1.0 INTRODUCTION

1.1 Purpose

ARINC 485 Part 2 defined a low-speed serial communications interface between Electronic equipment in the passenger seat. Its design focused on obtaining status from in-seat electronic equipment.

Cabin Equipment has evolved from the very simple to quite sophisticated systems. The resulting communications needs have surpassed the ability of ARINC 485 to provide the necessary data capacity and response times. The basic requirements for low latency, full duplex, elimination of ARINC 485 Master/Slave polling and lower weight drives the selection of IEEE 802.3bw (100BaseT1) as the preferred bus format.

This document specifies the Cabin Equipment Network Bus utilizing a new, serial communications protocol based on IEEE 802.3bw operating at 100 Mbps and utilizing a single twisted pair wire.

1.2 Applicable Documents

ARINC Specification 485: *Cabin Equipment Interfaces Part 1, Head End Equipment Protocol*

ARINC Specification 628: *Cabin Equipment Interfaces Part 1, Cabin Management and Entertainment System - Peripherals*

ARINC Specification 628: *Cabin Equipment Interfaces Part 2, Cabin Management and Entertainment System – Seat Interfaces*

ARINC Specification 628: *Cabin Equipment Interfaces Part 3, In-Flight Entertainment System (IFES) to Aircraft Systems Interfaces*

ARINC Specification 628: *Cabin Equipment Interfaces Part 4A, Cabin Management and Entertainment System - Cabin Distribution System – Daisy Chain*

ARINC Specification 628: *Cabin Equipment Interfaces Part 4B, Cabin Management and Entertainment System - Cabin Distribution System – Daisy Chain*

ARINC Specification 628: *Cabin Equipment Interfaces Part 9, Cabin Interface Network (CIN)*

IEEE 802-2014*: IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*

IEEE 802.3-2012*: IEEE Standard for Ethernet*

IEEE 802.3bw-2015: Physical Layer Specifications and Management Parameters for 100 Mb/s Operation over a Single Balanced Twisted Pair Cable (100BASE-T1)

TIA/EIA-485: *Standard for Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multipoint Systems*

TIA/ EIA Telecommunications System Bulletin TSB 89: *Application Guideline for TIA/EIA-485-A*

1.3 Scope

This document specifies the implementation of a high speed Ethernet Local Area Network (LAN) for use in a Seat network and which is extensible to additional domains. This specification will address

the bus itself (e.g. electrical, signaling), overall LAN architecture and common elements of the communication protocol.

2.0 BUS ARCHITECTURE / PHYSICAL LAYER

2.1 Physical layer

An IEEE 802.3bw network link consists of two network interfaces and the twisted pair interconnect wires between them. Communications between the nodes over the link is full duplex (both nodes can transmit at the same time). Each network interface will have electrical isolation such as provided by a transformer and PHY as Illustrated in Figure 1.

Figure 1: Physical Layer

COMMENTARY

The magnetic transformer symbol used to represent electrical isolation in all the figures of this document are just an illustration and are not meant to imply implementation

While the 100BaseT1 standard calls out unshielded twisted pair wire, it is common in the aircraft industry to utilize shielded twisted pair due to the more stringent emissions containment required in a commercial aircraft. Following the latest ARINC-CSS guidance, all 100BaseT1 cables and connectors must be shielded as per A800P3.

2.1.1 Wiring

The 100BaseT1 PHY is designed to operate over a single balanced twisted-pair cabling system. Single balanced twisted-pair cable supports an effective data rate of 100 Mb/s in each direction simultaneously. The link segment for a 100BaseT1 PHY system consists of up to 15m of single balanced twisted-pair cabling, with up to four in-line connectors and two mating connectors.

Details are described in section 96.7 of IEEE 802.3BW document.

Figure 2 illustrates the 100BaseT1 point-to-point connection.

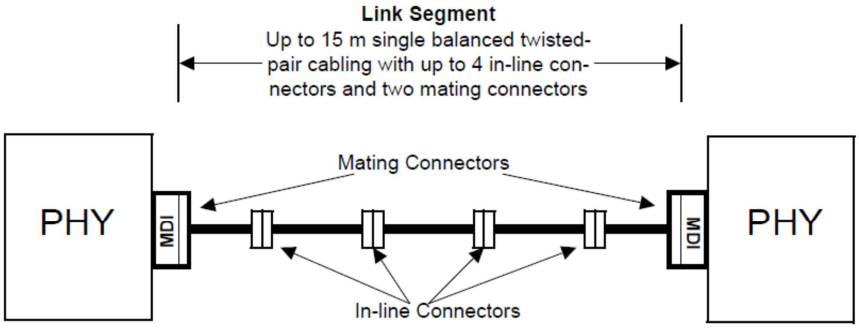


Figure 2: 100baseT1 Point-to-Point Connection

2.1.2 Connectors

The following will be confirmed after the ARINC committee in Cocoa Beach in February.

Dedicated connectors on both ends of the link should be used:

LRU connector side:

- 4 Pin - Hirose P/N: GT17H-4S-2C(B) (Key color: Green)

Cable connector side:

- 4 Pin – Hirose P/N:

Housing	GT17HS-4S-HU	
Insulator	GT17H-4S-2C(B)	Key - Green
Outer Shelf	GT17HS-4S-5CF	
Contact Terminal	GT8-2428SCF(70)	#24 to #28 AWG

2.2 Ethernet Link Establishment

The IEEE 802.3bw PHYs support full duplex communications using a technique called Echo Cancellation. In principle, each node subtracts the signal it is transmitting from the signal it is receiving with the result of the subtraction being the signal from the distant node. The IEEE 802.3bw specification calls for one PHY on a link to be set up as MASTER and the PHY on the other side must be set up as SLAVE. The specification indicates that operation is undefined if both sides of a link are the same (MASTER or SLAVE).

Commentary

The Master/Slave negotiation happens automatically as part of link establishment which occurs at the link layer level.

2.3 Generic Network

Multiple nodes can be combined into an extended network by utilizing components called network switches that receive and retransmit messages based on the addressing rules appropriate for the protocol layer in which they operate.

Four types of network nodes can exist:

- Endpoint Node (one port)
- Intermediate Node (two ports)
- Star Node (more than two ports)
- Router Node (connects two independent networks)

These nodes can be combined in a large number of ways to construct a complete private network. In addition this private network can be connected to a larger network.

2.3.1 Two-Node Network

The simplest network consists of two End-Point nodes with a network link between them as illustrated in Figure 3. In such a network, one of the End Point nodes will be designated a master and the other must be designated a slave (see Master/Slave Relationship).

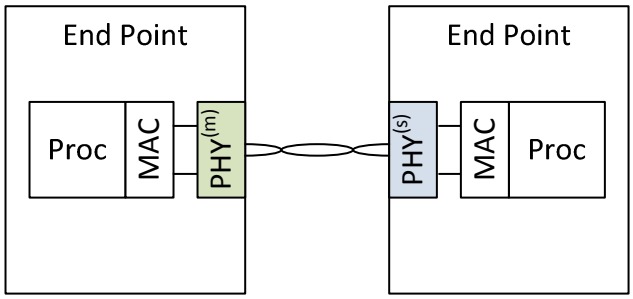


Figure 3: Simple One-Link with Two Endpoints

2.3.2 Three-Node Network

The next level of network sophistication is a three-node network where one of the network nodes must perform a relay function between two endpoint nodes as illustrated in Figure 4. In this configuration, an intermediate node is necessary.

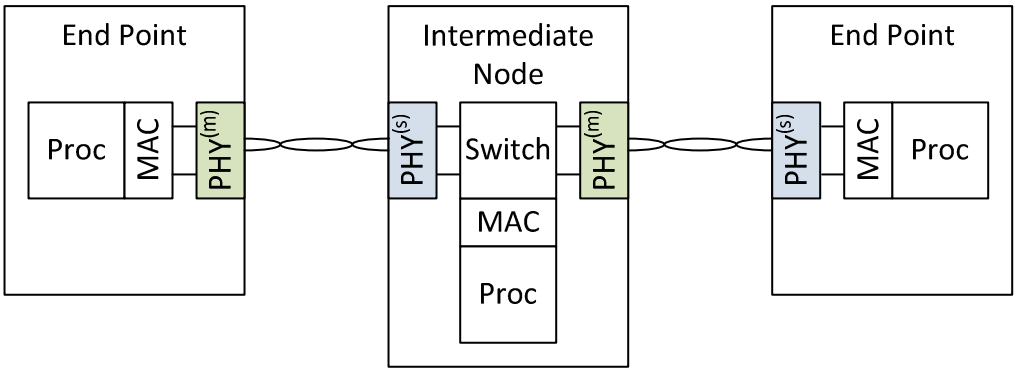


Figure 4: Three Node Network: Intermediate with two End-Points

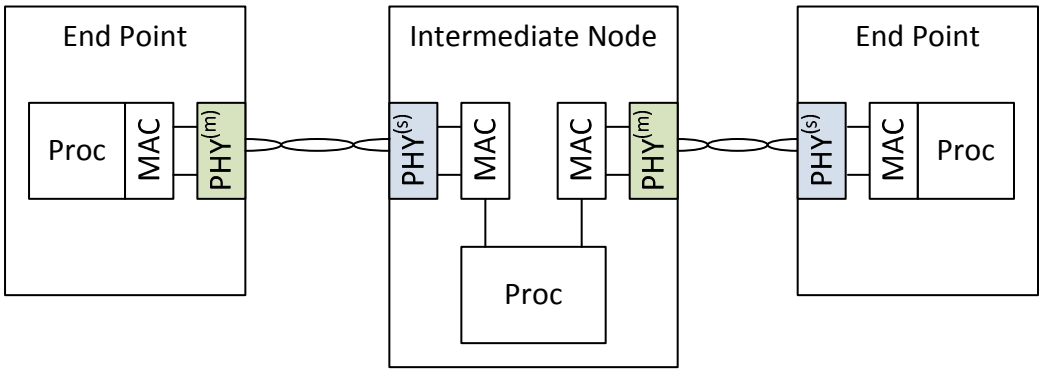


Figure 4a: Three Node Network: non switch-based Intermediate with two End-Points

2.3.3 Four Node Networks

As more nodes are added, the variety of potential interconnect strategies, increases as well. One way in which the network can be expanded is to add additional Intermediate nodes as illustrated in Figure 5a.

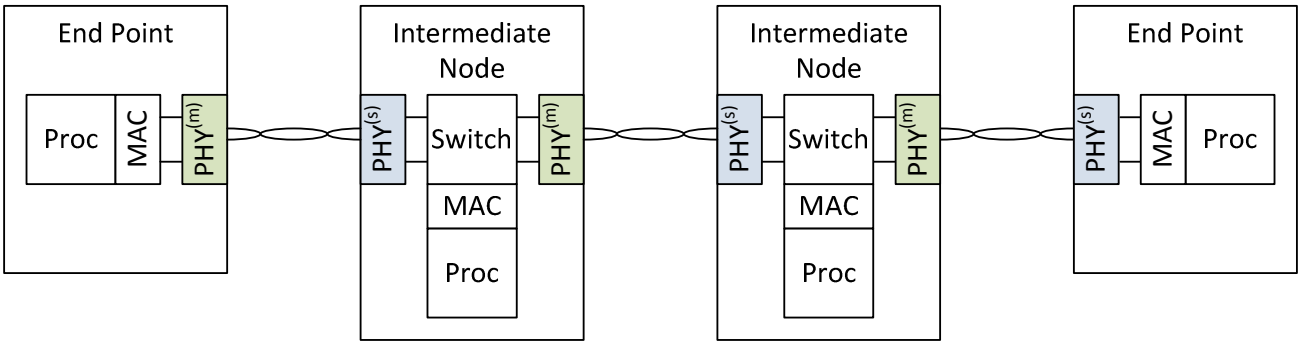


Figure 5a: Four Node Network: Two Intermediate and Two End-points

An alternate approach can be used by introducing a Star Node into the architecture. As illustrated in Figure 5b. This architecture requires a slightly more sophisticated intermediate connection (the Star Node) but permits all other nodes to be simple end-points.

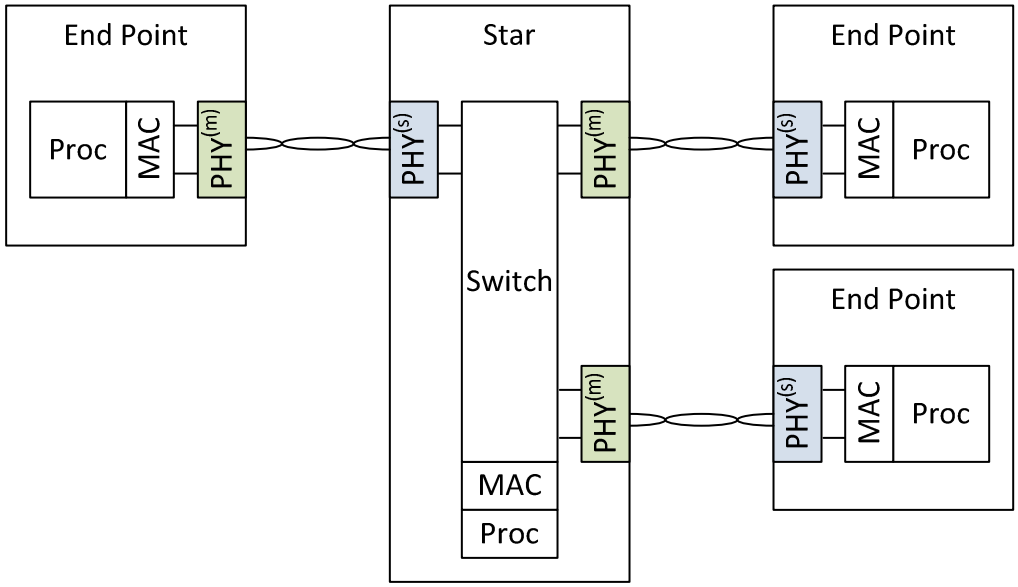


Figure 5b: Four Node Network: Three End-Points and one Star

2.3.4 Router

In an application like a Cabin System, the local private network may in fact be part of a bigger system. In such an application, one of the nodes may need to be a network router between the local private network and the larger system network. In addition, it is often desirable to limit the amount of traffic and to restrict the interaction between the large network and the local private network. In figure 6, such a configuration is illustrated using a Router Node between a larger network (using 4-TP Gigabit Ethernet in the example) and the local network.

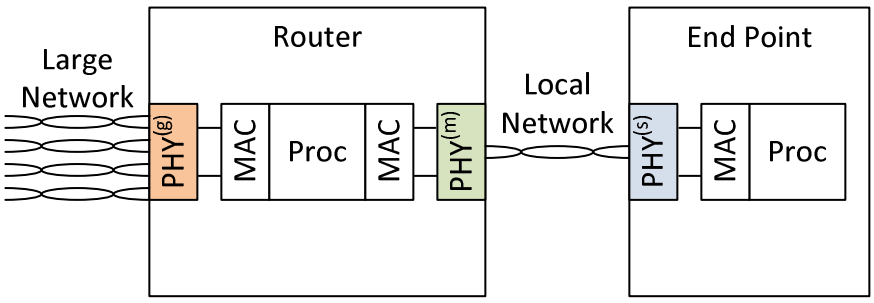


Figure 6: Two Node network with Router Node to Larger Network

2.4 Application to Passenger Seat

With the types of network nodes defined, we can look at a specific application of this network. The architecture illustrated in Figure 7 shows an SEB functioning as a Router Node between the more global cabin network (4-TP Gigabit Ethernet) and the local seat network. In this example, the local network consists of the SEB (Router node), an SPB (star node), an ECU/SAC (Intermediate node), a PCU, (end-point) and an LC (end-point).

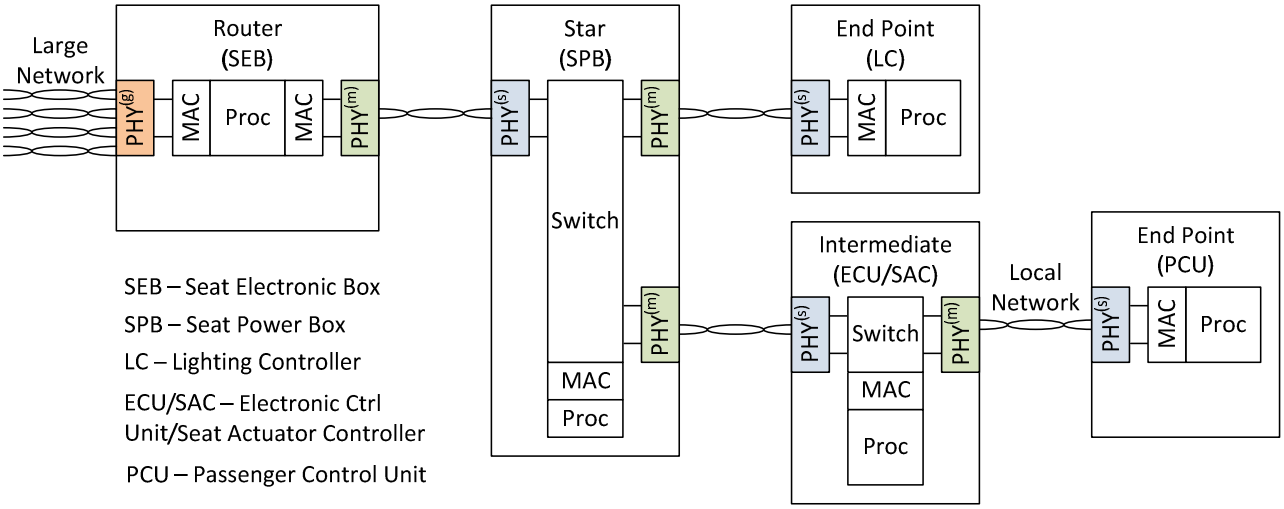


Figure 7: Complex Seat Application (Notional Architecture)

3.0 BUS PROTOCOL LAYERS

The IEEE 802 / IETF protocol layers selected for the Cabin Network Bus are identified in this section. The details of the various formats and fields are contained in the specifications referenced.

In most instances, developers of equipment that uses the Cabin Network Bus do not have to deal with the details of the protocols identified herein. The network protocol stack selected by each supplier should provide the assembly and encapsulation described in this section.

3.1 Virtual Local Area Networks (VLANs)

VLAN tagging per 802.1Q should be supported by the Cabin Equipment Network LRUs.

3.2 Media Access Control (MAC) Address

Manufacturers of equipment to be placed on any Ethernet network must obtain a block of addresses from the IEEE. Information on the procedure for obtaining MAC address blocks is available from the following IEEE website:

http://standards.ieee.org/develop/regauth/grpmac/

Once a manufacturer has their block of MAC addresses, it is the obligation of the manufacturer to avoid any duplications. Should a duplicate MAC address appear in any network, the performance of the entire network may be seriously degraded.

3.3 Media Access Control (MAC) Channel Access

The Media Access Control (MAC) Channel access method for 100BaseT1 is full-duplex (no contention on the media).

3.4 Network Layer (OSI Layer 3)

It is undesirable for the potentially large volume of unrelated traffic to appear on a Cabin Equipment Network Bus. It is desirable for each Cabin Equipment Network Bus to be isolated from large cabin networks and each other with communications between Cabin Equipment Network bus and more extensive busses or between Cabin Equipment Network Busses to be limited and managed by Router nodes.

The Network Layer for the Cabin Equipment Network Bus is Internet Protocol Version 4 (IPv4) explicitly. IPv6 is not supported on this network. Furthermore, each Cabin Equipment Network bus is an isolated private network consistent with RFC 1918.

Commentary

Note that an IFE Cabin Network is also an isolated private network in accordance with RFC 1918 as well but using a different address range. The Cabin IP Address Scheme is specified in ARINC 628 Part 9 attachment 4

3.4.1 Cabin Equipment Network Bus Address Range

In accordance with RFC1918, nodes on the Cabin Equipment Network Bus are assigned addresses in the address space: 192.168.237.x or 192.168.237.0/24. The netmask applied for components on this bus is 255.255.255.0 (appropriate for the /24 address space).

COMMENTARY

In ARINC664P4-2, the following ranges are reserved for future assignment.

- 172.21.0.0 – 172.21.255.255,
- 172.25.0.0 – 172.26.255.255,
- 192.168.16.0 – 192.168.255.255

The range of 192.168.237.0 – 192.168.237.255 is selected for the new seat network (subnet 192.168.237.0/24).

The rationales behind this choice are:

- Create a private Seat-End network.
- IFE Node becomes the gateway between the private Seat-End network and IFE network. There is no direct layer 2/3 communication across Seat-End, i.e. the private network at each seat enables the reuse of IP addresses at each seat for the same LRUs.

This is already the communication paradigm with RS-485-based hierarchy, where the master on the bus is the gateway between the IFE network and the seat peripherals network.

3.4.2 Cabin Equipment Network Bus Address Assignments

A Cabin Equipment Network Bus is a relatively small, fixed network with a fairly static configuration. Any change to the network would require wiring changes and the appropriate level of certification oversight. The nodes on the network should be known and fixed when assembled and installed on the aircraft and the network should identify and flag any changes as potential security breaches.

For these reasons, a Static IP addressing scheme is adequate for this network type.

The network is made of nodes with pre-programmed IP addresses based on the type of equipment with variation within the same type based on pin-programming.

The following IP addresses should be used by the equipment on the seat peripheral network:

Table 1: IP Addresses

LRU	Addresses
IFE Nodes	192.168.237.1 to 7, netmask 255.255.255.0
Seat Power Boxes	192.168.237.8 to 14, netmask 255.255.255.0
Seat Actuator Controllers	192.168.237.15 to 21, netmask 255.255.255.0
In-Seat Lighting System	192.168.237.22 to 28, netmask 255.255.255.0
Passenger control Units	192.168.237.29 to 42, netmask 255.255.255.0

3.5 Transport Layer (OSI Layer 4)

While there are a variety of Transport Layer protocols available, at a minimum nodes on the Cabin Equipment Network Bus should support the following transport layer protocols:

- User Datagram Protocol (UDP) number 0x11 from RFC 768
- Transport Control Protocol (TCP) number 0x06 from RFC 793
- Internet Control Message Protocol (ICMP) number 0x01 from RFC 792

Since it is anticipated that most message traffic will be point to point with message integrity verification desired, TCP is the most likely protocol to be used on a wide basis.

Other Transport Layer protocols that might be relevant in the future but which are not currently identified as applicable on this bus are as follows:

- Internet Group Management Protocol (IGMP) number 0x02 from RFC 1112

3.5.1 Transport control Protocol (TCP)

The basic characteristics of TCP are contained in RFC 793.

It is anticipated that the bulk of communications on the Cabin Equipment Network Bus will be messages between two nodes. The protocol most often applied to this type of communications is Transport Control Protocol (TCP) as it provides error checking and retry mechanisms within the protocol itself removing these from the concern of the applications.

The Cabin Equipment Network Bus will use TCP sockets for peer-to-peer communications. TCP supports a client/server model over which nodes can communicate. TCP sockets use predefined port numbers to identify different server services.

COMMENTARY

This full duplex connection-oriented protocol provides a simple way to establish a session by means of 3-way handshake between each transmitter (potentially each LRU in the LAN). TCP provides error checking although it comes at the cost of some overhead traffic as well as more elaborate IP stacks and micro-controllers. With the TCP protocol, the “Application” does not need to keep track of acknowledgment and retransmission as this is directly handled at the Transport layer.

TCP sockets should be used for peer communication within the Cabin Equipment Network. TCP sockets follow a client/server model, where the IFE Node acts as the server and each Cabin Equipment Network LRUs act as clients for their associated TCP socket.

The server has a fixed IP address and listens to the well-known port number for incoming request for connection.

There is only one server allowed within the seat group network. Once a TCP connection is established, application messages are exchanged bi-directionally via

this connection. The server allows for only one TCP connection at a time from a specific client.

TCP port number 24443 for Secure WebSocket connections tunneled over Transport Layer Security (TLS) should be used as both source and destination.

3.5.2 User Datagram protocol (UDP)

The basic characteristics of UDP are contained in RFC 768.

COMMENTARY

User Datagram Protocol (UDP) is used where error checking and correction are either not necessary or is performed at higher levels in the protocol stack. Time-Sensitive applications favor UDP as dropping packets is often favorable to the complexities of retransmission delay, out-of-order arrival, etc. Multicast and broadcast traffic utilizes UDP as the destination IP address does not represent a single network node.

The port number 24924 should be used as UDP source. The port number 24925 should be used as UDP destination.

3.6 Application Layer (OSI Layer 7)

The Secure WebSocket protocol (RFC 6455) over TLS 1.2 (RFC 5246) should be used for application layer. As mentioned in 3.5.13.5.1 above, port number 24443 in lieu of 443 (from RFC 6455) should be used.

3.6.1 Message Format Description

Four message formats are defined for the application layer. These messages are encapsulated within the application payload of a UDP/IP or TCP/IP message.

Type 1 Message Format:

Name	Bytes	Description	Comment
Protocol_Identifier	1	01h	Revision of the protocol
Command	1	Command Code	

Type 2 Command_2 Message Format:

Name	Bytes	Description	Comment
Protocol_Identifier	1	01h	Revision of the protocol
Command	1	Command Code (F4h)	
Data Length	1	Data length of the Command_2 and Data fields	
Command_2	3	Command _2 Code	
Data	n	Data field	Up to 252 bytes

Type 3 Message Format:

Name	Bytes	Description	Comment
Protocol_Identifier	1	01h	Revision of the protocol
Command	1	Command Code	
Data Length	1	Data length of the data field	
Data	n	Data field	Up to 255 bytes

Type 4 Message Format:

Name	Bytes	Description	Comment
Protocol_Identifier	1	01h	Revision of the protocol
Command	1	Type 4 command code	
Data Length	2	Data length of the data field	Byte 1 is the most significant byte of the data length. Byte 2 is the least significant byte of the data length.
Data	n	Data field	The data should not exceed 2048 bytes

Type 4 Command_2 Message Format:

Name	Bytes	Description	Comment
Protocol_Identifier	1	01h	Revision of the protocol
Command	1	Command Code (F6h)	
Data Length	2	Data length of the data field	Byte 1 is the most significant byte of the data length. Byte 2 is the least significant byte of the data length.
Command_2	3	Command _2 Code	
Data	n	Data field	The data should not exceed 2045 bytes

Example: Power_Up_Status message with Filename “THASVD01”.

This Power_Up_Status is encapsulated within the application payload of a UDP/IP message.

Byte	Data in Payload	Note
0	01h	Protocol Identifier
1	97h	Command
2	08h	Data Length
3	54h	T
4	48h	H
5	41h	A
6	53h	S
7	36h	V
8	44h	D
9	30h	0
10	31h	1

4.0 BUS OPERATION

4.1 Power-Up Initialization

Before any equipment on the Cabin Equipment Network Bus can communicate, the IFE Node and Seat-End LRUs should initialize the interface by performing a series of message exchange:

- Power-Up Sequence
- Communication Authentication
- Communication Initialization

The following is a flowchart of the IFE Node initialization logic:

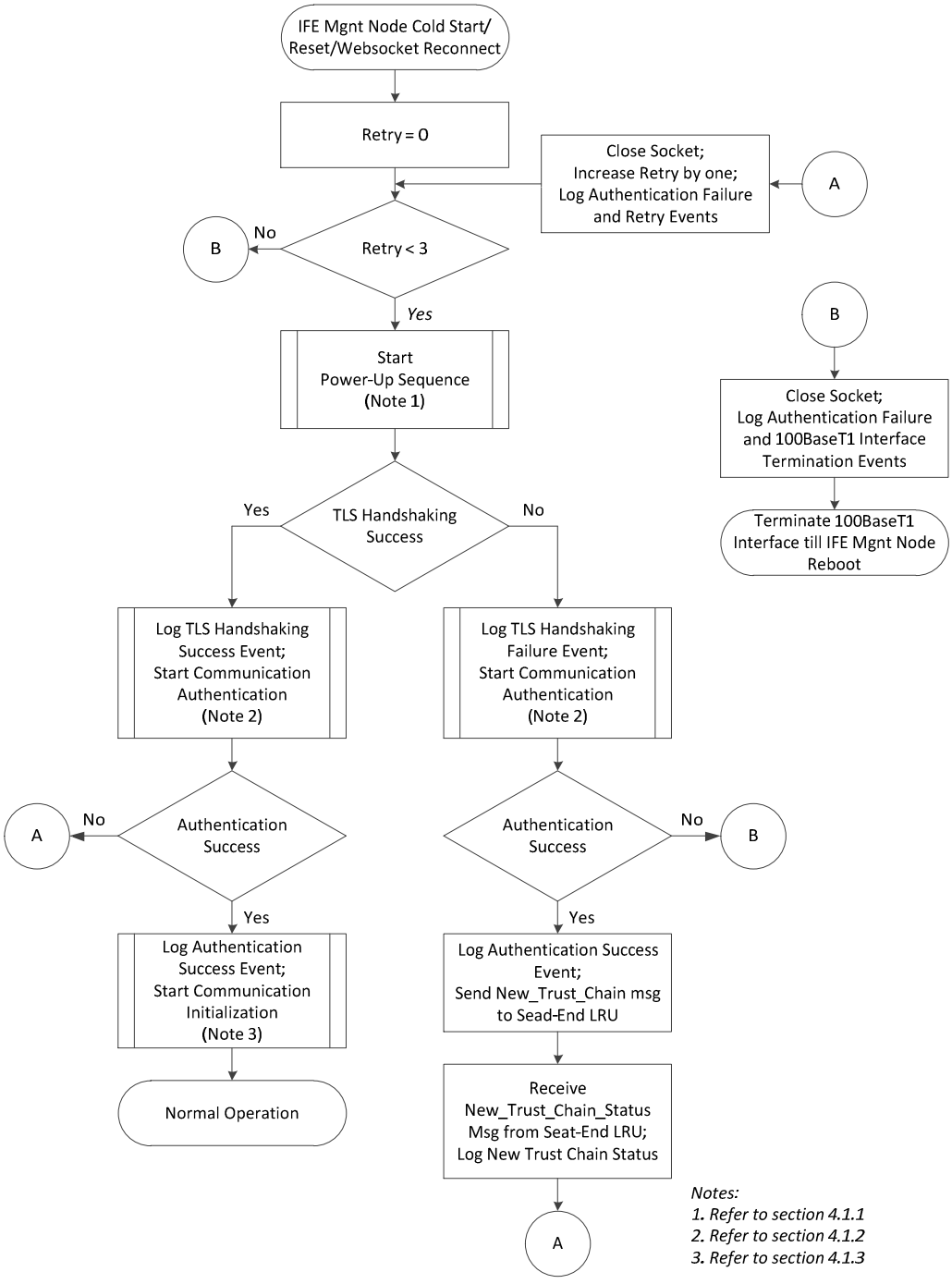


Figure 8: IFE Node Initialization Logic

The following is a flowchart of the Seat-End LRU initialization logic:

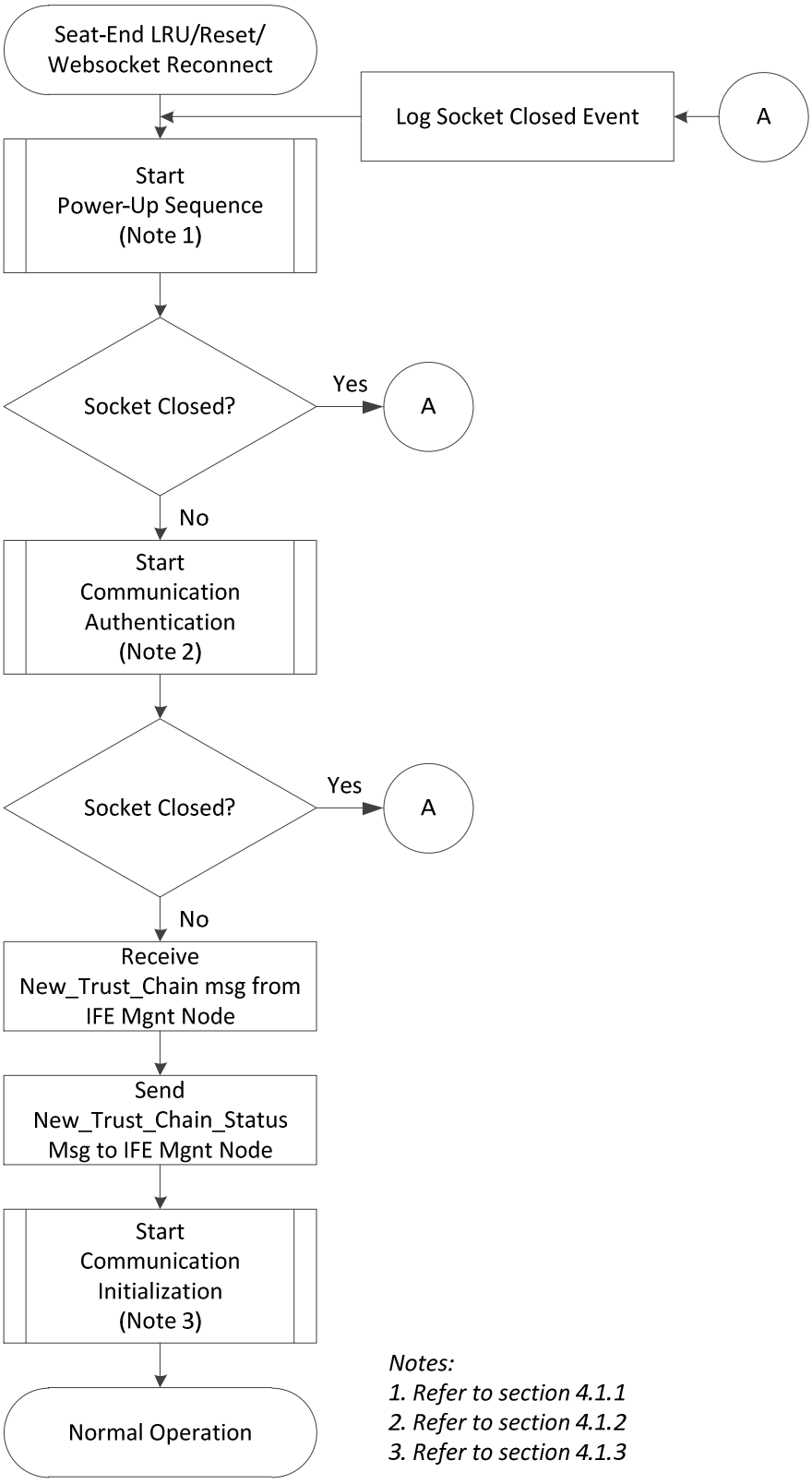


Figure 9: Seat-End LRU Initialization Logic

4.1.1 Power-Up Sequence

The power sequence should follow the following logic:

1. **The IFE Node Power-Up First:**
   - The IFE Node unicasts the Power_Up_Status message to the Seat-End LRU once a second till the ClientHello message is received.
   - Upon reception of the Power_Up_Status, the Seat-End LRU starts the TLS handshake protocol as specified in Figure 10 and 11.

     COMMENTARY

     The IFE Node Power-Up means that the IFE Node has completed its internal initialization.

     The TLS handshaking protocol is defined in section 7 of the RFC 5246.

     For security reasons and in order to guarantee that the Power-up sequence stays deterministic across IFE Node and Seat-End equipment reboots, the Power_Up_Status message is a unicast message (vs multicast or broadcast).

     Additionally, since the list of seat-end equipment of a given aircraft configuration does not evolve over-time (without major changes in software configuration and wiring), the IFE node is configured with the list of expected seat-end equipment.

     When the IFE Node powers-up first, the IFE Node unicasts the Power_Up_Status message to each equipment listed in its configuration.

2. **The Seat-End LRU Power-Up First:**
   - The Seat-End LRU waits for the IFE Node to power up (waits for the Power_Up_Status message).

     COMMENTARY

     The communication failure handling described in section 5.2 is not applicable to this power up sequence. That means if the Seat-End LRU has not received any message from the IFE Node for more than 30 seconds, the Seat-End LRU does not close its socket.

   - Upon reception of the Power_Up_Status, the Seat-End LRU starts TLS handshake protocol as specified in Figure 10 and 11.

     COMMENTARY

     The Seat-End LRU power-up means that the Seat-End LRU has completed its internal initialization and is ready to start the communication initialization.

     The TLS handshaking protocol is defined in section 7 of the RFC 5246.

3. After the TLS handshake protocol is completed, the Seat-End LRU initiates the HTTP protocol upgrade process. Upon reception of the protocol upgrade request, the IFE Node confirms the protocol upgrade.

COMMENTARY

The HTTP protocol upgrade process is defined in section 1.3 of RFC 6455.

4. After the HTTP protocol upgrade process is completed, the IFE Node and Seat-End LRU should start the Communication Authentication as described in section 4.1.2.

4.1.2 Communication Authentication

As the WebSocket protocol (RFC 6455) does not inherently prescribe any particular way to handle the Authentication and Authorization between the server (IFE Node) and clients (Seat-End LRUs), authentication needs to be handled at the Application Layer of the TCP/IP model. Also to guarantee confidentiality of this authentication mechanism, this authentication occurs over a WebSocket Secure (WSS).

The authentication will be requested at each connection attempt.

After the Power-Up Sequence, the IFE Node and Seat-End LRU should execute the following procedures to authenticate the communication:

1. The Seat-End LRU connects to the WebSocket Secure of the IFE Node and provides its unique ID and the revision of the security key to the IFE Node via the Hello message.
2. Upon reception of the Hello message, the IFE Node transmits the Welcome message with the current timestamp to the Seat-End LRU within one second.
3. Upon reception of the Welcome message, the Seat-End LRU generates the destination hash and transmits the destination hash to the IFE Node via the Verification_Hash message within 5 seconds.
    - A hash is a cryptographic checksum. It is the SHA-256 algorithm as defined in RFC 4634.
    - The destination hash is a hash of the concatenation of the security key that is stored in the Seat-End LRU and the timestamp that is provided by the Welcome message. The Seat-End LRU should use 10, 000 iterations of SHA-256 hash (as a minimum).

      Note: The concatenation sequence is the security key first and then the timestamp. The Input string format for SHA-256 Hash computation is defined in section 5.2.12.
4. The IFE Node generates origination hash and compares it with received destination hash from the Verification_Hash message.
    - The IFE Node contains all revisions of the security key for each Seat-End LRU. Based on the Seat-End LRU unique ID and the security key revision that are provided by Hello message, the IFE Node is able to retrieve the associated security key to generate an origination Hash.
    - The origination hash is a hash of the concatenation of the security key of the Seat-End LRU and the timestamp (the same timestamp that was provided by the Welcome message as described in step 2). The IFE Node should use 100,000 iterations of SHA-256 hash.

      Note: The concatenation sequence is the security key first and then the timestamp. The Input string format for SHA-256 Hash computation is defined in section 6.2.12.

5. Upon detection of an authentication failure, the IFE Node should log the failure event, close the socket, and re-start the Power-Up Initialization for up to 2 retries (including the first Power-Up Initialization, 3 times total). If reach the maximum retries, the IFE Node should log the failure event, close its socket, and do not allow the Seat-End LRU to re-connect to the socket till cycle power or reset the IFE Node

Notes:

1) The IFE Node declares the authentication failure, if any of the following condition occurs:
   a. The Seat-End LRU fails to transmit the Verification_Hash message in response to the Hello message within 5 seconds.
   b. If the IFE Node detects that the destination hash does not match the origination hash as expected for this LRU (identified by the ID and security key revision).
2) After detection of three authentication failures (reach maximum retries), the IFE Node does not accept any messages sent by the Seat-End LRU.

6. Upon detection of the authentication success, the IFE Node should log the success event and start the Communication Initialization as described in section 4.1.3.
7. After the communication has been authenticated and prior to enter into the communication initialization, if the IFE Node detects that a newer security key is available in its database, the IFE Node should initiate the security update process as describe in section 4.6.

4.1.3 Communication Initialization

After the communication has been authenticated, the IFE Node and Seat-End LRU should proceed with the communication initialization as follows:

1. The IFE Node transmits the Airplane_Flight_Mode message to the Seat-End LRU.
2. The IFE Node transmits the Configuration_Request message to the Seat-End LRU. The Seat-End LRU responds with the Configuration_Response message.
3. The IFE Node transmits the BITE_Data_Request message to the Seat-End LRU to request for current active faults only. The Seat-End LRU responds with the BITE_Data message with all current active faults.

COMMENTARY

The IFE Node should reset Seat-End LRU faults status to initial state prior to transmitting BITE_Data_Request message.

4. The IFE Node transmits the LRU_Status_Request message to the Seat-End LRU. The Seat-End LRU responds with an LRU_Status message.
5. After Communication Initialization is completed, the IFE Node and Seat-End LRU enter into normal operation.

Figure 10 illustrates TLS handshaking protocol between the IFE Node and a Seat-End LRU that shows an IFE vendor Certificate Authority (CA) certificate validated successfully by the Seat-End LRU.

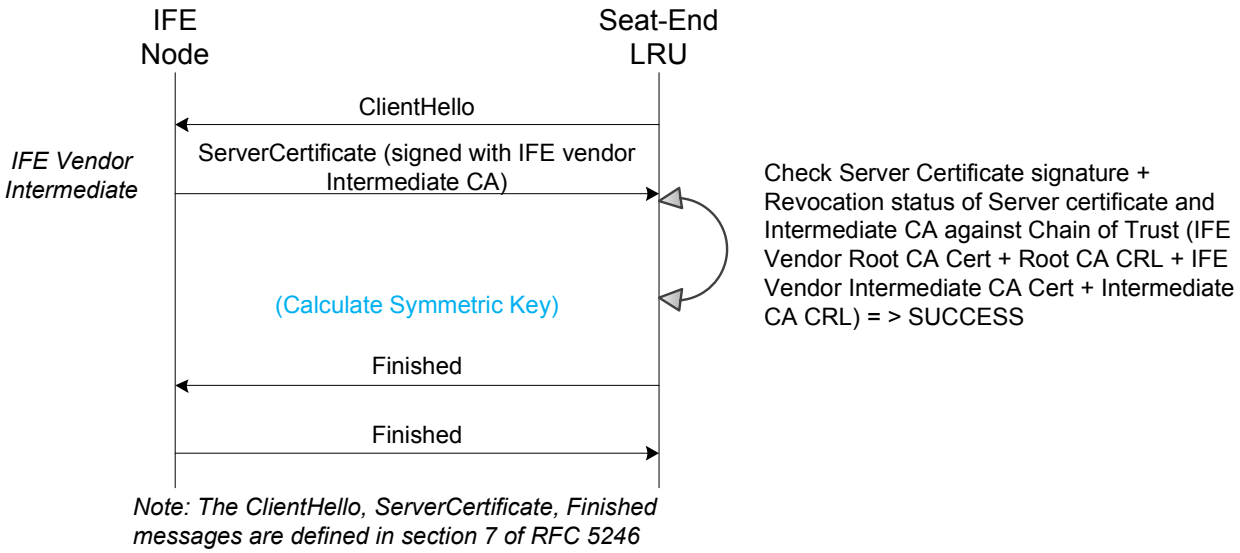
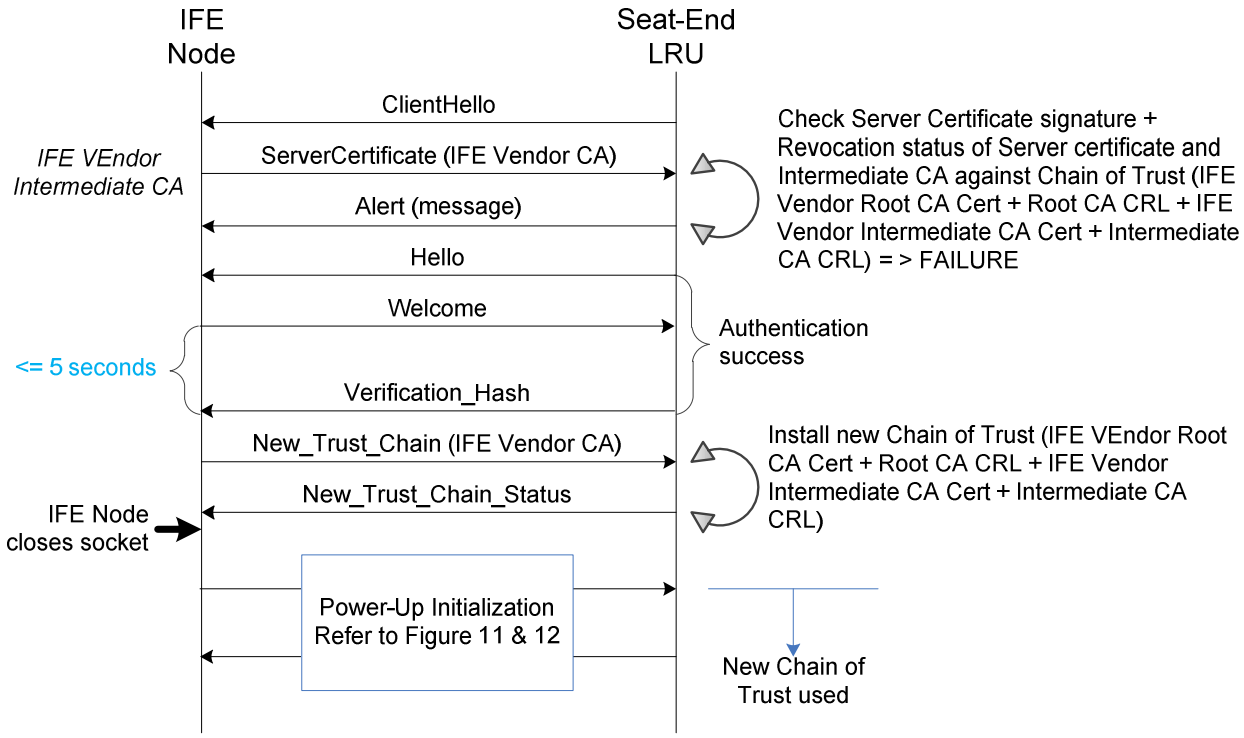


Figure 10: TLS Handshaking Protocol – Success

Figure 11 illustrates TLS handshaking protocol between the IFE Node and a Seat-End LRU that shows an IFE vendor CA certificate validation failure such as what would happen if the CA was revoked (by its signer), has expired, is not currently valid, or if an unspecified issue arose in processing the certificate by the Seat-End LRU.



Notes:
1. The ClientHello, ServerCertificate, and Alert messages are defined in section 7 of RFC 5246
2. Alert message could be the certificate_revoked(44), certificate_expired(45), or certificate_unknown(46).

Figure 11: TLS Handshaking Protocol – Failure

Figure 12 illustrates the Chain of Trust and Revocation List management.

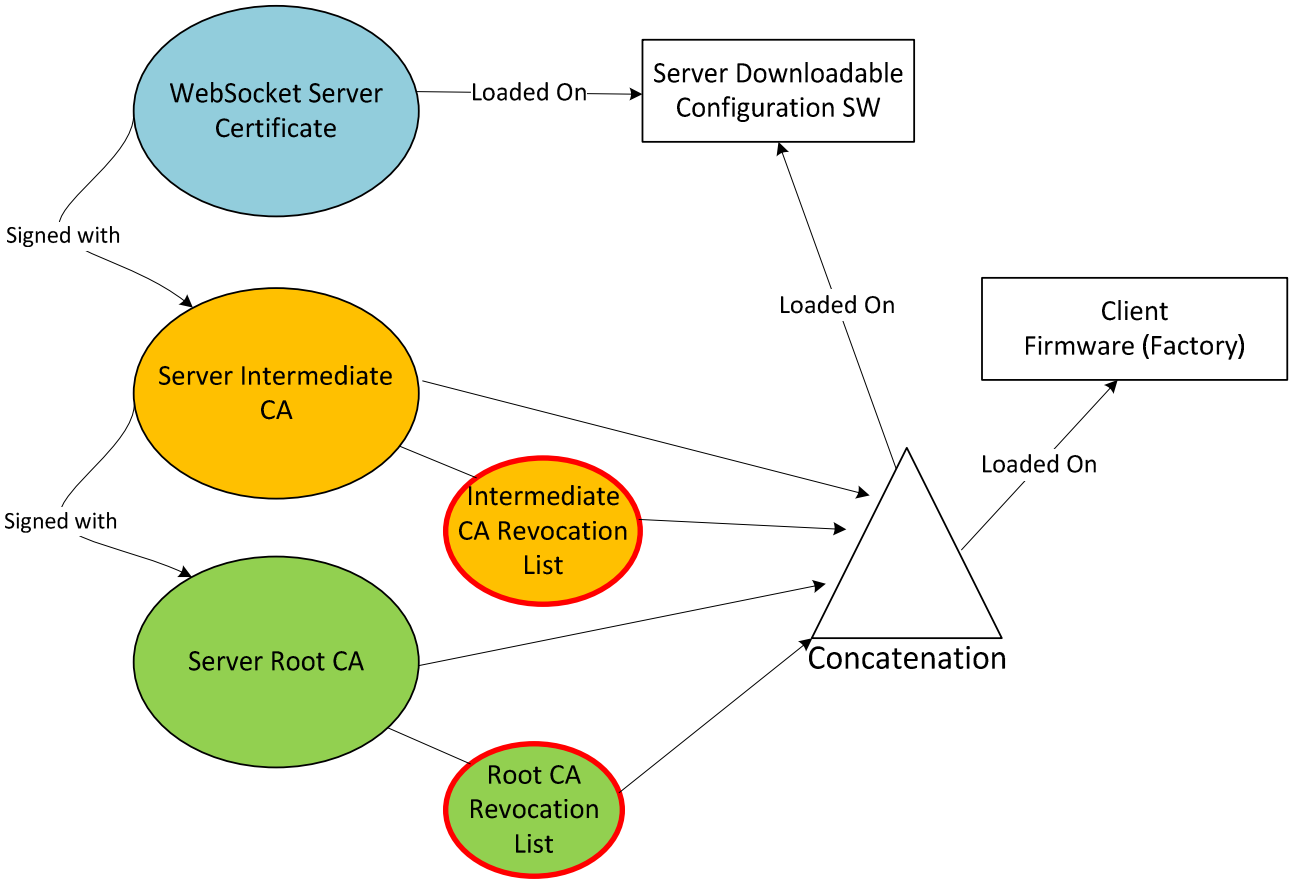
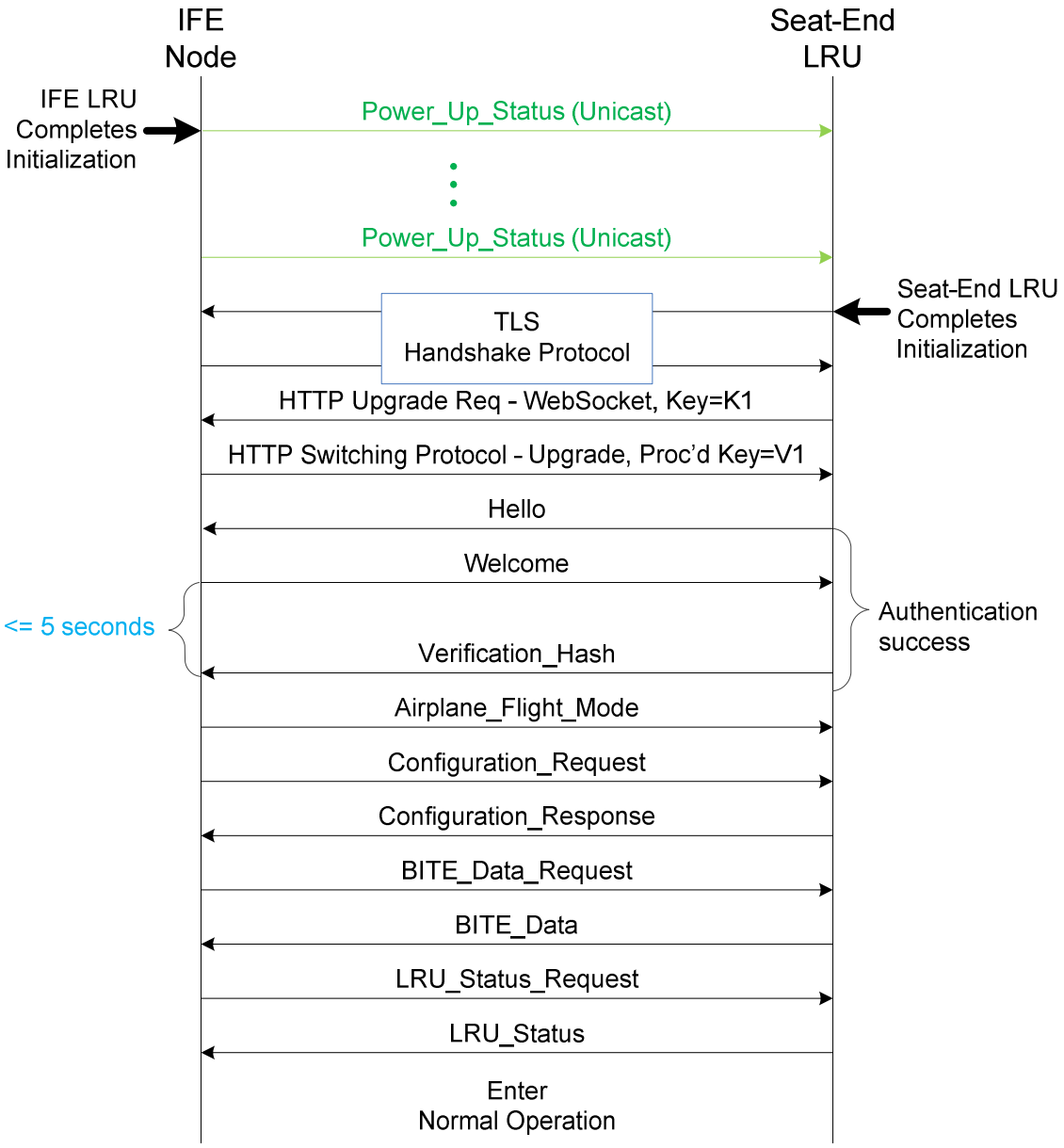


Figure 12: Chain of Trust and Revocation List

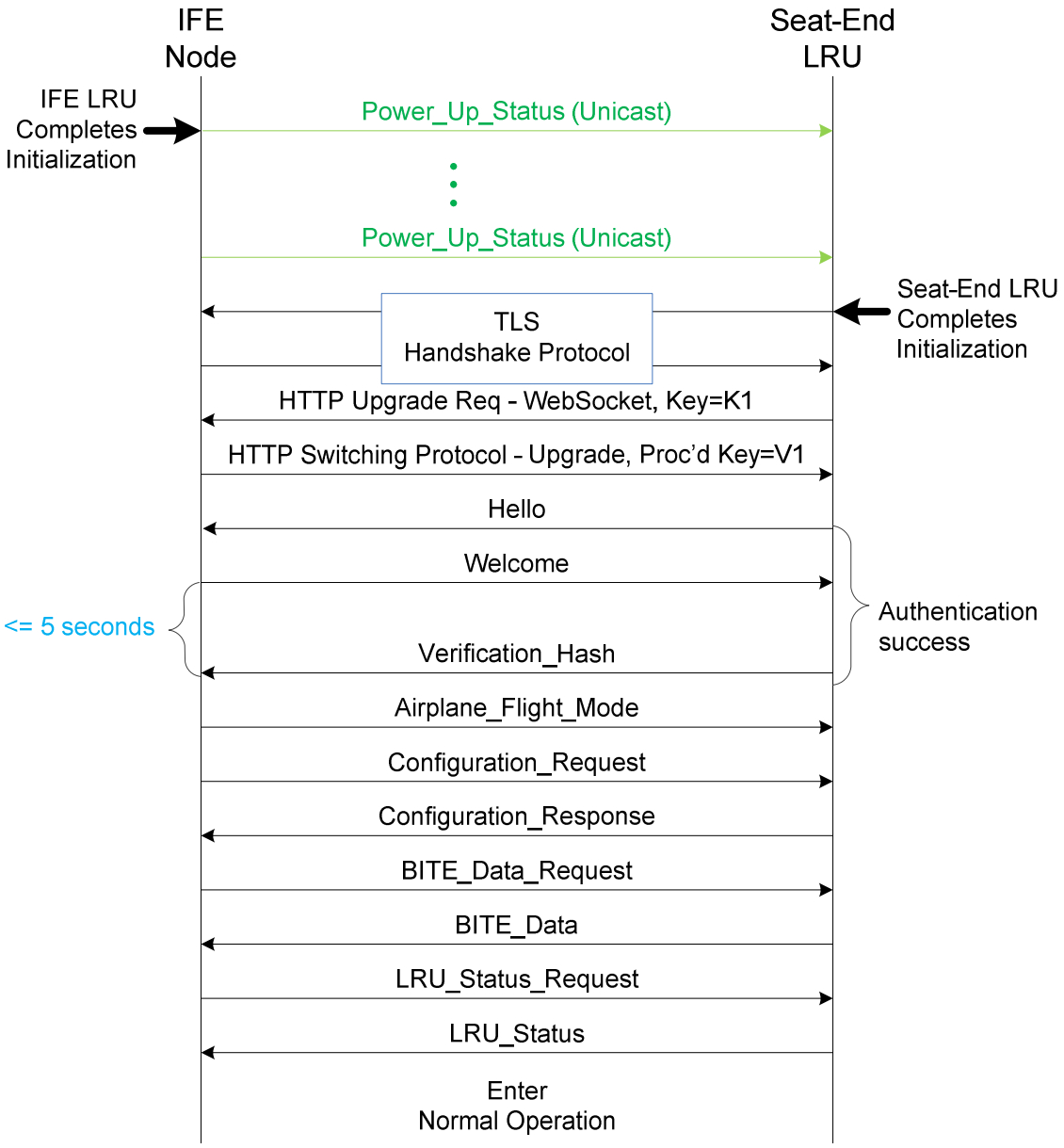
Figure 13 illustrates messages exchange between the IFE Node and a Seat-End LRU during power-up initialization when the IFE Node powers-up first.



Notes:
1. UDP Message is highlighted in green. TCP messages are highlighted in black.
2. HTTP Upgrade Req and HTTP Switching Protocol are defined in section 1.3 of RFC 6455.

Figure 13: Power-Up Initialization - IFE Node Power-Up First

Figure 14 illustrates messages exchange between the IFE Node and a Seat-End LRU during power-up initialization when the Seat-End LRU powers-up first.



Notes:
1. UDP Message is highlighted in green. TCP messages are highlighted in black.
2. HTTP Upgrade Req and HTTP Switching Protocol are defined in section 1.3 of RFC 6455.

Figure 14: Power-Up Initialization - Seat-End LRU Power-Up First

4.2 Normal Operation

The IFE Node should broadcast a Status_Request message to all Seat-End equipment with a minimum rate of once every 10 seconds for keeping the communication alive.

During normal operation, if the Seat-End LRU detects any status change, the Seat-End LRU should transmit LRU_Status message to the IFE Node within 100 ms; otherwise, once in every 10 seconds minimum.

Upon detection of the status change, the Seat-End LRU transmits the LRU_Status message to the IFE Node without the request from the IFE Node.

The IFE Node should declare a communication failure, when no message has been received from the Seat-End LRU for 30 seconds or more.

The Seat-End LRU should declare a communication failure, when no message has been received from the IFE Node for 30 seconds or more.

When the IFE Node detects a communication failure, the IFE Node closes its socket and executes the power-up initialization as described in section 5.1.

When the Seat-End LRU detects the communication failure, the Seat-End LRU closes its socket and tries to re-connect to the IFE Node via power-up initialization as described in section 4.1.

Figure 15 illustrates messages exchange between the IFE Node and a Seat-End LRU during normal operation.

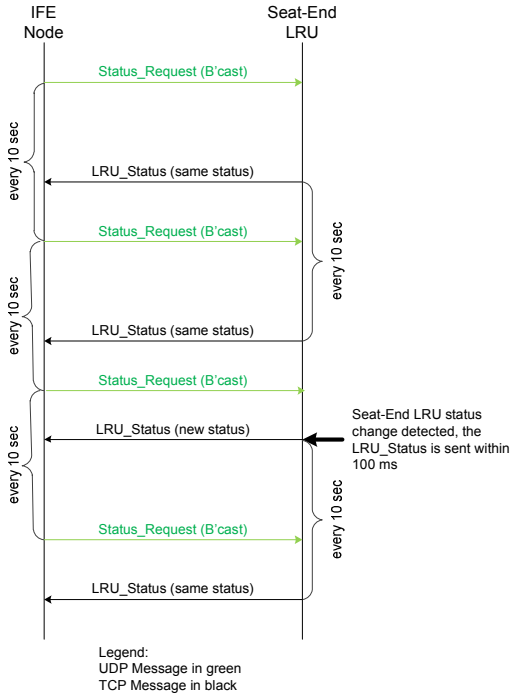


Figure 15: Normal Operation

Figure 16 illustrates messages exchange between the IFE Node and a Seat-End LRU for a communication failure that is caused by the Seat-End LRU.

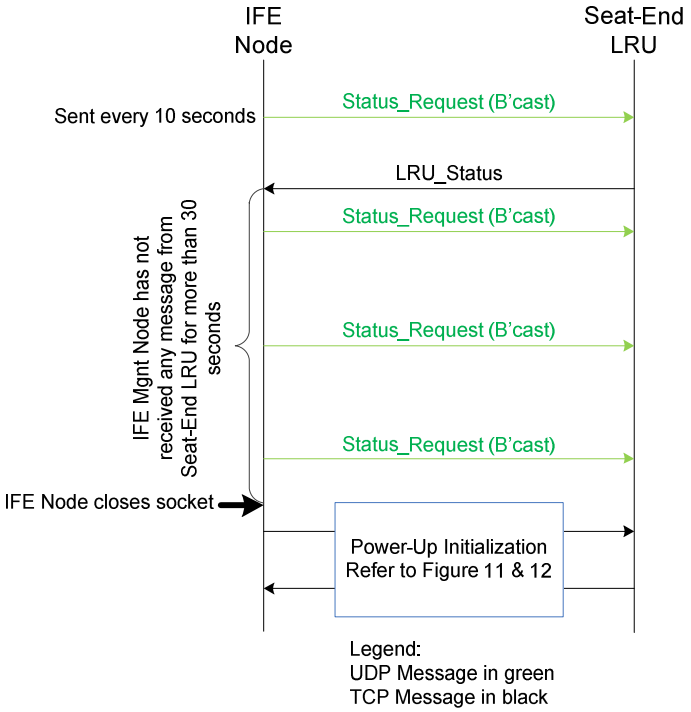


Figure 16: Communication Failure – Seat-End Failure

Figure 17 illustrates messages exchange between the IFE Node and a Seat-End LRU for a communication failure that is caused by the IFE Node.

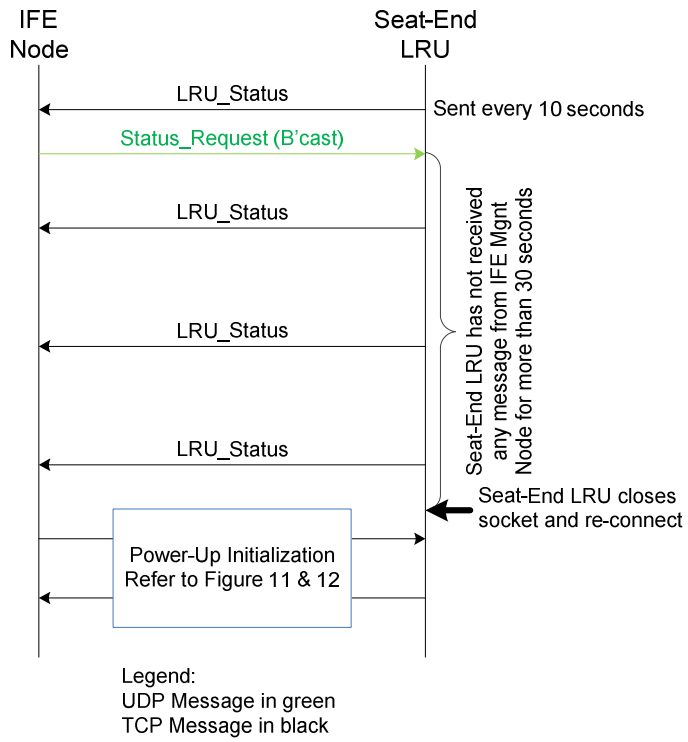


Figure 17: Communication Failure – IFE Node Failure

4.3 Configuration Request

The IFE Node queries the Seat-End LRU with the Configuration_Request message.

The Seat-End LRU should respond with the Configuration_Response message within 1 second.

4.4 Continuous Build-In Test (BIT)

All Seat-End LRUs should support continuous BIT monitoring.

The Seat-End LRU reports the fault data when the Seat-End LRU detects a fault transition state change, i.e., either a change from normal (fault inactive) to abnormal (fault active) state or a change from abnormal state (fault active) to normal (fault inactive) state.

Upon detection of BIT fault state change, the Seat-End LRU should transmit BITE_Data message to the IFE Node within 1 second.

Note: The Seat-End LRU transmits the BITE_Data message without IFE Node's request.

Upon reception of the Power_Up_Status message, the Seat-End LRU should reset the fault status to initial state and then re-start its BIT monitoring.

If the Seat-End LRU encounters a power cycle/reset, the Seat-End LRU should reset the fault status to initial state and then re-start its BIT monitoring.

After the communication is re-established from a power cycle/reset/communication failure, the Seat-End LRU should transmit all active faults to the IFE Node per communication initialization as described in section 5.1.

Figure 18 illustrates an example of messages exchange between the IFE Node and Seat-End LRU for the Continuous BIT.

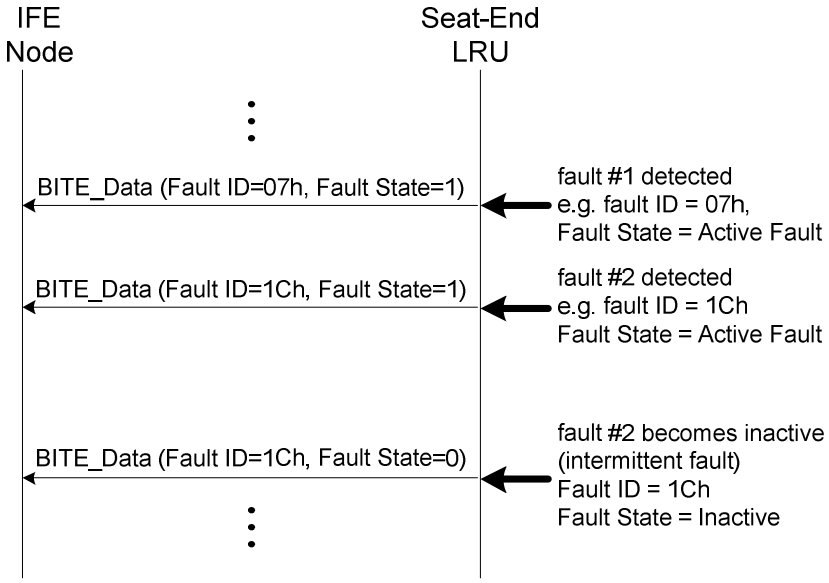


Figure 18: Continuous BIT

4.5 Periodic Message Transmit

The IFE Node may periodically transmit the same messages to the Seat-End LRU and vice versa.

4.5.1 Particular case: manual control held activated on the IFE to be transmitted to the seat peripherals

When a control is activated and held (i.e. button pressed and held) within the IFES, the IFE Node should periodically transmit the control message that is associated with this control to the Seat-End LRU once every 100 ms.

When the control is released, the IFE Node should transmit Button_Released message to the Seat-End within 100 ms.

Upon reception of the Button_Released message, the Seat-End LRU should transmit the LRU_Status message to the IFE Node within 100 ms.

4.5.2 Particular case: manual control held activated on the seat peripherals to be transmitted to the IFE

When a control is activated and held (i.e. button pressed and held) within the seat-end LRUs, the Seat-End LRU should periodically be transmitting the message to the IFE Node once in every 100 ms.

When the control is released, the Seat-End LRU should transmit the Button_Released message to the IFE Node within 100 ms, and then transmit LRU_Status message to the IFE Node within 100 ms.

Figure 19 illustrates a message exchange between an IFE Node and an SAC when a seat control button on one of IFE's PCU is pressed and held active:

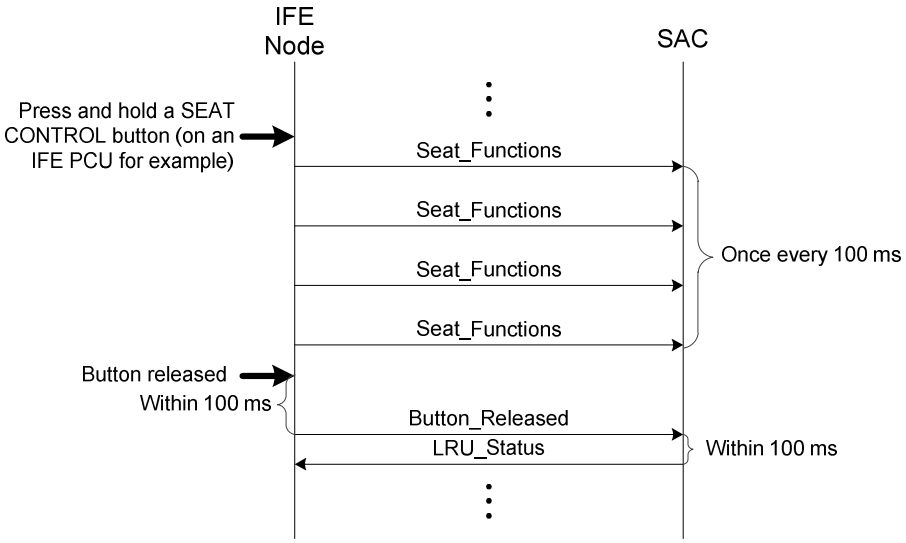


Figure 19: Periodic Message Transmission from IFE Node

Figure 20 illustrates a messages exchange between the IFE Node and a seat-end PCU when a volume control button on a seat-end PCU is pressed and held active:

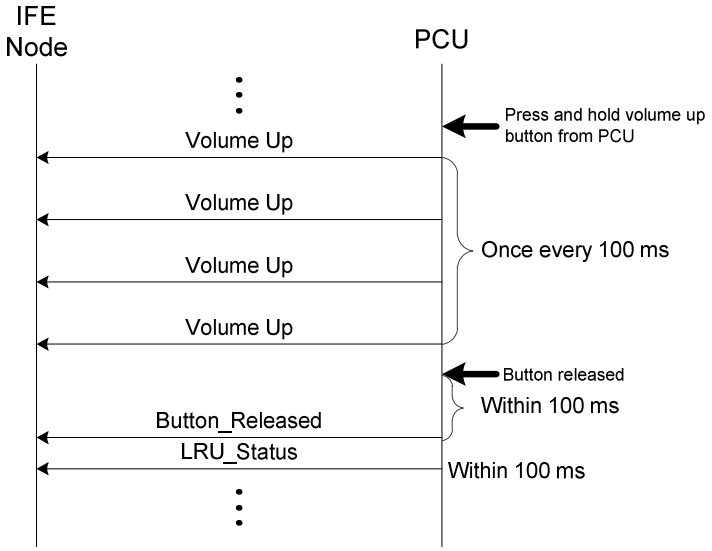


Figure 20: Periodic Messages Transmission from PCU

Notes:

The IFE Node may send two commands to SAC back to back.

The IFE Node may send two different commands back to back, if two controls are activated simultaneously on the IFE side.

4.6 Security Key Update

The Seat-End LRU is pre-installed with a security key in the factory. In the field, the Seat-End LRUs are allowed to update their security key via their interface to the Cabin Equipment Network Bus.

After authentication logic is completed as described in section 4.1.2, the IFE Node and Seat-End LRU should execute the following logic to update the seat end security key:

1. After the communication has been authenticated successfully, if the IFE Node detects that a newer version of the security key is available in its database, the IFE Node transmits the new security key to the Seat-End LRU via the New_Security_Key message.

   Note: In order to protect the confidentiality of the new security key, the Security Key exchange should occur over an encrypted channel over a WebSocket Secure.

2. Upon reception of the new security key, the Seat-End LRU replaces the old security key with the new security key. The old security key is disposed securely per clearing process as defined in section 5 of the NIST SP 800-88 document.
3. The Seat-End LRU transmits the Security_Key_Update_Status to the IFE Node in response to the New_Security_Key message within one second, to report security key update status - success or fail.
4. Upon reception of the Security_Key_Update_Status message, the IFE Node should log the security key update status.
5. Upon reception of the success status, the IFE Node closes its socket and initiates the power-up Initialization as described in section 5.1. If the IFE Node receives the failure status, the IFE Node logs the failure event and enters into the normal operation.

Figure 21 illustrates the message exchange between the IFE Node and the Seat-End LRU to update its security key.

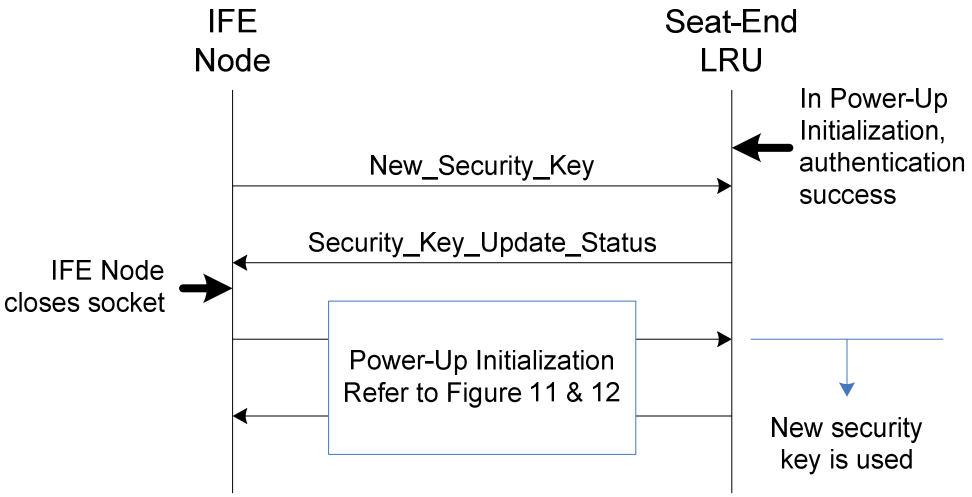


Figure 21: Security Key Update

5.0 COMMON MESSAGE SET

The following messages should be transmitted over an encrypted channel (i.e. WebSocket Secure).

The authentication logic should be requested at each connection attempt from the Seat-End LRU.

5.1 Common Message List

A summary of common messages sent over the Cabin Equipment Network Bus is listed in Table 2.

Table 2: Common Message List

Message	Transmitted by	Transmitted to	Req'd Response Message
Power_Up_Status (unicast)	IFE Node	Seat-End LRU	
Status_Request (broadcast)	IFE Node	Seat-End LRUs	
LRU_Status_Request	IFE Node	Seat-End LRU	LRU_Status
LRU_Status	Seat-End LRU	IFE Node	Note
BITE_Data_Request	IFE Node	Seat-End LRU	BITE_Data
BITE_Data	Seat-End LRU	IFE Node	Note
Configuration_Request	IFE Node	Seat-End LRU	Configuration_Response
Configuration_Response	Seat-End LRU	IFE Node	
Airplane_Flight_Mode	IFE Node	Seat-End LRU	
Hello	Seat-End LRU	IFE Node	Welcome
Welcome	IFE Node	Seat-End LRU	
Verification_Hash	Seat-End LRU	IFE Node	
New_Security_Key	IFE Node	Seat-End LRU	
Security_Key_Update_Status	Seat-End LRU	IFE Node	
New_Trust_Chain	IFE Node	Seat-End LRU	
New_trust_Chain_Status	Seat-End LRU	IFE Node	

Notes: The system allows the Seat-End LRU to initiate the transmission of this message without an IFE Node's request (LRU_Status_Request or BITE_Data_Request).

Table 3 lists command codes for Type 1 and Type 3 common messages.

Table 3: Command Code - Type 1 and Type 3 Command Messages

Message	Command Code (Decimal)	Command Code (Hex)	Message Format
Power_Up_Status	151	97h	Type 3
Status_Request	155	9Bh	Type 1
BITE_Data_Request	181	B5h	Type 3
BITE_Data	182	B6h	Type 3
Configuration_Request	161	A1h	Type 1
Configuration_Response	162	A2h	Type 3

Table 4 lists command codes for Command_2 common messages.

Table 4: Command Code - Common Command_2 Messages

Message	Command_2 Code	Message Format
LRU_Status_Request	LSR	Type 2 Command_2
LRU_Status	RLS	Type 2 Command_2
Airplane_Flight_Mode	AFM	Type 2 Command_2
Hello	HLO	Type 2 Command_2
Welcome	WLM	Type 2 Command_2
Verification_Hash	VFH	Type 2 Command_2
New_Security_Key	NSK	Type 2 Command_2
Security_Key_Update_Status	SUS	Type 2 Command_2
New_Trust_Chain	NTC	Type 4 Command_2
New_Trust_Chain_Status	NTS	Type 2 Command_2

5.2 Common Messages

The following sections define all Seat-End LRU common messages.

5.2.1 Power_Up_Status (151)

Protocol Identifier: 01h
Command: 97h
Data Length: 08h
LRU File Name (8 Bytes)

The Power_Up_Status is transmitted by the IFE Node to the Seat-End LRUs as part of power-up initialization.

The IFE Node should unicast the Power_Up_Status message to the Seat-End LRU once a second using UDP protocol after IFE Node powers up.

Note: Refer to section 3.4.2 for the UDP protocol.

Upon reception of this message, the Seat-End LRU should execute the power-up initialization as described in section 5.1.

LRU File Name: Contains the LRU File Name of the originator of the message. The Seat-End LRU should not check the content of the LRU File Name field sent from the IFE Node. This field is eight ASCII characters in MMMLLLLL format where

MMM = Manufacturer Code.

LLLLL = LRU Type

Examples for IFE LRU: SDB01, SEB03, where 01 and 03 are software revision number.

Examples for Seat end LRU: SPB01, SAC02, PCU03, where 01, 02, 03 are software revision number.

5.2.2 Status_Request (155)

Protocol Identifier: 01h
Command: 9Bh

The IFE Node should broadcast a Status_Request message to Seat-End LRU, using UDP protocol, once in every 10 seconds during normal operation.

5.2.3 LRU_Status_Request (LSR)

Protocol Identifier: 01h
Command: F4h
Data Length: 04h
Command_2: LSR
Status Table Index*

The LRU_Status_Request is transmitted by the IFE Node to the Seat-End LRU to request LRU status.

Upon reception of this message, the Seat-End LRU should respond with the LRU_Status message.

**Status Table Index: ***This field is used by SACs only. Other Seat-End LRUs should set it to zero.

00h: Global status table

01h: SAC and passenger status table PAX1

02h: SAC and passenger status table PAX2

03h: SAC and passenger status table PAX3

FFh: Global, SACs and passenger status for all table (all PAX)

5.2.4 LRU_Status (RLS)

Protocol Identifier: 01h
Command: F4h
Data Length:
Command_2: RLS
LRU Status Table (n Bytes)

The Seat-End LRU should transmit LRU_Status message to the IFE Node in response to the LRU_Status_Request within 100 ms.

Upon detection of any status change, the Seat-End LRU should transmit LRU_Status message to the IFE Node within 100 ms; otherwise, once in 10 seconds.

Note: The Seat-End LRU is able to transmit the LRU_Status message to the IFE Node in the following conditions:

- In response to the LRU_Status_Request message
- Upon detection a status change, initiates the transmission without IFE Node's request (LRU_Status_Request)

Data Length: Refer to LRU specific section in this document.

LRU Status Table: Refer to LRU specific section in this document.

5.2.5 BITE_Data_Request (181)

Protocol Identifier: 01h
Command: B5h
Data Length: 08h
LRU File Name (8 Bytes)

The BITE_Data_Request is transmitted by the IFE Node to the Seat-End LRU to request for all active BIT faults.

Upon reception of this message, the Seat-End LRU should respond with the BITE_Data message.

LRU File Name: Refer to section 5.2.1.

5.2.6 BITE_Data (182)

Protocol Identifier: 01h
Command: B6h
Data Length:
LRU File Name (8 Bytes)
Number of Faults
Fault ID Code
Fault State
• • •
Fault ID Code
Fault State

The Seat-End LRU should transmit BITE_Data message to the IFE Node in response to a BITE_Data_Request within 1 second with all active faults only.

Upon detection of BIT fault(s), the Seat-End LRU should transmit BITE_Data message to the IFE Node within 1 second.

Notes:

1. *If the Seat-End LRU transmits this message without IFE Node's request (BITE_Data_Request), the Seat-End LRU only reports faults (both active and inactive) that were detected since previous BITE_Data was transmitted.*
2. *The Seat-End LRU is able to transmit the BITE_Data message to the IFE Node in the following conditions:*
   a) *In response to the BITE_Data_Request message*
   b) *Upon detection of a fault, initiates the transmission without IFE Node's request (BITE_Data_Request).*

Data Length: Number of Faults * 2 + 9.

LRU File Name: Refer to section 5.2.1.

Number of Faults: Range from 0 to 255.

Fault ID Code: Refer to LRU specific ICD.

Fault State: 0 = Inactive fault, 1 = Active fault

5.2.7 Configuration_Request (161)

Protocol Identifier: 01h
Command: A1h

The Configuration_Request is transmitted by the IFE Node to the Seat-End LRU to request for the LRU configuration.

Upon reception of the Configuration_Request, the Seat-End LRU should respond with the Configuration_Response message within one second.

5.2.8 Configuration_Response (162)

Protocol Identifier: 01h
Command: A2h
Data Length: 4Ch
LRU File Name (8 Bytes)
HW Part Number (16 Bytes)
OPS SW Part Number (16 Bytes)
Database Part Number (16 Bytes)
Serial Number (16 Bytes)
Mod Level (2 Bytes)
Security Key Revision (2 Bytes)

The Seat-End LRU should transmit Configuration_Response message to the IFE Node in response to a Configuration_Request within 1 second.

LRU File Name: Refer to section 5.2.1.

HW Part Number: This sixteen ASCII character field should contain an unalterable hardware part number provided by the manufacturer.

OPS SW Part Number: This sixteen ASCII character field should contain an alterable Operational Software (OPS) part number provided by the manufacturer.

Database Part Number: This sixteen ASCII character field should contain an alterable database part number provided by the manufacturer.

Serial Number: This sixteen ASCII character field should contain an unalterable serial number provided by the manufacturer.

Mod Level: This two ASCII character field should contain an alterable mod level provided by the manufacturer.

Security Key Revision: This two ASCII character field should contain an alterable security key revision provided by the manufacturer.

All number fields are left justified and padded with ASCII space characters (20h). If the number field is not applicable it should be filled with ASCII space characters (20h).

5.2.9 Airplane_Flight_Mode (AFM)

Protocol Identifier: 01h
Command: F4h
Data Length: 0Dh
Command_2: AFM
Flight Phase
Aircraft Time (per ARINC 628 part 3)
Aircraft Identification (3 Bytes)

The Airplane_Flight_Mode is transmitted by the IFE Node to the Seat-End LRU:

1. During initialization.
2. No more than 100ms after the flight phase changes.
3. Otherwise, once a second.

- **Flight Phase:**

  0 = Unknown

  1 = Pre-Flight Ground

  2 = Taxi Out

  3 = Take Off

  4 = Climb

  5 = Cruise

6 = Descent/Approach

7 = Touch Down

8 = Taxi In

9 = Post Flight Ground

Note: Refer to Appendix B for Aircraft Flight Phase Mapping.

- **Aircraft Time:** Refer to ARINC 628 Part 3.
- **Aircraft identification:** Per ICAO standard 24-bit code definition.

5.2.10 Hello (HLO)

Protocol Identifier: 01h
Command: F4h
Data Length: 15h
Command_2: HLO
LRU ID (16 Bytes)
Security Key Revision (2 Bytes)

The Hello message is transmitted by the Seat-End LRU to the IFE Node for the communication authentication.

Upon reception of this message, the IFE Node should respond with the Welcome message within one second.

LRU ID: This sixteen ASCII character field should contain an unalterable hardware part number provided by the manufacturer.

Security Key Revision: This two ASCII character field should contain an alterable security key revision provided by the manufacturer.

5.2.11 Welcome (WLM)

Protocol Identifier: 01h
Command: F4h
Data Length: 11h
Command_2: WLM
Year (4 Bytes)
Month (2 Bytes)
Day (2 Bytes)

Hour (2 Bytes)
Minute (2 Bytes)
Second (2 Bytes)

The Welcome message is transmitted by the IFE Node to the Seat-End LRU for communication authentication.

Upon reception of the Hello message, the IFE Node should respond with this message within one second.

- **Year:** This 4 bytes ASCII character indicate the year in GMT
- **Month:** This 2 bytes ASCII character indicate the month in GMT
- **Day:** This 2 bytes ASCII character indicate the day in GMT
- **Hour:** This 2 bytes ASCII character indicate the 24-hour format of hour in GMT
- **Minute:** This 2 bytes ASCII character indicate the minute in GMT
- **Second:** This 2 bytes ASCII character indicate the second in GMT

Example: February 7, 2017 at 10:41 PM 25 seconds:

Year: 2017 (32h 30h 31h 37h)

Month: February (30h 32h)

Day: 07 (30h 37h)

Hour: 10 PM (32h 32h)

Minute: 41 (34h 31h)

Second: 25 (32h 35h)

5.2.12 Verification_Hash (VFH)

Protocol Identifier: 01h
Command: F4h
Data Length: 43h
Command_2: VFH
Destination Hash (64 Bytes)

The Verification_Hash is transmitted by the Seat-End LRU to the IFE Node for the communication authentication.

The Seat-End LRU should transmit the Verification_Hash to the IFE Node in response to the Welcome message within 5 seconds.

If the IFE Node detects that Destination Hash does not match the Origination Hash, all subsequent messages from the Seat-End LRU should be denied.

Destination Hash: A 64-byte SHA-256 hash code in ASCII format.

COMMENTARY

A hash is a cryptographic checksum. It should be the SHA-256 algorithm as defined in RFC4634. The Destination Hash generated by the Seat-End LRU which is the concatenation of the security key and timestamp (the same timestamp that is provided by the Welcome message). The concatenation sequence is security key first and then the timestamp.

Input string format for SHA-256 hash computation (in ASCII):

Security Key (16 bytes)	Year (4 bytes)	Month (2 bytes)	Day (2 bytes)	Hour (2 bytes)	Minute (2 bytes)	Second (2 bytes)

Figure 22 illustrates the algorithm to compute the Destination hash.

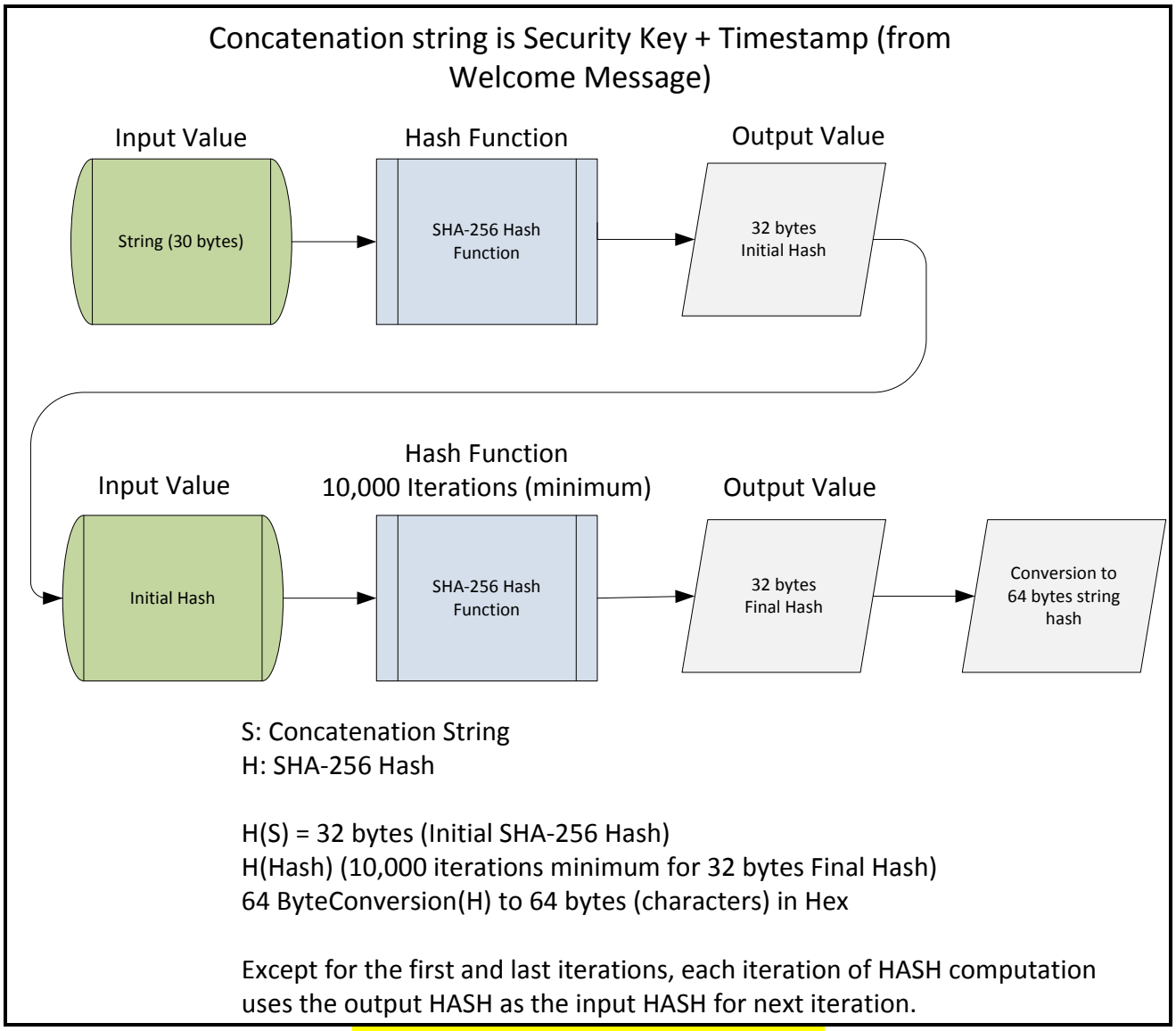


Figure 22: Destination Hash algorithm

5.2.13 New_Security_Key (NSK)

Protocol Identifier: 01h
Command: F4h
Data Length: 15h
Command_2: NSK
New Security Key Revision (2 Bytes)

New Security Key (16 Bytes)

The New_Security_Key is transmitted by the IFE Node to the Seat-End LRU to provide the new security key for the Seat-End LRU.

Upon reception of this message, the Seat-End LRU should replace the old security key with this new security key and store it in its NV RAM.

New Security Key Revision: This two ASCII character field should contain an alterable security key revision provided by the manufacturer.

New Security Key: A 16 bytes binary codes.

5.2.14 Security_Key_Update_Status (SUS)

Protocol Identifier: 01h
Command: F4h
Data Length: 06h
Command_2: SUS
Security Key Revision (2 Bytes)
Status

The Security_Key_Update_Status message is used by the Seat-End LRU to report the security key update status to the IFE Node.

The Security_Key_Update_Status message should be transmitted by Seat-End LRU to the IFE Node in response to the New_Security_Key within 1 second.

Security Key Revision: This two ASCII character field should contain an alterable security key revision provided by the manufacturer.

Status: 0 = Security Key change failed; 1 = Security Key change successful.

5.2.15 New_Trust_Chain (NTC)

Protocol Identifier: 01h
Command: F6h
Data Length (MSB)
Data Length (LSB)
Command_2: NTC
New IFE Vendor CA (n Bytes)

The New_Trust_Chain message is transmitted by the IFE Node to the Seat-End LRU to provide the new IFE Vendor CA for the Seat-End LRU.

Upon reception of this message, the Seat-End LRU should replace the old IFE Vendor CA with this new IFE Vendor CA.

Data Length: This field contains the value of the data length of the “New IFE Vendor CA” field + 3 bytes of Command_2.

New IFE Vendor CA: Up to 2045 bytes binary codes in Certificate Revocation List (CRL) format.

5.2.16 New_Trust_Chain_Status (NTS)

Protocol Identifier: 01h
Command: F4h
Data Length: 04h
Command_2: NTS
Status

The New_Trust_Chain_Status message is used by the Seat-End LRU to report the trust chain update status to the IFE Node.

The New_Trust_Chain_Status message should be transmitted by Seat-End LRU to the IFE Node in response to the New_Trust_Chain within 1 second.

Status: 0 = CA update fails; 1 = CA update successful.

6.0 SECURITY

Historically, Cabin Systems have been considered secure through the use of physical security. That is to say, physical access had to be obtained through the penetration of physical barriers (shrouds, covers, etc.). Today, there is strong emphasis on "opening" up cabin systems to interaction and control by commercial devices which will not require physical access to the system. In addition, several incidents of physical breach of cabin equipment/systems have occurred casting doubt on the effectiveness of continued use of physical security as the only method of maintaining the integrity of a cabin system.

At the same time, a wide range of techniques are evolving to provide security to small, low power, low costs nodes on a network. Often referred to as the Internet of Things (IoT) the domain of sensor nodes on a broader network being secure but accessible has become a major area of technical development.

It is highly desirable for nodes on the Cabin Equipment Network Bus to be simple, small, and low cost. The underlying technology of IoT devices should provide this as long as our standard adopts the appropriate limitations associated with IoT equipment.

Security is often approached through the use of a "layering" of procedures and actions. Each layer of protection maintains significant independence from the other layers so the breach of one layer does not compromise other layers.

6.1 Ports Configuration

By default (out of ATP), only the ports between the IFE Node and the seat end equipment directly connected to it should be open, the rest should be closed.

6.2 Network Communication

6.2.1 Encryption

To ensure confidentiality of the Seat-End LRUs authentication to the IFE Node, all connections should be delivered in an encrypted channel (WebSocket over TLS i.e. WebSocket Secure).

6.2.2 Authentication

To avoid cases where a hacker could connect to an unused port (or reused an existing port) of a Seat-End LRU, there is a need for all communications from Seat-End LRU to the IFE Node to be authenticated.

The authentication is enforced on each connection attempt from the Seat-End LRU to IFE Node.

The challenge/response authentication protocol should work as illustrated in Figure 23.

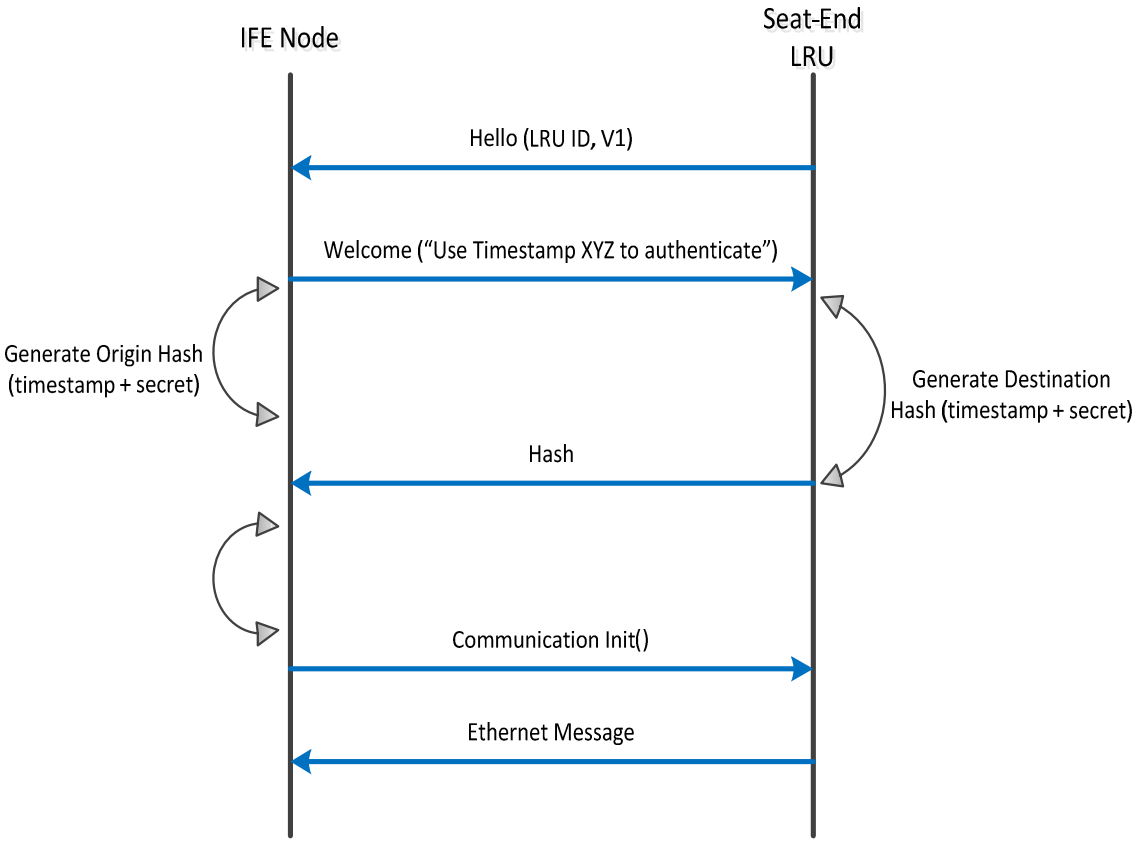


Figure 23: Challenge/Response Authentication

At boot-up, the IFE Node waits for connection attempts from Seat-End LRUs.

Upon connection over a WebSocket Secure, the Seat-End LRU provides its unique ID and the revision of the security key.

If a Seat-End LRU does not answer to the challenge/response correctly, all subsequent commands from the Seat-End LRU should be denied by the IFE Node.

The IFE Node requests the Seat-End LRU at each connection attempt. If connection drops, the IFE Node requests the Seat-End LRU to re-authenticate at the next connection attempt.

All Seat-End LRUs are pre-configured with a unique IP. All commands received by an unknown IP should be denied.

Pre-requisite:

- Each SAC type (same secret for all SAC of a type) needs to be loaded with a unique secret provided by the IFE Vendor.
- Each SPB type (same secret for all SPB of a type) needs to be loaded with a unique secret provided by the IFE Vendor.
- Each PCU type (same secret for all PCU of a type) needs to be loaded with a unique secret provided by the IFE Vendor.

- Each Lighting System type (same secret for all Lighting System of a type) needs to be loaded with a unique secret provided by the IFE Vendor.

6.3 Firewalling

Since the IFE Node is the gateway for all communication coming from the Seat-End LRU, a firewall should be deployed on the IFE Node.

At boot-up, the IFE Node reads its seat-configuration and only allows communication for the IPs of the Seat-End LRU on the specific WebSocket Secure port defined by the in seat-configuration.

The firewall should filter all traffic coming from the IFE network going to the Seat-End LRU. Only the IFE 100BaseT1 Master connected to the seat end LRU should be allowed to communicate to the Seat-End LRU on specific ports.

The IFE Node should not forward any traffic from IFE domain to Seat-End LRUs.

The firewall should filter all traffic coming from the Seat-End LRUs (except if originally initiated from the IFE Node). In other words, the IFE Node should not forward any traffic from the Seat-End LRU to the IFE domain.

6.4 Recommended Cipher Suites for the TLS Communication

The table lists the recommended cipher suites for SSL/TLS 1.2 connections.

ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-CHACHA20-POLY1305
ECDHE-RSA-CHACHA20-POLY1305
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256

Figure 23: Challenge/Response Authentication

7.0 EQUIPMENT SPECIFIC MESSAGES

This section describes equipment specific message sets based on the seat network architecture proposed in Figure 7.

7.1 ECU/SAC Messages

The message set between the IFE Node and the ECU/SAC should include messages to control and get feedback on the following set of features (if implemented):

- Seat actuation
- Seat preset positions
- In-seat lighting (including mood lighting)
- In-seat PCU (under seat ECU/SAC control)
- Electro-mechanical window shades control
- Mechanical partition control
- Maintenance exchange

7.1.1 Message Catalogue

Table 5 and Table 6 list command codes for the ECU/SAC specific messages.

Table 5: Command Codes – ECU/SAC Type 3 Specific Commands

Message	Command Code (Decimal)	Command Code (Hex)	Message Type
BITE_Data	182	B6h	Type 3

Table 6: Command CodeS - SAC Specific Command_2

Message	Command_2 Code
Button_Released	BTR (42h 54h 52h)
LRU_Status	RLS (52h 4Ch 53h)
Direct_Seat_Functions	SFC (53h 46h 43h)
Light_Control	LTC (4Ch 54h 43h)
Mood_Lighting Control	MLC (4Dh 4Ch 43h)
Do_Not_Disturb	DND (44h 4Eh 44h)

Message	Command_2 Code
InSeatScreen_On_Off_Toggle	TVT (54h 56h 54h)
Volume_Up	VOU (56h 4Fh 55h)
Volume_Down	VOD (56h 4Fh 44h)
AVOD_Play_Pause_Toggle	PPT (50h 50h 54h)
Flight_Attendant_Call	FAC (46h 41h 49h)
Airplane_Flight_Information	AFI (41h 46h 49h)

7.1.2 Detailed Description

In this section, all messages from the message catalogue are detailed.

7.1.2.1 BITE_Data (182)

Protocol Identifier: 01h
Command: B6h
Data Length:
LRU File name (8 Bytes)
Fault Status
Number of Faults (1 Byte)
Fault ID Code (1 Byte)
Fault State (1 Byte)
. . .
Fault ID Code (1 Byte)
Fault State (1 Byte)

The SAC should transmit the BITE_Data message with all active faults to the IFE Node in response to a BITE_Data_Request within 1 second.

Upon detection of any BIT faults, the SAC should transmit the BITE_Data message

with active and inactive faults to the IFE Node within 1 second.

Note: The SAC is able to transmit the BITE_Data message to the IFE Node in the following conditions:

- *In response to the BITE_Data_Request message. The SAC only reports all active faults.*
- *Upon detection of a fault, the SAC initiates the transmission without IFE Node's request (BITE_Data_Request). The SAC reports both active and inactive faults that were detected since pervious BITE_Data was transmitted.*

LRU File Name: Refer to section 5.2.1.

Fault Status:

0 = this message only contains current active faults.

1 = this message contains both active and inactive faults that were detected since previous BITE_Data message was sent.

Number of Faults (in Hex): Range from 0 to 255.

Fault ID Code (in Hex): Fault ID Codes are defined by the SAC/ECU vendor

Fault State (in Hex): Current state of the fault.00h = Inactive fault

01h = Active fault

02h to FFh = Unused

7.1.2.2 Button_Released (Command_2: BTR 42h 54h 52h)

The Button_Released message is transmitted by the SAC to the IFE NODE when a button is released from the press and hold event. The structure of the message is as follows:

Protocol Identifier: 01h
Command: F4h
Data Length: 03h
Command_2: BTR

7.1.2.3 LRU_Status (Command_2: RLS 52h 4Ch 53h)

The SAC should transmit the LRU_Status message to the IFE Node in response to the LRU_Status_Request within 100 ms.

Upon detection of any status change, the SAC should transmit LRU_Status message to the IFE Node within 100 ms; otherwise, once every 10 seconds.

The structure of the message is as follows:

Protocol Identifier: 01h

Command: F4h
Data Length: Variable
Command_2: RLS
Status Table ID
Global Status
SAC Status Table (Variable)

Note: The Seat-End LRU is able to transmit the LRU_Status message to the IFE Node in the following conditions:

- *In response to the LRU_Status_Request message*
- *Upon detection of any status change, the SAC initiates the transmission without IFE Mgnt Node's request (LRU_Status_Request)*

The standard provisions for multiple seats under the control of one SAC/ECU. These are referred to as PAXn where n is the number of seats controlled by the SAC.

Status Table ID:

00h – Global status table

01h – SAC and status table seat PAX1

02h – SAC and status table seat PAX2

03h – SAC and status table seat PAX3

…

FFh – Global, SACs and passenger status for all table (all PAX)

SAC Status Table: Table 7 defines the SACS Global Status.

Table 7: SAC Status Tables

Global Status:

Byte	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
0	PBIT OK	THERMAL LIMITS REACHED	Power Limit Mode	SW Error	PBIT ONGOING	BIT Data Ready	Spare	Spare

SAC Status Table:

Byte	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0

Variable	SAC Vendor Defined

7.1.2.4 Direct_Seat_Functions (Command_2: SFC 53h 46h 43h)

This message is used by the IFE Node to control an SAC seat function directly. The structure of this message is as follows:

Protocol Identifier: 01h
Command: F4h
Data Length: 07h
Command_2: SFC
Seat Command (3 Bytes)
Seat Index

Seat Index (in Hex): This message supports one or more seats per SAC, with Seat Index providing the seat number (starting from zero). If only one seat is addressed the Seat Index should be set to zero.

Seat commands should be encoded in ASCII. The table below gives simple examples of ASCII encoding of common seat functions:

Seat Command	Mode of Control	Command Code (in ASCII)
Headrest Up	Press and Hold	HRU
Headrest Down	Press and Hold	HRD
Backrest Recline Up	Press and Hold	BRU
Backrest Recline Down	Press and Hold	BRD
Armrests Up	Press and Hold	ARU
Armrests Down	Press and Hold	ARD
Back to TTOL position	Press and Hold	TTL
Go to Bed position	Press and Hold	BED
Go to Dine position	Press and Hold	DIN

Seat Command	Mode of Control	Command Code (in ASCII)
Record current position	One Touch	MSV
Recall recorded position	Press and Hold	MRC

7.1.2.5 Light_Control (Command_2: LTC 4Ch 54h 43h)

This message allows the IFE Node to control a dimmable light within the seat. The structure of the message is as follows:

Protocol Identifier: 01h
Command: F4h
Data Length: 04h
Command_2: LTC
Light ID
Light Brightness

The Light_Control message is transmitted by the IFE Node to the SAC when the IFE Node needs to control an SAC-controlled seat environment light.

Upon reception of this message, the SAC should turn on (with brightness) or off the light within 100 ms.

If a seat light button is pressed and held, the SAC should transmit the Light_Control message periodically (at least once every 100 ms).

As soon as the button is released, the SAC should stop sending the Light_Control message and should transmit the Button_Released message within 100 ms.

Light ID (in Hex): indicates which light within the SAC domain to address. Default is zero if only one light is present.

Light Brightness (in Hex): Range from 0x00 (off) to 0xFF (max level).

7.1.3 Mood_Lighting_Control (Command_2: MLC 4Dh 4Ch 43h)

The Mood_Lighting_Control message is transmitted by the IFE NODE to the SAC.

Mood Lighting is managed by the Cabin System per ARINC Specification 628 part 3.

The structure of the message is as follows:

Protocol Identifier: 01h
Command: F4h
Data Length: 04h
Command_2: MLC
Scene ID

This message assumes that the SACS contains a scene database. And that the IFE Node can translate a Scene status from the Cabin System into a corresponding Scene ID for the SAC.

Upon reception of this message, the SACS should change the mood lighting from its current scene to the scene identified by Scene ID within 100ms.

Scene ID (in Hex): Range from 0x00 to 0xFF.

7.1.3.1 Do_Not_Disturb (Command_2: DND 44h 4Eh 44h)

A seat may include a visual do-not-disturb sign to inform the crew that a passenger does not want to be disturbed during non-emergency situations such as a meal service for example. This message is used when the toggle of this indicator can be triggered from the IFE. The structure of this message is as follows:

Protocol Identifier: 01h
Command: F4h
Data Length: 03h
Command_2: DND

The Do_Not_Disturb message is transmitted by the IFE NODE to the SAC.

Upon reception of this message, the SAC should toggle the Do Not Disturb indicator within 100ms.

7.1.3.2 InSeatScreen_On_Off_Toggle (Command_2: TVT 54h 56h 54h)

This message is used by the SAC when a dedicated TV ON/OFF control is within the SAC perimeter. The structure of this message is as follows:

Protocol Identifier: 01h
Command: F4h
Data Length: 03h
Command_2: TVT

The InSeatScreen_On_Off_Toggle message is transmitted by the SAC to the IFE NODE.

Upon reception of this message, the IFE Node shall toggle the backlight on/off of all in-seat screens within 100ms.

7.1.3.3 Volume_Up (Command_2: VOU 56h 4Fh 55h)

The VOLUME_UP message is defined so that the SAC can control the audio volume level of the IFE equipment. It is assumed a “volume up” control/button is available in the seat and controlled by the SAC. The structure of this message is as follows:

Protocol Identifier: 01h
Command: F4h

Data Length: 03h
Command_2: VOU

The Volume_Up message is transmitted by the SAC to the IFE NODE.

Upon reception of this message, the IFEC should increase the headphone volume by one step (under IFE vendor control) within 100 ms.

If the volume up button is pressed and held, the SAC should transmit the Volume_Up message periodically (once every 100 ms).

As soon as the volume up button is released, the SAC should stop sending the Volume_Up message.

As soon as the volume up button is released, the SAC should transmit the Button_Released message within 100 ms.

7.1.3.4 Volume_Down (Command_2: VOD 56h 4Fh 44h)

The VOLUME_DOWN message is defined so that the SAC can control the audio volume level of the IFE equipment. It is assumed a “volume down” control/button is available in the seat and controlled by the SAC. The structure of this message is as follows:

Protocol Identifier: 01h
Command: F4h
Data Length: 03h
Command_2: VOD

The Volume_Down message is transmitted by the SAC to the IFE NODE.

Upon reception of this message, the IFEC should decrease the headphone volume by one step (under IFE vendor control) within 100 ms.

If the volume down button is pressed and held, the SAC should transmit the Volume_Down message periodically (once every 100 ms).

As soon as the volume up button is released, the SAC should stop sending the Volume_Down message.

As soon as the volume up button is released, the SAC should transmit the Button_Released message within 100ms.

7.1.3.5 AVOD_Play_Pause_Toggle (Command_2: PPT 50h 50h 54h)

This message is defined so that a seat can include a dedicated control to pause and resume all Audio Video On Demand (AVOD) activity. The structure of this message is as follows:

Protocol Identifier: 01h
Command: F4h

Data Length: 03h
Command_2: PPT

The AVOD_Play_Pause_Toggle message is transmitted by the SAC to the IFE NODE.

Upon reception of this message, the IFEC should toggle play/pause the AVOD within 100ms.

If the button is pressed and held, the SAC should only transmit the AVOD_Play_Pause_Toggle message once.

7.1.3.6 Flight_Attendant_Call (Command_2: FAC 46h 41h 43h)

This message is defined so that a seat can include a dedicated indicator that a flight attendant call is pending (either for the crew or for the passenger or both). The structure of this message is as follows:

Protocol Identifier: 01h
Command: F4h
Data Length: 04h
Command_2: FAC
FA Call State

The Flight_Attendant_Call is transmitted by the IFE NODE to the SAC.

Upon reception of this message, the SAC should turn on/off the FA Call indicator within 100 ms.

FA Call State (in Hex): 0 = FA Call Cancel; 1 = FA Call, other = ignore.

7.1.3.7 Airplane_Flight_Information (Command_2: AFI 41h 46h 49h)

This message is defined so that the IFE Node can transmit the status of the flight it receives from the Cabin System per ARINC 628 part 3 to the SAC. The SAC can use this information as it sees fit. The structure of this message is as follows:

Protocol Identifier: 01h
Command: F4h
Data Length: 28h
Command_2: AFI

ARINC 628 part 3 Flight Information Table

The Airplane_Flight_Info message is transmitted by the IFE NODE to the ECU/SAC at least once a second.

7.2 Lighting System Messages

TBD

7.3 PCU Messages

TBD

7.4 Seat Power Messages

TBD

APPENDIX A LIST OF ACRONYMS

ACK	Acknowledgement
ARINC	Aeronautical Radio Inc
CDS	Cabin Distribution System
CFR	LRU Configuration Request
DSRQ	Download Status Request
DRQ	Download Request
DC	Download Complete
DS	Download Start
ECU	Electronic Control Unit
EIA	Electronic Industry Association
ELC	Error Log Clear
ELR	Error Log Request
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFES	In-Flight Entertainment System
ISPSU	In-Seat Power Supply Unit
LRU	Line Replaceable Unit
NAK	Negative-Acknowledgement
NVM	Non Volatile Memory
OPS	Operational Software
PAC	Power Actuator Control
PAR	Power Actuator Response
PCS	Power Control State
PCU	Passenger Control Unit
PDU	Protocol Data Unit
PUS	Power Up Status
SAC	Seat Actuator Controller
SACS	Seat Actuator Controller System
SAE	Society of Automotive Engineers
SEB	Seat Electronics Box
SFC	Seat Functions
SFR	Seat Functions Response
SPB	Seat Power box
TIA	Telecommunications Industry Association

APPENDIX B FLIGTH PHASE MAPPING

The following table illustrates how flight phase is mapped.

Flight Phase	Description	Boeing	Airbus
0	Unknown		
1	Pre-Flight Ground		
2	Taxi Out		
3	Take Off		
4	Climb		
5	Cruise		
6	Descent/Approach		
7	Touch Down		
8	Taxi In		
9	Post-Flight Ground		