx device can meet the requirement for the minimum communications range to the handheld NG determined by the owner/user-defined requirement.
 H_A : The SCINetEx device cannot meet the requirement for the minimum communications range to the handheld NG determined by the owner/user-defined requirement.
- 3 H_0 : The SCINetEx device can meet the minimum cellular communications requirement for connectivity attempts until message receipt acknowledgement.
 H_A : The SCINetEx device cannot meet the minimum cellular communications requirement for connectivity attempts until message receipt acknowledgement.
- 4 H_0 : The SCINetEx device can meet the minimum overall communications requirement for communication mode selection and prioritization.
 H_A : The SCINetEx device cannot meet the minimum overall communications requirement for communication mode selection and prioritization.
- 5 H_0 : The SCINetEx device GPS provides location accuracy to no less than 40 feet while mounted on a stationary asset.
 H_A : The SCINetEx device GPS does not provide location accuracy to no less than 40 feet while mounted on a stationary asset.
- 6 H_0 : The SCINetEx device TGPS provides location accuracy and geo-fencing to no less than 40 feet while mounted on a moving asset.
 H_A : The SCINetEx device TGPS does not provide location accuracy and geo-fencing to no less than 40 feet while mounted on a moving asset.
- 7 H_0 : The SCINetEx device TGPS provides satellite communications connectivity while mounted on assets traveling at speeds determined by the owner/user-defined requirement.
 H_A : The SCINetEx device TGPS does not provide satellite communications connectivity while mounted on assets traveling at speeds determined by the owner/user-defined requirement.

- 8 **H₀:** The SCINetEx device can operate and survive as specified during the environmental conditions in the owner/user-defined requirement.

H_a: The SCINetEx device cannot operate and survive as specified during the environmental conditions in the owner/user-defined requirement.

- 9 **H₀:** The SCINetEx device can withstand the temperature and humidity conditions experienced in the owner/user-defined application, and continue to work as expected.
H_A: The SCINetEx device cannot withstand the temperature and humidity conditions experienced in the owner/user-defined application, and continue to work as expected.
- 10 **H₀:** The SCINetEx device can withstand the shock and vibration conditions experienced in the owner/user-defined application, and continue to work as expected.
H_A: The SCINetEx device cannot withstand the shock and vibration conditions experienced in the owner/user-defined application, and continue to work as expected.
- 11 **H₀:** The SCINetEx device can withstand the precipitation conditions in the owner/user-defined application, and continue to work as expected.
H_A: The SCINetEx device cannot withstand the precipitation conditions in the owner/user-defined application, and continue to work as expected.
- 12 **H₀:** The SCINetEx device can operate in and withstand the potential Radio Frequency (RF) conditions in the owner/user-defined application.
H_A: The SCINetEx device cannot operate in and withstand the potential Radio Frequency (RF) conditions in the owner/user-defined application.
- 13 **H₀:** The SCINetEx device can operate in and withstand the potential radiation that may be experienced in the owner/user-defined application.
H_A: The SCINetEx device cannot operate in and withstand the potential radiation that may be experienced in the owner/user-defined application.
- 14 **H₀:** The SCINetEx device has sufficient battery power to operate over expected trip duration providing a minimum of four (4) data uploads per trip in the owner/user-defined application, and continue to work as expected.
H_A: The SCINetEx device does not have sufficient battery power to operate over the expected trip duration providing a minimum of four (4) data uploads per trip in the owner/user-defined application, and continue to work as expected.

B.2.2.4 Rate of Failure

Rate of Failure

- 1 **H₀:** The SCINetEx device can meet the threshold for rate of failure (R_{tf}) of one (1) communications connectivity failure per one thousand (1,000) attempts to associate.
H_A: The SCINetEx device cannot meet the threshold for rate of failure (R_{tf}) of one (1) communications connectivity failure per one thousand (1,000) attempts to associate.

- 2 H_0 : The SCINetEx device can meet the goal for rate of failure (Rtf) of one (1) GPS location failure per one thousand (1,000) attempts to take GPS read.

H_A : The SCINetEx device cannot meet the goal for rate of failure (Rtf) of one (1) GPS location failure per one thousand (1,000) attempts to take GPS read.

B.2.2.5 Security

Security Hypotheses

- 1 H_0 : The SCINetEx device uses reliable and robust communications as defined by the owner/user requirement.
 H_A : The SCINetEx device does not use reliable and robust communications as defined by the owner/user requirement.
- 2 H_0 : The SCINetEx device program code cannot be modified, replaced or deleted other than by the manufacturer.
 H_A : The SCINetEx device program code can be modified, replaced or deleted by someone other than the manufacturer.
- 3 H_0 : The SCINetEx device has tamper-evident mechanisms.
 H_A : The SCINetEx device does not have tamper-evident mechanisms.
- 4 H_0 : The SCINetEx device component interfaces meet the security requirements.
 H_A : The SCINetEx device component interfaces do not meet the security requirements.
- 5 H_0 : The SCINetEx device cannot be defeated by an owner/user-specified level of adversary.
 H_A : The SCINetEx device can be defeated by an owner/user-specified level of adversary.
- 6 H_0 : Data stored in or passed through the SCINetEx device cannot be accessed by an owner/user-specified level of adversary.
 H_A : Data stored in or passed through the SCINetEx device can be accessed by an owner/user-specified level of adversary.
- 7 H_0 : The SCINetEx device availability cannot be diminished by an owner/user-specified level of adversary.
 H_A : The SCINetEx device availability can be diminished by an owner/user-specified level of adversary.

This page intentionally left blank.

INITIAL DISTRIBUTION

84300	Library	(1)
85300	Archive/Stock	(1)
55360	R. Clement	(1)
55360	S. Lauff	(1)

Defense Technical Information Center Fort Belvoir, VA 22060-6218	(1)
---	-----

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-01-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden to Department of Defense, Washington Headquarters Services Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE		3. DATES COVERED (From - To)	
November 2018		Final			
4. TITLE AND SUBTITLE				5a. CONTRACT NUMBER	
Secure Connectionless Intelligent Network Extension (SCINetEx) for Autonomic Messaging					
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHORS				5d. PROJECT NUMBER	
Russ Clement Sarah Lauff					
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)				8. PERFORMING ORGANIZATION REPORT NUMBER	
SSC Pacific 53560 Hull Street San Diego, CA 92152-5001				TR 3168	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
Expeditionary Energy Office (E2O) DC CD&I, Headquarters Marine Corps 3300 Russell Rd, Quantico VA				E2O	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT					
Approved for public release.					
13. SUPPLEMENTARY NOTES					
This is work of the United States Government and therefore is not copyrighted. This work may be copied and disseminated without restriction.					
14. ABSTRACT					
This technical report on Secure Connectionless Intelligent Network Extension (SCINetEx) is based on content that was created as a text book for instruction and reference in developing low-power wireless network extensions described in US Navy Patent #8855311. All commercial and government intellectual property rights for this patent are held by the US Government as part of an open architecture system. The report includes concepts and air interface protocols reviewed, tested and validated by teams from US Navy, DOE and DHS. A detailed discussion is also included that describes hierarchal messaging and network configurations supported by an encryption key management protocol for enhanced security when using untrusted Wide Area Networks (WANs). Regulatory requirements are also discussed as applied to the primary wireless medium that implements the IEEE Standard 802.15.4 waveform. Various network configurations are detailed that support autonomic terse messaging for applications such as in-transit visibility, transport and physical security, fleet optimization and management as well as sentient machine-to-machine communications. There are many topics addressed in this report specific to Network topology, data frame structures and operation including Network protocol stack set up, MAC protocol configuration set up, Network PAN ID standardization, Ad-hoc/mesh network topology, Red Team testing and message encryption. There are over 40 figures included that help to make complex configurations addressed in this report easy to understand.					
15. SUBJECT TERMS					
Network topology; PAN ID; message encryption; WAN; in-transit visibility; fleet optimization;					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Russ Clement
U	U	U	U	222	19b. TELEPHONE NUMBER (Include area code) (619)-553-5433

This page intentionally left blank.

Approved for public release.



SSC Pacific
San Diego, CA 92152-5001