FAA BAA Call 3:
UAS Command & Control (006)

Contract Number: 697DCK-22-C-00263

Final Test Report (FTR)
Full Report with Appendices B & C

November 20, 2023

Document No.: TestReport-263_Honeywell_20231120-full-Rev2

Revision No.: 2.0

Prepared by:

Honeywell
Aerospace Advanced Technology, ACP RTC
Baltimore, MD and Minneapolis, MN

Northern Plains UAS Test Site
Grand Forks, ND

DOCUMENT REVISION LOG

Revision	Description	Date
1.0	Internal draft	27 Oct 2023
2.0	Added executive summary, updated section 4.1.2	20 Nov 2023

TRADEMARK DISCLAIMER

Table of Contents

Table of Figures

List of Tables

UAS COMMAND & CONTROL (006) - EXECUTIVE SUMMARY

Introduction and Objectives:

The objectives of this project were to develop and demonstrate a multi-link UAS C2 communication system and evaluate the performance in a flight test environment, validate technologies for cybersecurity of C2 links (authentication, integrity, and confidentiality), and also test an alternative positioning navigation system for UAS operations in GPS-denied environments using Honeywell's vision-aided navigation (VAN) system. The technology developed and demonstrated during this project is immensely beneficial for several UAS use cases such as Urban Air Mobility (UAM) air taxi, cargo delivery, or infrastructure inspection (railroad, powerlines, etc.) among others. Accomplishments and benefits from this work:

- Demonstrated seamless C2 communications with CNPC radio links. Communications along the flight path of the UA require the C2 link be switched from one CNPC radio tower to another as the UA flies from LOS to BVLOS. This project demonstrated link switchovers and link transitions under various flight conditions demonstrating BVLOS capability.
- Mitigate lost link scenarios. Honeywell had validated the DO-377A MASPS cybersecurity network switching and interworking requirements in the laboratory under a previous FAA contract. This project validated the C2 link system performance and security in flight trials using multiple C2 link networks, including C-Band, SATCOM, and cellular, switching links as needed to maintain connectivity.
- Advanced alternate navigation technologies. This project demonstrated an alternative vision-aided navigation system based on an infrared camera, map database, and inertial system that Honeywell had previously developed and flight tested to TRL6.

UAS C2 system installed on Alta-X drone (left); Honeywell vision aided navigation (VAN) system installed on Cessna (right)

Technology Description – UAS C2 communication system:

The multi-link UAS C2 communication system that was developed and demonstrated for this project used three commercially available radio links: a C-Band radio from uAvionix, and a small-footprint SATCOM unit from Honeywell that contains both an Inmarsat SATCOM radio and a cellular/LTE radio. The radios interfaced with a Raspberry Pi General Purpose Processor

board, where the C2 link routing and security communication system were implemented. The C2 system was mounted and flown on a Freefly Alta-X drone. However, the Alta-X drone used an independent C2 link for vehicle control to mitigate the risk of depending on the C2 system under test for vehicle control and potentially losing vehicle control during the test flights.

Our C2 system developed and used during this project had two levels of encryption and authentication over each of the links, first using endpoint encryption using WireGuard VPN, and second through the DTLS secure session between the DTSRs.

Technology Description – Alternate Positioning: Honeywell Vision Aided Navigation (VAN)

The airborne components of the vision navigation system were mounted and flight-tested in a Cessna 182 General Aviation (GA) aircraft. However, the vision aided navigation system under test was isolated from any data or power to the aircraft: there were no data or power interfaces to the Cessna aircraft. The main unit with the camera was mounted to the exterior of the Cessna using a Meeker wing-strut mount. An external GPS unit was also mounted to the top of the Cessna for collecting the ground truth positioning data used for performance assessment and validation, and other system components were mounted inside the cabin such as the power supply and a pressure altimeter. The equipment installation on the Cessna required an airworthiness inspection which was conducted by the Flight Standards District Office (FSDO) at Fargo, ND. The Honeywell VAN has now been flight tested on several platforms across many different terrains, flight conditions, and time of day. The current prototype system was originally developed for flight at high altitude on large aircraft, however, during this project, it was successfully demonstrated on a Cessna GA aircraft.

Performance Results – UAS C2 communication system

The C2 system was evaluated on a total of 19 tests on the Alta-X drone: 17 flights plus 2 ground tests. There were 4 distinct test procedures among the 19 tests: 9 flights tested the C2 link lost and recovery procedure, 4 flights tested the flying out of C-Band range procedure, 4 flights tested the link switchover procedure, and the 2 ground tests tested the ground procedure.

Although the tests spanned multiple flights and multiple procedures, key metrics and parameters were collected consistently across all tests such as message latency, switchover times, and signal strength indicators for each of the links.

DO-377A specifies a latency requirement of 1.0 second at least 95% of the time. This latency requirement was met by the cellular/LTE link on all tests. The SATCOM link met the latency requirement on 16 out of 19 flights. And the C-Band link met the latency requirement on all flights (if we exclude the first 7 flights where there were known issues with the C-Band radios that were resolved after the 7th flight).

DO-377A MASPS specifies a requirement for RLP TET of under 3.0 sec. for surface, departure, arrival, and under 5.0 sec. for cruise in class B, C, E, & G airspaces. RLP TET was evaluated by the link switchover commands. During the testing for this project, a total of 65 manually commanded link switchovers were conducted. Out of the 65 switchovers, 51 (78%) met the requirement and completed within the TET limit, and 14 (22%) took longer than the TET limit.

Performance Results – Alternate Positioning: Honeywell Vision Aided Navigation (VAN):

The Honeywell VAN performed as expected during the test scenario, providing accurate navigation information in the absence of GPS. The alternate positioning test scenario was flown twice, with GPS disabled during both tests to demonstrate the APNT solution. The horizontal

position error was less than 5 meters CEP50 for both flights while GPS was disabled. This matches previous flight tests that Honeywell has conducted on other aircraft.

With a fixed focal length camera such as the one used during this testing, position error will increase with altitude due to the matched features in the image becoming larger. The VAN performance of the horizontal position error was 2.7 meters CEP50 at 1,000 ft AGL, and 4.0 meters CEP50 at 3,000 ft AGL.

Findings and Lessons Learned

For next steps, Honeywell has considered how to progress the UAS work accomplished under this project and made submissions under Call 004 and Call 005 BAA that outline our recommended path forward in this area. In these whitepapers, Honeywell plans to incorporate the lessons learned from this project and flight test these improvements and additional features.

Our implementation of the DTSRs used optional procedure 2 as presented in DO-377A: C2 Link System Route Switchovers. We assert that any implementation of this procedure would need to support scenarios where the active link state is inconsistent throughout the network, at least temporarily. Maintaining consistency reliably in the presence of faults is a difficult problem. Therefore, such provisions would ultimately add significant complexity to the software to safely support UAVs in real operational environments.

A C2 link approach consistent with Multilink Operations, as presented in DO-377A, might be used to implement what can be referred to as continuous switchovers or stateless redundancy. This approach would eliminate the need to declare and maintain an active link. Instead, each DTSRs would be able to send and receive messages over any of the available links, eliminating the need to maintain a consistent distributed state across the network at all times.

The C-Band system was unstable and unreliable during initial development and provisioning, having symptoms of very high latency, dropping messages, and intermittently dropping the link at the radio-level. With these symptoms, our C2 software was unable to detect the C-Band link as a suitable link option. During the project, we were able to identify and resolve 3 separate root-causes for the issues observed during the first 7 test flights. First was ground antenna coverage sensitivity, second was issues with having too strong of a signal, and third were software configuration issues with the data rate limits from the radios. However, even after these issues were resolved and the link was adequate for maintaining a secure active link session, the C-Band link continued to have reliability issues because user data messages were still occasionally dropped.

The current Honeywell vision aided navigation (VAN) prototype system is not size, weight, or power (SWAP) optimized and was originally developed for flight at high altitude on large aircraft. For BVLOS operations on a small unmanned UAS, the Honeywell VAN could be implemented using existing sensors on the UAS and ported to the Honeywell Compact Inertial Navigation System (HCINS). HCINS is a small (162 cm3) and lightweight (115 grams) navigation system designed for UAS operations.

FAA UAS Command & Control (006)
Final Test Report

1 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to present the results of inspections, flight tests, and post-flight analyses performed for the Unmanned Aircraft System (UAS) Command and Control (UAS-C2) project under FAA Contract 697DCK-22-C-00263.

1.2 SCOPE

The scope of this report includes the qualitative and quantitative results of inspections and formal flight tests using a representative proof-of-concept system and procedure described in the Detailed Test Procedures [DTP] document.

The report summarizes the flight test results with respect to pass/fail criteria, provides post-test analysis results (e.g., quantitative time-based measurements), and reports the results of inspection activities performed interdependent of the flight tests. This document also presents lessons learned and recommendations for future tests/demonstrations.

1.3 DOCUMENT OVERVIEW

This document is organized into the following sections:

- Section 1 – Introduction

  This section identifies the purpose and scope of the document, summarizes the document organization and provides acronyms, definitions of terminology and references to applicable documents.

- Section 2 – System Under Test Configuration

  This section documents the final flight test configuration of the as-tested C2 Link System under test.

- Section 3 – Inspection and Test Summary

  This section summarizes the structure used in this document to present the result of inspection procedures and test procedures conducted on the C2 Link System under test.

- Section 4 – Inspection Results

  This section documents the detailed inspection and analysis procedures, including both project-specific procedures as well as procedures that are shared in common between the UAS Privacy Protections (UAS-PP) project and the UAS Command and Control (UAS-C2) project. Note that the common inspection/analysis procedures are repeated in each project-specific deliverable.

- Section 5 – Test Results

  This section presents the results of the formal flight and ground-based testing including: a summary of pass/fail results for each of the test cases performed;

results of post-test analyses; and any variances or deviations encountered during testing.

- Section 6 – Summary and Recommendations

  This section provides an overall assessment of the test/inspection results, and where appropriate, provides lessons learned and recommendation for further testing.

- Appendix A – Expected Results

  This appendix documents the expected results for the verification steps in each test procedure.

- Appendix B – Inspection Results- UAS C2 Link System Security

  This appendix documents the results of the inspection for the link system security.

- Appendix C – Inspection Results- VPN for Protecting the UA to the CS

  This appendix documents the results of the inspection of the VPN.

1.4 TERMS AND ABBREVIATIONS

1.4.1 Acronyms

The following acronyms and abbreviations may appear in this document.

Acronym or Abbreviation	Definition
A/G	Air-Ground
AES	Advanced Encryption Standard
AGL	Above Ground Level
ANSI	American National Standards Institute
API	Application Programming Interface
APNT	Alternate Position, Navigation, and Timing
ARS	Airborne Radio System
ATC	Air Traffic Control
BAA	Broad Agency Announcement
BbM	Break before Make
BVLOS	Beyond Visual Line of Sight
C2	Command and Control
C2CSP	Command and Control Communication Service Provider
CM	Common
CNPC	Command and Non-Payload Communications
CS	Control Station
CSP	Communication Service Provider
DC	Direct Current
DSS	Digital Signature Standard
DTLS	Datagram Transport Layer Security
DTP	Detailed Test Plan
DTSR	Data Transfer, Security and Routing
ECDHE	Elliptic Curve Diffie-Hellman - Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
FAA	(US) Federal Aviation Administration
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
FS	File System
GA	General Aviation
GCM	Galois Counter Mode
GCS	Ground Control Station
GPS	Global Positioning System
GPSD	Global Positioning System Denied
GRS	Ground Radio System
GUI	Graphical user Interface
HMAC	Hashed Message Authentication Code
HTTPS	Hypertext Transport Protocol – Secure
Hz	Hertz
I/O	Input/Output
ID	Identifier
IMU	Inertial Measurement Unit
IP	Internet Protocol
IP	Inspection Procedure
IPv4 / IPv6	Internet Protocol version 4 / version 6
IR	Interworking Requirement
ITU	International Telecommunication Union
KPI	Key Performance Indicator
kts	Knots
LMSF	Link Management and Security Function
LOS	Line of Sight
LSMA	Local Storage and Management Application
LTE	Long Term Evolution
LTS	Long Term Support
LWIR	Long Wavelength Infrared

LZ	Landing Zone
MASPS	Minimum Aircraft System Performance Specification
MbB	Make-before-Break
MoC	Means of Communication
MSG	Message
MSL	Mean Sea Level
MTU	Maximum Transmission Unit
N/A	Not Applicable
NIST	National Institute of Standards and Technology
NM	Nautical Mile
NPUASTS	Northern Plains UAS Test Site
NTP	Network Time protocol
OS	Operating System
PP	Privacy Protections
PR	Performance Requirement
RAN	Radio-based Alternate Navigation
RF	Radio Frequency
RFC	Request For Comment
RLP	Required Link Performance
RLTP	Required Link Technical Performance
R-Pi	Raspberry Pi
RPIC	Remote Pilot In Command
RSSI	Received Signal Strength Indicator
Satcom	Satellite Communication
S/N	Serial Number
SER	Security Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SoW	Statement of Work
SR	Status Report
SRS	System Requirements Specification
SSL	Secure Sockets Layer
STP	System Test Plan
TC	Test Case
TCP	Transport Control Protocol
TP	Test Procedure
TET	Transaction Expiration Time
UA	Unmanned/Uncrewed Aircraft
UAS	Unmanned/Uncrewed Aircraft System
UAS-C2	UAS Command and Control (project)
UAS-PP	UAS Privacy Protections (project)
UDMD	User Data Multiplexer-Demultiplexer
UDP	User Datagram Protocol
UND	University of North Dakota
US	United States
USB	Universal Serial Bus
VAC	Volts, Alternating Current
VAN	(Honeywell) Vision Aided Navigation
VDC	Volts, Direct Current
VLAN	Virtual Local Area Network
VLOS	Visual Line of Sight
VM	Virtual Machine
VPN	Virtual Private Network

1.4.2 Terminology

Term	Definition
C2 Link System	The totality of Air/Ground Links, Ground/Ground Links, and DTSR capabilities that support the exchange of C2 Link User Data between the CS and UA C2 Link Executive Management System.
C2 Link System Communication Service Provider	The C2 Link System Communication Service Provider (C2CSP) provides a portion of or all of the C2 Link System for the operation of a UAS. The C2CSP is integrated into the Safety Management System process of the certified UAS operation and is overseen by a Competent Authority designated by the certifying aviation authority.
C2 Link System Control Messages	The various messages used to establish, maintain, terminate, switchover, and handover a C2 Link System Connection. These messages are carried on the logical Control Plane part of the C2 Link System Connection. Note: In this document, use of the truncated term "Control Messages" should be interpreted as "C2 Link System Control Messages."
C2 Link System Scheduled Switchover	A switchover that is scheduled to occur at a specific time and/or with the UA in a specific location.
C2 Link System User Data	Data coming from and going to CS and UA applications and subsystems that is exchanged over the C2 Link System Connection to support the remote pilot's Aviate, Communicate, Navigate, Integrate and Manage C2 Link System tasks. This data is carried on the logical User Plane part of the C2 Link System Connection. Note: In this document, use of the truncated term "User Data" should be interpreted as "C2 Link System User Data."
Control Messages	See definition for C2 Link System Control Messages
Control Plane Traffic	Control plane traffic is signaling traffic between CS and US C2 Link management functions to support establishing, maintaining, and terminating C2 Link System connectivity between the CS and UA. See definiton of C2 Link System Control Messages.
DTSR Subsystem	The subsystem that is responsible for establishing secure, i.e., authenticated, connections between per security systems on the UA and CS, for selecting the route/path that the C2 Link User Data flows and for switching the route when more than one path through the C2 Link is possible
Networked Link	A terrestrial or Satcom link between a UA and CS that uses a multiple access (multi-user) RF link between the UA and a Terrestrial or Satcom Air/Ground Access Network and a secure connection between the CS and the Air/Ground Access Network Gateway to provide a link between the UA and CS. This networked link may be provided by a C2 Link System Communications Service Provider (C2CSP).
User Data	See definition for C2 Link System User Data
User Plane Traffic	User plane (also called end-to-end or data plane) traffic is user traffic communicated between the UA and the pilot station. See definition of C2 Link System User Data.

1.5 APPLICABLE REFERENCE DOCUMENTS

The following documents are referenced in this report using the notation [XXX], where XXX is the shorthand document reference.

1.5.1 Industry – RTCA

Shorthand	Document Number	Document Description
DO-377A	DO-377A	Minimum Aviation System Performance Standards for C2 Link Systems Supporting Operations of Unmanned Aircraft Systems in US Airspace, 16 September 2021

1.5.2 Industry – NIST

Shorthand	Document Number	Document Description
38D	SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf
56A	SP 800-56A, Rev. 3	Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, April 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
131A	SP 800-131A, Rev. 2	Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf
180-4	FIPS 180-4	Secure Hash Standard (SHS), August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
186-4	FIPS 186-4	Digital Signature Standard (DSS), July 2013 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
197	FIPS 197	Advanced Encryption Standard (AES), November 2001 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
198-1	FIPS 198-1	The Keyed-Hashed Message Authentication Code (HMAC), July 2008 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf

1.5.3 Industry – International Telecommunication Union (ITU)

Shorthand	Document Number	Document Description
X.509	ITU-T X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks, October 2019 https://www.itu.int/rec/T-REC-X.509-201910-I/en

1.5.4 Industry – Internet Request for Comment (RFC)

Shorthand	Document Number	Document Description
6347	RFC 6347	Datagram Transport Layer Security Protocol Version 1.2 https://datatracker.ietf.org/doc/html/rfc6347

1.5.5 Project Documents

Shorthand	Document Number	Document Description
DTP	TestProcedures-263_HON_20230501	FAA BAA Call 3: UAS Command and Control (006) – Detailed Test Procedures, 01 May 2023
STP	TestPlan-265_Honeywell_20230127	FAA BAA Call 3: Command and Control (006) – System Test Plan, 01 February 2023

2 SYSTEM UNDER TEST CONFIGURATION

This section documents the final flight test configuration of the as-tested C2 Link System under test.

2.1 FLIGHT TEST CONFIGURATION

2.1.1 Airborne System

The UAS-C2 project was configured with two separate flight configurations for each of the two flight scenarios. The first configuration for the C2 system that was flown on the Alta-X drone is illustrated in Figure 2-1, and the second configuration for the Vision Aided Navigation system that was flown on the Cessna is illustrated in Figure 2-3.

The C2 Link System interworking and security functionality is implemented in software running on a Raspberry Pi 4B computing platform (Figure 2-1, right). The integrated Honeywell VersaWave® Satcom avionics (Figure 2-1, upper-left) interconnects with the Raspberry Pi via an Ethernet connection. The Satcom avionics interfaces with a Satcom antenna unit and four LTE antennas. The uAvionix C-Band Airborne Radio System (ARS, Figure 2-1, lower-left) interface with the Raspberry Pi via RS-232 serial connections, one directly to an RS-232 port and one through an RS-232 to USB converter.

The airborne components for the UA were integrated by NPUASTS on an Alta-X Freefly drone owned by NPUASTS. As part of the integration activity, NPUASTS provided an on-vehicle power module that supplies 28VDC to the Satcom+LTE avionics unit and to the C-Band radio, and 5VDC to the Raspberry Pi.

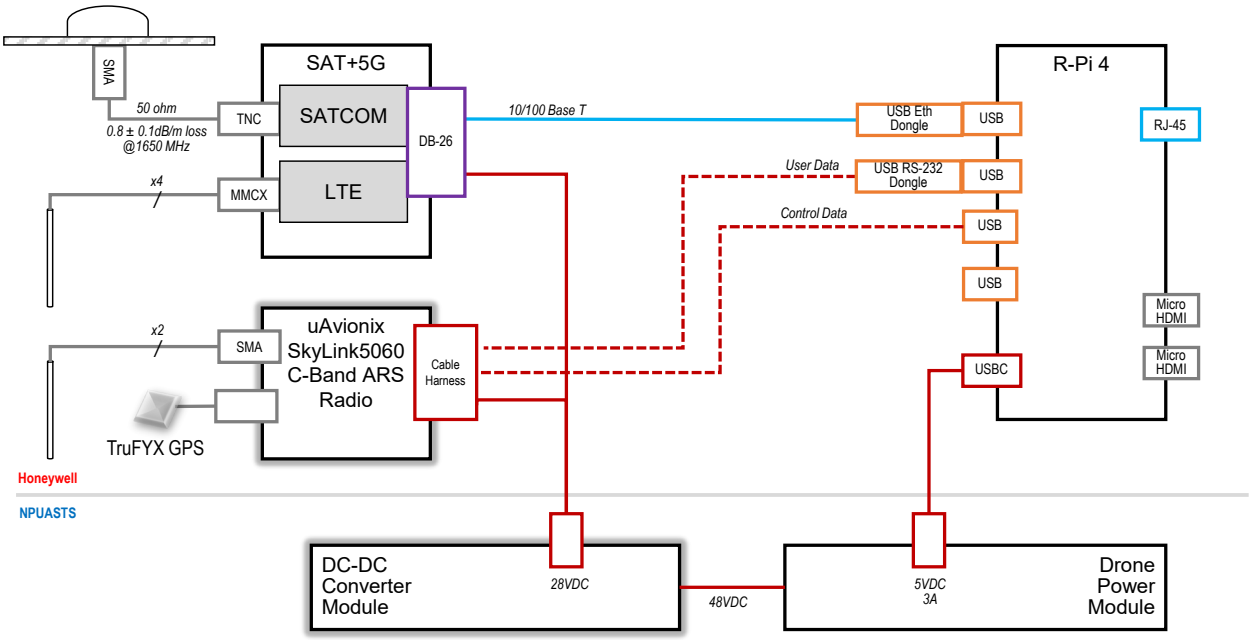


Figure 2-1. Airborne System Configuration for C2 System on Alta-X drone

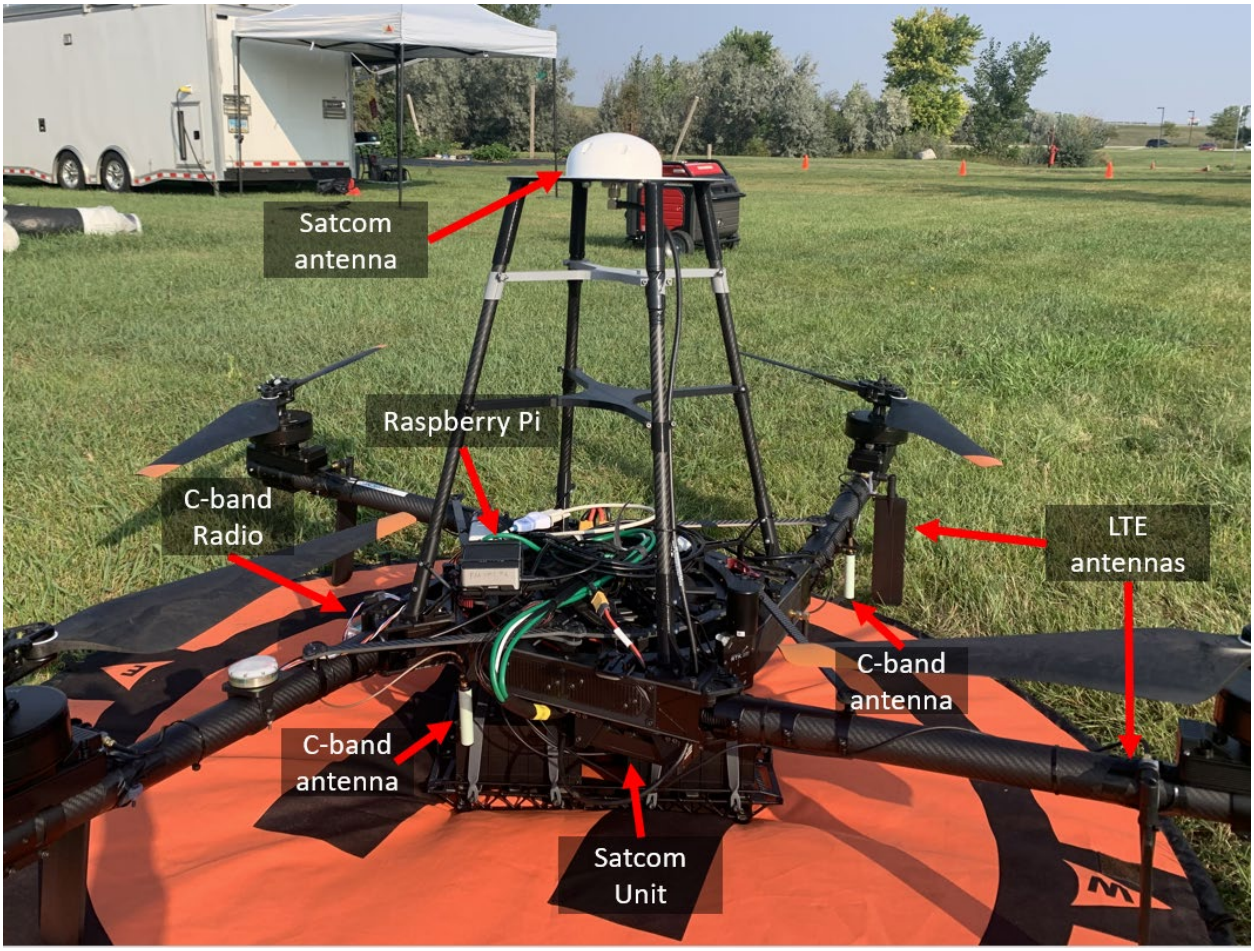


Figure 2-2. Alta-X drone Configured for C2 System

The Honeywell Vision-Aided Navigation (VAN) system (Figure 2-3, upper-left) interfaces with the VAN Operator Laptop and with a Pressure Altimeter via Ethernet connections through the Ethernet switch.

The airborne components for the UA were integrated by NPUASTS in a Cessna 182 General Aviation (GA) aircraft that is subcontracted by NPUASTS. The avionics components were integrated inside the aircraft, and the GPS antenna was mounted externally in a manner (e.g., hand-tightened brackets, speed-tape) that does not damage the aircraft fuselage. As part of the integration activity, NPUASTS provided an on-vehicle power module that supplies 115VAC to power DC power supplies that provide 28VDC (VAN System) and 12VDC (Ethernet switch and Pressure Altimeter), and 115VAC for the laptop used by the VAN Operator.

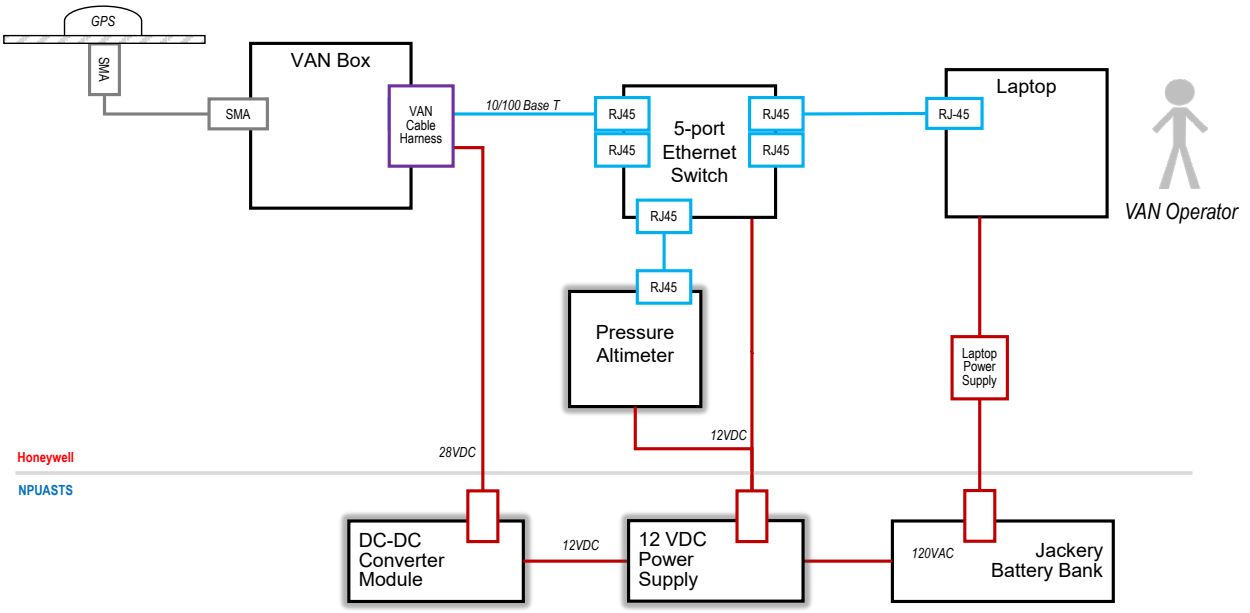


Figure 2-3. Airborne System Configuration for VAN System on Cessna

2.1.2 Ground System

As illustrated in Figure 2-4, the C2 Link System will be controlled and monitored from the ground Control Station laptop by a ground-based CS Operator. The CS laptop was installed in a NPUASTS mobile command center that provided internet connectivity via a CradlePoint IBR-900 ruggedized router provided by NPUASTS. The IBR-900 provides LTE connectivity to the internet, and it also includes a firewall, filtering, and threat management functionality.

The CS software runs on a virtual machine[1] using the VirtualBox hypervisor hosted on the laptop. The internet connectivity provides access to the C2 Communication Service Provider networking infrastructure (i.e., Satcom, LTE, and C-Band air-ground links to the UA).

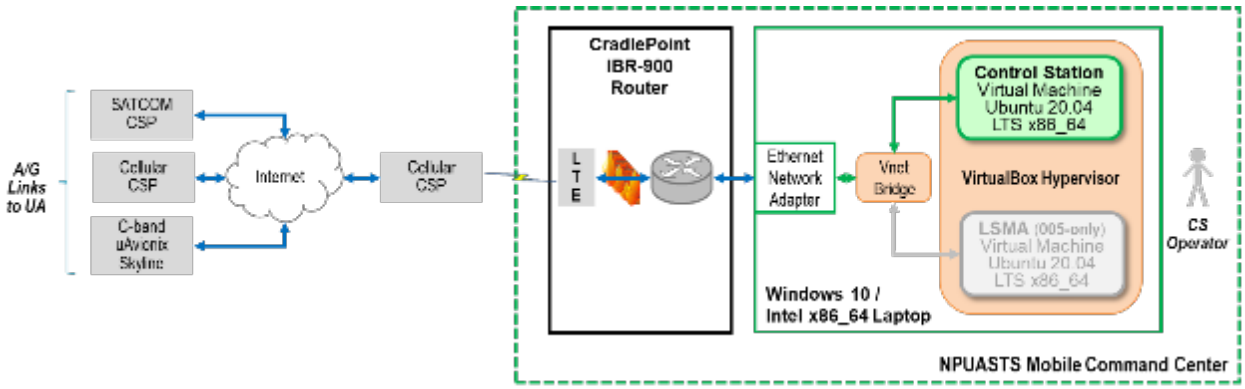


Figure 2-4. Ground System Configuration

[1] Note that since the same laptop is being used for both the UAS-C2 and UAS-PP projects, the laptop also hosts an independent virtual machine for the Local Storage Management Application (LSMA) that is used only by the UAS-PP project. This virtual machine is shown greyed-out since it is not used-by or applicable-to the UAS-C2 project.

2.2 FLIGHT TEST COMPONENT SUMMARY

The specific systems and components under test are documented in Table 2-1 – SUT Component Summary. The table includes a short description of the component, the model or part number, the serial number, and the software version (if applicable). Note that only key C2 Link System components are included; additional support systems (e.g., displays/monitors) and standard networking systems are not included.

Table 2-1. SUT Component Summary

System	Component	Model/Part No.	Serial No.	Version	Comments
UA Platform	HW: GA Aircraft	Cessna 182Q	N735GS	N/A	Asset owned by iSight
	HW: Drone	Freefly Alta-X Blue	AX363658	Package: 1.3.111 FMU: 1.3.31	Asset owned by NPUASTS QGroundControl: 1.3.9
UA C2 Link System Under Test	HW: Processor	Raspberry Pi 4B	e4:5f:01:05:42:9b	N/A	RPI #8
	HW: Ethernet Switch	Netgear ProSafe Plus GS105E	N/A	N/A	
	HW: SATCOM Radio	Honeywell Versawave Satcom+5G	11	N/A	Engineering Prototype
	HW: SATCOM Antenna	Honeywell 89000015-009	6108	N/A	Class15 Antenna
	HW: SATCOM RF Cable	Pasternack PE3W02802/HS-48	N/A	N/A	
	HW: SATCOM SIM	Honeywell 90411231	IMEI:89870-99204-15019-201	N/A	Inmarsat SBB via Honeywell Forge Connectivity
	HW: Cellular Antenna	Sierra Wireless 6001343	N/A	N/A	Qty = 4
	HW: C-Band ARS Radio	uAvionix UAV-1006082-001	6100037	0.4.12 / 0.4.3	RadioID: 0x010026004E SkyLink5060
	HW: C-Band Antenna	uAvionix UAV-1006288-001	N/A	N/A	
	HW: VAN System	Honeywell VAN	0004	N/A	
	HW: Power Supply	Jackery Explorer 500	FU127080160448	N/A	Main battery bank for Cessna
	HW: Power Supply	CUI VHK200W-Q24-S28	N/A	N/A	12VDC to 28VDC for Honeywell VAN on Cessna
	HW: Power Supply	CUI VHK200W-Q48-S28	N/A	N/A	12VDC to 28VDC for Honeywell Satcom on Alta-X
	SW: Operating System	Raspberry Pi OS (64-bit) Linux	N/A	Bullseye 11 arm64 2023-05-03	Kernel: 5.15.61-v8+
	SW: UA C2 Link System Software	GFE	N/A	N/A	
	SW: Cryptographic Library	wolfSSL	N/A	4.4.0-gplv3-fips-ready	
	SW: Wireguard VPN	Wireguard	N/A	v1.0.20210223	
C-Band Ground Radios	HW: C-Band GRS Radio	uAvionix UAV-1006090-001	6200049	Firmware v0.4.12	GRS1, RadioID: 0x01004C0044
	HW: C-Band GRS Hub	uAvionix UAV-1006103-001	54:6F:71:10:00:DC	Firmware v0.0.23	
	HW: C-Band GRS Radio	uAvionix UAV-1006090-001	6200058	Firmware v0.4.12	GRS2, RadioID: 0x0100230020
	HW: C-Band GRS Hub	uAvionix UAV-1006103-001	54:6F:71:10:00:DB	Firmware v0.0.23	
	HW: C-Band GRS Radio	uAvionix UAV-1006090-001	6200047	Firmware v0.4.12	GRS3, RadioID: 0x01004B0053
	HW: C-Band GRS Hub	uAvionix UAV-1006103-001	54:6F:71:10:00:DE	Firmware v0.0.23	
CS C2 Link System Under Test	HW: Router	CradlePoint IBR-1100	MM150120800336	7.0.40	Asset owned by NPUASTS (device aa1)
	HW: Processor	Dell Precision 7560	2NJB3M3	N/A	PC Name: MN74LT2NJB3M3
	SW: Operating System (Main)	Microsoft Windows 10 (x64)	N/A	Build: 19042.2846	Version: 20H2
	SW: Operating System (VM)	Ubuntu 20.04 (Focal) Linux	N/A	20.04.6 LTS x86_64	Kernel: 5.15.0-72-generic
	SW: Virtual Machine	VirtualBox Hypervisor	N/A	7.0.8 r156879	
	SW: CS C2 Link System Software	GFE	N/A	N/A	
	SW: Cryptographic Library	wolfSSL	N/A	4.4.0-gplv3-fips-ready	
	SW: Wireguard VPN	Wireguard	N/A	v1.0.20210223	

3 INSPECTION AND TEST REPORTING APPROACH

3.1 RESULT REPORTING

The inspection and test results reported in Sections 4 and 5 respectively are structured to present the following information:

- A summary-level result of the inspection or test using the values defined in Section 3.2. Where a test scenario consists of multiple test procedures, a summary-level result is included for each test procedure within the test scenario.
- Detailed results that are the output of an inspection procedure or a post-test analysis performed. For post-test analysis, the analysis output is compared with known expected results, which are documented in Appendix A. If the analysis output matches the expected result, then no further detail if provided; however, in the event of a difference, and detailed explanation of the deviation is provided.

3.2 RESULT DEFINITIONS

The result of executing an inspection or test procedure may be one of the following:

Table 3-1. Result Definitions

Result	Definition
PASS	The result complies with the Pass criteria specified in the detailed test procedures [DTP]
PARTIAL	The result complies partially with the Pass criteria specified in the detailed test procedures [DTP]. For example, positive results with an exception condition identified during the execution of one or more steps within a test procedure.
FAIL	The result does not comply with the Pass criteria (i.e., meets the Fail criteria) specified in the detailed test procedures [DTP].
NONE	An inspection or test procedure that could not be performed.

For any result other than "PASS," an explanation of any deviation/exception/issue is provided in the text as part of the detailed test result reporting.

4 INSPECTION RESULTS

This section documents the results of procedures where the requirement verification method is inspection or analysis, which are methods that were performed either prior to or after flight tests or ground-based tests.

4.1 RESULTS OF COMMON INSPECTION PROCEDURES

This section documents the result of inspection/analysis procedures that are shared in common between the UAS-PP and UAS-C2 projects. The inspection/analysis was performed once, but the results are reported in each project-specific final report deliverable.

4.1.1 IP_CM_001 – Crypto-Module Configuration

4.1.1.1 IP_CM_001A – UA AND CS C2 APPLICATION SOFTWARE CRYPTOGRAPHY

Result = PASS: This inspection shows that the system application software crypto-library is configured to use crypto-algorithms and key lengths that meet the requirements of NIST SP 800-131A, Rev2 (or equivalent MoC).

Detailed Results: Appendix B documents the detailed inspection results.

4.1.1.2 IP_CM_001B – VPN CRYPTOGRAPHY

Result = PARTIAL: This inspection shows that the VPN (Wireguard) is partially compliant with the security requirements in the MASPS. SER-02/SER-09, SER-03/SER-10, SER-04 and SER-11 pass. However the key establishment scheme and security algorithms that Wireguard uses are only partially compliant.

Detailed Results:

Appendix C documents the detailed inspection results and further explains what parts of the security requirements are not fully MASP compliant.

4.1.2 IP_CM_002 – User Data and Status Report Performance during All Flight Phases

The logs containing User Data associated with each in-scope function (aviate, navigate, and Status Reports) were analyzed to compute RLP Latency and RLP TET, and missing data duration.

- RLP Latency – The time for C2 Link User Data to pass, one-way, through the C2 Link System (i.e., UA DTSR, air/ground links, ground/ground links, CS DTSR) that was used to develop the TET.
- RLP TET – The maximum time that can be allowed for a transaction before airspace safety is materially affected.

Result = PARTIAL: This inspection shows that for each airspace and operational condition, RLP Latency is less than the required time in that airspace on average, however there are a few

individual instances where latency exceeded the 1.0 second limit; RLP TET was less than or equal to the required time in that airspace on 78% of the switchover transactions.

Detailed Results:

For each flight, a stream of continuous user data was sent over the user data plane throughout the duration of the flight, both in the uplink and downlink directions. This data was representative C2 application data that was collected from a network capture of an actual flight of the Alta-X drone at NPUASTS. Messages were sent at a rate of 1 to 2 seconds, and each message varied in length between 50 and 600 bytes. Each message was analyzed and inspected to determine which link was used for its transmission and ensure its successful delivery at the receiver.

Latencies for each of these messages is defined as the elapsed time from when the message was sent to when the message was received by each of the DTSRs. However, due to the challenges from synchronizing both clocks from the sender and the receiver, our approach to latency analysis was to use the keep-alive messaging system, which measures the round-trip time of a message, subtracting the processing time by the remote receiver. These keep-alive messages were continuously sent throughout each flight over each link at a rate of about 1 message per second.

Some user data messages that were sent, failed a successful transmission and receipt by the receiver. The causes for failed message transmissions were during a link switchover, during a total link loss, or during times when the DTSR entered a failed state.

The average latencies observed during our flights satisfy the strictest limit of 1.0 seconds for aviate and navigate messages on all airspaces and operational conditions. However, there were instances when link latencies degraded beyond the 1 second limit. Section 5 shows the detailed data for each of the flights.

The “nan” values in Table 4-1 for C-Band indicate “not a number”, because during flights 2, 3, 6, and 7, C-Band was not operational and not working, so there was no data or messages exchanged through the C-Band link, and no latency data was available.

The column showing the “C-Band average latency” is the average for the flight, and the final row is the average of the averages from all flights. But flights 2, 3, 6, and 7 had no C-band data, so the average for these flights was not possible to compute.

Section 6.2.5 explains the reason why C-Band was not operational during these flights. Citing the root cause of the problems with C-Band during the first 7 flights.

Table 4-1. Average Link Latency per flight for 006-C2

Flight ID	Satcom Average Latency (ms)	Cellular Average Latency (ms)	Cband Average Latency (ms)	Satcom Latency Measurements under 1 sec (%)	Cellular Latency Measurements under 1 sec (%)	C-Band Latency Measurements under 1 sec (%)
Flight 1	657	214	1,134	96.254	100	48.43
Flight 2	670	206	nan	88.155	100	nan
Flight 3	610	203	nan	94.678	100	nan
Flight 4	611	225	418	99.674	100	87.469
Flight 5	714	209	347	94.872	100	98.427
Flight 6	604	232	nan	99.213	100	nan
Flight 7	594	234	nan	99.358	100	nan
Flight 8	677	237	319	99.044	100	99.712
Flight 9	635	225	378	98.611	100	99.435
Flight 10	635	244	303	96.396	100	99.42
Flight 11	591	230	312	98	100	100
Flight 12	669	212	303	100	100	99.673
Flight 13	718	219	293	98.352	100	100
Flight 14	584	215	311	100	100	100
Flight 15	779	210	314	96.682	100	100
Flight 16	721	218	415	99.118	100	100
Flight 17	603	211	505	98.519	100	97.79
Flight 18	754	213	363	99.225	100	100
Flight 19	710	241	386	96.886	100	100
Average	**660**	**221**	**407**	**97.3**	**100**	**96.3**

Table 4-2. User Plane Message delivery rate per flight for 006-C2

Flight ID	User Messages Sent (uplink + downlink)	User Messages Received (uplink + downlink)	Success Rate (uplink + downlink)
Flight 1	2,380	2,048	86.1%
Flight 2	2,032	1,745	85.9%
Flight 3	1,758	1,441	82.0%
Flight 4	2,373	2,081	87.7%
Flight 5	2,361	1,125	47.6%
Flight 6	1,008	663	65.8%
Flight 7	873	731	83.7%
Flight 8	962	682	70.9%
Flight 9	771	594	77.0%
Flight 10	653	542	83.0%
Flight 11	542	509	93.9%

Flight 12	714	686	96.1%
Flight 13	429	381	88.8%
Flight 14	615	574	93.3%
Flight 15	505	481	95.2%
Flight 16	746	669	89.7%
Flight 17	731	652	89.2%
Flight 18	1,254	1,251	99.8%
Flight 19	558	557	99.8%
Total	**21,265**	**17,412**	**81.9%**

RLP TET was evaluated by the link switchover commands. Section 5.3 provides detailed results for each of the Switchover commands. In summary, out of the 65 switchovers, 51 (78%) completed the transaction within the limit, and 14 (22%) exceeded the TET limit.

The improvement in success rate shown on Table 4-2 is due to several factors:

- The first 9 flights have the lowest "user message transfer success rate" because the first 9 flights were testing the "lost link & recovery" scenario.
- For the "total lost link" flights, when the active link was disabled with no other links available, the C2 system was offline for a period of up to 35 seconds as it was attempting to automatically re-establish the link.
- During this recovery time when the link was not established, user messages were accounted as 'dropped'.
- Flight 5 had the lowest "user message transfer success rate" because it was a "lost link & recovery" scenario and it was primarily over C-Band, while the C-Band issues had not been yet resolved.
- Flights 6 had the 2nd lowest "user message transfer success rate" because of the CS Connection issue that the CS lost connection mid-flight due to the "accidental disconnection of our LTE access point."
- Flights 8 and 9 were the 3rd and 4th lowest "user message transfer success rate" because even though the C-Band issues were resolved, this was still a "lost link & recovery" scenario, with C-Band as the focus link. And even with the C-Band issues resolved, the C-Band link was not as reliable as the LTE or Satcom Links.

5 TEST RESULTS

This section documents the results of test procedures where the requirement verification method is test or demonstration, which are methods that were performed during flight tests or ground-based tests.

5.1 FLIGHT TEST RESULTS

This section documents the results of flight test performed in accordance with flight test cards and detailed test procedures specified in [DTP]. Each flight test identifies the associated test card and test scenario, the flight number (within the series of twenty flight tests), the test date, and the test start/end times. General test observations (e.g., issues or unexpected conditions encountered during the flight test) are documented. The test results, which are presented in a tabular form, identity the individual test procedures specified in the test card, report the result of each test procedure, and provide notes, as necessary, to describe conditions observed during the execution of the specific test procedure and/or to explain a result other than pass.

5.1.1 C2 Link Loss and Recovery (LTE)– Flight 1-of-9

Result = PASS: This flight test demonstrated seamless link transitions among C-Band, cellular and SATCOM networks, seamless transitions between LOS and BVLOS flight operations, and C2 link recovery after link loss.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
1	Scenario 1 – TP_C2_003A: C2 Link Loss and Recovery (LTE)	1	06 Sept 2023	10:21 CDT	10:45 CDT

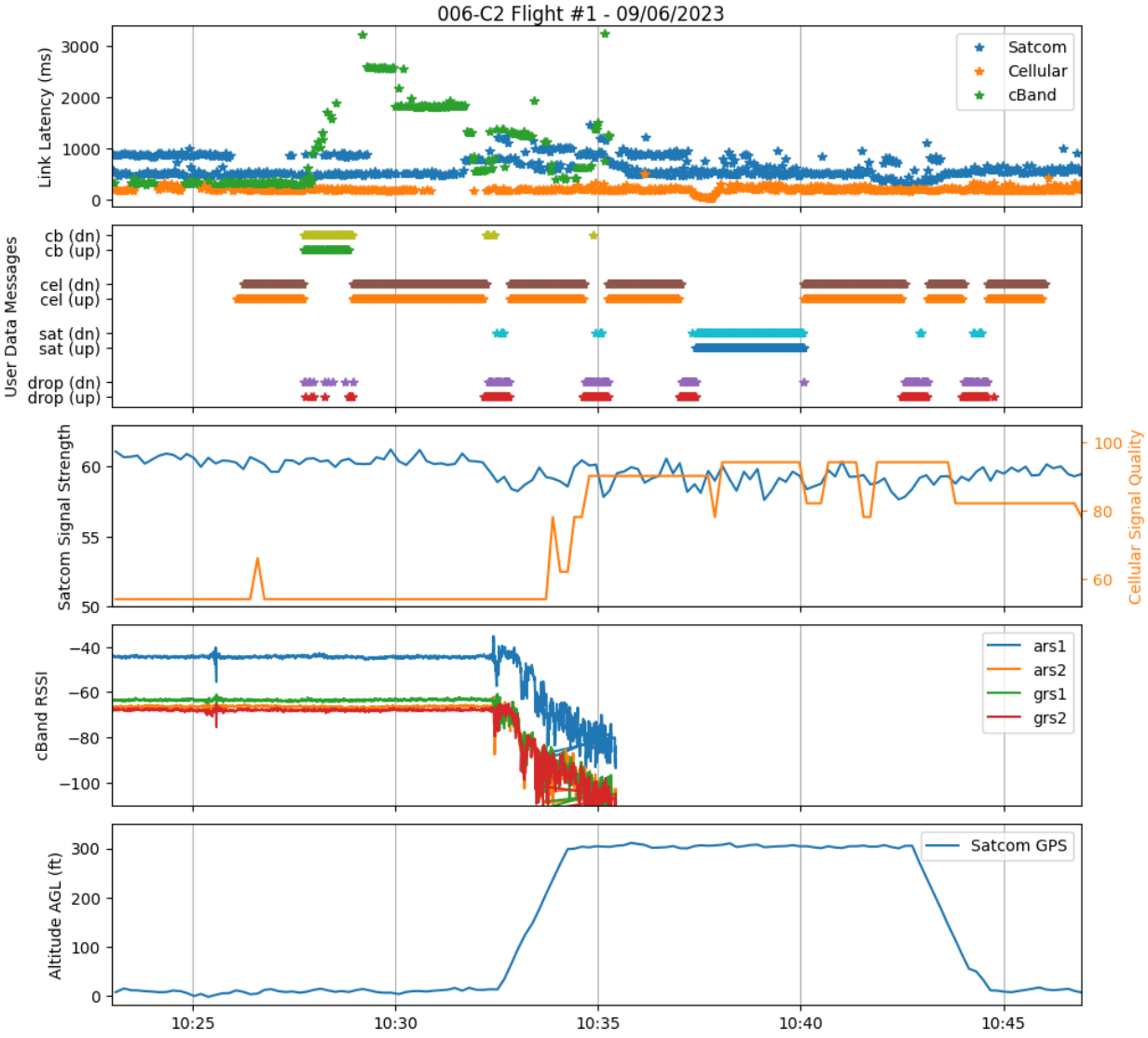
General Test Observations: The C-Band ARS was lost mid-flight at about 10:33-10:35. It did not come back online. It showed as offline in skyline. The flight continued with LTE and Satcom links, as the C-Band link was not necessary to meet the objectives of this test procedure.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	10:21 Starting Procedure. CM-001 10:22 CS Status secure then UA: N/2 good. 10:22 UA send n=1, not recd - good. 10:23 CS Status 1,2,3 all up nominal, then UA nominal - good 10:23 UA Secure Start - good on LTE - good. 10:25 CS status secure, then UA, Y/2 - good 10:26 while on LTE, starting continuous data stream from CS, then UA - good

Procedure	Description	Result	Notes
TP_CM_004A	User Data exchanges < MTU	**PASS**	10:26 TP_004 UA, n=1, recd id=4 - good. 10:27 Switchover from LTE to C-Band, switch 3 - good. 10:28 UA set tet to 3 sec, then CS, good
TP_C2_003A (Begin)	C2 Link Loss and Recovery	**PASS**	10:28 Status Secure UA Y/3, then CS, Y/3 - good. 10:28 Switch 2 from C-Band to LTE - good 10:29 UA status secure Y/2, then CS Y/2 - good. 10:30 Cleared for takeoff.
TP_C2_003A (Takeoff)	C2 Link Loss and Recovery	**PASS**	10:31 Arming / takeoff / START OF FLIGHT #1 - LTE Focus 10:32 Disable 1, 3, 2, - Enable link 2. 10:32 UA Status secure Y/2 then CS Y/2 good. 10:33 200 ft. TET Exceeded msgs observed.
TP_C2_003A (Departure)	C2 Link Loss and Recovery	**PASS**	10:33 250 ft TET = 5 10:34 disable LTE, no links. waited 5 sec, then enable LTE. 10:35 UA status secure. Y/1 ISSUE/ERROR wrong indication 10:35 TET notification over 7 sec. 10:35 Cruising. Enable 1, and 3. ISSUE/ERROR C-Band did not come online. 10:36 CS Status 123, Satcom and LTE Up. C-Band down. 10:36 disable LTE, 10:37 CS status secure Y/1 good. 10:38 enable lte
TP_C2_003A (Cruise)	C2 Link Loss and Recovery	**PASS**	10:38 Status 2, LTE Up nominal, good. 10:40 Switch 2. good from satcom to LTE good 10:41 UA status secure. 10:41 Disable 1, 3 10:42 Set TET 3. 10:42 Disable 2, then enable LTE. good. 10:42 Status secure Y/2 - good observed TET exceeded notification. 10:43 150-ft 100-ft Disable 2. then Reenable 10:44 Status Secure Y/2 good. observed TET notification.
TP_C2_003A (Arrival)	C2 Link Loss and Recovery	**PASS**	
TP_C2_003A (Land)	C2 Link Loss and Recovery	**PASS**	10:45 LANDED / END OF FLIGHT #1

Procedure	Description	Result	Notes
TP_CM_011	Control / User Plane Termination	**PASS**	10:45 status secure CS then UA Y/2 Good. 10:46 stopped data stream. then Secure stop. 10:46 CS then UA Status Secure N/2 good. 10:46 UA send n=1, not recd.

Detailed Results:



At 10:34, while cruising with LTE as the active link, with no other links available, the LTE link was disabled for over 5 seconds to simulate a total link loss. After LTE was re-enabled, the DTSR "status secure" command displayed incorrectly that the active link was on Satcom, when the system was using LTE as the active link. However, the system was functioning correctly, and the system recovered with accurate and correct indications afterwards. This condition was later determined that it was a minor temporary display issue, that the DTSR took a few seconds to display the correct active link.

This first flight test tested four separate total link loss events, at 10:32, 10:34, 10:42, and 10:43, where the active link was disabled (with no alternate links available) to simulate the link lost scenario. On each of the four events, a message was displayed to the operator indicating the TET had been exceeded while the C2 system attempted to reestablish the link. The method for simulating the lost link was to disable the uplink route at the CS, so data from the UA could still reach the CS, but data from the CS could not reach the UA in the uplink direction. On these four events the link was disabled for a duration of about 3 to 8 seconds, and then re-enabled. The table below shows the recovery times of the C2 system to re-establish the active link. During this recovery time, the figure above shows that user data was dropped as there was no active link while the DTSRs were attempting to reestablish an active link.

At 10:37 on this first flight, a test was performed to simulate losing the active link while a backup link was available; in this case the C2 system had both LTE and Satcom links available, and after the active link, LTE, was disabled, the C2 system automatically transitioned to the Satcom link within 23 seconds, automatically resuming the stream of user data messages. However, during the recovery period, user data messages were dropped as the system was attempting to reestablish an active link.

Table 5-1. Lost Link Events for C2 Flight #1

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/06/2023 10:32:13.811174	Takeoff	34,981	LTE	LTE	Total Link Loss Recovery
09/06/2023 10:34:40.727226	Cruise	34,996	LTE	LTE	Total Link Loss Recovery
09/06/2023 10:37:03.136348	Cruise	23,888	LTE	Satcom	Link Loss with Alternate
09/06/2023 10:42:33.653487	Descent	34,984	LTE	LTE	Total Link Loss Recovery
09/06/2023 10:44:01.709678	Landing	35,200	LTE	LTE	Total Link Loss Recovery

5.1.2 C2 Link Loss and Recovery (LTE)– Flight 2-of-9

Result = PASS: This flight test demonstrated seamless link transitions among C-Band, cellular and SATCOM networks, seamless transitions between LOS and BVLOS flight operations, and C2 link recovery after link loss.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
1	Scenario 1 – TP_C2_003A: C2 Link Loss and Recovery (LTE)	2	06 Sept 2023	11:33 CDT	11:54 CDT

General Test Observations: For this flight (and all first 7 flights), the C-Band link was not fully operational as we were still troubleshooting the C-Band system, Section 6.3 details the lessons learned.
11:30 ISSUE/ERROR C-Band shows very high latencies of about 7 seconds, so C-Band will be not available. RSSI ARS: -40/-72, GRS1: -70

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	11:33 Starting procedure** for Flight #2 11:34 CS status secure, then UA, N/2 both, good. 11:34 UA N=1, not recd, good. 11:34 Status 123, Satcom and LTE up, C-Band down. nominal good Note: C-Band is not available! 11:35 Secure Start from UA. established on LTE - good 11:36 CS status secure: Y/2, then UA, Y/2 good 11:36 CS starting continuous data stream, then UA.
TP_CM_004A	User Data exchanges < MTU	**PASS**	11:37 UA send n=1, recd id=4, 11:38 switch 3, but link is down. ISSUE/ERROR C-Band is down
TP_C2_003A (Begin)	C2 Link Loss and Recovery	**PASS**	11:38 set tet=3 11:39 UA status secure: Y/2, then CS, Y/2 good. 11:39 cleared for takeoff. 11:39 disable links 1, 3.
TP_C2_003A (Takeoff)	C2 Link Loss and Recovery	**PASS**	11:40 ARMING / takeoff Flight #2. 11:40 disable link 2, waited 3 sec, then enable link 2.
TP_C2_003A (Departure)	C2 Link Loss and Recovery	**PASS**	11:41 50 ft. CS and UA status secure, Y/2 both, good, 100ft. 11:42 200 ft. set TET = 5, 250-ft.

Procedure	Description	Result	Notes
TP_C2_003A (Cruise)	C2 Link Loss and Recovery	**PASS**	11:42 Cruising. Disable link 2, no other links available. waiting 5 sec... enable link 2. 11:43 UA status secure, Y/3. then CS: Y/2 ISSUE/ERROR wrong display of active link. 11:44 while on LTE, enable link 1. enable 3 good. 11:44 CS Status 123: Satcom and LTE UP nominal, C-Band is down ISSUE/ERROR C-Band should have been up. 11:45 disable link 2. (it auto switched from LTE to satcom) CS Status secure: Y/1 good. 11:45 enable link 2. 11:46 UA status secure: Y/1 good. 11:46 status 2. Link is UP. There was an indication that the switchover exceeded TET. ISSUE/ERROR this should not have exceeded. 11:47 UA status secure: Y/2 then CS. Y/2. 11:48 disabling Link 1 & 3. still on LTE. 11:49 Issued command to return to land, descending... 11:49 set tet =3 11:50 disable 2, then enable 2. 50 ft. 11:50 UA status secure, Y/1 ISSUE/ERROR, showing satcom when really on LTE. 11:51 observed exceeded notification. 11:51 disable 2, no other links, enable link 2. observed exceeded notification. 11:51 status secure Y/2 on both. observed notification of TET exceeded. 11:52 hovering... landing. 11:53 LANDED / ON GROUND / Disarmed. END OF FLIGHT 11:53 CS status secure: Y/2, then UA Y/2 11:53 stopping data stream. then UA Secure stop 11:54 CS status secure. N/2 on both. good. 11:54 UA send n=1, not recd.
TP_C2_003A (Arrival)	C2 Link Loss and Recovery	**PASS**	
TP_C2_003A (Land)	C2 Link Loss and Recovery	**PASS**	
TP_CM_011	Control / User Plane Termination	**PASS**	

Detailed Results:

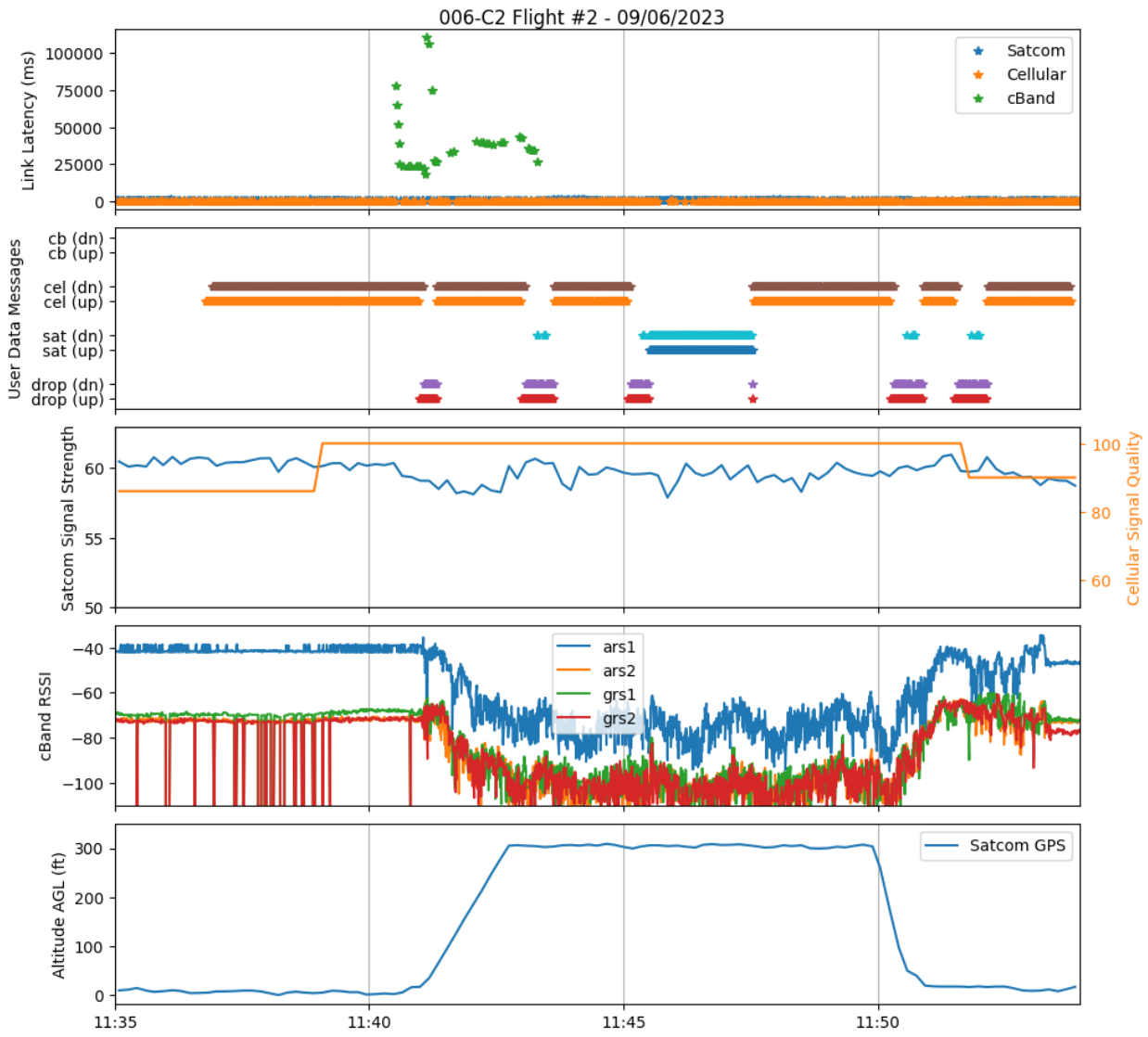
At 11:43 and 11:50 we observed the same display issue as on Flight #1, where the DTSR briefly showed the wrong active link.

This test sequence demonstrated four successful system recoveries from the lost link condition, and one successful recovery from losing the active LTE link while the Satcom link was available.

Although the duration of the four total link loss instances were all under 10 seconds, the figure below shows there was a gap, or an interruption in the user data for a longer duration. The interruption to the user data stream was caused by the time the DTSRs required to re-establish the secure link. The method to establish the new link focused on solution convergence (see Section 6.2.3 for details on this solution), rather than performance, as there are no set performance requirements re-establishing a link after a lost link scenario.

Table 5-2. Lost Link Events for C2 Flight #2

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/06/2023 11:41:04.521957	Takeoff	16,654	LTE	LTE	Total Link Loss Recovery
09/06/2023 11:43:04.088570	Cruise	35,031	LTE	LTE	Total Link Loss Recovery
09/06/2023 11:45:08.744439	Cruise	23,700	LTE	Satcom	Link Loss with Alternate
09/06/2023 11:50:18.926208	Descent	35,619	LTE	LTE	Total Link Loss Recovery
09/06/2023 11:51:34.436988	Landing	35,348	LTE	LTE	Total Link Loss Recovery



5.1.3 C2 Link Loss and Recovery (LTE)– Flight 3-of-9

Result = PASS: This flight test demonstrated seamless link transitions among C-Band, cellular and SATCOM networks, seamless transitions between LOS and BVLOS flight operations, and C2 link recovery after link loss.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
1	Scenario 1 – TP_C2_003A: C2 Link Loss and Recovery (LTE)	3	06 Sept 2023	12:30 CDT	12:49 CDT

General Test Observations: For this flight (and all first 7 flights), the C-Band link was not fully operational as we were still troubleshooting the C-Band system; Section 6.3 details the lessons learned.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	12:30 CS Status secure N/2, then UA. good 12:31 UA send n=1 not recd = good 12:31 CS status 123. satcom and LTE are up, nominal. C-Band is down. 12:31 UA status 123. same, good. 12:31 UA Secure start - came up on LTE. good. 12:32 CS status secure Y/2, then UA, both Y/2 good. 12:33 CS starting continuous data stream. then UA. good.
TP_CM_004A	User Data exchanges < MTU	**PASS**	12:33 UA send n=1, recd ID=4. 12:34 UA Set TET =3 good.
TP_C2_003A (Begin)	C2 Link Loss and Recovery	**PASS**	12:35 Status Secure UA, then CS. both Y/2 LTE, good. 12:36 cleared for takeoff. 12:36 disabled links 3, and 1, then 2. TAKEOFF / ARMING / flight #3.
TP_C2_003A (Takeoff)	C2 Link Loss and Recovery	**PASS**	12:36 disable 2. wait 3 seconds. enable link 2. 12:36 observed TET exceeded notification. 12:37 Climbing 100 ft. 150 ft.
TP_C2_003A (Departure)	C2 Link Loss and Recovery	**PASS**	12:38 250. Satcom is disabled, only on LTE. 12:38 cruising 300 ft. set tet = 5.

Procedure	Description	Result	Notes
TP_C2_003A (Cruise)	C2 Link Loss and Recovery	**PASS**	12:38 disable link 2, no other links available. wait 5 seconds. then enable link 2. 12:39 UA status secure: Y/2 then CS. Y/2 both good. 12:39 observed TET exceeded notification 12:39 enable link 1, and 3. satcom is green available. 12:40 CS Status 123. Satcom and LTE are up nominal, C-Band is down. 12:40 Disable link 2, with satcom available. auto switchover to satcom. 12:41: status secure: Y/1 on CS. good. 12:41 enable 2 LTE, still on satcom. 12:41 UA Status secure. Y/1 good. 12:41 CS Status 2. UP. ISSUE/ERROR observed TET exceeded notification. Switch 2, from satcom to LTE. good. 12:42 UA status secure: Y/2 good. then CS. Y/2 good. 12:43 Disable satcom while on LTE, disable 1 and 3. still on lte. 12:43 Cleared to land. 12:44 Set tet =3 descending.
TP_C2_003A (Arrival)	C2 Link Loss and Recovery	**PASS**	12:45 Disable link 2 with no others available. 200 ft. waiting 3 sec. then reenable link 2. 12:45 150 ft. UA Status secure then CS Y/2 TET Exceeded notification.
TP_C2_003A (Land)	C2 Link Loss and Recovery	**PASS**	12:46 disable link 2 with no others available. 50 ft landing... waiting 3 sec. enable. 12:46 status secure. Y/2 on UA then CS. Y/2 both good. LANDED / ON GROUND / Disarmed. END OF FLIGHT 3 12:47 UA Status secure: Y/2 then CS. Y/2
TP_CM_011	Control / User Plane Termination	**PASS**	12:48 stopping data stream from CS And UA. 12:48 UA Secure Stop good. 12:48 UA Status secure, then CS N/2 good. 12:49 UA Send n=1 not recd. 12:57-ish shutdown RPI, batteries off. power off drone.

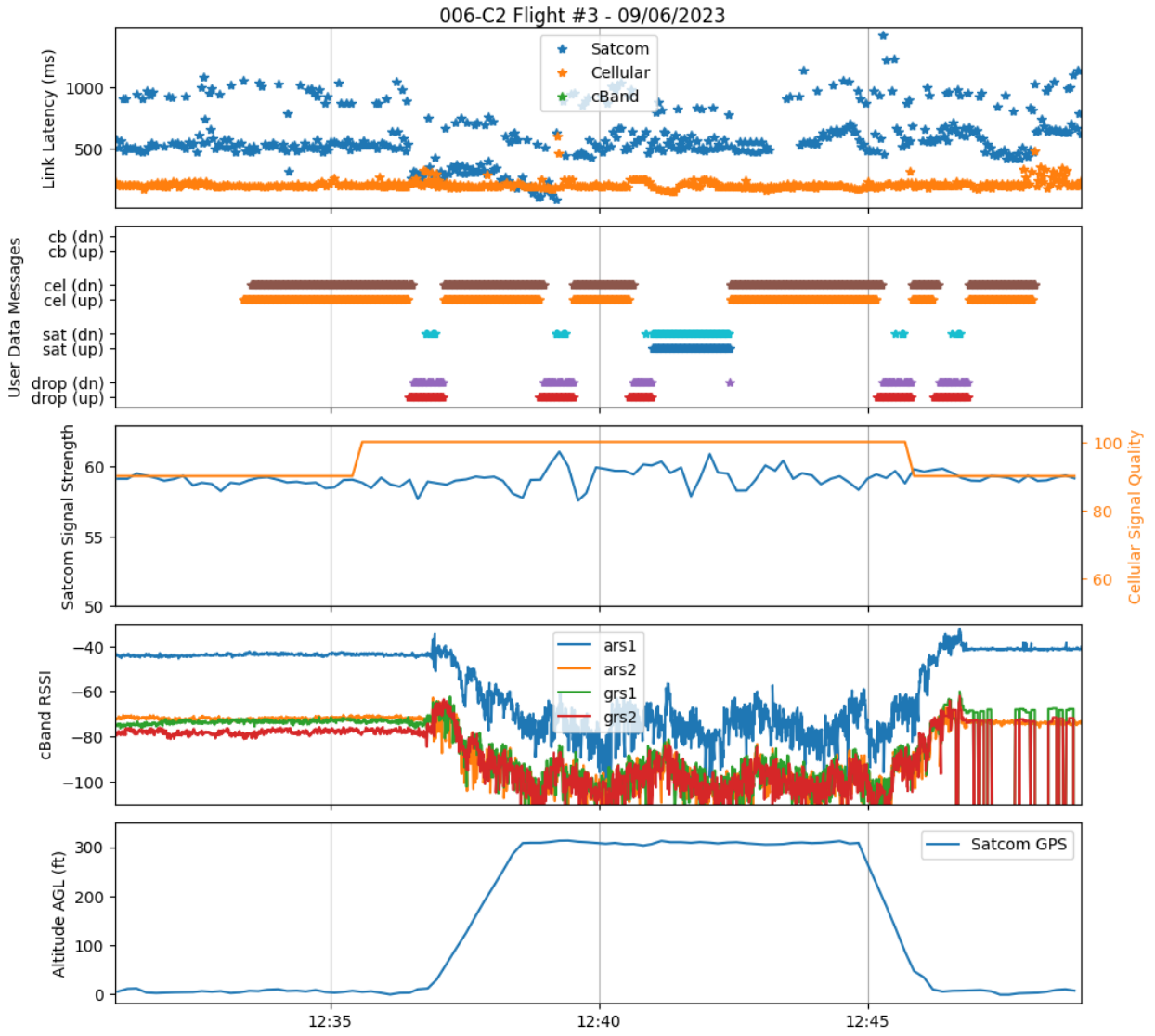
Detailed Results:

This test sequence demonstrated a total link loss condition four times, while LTE was the active link. In all four instances, the link was successfully reestablished back on LTE after re-enabling the link.

Although the duration of the four total link loss instances were all under 10 seconds, the figure below shows there was a gap, or an interruption in the user data for a longer duration.

Table 5-3. Lost Link Events for C2 Flight #3

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/06/2023 12:36:32.760423	Takeoff	34,947	LTE	LTE	Total Link Loss Recovery
09/06/2023 12:38:58.386448	Cruise	34,218	LTE	LTE	Total Link Loss Recovery
09/06/2023 12:40:38.283629	Cruise	23,935	LTE	Satcom	Link Loss with Alternate
09/06/2023 12:45:16.018356	Descent	35,011	LTE	LTE	Total Link Loss Recovery
09/06/2023 12:46:18.855143	Landing	34,927	LTE	LTE	Total Link Loss Recovery



5.1.4 C2 Link Loss and Recovery (SATCOM) – Flight 4-of-9

Result = PASS: This flight test demonstrated seamless link transitions among C-Band, cellular and SATCOM networks, seamless transitions between LOS and BVLOS flight operations, and C2 link recovery after link loss.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
1	Scenario 1 – TP_C2_003B: C2 Link Loss and Recovery (SATCOM)	4	06 Sept 2023	2:47 CDT	3:10 CDT

General Test Observations: For this flight (and all first 7 flights), the C-Band link was not fully operational as we were still troubleshooting the C-Band system, Section 6.3 details the lessons learned.
We changed the GRS1 LZ antenna from pointing west to pointing south to lower the RSSI.
RSSI Now at: ARS: -50/-80. GRS1: -74

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	2:47 CS status secure N/2, then UA, same N/2 both good 2:48 UA Send n=1, sent not recd, good. 2:48 CS Status 123. all links up, with nominal. then UA. same good nominal. 2:48 UA Secure Start... good session on LTE. 2:49 CS Status secure: Y/2, then UA, Y/2, both good.
TP_CM_004A	User Data exchanges < MTU	**PASS**	2:50 CS starting continuous data stream. then UA. 2:51 UA send n=1, recd id=4
TP_C2_003B (Begin)	C2 Link Loss and Recovery	**PASS**	2:51 UA Switch 3. from LTE to C-Band. 2:52 UA Y/3 status secure, good. 2:52 Set TET =3 on both good. 2:52 UA SWITCH 2 from C-Band to LTE. 2:53 Status secure Y/2 on both.
TP_C2_003B (Takeoff)	C2 Link Loss and Recovery	**PASS**	2:54 ARMING / TAKEOFF / Disabled links 1, 3, then 2. All links lost. enable link 2. 2:55 Climbing... status Y/2, on UA then CS... 250 ft.
TP_C2_003B (Departure)	C2 Link Loss and Recovery	**PASS**	2:56 Enable link -1. switch to link 1. Satcom. disable link 2. 2:56 CS status: Y/2. 2:57 CS enable link 2. UA Status secure Y/2 Good. observed exceeded notification.

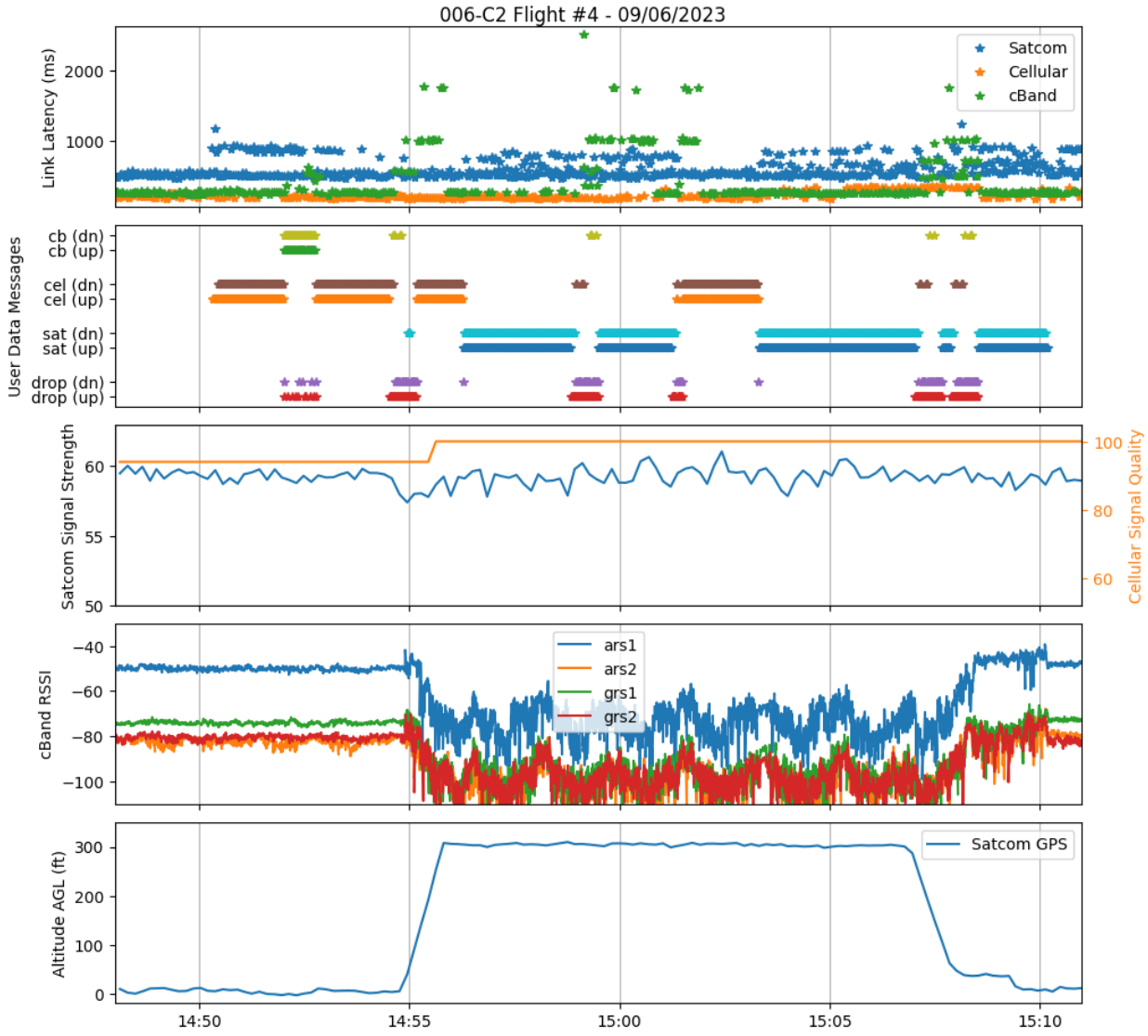
Procedure	Description	Result	Notes
TP_C2_003B (Cruise)	C2 Link Loss and Recovery	**PASS**	2:58 Set TET 5.. cruising. disable link 2, then 1. all links lost. 2:59 enable link-1 satcom. 2:59 CS Status secure Y/1, then enable link 2, 3. 3:00 UA Status secure: Y/1, 3:00 CS Status 123, all links up, nominal. C-Band shows 2-sec latency!! 3:01 disabled satcom with lte and C-Band green, switched to LTE automatically. exceeded TET during switchover. 3:02 UA Status secure Y/2 then CS. on both good. 3:02 enable link 1 with LTE as session. all links up. 3:03 Status 1. satcom up. Switch 1 from LTE to Satcom. switchover in 3.2 sec. on UA, CS shows 2.6 sec. 3:04 status: Y/1 on UA. CS Status: Y/1. no indication of exceeded tet. 3:05 Set TET = 3, all links up. on Satcom. Disable links 2, 3. Remain on satcom.
TP_C2_003B (Arrival)	C2 Link Loss and Recovery	**PASS**	3:07 Descending. 250. Disable link 1. wait 3 sec. enable link 1. 200ft. 3:07 status secure: Y/3 on CS WRONG. waited then Y/1. on both sides. 3:08 Disable 1. wait 3 seconds. enable 1... 3:08 Status Secure. Enable link 2. Status secure. Y/1 3:09 clear to land. holding at 50 ft... landing...
TP_C2_003B (Land)	C2 Link Loss and Recovery	**PASS**	3:09 status: CS Y/1 then UA both good. 3:10 LANDED / ON GROUND end of flight 4.
TP_CM_011	Control / User Plane Termination	**PASS**	3:10 stopping data stream. then secure STOP. Status: N/1 on both. 3:10 send n=1, not recd. good.

Detailed Results:

At 3:07 we observed the same display issue as on Flight #1, where the DTSR briefly showed the wrong active link.

Table 5-4. Lost Link Events for C2 Flight #4

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/06/2023 14:54:35.912059	Takeoff	35,069	LTE	LTE	Total Link Loss Recovery
09/06/2023 14:58:55.939195	Cruise	35,592	Satcom	Satcom	Total Link Loss Recovery
09/06/2023 15:01:20.032829	Cruise	10,595	Satcom	LTE	Link Loss with Alternate
09/06/2023 15:07:06.494473	Descent	35,657	Satcom	Satcom	Total Link Loss Recovery
09/06/2023 15:07:57.454637	Landing	36,383	Satcom	Satcom	Total Link Loss Recovery



5.1.5 C2 Link Loss and Recovery (C-Band) – Flight 5-of-9

Result = PARTIAL: This flight test attempted link transitions among C-Band, cellular and SATCOM networks, seamless transitions between LOS and BVLOS flight operations, and C2 link recovery after link loss. However, after a lost link scenario while on C-Band, the user data messages failed to recover in the uplink direction.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
1	Scenario 1 – TP_C2_003C: C2 Link Loss and Recovery (C-Band)	5	06 Sept 2023	3:33 CDT	3:56 CDT

General Test Observations: There were two C-Band GRS antennas for this flight. This test demonstrated seamless transition from one GRS to another. User data messages stopped transmitting in the uplink direction during the cruise phase at 3:42. Also, for this flight (and all first 7 flights), the C-Band link was not fully operational as we were still troubleshooting the C-Band system, Section 6.3 details the lessons learned.

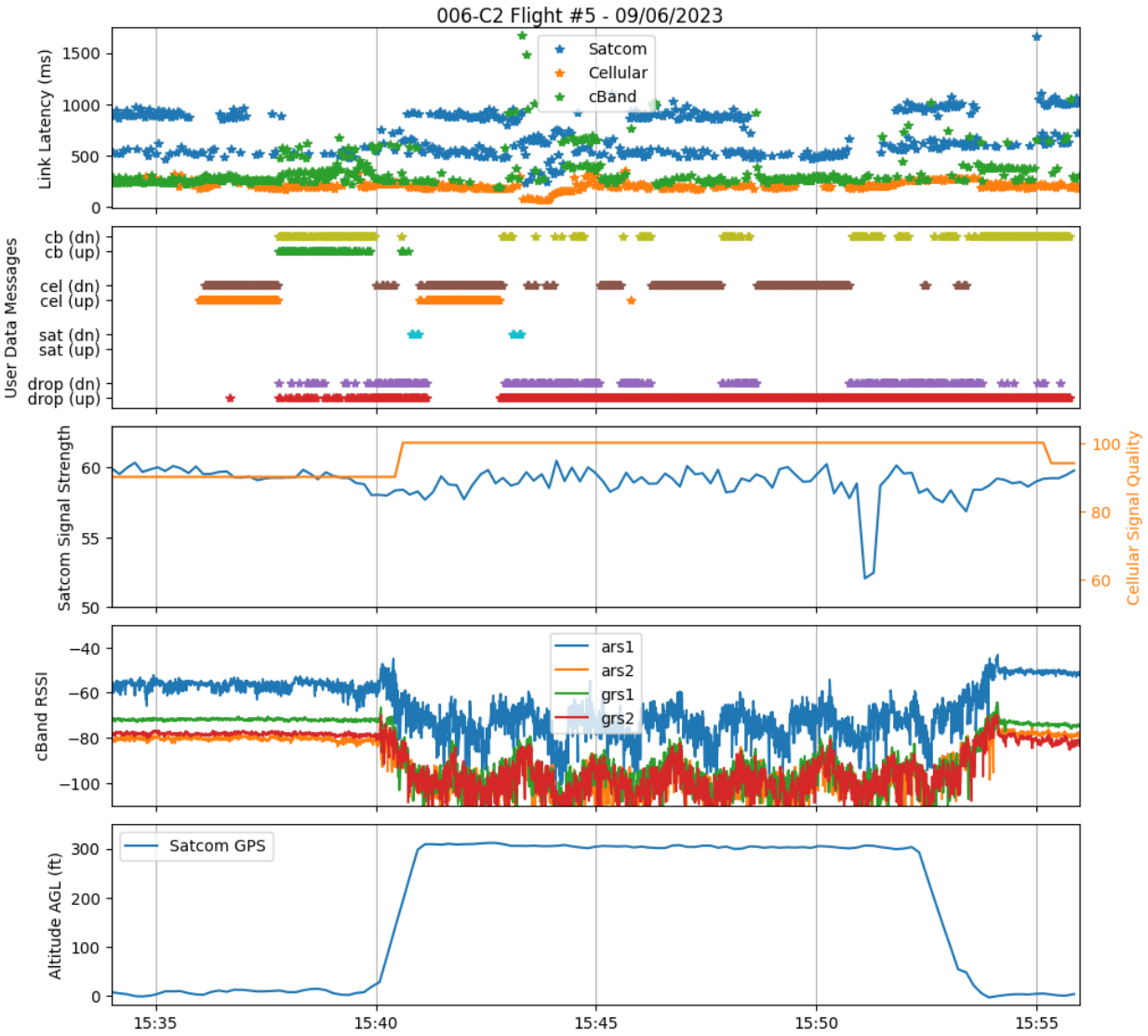
Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	3:33 status: N/2 both good. 3:33 UA send n=1, not recd good. 3:34 status 123 all links up. Nominal good. then UA. same all good. all links UP. 3:34 Secure START UA. session on LTE good. all links up. 3:35 status: Y/2 cs then UA. both good. all links up.
TP_CM_004A	User Data exchanges < MTU	**PASS**	3:35 starting data streams, cs, then UA. 3:36 UA Send n=1, recd id=4. good.
TP_C2_003B (Begin)	C2 Link Loss and Recovery	**PASS**	3:37 SWITCHOVER to 3 C-Band. good. all links up. status: Y/3 good. 3:38 CS status 123. all links up. nominal. 3:39 cleared for takeoff! 3:39 send n=1, recd id=6
TP_C2_003B (Takeoff)	C2 Link Loss and Recovery	**PASS**	3:39 TAKEOFF. disabled 2, 1, then 3. waited 3 seconds. 50ft. enable link 3
TP_C2_003B (Departure)	C2 Link Loss and Recovery	**PASS**	3:40 enable link 2. cruising altitude. 3:41 set tet =5

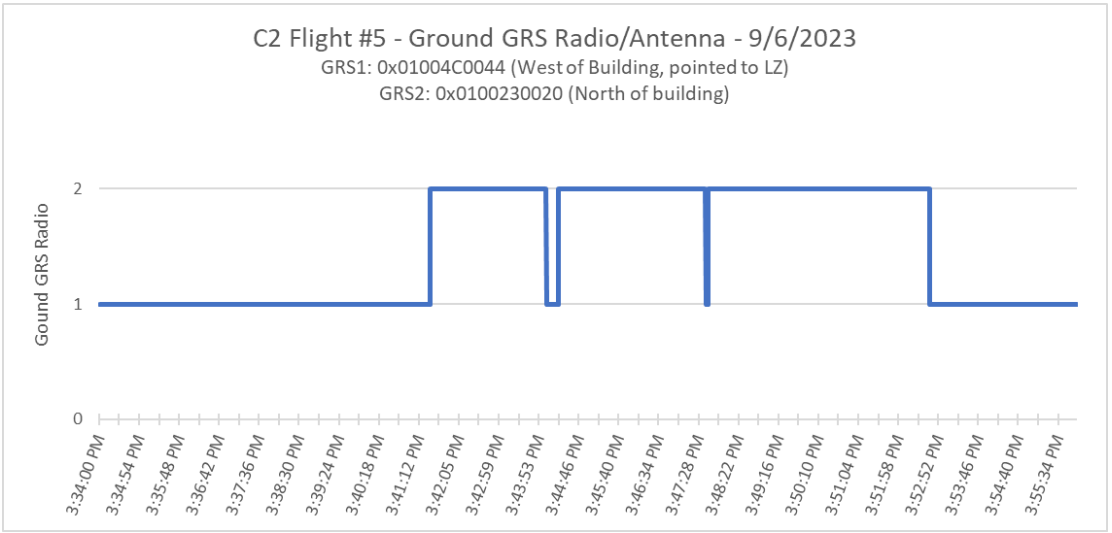
Procedure	Description	Result	Notes
TP_C2_003B (Cruise)	C2 Link Loss and Recovery	**FAIL**	on LTE session. disabled 3, disabled 1. disable 2. wait 5 sec. disabled 2. enabled 3. waiting for secure session over C-Band. 3:44 on C-Band secure. enabling 1, 2. 3:44 status Y/3. Exceeded TET. 3:44 CS Status 123. auto switchover to 2. 3:45 switch to 3 manually.. link is not very stable. 3:46 disable 3. auto switched to LTE. 3:46 Status Y/2, then CS. same good. 3:47 enable C-Band-3. all links now up. 3:47 status 3: UP nominal. 3:48 switch 3. from lte to C-Band. 1.2 sec switchover in CS. 1.49 sec on UA. 3:49 status: Y/2 - then CS. 3:49 Set TET 3 sec.
TP_C2_003B (Arrival)	C2 Link Loss and Recovery	**FAIL**	3:50 Switch 2. from LTE to C-Band. 3:50 disable 1, 2 clear to return to land. 3:51 disable 3. descending. 200 ft. enable 3. 150 ft.
TP_C2_003B (Land)	C2 Link Loss and Recovery	**FAIL**	3:52 disable 3. wait 3 sec. enable 3 enable 2. 3:53 LANDED / ON GROUND 3:54 observed TET exceeded. 3:54 status: Y/3 C-Band good. 3:55 stopping data stream. good.
TP_CM_011	Control / User Plane Termination	**FAIL**	3:55 Secure STOP. 3:56 Status N/3 both good. 3:56 send n=1, not recd.

Detailed Results:

User data messages failed to transmit in the uplink direction from the CS to the UA after the total Link Loss event at 3:42:48, even though the secure session was reestablished after the C2 system reacquired the C-Band link at 3:44 after that Link Loss event. Downlink messages were successfully exchanged and received by the CS.

For this flight test, two GRS ground C-Band radios were used, and the figure below illustrates the times when the drone flew out of range of one, and transitioned several times across the coverage areas of the two ground radios. Downlink user data messages continued to be exchanged and received by the CS throughout the flight, demonstrating both radios were used for the C-Band link.





5.1.6 C2 Link Loss and Recovery (SATCOM) – Flight 6-of-9

Result = PARTIAL: This flight test demonstrated seamless link transitions among C-Band, cellular and SATCOM networks, seamless transitions between LOS and BVLOS flight operations, and C2 link recovery after link loss.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
1	Scenario 1 – TP_C2_003B: C2 Link Loss and Recovery (SATCOM)	6	06 Sept 2023	4:17 CDT	4:42 CDT

General Test Observations: We changed the C-Band GRS-2 antenna pointing from due east to due west so we get a stronger signal when flying on the pattern. At 4:33, while the drone was descending, a tester accidently disconnected the cradlepoint and this disrupted the user data. The CS operator attempted to restart the UA consoles and the user data stream, but because the connection disruption occurred during the descent phase of flight, the connection was not reestablished before landing.
For this flight, the C-Band link was not available as we were still troubleshooting the C-Band system; Section 6.3 details the lessons learned.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	4:17 starting procedure: Status: N/2 both good. 4:18 send n=1, not recd. 4:18 CS Status 123. satcom and lte are UP. C-Band is up. C-Band has 22-sec delay. same on UA. 4:19 Secure START - good on LTE. Status CS: Y/2. then UA Y/2 good.
TP_CM_004A	User Data exchanges < MTU	**PASS**	4:20 start continuous data stream. CS then UA. 4:20 ua send n=1, recd id=4. 4:21 set tet = 3 4:21 status Y/2 satcom UP, C-Band is down.
TP_C2_003B (Begin)	C2 Link Loss and Recovery	**PASS**	4:21 Switch 1. from LTE to satcom. - good Y/1 UA then CS. 4:22 CS Status 123 satcom and LTE are UP nominal. C-Band still 22 seconds delay so it is down.
TP_C2_003B (Takeoff)	C2 Link Loss and Recovery	**PASS**	4:23 disabled LTE and C-Band. ARMING / TAKEOFF disabled satcom. wait 3 seconds. enable link 1.
TP_C2_003B (Departure)	C2 Link Loss and Recovery	**PASS**	4:24 climbing 50 ft. status. Y/1 150 ft. enable LTE. (still on satcom) 200 ft.

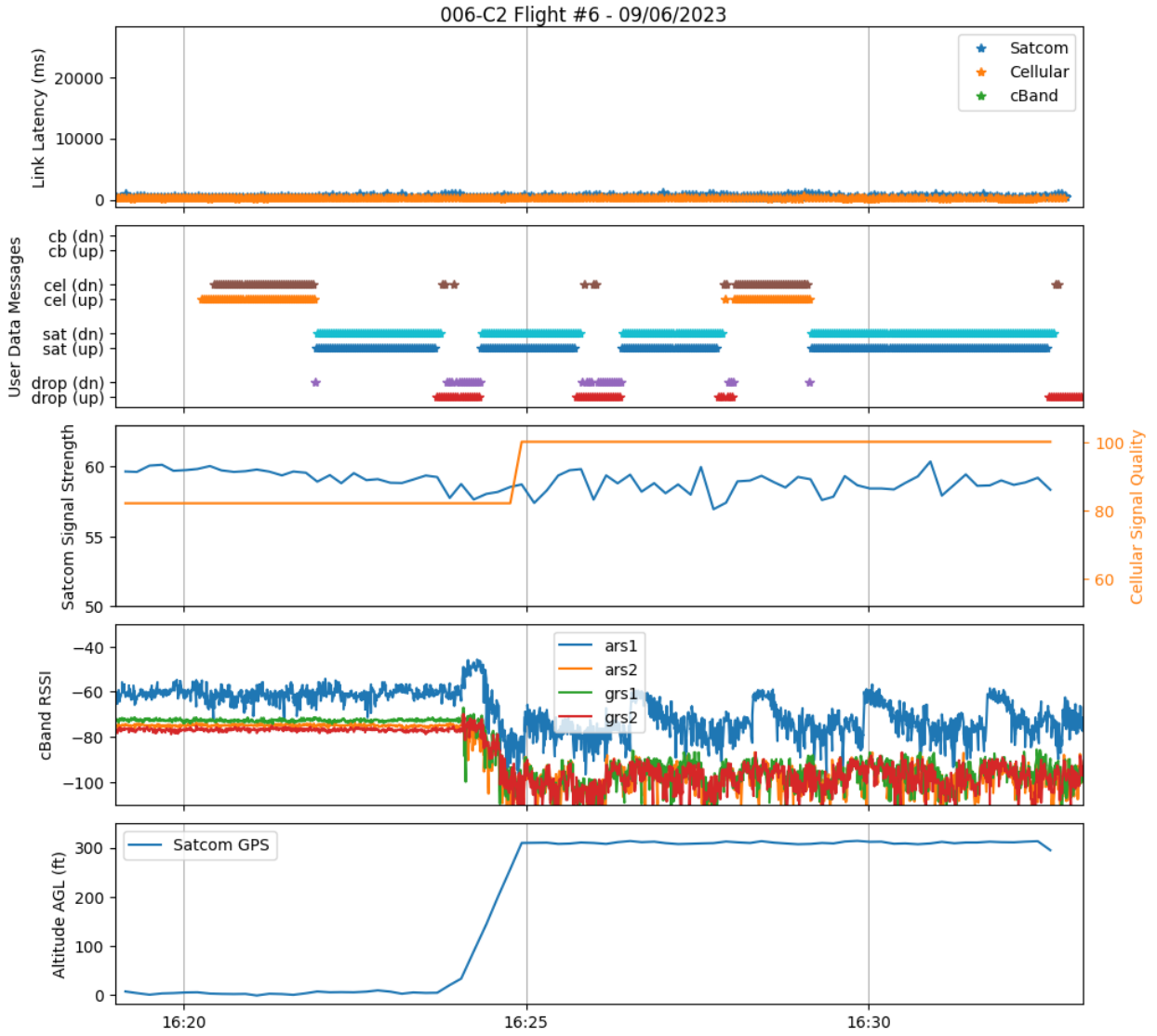
Procedure	Description	Result	Notes
TP_C2_003B (Cruise)	C2 Link Loss and Recovery	**PASS**	4:24 status Y/1. exceeded notification observed. cruising. set TET = 5. 4:25 still on satcom, w LTE available. Disable 2, 1. wait 5 seconds. enable 1. 4:26 satcom came back up. status: Y/1. Enable 2,3. (C-Band still not working.) 4:26 UA status: Y/1 (satcom) with LTE available. exceeded tet message observed. 4:27 CS Status 123. Sat+LTE are UP. nominal. C-Band has latencies of 22 sec. 4:27 disable 1, with LTE available. switched to LTE auto. good. 4:27 exceeded TET on this auto switchover. (step fails) 4:28 status: Y/2, on UA then CS. 4:28 enable 1, while on LTE. good. status 1, Satcom UP nominal. 4:29 switch 1 manual. good. 2.8 sec on UA. 2.2 sec on CS. 4:30 UA status : Y/1, (with LTE available). same on CS. 4:30 set TET 3, disable 2, 3 (stay on Satcom). 4:31 Cleared to land
TP_C2_003B (Arrival)	C2 Link Loss and Recovery	**FAIL**	4:32 disable 1. wait 3 sec. enable 1. 4:33 200 ft. 4:33 Tripped over the CRADLEPOINT!!
TP_C2_003B (Land)	C2 Link Loss and Recovery	**FAIL**	4:36 disabled 1 first (accidentally), enable 1, disabled 2, disable 1. lost track... 4:38 hovering... cleared to land... LANDED // ON GROUND / Disarmed End of flight #6 (15 minute flight)
TP_CM_011	Control / User Plane Termination	**FAIL**	4:39 status secure shows wrong status. ISSUE/ERROR UA shows N/2, CS shows Y/3, GUI shows Satcom active. 4:40 UA send n=1, NOT RECD ISSUE/ERROR GUI shows active secure session. 4:41 Secure Stop. 4:42 Status: CS: Y/2 ISSUE/ERROR UA, N/2

Detailed Results:

At 4:33, our ground control station lost internet connectivity after an accidental disconnection of our LTE access point. After this point, the system was unable to recover, losing subsequent user data messages.

Table 5-5. Lost Link Events for C2 Flight #6

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/06/2023 16:23:45.303392	Takeoff	36,847	Satcom	Satcom	Total Link Loss Recovery
09/06/2023 16:25:48.360749	Cruise	36,990	Satcom	Satcom	Total Link Loss Recovery
09/06/2023 16:27:51.685284	Cruise	11,264	Satcom	LTE	Link Loss with Alternate
09/06/2023 16:32:42.639343	Descent		Satcom		Total Link Loss. Lost GCS



5.1.7 C2 Link Loss and Recovery (SATCOM) – Flight 7-of-9

Result = PASS: This flight test demonstrated seamless link transitions among C-Band, cellular and SATCOM networks, seamless transitions between LOS and BVLOS flight operations, and C2 link recovery after link loss.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
1	Scenario 1 – TP_C2_003B: C2 Link Loss and Recovery (SATCOM)	7	06 Sept 2023	5:03 CDT	5:21 CDT

General Test Observations: For this flight, the C-Band link was not available as we were still troubleshooting the C-Band system; Section 6.3 details the lessons learned.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	5:03 starting procedure 5:03 CS status N/2 then UA both good. Send N=1, not recd. good. 5:04 status 123. satcom + lte are up. nominal. C-Band latencies slow then UA. 5:05 Secure START. good on LTE. 5:05 CS Status Y/2 UA Y/2 both good.
TP_CM_004A	User Data exchanges < MTU	**PASS**	5:06 start continuous data stream. then UA send n=1, recd id=4. 5:07 set tet 3 5:07 UA Status Y/2, then CS Y/2 same both good.
TP_C2_003C (Begin)	C2 Link Loss and Recovery	**PASS**	5:07 SWITCHOVER 1. manual from LTE to satcom. good. 5:08 status UA Y/1 then CS Y/1 both good. 5:08 CS status 123, satcom and LTE UP , C-Band down.
TP_C2_003C (Takeoff)	C2 Link Loss and Recovery	**PASS**	5:08 cleared for takeoff: d 5:09 disabled 2, 3. 5:10 ARMING / TAKEOFF. disable 1 wait 3 sec. enable 1.
TP_C2_003C (Departure)	C2 Link Loss and Recovery	**PASS**	5:10 100ft. 150ft. Status Y/1. enable LTE. 200 ft.

Procedure	Description	Result	Notes
TP_C2_003C (Cruise)	C2 Link Loss and Recovery	**PASS**	5:11 UA status: Y/1 250-ft. observed TET exceeded. Cruising..... 5:11 set TET=5 5:11 disable 2, disable 1 (satcom was active secure). now no links. wait 3 sec. enable 1. 5:12 now on satcom secure, only active link. 5:12 enable 2, 3. (C-Band not working). 5:12 UA status: Y/1 good. 5:13 CS status 123. Satcom and LTE UP nominal. C-Band not working... 5:13 disable 1, with LTE UP. auto switchover good. 5:13 UA status secure: Y/2 - good. (Satcom disabled). CS status y/2 5:14 Enable 1 satcom. Status 1. UP nominal good. Switch 1 (from LTE to satcom). good. 5:14 UA switchover took 2.9 sec. CS time took 2.341 sec. 5:15 UA status: Y/1 CS: Y/1 5:16 Set TET 3.. 5:16 still secure on satcom. with LTE UP. 5:16 disable 2, 3. Return to Land command issued.... 5:17 disable 1. wait 3 sec. enable 1. 220 ft. 200ft. 5:17 CS Y/1. disable 1. 100ft. wait 3 sec. enable 1. 5:18 CS status secure: Y/1 enable 2. observed TET Exceeded on UA. (x2)
TP_C2_003C (Arrival)	C2 Link Loss and Recovery	**PASS**	5:19 UA Y/1. cleared to land. holding at 50 ft.
TP_C2_003C (Land)	C2 Link Loss and Recovery	**PASS**	5:20 LANDED / Disarmed. 10 minute flight 5:20 CS Status Y/1. then UA Y/1. good.
TP_CM_011	Control / User Plane Termination	**PASS**	5:20 stop data streams. 5:21 secure STOP 5:21 status: CS: N/1, UA: N/1. UA send n=1, not recd good.

Detailed Results:

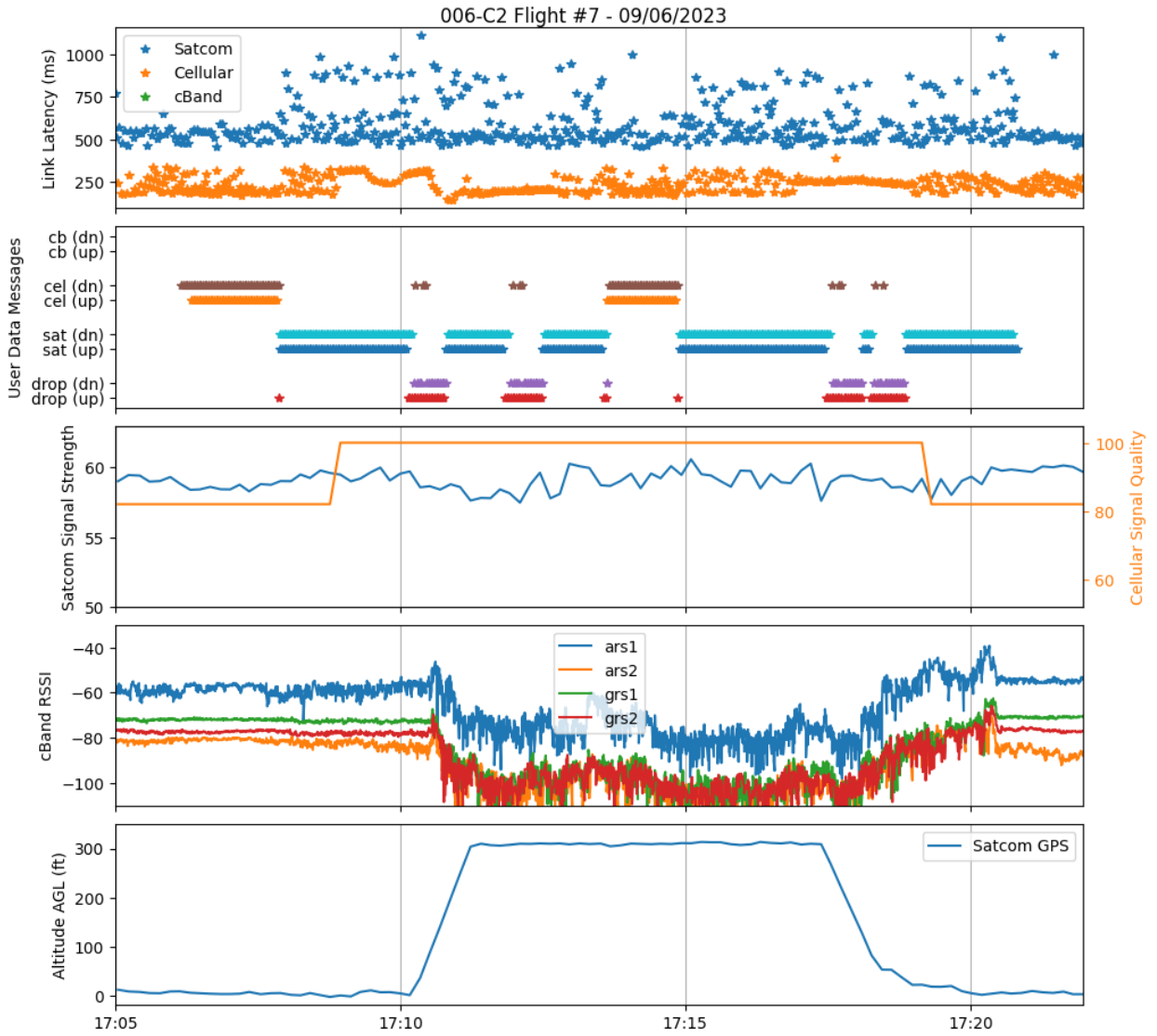
This test sequence demonstrated a total link loss condition four times, while Satcom was the active link. In all four instances, the link was successfully reestablished back on Satcom after re-enabling the link.

Although the duration of the four total link loss instances were all under 10 seconds, the figure below shows there was a gap, or an interruption in the user data for a longer duration.

We performed a link loss test at 5:13 while on Satcom, with LTE available as a backup. The C2 system successfully switched the active link from Satcom to LTE.

Table 5-6. Lost Link Events for C2 Flight #7

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/06/2023 17:10:13.398545	Takeoff	36,633	Satcom	Satcom	Total Link Loss Recovery
09/06/2023 17:11:55.454219	Cruise	36,888	Satcom	Satcom	Total Link Loss Recovery
09/06/2023 17:13:37.954870	Cruise	1,532	Satcom	LTE	Link Loss with Alternate
09/06/2023 17:17:31.748594	Descent	36,558	Satcom	Satcom	Total Link Loss Recovery
09/06/2023 17:18:16.746931	Landing	37,291	Satcom	Satcom	Total Link Loss Recovery



5.1.8 C2 Link Loss and Recovery (C-Band) – Flight 8-of-9

Result = PASS: This flight test demonstrated seamless link transitions among C-Band, cellular and SATCOM networks, seamless transitions between LOS and BVLOS flight operations, and C2 link recovery after link loss.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
1	Scenario 1 – TP_C2_003C: C2 Link Loss and Recovery (C-Band)	8	07 Sept 2023	4:17 CDT	4:37 CDT

General Test Observations: During this flight, the CS operator had to command the CS and UA to switch from LTE/satcom back to C-Band four times because the DTSRs had automatically moved to either LTE or satcom because the C-Band link was unstable. This was our first formal test flight after stabilizing the C-Band link, however, this flight helped diagnose the impact of the vertical coverage from the ground antenna to the UA. It was determined that the GRS C-Band antenna was positioned at the ground level, and oriented towards the ground area of the landing zone, so when the UA was flying at higher altitudes of about 200 ft and flying laterally outward beyond the cone of coverage, near the ground antenna, the RSSI signal strength was significantly degraded. Therefore, subsequent flights optimized the flying pattern to limit altitudes to 100 ft, and to stay within a closer lateral distance from the coverage cone from the GRS C-Band antenna.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	4:17 CS Status secure: N/2, then UA N/2. send n=1, not recd good. CS Status 123 all links UP nominal. 4:18 UA Status 123 all up nominal 4:18 Secure Start CS Status secure: Y/2 UA Y/2 both good. 4:19 start continuous data stream. with 2 sec delay.
TP_CM_004A	User Data exchanges < MTU	**PASS**	4:19 UA send n=1, recd id=6
TP_C2_003C (Begin)	C2 Link Loss and Recovery	**PASS**	4:20 UA Switch 3 from LTE to C-Band 4:20 UA Set TET =3, then CS = 3 4:20 UA Status Y/3, CS Y/3 both good CS Status 123 all links up nominal.
TP_C2_003C (Takeoff)	C2 Link Loss and Recovery	**PASS**	4:21 Cleared for takeoff!!! Disable 1,2 4:21 ARMING / SPINNING / TAKEOFF. disable 3 wait 3 sec. enable 3. good

Procedure	Description	Result	Notes
TP_C2_003C (Departure)	C2 Link Loss and Recovery	**PASS**	4:22 CS Status Y/3 enable 2, 4:22 UA status Y/3, observed TET exceeded - good. 100 ft. climbing 150 ft. 4:22 Set TET=5 4:23 Switch 3. but C-Band went down. disable 2. disable 3 4:23 enable 3. 4:24 drone lowered to 100 ft. 4:24 status secure Y/2. C-Band is flaky enable 1,2. Secure on SATCOM. TET exceeded. 4:25 CS Status123: all up nominal. SWITCH 3 from satcom to C-Band.
TP_C2_003C (Cruise)	C2 Link Loss and Recovery	**PASS**	4:26 disable 3, switched auto to LTE - good. UA Status Y/2, CS Y/2 4:26 Enable C-Band while on LTE. 4:27 status 3 up nominal, but went down SWITCH 3, good. 4:28 auto switchover to LTE> C-Band dropped. gray. 4:29 set tet =3. we are on LTE. 4:31 Instructed to go to center and hold. SWITCH 3 4:31 Disable 1, 2 4:32 return to land.
TP_C2_003C (Arrival)	C2 Link Loss and Recovery	**PASS**	4:32 Disable 3. wait 3 sec. enable 3. 4:33 on C-Band, status sec. Y/3 4:33 coming to land. disable 3 (only link), wait 3 enable C-Band. good.
TP_C2_003C (Land)	C2 Link Loss and Recovery	**PASS**	4:33 CS Status Y/3, enable 2 good. 4:34 LANDED. ON GROUND. 4:34 UA status secure Y/3.
TP_CM_011	Control / User Plane Termination	**PASS**	CS Status Y/3, then UA Y/3 UA Stop data streams 4:35 UA Secure stop CS Status N/3, UA same N/3. send n=1, not recd, good.

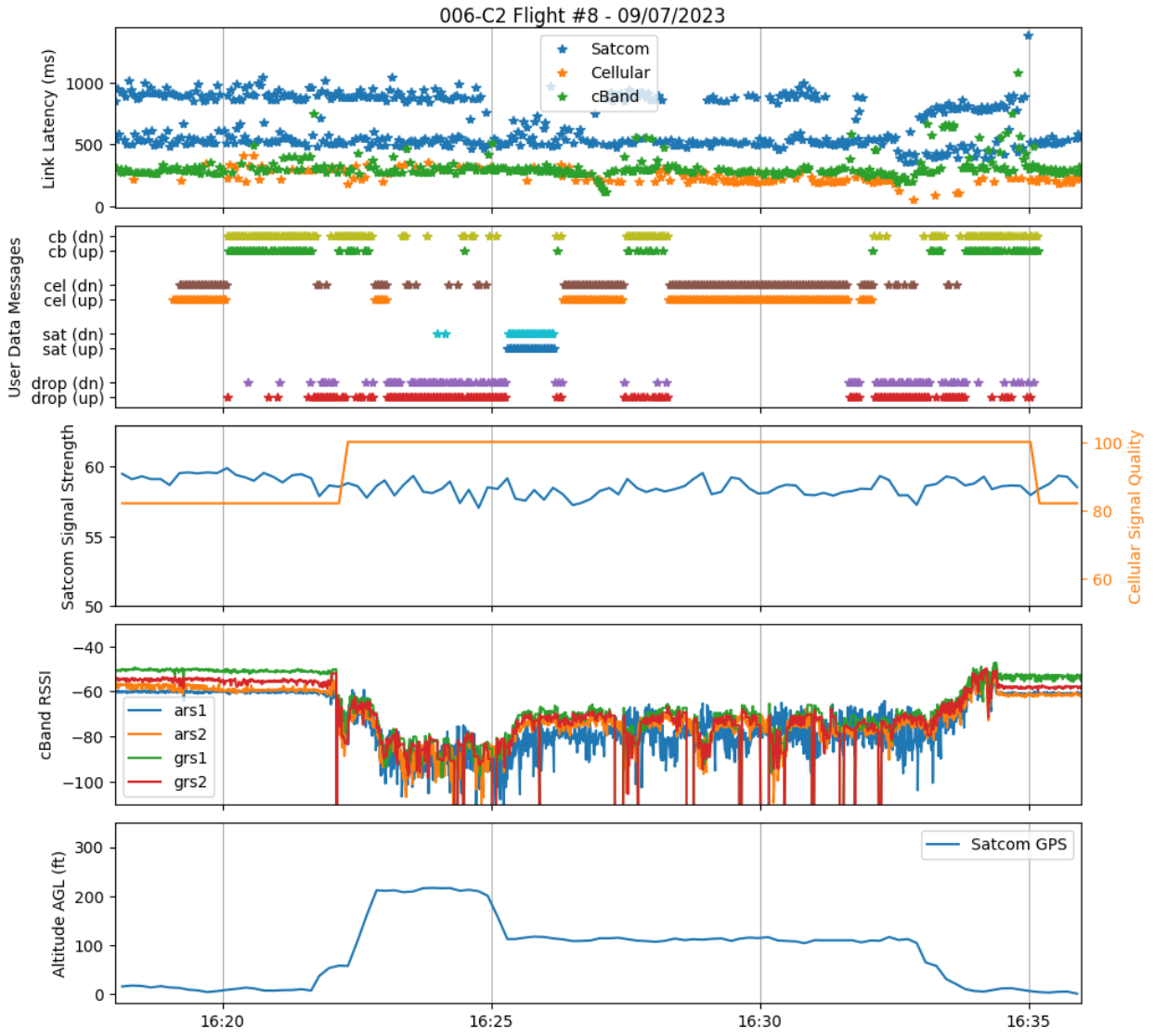
Detailed Results:

Table 5-7. Manual Commanded Switchovers for C2 Flight #8

Time (CDT)	From	To	Flight Phase	Switchover time (ms)	TET	<TET
16:20	LTE	C-Band	surface	1,798	3,000	Y
16:23	LTE	C-Band	cruise	1,622	5,000	Y
16:26	satcom	C-Band	cruise	1,668	5,000	Y
16:27	LTE	C-Band	cruise	1,599	5,000	Y
16:31	satcom	C-Band	cruise	7,596	5,000	N

Table 5-8. Lost Link Events for C2 Flight #8

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/07/2023 16:21:45.640609	Takeoff		C-Band		followed by other switchover
09/07/2023 16:22:00.655388	Takeoff	4,699	C-Band	C-Band	Total Link Loss Recovery
09/07/2023 16:22:48.927872	Cruise	1,439	C-Band	LTE	auto. unstable link
09/07/2023 16:23:25.193864	Cruise		C-Band		followed by other switchover
09/07/2023 16:24:24.826015	Cruise	53,929	C-Band	Satcom	Total Link Loss Recovery
09/07/2023 16:26:18.986761	Cruise	1,452	C-Band	LTE	Link Loss with Alternate
09/07/2023 16:28:17.545889	Cruise	1,443	C-Band	LTE	auto. unstable link
09/07/2023 16:32:06.945871	Descent		C-Band		followed by other switchover
09/07/2023 16:32:18.951323	Descent		C-Band		followed by other switchover
09/07/2023 16:32:20.452080	Descent	50,364	C-Band	C-Band	Total Link Loss Recovery
09/07/2023 16:33:27.469887	Landing	22,938	C-Band	C-Band	Total Link Loss Recovery



5.1.9 C2 Link Loss and Recovery (C-Band) – Flight 9-of-9

Result = PASS: This flight test demonstrated seamless link transitions among C-Band, cellular and SATCOM networks, seamless transitions between LOS and BVLOS flight operations, and C2 link recovery after link loss.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
1	Scenario 1 – TP_C2_003C: C2 Link Loss and Recovery (C-Band)	9	07 Sept 2023	4:53 CDT	5:08 CDT

General Test Observations: During this flight, the CS operator issued the command "status" and the status response differed from the GUI display. This problem occurred at 4:58 and 5:06, and we determined there is a delay for the STATUS command to update by about 3 seconds.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	4:53 CS status N/2 then UA N/2 4:53 UA send n=1, not recd. good. 4:54 CS status 123 - all up nominal. good. 4:54 UA Status 123 - all up nominal. good. 4:54 UA secure start. - good on LTE. good. 4:54 CS Status Y/2, then UA, Y/2 4:55 CS start data stream, 2-sec delay. good. then UA.
TP_CM_004A	User Data exchanges < MTU	**PASS**	4:55 UA send n=1, ID=4 4:56 UA switch 3 good.
TP_C2_003C (Begin)	C2 Link Loss and Recovery	**PASS**	set TET=3 UA then CS. 4:56 UA status: Y/3, then CS Y/3 4:56 CS Status 123. all up nominal.
TP_C2_003C (Takeoff)	C2 Link Loss and Recovery	**PASS**	4:57 cleared for takeoff Flight 9, disable 2,1. 4:57 ARMING / SPINNING / TAKEOFF disable 3, wait 3 sec., enable 3. good.
TP_C2_003C (Departure)	C2 Link Loss and Recovery	**PASS**	4:58 CS Status Y/2. ISSUE/ERROR gui shows secure on 3, but status says Y/2. Enable 2. 4:58 UA Y/3. cruising at 100-ft. 4:59 Set TET=5, disable 2, 3 (no links active) wait 5 sec. enable 3.good.
TP_C2_003C (Cruise)	C2 Link Loss and Recovery	**PASS**	5:00 CS Status Y/3. 5:01 enable 1,2 while on C-Band. good. UA Status Y/3 good. observed exceeded TET. CS Status 123, all up, nominal. 5:02 all links up, disable 3. auto switchover to LTE. ISSUE/ERROR switch took longer. Status Y/2 on both. 5:02 enable 3, all links up. CS status 3, UP. good. Switch 3 from LTE to C-Band. Switchover time: CS: 1.281 sec, UA 1.641 sec 5:04 UA Status: Y/3, good.
TP_C2_003C (Arrival)	C2 Link Loss and Recovery	**PASS**	5:05 CS Status, Y/3, good. 5:05 Set TET=3. 5:05 Disable 1, 2. Return to land. 5:05 disable 3. wait 3 sec. enable 3, up good.

Procedure	Description	Result	Notes
TP_C2_003C (Land)	C2 Link Loss and Recovery	**PASS**	5:06 CS status : Y/2 ISSUE/ERROR Should be Y/3. disable 3, with 3 sec... enable 3 =- up good. 5:07 Enable 2, good status: Y/3. exceeded TET notifications. LANDED / ON GROUND END OF FLIGHT 9. UA Status: Y/3. 5:08 Status secure Y/3, both. stopping data streams. UA Secure STOP. session gone.
TP_CM_011	Control / User Plane Termination	**PASS**	good. status N/3 CS then UA. N/3. 5:08 UA send n=1, not recd, good.! flight, max altitude 100 ft. close tighter box closer to GRS

Detailed Results:

At 4:58 and 5:06 we observed the same display issue as on Flight #1, where the DTSR briefly showed the wrong active link.

This test sequence demonstrated the total link loss condition four times, while C-Band was providing the secure link. In all four instances, the link was successfully reestablished back on C-Band after re-enabling the link.

Although the duration of the four total link loss instances were all under 10 seconds, the figure below shows there was a gap, or an interruption in the user data for a longer duration.

We performed a link loss test at 5:02 while on C-Band, with LTE available as a backup. The C2 system successfully switched the active link from C-Band to LTE as expected.

Table 5-9. Lost Link Events for C2 Flight #9

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/07/2023 16:57:53.509804	Takeoff	41,206	C-Band	C-Band	Total Link Loss Recovery
09/07/2023 16:59:38.665476	Cruise	22,962	C-Band	C-Band	Total Link Loss Recovery
09/07/2023 17:02:11.840487	Cruise	10,222	C-Band	LTE	Link Loss with alternate
09/07/2023 17:06:01.447274	Descent	23,430	C-Band	C-Band	Total Link Loss Recovery
09/07/2023 17:06:34.576339	Landing	23,142	C-Band	C-Band	Total Link Loss Recovery

5.1.10 Flying out of C-Band range – Flight 1-of-4

Result = PASS: This flight test demonstrated CNPC performance in both LOS and BVLOS representative operational environments.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
2	Scenario 2 – Flying out of C-Band range (TP_C2_001: BVLOS, Multiple Radio Towers in Dept/Approach)	14	07 Sept 2023	6:33 CDT	6:46 CDT

General Test Observations: This Flight Test Card was modified from a multi-tower test, to flying out of range of C-Band. For these flights (#14-#17), the test was configured with a single ground GRS antenna as explained in Section 6, lessons learned, because of issues experienced with the C-Band link. However, we were able to configure the flights such that when the UA

was flying directly over the ground GRS antenna, the RSSI signal strength would drop to below -100 dB, and the data would not be transmitted between the UA and the CS. There was no need to disconnect radios or to reposition antennas in order to lose the C-Band signal. The procedure to fly out of range was to increase the altitude of the UA from 100 ft to 300 ft, and to reposition the drone to fly directly over the ground GRS antenna.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	6:33 - cs ua: N/2 6:34 ua send n=1 not recd good. cs status 123. all links up nominal secure start. good on LTE. 6:34 cs Y/2 ua: Y/2
TP_CM_004A	User Data exchanges < MTU	**PASS**	6:35 start data stream. 6:35 send n=1 recd id =4 good. 6:36 cs 123 all up nominal good.
TP_C2_001 (Takeoff)	BVLOS, Flying out of C-Band range	**PASS**	cs Y/2 ua Y/2 set TET 3 6:36 cleared for takeoff. RSSI grs -50 UA -55 6:37 cs: status Y/2 ua: Y/2 6:38 set TET = 5. going out of range... switch 3 from LTE 6:39 drone flew over GRS. C-Band dropped. autoswitchover to LTE. Pass.
TP_C2_001 (Cruise)	BVLOS, Flying out of C-Band range	**PASS**	6:40 RSSI -90. 6:41 cs Y/2. RSSI -100 6:42 C-Band dropped at 300 ft. over antenna GRS. 6:43 RSSI -100 / -95. RSSI improved. status 123 cs: all up nominal good. Switch 3. good. 6:44 ua Y/3 cs: Y/3
TP_C2_001 (Land)	BVLOS, Flying out of C-Band range	**PASS**	6:45 LANDED / ON GROUND.
TP_CM_011	Control / User Plane Termination	**PASS**	6:45 Y/3 ua: Y/3 stop data streams. 6:46 secure start (error) then stop. send n=1 not recd good.

Detailed Results:

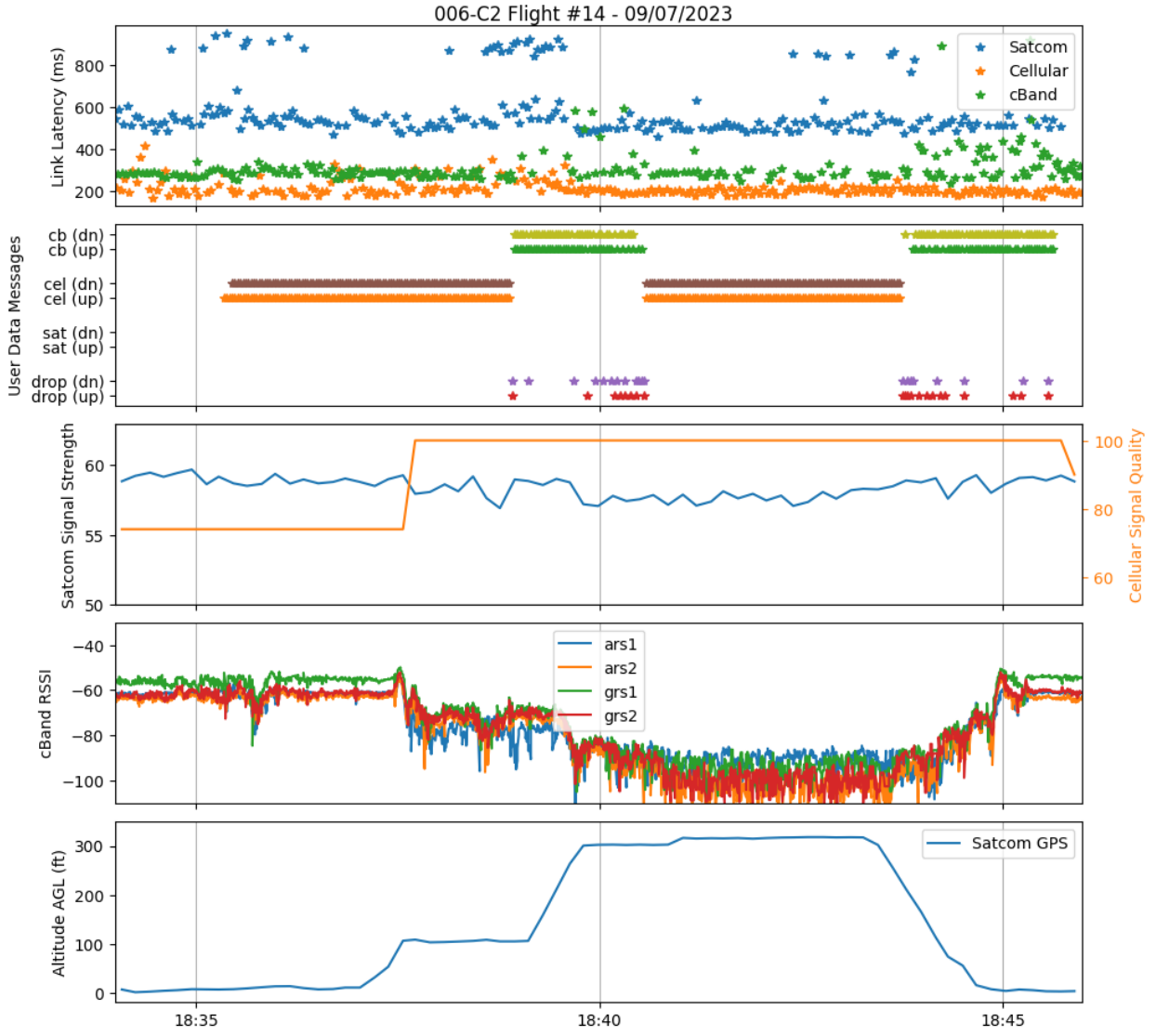
At 6:40, as the UA was flying out of range of C-Band, the RSSI dropped to about -90 dB and the C2 system automatically switched from C-Band to LTE as it detected the link was lost.

The C-Band latencies do not significantly increase as the UA is flying out of range. Even during the C-Band drop, while the UA is still out of range, some control keep-alive messages indicating

the latency continue to transmit. However, the RSSI signal strength is still insufficient for maintaining an active session through the C-Band link.

Table 5-10. Lost Link Events for C2 Flight #14

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/07/2023 18:40:33.390610	Cruise	1,439	C-Band	LTE	Flew out of range of C-Band



5.1.11 Flying out of C-Band range – Flight 2-of-4

Result = PASS: This flight test demonstrated CNPC performance in both LOS and BVLOS representative operational environments.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
2	Scenario 2 – Tower Swap (TP_C2_001: BVLOS, Multiple Radio Towers in Dept/Approach)	15	07 Sept 2023	6:54 CDT	7:06 CDT

General Test Observations: This Flight Test Card was modified from a multi-tower test, to flying out of range of C-Band. For these flights (#14-#17), the test was configured with a single ground GRS antenna as explained in Section 6, lessons learned, because of issues experienced with the C-Band link. However, we were able to configure the flights such that when the UA was flying directly over the ground GRS antenna, the RSSI signal strength would drop to below -100 dB, and the data would not be transmitted between the UA and the CS. There was no need to disconnect radios or to reposition antennas in order to lose the C-Band signal. The procedure to fly out of range was to increase the altitude of the UA from 100 ft to 300 ft, and to reposition the drone to fly directly over the ground GRS antenna.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	6:55 cs N/2, ua N/2 6:56 ua send n=1 not recd good. cs status 123 all up nominal good. then ua. nominal good. 6:57 secure start ua. session on LTE. good.
TP_CM_004A	User Data exchanges < MTU	PASS	6:57 cs Y/2, ua Y/2 cs start continuous data stream. then ua good. 6:58 ua send n=1 recd id=4. 6:58 switch 3. good.
TP_C2_001 (Takeoff)	BVLOS, Flying out of C-Band range	PASS	cs Y/3 cs status 123 all up nominal good. 6:59 cs Y/3 set tet = 3 TAKEOFF ARMING rssi -60 / -75.
TP_C2_001 (Departure)	BVLOS, Flying out of C-Band range	PASS	

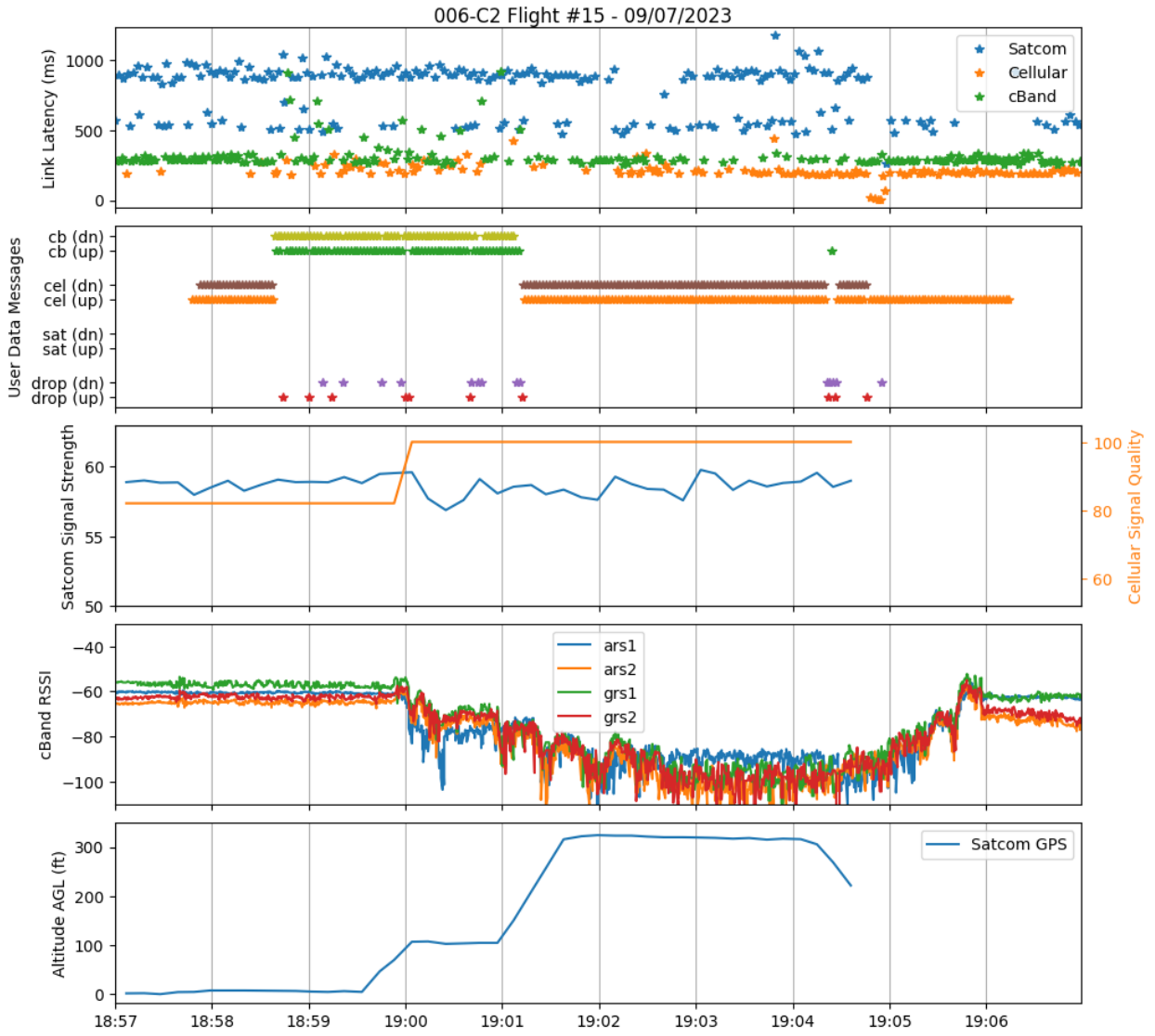
Procedure	Description	Result	Notes
TP_C2_001 (Cruise)	BVLOS, Flying out of C-Band range	**PASS**	7:00 cs: Y/3, ua: Y/3 set TET =5 100 ft cruising. 7:01 lost C-Band autoswitchover to LTE. no tet exceeded good ua Y/2. cs Y/2 RSSI -80 / -88 RSSI -100 / -90. C-Band is gray/green 7:02 cs: Y/2. ua Y/2 7:03 return to land.
TP_C2_001 (Arrival)	BVLOS, Flying out of C-Band range	**PASS**	switch 3. good. autoswitchover to LTE. 7:05 ua: Y/2 there is a TET exceeded notification. but not on CS.
TP_C2_001 (Land)	BVLOS, Flying out of C-Band range	**PASS**	7:05 LANDED / ON GROUND.
TP_CM_011	Control / User Plane Termination	**PASS**	7:06 cs Y/2 ua: Y/2 good. stop data stream. 7:06 secure stop. good. cs N/2. ua N/2. ua send n=1 not recd good.

Detailed Results:

At 7:04, the Satcom/LTE unit stopped reporting signal strength and altitude information from the Satcom GPS. However, the Satcom and LTE links were still online and communicating between the CS and the UA.

Table 5-11. Lost Link Events for C2 Flight #15

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/07/2023 19:01:11.339600	Cruise	1,535	C-Band	LTE	Flew out of range of C-Band



5.1.12 Flying out of C-Band range – Flight 3-of-4

Result = PARTIAL: This flight test demonstrated CNPC performance in both LOS and BVLOS representative operational environments.

General Test Observations: This Flight Test Card was modified from a multi-tower test, to flying out of range of C-Band. For these flights (#14-#17), the test was configured with a single ground GRS antenna as explained in Section 6, lessons learned, because of issues experienced with the C-Band link. However, we were able to configure the flights such that when the UA was flying directly over the ground GRS antenna, the RSSI signal strength would drop to below -100 dB, and the data would not be transmitted between the UA and the CS. There was no need to disconnect radios or to reposition antennas in order to lose the C-Band signal. The procedure to fly out of range was to increase the altitude of the UA from 100 ft to 300 ft, and to reposition the drone to fly directly over the ground GRS antenna.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
2	Scenario 2 – Tower Swap (TP_C2_001: BVLOS, Multiple Radio Towers in Dept/Approach)	16	08 Sept 2023	9:35 CDT	9:50 CDT

General Test Observations: Using 1 GRS south of parking/command trailer.
ARS has attenuators.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	9:35 starting procedure for Flight 16 cs N/2 ua N/2 ua send n=1, not recd good 9:35 cs status 123: all up nominal good 9:36 ua status 123: all up nominal good ua secure START... up on LTE good cs Y/2, ua Y/2 good
TP_CM_004A	User Data exchanges < MTU	**PASS**	9:37 start user data stream. cs then ua. 2 sec delay good 9:37 send n=1 ua recd id=4 9:38 switch 3 good.
TP_C2_001 (Takeoff)	BVLOS, Flying out of C-Band range	**PASS**	cs Y/3 ua Y/3 set tet =3 TAKEOFF / ARMING 9:39 ua: Y/3 cs Y/3 still on C-Band 9:41 set tet=5
TP_C2_001 (Departure)	BVLOS, Flying out of C-Band range	**PASS**	flying out of range of C-Band climbing. C-Band intermittent down. 9:43 while climbing from 100 to 300 C-Band went down. auto switchover to LTE. 9:43 switchover exceeded TET
TP_C2_001 (Cruise)	BVLOS, Flying out of C-Band range	**PASS**	Drone positioned over antenna dead spot for out of range... C-Band going gray intermittent RSSI in mid-90s. 9:45 cs: Y/2 ua Y/2 still at 300 ft over antenna.
TP_C2_001 (Arrival)	BVLOS, Flying out of C-Band range	**PASS**	9:46 flying to box at 100 ft... descending... 9:47 reached box at 100 ft. cs status 123 all up, nominal.
TP_C2_001 (Land)	BVLOS, Flying out of C-Band range	**FAIL**	SWITCH 3. good. 9:48 LANDED / ON GROUND / Y/3 Y/3 good

Procedure	Description	Result	Notes
TP_CM_011	Control / User Plane Termination	**PASS**	9:49 cs Y/3 ua Y/3 good. stopping data stream secure STOP. cs N/3, ua N/3 9:50 send n=1 not recd good.

Detailed Results:

As the UA was flying out of range of C-Band, climbing from 100 ft to 300 ft, and from the coverage area to over the C-Band antenna, at 9:42, the C2 system automatically switched the active link from C-Band to LTE, because the C-Band signal had degraded to about -90 dB.

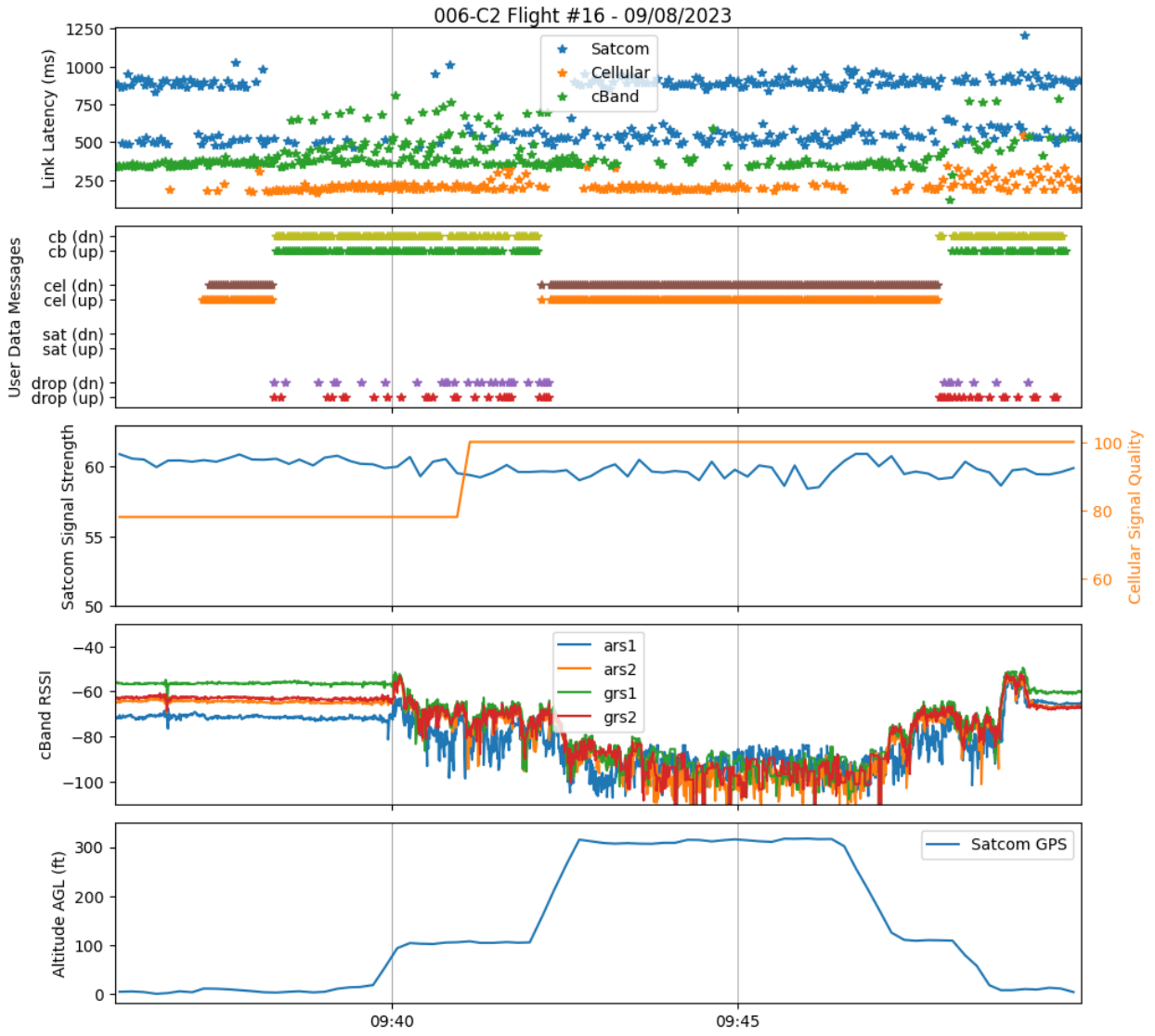
The manually commanded switchover from LTE to C-Band at 9:47 succeeded in switching over the active link. However, the switchover exceeded the TET limit.

Table 5-12. Manually Commanded Switchovers C2 Flight #16

Time (CDT)	From	To	Flight Phase	Switchover time (ms)	TET	<TET
9:38	LTE	C-Band	surface	1,894	3,000	Y
9:47	LTE	C-Band	arrival	11,813	3,000	N

Table 5-13. Lost Link Events for C2 Flight #16

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/08/2023 09:41:42.608421	Cruise	4,878	C-Band	C-Band	auto. Unstable link
09/08/2023 09:42:08.120258	Cruise	10,626	C-Band	LTE	Flew out of range of C-Band
09/08/2023 09:48:06.564275	Landing	626	C-Band	C-Band	auto. Unstable link



5.1.13 Flying out of C-Band range – Flight 4-of-4

Result = PASS: This flight test demonstrated CNPC performance in both LOS and BVLOS representative operational environments.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
2	Scenario 2 – Tower Swap (TP_C2_001: BVLOS, Multiple Radio Towers in Dept/Approach)	17	08 Sept 2023	9:59 CDT	10:15 CDT

General Test Observations: This Flight Test Card was modified from a multi-tower test, to flying out of range of C-Band. For these flights (#14-#17), the test was configured with a single ground GRS antenna as explained in Section 6, lessons learned, because of issues experienced with the C-Band link. However, we were able to configure the flights such that when the UA was flying directly over the ground GRS antenna, the RSSI signal strength would drop to below -

100 dB, and the data would not be transmitted between the UA and the CS. There was no need to disconnect radios or to reposition antennas in order to lose the C-Band signal. The procedure to fly out of range was to increase the altitude of the UA from 100 ft to 300 ft, and to reposition the drone to fly directly over the ground GRS antenna.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	9:59 CS N/2 10:00 ua N/2 good. ua send n=1 not recd good. CS status 123 all up nominal. good. 10:01 ua status 123 all up nominal. good. ua secure start. up on LTE good. cs Y/2, ua: Y/2 good.
TP_CM_004A	User Data exchanges < MTU	**PASS**	10:02 cs start continuous data stream, then ua. good. 10:02 ua send n=1 recd id=4 good.
TP_C2_001 (on ground)	BVLOS, Flying out of C-Band range	**PASS**	10:02 switch 3. from LTE to C-Band good. cs status 123 all links up nominal. cs Y/3 10:03 set tet =3 ready for takeoff...
TP_C2_001 (Departure)	BVLOS, Flying out of C-Band range	**PASS**	10:03 ARMING / TAKEOFF 10:04 noted auto switchover to LTE. switch 3. failed to switch link up/down. TET exceeded. 10:05 switch 3. good. TET good. auto switchover to LTE 10:06 set TET =5 switch 3. good. cs: y/3 auto switchover during climbing out of range - GOOD. 10:07 still climbing out of range, still on LTE 10:08 C-Band going up/down green/gray.
TP_C2_001 (Cruise)	BVLOS, Flying out of C-Band range	**PASS**	reached far position. C-Band shows gray. ua: Y/2 cs: Y/2 good. RSSI: -100 RSSI ARS showing intermittent 'down' on skyline. Cs: Y/2 ua Y/2 10:09 still out of range position. 10:10 returning to 'box' at 100 ft... descending.... 10:11 reached box at 100 ft. RSSI -65ish cs all links up nominal good. switch 3. switchover time 1.783 sec. on CS.

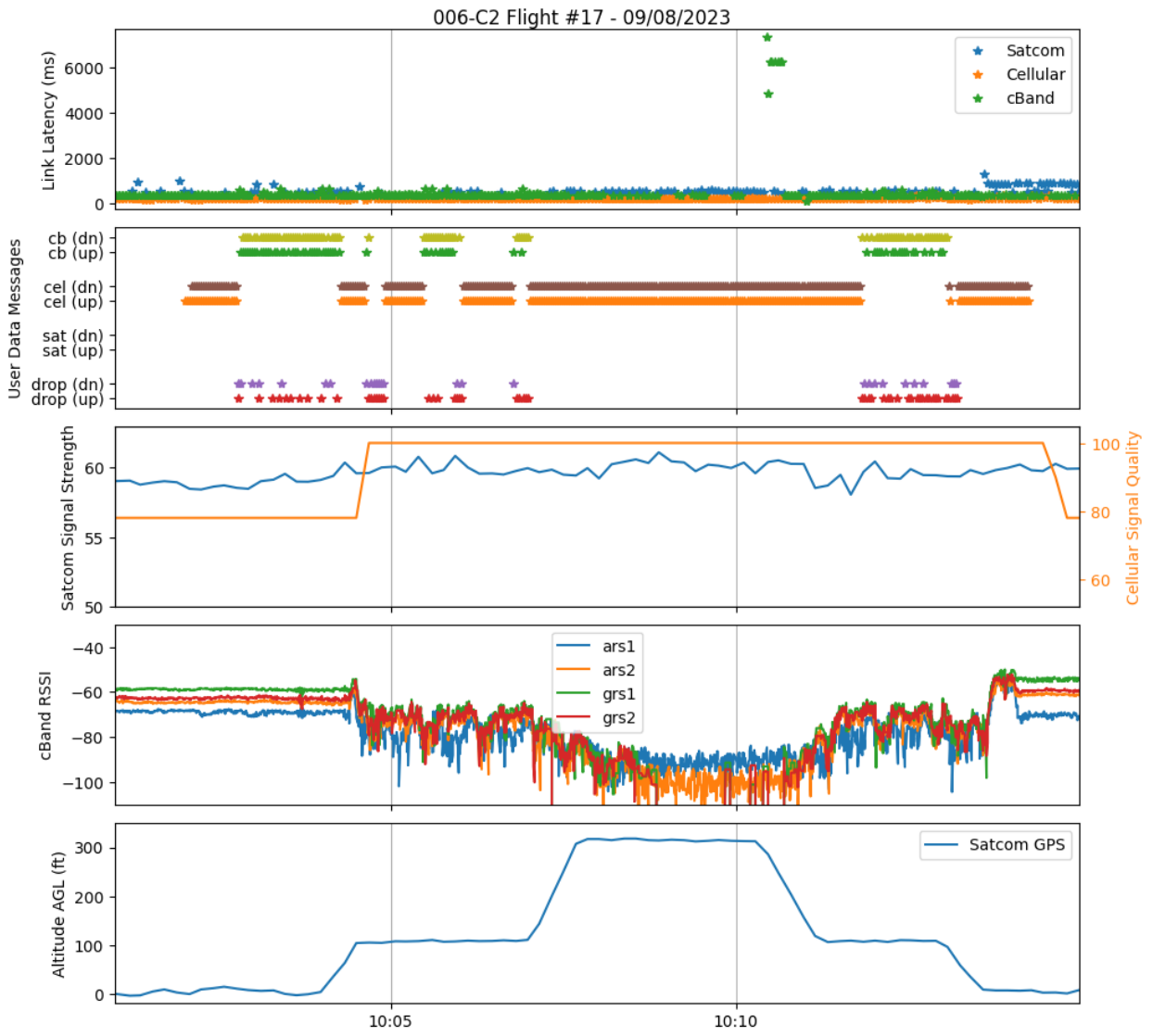
Procedure	Description	Result	Notes
TP_C2_001 (Arrival)	BVLOS, Flying out of C-Band range	PASS	10:12 ua Y/3 cs Y/3 good. no switchover. cleared to land...
TP_C2_001 (Land)	BVLOS, Flying out of C-Band range	PASS	10:13 auto switch over to LTE> exceeded TET. 10:13 LANDED / ON GROUND cs: Y/2, ua: Y/2 good.
TP_CM_011	Control / User Plane Termination	PASS	10:14 stopping data streams ua secure stop cs N/2, ua: N/2 ua send n=1 not recd. good.

Detailed Results:

As the UA was flying out of range of C-Band, climbing from 100 ft to 300 ft, and from the coverage area to over the C-Band antenna, at 10:07, the C2 system automatically switched the active link from C-Band to LTE, because the C-Band signal had degraded to about -90 dB.

Table 5-14. Lost Link Events for C2 Flight #17

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/08/2023 10:04:16.435092	Departure	1,389	C-Band	LTE	auto. Unstable link
09/08/2023 10:06:01.490131	Cruise	1,418	C-Band	LTE	auto. Unstable link
09/08/2023 10:07:00.060217	Cruise	1,452	C-Band	LTE	Flew out of range of C-Band
09/08/2023 10:13:03.280394	Descent	10,574	C-Band	LTE	auto. Unstable link



5.1.14 Link Switchovers – Flight 1-of-4

Result = PARTIAL: This flight test demonstrated an integrated C2 system in an operational environment using multiple networks to provide seamless service in all flight phases. Some procedures in this test sequence passed while others failed.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
3	Scenario 3 – Link Switchovers (TP_C2_004: C2 Switchovers)	10	07 Sept 2023	5:18 CDT	5:31 CDT

General Test Observations: During this test flight, there were two automatic switchovers, at 5:23 and at 5:24, the system switched from C-Band to LTE automatically because the C2 system detected the C-Band link was down due to a weak signal.

Four out of the 10 manually commanded link switchovers exceeded the TET limit.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	5:19 Secure Start session on LTE. all green. good. CS Status Y/2 then UA Y/2 good both. 5:19 start data stream CS then UA.
TP_CM_004A	User Data exchanges < MTU	**PASS**	5:20 send n=1, recd id=4 5:21 set TET=3 UA Status Y/2 then CS. 5:21 Cleared for takeoff. 5:22 ARMING TAKEOFF Switch 1.
TP_C2_004 (on ground)	C2 Switchovers	**FAIL**	UA Status: Y/1 CS: Y/1. UA Switch 3 good. 5:22 UA Status: Y/3, CS: Y/3 - good. CS Status 123: all links up. nominal. 5:23 UA status 123. all up nominal.
TP_C2_004 (departure)	C2 Switchovers	**PASS**	
TP_C2_004 (cruise)	C2 Switchovers	**FAIL**	5:23 UA status 123. all up nominal. 100 ft. cruising. set TET-=5 Switch 3. from LTE. UA Y/3 5:24 CS: Y/3 auto switchover to LTE. Switch 3. 5:25 Switch 1.... waiting. exceeded notification observed. GUI shows secure on 3. Now GUI shows satcom. Status CS Y/1. Switch 2. good. 5:26 Status: UA Y/2 then CS: Y/2 CS Status 123. all up, nominal. 5:27 UA status 123. all up, nominal. UA Set TET =3 5:27 Return to land. UA switch 3... slooow to switch.... still on LTE. GOOD. 5:28 gui on 3.
TP_C2_004 (arrival)	C2 Switchovers	**FAIL**	LANDED. UA Status Y/3, CS: Y/3. UA switch 1. UA status Y/1, CS: Y/1 UA switch 2. good.

Procedure	Description	Result	Notes
TP_CM_011	Control / User Plane Termination	**PASS**	5:29 Status Y/2, CS: Y/2 Switch 1 good. UA status: Y/1, CS, Y/1 good. 5:30 status: CS: Y/1, UA: Y/1. good. stopping data streams. UA, then CS. SECURE STOP. Status: N/1, N/1 good. 5:31 Send n=1 not recd

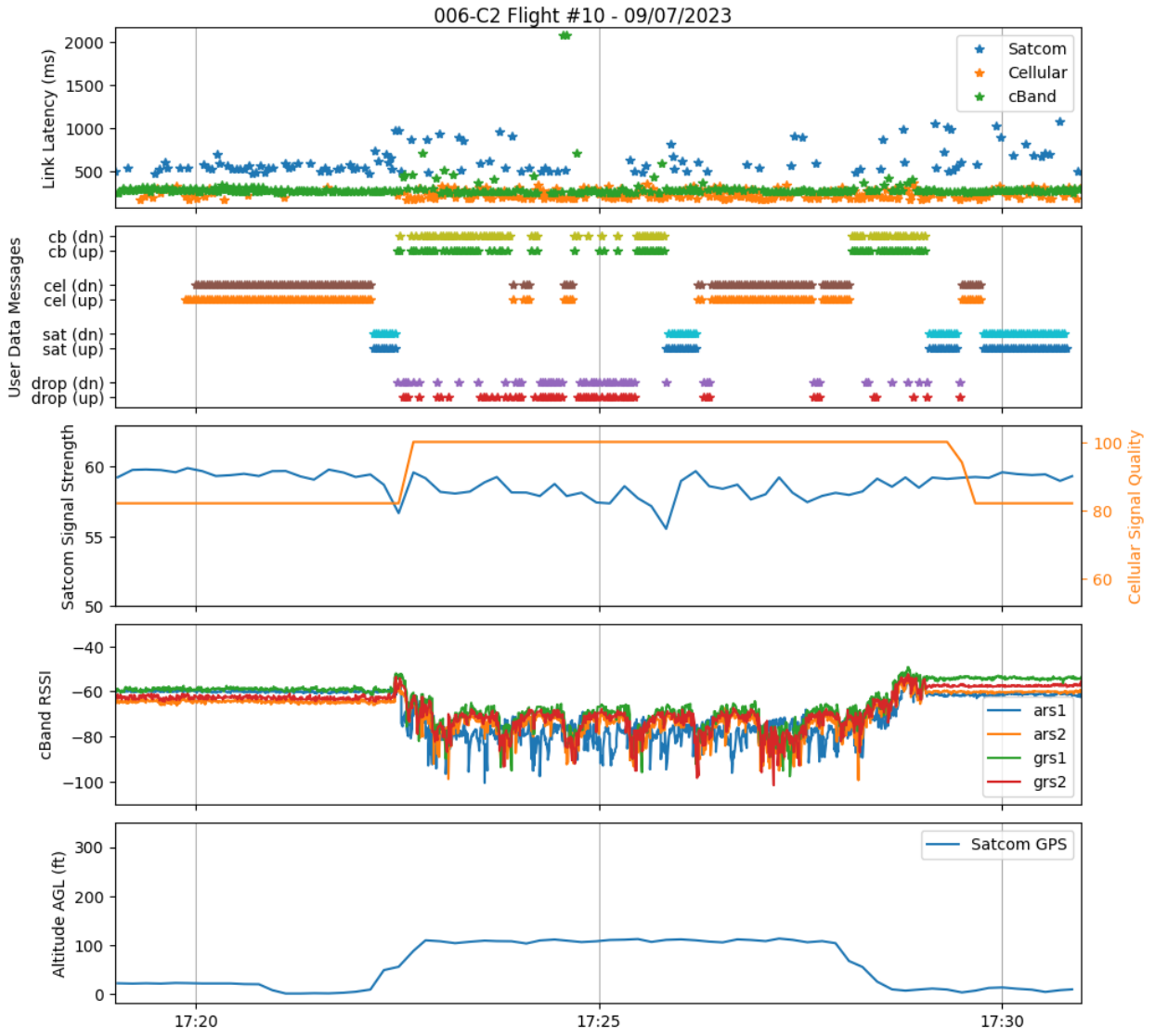
Detailed Results:

Table 5-15. Manually Commanded Switchovers for C2 Flight #10

Time (CDT)	From	To	Flight Phase	Switchover time (ms)	TET	<TET
17:22	LTE	satcom	takeoff	2,594	5,000	Y
17:22	satcom	C-Band	departure	10,905	5,000	N
17:24	LTE	C-Band	cruise	1,666	5,000	Y
17:25	LTE	C-Band	cruise	19,871	5,000	N
17:25	C-Band	satcom	cruise	2,230	5,000	Y
17:26	satcom	LTE	cruise	10,766	5,000	N
17:27	LTE	C-Band	arrival	7,723	3,000	N
17:29	C-Band	satcom	post-landing	2,184	3,000	Y
17:29	satcom	LTE	post-landing	1,435	3,000	Y
17:29	LTE	satcom	post-landing	2,970	3,000	Y

Table 5-16. Lost Link Events for C2 Flight #10

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/07/2023 17:23:53.516232	Cruise	10,560	C-Band	LTE	auto. Unstable link
09/07/2023 17:24:32.533736	Cruise	1,464	C-Band	LTE	auto. Unstable link



5.1.15 Link Switchovers – Flight 2-of-4

Result = PARTIAL: This flight test demonstrated an integrated C2 system in an operational environment using multiple networks to provide seamless service in all flight phases. Some procedures in this test sequence passed while others failed.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
3	Scenario 3 – Link Switchovers (TP_C2_004: C2 Switchovers)	11	07 Sept 2023	5:39 CDT	5:50 CDT

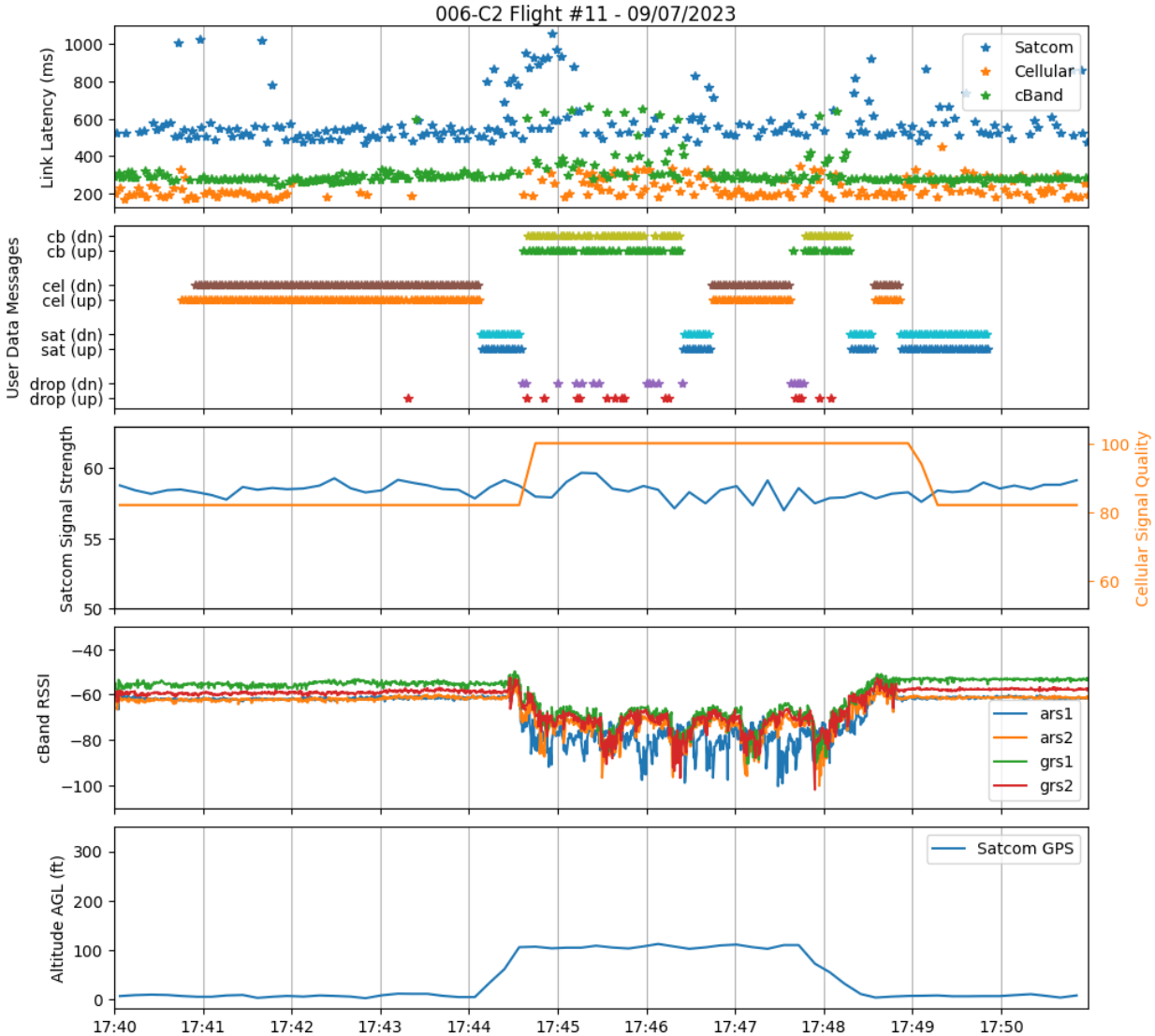
General Test Observations: One out of the 7 manually commanded link switchovers exceeded the TET limit.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	5:39 Status: N/2 both good. 5:39 ua send n=1, not recd good. 5:39 cs status 123: all up nominal. ua status 123: all up nominal. 5:40 Ua secure start. LTE good. status: Y/2 both good. start data streams. 5:41 ua send n=1, recd id=4 set tet=3 5:42 status: Y/2. both good. 5:42 cleared for takeoff.
TP_C2_004 (on ground)	C2 Switchovers	**PASS**	
TP_C2_004 (departure)	C2 Switchovers	**PASS**	5:44 ARMING / TAKEOFF switch 1. good. all up. UA status: Y/1 both good. Switch 3 - good. UA Y/3, CS: Status :Y/3 CS: Status 123: all up, nominal. flight RSSI: -70. 5:45 UA status 123 all up nominal. 5:45 UA status 123 all up nominal. 100 ft cruising. set tet=5 still on C-Band. 5:46 status: Y/3 switch 1 from C-Band to satcom. UA Y/1, CS: Y/1 Switch 2. satcom to LTE good. UA Y/2, CS: Y/2 5:46 CS status 123. all up, nominal UA status 123, all up nominal UA set tet=3. RETURN to land. Switch 3... exceeded TET. 5:48 UA Y/3, CS: Y/3 ua Switch 1. from C-Band. good. ua Y/1. cs: Y/1 LANDED!! ON GROUND END OF FLIGHT 11. Switch 2. CS: Y/2, Switch 1. ua: Y/1. 5:49 cs: Y/1. CS: Y/1, UA: Y/1. ua stop data streams. 5:50 ua secure stop. ua N/1, cs: N/1 5:50 ua send n=1. not recd.
TP_C2_004 (cruise)	C2 Switchovers	**PASS**	
TP_C2_004 (arrival)	C2 Switchovers	**FAIL**	
TP_CM_011	Control / User Plane Termination	**PASS**	

Detailed Results:

Table 5-17. Lost Link Events for C2 Flight #11

Time (CDT)	From	To	Flight Phase	Switchover time (ms)	TET	<TET
17:44	satcom	C-Band	departure	1,658	5,000	Y
17:46	C-Band	satcom	cruise	2,087	5,000	Y
17:46	satcom	LTE	cruise	1,489	5,000	Y
17:47	LTE	C-Band	arrival	10,738	3,000	N
17:48	C-Band	satcom	post-landing	2,169	5,000	Y
17:48	satcom	LTE	post-landing	1,442	5,000	Y
17:48	LTE	satcom	post-landing	2,213	5,000	Y



5.1.16 Link Switchovers – Flight 3-of-4

Result = PASS: This flight test demonstrated an integrated C2 system in an operational environment using multiple networks to provide seamless service in all flight phases.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
3	Scenario 3 – Link Switchovers (TP_C2_004: C2 Switchovers)	12	07 Sept 2023	5:56 CDT	6:10 CDT

General Test Observations: All 9 manually commanded link switchovers executed successfully within the TET limit during this test flight.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	5:56 restarted DTSR. Status: N/2 send n=1 5:56 CS Status 123: all up nominal good. 5:57 UA status 123: all up nominal good. ua Secure start. good on LTE. cs: Y/2 ua: Y/2 start continuous data stream. 5:58 ua send n=1, recd id=4. set tet =3 5:59 ua Y/2. CS Y/2
TP_CM_004A	User Data exchanges < MTU	**PASS**	5:58 ua send n=1, recd id=4. cleared for takeoff.
TP_C2_004 (on ground)	C2 Switchovers	**PASS**	6:00 RSSI -60 on ground. with attenuators. 6:01 ARMING ... cancel/abort. 6:03 rebooting drone control.. 6:04 ARMING / SPINNING / TAKEOFF switch 1 ua: Y/1 100 ft. cs: Y/1 Switch 3 from satcom to C-Band good ua: Y/3, cs: Y/3 6:05 cs status 123 all up nominal good then UA same good
TP_C2_004 (departure)	C2 Switchovers	**PASS**	

Procedure	Description	Result	Notes
TP_C2_004 (cruise)	C2 Switchovers	PASS	6:06 cruising at 100. set tet = 5 auto switch over to 2 switch back to 3. ua: Y/3 cs Y/3 6:07 switch 1 from C-Band. ua Y/1 cs Y/1 good. ua switch 2 from satcom to lte. ua Y/2 cs: Y/2 good cs status 123 all up nominal. session on LTE 6:08 ua status 123 all up nominal return to land. set tet = 5 Switch 3. ua Y/3 both good. switch 1. ua Y/1 cs Y/1 switch 2. ua Y/2, cs: Y/2 switch 1. 6:09 ua Y/1 cs Y/1 LANDED / ON GROUND / cs Y/1 ua Y/1 good stop continuous data stream. ua secure Stop. 6:10 CS N/1 ua N/1 ua send n=1, not recd.
TP_C2_004 (arrival)	C2 Switchovers	PASS	
TP_CM_011	Control / User Plane Termination	PASS	

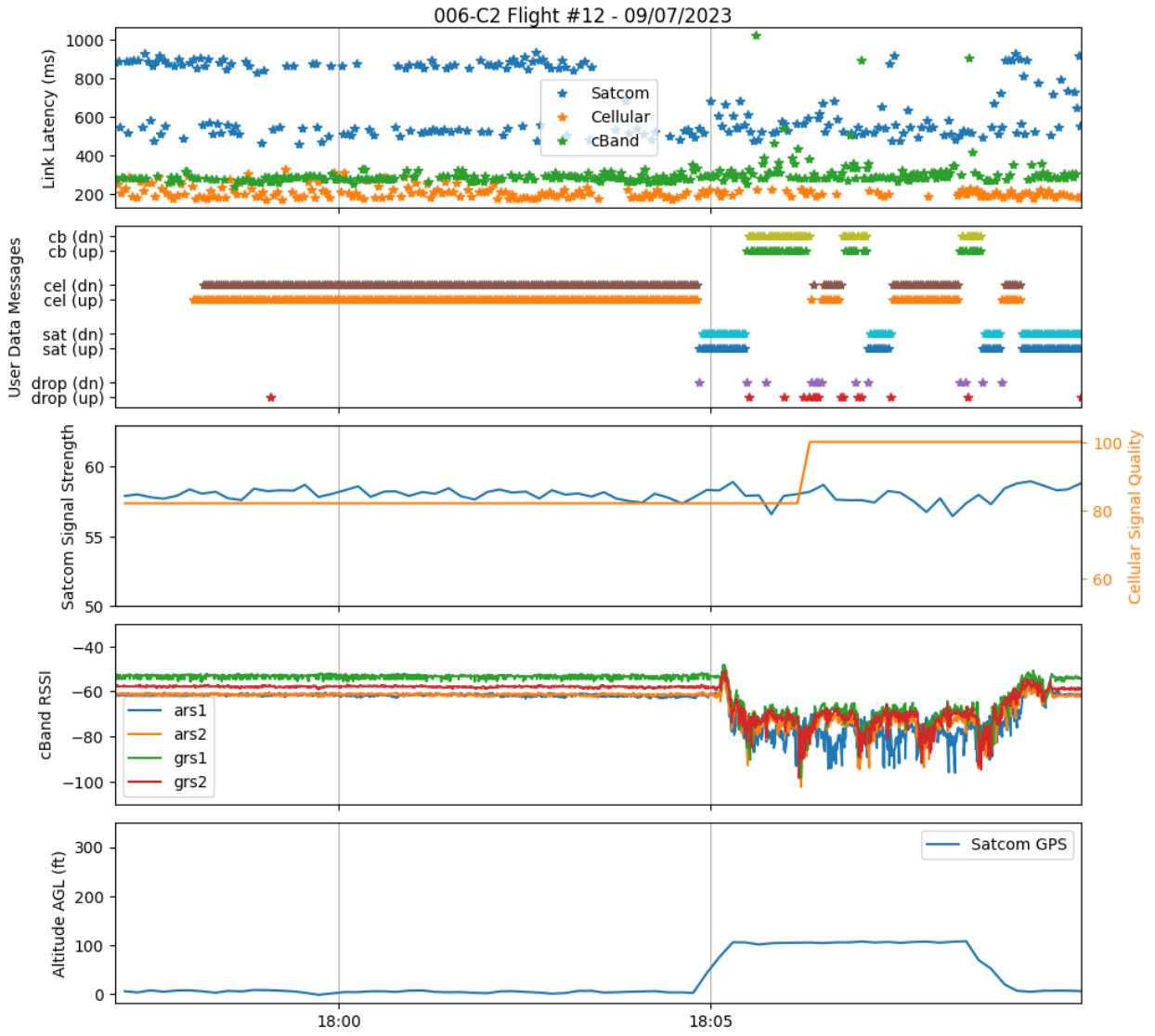
Detailed Results:

Table 5-18. Manually Commanded Switchovers for C2 Flight #12

Time (CDT)	From	To	Flight Phase	Switchover time (ms)	TET	<TET
18:04	LTE	satcom	takeoff	2,768	5,000	Y
18:04	satcom	C-Band	cruise	1,601	5,000	Y
18:06	LTE	C-Band	cruise	1,734	5,000	Y
18:07	C-Band	satcom	cruise	2,775	5,000	Y
18:07	satcom	LTE	cruise	1,447	5,000	Y
18:08	LTE	C-Band	descent	1,614	5,000	Y
18:08	C-Band	satcom	descent	2,849	5,000	Y
18:08	satcom	LTE	descent	1,446	5,000	Y
18:08	LTE	satcom	landing	2,062	5,000	Y

Table 5-19. Lost Link Events for C2 Flight #12

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/07/2023 18:06:19.468422	Cruise	10,564	C-Band	LTE	auto. Unstable link



5.1.17 Link Switchovers – Flight 4-of-4

Result = PARTIAL: This flight test demonstrated an integrated C2 system in an operational environment using multiple networks to provide seamless service in all flight phases. Some procedures in this test sequence passed while others failed.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
3	Scenario 3 – Link Switchovers (TP_C2_004: C2 Switchovers)	13	07 Sept 2023	6:12 CDT	6:21 CDT

General Test Observations: Four out of the 8 manually commanded link switchovers exceeded the TET limit.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	6:12 starting flight 13 cs N/2 ua N/2 ua send n=1, not recd. all links green. cs status 123. all links up nominal good. 6:13 ua status 123. all links up nominal good. 6:13 secure start. gui shows session on LTE. cs Y/2 ua: Y/2 both good.
TP_CM_004A	User Data exchanges < MTU	**PASS**	6:14 start continuous data stream. ua send n=1, recd id=10. set tet = 3
TP_C2_004 (on ground)	C2 Switchovers	**PASS**	
TP_C2_004 (departure)	C2 Switchovers	**PASS**	6:15 ua: Y/2 cs: Y/2 6:16 ARMING / SPINNING / TAKEOFF switch 1ua Y/1. 50 ft. cs: Y/1 switch 3 from satcom. to C-Band. 100 ft. ua Y/3. cs: Y/3 cs status 123 all up nominal good. 6:17 ua status 123 all up nominal good. cruising at 100 ft. set tet =5.
TP_C2_004 (cruise)	C2 Switchovers	**FAIL**	6:17 switch 3.ua Y/3 cs: Y/3 Switch 1 from C-Band good. ua Y/1 cs: Y/1 6:18 switch 2 good. exceeded TET ua: Y/2 cs: Y/2 cs 123 all up nominal good. ua 123 all up nominal good. set TET =3
TP_C2_004 (arrival)	C2 Switchovers	**FAIL**	6:19 return to land command switch 3. good. ua Y/3 cs: Y/3 switch 1. good. ua: Y/1 cs: Y/1 switch 2 TET exceeded ua: Y/2 cs: Y/2 6:20 switch 1 good LANDED / ON GROUND ua cs Y/1 *** NOTICED Satcom went down briefly, and exceeded TET??
TP_CM_011	Control / User Plane Termination	**PASS**	6:21 secure stop. cs: N/1, ua N/1 send n=1 not recd good.

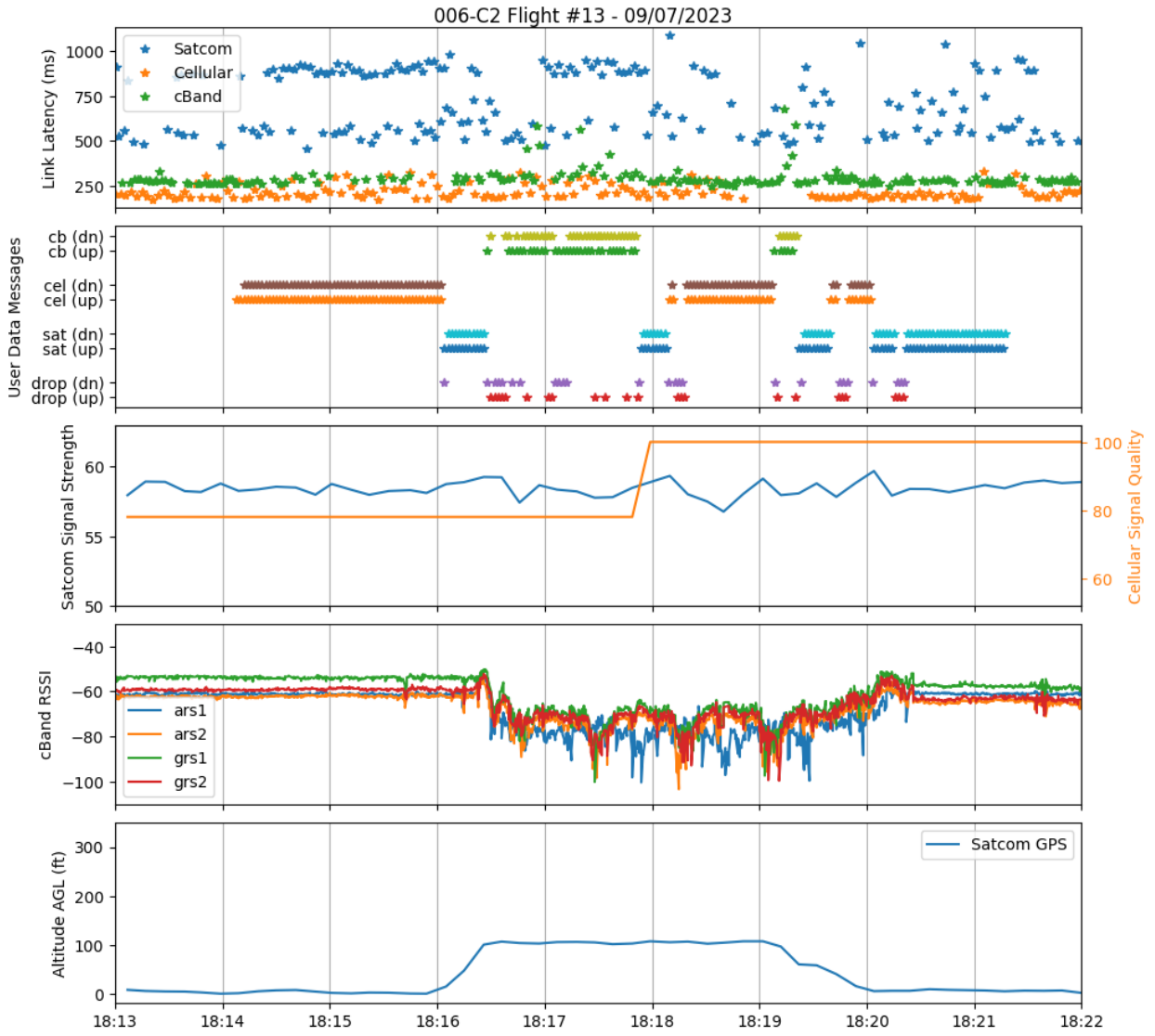
Detailed Results:

Table 5-20. Manually Commanded Switchovers for C2 Flight #13

Time (CDT)	From	To	Flight Phase	Switchover time (ms)	TET	<TET
18:16	LTE	satcom	takeoff	3,178	3,000	Y
18:16	satcom	C-Band	departure	10,951	3,000	N
18:17	C-Band	satcom	cruise	2,156	5,000	Y
18:18	satcom	LTE	cruise	10,589	5,000	N
18:19	LTE	C-Band	arrival	1,663	3,000	Y
18:19	C-Band	satcom	arrival	2,888	3,000	Y
18:19	satcom	LTE	arrival	10,588	3,000	N
18:20	LTE	satcom	landing	3,013	3,000	N

Table 5-21. Lost Link Events for C2 Flight #13

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
09/07/2023 18:20:15.627597	surface	8,096	Satcom	Satcom	auto. Unstable link



5.1.18 Itasca Grid – Flight 1-of-2

Result = PASS: This flight test demonstrated APN using the VAN system during Scenario 4. Navigation error was within expected bounds across all flight conditions. GPS was disabled for 90 minutes. The VAN mitigation procedure was tested during this flight.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
5	Scenario 4 – Itasca Grid (APN using VAN)	1	19 Sept 2023	8:40 CDT	10:55 CDT

General Test Observations: During checkout and integration flights, it was determined that the calibration maneuver specified in the procedure and test card was not required. Since the C2 system was not present on the Cessna, the system status was monitored by an operator using a laptop, who also sent commands through the defined C2 interface.

Procedure	Description	Result	Notes
TP_VN_001	VAN Startup Procedure	**PASS**	8:40 – VAN Power ON 8:47 – VAN Nav Engaged 9:02 – Cessna Engine ON 9:07 – Takeoff 9:10 – Camera Enabled
TP_VN_002	VAN System Flight Procedure	**PASS**	9:20 – GPS Disabled 9:37 – VAN Mitigation 9:39 – GPS Disabled 9:41 – VAN Mitigation 9:42 – GPS Disabled
TP_VN_004	VAN Landing procedure	**PASS**	10:54 – GPS Enabled 10:54 – Camera Disabled 10:55 – Landing
TP_VN_005	VAN System Post-Flight Procedure	**PASS**	10:55 – Stop VAN Software

Detailed Results:

The flight path for the first Scenario 4 flight is show in Figure 5-1. The trapezoids represent the view of the IR camera on the ground. Each shape is color coded to represent the type of image measurement that was processed. Red indicates no valid measurements, green indicates a valid translation (notionally North & East) measurement, and blue indicates both translation and rotation (notionally heading) and scale (notionally altitude).

Figure 5-1. Itasca Flight 1 Path

After departure from Mayville, the Cessna 182 proceeded to the grid location at 3000 ft AGL. GPS was disabled shortly before crossing into Minnesota. Prior to entering the grid, the VAN mitigation procedure was tested to ensure that the system could reacquire GPS as needed. The Cessna descended to 1000 ft AGL prior to entering the grid and stayed at that altitude through the grid. After grid completion, the Cessna returned to 3000 ft AGL and returned to Mayville. Just prior to landing, GPS was re-enabled.

The navigation errors during the simulated GPS outage are shown in Figure 5-2. The actual computed error (as compared to the truth INS/GPS solution) is the blue trace. The red and orange lines show the navigation filter's estimate of the 50% and 90% error bounds. CEP50 is computed as a factor multiplied by the standard error, where x is the measured value, $\bar{x}$ is the most likely expected value (computed from truth), and n is the number of points used.

$$CEP50 = 0.5887\sqrt{\frac{\sum(x-\bar{x})^2}{n-1}}$$

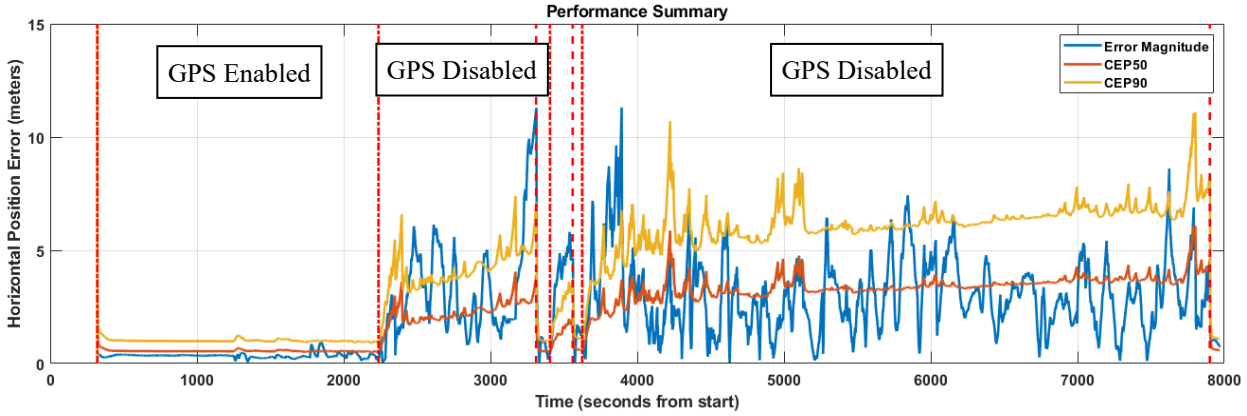


Figure 5-2. Itasca Flight 1 Performance

For the GPS disabled sections for this flight, CEP50 was 2.8 meters. This means that the horizontal position error was less than 2.8 meters for half of the flight. As shown in Figure 5-2, the peak horizontal error was 12 meters. SEP represents the full three-dimensional position error. The SEP50 for this flight was 6.1 meters.

These results are within the expected error for the Honeywell VAN as compared to previous testing.

5.1.19 Itasca Grid – Flight 2-of-2

Result = PASS: This flight test demonstrated APN using the VAN system during Scenario 4. Navigation error was within expected bounds across all flight conditions. GPS was denied for 90 minutes.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
5	Scenario 4 – Itasca Grid (APN using VAN)	VAN-2	19 Sept 2023	13:24 CDT	15:31 CDT

General Test Observations: During checkout and integration flights, it was determined that the calibration maneuver specified in the procedure and test card was not required. Since the C2 system was not present on the Cessna, the system status was monitored by an operator using a laptop, who also sent commands through the defined C2 interface.

Procedure	Description	Result	Notes
TP_VN_001	VAN Startup Procedure	PASS	13:24 – VAN Power ON 13:30 – VAN Nav Engaged 13:38 – Cessna Engine ON 13:44 – Takeoff
TP_VN_002	VAN System Flight Procedure	PASS	13:46 – Camera Enabled 13:52 – GPS Disabled 15:30 – GPS Enabled
TP_VN_004	VAN Landing procedure	PASS	15:30 – Camera Disabled 15:31 – Landing

Procedure	Description	Result	Notes
TP_VN_005	VAN System Post-Flight Procedure	PASS	15:31 – Stop VAN Software

Detailed Results:

The flight path for the first Scenario 4 flight is show in Figure 5-3.

Figure 5-3. Itasca Flight 2 Path

After departure from Mayville, the Cessna 182 proceeded to the grid location at 3000 ft AGL. GPS was disabled shortly after crossing I-29. The Cessna descended to 1000 ft AGL prior to entering the grid and stayed at that altitude through the grid. After grid completion, the Cessna returned to 3000 ft AGL and returned to Mayville. Just prior to landing, GPS was re-enabled.

The navigation errors during the simulated GPS outage are shown in Figure 5-4.

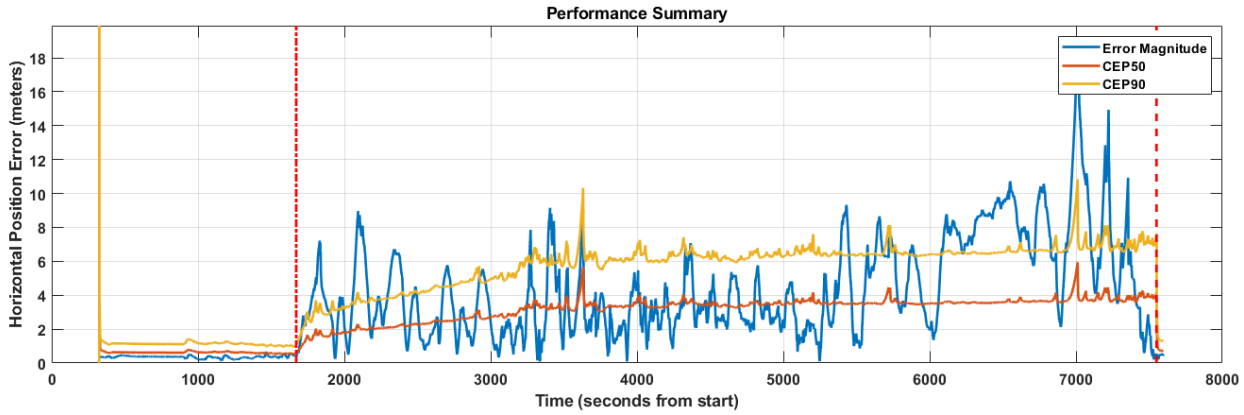


Figure 5-4. Itasca Flight 2 Performance

For the GPS disabled sections for this flight, CEP50 was 4.3 meters. As shown in Figure 5-4, the peak horizontal error was 18 meters. The SEP50 for this flight was 7.9 meters. A sustained ~6 meter error was introduced into the system after the completion of the grid and during the ascent back to 3000 ft AGL.

However, the results were still within the expected error bound as compared to previous Honeywell VAN flight tests.

5.2 GROUND TEST RESULTS

This section documents the results of ground-based test performed in accordance with detailed test procedures specified in [DTP]. Each ground-based test identifies the associated test card (if applicable) and test scenario, the test date, and the test start/end times. General test observations (e.g., issues or unexpected conditions encountered during the ground-based test) are documented. The test results, which are presented in a tabular form, identity the individual test procedures specified, report the result of each test procedure, and provide notes, as necessary, to describe conditions observed during the execution of the specific test procedure and/or to explain a result other than pass.

5.2.1 Ground-based Tests – 1-of-2

Result = PARTIAL: This ground test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under non-nominal conditions with encryption disabled. This test also demonstrated the ability to control access to the UA and to the CS; however, user data messages were transmitted even though a secure user plane connection was not supposed to exist.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
4	Scenario 4 – Ground-based Tests	18	08 Sept 2023	10:27 CDT	11:03 CDT

General Test Observations: The session was successfully established without encryption, and user data messages were successfully exchanged.

Procedure	Description	Result	Notes
TP_CM_001	Control Plane and User Plane Traffic Mutual Authentication with User Plane Traffic Access Control Allowed	PASS	10:24 reconfiguring for "Null Encryption"... 10:27 ready with null encryption STARTING GROUND cs N/2, ua N/2 ua send n=1, not recd good. cs status 123 all up nominal good. ua status 123 all up nominal good. 10:28 secure start - up on LTE good. cs Y/2, ua Y/2 10:29 start continouous data streams
TP_CM_008	Control Message Exchanges without Encryption	PASS	
TP_CM_005A	User Data Exchanges without Encryption, Payload Data <MTU	PASS	10:30 TP-CM-005-a (less than MTU) send N=1, recd ID=10 good.

Procedure	Description	Result	Notes
TP_CM_005B	User Data Exchanges without Encryption, Payload Data >MTU	**PASS**	10:31 TP-CM-005-b (greater than MTU.) we will use SCP to copy a file File is 2626 bytes. 10:36 SCP command issued. 10:37 copying TXT file to validation logs. copied from 10.100.0.1 and TCP port=22 seen on user sniffer.
TP_CM_009	Link Switchover < TET	**PASS**	10:44 starting: TP-CM-009 switchover less than TET cs status 123 - all links up nominal good 10:45 UA status 123 - all links up nominal good. switch 1. from lte to satcom. veryfing timestamps.. switch 2.857 sec on UA . swichover tool: 2.239 sec on CS 10:46 ua: Y/1, cs: Y/1 good. did not exeeded TET. 10:47 dtsr live log on UA. verified network layer switchover verification. 10:48 dtsr live log on CS. verified connection request/confirm mesages. 10:49 cs status: Y/1, ua: Y/1. good. 10:50 stop data streams.
TP_CM_011	Control Plane and User Plane Link Termination	**FAIL**	ua Secure stop. FAILED. (did not stop the secure session) had to issue secure stop on CS ISSUE/ERROR!! cs status: N/1, ua: N/1 10:51 send n=1 not recd, good.

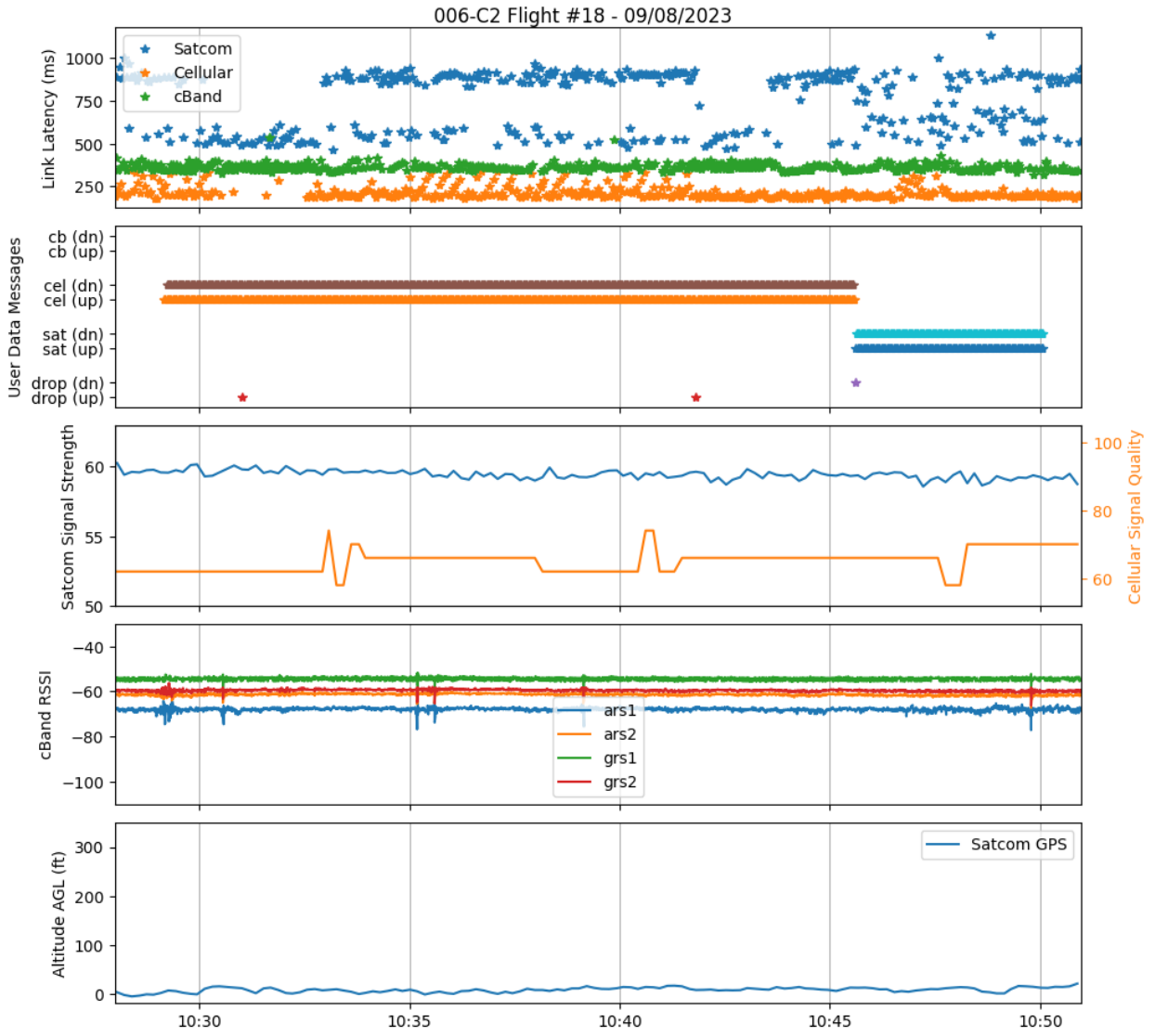
Procedure	Description	Result	Notes
TP_CM_002	User Plane Traffic Mutual Authentication with UA Access to the CS Denied	**FAIL**	10:54 ****** RECONFIGURING TO ACCESS DENIED PEER. Ua access will be denied by CS. cs: N/2, ua N/2. send n=1 not recd good. 10:55 cs status 123 all links up, nominal. then UA, nominal both good. ua secure start... session not established because access is denied, as expected. good! cs status secure: N/2. ua status secure: N/2 - good. ua send n=1. not recd, as expected!!! good!!! 10:58 cs: send n=1. not recd. as expected good!!! 10:59 END OF TP-CM-002. -- NOTE: Step 16 fails. CS_DTSR log shows the n=1 message is sent at 10:58:23. with ID 0002. The CS should not have sent this message because a secure connection was not supposed to exist. CS Main sniffer shows message is sent at 10:58:23.866 (fail). The UA DSTR log shows there is nothing received at this time which is good.

Procedure	Description	Result	Notes
TP_CM_003	User Plane Traffic Mutual Authentication with CS Access to the UA Denied	**FAIL**	11:00 ********* RECONFIGURING to ACCESS DENIED PEER CS will deny access by UA. restarted DTSR's only. TP-CM-003 CS access to the ua denied. 11:01 cs N/2, ua N/2 ua send n=1, not recd. good. cs status 123 all links up. nominal. good. ua status 123 all links up. nominal. good. 11:02 ua secure start.... did not establish because it was denied as expected. good!!! 11:03 cs status secure: N/2, ua N/2 good! 11:03 ua send n=1, not recd, as expected good! 11:03 cs send n=1, not recd, as expected good! -- NOTE: CS Main sniffer shows message is sent at 11:03:53.949 (fail).

Detailed Results:

TP_CM_002 and TP_CM_003 Fail because the user data message is still sent by the CS even though the secure session is not established. Although the messages are sent, the receiver is unable to decrypt the message, as the receiving DTSR's cannot decrypt the user data. This is why at the user console when executing the test, it appeared to have passed because the receiving DTSR is unable to read the encrypted message.

TP_CM_011 failed because the UA did not end the secure session when the command was issued at 10:50. The secure session had to be manually terminated at the CS.



5.2.2 Ground-based Tests – 2-of-2

Result = PARTIAL: This ground test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under non-nominal conditions with encryption disabled. This test also demonstrated the ability to control access to the UA and to the CS; however, user data messages were transmitted even though a secure user plane connection was not supposed to exist.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
4	Scenario 4 – Ground-based Tests	19	08 Sept 2023	11:04 CDT	11:24 CDT

General Test Observations: The session was successfully established without encryption, and user data messages were successfully exchanged.

Procedure	Description	Result	Notes
TP_CM_001	Control Plane and User Plane Traffic Mutual Authentication with User Plane Traffic Access Control Allowed	**PASS**	11:04 configured for NULL encryption. 11:05 cs: N/2, ua N/2 11:06 cs status 123 all up nominal. good. then ua. all up nominal. ua secure start... up session on LTE good as expected. 11:07 cs Y/2, ua Y/2. good. cs start user data stream, then ua. good.
TP_CM_008	Control Message Exchanges without Encryption	**PASS**	
TP_CM_005A	User Data Exchanges without Encryption, Payload Data <MTU	**PASS**	11:08 TP-CM-005-a 11:08 ua send n=1, recd id=24. good.
TP_CM_005B	User Data Exchanges without Encryption, Payload Data >MTU	**PASS**	11:08 sending file larger than MTU. from CS command: scp UA->CS via SCP... 11:10 "TP-CM-005B-2.txt"
TP_CM_009	Link Switchover < TET	**PASS**	11:12 cs status 123 all up nominal, good. then UA. both good all up nominal good. 11:13 ua SWITCH 1 from LTE to Satcom. good. ua 2.118 sec, cs: 1.458 sec switchover times. 11:14 ua Y/1. no tet messages good, then CS . all good. good. 11:14 messages verified on dtsr live log. good.
TP_CM_011	Control Plane and User Plane Link Termination	**PASS**	11:15 TP-CM-011 11:16 cs status Y/1, ua: Y/1. 11:16 stopping user data streams. ua secure stop. good. cs N/1, ua N/1 11:17 ua send n=1, not recd, good.

Procedure	Description	Result	Notes
TP_CM_002	User Plane Traffic Mutual Authentication with UA Access to the CS Denied	**FAIL**	11:18 ***** reconfigure to UA ACCESS DENIED TP-CM-002 cs N/2, ua: N/2 11:19 ua send n=1. not recd good. cs status 123 all up nominal LTE is going up/down. 11:20 secure START... denied as expected. cs status: N/2, ua N/2 ua send n=1... not recd. good. 11:21 cs. send n=1 not recd. good. -- NOTE: Step 16 and 17 fail. The CS DTSR log shows the CS sent n=1 with ID 06 at 11:21:30.436 even though a secure connection should not have existed. The CS Main sniffer shows the message was sent (Fail). The UA Main Sniffer shows the n=1 message was received.
TP_CM_003	User Plane Traffic Mutual Authentication with CS Access to the UA Denied	**FAIL**	11:21 ***** RECONFIGURING TO CS ACCESS DENIED (Ua is denying peer) 11:22 restarted DTSRs. 11:22 TP-CM-003 cs N/2, ua N/2 good. ua send n=1 not recd good. 11:23 cs status 123 all links up nominal good. ua all links up nominal good. 11:23 ua secure START (not established as expected bc denied) good! cs status: N/2, ua: N/2 good 11:24 cs send n=1 not recd. good. ua send n=1 not recd. good. 11:25 DONE!!!!!!!!!! -- NOTE: Step 16 and 17 fail. The CS Main sniffer shows the message was sent at 11:24:21.545 CDT even though a secure connection should not have existed. (Fail). The UA Main Sniffer shows the n=1 message was received.

Detailed Results:

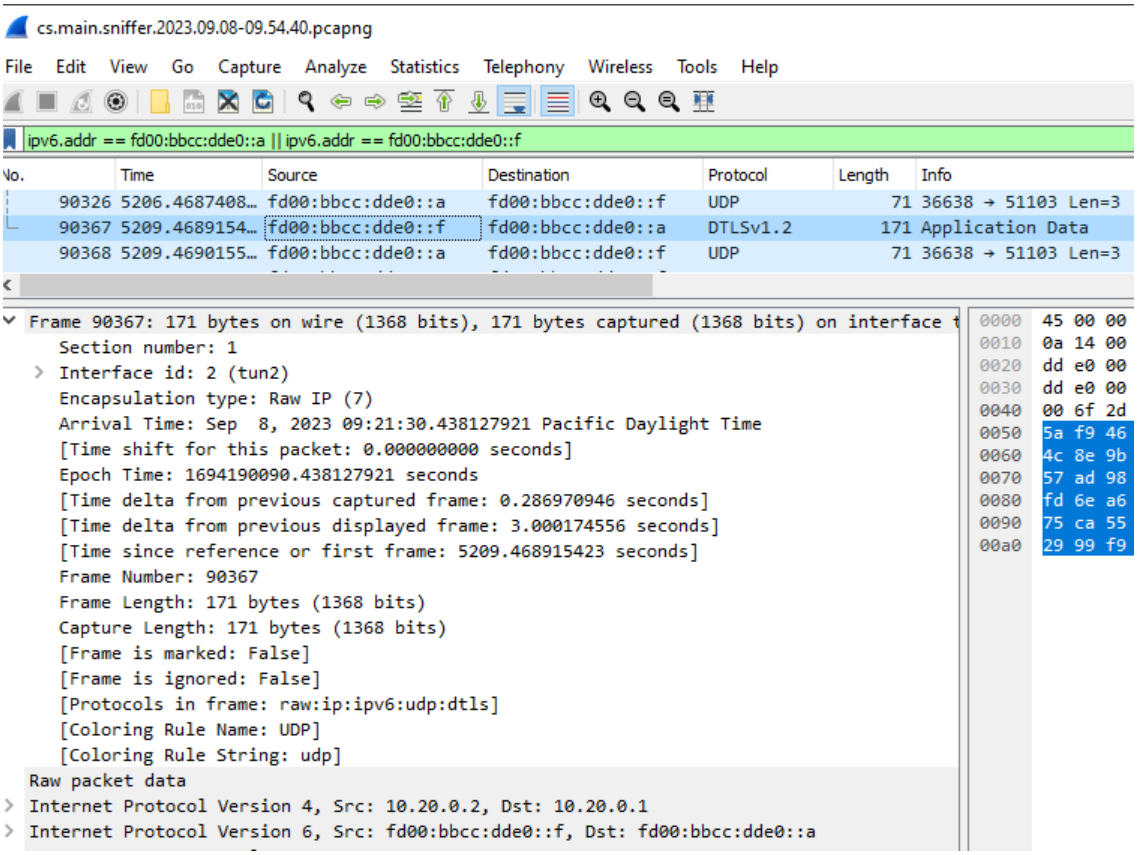
TP_CM_002 and TP_CM_003 Fail because the user data message is still sent by the CS even though the secure session is not established. Although the messages are sent, the receiver is unable to decrypt the message, as the receiving DTSR's cannot decrypt the user data. This is why at the user console when executing the test, it appeared to have passed because the receiving DTSR is unable to read the encrypted message.

Step 16 Fails.

CS DTSR log shows UDMD message with ID 006 was sent.

```
2023-09-08 16:21:30.436621 GMT INFO     UdmdIn.cpp:51
Received: ID: 00000006 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE Data:
UD-AAAAAAAAAAAAAAAAAAA-000006
Sending user data message to peer
User Output: Sent 66 bytes.
```

CS Main sniffer shows n=1 message is sent to the UA.



Step 17 fails.

UA Main Sniffer shows n=1 message is received, but it is not processed in the UA DTSR log.

ua.main.sniffer.2023.09.08-09.50.59.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.	Time	Source	Destination	Protocol	Length	Info
110082	5427.5451434…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	36638 → 51103 Len=
110085	5427.9566897…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	171	Application Data
110147	5430.5456122…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	36638 → 51103 Len=
110208	5433.5460802…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	36638 → 51103 Len=

```
Frame 110085: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface
    Section number: 1
  > Interface id: 1 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Sep  8, 2023 09:21:31.335316994 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1694190091.335316994 seconds
    [Time delta from previous captured frame: 0.410899477 seconds]
    [Time delta from previous displayed frame: 0.411546300 seconds]
    [Time since reference or first frame: 5427.956689708 seconds]
    Frame Number: 110085
    Frame Length: 171 bytes (1368 bits)
    Capture Length: 171 bytes (1368 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:ipv6:udp:dtls]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dde0::a
v User Datagram Protocol, Src Port: 51102, Dst Port: 39536
    Source Port: 51102
    Destination Port: 39536
    Length: 111
    Checksum: 0x0bf9 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 157]
  > [Timestamps]
    UDP payload (103 bytes)
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 1
      Sequence Number: 1
      Length: 90
      Encrypted Application Data: f94669f4ed554e221d0b9741ed8c664c8e9b6953ee7b8bba6749201
```

```
0000  45 00 0
0010  0a 14 0
0020  dd e0 0
0030  dd e0 0
0040  00 6f 0
0050  5a f9 4
0060  4c 8e 9
0070  57 ad 9
0080  fd 6e a
0090  75 ca 5
00a0  29 99 f
```

5.3 LINK SWITCHOVER TIMING ANALYSIS

During each of the test flights, multiple link switchover commands were executed at various phases of flight, between each of the possible link combinations. In summary, for this 006-C2 project, a total of 65 link switchover commands were executed. Each switchover was measured at both the UA and the CS systems, even though the command always initiated from the UA. So the switchover time at the UA was always slightly longer than at the CS. Out of the 65 switchovers, 14 exceeded the TET (21%).

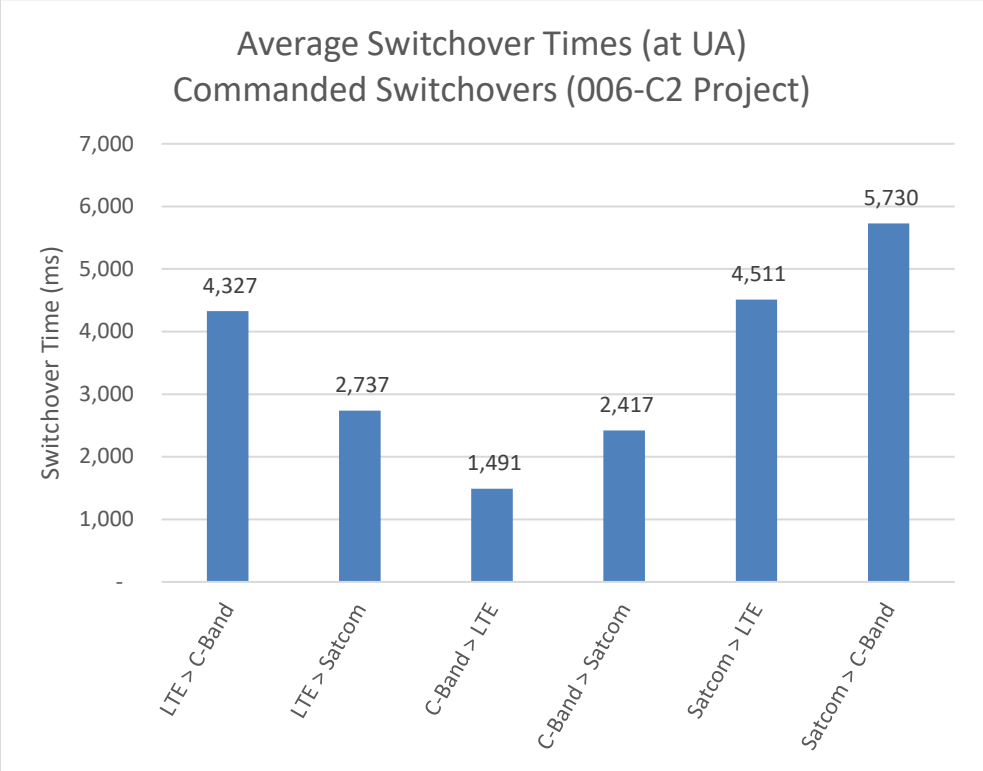


Figure 5-5. Average Switchover Times, measured at the UA

Table 5-22. Switchover Times for all commanded Link Switchovers

Flight No	System	Date	Time (CDT)	From	To	Flight Phase	Switchover time (ms)	TET	<TET
1	UA	6-Sep	10:27	LTE	C-Band	surface	2,049	3,000	Y
1	CS	6-Sep	10:27	LTE	C-Band	surface	1,150	3,000	Y
1	UA	6-Sep	10:28	C-Band	LTE	surface	1,568	3,000	Y
1	CS	6-Sep	10:28	C-Band	LTE	surface	360	3,000	Y
3	UA	6-Sep	12:41	satcom	LTE	cruise	1,396	5,000	Y
3	CS	6-Sep	12:41	satcom	LTE	cruise	486	5,000	Y
4	UA	6-Sep	14:51	LTE	C-Band	surface	1,630	3,000	Y
4	CS	6-Sep	14:51	LTE	C-Band	surface	1,164	3,000	Y
4	UA	6-Sep	14:52	C-Band	LTE	surface	1,413	3,000	Y
4	CS	6-Sep	14:52	C-Band	LTE	surface	672	3,000	Y
4	UA	6-Sep	15:03	LTE	satcom	cruise	3,276	5,000	Y
4	CS	6-Sep	15:03	LTE	satcom	cruise	2,632	5,000	Y
5	UA	6-Sep	15:37	LTE	C-Band	surface	1,594	3,000	Y
5	CS	6-Sep	15:37	LTE	C-Band	surface	1,183	3,000	Y
5	UA	6-Sep	15:45	LTE	C-Band	cruise	10,795	5,000	N
5	CS	6-Sep	15:45	LTE	C-Band	cruise	10,661	5,000	N
5	UA	6-Sep	15:48	LTE	C-Band	cruise	1,660	5,000	Y
5	CS	6-Sep	15:47	LTE	C-Band	cruise	1,262	5,000	Y
5	UA	6-Sep	15:50	LTE	C-Band	cruise	1,741	5,000	Y
5	CS	6-Sep	15:50	LTE	C-Band	cruise	1,296	5,000	Y
6	UA	6-Sep	16:21	LTE	satcom	surface	2,220	3,000	Y
6	CS	6-Sep	16:21	LTE	satcom	surface	1,562	3,000	Y
6	UA	6-Sep	16:29	LTE	satcom	cruise	2,834	5,000	Y
6	CS	6-Sep	16:29	LTE	satcom	cruise	2,200	5,000	Y
7	UA	6-Sep	17:07	LTE	satcom	surface	2,732	3,000	Y
7	CS	6-Sep	17:07	LTE	satcom	surface	2,066	3,000	Y
7	UA	6-Sep	17:14	LTE	satcom	cruise	2,986	5,000	Y
7	CS	6-Sep	17:14	LTE	satcom	cruise	2,341	5,000	Y
8	UA	7-Sep	16:20	LTE	C-Band	surface	1,798	3,000	Y
8	CS	7-Sep	16:20	LTE	C-Band	surface	1,333	3,000	Y
8	UA	7-Sep	16:23	LTE	C-Band	cruise	1,622	5,000	Y
8	CS	7-Sep	16:23	LTE	C-Band	cruise	1,262	5,000	Y
8	UA	7-Sep	16:26	satcom	C-Band	cruise	1,668	5,000	Y
8	CS	7-Sep	16:26	satcom	C-Band	cruise	71	5,000	Y
8	UA	7-Sep	16:27	LTE	C-Band	cruise	1,599	5,000	Y
8	CS	7-Sep	16:27	LTE	C-Band	cruise	1,252	5,000	Y
8	UA	7-Sep	16:31	satcom	C-Band	cruise	7,596	5,000	N
8	CS	7-Sep	16:31	satcom	C-Band	cruise	12,413	5,000	N
9	UA	7-Sep	16:56	LTE	C-Band	surface	1,951	3,000	Y
9	CS	7-Sep	16:56	LTE	C-Band	surface	1,570	3,000	Y
9	UA	7-Sep	17:03	LTE	C-Band	cruise	1,641	5,000	Y
9	CS	7-Sep	17:03	LTE	C-Band	cruise	1,281	5,000	Y

10	UA	7-Sep	17:22	LTE	satcom	takeoff	2,594	5,000	Y
10	CS	7-Sep	17:22	LTE	satcom	takeoff	1,952	5,000	Y
10	UA	7-Sep	17:22	satcom	C-Band	departure	10,905	5,000	N
10	CS	7-Sep	17:22	satcom	C-Band	departure	876	5,000	Y
10	UA	7-Sep	17:24	LTE	C-Band	cruise	1,666	5,000	Y
10	CS	7-Sep	17:24	LTE	C-Band	cruise	1,273	5,000	Y
10	UA	7-Sep	17:25	LTE	C-Band	cruise	19,871	5,000	N
10	CS	7-Sep	17:25	LTE	C-Band	cruise	1,284	5,000	Y
10	UA	7-Sep	17:25	C-Band	satcom	cruise	2,230	5,000	Y
10	CS	7-Sep	17:25	C-Band	satcom	cruise	1,118	5,000	Y
10	UA	7-Sep	17:26	satcom	LTE	cruise	10,766	5,000	N
10	CS	7-Sep	17:26	satcom	LTE	cruise	8,938	5,000	N
10	UA	7-Sep	17:27	LTE	C-Band	arrival	7,723	3,000	N
10	CS	7-Sep	17:27	LTE	C-Band	arrival	1,245	5,000	Y
10	UA	7-Sep	17:29	C-Band	satcom	post-landing	2,184	3,000	Y
10	CS	7-Sep	17:29	C-Band	satcom	post-landing	1,278	3,000	Y
10	UA	7-Sep	17:29	satcom	LTE	post-landing	1,435	3,000	Y
10	CS	7-Sep	17:29	satcom	LTE	post-landing	22	3,000	Y
10	UA	7-Sep	17:29	LTE	satcom	post-landing	2,970	3,000	Y
10	CS	7-Sep	17:29	LTE	satcom	post-landing	2,304	5,000	Y
11	UA	7-Sep	17:44	satcom	C-Band	departure	1,658	5,000	Y
11	CS	7-Sep	17:44	satcom	C-Band	departure	733	3,000	Y
11	UA	7-Sep	17:46	C-Band	satcom	cruise	2,087	5,000	Y
11	CS	7-Sep	17:46	C-Band	satcom	cruise	928	5,000	Y
11	UA	7-Sep	17:46	satcom	LTE	cruise	1,489	5,000	Y
11	CS	7-Sep	17:46	satcom	LTE	cruise	727	5,000	Y
11	UA	7-Sep	17:47	LTE	C-Band	arrival	10,738	3,000	N
11	CS	7-Sep	17:47	LTE	C-Band	arrival	10,413	3,000	N
11	UA	7-Sep	17:48	C-Band	satcom	post-landing	2,169	5,000	Y
11	CS	7-Sep	17:48	C-Band	satcom	post-landing	1,264	5,000	Y
11	UA	7-Sep	17:48	satcom	LTE	post-landing	1,442	5,000	Y
11	CS	7-Sep	17:48	satcom	LTE	post-landing	658	5,000	Y
11	UA	7-Sep	17:48	LTE	satcom	post-landing	2,213	5,000	Y
11	CS	7-Sep	17:48	LTE	satcom	post-landing	1,589	5,000	Y
12	UA	7-Sep	18:04	LTE	satcom	takeoff	2,768	5,000	Y
12	CS	7-Sep	18:04	LTE	satcom	takeoff	2,147	5,000	Y
12	UA	7-Sep	18:04	satcom	C-Band	cruise	1,601	5,000	Y
12	CS	7-Sep	18:05	satcom	C-Band	cruise	875	5,000	Y
12	UA	7-Sep	18:06	LTE	C-Band	cruise	1,734	5,000	Y
12	CS	7-Sep	18:06	LTE	C-Band	cruise	1,381	5,000	Y
12	UA	7-Sep	18:07	C-Band	satcom	cruise	2,775	5,000	Y
12	CS	7-Sep	18:07	C-Band	satcom	cruise	1,875	5,000	Y
12	UA	7-Sep	18:07	satcom	LTE	cruise	1,447	5,000	Y
12	CS	7-Sep	18:07	satcom	LTE	cruise	360	5,000	Y
12	UA	7-Sep	18:08	LTE	C-Band	descent	1,614	5,000	Y
12	CS	7-Sep	18:08	LTE	C-Band	descent	1,293	5,000	Y
12	UA	7-Sep	18:08	C-Band	satcom	descent	2,849	5,000	Y
12	CS	7-Sep	18:08	C-Band	satcom	descent	981	5,000	Y
12	UA	7-Sep	18:08	satcom	LTE	descent	1,446	5,000	Y
12	CS	7-Sep	18:08	satcom	LTE	descent	635	5,000	Y
12	UA	7-Sep	18:08	LTE	satcom	landing	2,062	5,000	Y
12	CS	7-Sep	18:08	LTE	satcom	landing	1,432	5,000	Y
13	UA	7-Sep	18:16	LTE	satcom	takeoff	3,178	3,000	Y
13	CS	7-Sep	18:16	LTE	satcom	takeoff	2,534	3,000	Y
13	UA	7-Sep	18:16	satcom	C-Band	departure	10,951	3,000	N
13	CS	7-Sep	18:16	satcom	C-Band	departure	10,071	3,000	N
13	UA	7-Sep	18:17	C-Band	satcom	cruise	2,156	5,000	Y
13	CS	7-Sep	18:17	C-Band	satcom	cruise	1,256	5,000	Y
13	UA	7-Sep	18:18	satcom	LTE	cruise	10,589	5,000	N
13	CS	7-Sep	18:18	satcom	LTE	cruise	9,119	5,000	N
13	UA	7-Sep	18:19	LTE	C-Band	arrival	1,663	3,000	Y
13	CS	7-Sep	18:19	LTE	C-Band	arrival	1,265	3,000	Y
13	UA	7-Sep	18:19	C-Band	satcom	arrival	2,888	3,000	Y
13	CS	7-Sep	18:19	C-Band	satcom	arrival	1,895	3,000	Y
13	UA	7-Sep	18:19	satcom	LTE	arrival	10,588	3,000	N
13	CS	7-Sep	18:19	satcom	LTE	arrival	9,081	3,000	N
13	UA	7-Sep	18:20	LTE	satcom	landing	3,013	3,000	N
13	CS	7-Sep	18:20	LTE	satcom	landing	2,395	3,000	Y
14	UA	7-Sep	18:38	LTE	C-Band	departure	1,775	3,000	Y
14	CS	7-Sep	18:38	LTE	C-Band	departure	1,394	3,000	Y
14	UA	7-Sep	18:43	LTE	C-Band	cruise	10,763	5,000	N
14	CS	7-Sep	18:43	LTE	C-Band	cruise	1,282	5,000	Y
15	UA	7-Sep	18:58	LTE	C-Band	surface	1,649	3,000	Y
15	CS	7-Sep	18:58	LTE	C-Band	surface	1,316	3,000	Y
15	UA	7-Sep	19:03	LTE	C-Band	arrival	7,538	3,000	N
15	CS	7-Sep	19:03	LTE	C-Band	arrival	1,306	3,000	Y
16	UA	8-Sep	9:38	LTE	C-Band	surface	1,894	3,000	Y
16	CS	8-Sep	9:38	LTE	C-Band	surface	1,466	3,000	Y
17	UA	8-Sep	10:02	LTE	C-Band	surface	2,372	3,000	Y
17	CS	8-Sep	10:02	LTE	C-Band	surface	1,848	3,000	Y
17	UA	8-Sep	10:04	LTE	C-Band	departure	16,643	3,000	N
17	CS	8-Sep	10:04	LTE	C-Band	departure	6,258	3,000	N
17	UA	8-Sep	10:05	LTE	C-Band	departure	1,783	3,000	Y
17	CS	8-Sep	10:05	LTE	C-Band	departure	1,325	3,000	Y
17	UA	8-Sep	10:06	LTE	C-Band	cruise	1,854	5,000	Y
17	CS	8-Sep	10:06	LTE	C-Band	cruise	1,355	5,000	Y
17	UA	8-Sep	10:11	LTE	C-Band	arrival	1,783	3,000	Y
17	CS	8-Sep	10:11	LTE	C-Band	arrival	1,368	3,000	Y

6 SUMMARY AND RECOMMENDATIONS

This section provides an overall assessment of the test/inspection results, and where appropriate, provides lessons learned and recommendation for further testing.

6.1 SUMMARY

For the UAS-C2 project, the following bullets summarize the three key performance indicators (KPIs):

1. Demonstrate the capabilities and limitations of CNPC over C-Band and cellular networks.
2. Compliance with [DO-377A] C2 Link System MASPS Security Requirements.
3. Demonstrate complementary Positioning, Navigation, and Timing (PNT) technology.

Table 6-1 identifies one or more metrics associated with each KPI and whether the project met or did not meet the metric.

Table 6-1. KPIs and Metrics

No.	KPI	Metric	Met/Not Met
1	Demonstrate the capabilities and limitations of CNPC over C-Band and cellular networks.	Demonstrate the CNPC signal-in-space performance per RTCA DO-362A C2 Data Link Minimum Operational Performance Standards (MOPS)	Met
2		Demonstrate the CNPC performance in both LOS and BVLOS representative operational environments where multiple radio towers provide CNPC link relays in departure and approach flight phases and determine the interference to existing cellular networks.	Partially met. We did not test link relays for multiple C-Band GRSs. We did not measure interference to cellular networks.
3		Demonstrate the integrated C2 communication system in an operational environment using CNPC, cellular and Satcom networks to provide seamless service as the UAS transitions between LOS and BVLOS flight operations.	Met
4	Compliance with [DO-377A] C2 Link System MASPS Security Requirements	Demonstrate RTCA DO-377A Minimum Aviation System Performance Standards (MASPS) compliant cybersecurity in networked C2 communication system operation to validate that C2 data can be exchanged securely through network switchovers while satisfying the latency and continuity of service requirements.	Met
5		Demonstrate cybersecurity technology to protect C2 signals for BVLOS operations (authentication, integrity and confidentiality).	Met
6	Demonstrate complementary Positioning, Navigation, and Timing (PNT) technology	Demonstrate Alternate Positioning, Navigation, and Timing (APNT) technologies using two technologies. First, a combination of CNPC and cellular services without relying on GPS, and second, an optical system integrated with an inertial system and onboard map database.	Partially met. We demonstrated this KPI through one system, but not two.

6.1.1 APNT with Honeywell Vision Aided Navigation (VAN)

The Honeywell VAN performed as expected during the test scenario, providing accurate navigation information in the absence of GPS. Scenario 4 was flown twice, with GPS disabled during both tests to demonstrate the APNT solution. The horizontal position error was less than 5 meters CEP50 for both flights while GPS was disabled. This matches previous flight tests that Honeywell has conducted on other aircraft.

Table 6-2 summarizes the VAN position performance at the two different altitudes flown. With a fixed focal length camera, position error will increase with altitude due to the matched features in the image becoming larger.

Table 6-2. VAN Position Error at Different Altitudes

Metric	1000 ft AGL	3000 ft AGL
CEP50 (meters)	2.7	4.0
SEP50 (meters)	4.5	8.0

6.2 RECOMMENDATIONS AND LESSONS LEARNED

6.2.1 Program Management Lessons Learned

Contractual delays between Honeywell and NPUASTS prevented the companies from procuring hardware on time as per the planned schedule. The delayed hardware procurement prevented hardware integration with the C2 software. Ideally, hardware and software integration would have been completed months prior to the flight demonstration as integration reduces technical risk. Our resulting schedule was so compressed that several integration issues were not resolved before our flight testing, and troubleshooting these issues consumed much of our time onsite at NPUASTS. Future programs facing contractual delays might consider purchasing equipment at risk to mitigate the technical risk of delaying integration.

6.2.2 Recommendations and Lessons Learned for Future Flight Tests

For next steps, Honeywell has considered how to progress the UAS work accomplished under this project, and made submissions under Call 004 and Call 005 BAA that outline our recommended path forward in this area. In these whitepapers, Honeywell plans to incorporate the lessons learned from this project and flight test these improvements and additional features.

6.2.2.1 INTEGRATION TESTING

We recommend that future teams budget time for the software team to be collocated with the hardware to perform integration testing. Remote software developers faced challenges with VPNs and network access that were overcome by being physically located in the lab. Future programs should plan for developers to be onsite for the duration of the integration and test phase.

Future programs should plan several days where the team has access to the aircraft for hardware integration, mounting, and ground based validation of the system on the aircraft before engaging the flight crews. Mounting of antennas is not trivial and affects the RF performance considerably. Future programs should engage with RF engineers to verify the planned antenna mounting to the aircraft. It was helpful for us to share pictures of our planned mounting solution

with antenna experts to get their feedback. Teams should avoid making assumptions about how antennas work and instead directly engage with the designer or supplier to get a mutual understanding of ideal mounting locations and system operation; these conversations can occur early in a program. Once the antenna mounting solution is identified, teams should plan flight tests specifically to verify the mounting of each system.

Troubleshooting interference issues requires data collection with each component transmitting, one by one. A methodical approach is required; therefore, interference testing cannot be rushed and should be undertaken only when the final configuration is ready.

We learned it is important to test the streaming of data over the radios when they are in a configuration identical to the final test setup. As an example, the C-Band radios were sensitive to the position of the ground station radios (GRSs). We had to make several last-minute adjustments to the C-Band system to account for issues: we re-configured the GRS location and orientation to obtain ideal reception, but we then needed to install attenuators to the drone C-Band antennas because the signal was too strong. We also needed to add a delay to throttle the data sent to the radio from both the ARS and GRS. While the team was able to overcome these technical issues, they illustrate the importance of streaming data using the flight test configuration during shakedown testing well prior to the flight test.

6.2.2.2 SYSTEMS DESIGN

From a system design perspective, we learned that fewer components create a better design. Each sub-system creates the opportunity for another set of technical issues and considerations. As an example, several subsystems in our C2 system required GPS, and they each needed their own GPS antenna; it was not possible to share one source. This meant each GPS antenna must be functional and have GPS lock for the subsystem to work. The inference from other systems to each antenna needed to be considered and the unique mounting solution required more consideration. In addition, we observed that the power source to subsystems should not be shared if possible. Some systems have special power-down procedures and others do not. Inflicting special procedures to accommodate these special power-down procedures each time the team needed to power cycle during troubleshooting during integration testing made testing less streamlined.

6.2.2.3 AIRCRAFT AIRWORTHINESS

The C2 project faced several challenges, most notably, how to resolve a concern with the airworthiness of the planned flight vehicle, a Cessna. With time, the team understood that mounting of the SATCOM antenna needed for the C2 system on the Cessna would not be possible without significant and costly modifications to the aircraft, and to meet the program goals, the team made a necessary but late decision to test the C2 system on an Alta-X instead. While this decision allowed the team to meet several KPIs for the C2 project, we were also unable to test the final flight test configuration early in the program. Ideally, the aircraft configuration, mounting, and equipment installation is solidified during the shakedown testing. This reduces technical risk and ensures all the program objectives can be met. Unfortunately, the airworthiness concern was raised 10 months into a 12-month contract, and the team was not prepared to quickly resolve the resulting issues on the planned air vehicle. NPUASTS and iSight, the aircraft owner, were unfamiliar with the airworthiness process, and building the application for Experimental Category was a learning process for both companies. Ultimately the teams obtained the experimental ticket for the Cessna to operate with the Honeywell VAN system, and this allowed the Cessna to be used as planned to meet KPI 6.

6.2.3 Software Improvements to the C2 Application

Existing switchover controls in the GFE software showed some limitations during the UAS-PP project that were corrected before the flights commenced for the UAS-C2 project. These software limitations arose from a couple of factors. Firstly, the UA and CS DTSRs could be out of sync with regard to the availability of any link for some brief time. Having a different assessment of the link availability sometimes made each DTSR choose different links as the most appropriate link to try attempt for a switchover. Secondly, once the DTSRs decided what link to try, the DTSR did not try any other link if it could not connect over it. Consequently, the UA and CS DTSRs were prone to getting stuck in a live-lock situation, hopelessly trying to connect with each other over different links. To avoid this problem, the C2 application software was changed after the UAS-PP flights, but before the UAS-C2 flights so that each DTSR would try to connect with the remote peer over every link, following a process that ensures convergence on a link that is available to both. This process continues uninterrupted until the DTSRs complete the switchover handshake over one of the links. To avoid discarding any switchover candidate links due to transient link status, both DTSRs try all links, regardless of availability status. Although this process might waste some time trying links that might be down in some situations, it ensures the UA and CS DTSRs will have the opportunity to test every link in a finite amount of time.

DTLS session establishment control software was also updated for the C2 test flights. Existing software required the CS DTSR to be running before its peer was brought up. The UA announced its availability to the CS with a single clear text message at start up. If the CS DTSR missed that message, it would reject the request to connect. This required the preferred link and the CS DTSR to be up on both sides before the UA DTSR could be started. In the new software, the UA announces its availability with some frequency, for as long as necessary, whenever a DTLS session is not active. This change allows the UA to make itself ready to initiate the DTLS handshake at any time.

6.2.4 Software Development Considerations

A significant source of issues during integration and testing came from components used to condition traffic for each of the IPv4 links. The associated risks can be mitigated in future implementations by requiring the following from each link solution:

1. Integrated VPN tunnel or similar traffic encryption support for defense in depth. Requiring the CS or UA to implement traffic encryption support impacts scalability and increases complexity.
2. Integrated framing protocol to facilitate tolerance of partial packet drops.
3. Integrated throttle control for UDP traffic over low data rate links.
4. Better, more regular access to control functions (e.g. device reset, config, status)

The high-level architecture of the software lends itself nicely to supporting C2 operations. Major modules correspond to well-defined aspects of the functionality involved. Interactions are well-defined and appropriate. However, some of the lower-level design choices have proven to be problematic. The following issues should be addressed in a production version of the C2 software:

1. A thread manager pattern is used extensively throughout the code for many of the components. Although it is well defined and useful for quick development, it results in the proliferation of Inter-Process Communication (IPC) queues and read/write threads

and promotes unnecessary message exchanges between threads within the same processes.
    - This might have a negative impact on performance since additional message copies need to be made and additional context switches are required for queue processing.
    - Decreases maintainability since it is more difficult to follow the messages through all queues and threads.
    - The use of multiple threads and IPCs could be replaced by a limited number of threads.
2. Many error conditions are not handled gracefully. Many components/threads will abort execution after hitting an error condition.
3. Triggering of session establishment is not implemented from the CS LMSF.
4. Many components have duplicate code.
5. No continuous integration support nor automated end-to-end tests.
6. No regular mechanism for user apps to interact with core C2 software beyond sending user data. LMSF test driver should be replaced by APIs that allow user applications to send commands to and handle notifications from the core C2 link management software.

Finally, manual adjustment of the DTLS_TIMEOUT_INIT parameter in the WolfSSL library file ./wolfssl/wolfssl/internal.h might be necessary to allow the software to complete the DTLS session establishment handshake over high-latency links. A value of four seconds worked well for the Satcom link for both projects.

6.2.5 C-Band Connection and Link Lessons Learned

During the first day of flight testing, 9/6/2023, the C-Band link was unstable and unreliable, having symptoms of very high latency, dropping messages, and intermittently dropping the link at the radio-level. With these symptoms, our C2 software was unable to detect the C-Band link as a suitable link option. During this first day of testing, the team was simultaneously proceeding with testing as well as troubleshooting these C-Band issues. The test configuration of the C-Band equipment was modified throughout the first 7 flights. However, after the 7th flight, the team was able to identify 3 separate root-causes for the issues observed during the first 7 flights. After the 7th flight all issues were identified and resolved so after the Flight #8, the C-Band link was available as a link option and used during testing.

Root causes of problems experienced with C-Band link:
1- The ground antenna coverage area.
2- Issues with a strong signal.
3- Software issues with the data rate.

<u>Ground GRS Antennas:</u>
Number of Ground Antennas:
Flights #1 through #7 were configured to have two C-Band GRS Ground Antennas, however, due to the connection issues experienced during testing, the test configuration was simplified for the remaining flights to remove the 2nd ground C-Band antenna, and test with a single antenna. Therefore, Flights #8 through #19 only used a single C-Band GRS Ground Station Antenna.

Ground Antenna Orientation:

The orientation of the ground antennas was observed to have a significant impact on the signal performance as the antennas are directional. The coverage cone from the ground antennas only extended about 40° laterally, and with an even smaller vertical window. The signal was observed to quickly degrade outside of these parameters.

Therefore, during testing, it was observed that the C-Band link became unreliable and unable to transmit data when the drone was flying over the ground antenna. The link was unusable even though the RSSI was at around -90 dB even though uAvionix indicated that RSSI between -80 and -100 dB is yellow scale of RSSI acceptable RSSI values and reception should work well up to -100 dB.

C-Band antenna attenuators:
Flights #1 through #7 were configured without any antenna attenuators. However, after consulting with uAvionix, based on their recommendation, attenuators were installed on the ARS for flight #8, and remained installed through flight #19. Without attenuators, the C-Band signal was too strong because of the close proximity between the GRS antenna and the ARS on the drone. The distance between the two antennas with the drone in the landing zone was about 90 feet, and with the GRS antennas pointed directly towards the drone, the signal strength lowered from -30 dB to -50 dB after installing the attenuators on the ARS. uAvionix specified that the C-Band radios fail when the signal is stronger than -40db.

C-Band data rate limit by uAvionix:
The data sent through the C-Band link had to be throttled by artificially adding a delay of 200 ms between each message. The radios otherwise became overwhelmed by the high throughput, and stopped transmitting. This delay was required to be inserted on both sides of the link, so both the ground control station and the ARS on the drone had to pause 200 ms before sending the next message through the C-Band link. This limitation clearly affects the overall data throughput capability of the C-Band link, however, without this delay, the link is unusable.

uAvionix Skyline Cloud Service:
The C-Band radio system supplied by uAvionix included an internet-based "Cloud" service for the communication link, where the data exchanges between the ground control station and the UA drone go through uAvionix Cloud service called "SkyLine". This SkyLine cloud service provides a central communication endpoint, where all uAvionix radios can be configured to automatically route all data messages and data traffic. Then this internet-based service becomes a common endpoint for connecting all ground control stations. This SkyLine Cloud service is optional, and it is not required for the operation of the uAvionix C-Band radio system.

Our baseline design for this project, and our test plans specified for us to use this SkyLine Cloud service for our flight testing. However, due to the challenges and instability of the C-Band system experienced in the field during testing, the team opted to bypass the SkyLine Cloud service after Flight #7 because of concerns of added delay or potential data corruption by the SkyLine Cloud service.

Because of this change in configuration during our testing, we observed that the SkyLine Cloud service added on average, about a 52-millisecond delay to the one-way latency. Which corresponds to 17% additional latency when comparing a 311 ms latency without SkyLine on Flight #14, and 363 ms latency with SkyLine on flight #18. However, even though there is a slight increase in latency, SkyLine was determined to not be a root-cause for our C-Band link

problems. Therefore, on flights 16 through 19, we re-enabled the C-Band system to connect through SkyLine.

CNPC through unsecure C2 links:
The uAvionix C-Band radio system includes the end-to-end C-Band Radios, but also includes the SkyLine Cloud system, which acts as the data endpoint on the ground for messaging and communicating with the UA. During system development and testing for this project, the team observed that there is no data encryption, no authentication, and no data security throughout any of the C-Band radio system components supplied by uAvionix. Even though this uAvionix data link is only at the link layer, it provides an unsecure direct path to the UA. This approach of an unauthenticated, in-the-clear link assumes that the Application for vehicle control will have all the necessary security controls in place to protect the flight operation.

However, common applications such as QGroundControl, which was used by NPUASTS for controlling the drone for this project, uses the lightweight Micro Air Vehicle Link (MAVLink) protocol for communication which lacks any security and is susceptible to attacks.
Similarly, the Honeywell SATCOM unit also provides a data link to the UA, by both Satcom and LTE, with an unsecure Internet connectivity, also assuming the Application will provide the security. Though the Honeywell Satcom unit is firewalled and does not have a publicly addressable endpoint as overt as the SkyLine service.

Our C2 system developed and used during this project had two levels of encryption and authentication over each of the links, first using endpoint encryption using WireGuard VPN, and second through the DTLS secure session between the DTSRs.

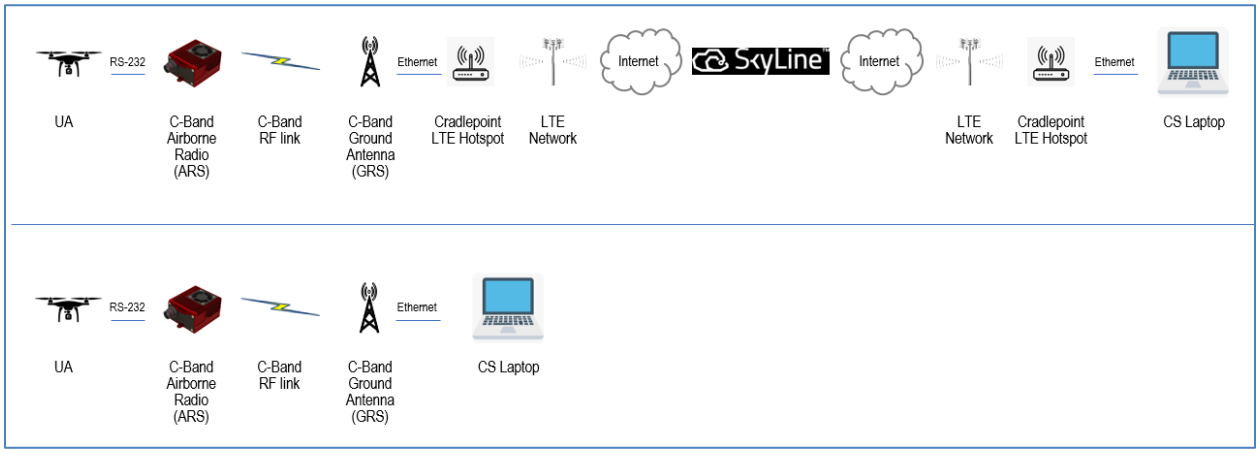


Figure 6-1. C-Band data path from UA to CS. Using uAvionix SkyLine (top), and without SkyLine (bottom)

Flight #	ARS with attenuators?	GRS1 Location	GRS1 orientation	GRS2 Location	GRS2 orientation	Skyline used?
Flight 1	no	west of building	to west (towards LZ)	north of building	to east (away)	Yes
Flight 2	no	west of building	to west (towards LZ)	north of building	to east (away)	Yes
Flight 3	no	west of building	to west (towards LZ)	north of building	to east (away)	Yes
Flight 4	no	west of building	to south	north of building	to east (away)	Yes
Flight 5	no	west of building	to south	north of building	to east (away)	Yes
Flight 6	no	west of building	to south	north of building	to west (to ARS)	Yes
Flight 7	no	west of building	to south	north of building	to west (to ARS)	Yes
Flight 8	Yes	south of LZ	to north (towards LZ)	n/a	n/a	no

Flight 9	Yes	south of LZ	to north (towards LZ)	n/a	n/a	no
Flight 10	Yes	south of LZ	to north (towards LZ)	n/a	n/a	no
Flight 11	Yes	south of LZ	to north (towards LZ)	n/a	n/a	no
Flight 12	Yes	south of LZ	to north (towards LZ)	n/a	n/a	no
Flight 13	Yes	south of LZ	to north (towards LZ)	n/a	n/a	no
Flight 14	Yes	south of LZ	to north (towards LZ)	n/a	n/a	no
Flight 15	Yes	south of LZ	to north (towards LZ)	n/a	n/a	no
Flight 16	Yes	south of LZ	to north (towards LZ)	n/a	n/a	Yes
Flight 17	Yes	south of LZ	to north (towards LZ)	n/a	n/a	Yes
Flight 18	Yes	south of LZ	to north (towards LZ)	n/a	n/a	Yes
Flight 19	Yes	south of LZ	to north (towards LZ)	n/a	n/a	Yes

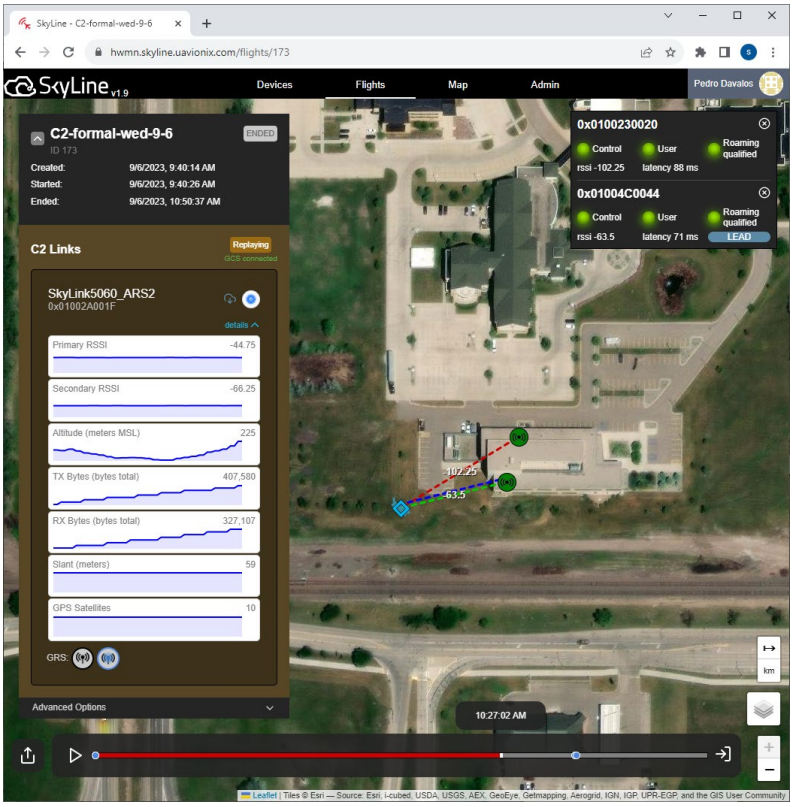


Figure 6-2. C2 Flight #1 - 9/6/2023 C-Band showing on Skyline with two GRS ground antennas.

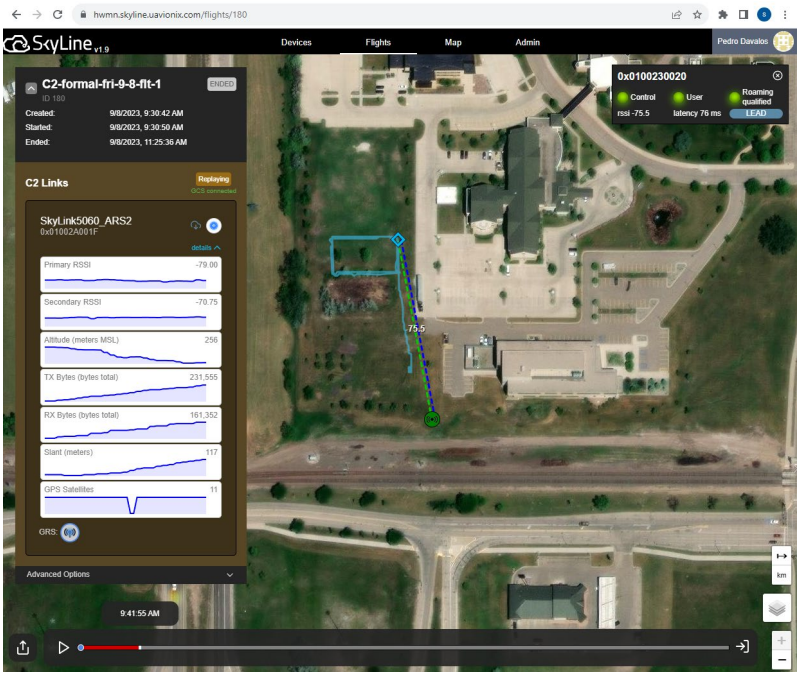


Figure 6-3. C2 Flight #16 - 9/8/2023 C-Band showing on Skyline with single GRS ground antenna.

6.2.6 C2 Link Routing Approach

Our implementation of the DTSRs use *C2 Link System Route Switchovers* (optional procedure 2, as presented in [DO-377A] (section 5.2.2)). In this type of procedure, the DTSRs rely on a single mapping from IPv6-to-IPv4 addresses in each direction to select the network link to use for user data and control message exchanges. When compared with the connection approach (optional procedure 1), route switchovers offer the advantage of having a single IPv6 address for each side of the C2 link throughout the whole network. However, it depends on maintaining the consistency of the two mappings across the network in a timely manner. This can be thought of, in general, as maintaining a consistent distributed state. The software problem can occur when one DTSR gets out of synch with the peer; in our case, the UA and CS DTSRs were talking on different tunnels and unable to communicate after hitting this condition. We assert that any implementation of this procedure would need to support scenarios where these mappings are, at least temporarily and possibly permanently, inconsistent throughout the network. Maintaining consistency reliably in the presence of faults is a difficult problem. Therefore, such provisions will ultimately add significant complexity to the software to safely support UAVs in real operational environments.

An approach consistent with *Multilink Operations*, as presented in [DO-377A] (section K.5.2.3), might be used to implement what can be referred to as continuous switchovers or stateless redundancy. This alternate approach would eliminate the need to declare and maintain a single IPv4 link as the *active* link. Instead, each DTSRs would be able to send and receive messages over any of the available links, eliminating the need to maintain a consistent distributed state across the network at all times. Link preference can be decided for each individual data message, if desired. Alternatively, virtual user plane channels can be defined; for example, each

user plane channel can have various throughput and latency requirements such that the DTSRs can make different routing decisions based on what channel is selected for each message by a user application.

Make-before-Break (MbB) switchovers require user data traffic to be sent over the active IPv4 link, while control messages are sent over the new link to setup the switchover. Since traditional IP routing can only provide one route per destination IP address at a given time, this kind of routing cannot be used to support the MbB behavior. The DTSRs in our implementation use traditional IP routing and therefore must stop sending user data before control messages can be sent over the new link. An alternative implementation might use policy-based routing to incorporate the destination ports for the user and control plane traffic to the routing criteria, enabling the routing of control and user traffic over different IPv4 links at the same time. Leveraging TunTap interfaces and the IP stack multiplexing functions to implement the UDMD proved to be an efficient and productive choice. This affords the following benefits:

- Collaborating user applications running on the UA and CS could communicate with each other using the well-known socket API without regard to lower level C2 link management behavior.
- User App development is largely decoupled from the availability of a C2 link subsystem. Most of it can proceed in easily accessible simulated network environments.
- Leverages maturity, availability, reliability, updatability and efficiency of existing IP stack implementations.

6.2.7 Honeywell VAN Recommendations

Honeywell VAN has been flight tested on several platforms across many different terrains, flight conditions, and time of day. The current prototype system is not SWAP optimized and was originally developed for flight at high altitude on large aircraft. For BVLOS operations on a small unmanned UAS, the Honeywell VAN could be implemented using existing sensors on the UAS and ported to the Honeywell Compact Inertial Navigation System (HCINS). HCINS is a small (162 cm^3) and lightweight (115 grams) navigation system designed for UAS operations.

A. EXPECTED RESULTS

This appendix documents the expected results for the verification steps in each test procedure. The results of post-flight analyses are compared with the expected results to ascertain compliance or identify deviations.

A.1 COMMON TEST PROCEDURES

A.1.1 TP_CM_001 – Control Plane and User Plane Traffic Mutual Authentication with User Plane Traffic Access Control Allowed

STEP	REQ	Action	Component	Description	Procedure

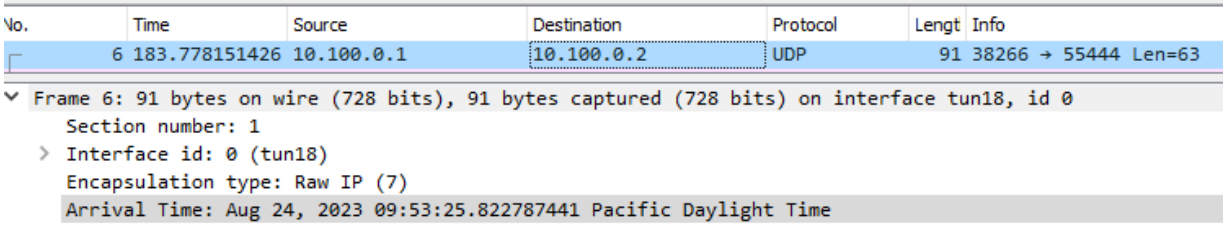
1	IR-03	VERIFY	CS LMSF console	CS status shows no secure connection for User Plane traffic or Control Plane traffic	`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: N/<ID> |`
					`Control: N/<ID>`

```
2023-08-24 16:52:58.364512 GMT Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

2	IR-03	VERIFY	UA LMSF console	UA status shows no secure connection for User Plane traffic or Control Plane traffic	`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: N/<ID> |`
					`Control: N/<ID>`

```
2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

3	IR-03	SEND	UA User Sniffer	Send User Data	UA User Sniffer shows n=1 message sent to DTSR at 09:53 PDT (11:53 CDT)



4	IR-03	VERIFY	UA Main Sniffer	User Data is not sent by the UA	Verify via the traffic sniffer log that the User Data message was not sent by the UA DTSR at 9:53 PDT (16:53 GMT)

STEP	REQ	Action	Component	Description	Procedure

ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.	Time	Source	Destination	Protocol	Lengt	Info
11172	1122.3852198…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	48274 → 51103 Len=3
12483	1168.3025248…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	39790 → 51103 Len=3
12511	1168.7277163…	10.20.0.2	10.20.0.1	ICMP	99	Destination unreachable (Port unreachable)
13215	1208.7926447…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	38594 → 51103 Len=3
19651	1477.3362272…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	38594 → 51103 Len=3

```
Frame 19651: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface tun2, id 0
   Section number: 1
   Interface id: 0 (tun2)
   Encapsulation type: Raw IP (7)
   Arrival Time: Aug 24, 2023 09:56:17.050257846 Pacific Daylight Time
```

Or the UA DTSR:
2023-08-24 16:53:25.822974 GMT INFO UdmdIn.cpp:51
Received: ID: 00000002 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE Data:
UD-AAAAAAAAAAAAAAAAAAA-000002
Sending user data message to peer
Secure session disabled - ID: 00000002 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE not sent to peer

5	IR-03	VERIFY	CS Main Sniffer	User Data is not received by the CS	Verify via the traffic sniffer log that the User Data message was not received by the CS DTSR at 09:53 PDT

ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

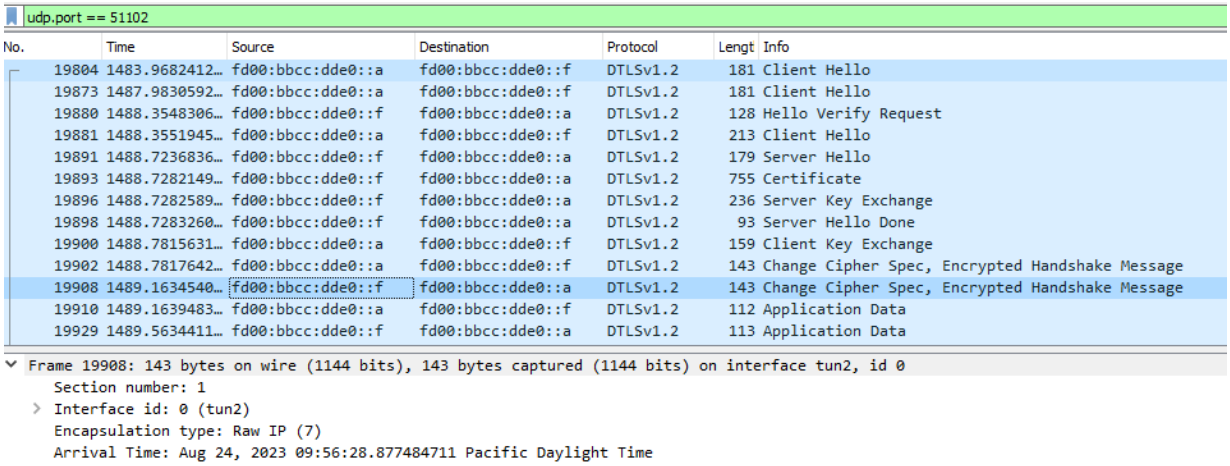
No.	Time	Source	Destination	Protocol	Lengt	Info
70075	3383.4103454…	10.20.0.2	10.20.0.1	ICMP	99	Destination unreachable (Port unreachable)
70880	3423.4603655…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	38594 → 51103 Len=3
77990	3691.8086652…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	38594 → 51103 Len=3

```
Frame 77990: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1
   Section number: 1
   Interface id: 1 (tun2)
   Encapsulation type: Raw IP (7)
   Arrival Time: Aug 24, 2023 09:56:16.611765841 Pacific Daylight Time
```

6	IR-08	OBSERVE	CS LMSF Console	View the status of all available links	lmsf lmsf> Status 1 Status 2 Status 3 Expected output Link 1 Up Link 2 Up Link 3 Up
7	IR-08	OBSERVE	UA LMSF Console	View the status of all available links at UA	cs-sh lmsf lmsf> Status 1 Status 2 Status 3 Expected output Link 1 Up Link 2 Up Link 3 Up
8	IR-01	SEND	UA LMSF Console	Establish secure session for the Control Plane and User Plane traffic	cs-sh lmsf lmsf> secure start

From UA DTSR Log:
2023-08-24 16:56:18.050748 GMT INFO ControlOut.cpp:193
Enabling secure session

STEP	REQ	Action	Component	Description	Procedure
9	IR-01 SER-08	OBSERVE	CS Main Sniffer	Secure session establishment are exchanged over the selected link	Observe secure session establishment messages exchanged



10	IR-07
	SER-07
	SER-08
		VERIFY	CS LMSF console	CS status shows:
				…secure session is established
				…which link is providing the connection
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

```
CS DTSR
2023-08-24 16:56:36.505869 GMT INFO      SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

11	IR-07
	SER-07
	SER-08
		VERIFY	UA LMSF console	UA status shows:
				…secure session is established
				…which link is providing the connection
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

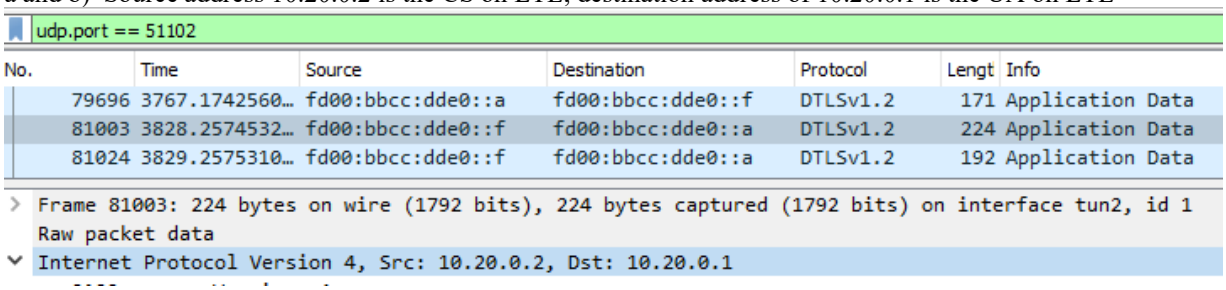
```
UA DTSR
2023-08-24 16:56:46.874857 GMT INFO      SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

12	IR-03	SEND	CS OS Console	Send User Data from CS to UA at a rate less than TET and size less than MTU	`uas-msg-sim cs`
13	IR-03	SEND	UA OS Console	Send User Data from UA to CS at a rate less than TET and size less than MTU	`uas-msg-sim ua`

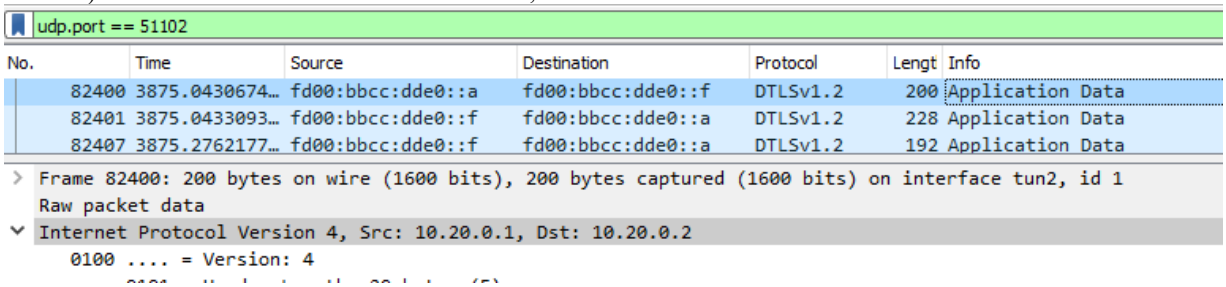
Post-test Log Analysis

STEP	REQ	Action	Component	Description	Procedure
14	IR-03 IR-04 IR-02	VERIFY	CS Main Sniffer	User Data is sent and received by the CS DTSR on the active link	Verify via the traffic sniffer log that: a) User Data messages were sent by the CS DTSR b) User Data messages were sent only via the link supporting the active connection c) User Data messages were received by the CS DTSR d) User Data messages were received only via the link supporting the active connection e) User Data and Control Messages include unique IP source and destination addresses that uniquely identify the UA and CS

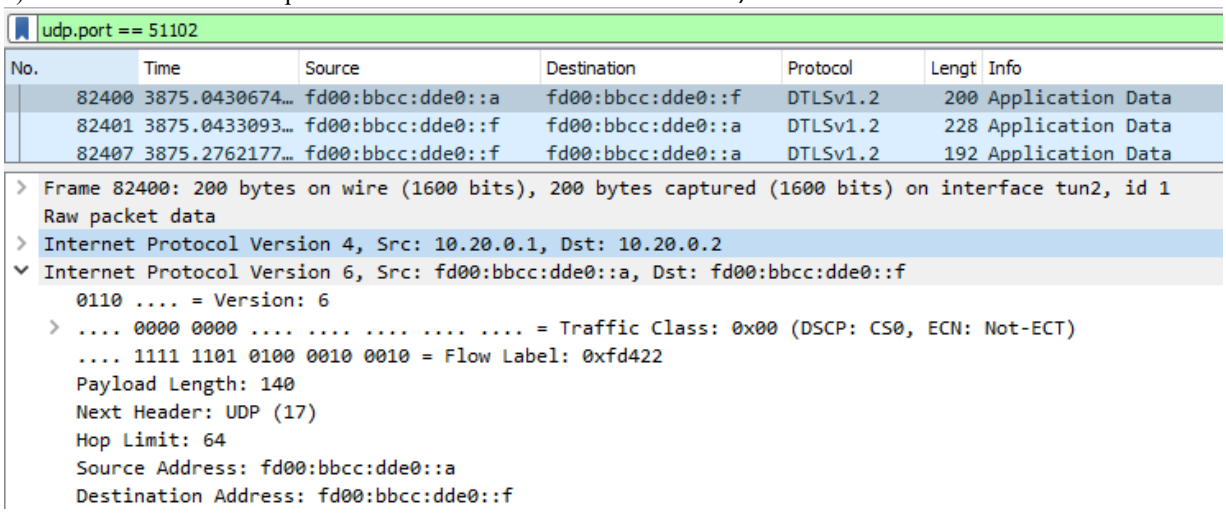
a and b) Source address 10.20.0.2 is the CS on LTE; destination address of 10.20.0.1 is the UA on LTE



C and d) Source address 10.20.0.1 is UA on LTE; destination address of 10.20.0.2 is CS on LTE

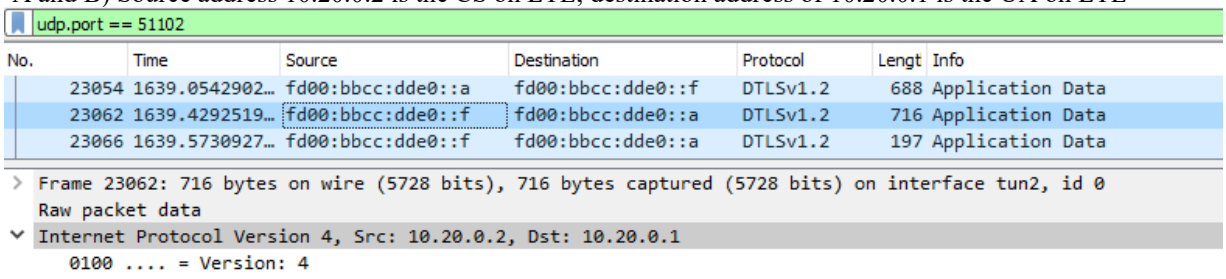


e) IPv6 addresses are unique. Fd00:bbcc:dde0::a is the UA DSTR; fd00:bbcc:dde0::f is the CS DTSR

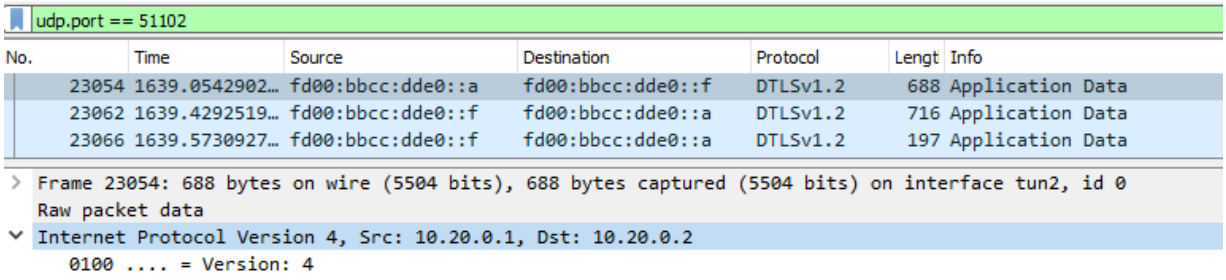


STEP	REQ	Action	Component	Description	Procedure
15	IR-03 IR-04 IR-02	VERIFY	UA Main Sniffer	User Data is sent and received by the UA DTSR on the active link	Verify the via traffic sniffer log that: a) User Data messages were received by the UA DTSR b) User Data messages were received only via the link supporting the active connection c) User Data messages were sent by the UA DTSR d) User Data messages were sent only via the link supporting the active connection e) User Data and Control Messages include unique IP source and destination addresses that uniquely identify the UA and CS

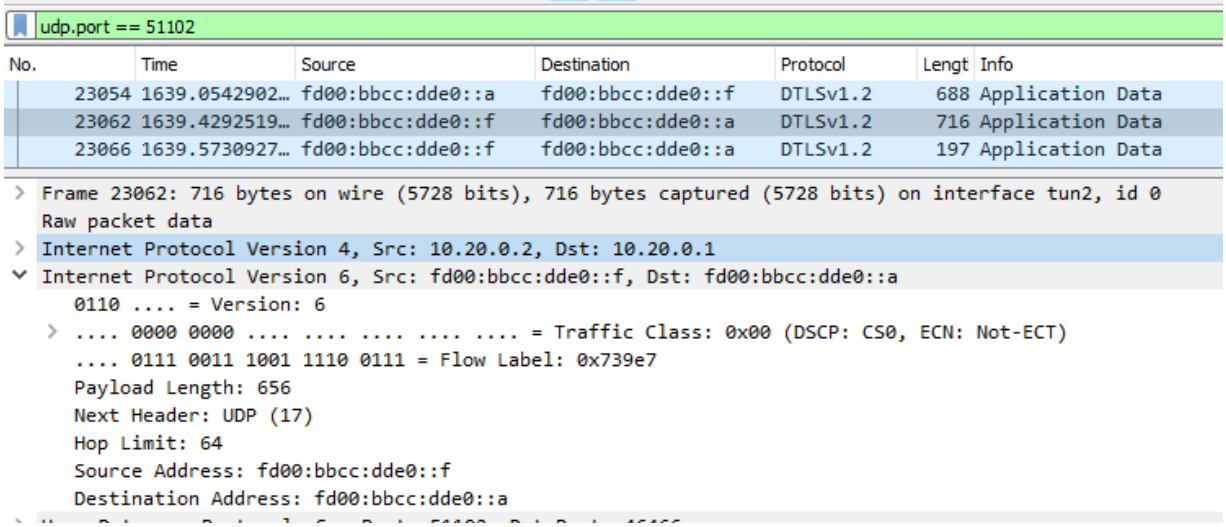
A and B) Source address 10.20.0.2 is the CS on LTE; destination address of 10.20.0.1 is the UA on LTE



C and D) Source address 10.20.0.1 is UA on LTE; destination address of 10.20.0.2 is CS on LTE



e) IPv6 addresses are unique. Fd00:bbcc:dde0::a is the UA DSTR; fd00:bbcc:dde0::f is the CS DTSR



A.1.2 TP_CM_002 – User Plane Traffic Mutual Authentication with UA Access to the CS Denied

STEP	REQ	Action	Component	Description	Procedure

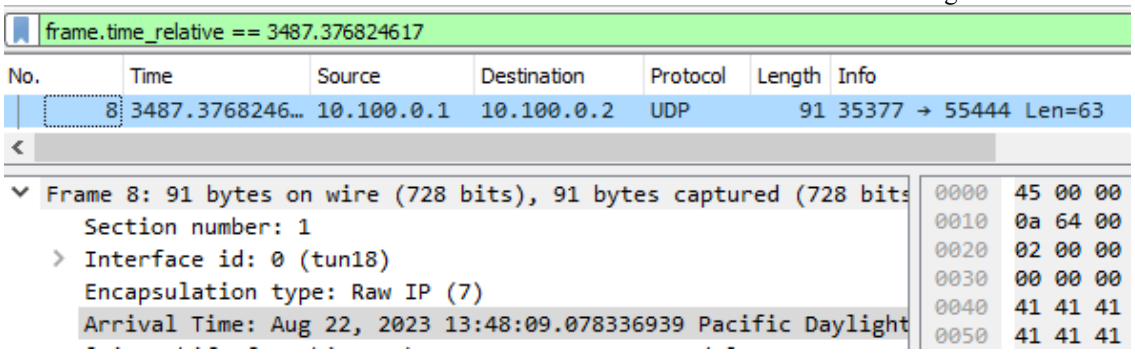
1	IR-03	VERIFY	CS LMSF console	CS status shows no secure connection for User Plane traffic or Control Plane traffic	`lmsf`
					`lmsf> status secure`
					
					Expected Console output:
					`STATUS User: N/<ID> |`
					`Control: N/<ID>`

```
2023-08-22 20:47:52.152545  Secure Link Detailed Status:
2023-08-22 20:47:52.152545       userOut enabled: 0
2023-08-22 20:47:52.152545        controlOut enabled: 0
2023-08-22 20:47:52.152545        user plane: NOT CONNECTED
2023-08-22 20:47:52.152545        control plane: NOT CONNECTED
```

2	IR-03	VERIFY	UA LMSF console	UA status shows no secure connection for User Plane traffic or Control Plane traffic	`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: N/<ID> |`
					`Control: N/<ID>`

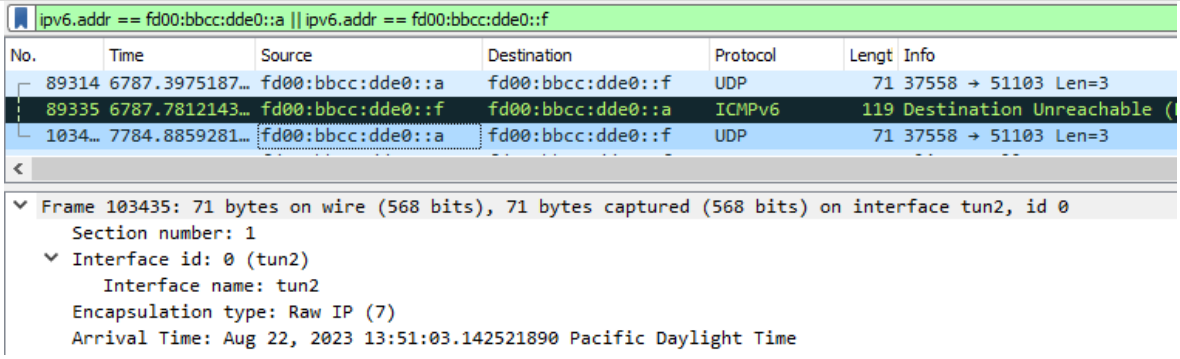
```
2023-08-22 20:47:45.071307 Secure Link Detailed Status:
2023-08-22 20:47:45.071307      userOut enabled: 0
2023-08-22 20:47:45.071307      controlOut enabled: 0
2023-08-22 20:47:45.071307      user plane: NOT CONNECTED
2023-08-22 20:47:45.071307      control plane: NOT CONNECTED
```

3	IR-03	SEND	UA User Sniffer	Send User Data	UA User Sniffer shows n=1 message sent to DTSR at 13:48



4	IR-03	VERIFY	UA Main Sniffer	User Data is not sent by the UA	The traffic sniffer log shows that User Data message was not sent by the UA DTSR at time 13:48

STEP	REQ	Action	Component	Description	Procedure

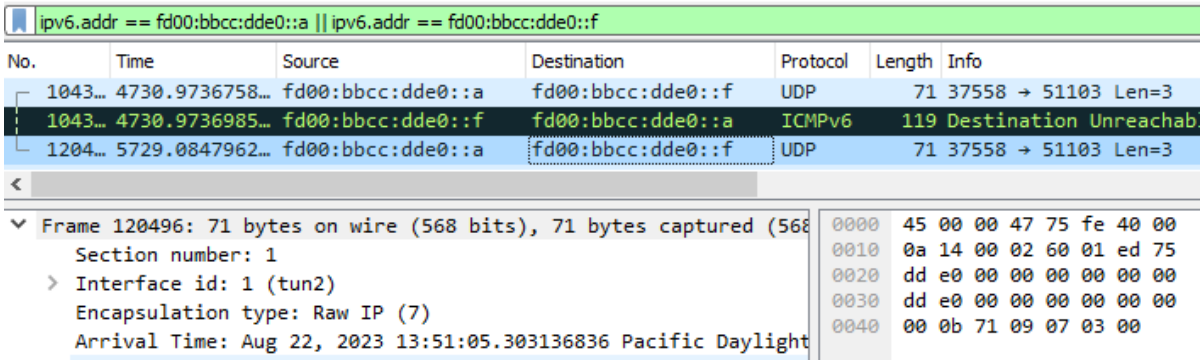


Or, we use the UA DTSR log:

```
2023-08-22 20:48:09.079004 GMT   SessionManager.cpp:293
Sending "ID: 00000008 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: " to lmsf_queue

2023-08-22 20:48:09.079042 GMT INFO     SessionManager.cpp:306
Sent "ID: 00000008 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: Secure session disabled - ID: 00000008 Origin: UDMD Cmd: SEND Size: 63
Rsp: FALSE not sent to peer to lmsf_queue
```

5	IR-03	VERIFY	CS Main Sniffer	User Data is not received by the CS	The traffic sniffer log shows that User Data message was not received by the CS DTSR at 13:48



6	IR-08	OBSERVE	CS LMSF Console	View the status of all available links at CS	`lmsf`
					`lmsf> status 1`
					`Status 2`

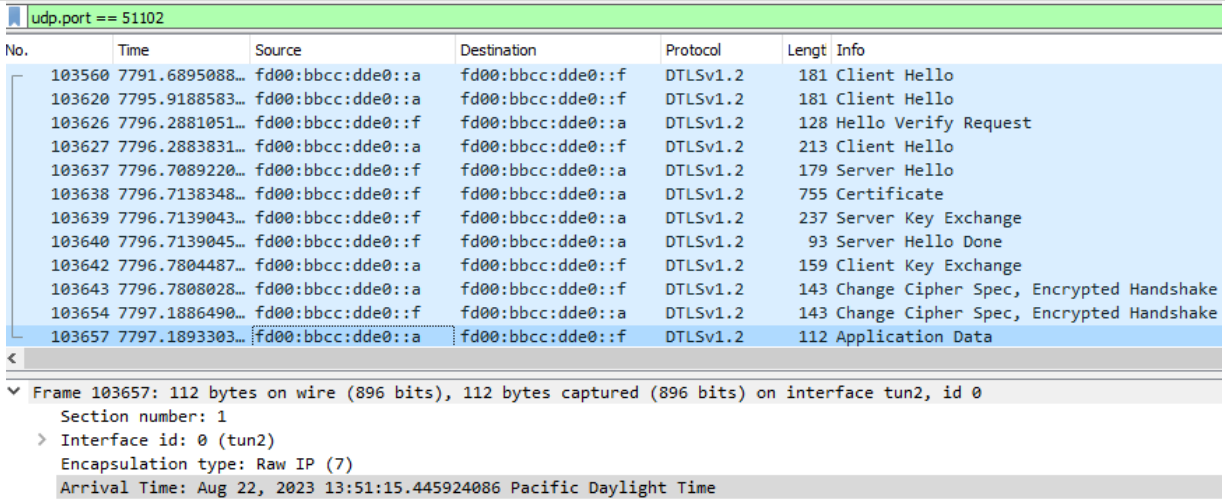
7	IR-08	OBSERVE	UA LMSF Console	View the status of all available links at UA	`cs-sh lmsf`
					`lmsf> status 1`
					`status 2`

8	IR-01	SEND	UA LMSF Console	Establish secure session for the Control Plane and User Plane traffic	`cs-sh lmsf` `lmsf> secure start`

```
2023-08-22 20:51:04.143057 GMT INFO     ControlOut.cpp:193
Enabling secure session
```

9	IR-01	OBSERVE	CS Main Sniffer	Secure session establishment messages are exchanged over the selected link	Observe secure session establishment messages exchanged

STEP	REQ	Action	Component	Description	Procedure



From the UA DTSR log:

```
2023-08-22 20:51:15.850216 GMT INFO     ControlIn.cpp:42
Received "DENY_CONNECT 3    " over secure session
Received DENY_CONNECT
Secure connection DENIED by remote peer.
```

10	SER-07 IR-07	VERIFY	CS LMSF Console	CS status shows no secure connection for User Plane traffic since UA access to the CS is denied	Lmsf lmsf> status secure Expected output: STATUS User: **N**/<ID> | Control: **N**/<ID>

```
From the CS DTSR log:
2023-08-22 20:51:58.067715 GMT INFO     SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 0
user plane: PENDING PEER
control plane: NOT CONNECTED
```

11	SER-07 IR-07	VERIFY	UA LMSF Console	UA status shows no secure connection for User Plane traffic since UA access to the CS is denied	cs-sh lmsf lmsf> status secure Expected output: STATUS User: **N**/<ID> | Control: **N**/<ID>

```
UA DTSR log:
2023-08-22 20:52:07.992178 GMT INFO     SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 0
user plane: PENDING PEER
control plane: NOT CONNECTED
```

12	IR-03	SEND	UA UDMD Console	Send User Data	UA User Sniffer shows n=1 message sent to DTSR at 13:52:18

STEP	REQ	Action	Component	Description	Procedure

frame.time_relative == 3736.387410022

No.	Time	Source	Destination	Protocol	Length	Info
9	3736.3874100…	10.100.0.1	10.100.0.2	UDP	91	35377 → 55444 Len=63

```
Frame 9: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface tun18, id 0
    Section number: 1
  > Interface id: 0 (tun18)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 22, 2023 13:52:18.088922344 Pacific Daylight Time
```

13	IR-03	VERIFY	UA Main Sniffer	User Data is <u>not</u> sent by the UA	The traffic sniffer log shows that User Data message was not sent by the UA DTSR.

Example from Sept 8th, where the UA Main sniffer shows no matching UDP message at the expected time (08:57:12) when the UDMD tried to send n=1. There are UDP messages before and after this time but not exactly at this time.

ua.main.sniffer.2023.09.08-09.50.59.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.	Time	Source	Destination	Protocol	Length	Info
78814	3961.3591656…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	51284
78841	3964.3594806…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	51284
78938	3967.3598159…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	51284
78964	3968.7004997…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	171	Appli
78998	3970.3604080…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	51284
79054	3973.3608586…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	51284
79139	3976.3612372…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	UDP	71	51284

```
Frame 78998: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface tun2,
    Section number: 1
  > Interface id: 1 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Sep  8, 2023 08:57:13.739035330 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
```

14	IR-03	VERIFY	CS User Sniffer	User Data is <u>not</u> received by the CS	The traffic sniffer log shows the User Data message was not received by the CS DTSR

cs.user.sniffer.2023.09.08-09.54.40.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
3968	3132.5862149…	10.100.0.1	10.100.0.2	UDP	548	32970 → 55447 Len=520
3969	3132.5862341…	10.100.0.2	10.100.0.1	ICMP	576	Destination unreachable (Por
3970	3133.1036504…	10.100.0.1	10.100.0.2	ICMP	85	Destination unreachable (Por
3975	3630.3100764…	10.100.0.2	10.100.0.1	UDP	91	53483 → 55444 Len=63
3983	3960.3921318…	10.100.0.2	10.100.0.1	WireGuard	91	Transport Data, receiver=0x0
3984	4163.3413533…	10.100.0.2	10.100.0.1	UDP	84	45854 → 55447 Len=56

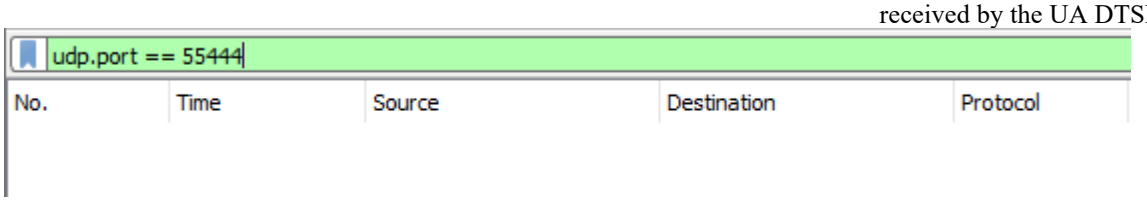
```
Frame 3975: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface tun18, id 0
    Section number: 1
  > Interface id: 0 (tun18)
    Encapsulation type: Raw IP (7)
    Arrival Time: Sep  8, 2023 08:58:23.865678246 Pacific Daylight Time
```

CS User sniffer shows no UDP message at 08:57:12 when the message from the UA was attempted.

STEP	REQ	Action	Component	Description	Procedure
15	IR-03	SEND	CS UDMD Console	Send User Data	udmd udmd> send n=1
16	IR-03	VERIFY	CS Main Sniffer	User Data is not sent by the CS	The traffic sniffer log shows that User Data message was not sent by the CS DTSR at time

The expected result is to see an error message in the DTSR log indicating the message cannot be sent. The CS Main sniffer should show no message at the instant the n=1 was attempted. None of the test cases passed for this condition to paste examples.

17	IR-03	VERIFY	UA Main Sniffer	User Data is not received by the UA	The traffic sniffer log shows the User Data message was not received by the UA DTSR



No messages for port 55444 (user data).

A.1.3 TP_CM_003 – User Plane Traffic Mutual Authentication with CS Access to the UA Denied

STEP	REQ	Action	Component	Description	Procedure
1	IR-03	VERIFY	CS LMSF console	CS status shows no secure connection for User Plane traffic or Control Plane traffic	lmsf lmsf> status secure Expected output: STATUS User: N/<ID> | Control: N/<ID>

```
2023-08-22 18:23:53.916215 GMT INFO  SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

2	IR-03	VERIFY	UA LMSF console	UA status shows no secure connection for User Plane traffic or Control Plane traffic	cs-sh lmsf lmsf> status secure Expected output: STATUS User: N/<ID> | Control: N/<ID>

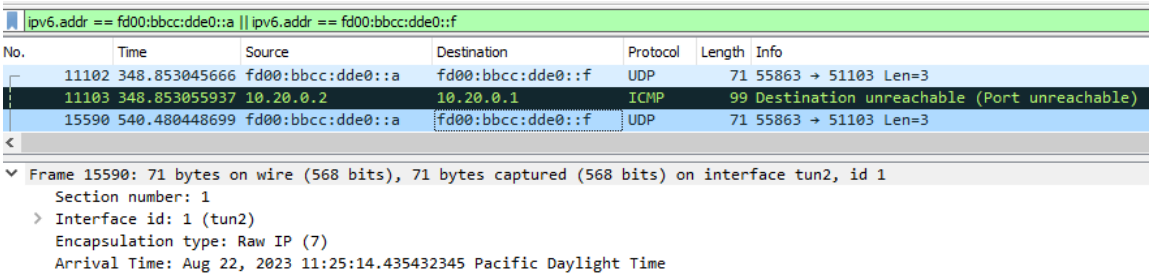
```
2023-08-22 18:24:00.234683 GMT INFO     SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

3	IR-03	SEND	UA UDMD Console	Send User Data	cs-sh udmd udmd> send n=1 at 18:24 GMT
4	IR-03	VERIFY	UA Main Sniffer	User Data is not sent by the UA	Verify via the traffic sniffer log that User Data message is not sent by the UA DTSR

STEP	REQ	Action	Component	Description	Procedure

2023-08-22 18:24:30.438765 GMT INFO UdmdIn.cpp:51
Received: ID: 00000002 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE
Data: UD-AAAAAAAAAAAAAAAAAAAA-000002
Sending user data message to peer
Secure session disabled - ID: 00000002
Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE not sent to peer
Sending "ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: " to lmsf_queue Unexpected message type: ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Sent "ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: Secure session disabled - ID: 00000002
Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE not sent to peer to lmsf_queue

5	IR-03	VERIFY	CS Main Sniffer	User Data is not received by the CS	Verify via the traffic sniffer log that the User Data message was not received by the CS DTSR at 11:24:30



CS Main sniffer shows message at 11:22, and next message at 11:25:14 (nothing at 11:24:30)

6	IR-08	OBSERVE	CS LMSF Console	View the status of all available links at CS	`lmsf` `lmsf> status`
7	IR-08	OBSERVE	UA LMSF Console	View the status of all available links at UA	`cs-sh lmsf` `lmsf> status`
8	IR-01	SEND	UA LMSF Console	Establish secure session for the Control Plane and User Plane traffic	`cs-sh lmsf` `lmsf> secure start`

```
2023-08-22 18:25:15.273392 GMT INFO      ControlOut.cpp:193
Enabling secure session
```

9	IR-01	OBSERVE	CS Main Sniffer	Secure session establishment are exchanged over the selected link	Observe secure session establishment messages exchanged

10	SER-07
	IR-07
		VERIFY	CS LMSF Console	CS status shows no secure connection for User Plane traffic since CS access to the UA is denied	`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: N/<ID> |`
					`Control: N/<ID>`

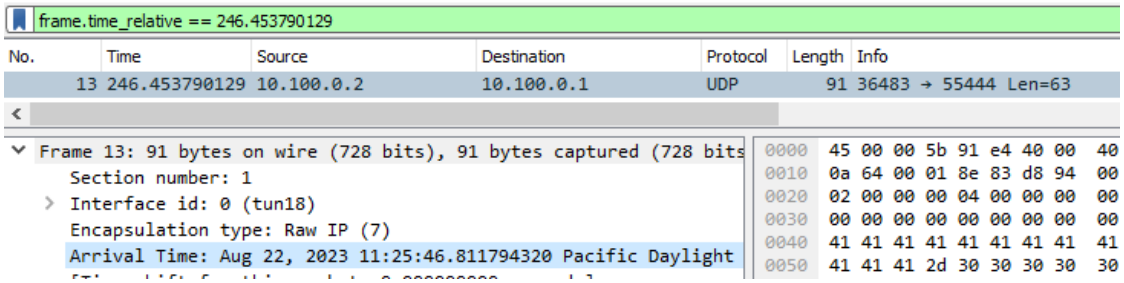
```
2023-08-22 18:25:32.068847 GMT INFO      SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

STEP	REQ	Action	Component	Description	Procedure

11	SER-07
	IR-07
		VERIFY	UA LMSF Console	UA status shows no secure connection for User Plane traffic since CS access to the UA is denied	`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: N/<ID> |`
					`Control: N/<ID>`

```
2023-08-22 18:25:37.654528 GMT INFO      SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

12	IR-03	SEND	CS UDMD Console	Send User Data	`udmd` `udmd> send n=1`




```
CS User sniffer shows UDMD message at 11:25:46 PDT
```

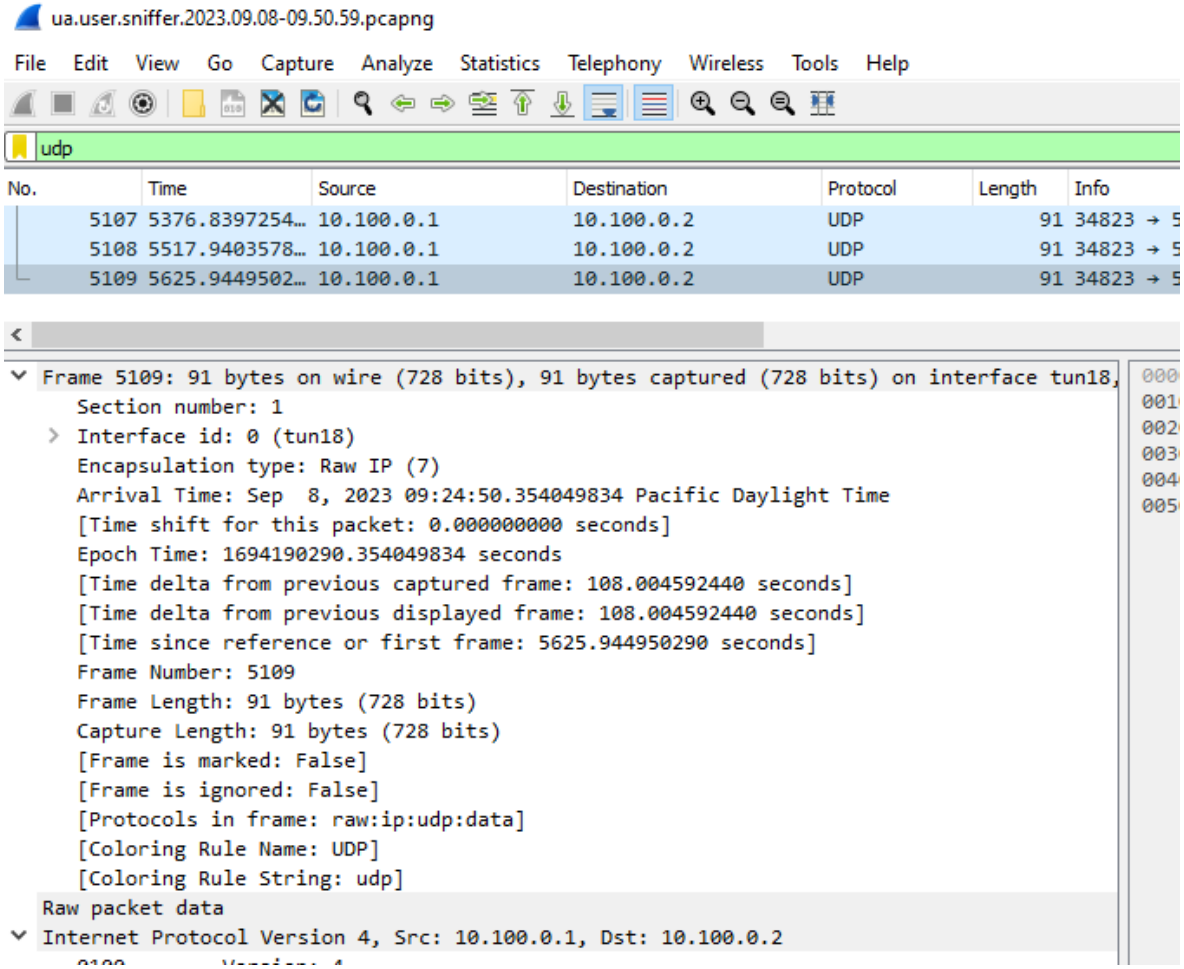
13	IR-03	VERIFY	CS Main Sniffer	User Data is not sent by the CS	The traffic sniffer log shows that User Data message was not sent by the CS DTSR at time 18:25:46 GMT

```
2023-08-22 18:25:46.811837 GMT INFO      UdmdIn.cpp:51
Received: ID: 00000002 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE
Data:UD-AAAAAAAAAAAAAAAAAAAA-000002
Sending user data message to peer
Secure session disabled - ID: 00000002 Origin: UDMD Cmd: SEND Size: 63 Rsp:
FALSE not sent to peer
Sending "ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: " to lmsf_queue
Sent "ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: Secure session disabled - ID: 00000002 Origin: UDMD Cmd: SEND Size: 63
Rsp: FALSE not sent to peer to lmsf_queue
```

14	IR-03	VERIFY	UA User Sniffer Log	User Data is not received by the UA	Verify via the traffic sniffer log that that no User Data message was received by the UA DTSR

STEP	REQ	Action	Component	Description	Procedure

Example from test on Sept 8th. CS sent n=1 at 9:24:21; UA User Sniffer shows no messages received at that time with source 10.100.0.2.

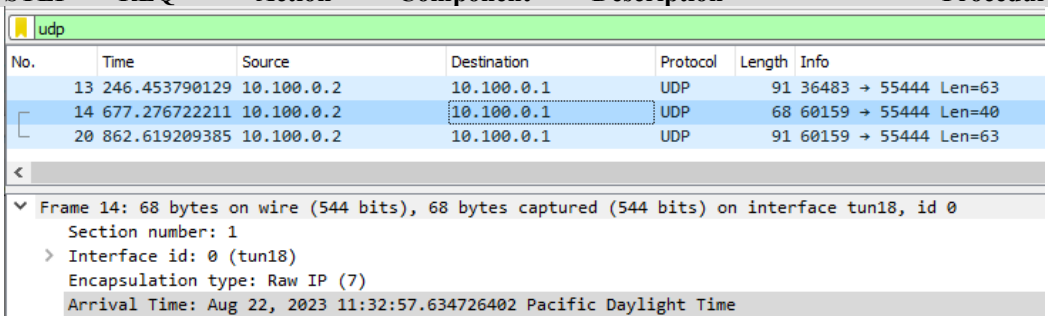


15	IR-03	SEND	UA UDMD Console	Send User Data	`udmd` `udmd> send n=1`
16	IR-03	VERIFY	UA Main Sniffer	User Data is not sent by the UA	Notification that User Data cannot be sent from the UA DTSR

```
2023-08-22 18:25:57.442190 GMT INFO      UdmdIn.cpp:51
Received: ID: 00000004 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE
Data:UD-AAAAAAAAAAAAAAAAAAAA-000004
Sending user data message to peer
Secure session disabled - ID: 00000004 Origin: UDMD Cmd: SEND Size: 63 Rsp:
FALSE not sent to peer
Sending "ID: 00000004 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: " to lmsf_queue
Sent "ID: 00000004 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: Secure session disabled - ID: 00000004 Origin: UDMD Cmd: SEND Size: 63
Rsp: FALSE not sent to peer to lmsf_queue
```

17	IR-03	VERIFY	CS User Sniffer	User Data is not received by the CS	Verify via the traffic sniffer log that no User Data message was received by the CS DTSR or UDMD

STEP	REQ	Action	Component	Description	Procedure



CS User Sniffer shows UDP message at 11:25:46 PDT and the next message is 11:32:57, which is the next scenario. Nothing at 11:25 or 11:26 when UDMD would expect to receive it.

A.1.4 TP_CM_004 – User Data Exchanges with Encryption

A.1.4.1 TP_CM_004A – USER DATA EXCHANGES WITH ENCRYPTION, PAYLOAD DATA < MTU

STEP	REQ	Action	Component	Description	Procedure
1	IR-09b	SEND	UA UDMD Console	Send a User Data less than MTU size	udmd udmd> send n=1

```
UA DTSR
2023-08-24 16:57:31.818437 GMT INFO     UdmdIn.cpp:51
Received: ID: 00000004 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE Data:
UD-AAAAAAAAAAAAAAAAAAA-000004
Sending user data message to peer
User Output: Sent 66 bytes.
Buffer Contents: [0542000400000002  000000040000007f  0000003f00000000
00000000fa107455 00000055442d4141  4141414141414141  4141414141414141
41412d3030303030  3400]
Sent "USER_DATA.REQ           66
```

2	IR-09b	VERIFY	CS Main Sniffer	User Data < MTU does not require segmentation	Verify via the traffic sniffer log that User Data was not segmented

STEP	REQ	Action	Component	Description	Procedure

ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.	Time	Source	Destination	Protocol	Lengt	Info
78263	3703.6367066…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	113	Application Data
79696	3767.1742560…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	171	Application Data
81003	3828.2574532…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	224	Application Data

```
> Frame 79696: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface tun2, id 1
  Raw packet data
v Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 171
    Identification: 0xde54 (56916)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: IPv6 (41)
    Header Checksum: 0x88aa [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.20.0.1
    Destination Address: 10.20.0.2
v Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1111 1101 0100 0010 0010 = Flow Label: 0xfd422
    Payload Length: 111
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: fd00:bbcc:dde0::a
    Destination Address: fd00:bbcc:dde0::f
> User Datagram Protocol, Src Port: 46466, Dst Port: 51102
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 1
      Sequence Number: 2
      Length: 90
      Encrypted Application Data: 0d966aa56d28d5ffd1cd3ec927d5cf74d0092e280ac91407014ef6ada0d3f3b08490400c…
```

3	SER-04	VERIFY	UA Main Sniffer	User Data sent is encrypted	Verify via the traffic sniffer log that the content of the User Data message sent cannot be discerned

udp.port == 51102

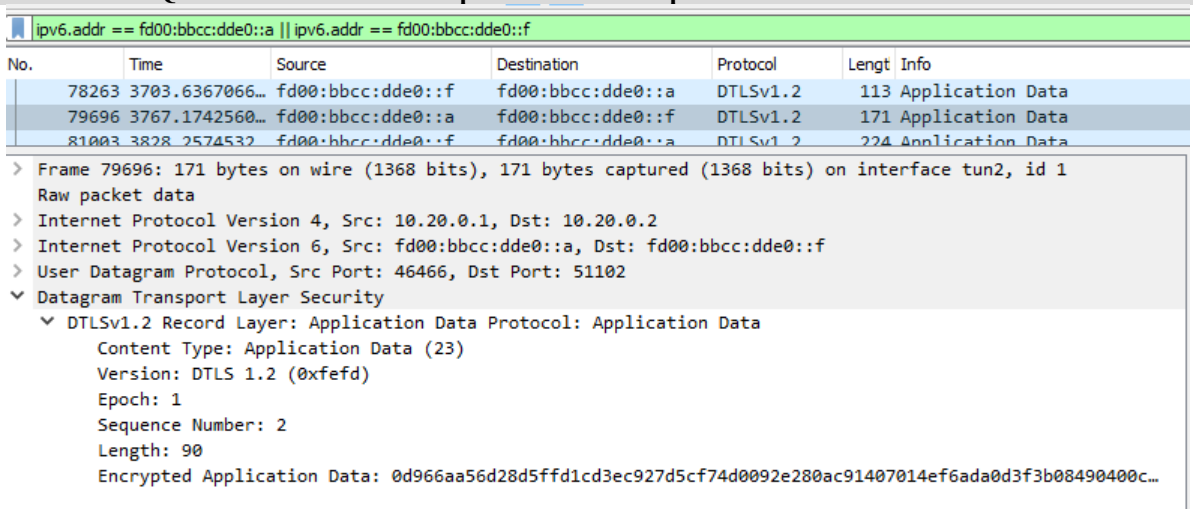
No.	Time	Source	Destination	Protocol	Lengt	Info
19929	1489.5634411…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	113	Application Data
21170	1552.1051299…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	171	Application Data
22327	1613.6457667…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	224	Application Data

```
> Frame 21170: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface tun2, id 0
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
> User Datagram Protocol, Src Port: 46466, Dst Port: 51102
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 1
      Sequence Number: 2
      Length: 90
      Encrypted Application Data: 0d966aa56d28d5ffd1cd3ec927d5cf74d0092e280ac91407014ef6ada0d3f3b08490400c…
```

UA Main sniffer shows application data is encrypted

4	SER-04	VERIFY	CS Main Sniffer	User Data received is encrypted	Verify via the traffic sniffer log that the content of the User Data message received cannot be discerned

STEP	REQ	Action	Component	Description	Procedure



CS Main Sniffer shows application data is encrypted

Post-test Log Analysis

5	SER-02 SER-04	VERIFY	CS and UA DTSR Live Log	User Data received matches User Data sent which indicates the message was accepted as authentic.	a) Compare the CS DTSR log with the source data on the UA to show that the sent and received contents are the same b) Compare the UA DTSR log with the source data on the CS to show that the sent and received contents are the same.

UA DTSR

```
2023-08-24 16:57:31.818437 GMT INFO     UdmdIn.cpp:51
Sending user data message to peer
User Output: Sent 66 bytes.
Buffer Contents: [0542000400000002  000000040000007f  0000003f00000000
00000000fa107455 00000055442d4141  4141414141414141  4141414141414141
41412d3030303030  3400]
```

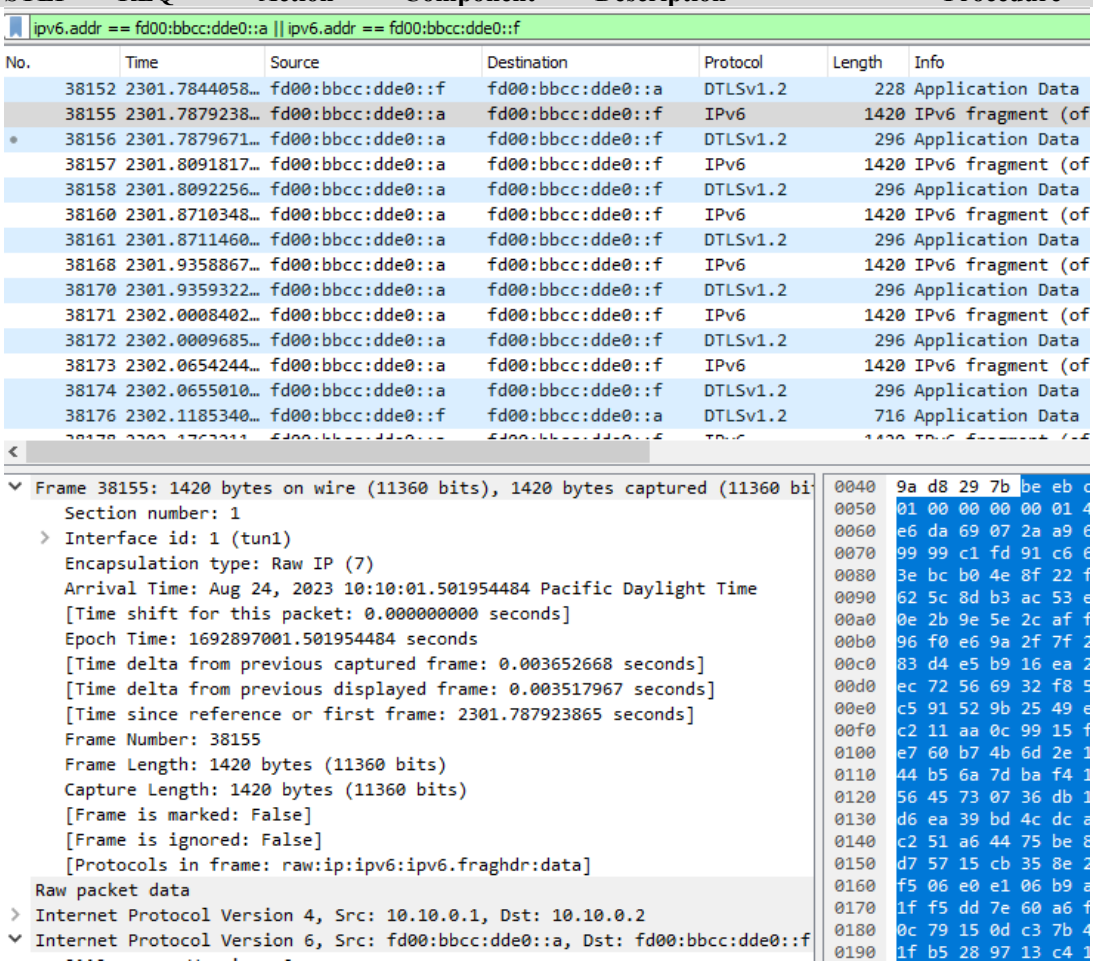
CS DTSR

```
2023-08-24 16:57:31.977458 GMT INFO     UserIn.cpp:43
Received "USER_DATA.REQ           66
0542000400000002  000000040000007f  0000003f00000000 00000000fa107455
00000055442d4141  4141414141414141  4141414141414141  41412d3030303030  3400
```

A.1.4.2 TP_CM_004B – USER DATA EXCHANGES WITH ENCRYPTION, PAYLOAD DATA > MTU

STEP	REQ	Action	Component	Description	Procedure
1	IR-09b	SEND	CS OS Console	Send a User Data greater than MTU size	`cs-rft <filename> <local filename>`
2	IR-09b	VERIFY	UA Main Sniffer	User Data > MTU is segmented	Verify via the traffic sniffer log that User Data was segmented

STEP	REQ	Action	Component	Description	Procedure



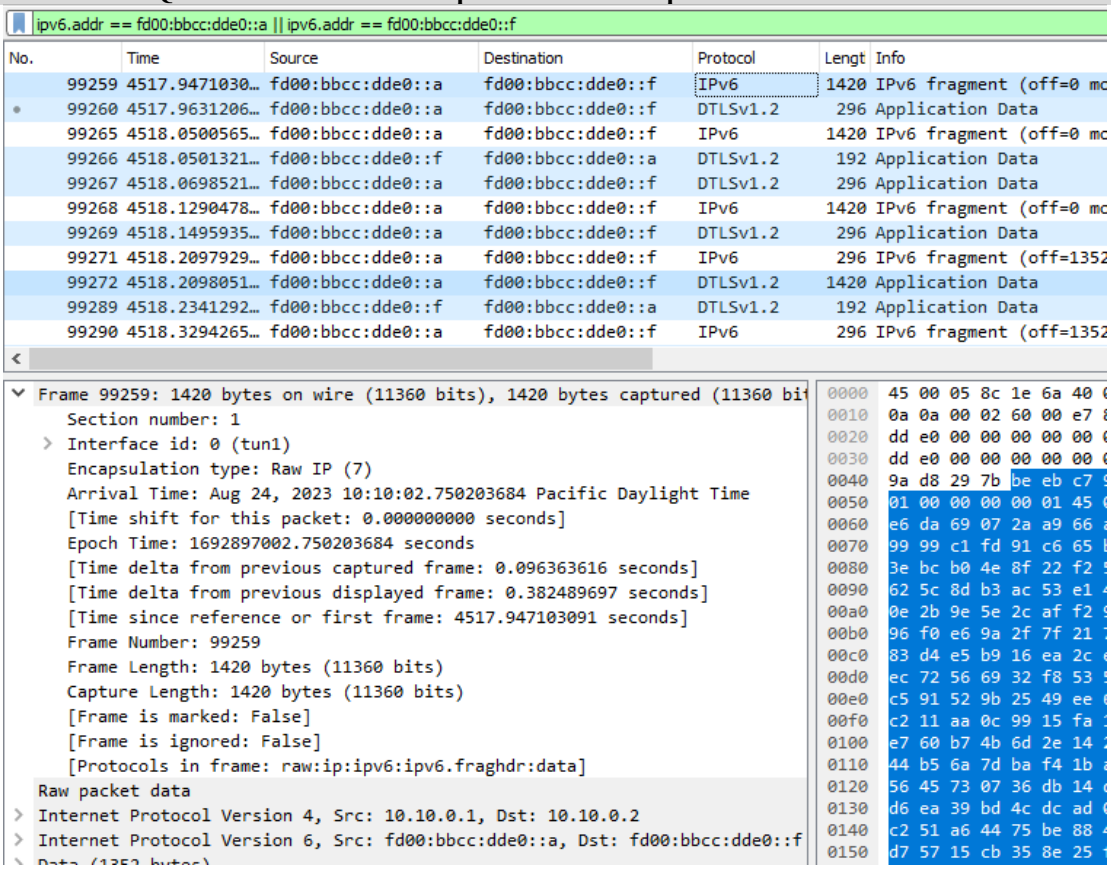
UA Main Sniffer shows messages are divided into max length of 1420 bytes.

3	SER-04	VERIFY	UA Main Sniffer	User Data sent is encrypted	Verify via the traffic sniffer log that the content of the User Data message sent cannot be discerned

UA Main sniffer log snapshot in step 2 shows message is encrypted.

4	SER-04	VERIFY	CS Main Sniffer	User Data received is encrypted	Verify via the traffic sniffer log that the content of the User Data message received cannot be discerned

STEP	REQ	Action	Component	Description	Procedure



CS Main sniffer shows messages are encrypted

Post-test Log Analysis

5	SER-02 SER-04	VERIFY	UA and CS Content Directory	User Data received matches User Data sent which indicates the message was accepted as authentic.	Compare the received User Data file with the source User Data file on the UA to show that the sent and received contents are the same

A.1.5 TP_CM_005 – User Data Exchanges without Encryption

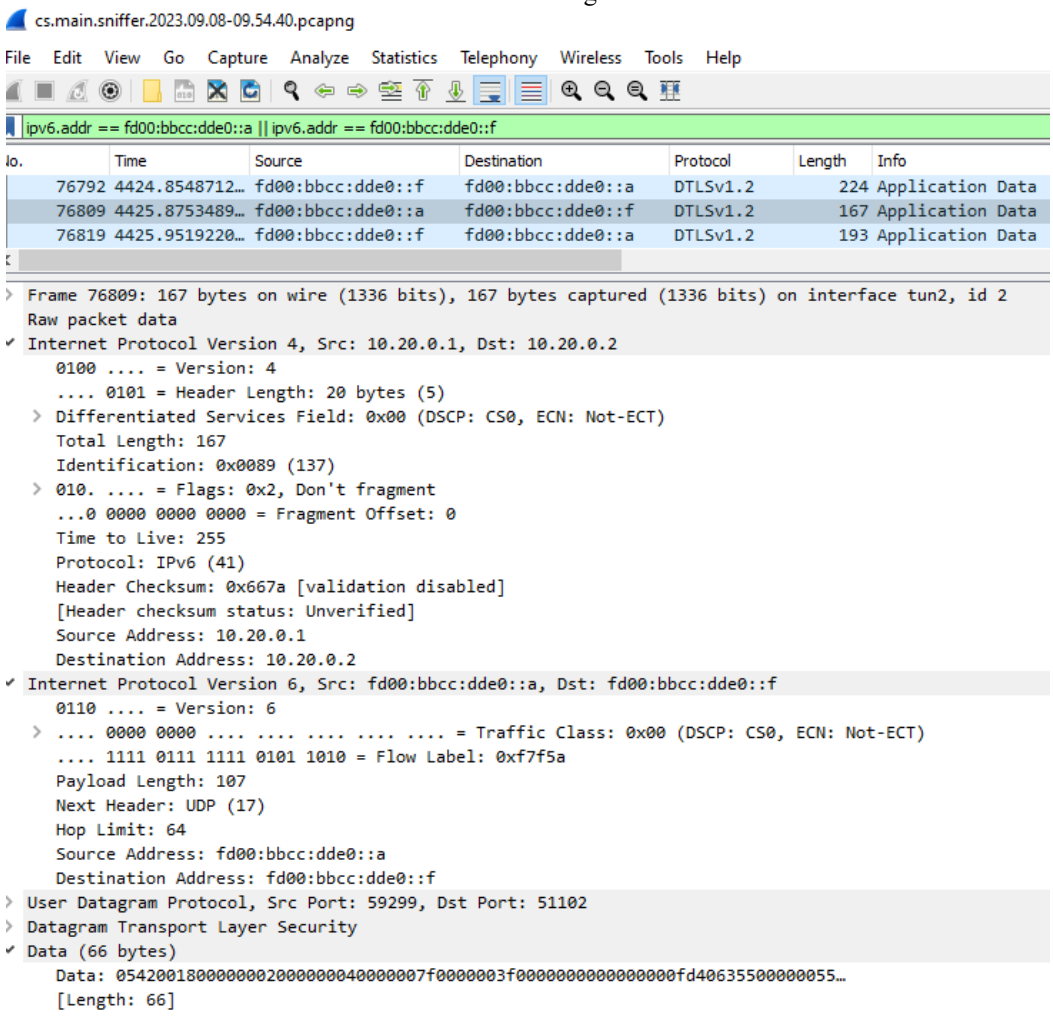
A.1.5.1 TP_CM_005A – USER DATA EXCHANGES WITHOUT ENCRYPTION, PAYLOAD DATA < MTU

Procedure:

STEP	REQ	Action	Component	Description	Procedure
1	IR-09b	SEND	UA UDMD Console	Send User Data less than MTU size	`cs-sh` `udmd> send n=1`

```
UA DTSR
2023-09-08 16:08:27.122153 GMT INFO     UdmdIn.cpp:51
Received: ID: 00000024 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE
Data: UD-AAAAAAAAAAAAAAAAAAAA-000024
Sending user data message to peer
User Output: Sent 66 bytes.
```

STEP	REQ	Action	Component	Description	Procedure
2	IR-09b	VERIFY	CS Main Sniffer	User Data < MTU does not require segmentation	Verify via the traffic sniffer log that User Data was not segmented



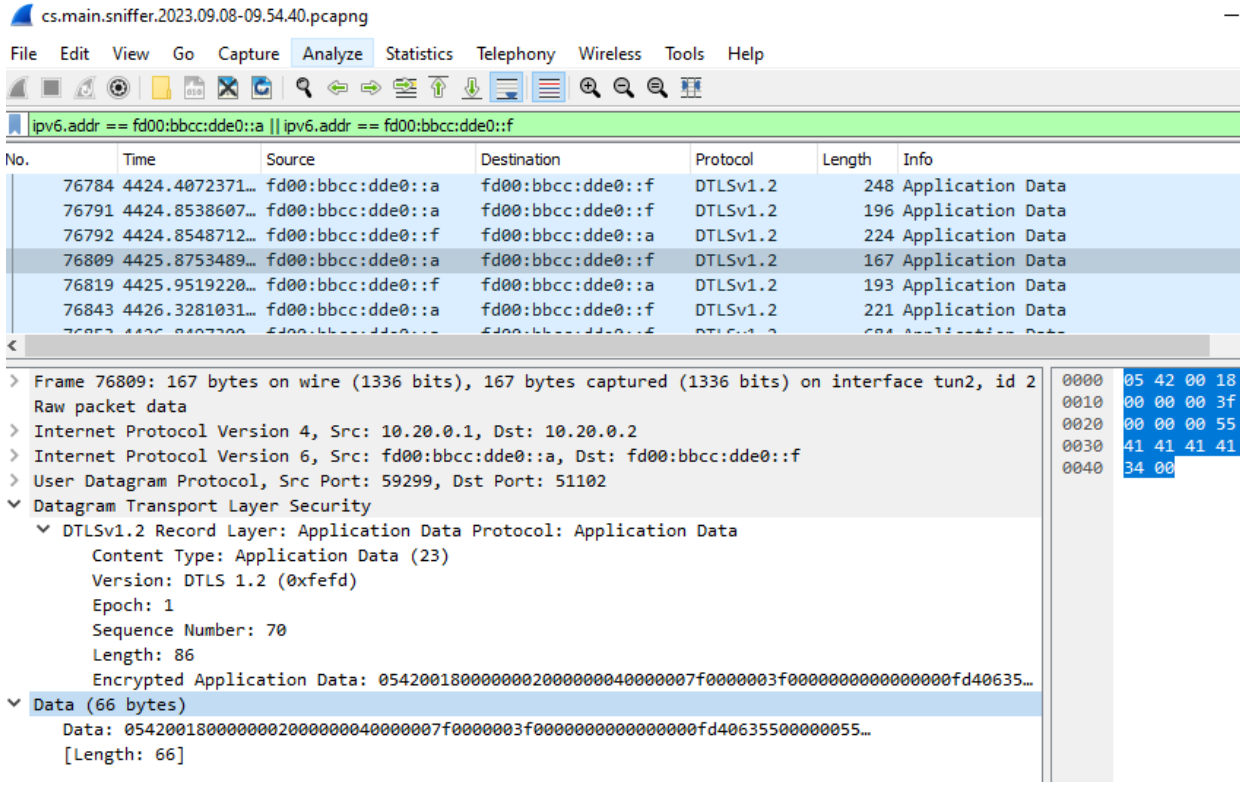
3	SER-02	VERIFY	CS and UA DTSR Live Log	User Data received matches User Data sent	Verify the received User Data message has the same contents as the one that was sent

CS DTSR
2023-09-08 16:08:26.844668 GMT DEBUG InputMessage.cpp:161
Received 66 bytes of data from User Input
User Input: Expected message size is 66 bytes
User Input Buffer Contents: [0542001800000002 000000040000007f 0000003f00000000
00000000fd406355 00000055442d4141 4141414141414141 4141414141414141 41412d3030303032 3400]
Processing USER_DATA.REQ
Sent "ID: 00000024 Origin: DTSR-UA Cmd: SEND Size: 63 Rsp: FALSE Data:
UD-AAAAAAAAAAAAAAAAAAA-000024" to udmd_queue

STEP	REQ	Action	Component	Description	Procedure
4	SER-02	VERIFY	CS Main Sniffer	User Data is not encrypted and authentication tag is at least 64 bits	Verify via the traffic sniffer log that: a) User Data is not encrypted (i.e., plaintext data is visible in the log) b) User Data messages contains an authentication tag that's least 64 bits

CS Sniffer log in step 2 shows data is not encrypted; the message is sent in the clear in binary.

b) The payload is 86 bytes long, while the message is only 66 bytes long. The other 20 bytes is the tag. The registered NULL cipher suite invokes the user of HMAC with the SHA-1 hash algorithm which produces a non-truncated 20 byte (160 bit) authentication tag.

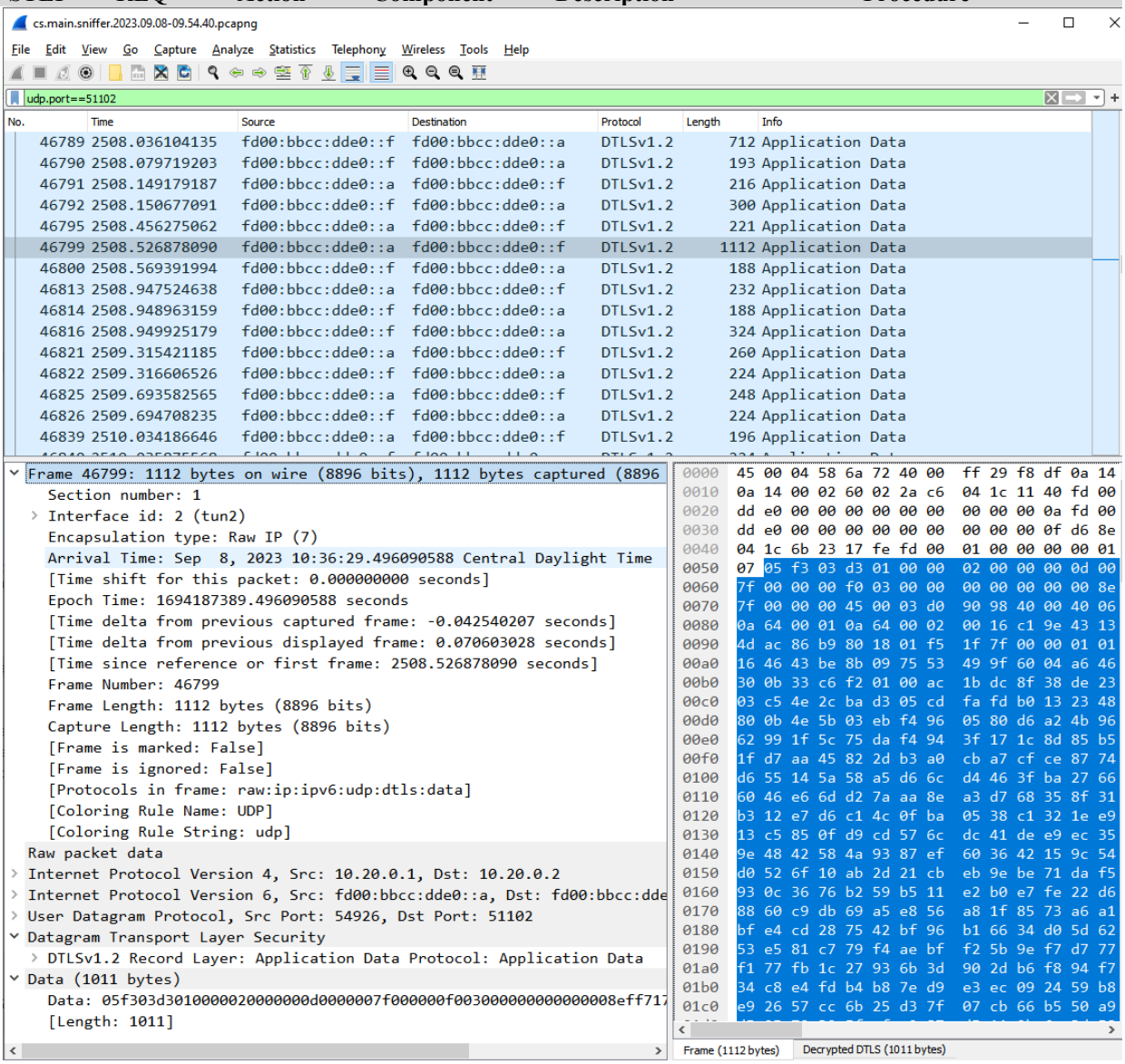


A.1.5.2 TP_CM_005B – USER DATA EXCHANGES WITHOUT ENCRYPTION, PAYLOAD DATA > MTU

Procedure:

STEP	REQ	Action	Component	Description	Procedure
1	IR-09b	SEND	CS OS Console	Send a User Data greater than MTU size	`scp uas-user@ua:validation-logs/TP-CM-005B.txt validation-logs/TP-CM-005B-2.txt`
2	IR-09b	VERIFY	CS Main Sniffer	User Data > MTU is segmented	Verify via the traffic sniffer log that User Data was segmented

STEP	REQ	Action	Component	Description	Procedure



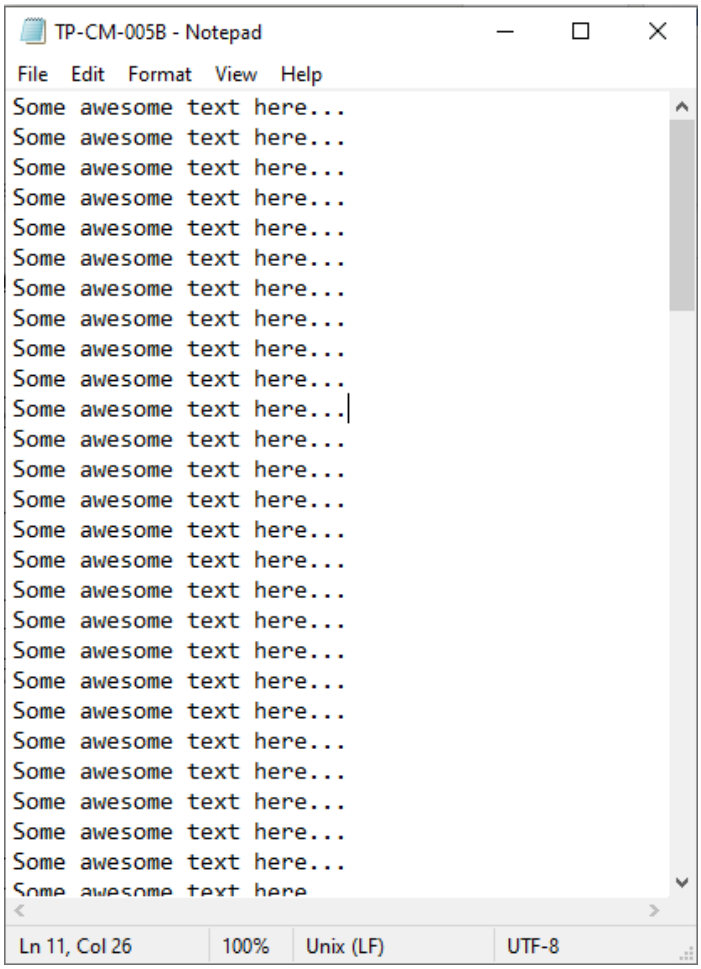
CS Sniffer shows messages of max length 1112 for the duration of the file transfer.
The payload data shows encrypted because it was transferred using Secure Copy Protocol (SCP), even though the link was not encrypted.

Post-test Log Analysis

3	SER-02	VERIFY	UA and CS Content Directory	User Data received matches User Data sent which indicates the message was accepted as authentic.	Compare the received User Data file with the source User Data file on the UA to show that the sent and received contents are the same

STEP	REQ	Action	Component	Description	Procedure

Text file sent and received matches.

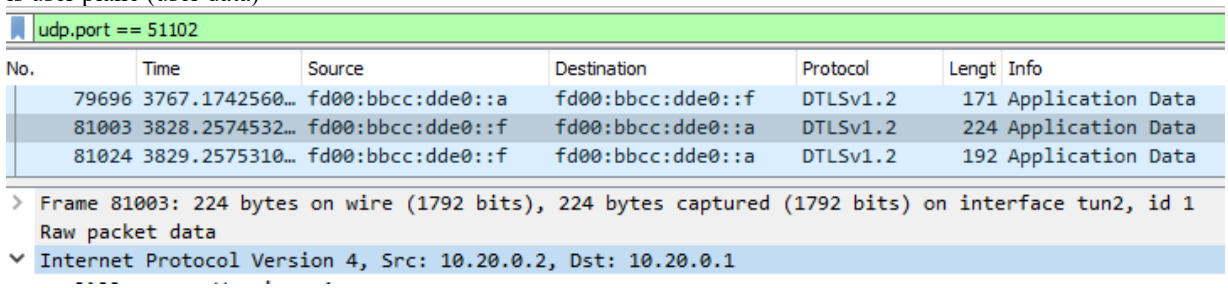


A.1.6 TP_CM_006 – User Data and Control Message Exchange with interruption < TET

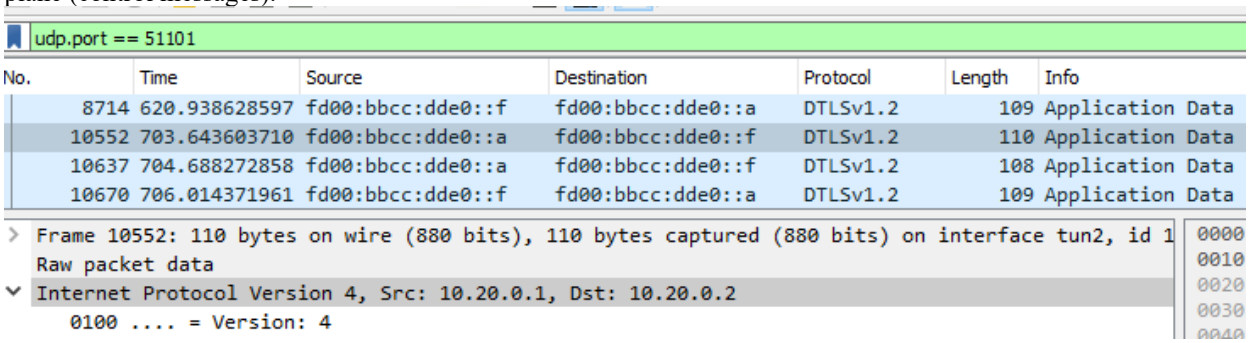
STEP	REQ	Action	Component	Description	Procedure
1		VERIFY	CS Main Sniffer	Control Messages are sent and User Data messages are received over the active link	Verify via the traffic sniffer log that: a) Verify that the User Data messages are only received via the link supporting the active connection b) Verify that Control Messages are sent to the UA via the link supporting the active Connection

STEP	REQ	Action	Component	Description	Procedure

Source address 10.20.0.2 is the CS on LTE; destination address of 10.20.0.1 is the UA on LTE. Udp.port 51102 is user plane (user data)



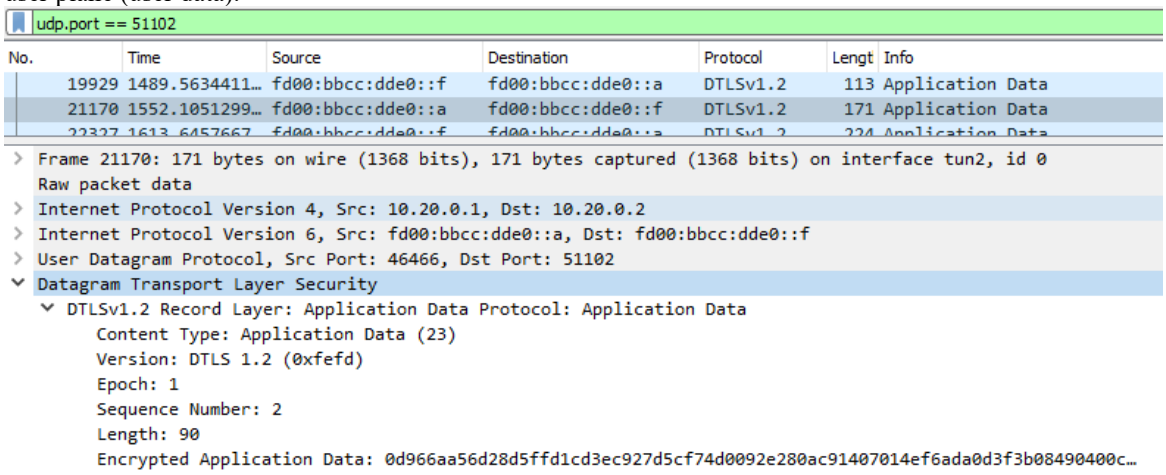
Source address 10.20.0.2 is CS on LTE; destination address 10.20.0.1 is UA on LTE. Udp port 51101 is control plane (control messages).



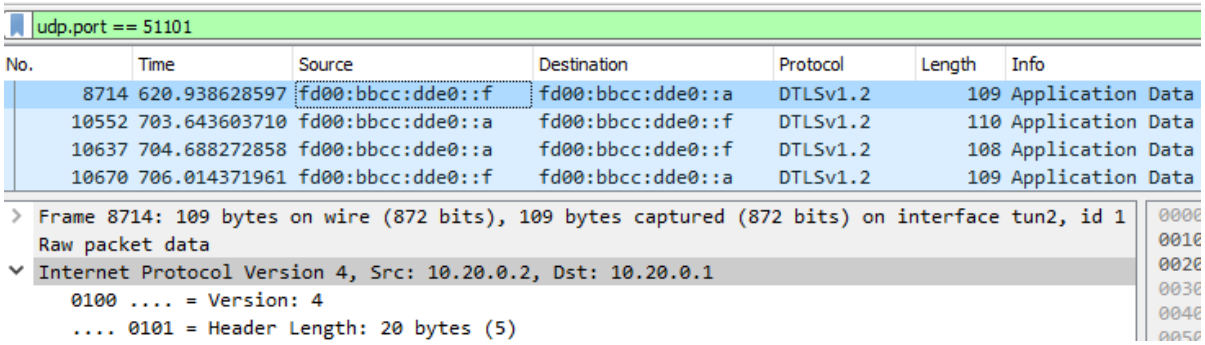
2		VERIFY	UA Main Sniffer	Control Messages are sent and User Data messages are received over the active link	Verify via the traffic sniffer log that: a) Verify that the User Data messages are only received via the link supporting the active connection b) Verify that the Control Data Messages are received by the UA via the link supporting the active Connection

STEP	REQ	Action	Component	Description	Procedure

Source address 10.20.0.1 is the UA on LTE; destination address 10.20.0.2 is the CS on LTE; Udp port 51102 is user plane (user data).



Source address 10.20.0.2 is CS on LTE; destination address of 10.20.0.1 is UA on LTE. Udp port 51101 is control plane (control messages)



3	IR-10	INVOKE	CS OS Console	Interrupt the Secure Connection between UA & CS DTSR for a time < TET	`disable_link <ID>` `enable_link <ID>`

4	IR-10	VERIFY	UA or CS LMSF Console	CS status shows:
				…secure session is established
				…the same link is providing the connection after the interruption
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/<ID> | Control: Y/<ID>`

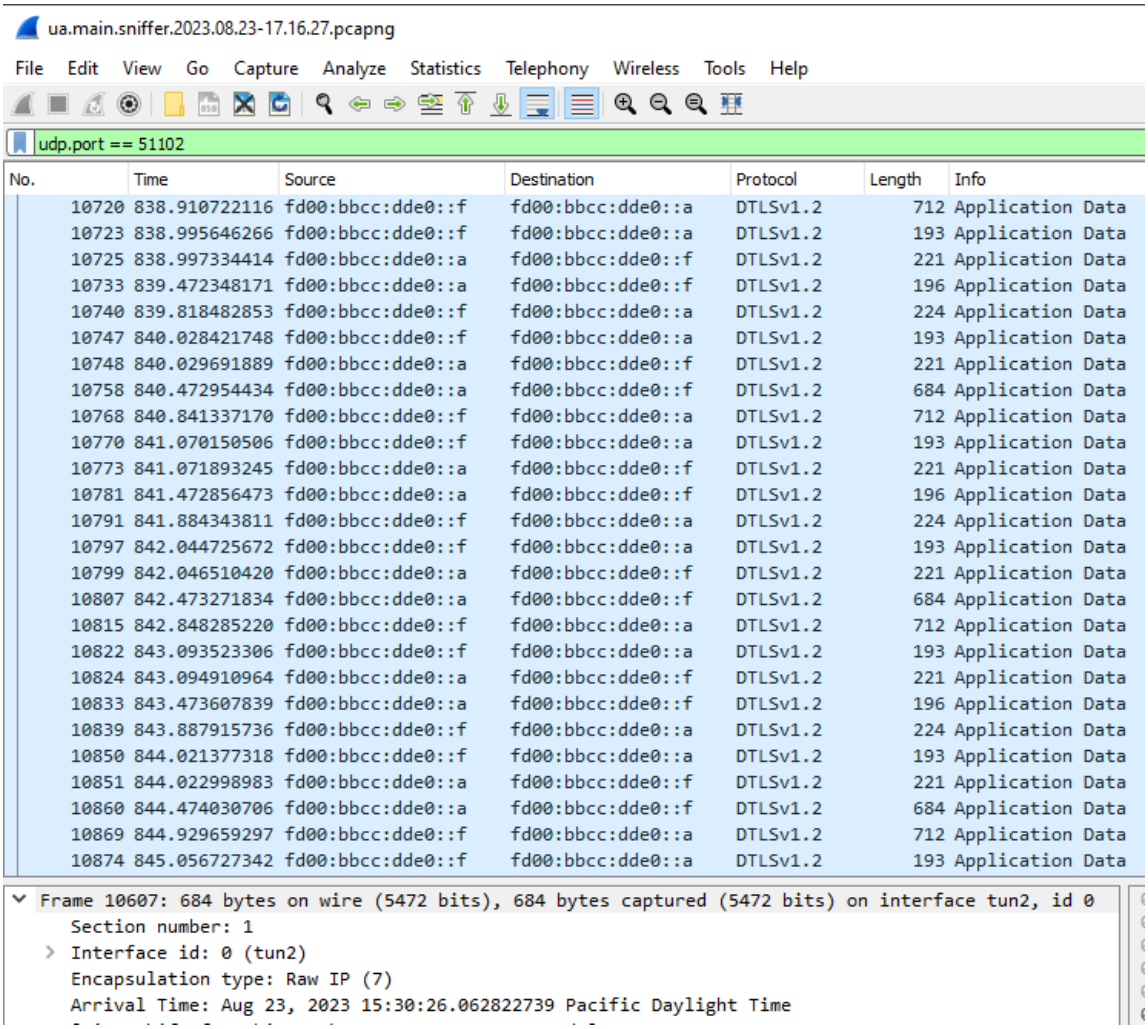
```
Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

Post-test Log Analysis

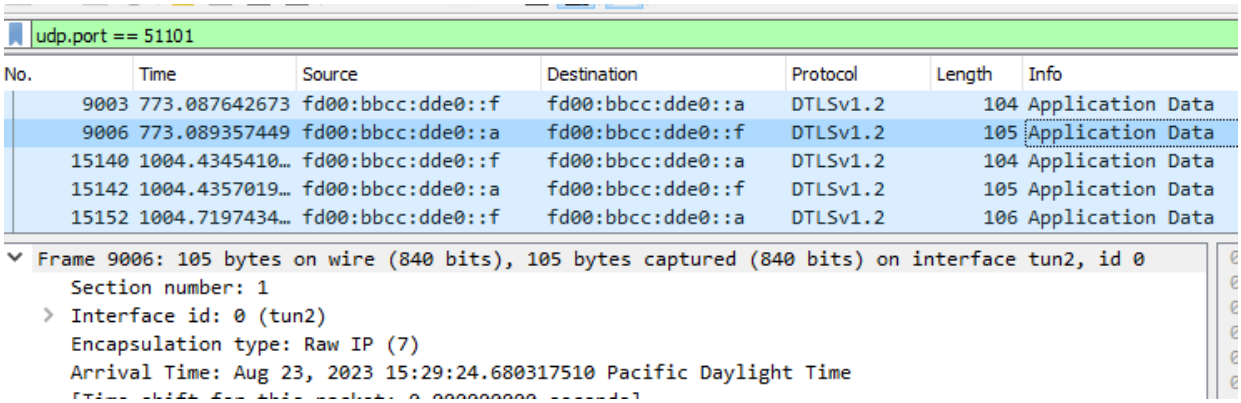
STEP	REQ	Action	Component	Description	Procedure
5	IR-10	VERIFY	UA and CS DTSR Inspect Log	Examine result of interruption < TET	Verify via the inspect logs that: a) the UA DTSR did not indicate an interruption > TET b) all User Data messages sent before and after the interruption are received c) all Control Messages sent are received

STEP	REQ	Action	Component	Description	Procedure

The UA Main Sniffer shows the user data messages are sent/received for the entirety of the interruption time.



Control plane messages continue for the length of the interruption.



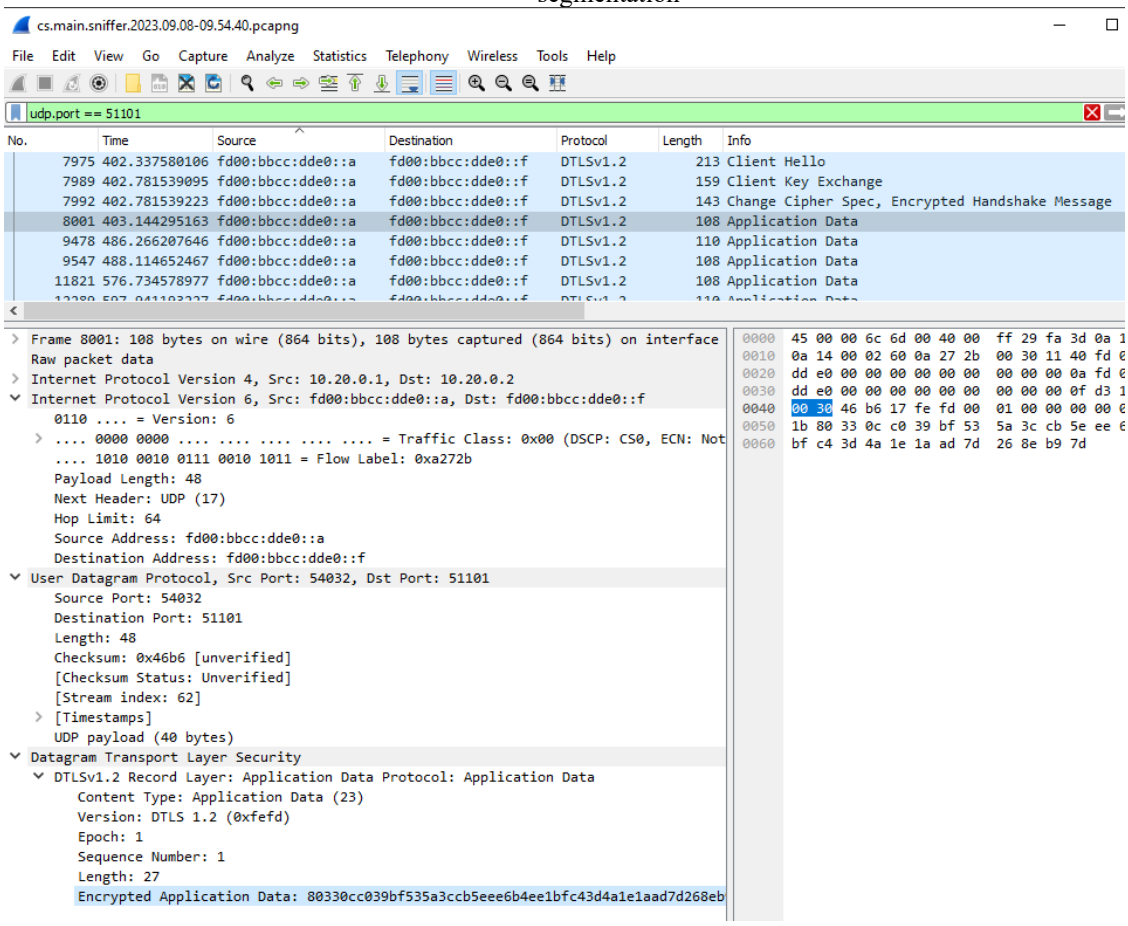
STEP	REQ	Action	Component	Description	Procedure
6	IR-10	VERIFY	CS DTSR Inspect logs	Examine result of interruption < TET	Verify via the inspect logs that: a) the CS DTSR did not indicate an interruption > TET b) all User Data and Control Messages are sent despite the interruption c) all User Data and Control Messages are received

No evidence of interruption in CS DTSR log for the entirety of the interruption.

Performance data shows all UA downlinks are sent for the duration of the interruption, and all CS uplinks are sent for the duration of the interruption.

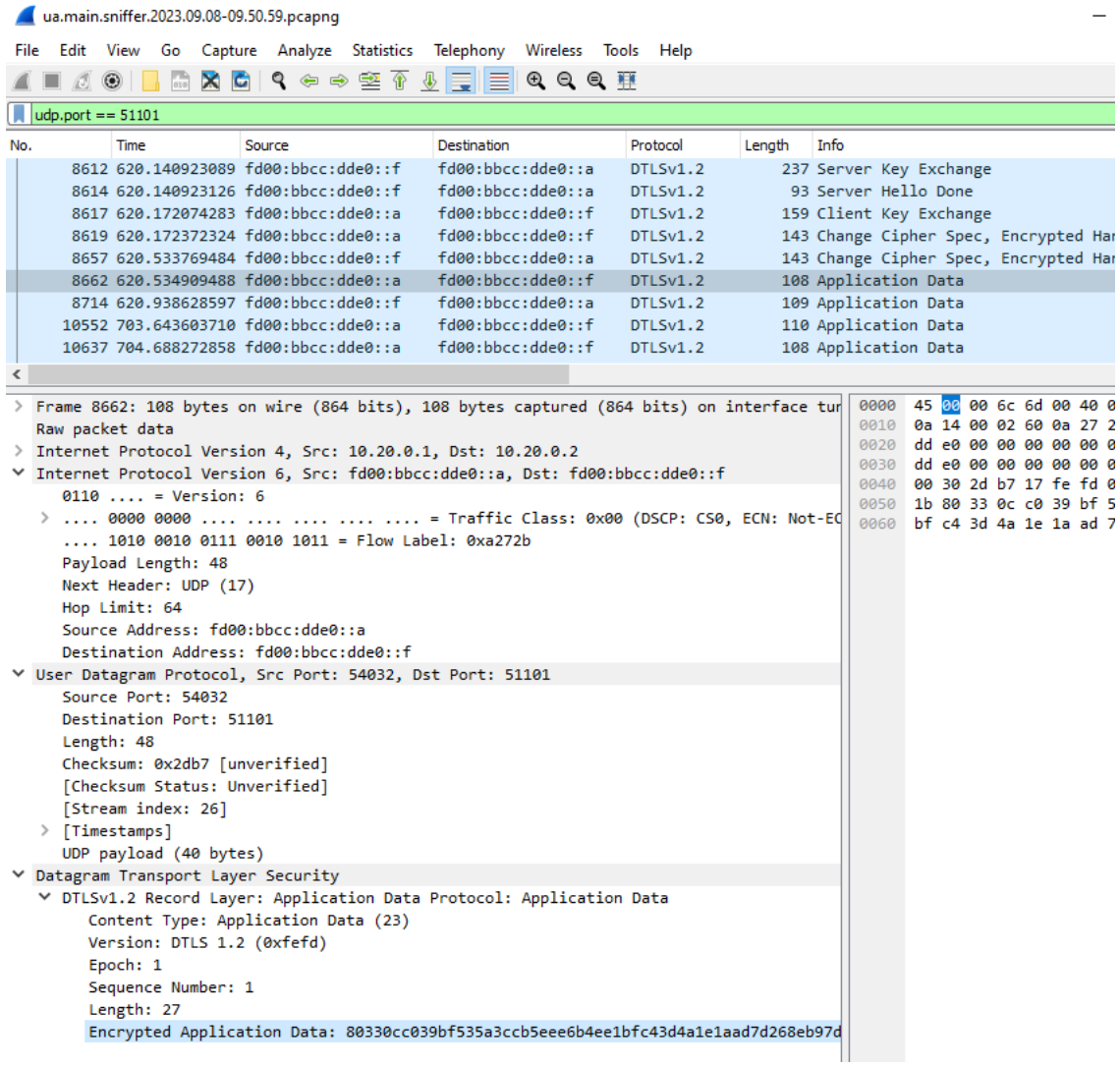
A.1.7 TP_CM_007 – Control Message Exchanges with Encryption

STEP	REQ	Action	Component	Description	Procedure
1	IR-09b	OBSERVE	CS DTSR Inspect Log	Status Reports are being sent	View the periodic Status Reports from the UA
2	IR-09b	VERIFY	CS Main Sniffer	Control Message < MTU does not require segmentation	Verify via the traffic sniffer log that segmentation does not occur



CS Main sniffer filtered on the control plane traffic (udp port 51101) shows messages are not segmented.

STEP	REQ	Action	Component	Description	Procedure
3	SER-09 SER-11	VERIFY	UA and CS Main Sniffers	Control Message received matches Control Message sent which indicates the message was accepted as authentic.	Compare the two sniffer logs to verify the received Control Message has the same contents as the one that was sent



Identical message is found in the UA Main sniffer.

4	SER-11	VERIFY	UA Main Sniffer	Control Message content cannot be discerned from the message in-transit (i.e., encrypted)	Verify via the traffic sniffer log that secure Control Message is transmitted

UA Main sniffer log shows application data is encrypted.

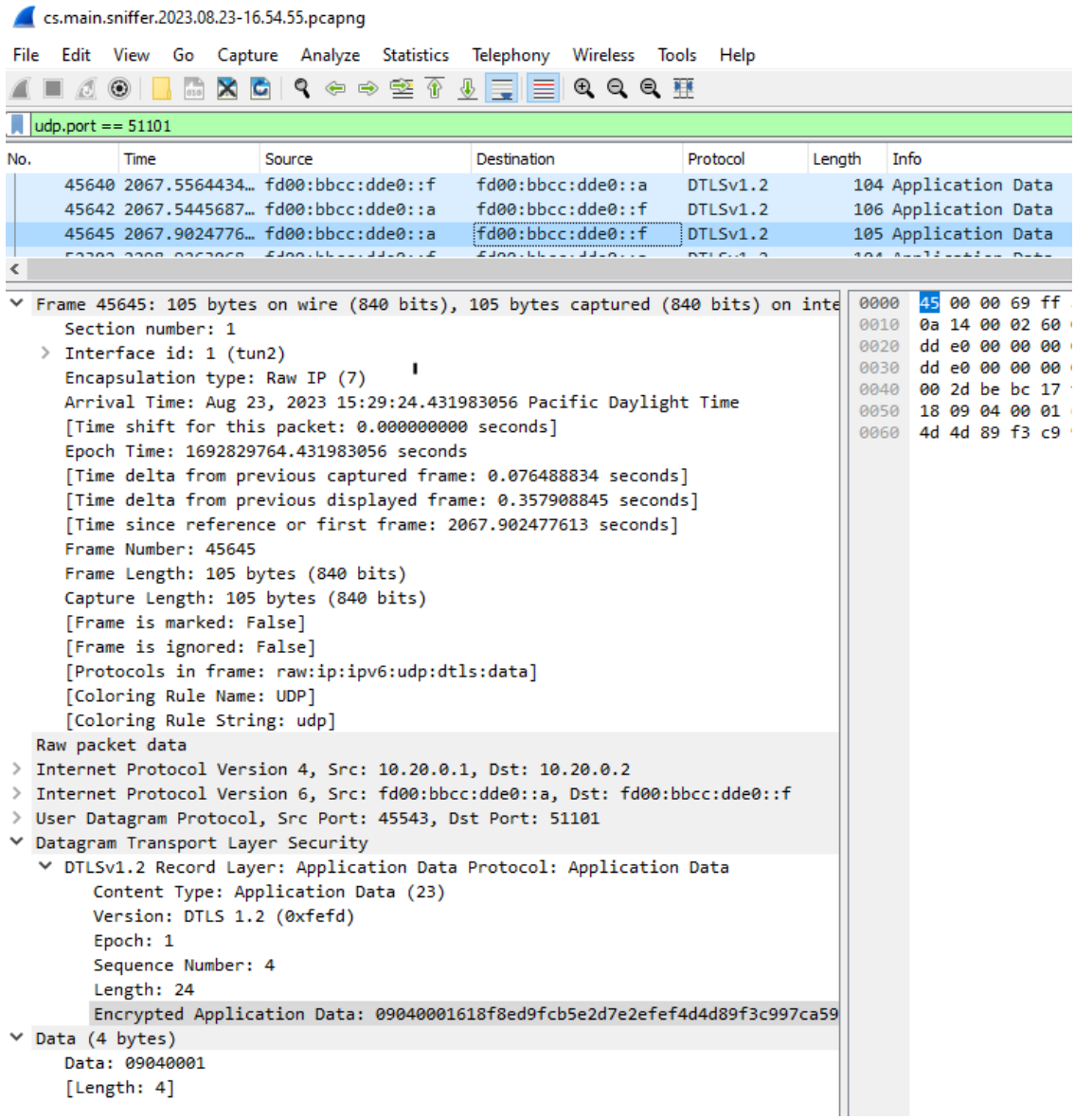
5	SER-11	VERIFY	CS Main Sniffer	Control Message content cannot be discerned from the message in-transit (i.e., encrypted)	Verify via the traffic sniffer log that the content of secure Control Message transmitted does not reveal content at the monitoring point

CS Main sniffer log shows application data is encrypted.

A.1.8 TP_CM_008 – Control Message Exchanges without Encryption

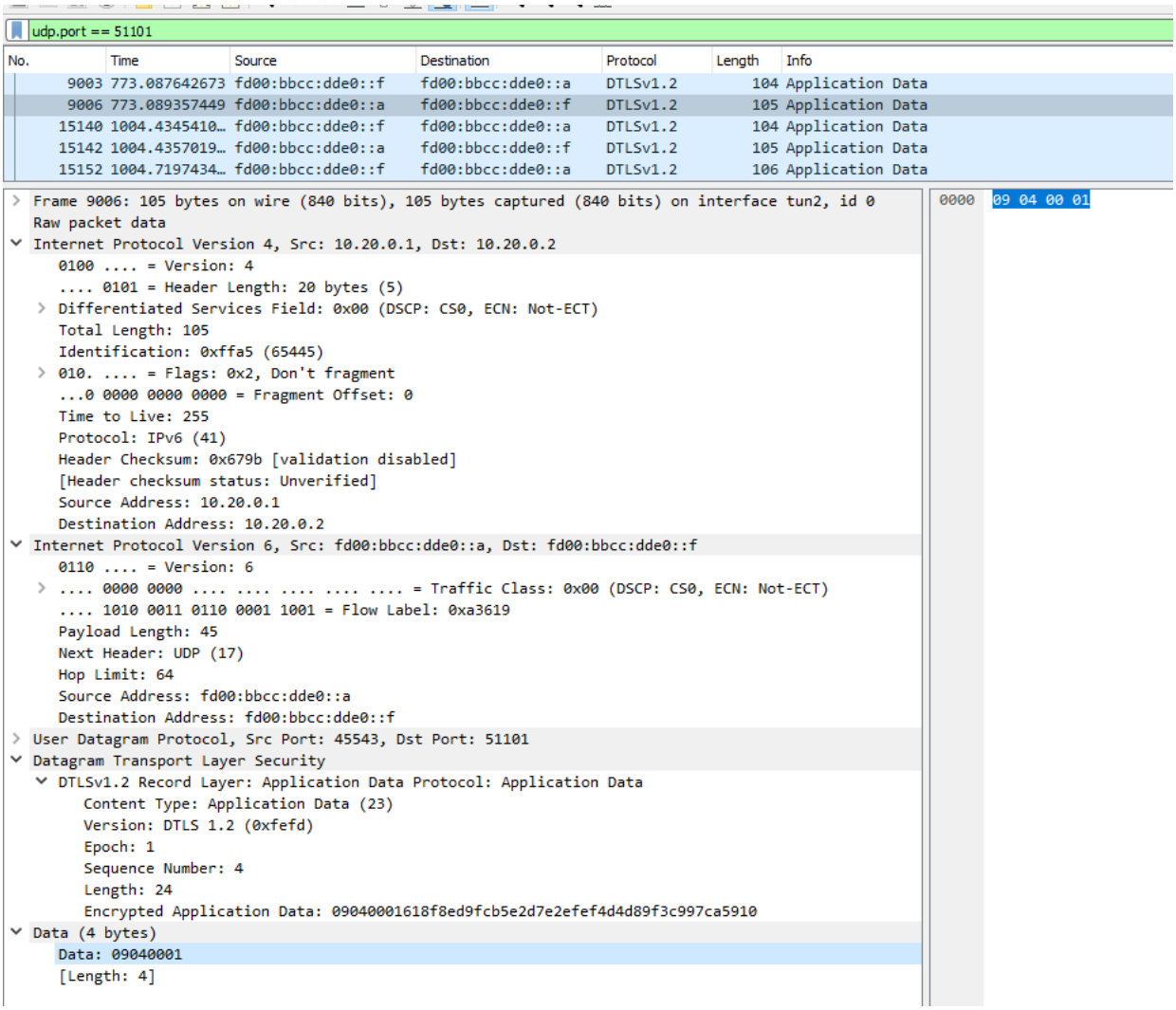
STEP	REQ	Action	Component	Description	Procedure
1	IR-09b	OBSERVE	CS DTSR Inspect Log	Status Reports are being sent	View the periodic Status Reports from the UA
2	IR-09b IR-02	VERIFY	CS Main Sniffer	Control Message < MTU does not require segmentation	Verify via the traffic sniffer log that: a) message segmentation does not occur for messages < MTU b) Control Messages include unique IP source and destination addresses that uniquely identify the UA and CS

CS Main Sniffer log shows control messages are not segmented (length is 105).
IPv6 addresses are unique. Fd00:bbcc:dde0::a is the UA DSTR; fd00:bbcc:dde0::f is the CS DTSR.



STEP	REQ	Action	Component	Description	Procedure
3	SER-09	VERIFY	CS and UA Main Sniffers	Control Message received matches Control Message sent which indicates the message was accepted as authentic.	Verify via the traffic sniffer logs that: a) the received Control Message has the same contents as the one that was sent b) the secure Control Message contains an authentication tag and the tag length is at least 64 bits

a) UA Main sniffer shows the exact same control message, where application data is 0904001.

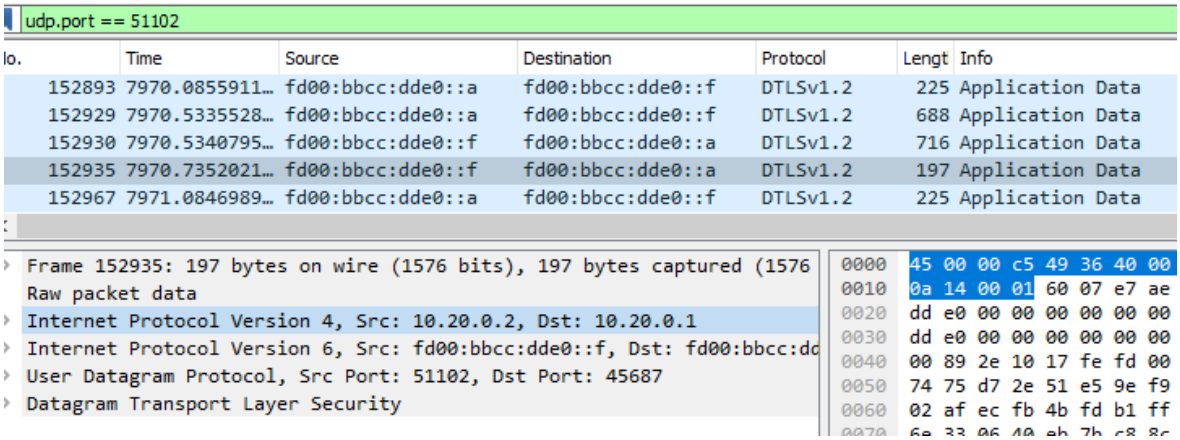


b) Above sniffer log shows the application data payload is 4 bytes; the remaining 20 bytes is the tag. The registered NULL cipher suite invokes the user of HMAC with the SHA-1 hash algorithm which produces a non-truncated 20 byte (160 bit) authentication tag.

A.1.9 TP_CM_009 – Link Switchover < TET

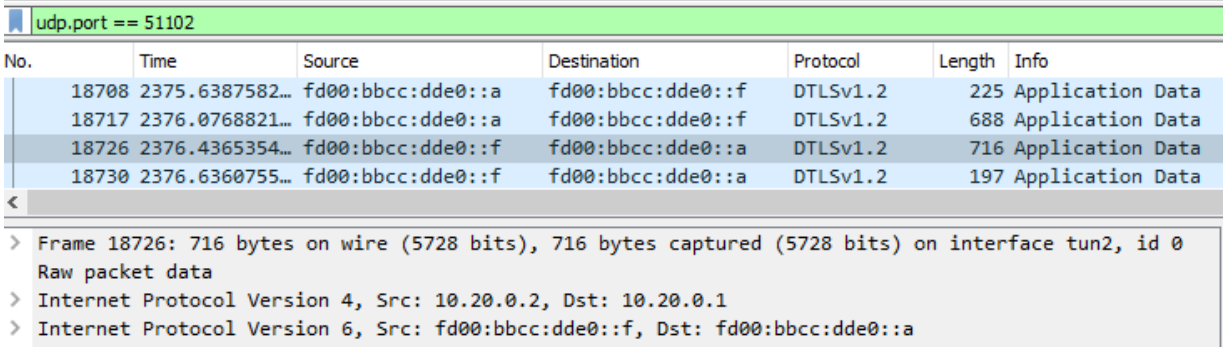
Example from Flight 2; LTE to SATCOM on Aug 24th at 1:07.

STEP	REQ	Action	Component	Description	Procedure
1	IR-04	VERIFY	CS Main Sniffer	Verify that User Data is sent over the active link	Verify via the traffic sniffer log that the User Data Messages are only sent by the CS via the link supporting the active Connection



Messages from the CS are sent from 10.20.0.2, which is LTE.

2	IR-04	VERIFY	UA Main Sniffer	Verify that User Data is received over the active link	Verify via the traffic sniffer log that the User Data Messages are only received by the UA via the link supporting the active Connection



Messages received by the UA have destination 10.20.0.1, which is LTE.

3	IR-08	OBSERVE	CS LMSF Console	View the status of all available links	`lmsf` `lmsf> status`
4	IR-08	OBSERVE	UA LMSF Console	View the status of all available links	`cs-sh lmsf` `lmsf> status`
5	IR-05	SEND	CS LMSF Console	Issue Switchover command for the desired alternate link	`lmsf` `lmsf> switch 1`

```
2023-08-24 18:07:56.279090 GMT INFO      ControlOut.cpp:294
Initiating switchover from 2 to 1
```

6	IR-06	OBSERVE	UA DTSR Live Log	Observe the Switchover and note the Switchover Time	Verify the start and end timestamps of the Switchover.
7	IR-06	OBSERVE	CS DTSR Live Log	Observe the Switchover and note the Switchover Time	Verify the start and end timestamps of the Switchover.

STEP	REQ	Action	Component	Description	Procedure

8	IR-05
	IR-07
	IR-10
		VERIFY	UA LMSF Console and DTSR Live Log	UA status shows:
				…secure session is established
				… which link is providing the connection
				…that the secure connection is maintained following the interruption
				…the UA DTSR did not indicate an interruption exceeding TET
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/1 | Control: Y/1`
					
					No indication that the interruption was greater than TET

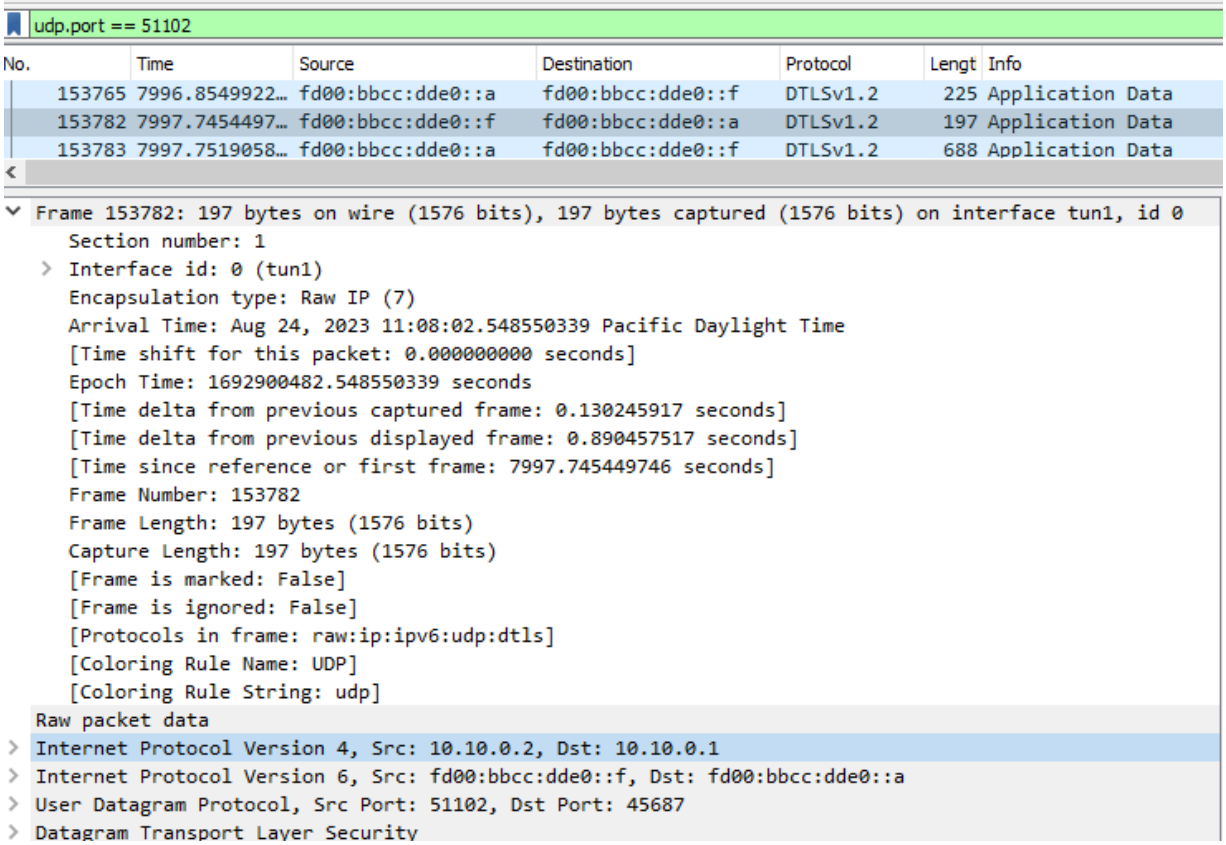
9	IR-05
	IR-07
	IR-10
		VERIFY	CS LMSF Console and DTSR Live Log	CS status shows:
				…secure session is established
				… which link is providing the connection
				…that the secure connection is maintained following the interruption
				…the CS DTSR did not indicate an interruption exceeding TET
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/1| Control: Y/1`
					
					No indication that the interruption was greater than TET

10	IR-04 IR-18 IR-19c	VERIFY	CS Main Sniffer	On the CS, verify: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data messages are sent to the UA only via the link supporting the active connection b) all exchanged messages include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links

```
2023-08-24 18:08:08.827965 GMT INFO Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

```
2023-08-24 18:08:17.860622 GMT INFO Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

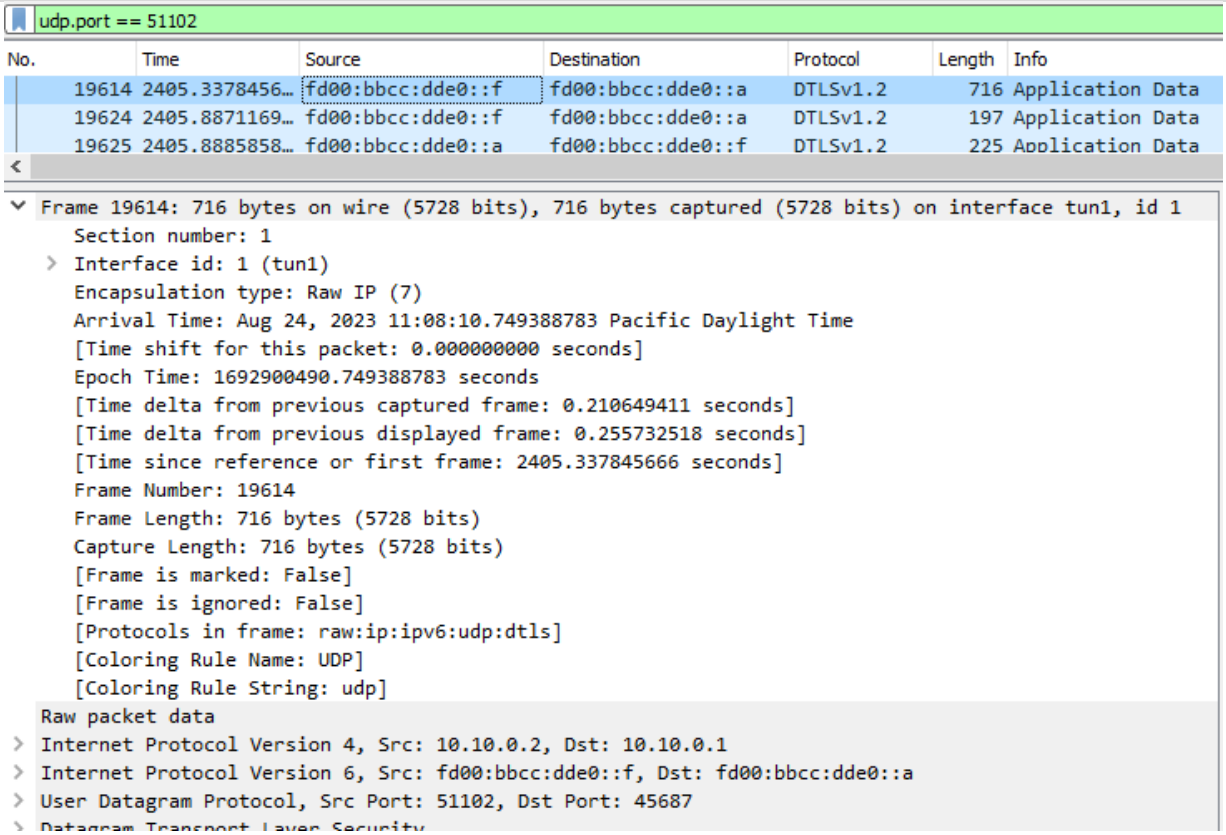
STEP	REQ	Action	Component	Description	Procedure



Source address is 10.10.0.2 which is the CS on SATCOM.

11	IR-04 IR-18 IR-19c	VERIFY	UA Main Sniffer	On the UA, verify: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data Messages are received by the UA only via the link supporting the active connection b) all exchanged messages include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links

STEP	REQ	Action	Component	Description	Procedure



Destination address is 10.10.0.1 which is the UA on SATCOM.

12	IR-20	VERIFY	UA DTSR Live Log and UA Main Sniffer	Verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	Verify via the traffic sniffer logs that: a) the Control Messages are the appropriate messages for a Network Layer Switchover b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)

2023-08-24 18:07:56.279071 GMT INFO ControlOut.cpp:291
Sent "SWITCHOVER_REQUEST.REQ 5 2 1" across secure connection

Successful switchover to LinkInfo: 1|Type: Satellite
Name: Satellite01|Address: 10.10.0.1|Adapter: tun1
Peer: 10.10.0.2|Status: Link Up

Sent "CONNECT.REQ 3 " across secure connection
Received "CONNECT.REQ 3 " over secure session
Sent "CONNECT.CNF 4 Accepted" across secure connection

STEP	REQ	Action	Component	Description	Procedure
13	IR-20	VERIFY	CS DTSR Live Log	Verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	Verify via the live log that: a) the Control Messages are the appropriate messages for a Network Layer Switchover b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)

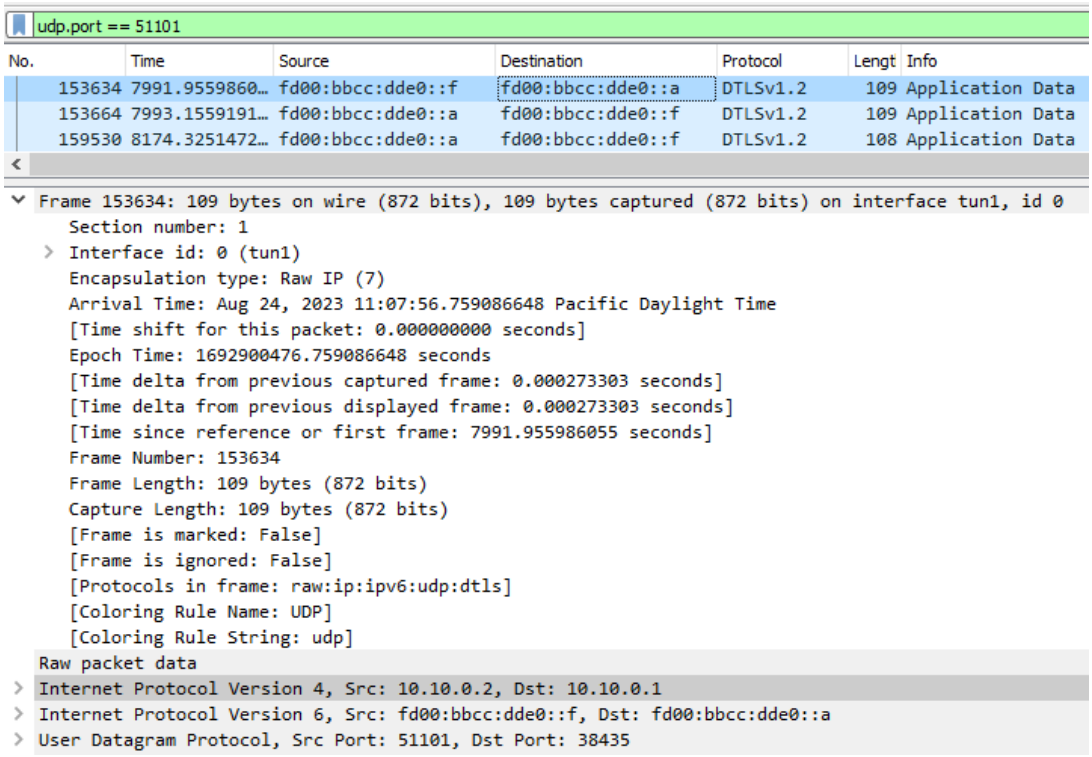
2023-08-24 18:07:56.142660 GMT INFO ControlIn.cpp:42
Received "SWITCHOVER_REQUEST.REQ 5 2 1" over secure session

2023-08-24 18:07:56.153734 GMT INFO LinkInfo.cpp:343
Successful switchover to LinkInfo: 1|Type: Satellite
Name: Satellite01|Address: 10.10.0.2|Adapter: tun1
Peer: 10.10.0.1|Status: Link Up

Sent "CONNECT.REQ 3 " across secure connection
Received "CONNECT.REQ 3 " over secure session
Sent "CONNECT.CNF 4 Accepted" across secure connection

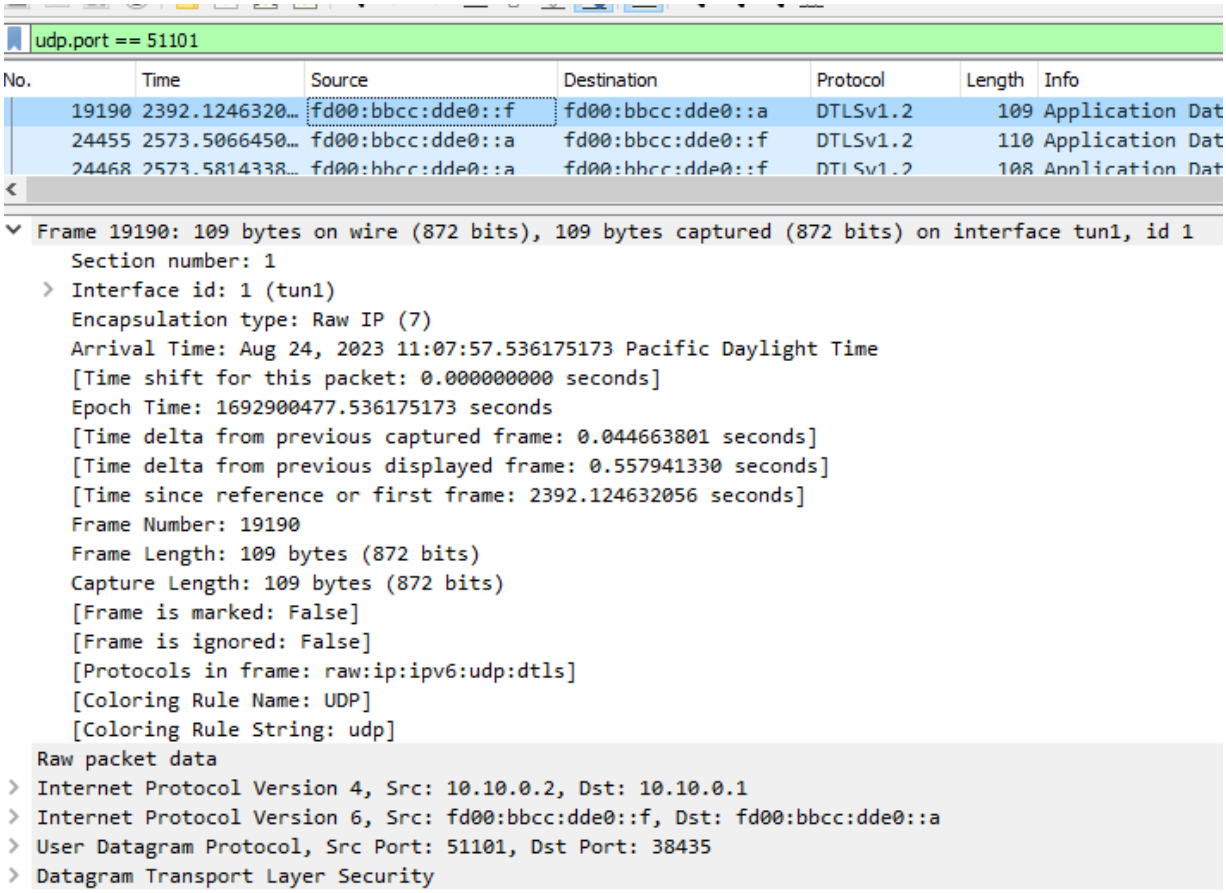
14	IR-21	VERIFY	UA DTSR Live Log	Verify User Data and Control Messages are exchanged over the new link and stop over the old link	Verify via live log that: a) User Data and Control Messages begin to be exchanged over the new Link b) no messages flow over the original link

User data looks like step 11.
Control messages are port 51101. Source address 10.10.0.2 is from the CS on SATCOM and destination address 10.10.0.1 is from the UA on SATCOM.



STEP	REQ	Action	Component	Description	Procedure
15	IR-21	VERIFY	CS DTSR Live Log	Verify User Data and Control Messages are exchanged over the new link and stop over the old link	Verify via live log that: a) User Data and Control Messages begin to be exchanged over the new Link b) no messages flow over the original link

User data looks like step 10.
Control messages are port 51101. Source address 10.10.0.2 is from the CS on SATCOM and destination address 10.10.0.1 is from the UA on SATCOM.



16	IR-06	VERIFY	CS DTSR Live Log	Verify the Switchover Time is less than the TET for a Scheduled MbB Switchover	Verify the Switchover time is less than TET for a Scheduled MbB Switchover

UA DTSR:
2023-08-24 18:07:56.977766 GMT INFO SessionManager.cpp:477 SWITCH completed in 699 ms
CS DTSR:
2023-08-24 18:07:56.758932 GMT INFO SessionManager.cpp:477 SWITCH completed in 616 ms

A.1.10 TP_CM_010 – Link Switchover > TET with Link Recovery

STEP	REQ	Action	Component	Description	Procedure
1	IR-04	VERIFY	CS Main Sniffer	Verify that User Data is sent over the active link	Verify via the traffic sniffer log that the User Data Messages are only sent by the CS via the link supporting the active Connection
Verification looks the same as step 1 of TP_CM_009; not repeating for conciseness.					
2	IR-04	VERIFY	UA Main Sniffer	Verify that User Data is received over the active link	Verify via the traffic sniffer log that the User Data Messages are only received by the UA via the link supporting the active Connection
Verification looks the same as step 2 of TP_CM_009; not repeating for conciseness.					
3	IR-08	OBSERVE	CS LMSF Console	View the status of all available links	`lmsf` `lmsf> status`
4	IR-08	OBSERVE	UA LMSF Console	View the status of all available links	`cs-sh lmsf` `lmsf> status`

5	IR-05	INVOKE	CS OS Console	Initiate a Switchover for the desired alternate link using a switchover time greater than TET	`disable_link 1`
					`disable_link 2`
					`disable_link 3`

6	IR-05	WAIT	CS Operator	"	Time greater than TET passes

7	IR-05	INVOKE	CS OS Console	"	`enable_link 1`
					`enable_link 2`
					`enable_link 3`

8	IR-08	OBSERVE	CS DTSR Live Log	Status indication that Lost C2 Link state has been declared	Observe notification indicating Lost C2 Link
9	IR-06	OBSERVE	UA DTSR Live Log	Observe the Switchover and note the Switchover Time	Verify the start and end timestamps of the Switchover.
10	IR-06	OBSERVE	CS DTSR Live Log	Observe the Switchover and note the Switchover Time	Verify the start and end timestamps of the Switchover.

11	IR-05
	IR-07
	IR-10
		VERIFY	UA LMSF Console and DTSR Live Log	UA status shows:
				…secure session is established
				…the link has changed to the specified link
				…the UA DTSR indicated an interruption exceeding TET
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/<ID> |`
					`Control: Y/<ID>`
					
					Indication that interruption was greater than TET

STEP	REQ	Action	Component	Description	Procedure
2023-09-06 19:55:02.831204 GMT Secure Link Detailed Status: userOut enabled: 1 controlOut enabled: 1 user plane: CONNECTED control plane: CONNECTED					

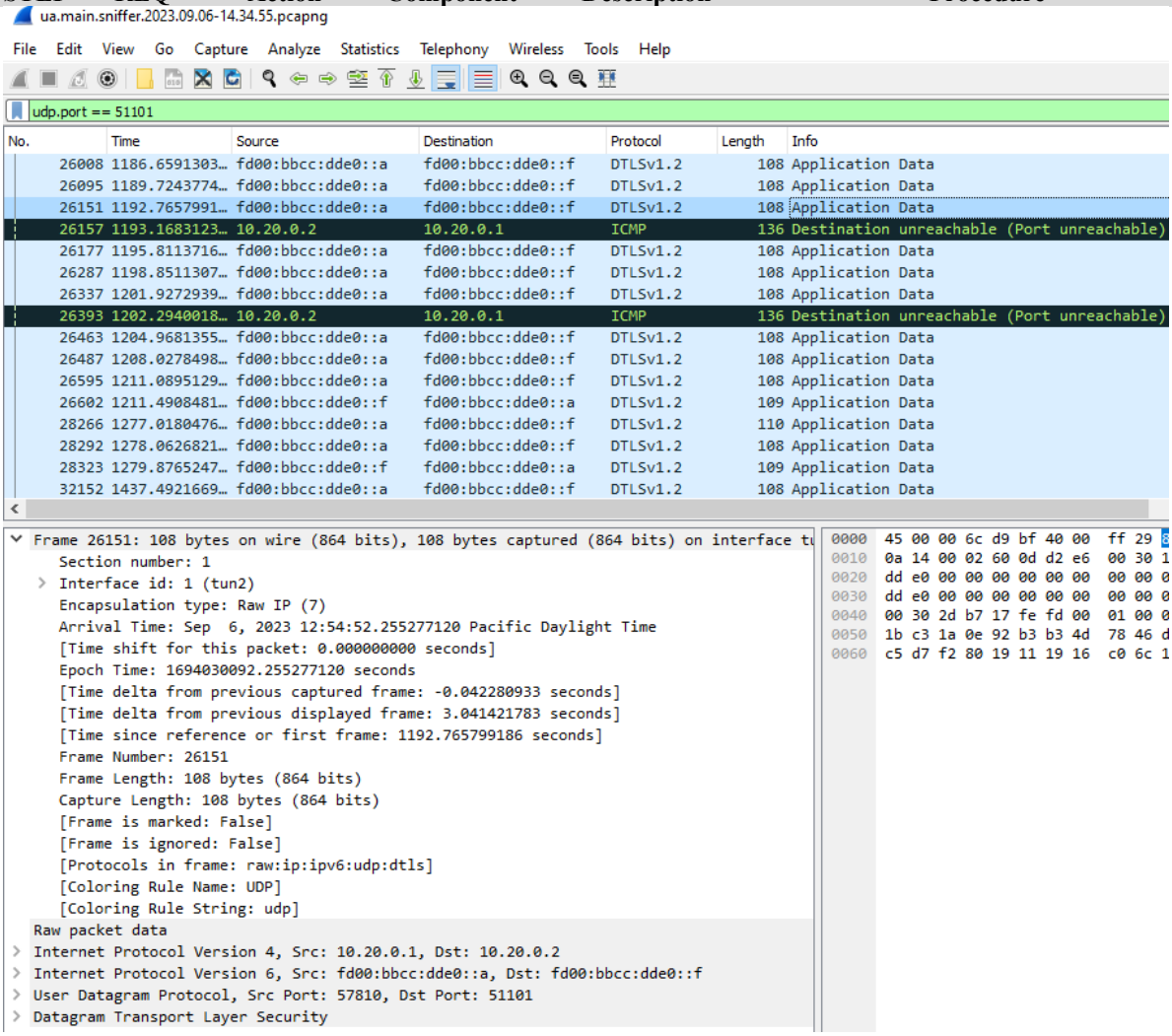
12	IR-05
	IR-07
	IR-10
		VERIFY	CS LMSF Console and DTSR Live Log	CS status shows:
				…secure session is established
				…the link has changed to the specified link
				…the CS DTSR indicated an interruption exceeding TET
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/<ID> | Control: Y/<ID>`
					
					Indication that interruption was greater than TET

2023-09-06 19:55:12.591624 GMT Secure Link Detailed Status: userOut enabled: 1 controlOut enabled: 1 user plane: CONNECTED control plane: CONNECTED					
13	IR-04 IR-18 IR-19c	VERIFY	CS Main Sniffer	On the CS, verify: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data messages are sent to the UA only via the link supporting the active connection b) all exchanged messages include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links
This verification step looks the same as step 10 of TP_CM_009; not repeating here for conciseness.					
14	IR-04 IR-18 IR-19c	VERIFY	UA Main Sniffer	On the UA, verify: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data Messages are received by the UA only via the link supporting the active connection b) all exchanged messages include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links
This verification step looks the same as step 11 of TP_CM_009; not repeating here for conciseness.					
15	IR-20	VERIFY	UA DTSR Live Log	Verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	Verify via live log that: a) the Control Messages are the appropriate messages for a Network Layer Switchover based on the messages. b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)

a) Control messages are shown in UA DTSR log.
2023-09-06 19:54:35.911741 GMT LIVE_VALIDATION LinkManager.cpp:213
Lost link for secure connection. Sending switch command.
Switch timer started
Initiating lost-link switchover0
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ 3
Switchover Innitiator Task: sent CONNECT_REQ over link 3
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ 3
Switchover Innitiator Task: sent CONNECT_REQ over link 1
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ 3
Switchover Innitiator Task: sent CONNECT_REQ over link 2
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ 3
Switchover Innitiator Task: sent CONNECT_REQ over link 3
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ 3
Switchover Innitiator Task: sent CONNECT_REQ over link 1
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ 3
Switchover Innitiator Task: sent CONNECT_REQ over link 2
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ 3
Switchover Innitiator Task: sent CONNECT_REQ over link 3
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ 3
Switchover Innitiator Task: sent CONNECT_REQ over link 1
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ 3
Switchover Innitiator Task: sent CONNECT_REQ over link 2
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ 3
Switchover Innitiator Task: sent CONNECT_REQ over link 3
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ 3
Switchover Innitiator Task: sent CONNECT_REQ over link 1
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ 3
Switchover Innitiator Task: sent CONNECT_REQ over link 2
CONTROL PLANE: CONNECT.CNF 4 Accepted[09040001]<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Received CONNECT.CNF. New link:

b) UA User Sniffer shows DTLS session is maintained for the duration of the connection disruption; no DTLS errors are logged.

STEP	REQ	Action	Component	Description	Procedure



16	IR-20	VERIFY	CS DTSR Live Log	Verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	Verify via live log that: a) the Control Messages are the appropriate messages for a Network Layer Switchover based on the messages b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)

a) CS DTSR log shows control messages exchanged.

```
2023-09-06 19:54:37.521032 GMT LIVE_VALIDATION LinkManager.cpp:213
Lost link for secure connection.  Sending switch command.
SWITCH timer started
Initiating lost-link switchover0
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
CONTROL PLANE: CONNECT.REQ          3   Processing suceeded.
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
CONTROL PLANE: CONNECT.REQ          3   Processing suceeded.
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
CONTROL PLANE: CONNECT.REQ          3   Processing suceeded.
CONTROL PLANE: CONNECT.CNF          4    Accepted[09040001]<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

b) CS Main Sniffer shows DTLS session is maintained for the duration of the connection disruption; no DTLS errors are logged.

STEP	REQ	Action	Component	Description	Procedure

cs.main.sniffer.2023.09.06-14.35.45.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 51101

	Time	Source	Destination	Protocol	Length	Info
22965	1144.4333162…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	108	Application Data
23007	1146.3871420…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	108	Application Data
23008	1146.3871686…	10.20.0.2	10.20.0.1	ICMP	136	Destination unreachab
23069	1149.5319225…	10.30.0.2	10.30.0.1	ICMP	150	Destination unreachab
23076	1149.5319014…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	108	Application Data
23156	1152.9332243…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	108	Application Data
23224	1155.5469247…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	108	Application Data
23225	1155.5469676…	10.20.0.2	10.20.0.1	ICMP	136	Destination unreachab
23356	1159.6008086…	10.30.0.2	10.30.0.1	ICMP	150	Destination unreachab
23359	1159.6007030…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	108	Application Data
23416	1162.0424587…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	108	Application Data
23418	1162.0424868…	10.10.0.2	10.10.0.1	ICMP	150	Destination unreachab
23462	1164.7129113…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	108	Application Data
23463	1164.7138708…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	109	Application Data
24876	1230.6248111…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	110	Application Data

```
Frame 23007: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on inte
   Section number: 1
   Interface id: 2 (tun2)
   Encapsulation type: Raw IP (7)
   Arrival Time: Sep  6, 2023 12:54:52.422426110 Pacific Daylight Time
   [Time shift for this packet: 0.000000000 seconds]
   Epoch Time: 1694030092.422426110 seconds
   [Time delta from previous captured frame: 0.201496985 seconds]
   [Time delta from previous displayed frame: 1.953825823 seconds]
   [Time since reference or first frame: 1146.387142035 seconds]
   Frame Number: 23007
   Frame Length: 108 bytes (864 bits)
   Capture Length: 108 bytes (864 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: raw:ip:ipv6:udp:dtls]
   [Coloring Rule Name: UDP]
   [Coloring Rule String: udp]
Raw packet data
Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
User Datagram Protocol, Src Port: 57810, Dst Port: 51101
Datagram Transport Layer Security
```

```
0000  45 00 00 6c d9 b
0010  0a 14 00 02 60 0
0020  dd e0 00 00 00 0
0030  dd e0 00 00 00 0
0040  00 30 6d 1a 17 f
0050  1b c3 1a 0e 92 b
0060  c5 d7 f2 80 19 1
```

17	IR-21	VERIFY	UA Main Sniffer	Verify User Data and Control Messages are exchanged over the new link and stop over the old link	Verify via the traffic sniffer log that: a) User Data and Control Messages begin to be exchanged over the new Link b) no messages flow over the original link

The verification for this step looks the same as step 15 from TP_CM_009; not repeating for conciseness.

STEP	REQ	Action	Component	Description	Procedure
18	IR-21	VERIFY	CS Main Sniffer	Verify User Data and Control Messages are exchanged over the new link and stop over the old link	Verify via the traffic sniffer log that: a) User Data and Control Messages begin to be exchanged over the new Link b) no messages flow over the original link
The verification for this step looks the same as step 16 from TP_CM_009; not repeating for conciseness.					
19	IR-06	VERIFY	CS DTSR Live Logs	Verify the Switchover Time is greater than the TET for a Scheduled MbB Switchover	Verify the Switchover time is greater than TET for a Scheduled MbB Switchover

UA DSTR:
2023-09-06 19:55:10.981102 GMT SWITCH completed in 35068 ms. Switchover TET set at 3000 ms.

CS DTSR:
2023-09-06 19:55:10.748371 GMT SWITCH completed in 33227 ms. Switchover TET set at 3000 ms.

A.1.11 TP_CM_011 – Control Plane and User Plane Traffic Link Termination

STEP	REQ	Action	Component	Description	Procedure

1	IR-07	VERIFY	CS LMSF console	CS status shows:
				…secure session is established
				…which link is providing the connection
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/<ID> | Control: Y/<ID>`

```
2023-08-24 18:15:02.880590 GMT Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

2	IR-07	VERIFY	UA LMSF console	UA status shows:
				…secure session is established
				…which link is providing the connection
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/<ID> | Control: Y/<ID>`

```
2023-08-24 18:14:34.141313 GMT Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

3	IR-04	VERIFY	CS Main Sniffer	User Data is sent over the active link	Verify via the traffic sniffer log that the User Data Messages are only sent to the UA via the link supporting the active Connection

STEP	REQ	Action	Component	Description	Procedure

udp.port == 51102

No.	Time	Source	Destination	Protocol	Lengt	Info
164930	8354.9033019…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	197	Application Data
164935	8355.2507989…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	225	Application Data
164944	8355.6915448…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	200	Application Data
164945	8355.6923926…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	228	Application Data
164951	8355.9039894…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	197	Application Data

```
Frame 164945: 228 bytes on wire (1824 bits), 228 bytes captured (1824 bits) on interface tun2, id 1
    Section number: 1
  > Interface id: 1 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 24, 2023 11:14:00.495493267 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1692900840.495493267 seconds
    [Time delta from previous captured frame: 0.000847823 seconds]
    [Time delta from previous displayed frame: 0.000847823 seconds]
    [Time since reference or first frame: 8355.692392674 seconds]
    Frame Number: 164945
    Frame Length: 228 bytes (1824 bits)
    Capture Length: 228 bytes (1824 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:ipv6:udp:dtls]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dde0::a
> User Datagram Protocol, Src Port: 51102, Dst Port: 45687
> Datagram Transport Layer Security
```

Source 10.20.0.2 is the CS on LTE

4	IR-04	VERIFY	UA Main Sniffer	User Data is received over the active link	Verify via the traffic sniffer log that the User Data Messages are only received via the link supporting the active Connection

STEP	REQ	Action	Component	Description	Procedure

udp.port == 51102

No.	Time	Source	Destination	Protocol	Length	Info
29441	2754.6323237…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	716	Application Data
29446	2754.7918463…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	197	Application Data
29448	2754.7926903…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	225	Application Data
29456	2755.2000159…	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	200	Application Data
29464	2755.5567013…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	228	Application Data
29472	2755.7888555…	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	197	Application Data

```
Frame 29446: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits) on interface tun2, id 0
   Section number: 1
   Interface id: 0 (tun2)
   Encapsulation type: Raw IP (7)
   Arrival Time: Aug 24, 2023 11:14:00.203389510 Pacific Daylight Time
   [Time shift for this packet: 0.000000000 seconds]
   Epoch Time: 1692900840.203389510 seconds
   [Time delta from previous captured frame: 0.000071824 seconds]
   [Time delta from previous displayed frame: 0.159522640 seconds]
   [Time since reference or first frame: 2754.791846393 seconds]
   Frame Number: 29446
   Frame Length: 197 bytes (1576 bits)
   Capture Length: 197 bytes (1576 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: raw:ip:ipv6:udp:dtls]
   [Coloring Rule Name: UDP]
   [Coloring Rule String: udp]
Raw packet data
Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1
Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dde0::a
User Datagram Protocol, Src Port: 51102, Dst Port: 45687
Datagram Transport Layer Security
```

Destination address 10.20.0.1 is UA on LTE.

5	IR-11	SEND	CS LMSF	Terminate the secure Control Plane traffic and User Plane traffic connection	`lmsf> secure stop`

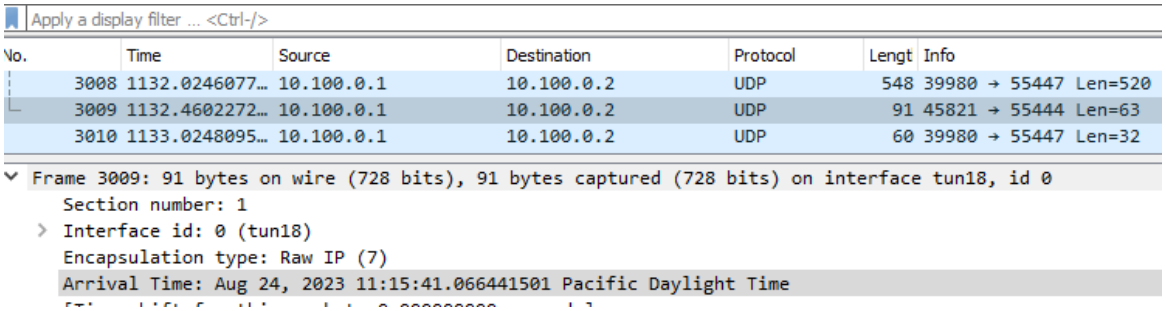
6	IR-07
	IR-11
		VERIFY	CS LMSF console	CS status shows no secure connection for User Plane traffic or Control Plane traffic	`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: N/<ID> |`
					`Control: N/<ID>`

```
2023-08-24 18:15:23.648267 GMT INFO    Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

7	IR-07
	IR-11
		VERIFY	UA LMSF console	UA status shows no secure connection for User Plane traffic or Control Plane traffic	`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: N/<ID> |`
					`Control: N/<ID>`

```
2023-08-24 18:15:32.307958 GMT Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

STEP	REQ	Action	Component	Description	Procedure
8	IR-04	SEND	UA UDMD Console	Send User Data	`cs-sh udmd` `udmd> send n=1 at 11:15 PDT`
9		VERIFY	UA User Sniffer	UDMD sent a User Data message to DTSR	From the traffic sniffer, verify the User Data message is sent from the UDMD to the DTSR

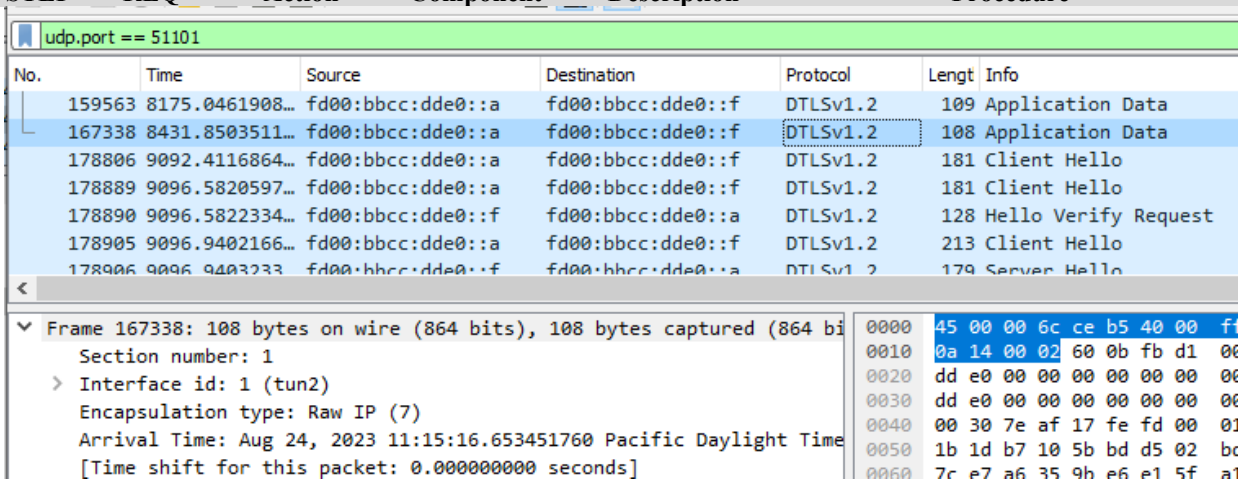


10	IR-04 IR-11	VERIFY	UA Main Sniffer	User Data and Control Messages are not transmitted by the UA DTSR	Verify via the traffic sniffer log that User Data and Control messages are not sent by UA

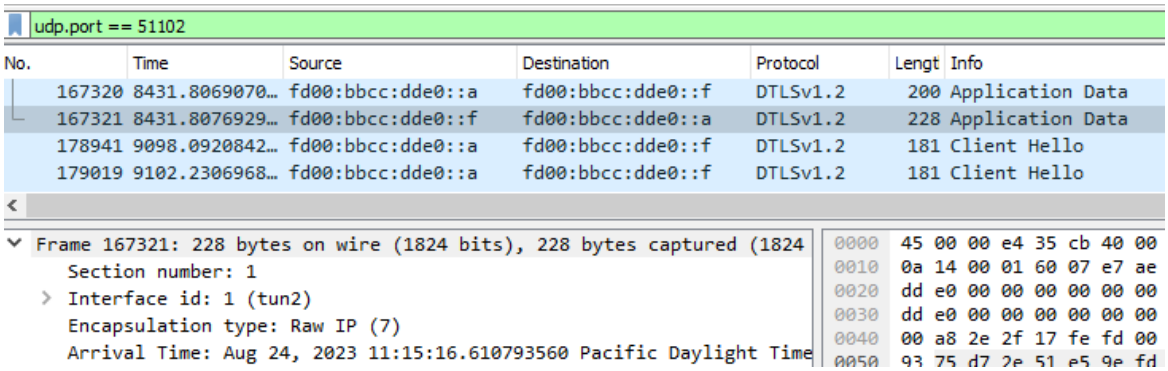
```
2023-08-24 18:15:41.066531 GMT INFO     UdmdIn.cpp:51
Received: ID: 00000014 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE Data:
UD-AAAAAAAAAAAAAAAAAAAA-000014
Secure session disabled - ID: 00000014 Origin: UDMD Cmd: SEND Size: 63 Rsp:
FALSE not sent to peer to lmsf_queue
```

11	IR-04 IR-11	VERIFY	CS Main Sniffer	User Data and Control Messages are not received by CS DTSR	Verify via the traffic sniffer log that the User Data and Control messages were not received

STEP	REQ	Action	Component	Description	Procedure



CS Main sniffer shows last control plane message at 11:15:16; next message is 11:26, which is the start of the next scenario.



CS Main sniffer shows last user plane message at 11:15:16; next message is at 11:26, which is the start of the next scenario.

12	IR-11	VERIFY	UA DTSR Live Log	Connection termination Control Messages have been exchanged between the UA and CS	Verify connection termination Control messages have been exchanged

```
2023-08-24 18:15:16.664426 GMT INFO     LmsfIn.cpp:129
Received ID: 00000016 Origin: LMSF Cmd: SECURE Size: 40 Rsp: FALSE Arg: 0
Forwarding ID: 00000016 Origin: LMSF Cmd: SECURE Size: 40 Rsp: FALSE Arg: 0
to control_plane
Secure Stop received from LMSF - notifying peer
Sent "USER_DISCONNECT.REQ     3    " across secure connection
Disabling secure session
```

13	IR-11	VERIFY	CS DTSR Live Log	Connection termination Control Messages have been exchanged between the UA and CS	Verify connection termination Control messages have been exchanged

STEP	REQ	Action	Component	Description	Procedure

```
2023-08-24 18:15:16.653621 GMT INFO
Received "USER_DISCONNECT.REQ     3    " over secure session
Disabling secure session
```

A.2 PROJECT-SPECIFIC TEST PROCEDURES

A.2.1 TP_C2_001 – Flying Out of C-Band Range

STEP	REQ	Action	Component	Description	Procedure

1	IR-08	OBSERVE	CS LMSF Console	Issue command "`status`" to view the status of all available links	`lmsf`
					`lmsf> status 1`
					`lmsf> status 2`
					`lmsf> status 3`
					
					Expected results:
					`Link 1 Up`
					`Link 2 Up`
					`Link 3 Up`

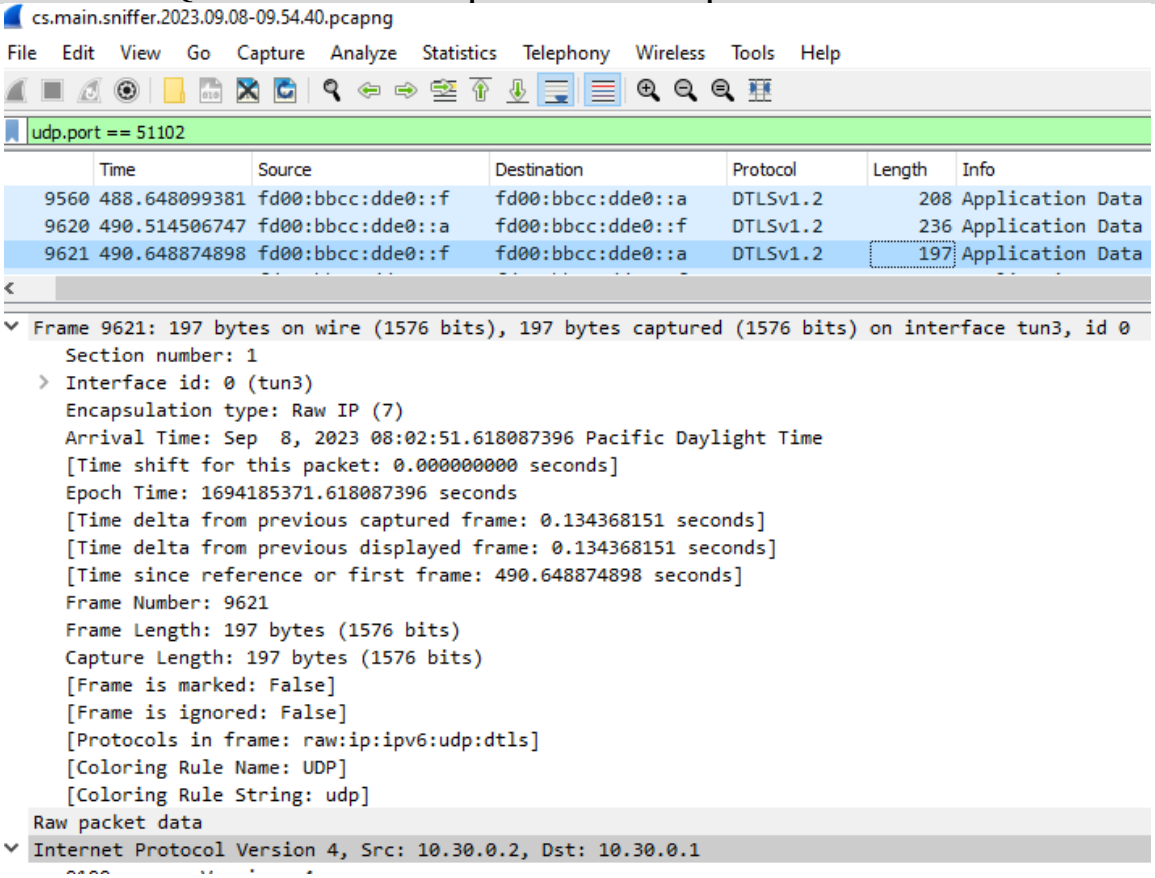
2	IR-05
	IR-07
	IR-10
		VERIFY	CS LMSF Console and DTSR Live Log	CS status shows secure session is established on C-Band	`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3|`
					`Control: Y/3`

```
2023-09-08 15:01:42.655509 GMT    Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

3		INVOKE	UA and CS LMSF Consoles	Change TET to surface/departure /arrival value	`lmsf> set_tet 3`
					`cs-sh lmsf`
					`lmsf> set_tet 3`

4	IR-04	VERIFY	CS Main Sniffer	User Data is sent over the active link	Verify via the traffic sniffer log that the User Data Messages are only sent to the UA via the link supporting the active Connection

STEP	REQ	Action	Component	Description	Procedure



Ipv4 address shows 10.30.0.2 which indicates C-Band.

5	IR-04	VERIFY	UA Main Sniffer	User Data is received over the active link	Verify via the traffic sniffer log that the User Data Messages are only received via the link supporting the active Connection

STEP	REQ	Action	Component	Description	Procedure

ua.main.sniffer.2023.09.08-09.50.59.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 51102

No.	Time	Source	Destination	Protocol	Length	Info
10681	707.374170929	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	208	Application Data
10686	707.374981460	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	236	Application Data
10693	708.184911851	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	688	Application Data

```
Frame 10681: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface tun3, id 0
    Section number: 1
  > Interface id: 0 (tun3)
    Encapsulation type: Raw IP (7)
    Arrival Time: Sep  8, 2023 08:02:50.752798215 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1694185370.752798215 seconds
    [Time delta from previous captured frame: 0.933648193 seconds]
    [Time delta from previous displayed frame: 1.189271251 seconds]
    [Time since reference or first frame: 707.374170929 seconds]
    Frame Number: 10681
    Frame Length: 208 bytes (1664 bits)
    Capture Length: 208 bytes (1664 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:ipv6:udp:dtls]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
  Raw packet data
> Internet Protocol Version 4, Src: 10.30.0.2, Dst: 10.30.0.1
```

Ipv4 address shows 10.30.0.2 which indicates C-Band.

6	WAIT	Pilot	Perform takeoff, navigate aircraft to C-Band coverage area Northwest of Building	Per Test Card
7	MONITOR	Skyline	Monitor the C-Band signal	Monitor the C-Band signal strength via Skyline

8	INVOKE	UA and CS LMSF Consoles	Once at cruise, change TET to cruise value (5 seconds)	`lmsf> set_tet 5`
				`cs-sh lmsf`
				`lmsf> set_tet 5`

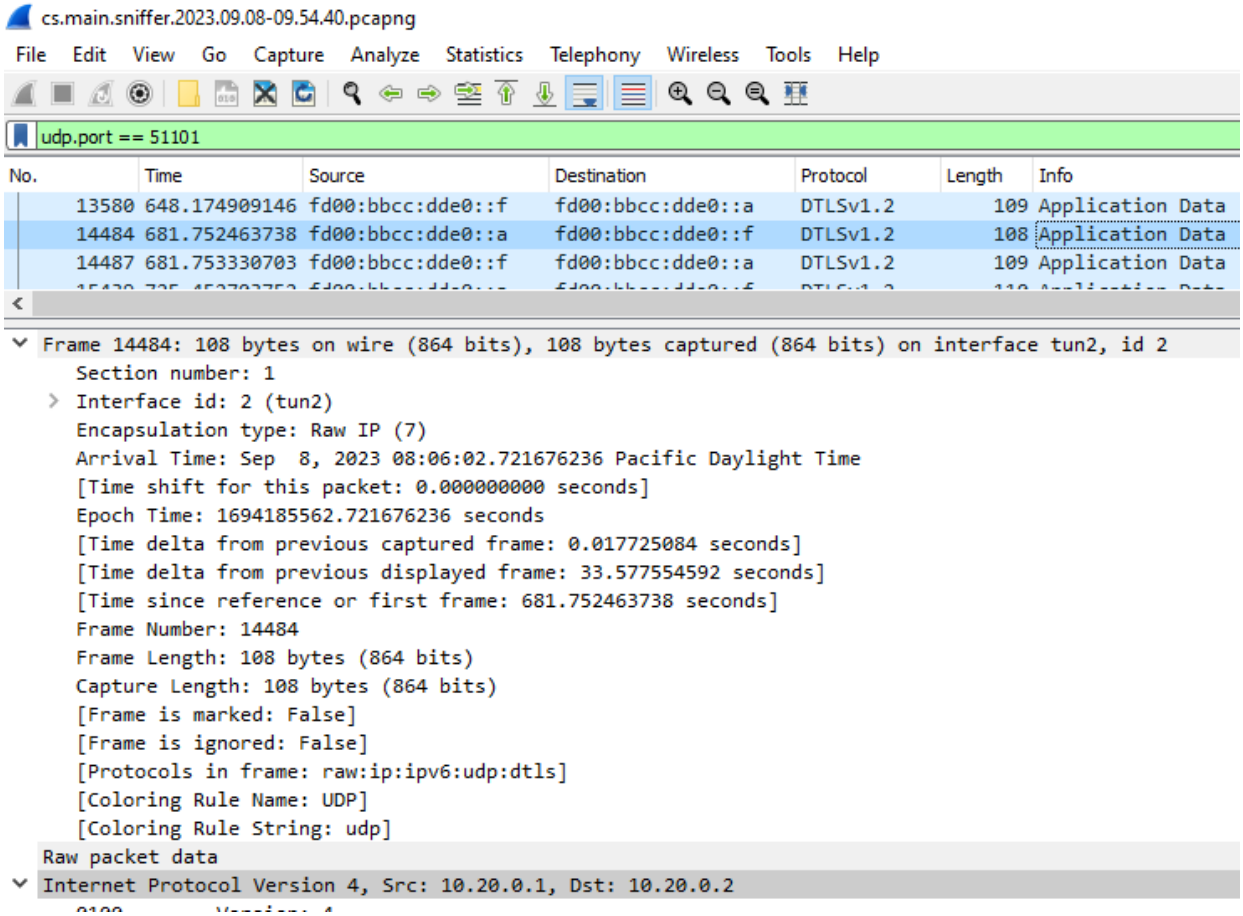
9	WAIT	Pilot	Pilot navigates out of C-Band coverage	Maneuvers drone to southeast side of building
10	MONITOR	Skyline	Monitor the C-Band signal	Monitor the C-Band signal strength via Skyline
11	OBSERVE	Skyline	Once aircraft is directly above the GRS, observe the RSSI of C-Band connection has declined	Monitor the RSSI of the C-Band connection via the Skyline GUI, noting the lowest RSSI occurs on the south side of building

STEP	REQ	Action	Component	Description	Procedure

12	IR-05
	IR-07
	IR-10
		VERIFY	CS LMSF Console and DTSR Live Log	CS status shows:
				…secure session is established
				…that the link has changed to the LTE
				…that the secure connection is maintained following the interruption
				…the CS DTSR did not indicate an interruption exceeding TET
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`
					
					<u>No</u> indication that the interruption was greater than TET

```
2023-09-08 15:06:01.945352 GMT  Lost link for secure connection.  Sending
switch command.
Initiating lost-link switchover0
CONTROL PLANE: >[080300]CONNECT.REQ              3
SWITCH completed in 775 ms.  Switchover TET set at 3000 ms.

Control plane messages change ipv4 address from C-Band to LTE, and messages
remain on same port 51101.
```

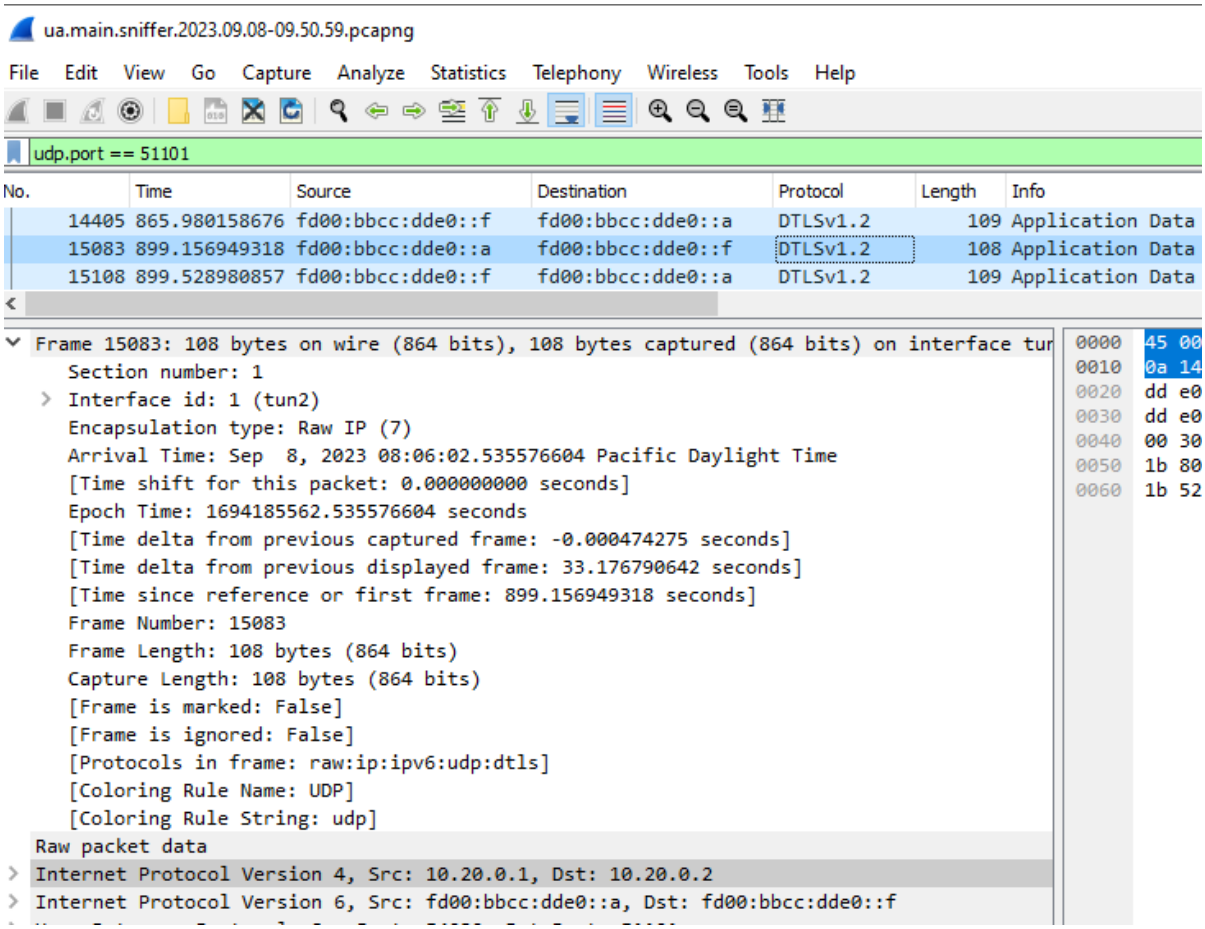


STEP	REQ	Action	Component	Description	Procedure

13	IR-05
	IR-07
	IR-10
		VERIFY	UA LMSF Console and DTSR Live Log	CS status shows:
				…secure session is established
				…that the link has changed to the LTE
				…that the secure connection is maintained following the interruption
				…the CS DTSR did not indicate an interruption exceeding TET
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`
					
					No indication that the interruption was greater than TET

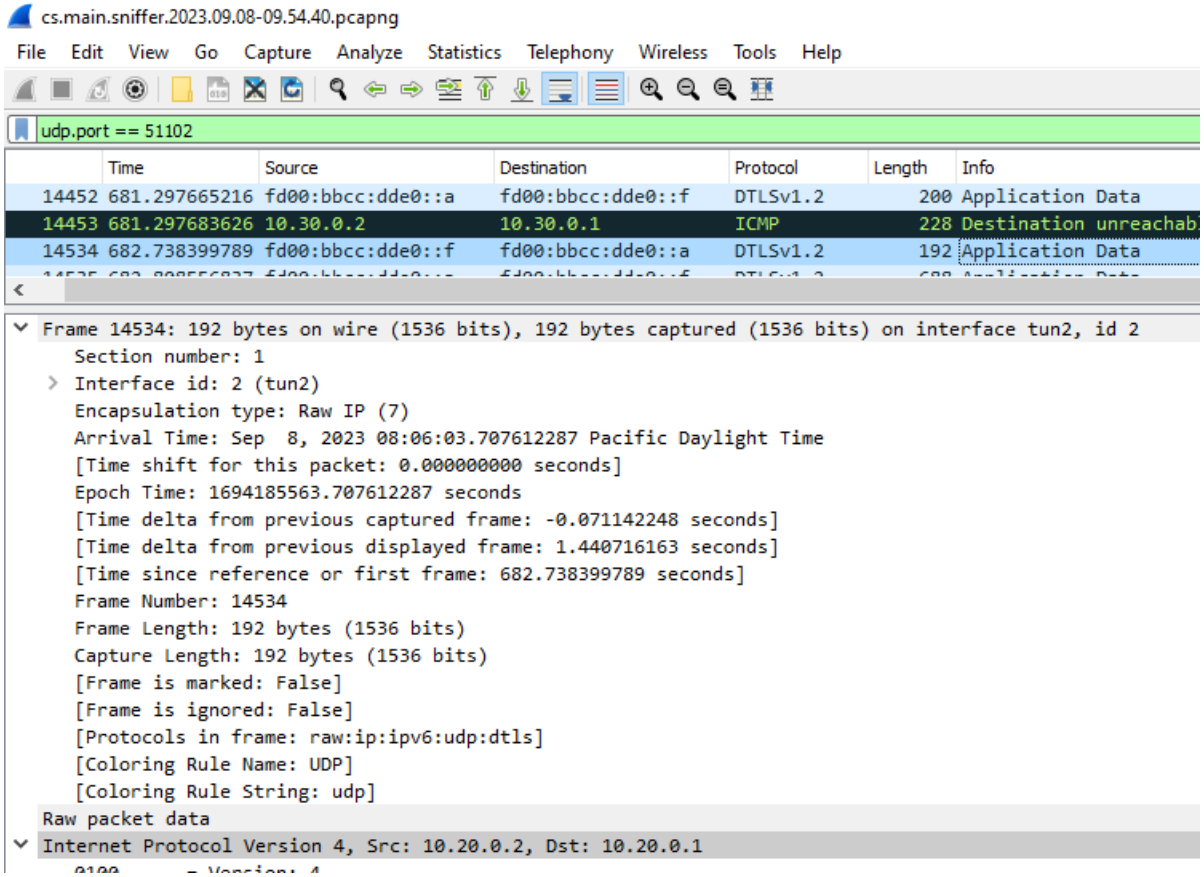
```
2023-09-08 15:06:01.490016 GMT Lost link for secure connection.  Sending
switch command.
Initiating lost-link switchover0
CONTROL PLANE: >[080300]CONNECT.REQ 3
sent CONNECT_REQ over link 2
CONTROL PLANE: CONNECT.CNF 4  Accepted[09040001]<<<
Received CONNECT.CNF.
SWITCH completed in 1417 ms.  Switchover TET set at 3000 ms.

Control plane messages change ipv4 address from C-Band to LTE, and messages
remain on same port 51101.
```



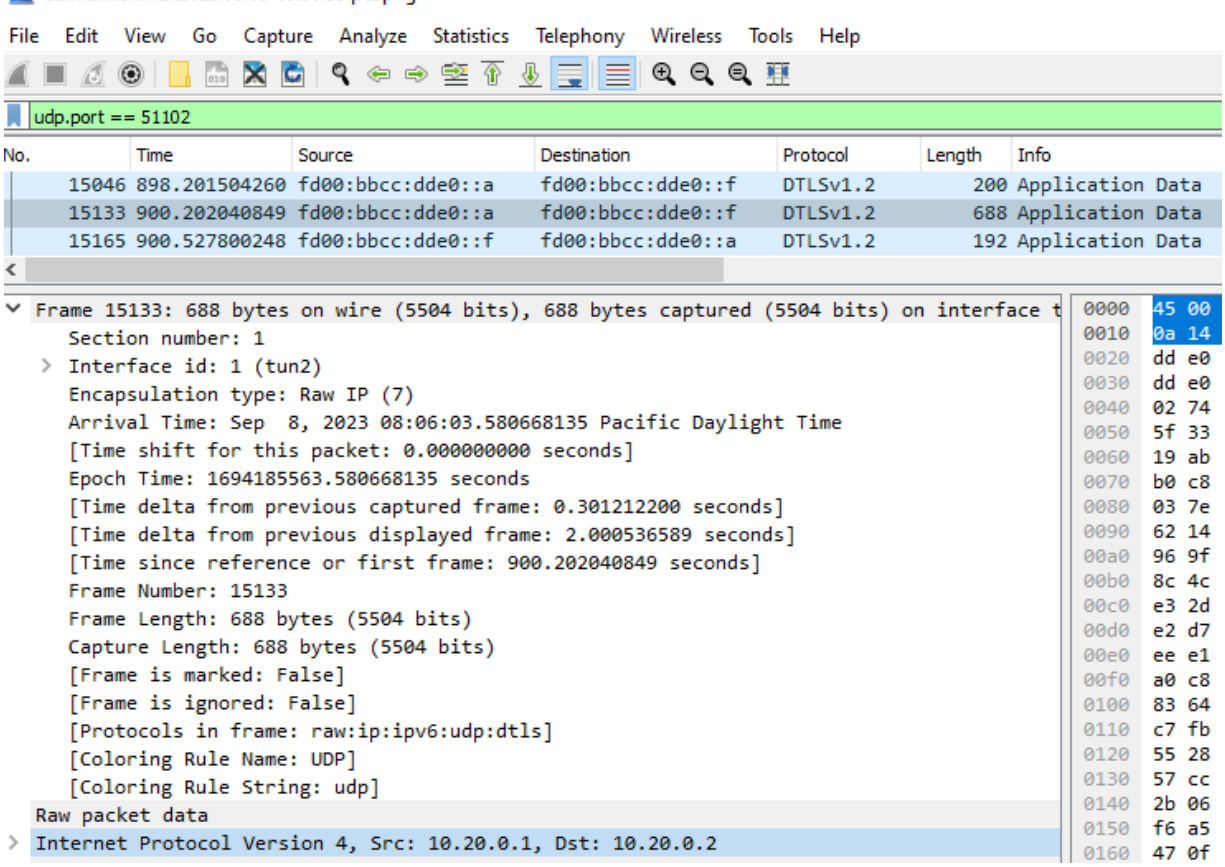
STEP	REQ	Action	Component	Description	Procedure
14	IR-04	VERIFY	CS Main Sniffer	User Data is sent over the active link (LTE)	Verify via the traffic sniffer log that the User Data Messages are only sent to the UA via the link supporting the active Connection

User plane messages change from C-Band to LTE IP addresses.



15	IR-04	VERIFY	UA Main Sniffer	User Data is received over the active link (LTE)	Verify via the traffic sniffer log that the User Data Messages are only received via the link supporting the active Connection

STEP	REQ	Action	Component	Description	Procedure
User plane messages change from C-Band to LTE IP addresses.					



16		WAIT	Pilot	Pilot navigates aircraft to landing area on west side of building into C-Band coverage	Per Test Card
17		MONITOR	Skyline	Monitor the increasing C-Band signal	Monitor the C-Band signal strength via Skyline

18	IR-08	OBSERVE	CS LMSF Console	Status indications for the current link and alternate links are available	`Lmsf`
					`lmsf> status 1`
					`lmsf> status 2`
					`lmsf> status 3`
					
					Expected Results:
					`Link 1 Up`
					`Link 2 Up`
					`Link 3 Up`

19	IR-05	SEND	CS LMSF Console	While cruising, issue Switchover command to C-Band	`lmsf` `lmsf> switch 3`

STEP	REQ	Action	Component	Description	Procedure

20	IR-05
	IR-07
	IR-10
		VERIFY	UA LMSF Console and DTSR Live Log	UA status shows:
				…secure session is established
				…that the link has changed to C-Band
				…that the secure connection is maintained following the interruption
				…the UA DTSR did not indicate an interruption exceeding TET
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`
					
					<u>No</u> indication that the interruption was greater than TET

```
2023-09-08 15:11:48.746043 GMT Initiating switchover from 2 to 3
CONTROL PLANE: >>>[080300]CONNECT.REQ 3
sent CONNECT_REQ over link 3
CONTROL PLANE: CONNECT.CNF 4   Accepted[09040001]<<<
Received CONNECT.CNF.
SWITCH completed in 1783 ms.  Switchover TET set at 5000 ms.

Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

STEP	REQ	Action	Component	Description	Procedure

21	IR-05
	IR-07
	IR-10
		VERIFY	CS LMSF Console and DTSR Live Log	CS status shows:
				…secure session is established
				…that the link has changed to C-Band
				…that the secure connection is maintained following the interruption
				…the CS DTSR did not indicate an interruption exceeding TET
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`
					
					<u>No</u> indication that the interruption was greater than TET

```
2023-09-08 15:11:48.476595 Initiating lost-link switchover3
CONTROL PLANE: >>> [080300]CONNECT.REQ 3
SWITCH completed in 1368 ms.  Switchover TET set at 5000 ms.
CONTROL PLANE: CONNECT.REQ 3   Processing succeeded.
CONTROL PLANE: CONNECT.CNF 4    Accepted[09040001]<<<<<<<<<

Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

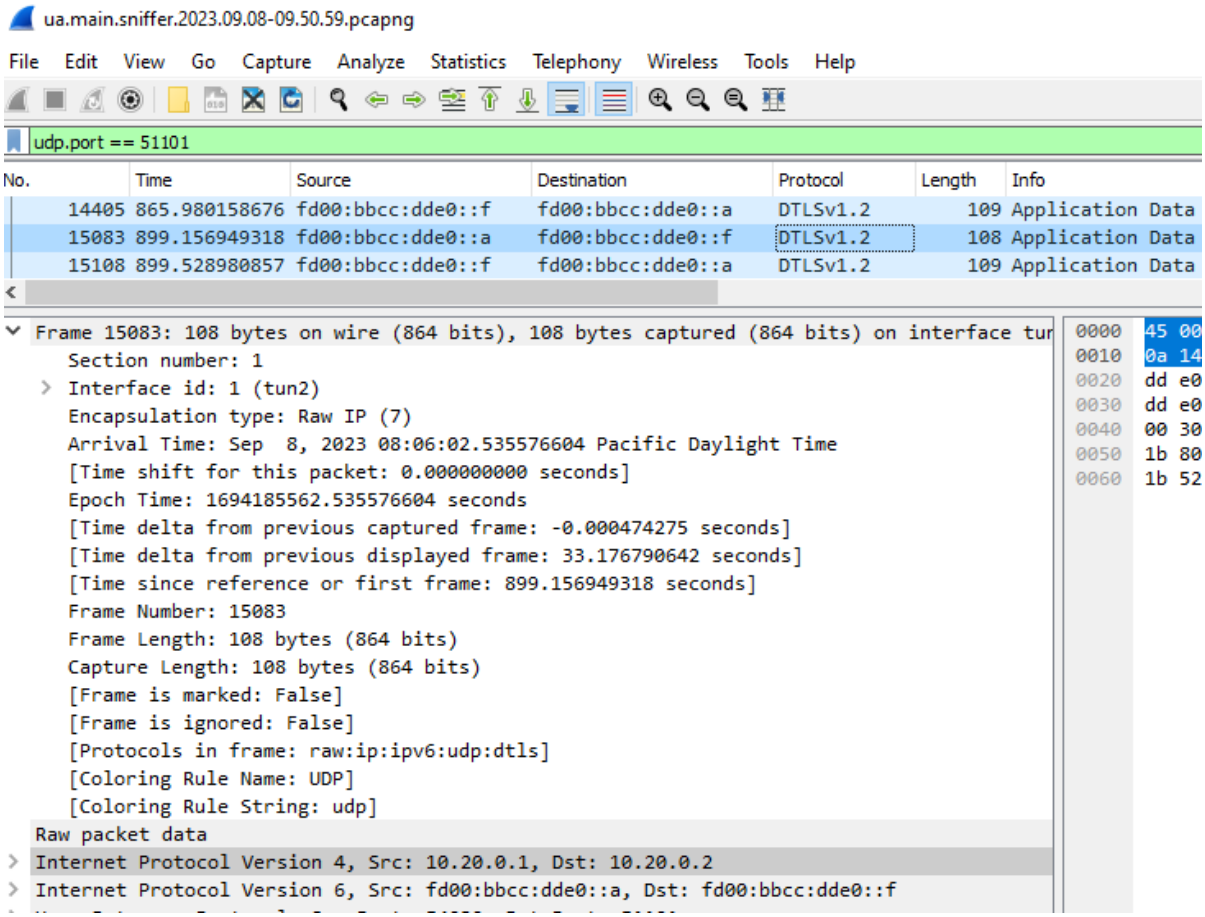
STEP	REQ	Action	Component	Description	Procedure
22		WAIT	Pilot	Pilot begins descent and lands the aircraft	Per Test Card

Post-Flight Analysis

STEP	REQ	Action	Component	Description	Procedure
23	IR-04 IR-18 IR-19c	VERIFY	CS Main Sniffer	For all switchovers, verify that: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data messages are sent to the UA only via the link supporting the active connection b) all exchanged messages before and after the switchover include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links
Verification for this step is the same as Step 14 where the ip addresses are unique after each switchover.					
24	IR-04 IR-18 IR-19c	VERIFY	UA Main Sniffer	For all switchovers, verify that: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data Messages are received by the UA only via the link supporting the active connection b) all exchanged messages before and after switchover include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links
Verification for this step is identical to Step 15 where the ip addresses are unique after every switchover.					
25	IR-20	VERIFY	UA DTSR Live Log	For all switchovers, verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	Verify via the live log that: a) the Control Messages are the appropriate messages for a Network Layer Switchover based on the messages b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)

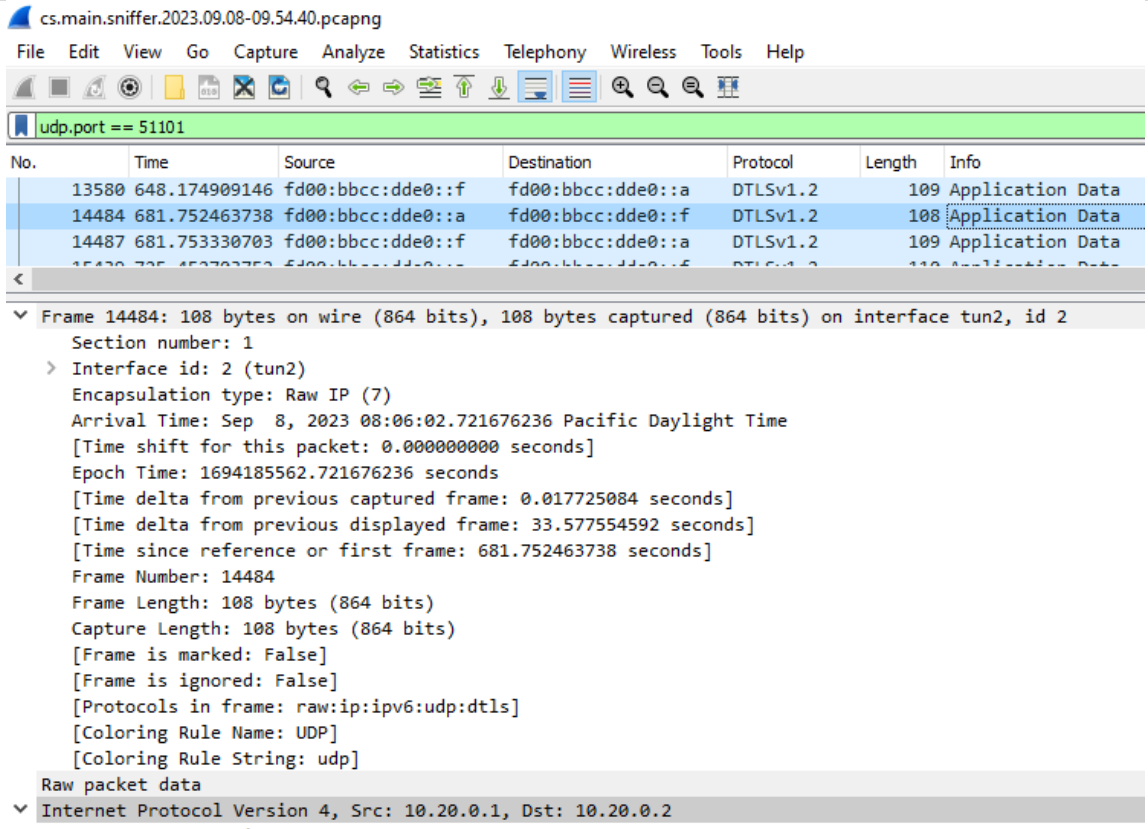
STEP	REQ	Action	Component	Description	Procedure

Control plane messages change ipv4 address from C-Band to LTE, and no new DTLS handshakes are required.



26	IR-20	VERIFY	CS DTSR Live Log	For all switchovers, verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	Verify via the live log that: a) the Control Messages are the appropriate messages for a Network Layer Switchover based on the messages b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)

STEP	REQ	Action	Component	Description	Procedure



Control plane messages change ipv4 address from C-Band to LTE, and no new DTLS handshakes are required.

27	IR-21	VERIFY	UA Main Sniffer	For all switchovers, verify User Data and Control Messages are exchanged over the new link and stop over the old link	Verify via the traffic sniffer log that: a) User Data and Control Messages begin to be exchanged over the new Link b) no messages flow over the original link

Same log check as step 25, where none of the application data messages are addressed to the old link.

28	IR-21	VERIFY	CS Main Sniffer	For all switchovers, verify User Data and Control Messages are exchanged over the new link and stop over the old link	Verify via the traffic sniffer log that: a) User Data and Control Messages begin to be exchanged over the new Link b) no messages flow over the original link

Same log check as step 26, where none of the application data messages are addressed to the old link.

29	IR-06	VERIFY	UA and CS DTSR Live Logs	For all switchovers, verify the Switchover Time is less than the TET for a Scheduled MbB Switchover	Verify the Switchover time is less than TET for a Scheduled MbB Switchover

```
CS DTSR:
SWITCH completed in 1368 ms.  Switchover TET set at 5000 ms.

UA DTSR:
SWITCH completed in 1783 ms.  Switchover TET set at 5000 ms.
```

A.2.2 TP_C2_003 – C2 Link Loss and Recovery

The test procedure for Link Loss and Recovery is included in the Final Report for completeness as edits have been made since the Test Procedures were delivered.
However, the verification steps for this procedure have already been defined in the common test procedures and will not be repeated here for conciseness.

TP_C2_003_A – LTE LINK LOSS AND RECOVERY

STEP	REQ	Action	Component	Description	Procedure

1		INVOKE	UA and CS LMSF Consoles	Change TET to surface/departure /arrival value	`lmsf> set_tet 3`
					`cs-sh lmsf`
					`lmsf> set_tet 3`

2	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

3	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

4	IR-05	SEND	UA LMSF Console	Issue Switchover command for the desired link (LTE)	`cs-sh lmsf` `lmsf> switch 2`

5	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

6	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

7	IR-04	VERIFY	CS Main Sniffer	User Data is sent over the active link; User Data is received over the active link (LTE)	Verify via the traffic sniffer log that the User Data Messages are only sent & received via the link supporting the active Connection
8	IR-04	VERIFY	UA Main Sniffer	User Data is received over the active link; User Data is sent over the active link (LTE)	Verify via the traffic sniffer log that the User Data Messages are only received via the link supporting the active Connection
9		WAIT	Pilot	Pilot initiates the takeoff	Per Test Card

10		INVOKE	CS OS Console	While taking off, simulate active link (LTE) is lost and other links are unavailable	`disable_link 1`
					`disable_link 3`
					`disable_link 2`

11		WAIT	CS Operator	Wait at least 3 seconds for TET to pass	Wait 3 seconds

STEP	REQ	Action	Component	Description	Procedure
12		INVOKE	CS OS Console	While climbing to cruise altitude, simulate the previously active link is available and other links are unavailable. (This could take several seconds)	`enable_link 2`

13	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established on LTE
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

14	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established on LTE
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

15	IR-08	OBSERVE	UA LMSF Console	Status indication that TET has been exceeded	Observe TET exceeded notification
16		WAIT	Pilot	Aircraft reaches cruising altitude	

17		INVOKE	UA and CS LMSF Consoles	Change TET to cruise value	`lmsf> set_tet 5`
					`cs-sh lmsf`
					`lmsf> set_tet 5`

18		INVOKE	CS OS Console	While cruising, simulate active link (LTE) is lost and other links are unavailable	`disable_link 2`
19		WAIT	CS Operator	Wait at least 5 seconds for TET to pass	Wait 5 seconds
20		INVOKE	CS OS Console	While cruising, simulate the previously active link is available and other links are unavailable. (This could take several seconds)	`enable_link 2`

21	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established on LTE
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

22	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established on LTE
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

23	IR-08	OBSERVE	UA LMSF Console	Status indication that TET was exceeded	Observe TET exceeded notification
24		INVOKE	CS OS Console	Enable Satcom and C-Band	`enable_link 1` `enable_link 3`

STEP	REQ	Action	Component	Description	Procedure

25	IR-08	OBSERVE	CS LMSF Console	Status indications for the current link and alternate links are available	`Lmsf`
					`lmsf> status 1`
					`lmsf> status 2`
					`lmsf> status 3`
					
					Expected Outputs:
					`Link 1 Up`
					`Link 2 Up`
					`Link 3 Up`

26		INVOKE	CS OS Console	While cruising, simulate active link (LTE) is lost and other links are available	`disable_link 2`

27	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established on C-Band
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 |`
					`Control: Y/3`

28	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established on C-Band
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3|`
					`Control: Y/3`

29		INVOKE	CS OS Console	Simulate the previously active link is available again. (This could take several seconds)	`enable_link 2`

30	IR-08	OBSERVE	CS LMSF Console	Status indication for LTE indicates satcom is available	`Lmsf`
					`lmsf> status 2`
					
					Expected output:
					`Link 2 Up`

31	IR-08	VERIFY	UA LMSF Console and DTSR Live Log	UA status shows the UA DTSR did not indicate an interruption exceeding TET	No indication that the interruption (when LTE was disabled) was greater than TET
32	IR-05	SEND	UA LMSF Console	Issue Switchover command for the desired link (LTE)	`lmsf` `lmsf> switch 2`

33	IR-05
	IR-07
	IR-10
		VERIFY	UA LMSF Console and DTSR Live Log	UA status shows:
				…secure session is established
				…that the link has changed to the specified link
				…that the secure connection is maintained following the interruption
				…the UA DTSR did not indicate an interruption exceeding TET
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 |`
					`Control: Y/2`
					
					No indication that the interruption was greater than TET

STEP	REQ	Action	Component	Description	Procedure

34	IR-05
	IR-07
	IR-10
		VERIFY	CS LMSF Console and DTSR Live Log	CS status shows:
				…secure session is established
				…that the link has changed to the specified link
				…that the secure connection is maintained following the interruption
				…the CS DTSR did not indicate an interruption exceeding TET
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`
					
					No indication that the interruption was greater than TET

35	IR-04	VERIFY	CS Main Sniffer	User Data is sent over the active link; User Data is received over the active link (LTE)	Verify via the traffic sniffer log that the User Data Messages are only sent & received via the link supporting the active Connection
36	IR-04	VERIFY	UA Main Sniffer	User Data is received over the active link; User Data is sent over the active link (LTE)	Verify via the traffic sniffer log that the User Data Messages are only received via the link supporting the active Connection
37		INVOKE	CS OS Console	While cruising, simulate backup links satcom and C-Band are lost.	`disable_link 1` `disable_link 3`
38		WAIT	Pilot	Pilot begins descent phase	Radio pilot to begin descent

39		INVOKE	UA and CS LMSF Consoles	Change TET to approach value, 3 seconds	`lmsf> set_tet 3`
					`cs-sh lmsf`
					`lmsf> set_tet 3`

40		INVOKE	CS OS Console	While in descent off, simulate active link (LTE) is lost and other links are unavailable	`disable_link 2`
41		WAIT	CS Operator	Wait to exceed TET	Wait 3 seconds
42		INVOKE	CS OS Console	While in descent, simulate the previously active link is available and other links are unavailable. (This could take several seconds)	`enable_link 2`

43	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

44	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

45	IR-08	OBSERVE	UA LMSF Console	Status indication that TET is exceeded	Observe TET exceeded notification when LTE was down

STEP	REQ	Action	Component	Description	Procedure
46		WAIT	Pilot	Pilot initiates landing phase	
47		INVOKE	CS OS Console	When the aircraft is near touching ground, simulate active link (LTE) is lost and other links are unavailable	`disable_link 2`
48		WAIT	CS Operator	Wait to exceed TET	Wait 3 seconds
49		INVOKE	CS OS Console	Simulate the previously active link is available and other links are unavailable. (This could take several seconds)	`enable_link 2`

50	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established on LTE
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

51	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established on LTE
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/<ID> | Control: Y/<ID>`

52	IR-08	OBSERVE	UA LMSF Console	Status indication that TET is exceeded	Observe TET exceeded notification when LTE was down
Post-flight analysis					
53	IR-04 IR-18 IR-19c IR-21	VERIFY	CS Main Sniffer	For every switchover, verify that: …messages flow over the new link …no messages flow over the original link …addresses are unique	Verify via the traffic sniffer log that: a) User Data and Control messages are exchanged over the new Link (the active connection) b) no messages flow over the original link c) all exchanged messages before and after the switchover include unique IP source and destination addresses that uniquely identify the UA and CS d) addresses are unique across paths over networked A/G links and over point-to-point A/G links

STEP	REQ	Action	Component	Description	Procedure
54	IR-04 IR-18 IR-19c IR-21	VERIFY	UA Main Sniffer	For every switchover, verify that: …messages flow over the new link …no messages flow over the original link …addresses are unique	Verify via the traffic sniffer log that: a) User Data and Control messages are exchanged over the new Link (the active connection) b) no messages flow over the original link c) all exchanged messages before and after the switchover include unique IP source and destination addresses that uniquely identify the UA and CS d) addresses are unique across paths over networked A/G links and over point-to-point A/G links
55	IR-20	VERIFY	UA DTSR Live Log	For every switchover and link loss scenario, verify the appropriate Control Messages were exchanged while maintaining not breaking the secure session	Verify via the live log that: a) the Control Messages are the appropriate messages for a Network Layer Switchover b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)
56	IR-20	VERIFY	CS DTSR Live Log	For every switchover, verify the appropriate Control Messages were exchanged while maintaining not breaking the secure session	Verify via the live log that: a) the Control Messages are the appropriate messages for a Network Layer Switchover b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)
57	IR-06	VERIFY	UA DTSR Live Log	For every switchover, calculate the Switchover Time	Verify the Switchover time is less than TET for a Scheduled MbB Switchover
58		ANALYZE	UA & CS DTSR Live Log	For every link loss condition, calculate the time to re-establish the link	Time to re-establish link = time from link loss determination to time User Data is flowing again
59	IR-06	OBSERVE	UA DTSR Live Log	Observe the Switchover and note the Switchover Time	Verify the start and end timestamps of the Switchover.

A.2.2 TP_C2_004 Link Switchovers

The test procedure for Link Switchovers is included in the Final Report for completeness as edits have been made since the Test Procedures were delivered.
However, the verification steps for this procedure have already been defined in the common test procedures (see TP_CM_009 and TP_CM_010) and will not be repeated here for conciseness.

STEP	REQ	Action	Component	Description	Procedure

1		INVOKE	UA and CS LMSF Consoles	Change TET to surface/departure /arrival value	`lmsf> set_tet 3`
					`cs-sh lmsf`
					`lmsf> set_tet 3`

2	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

3	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

4	IR-05	SEND	UA LMSF Console	Issue Switchover command for the desired link (LTE)	`cs-sh lmsf` `lmsf> switch 2`

5	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

6	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

7		WAIT	Pilot	Initiate Takeoff	Per Test Card
8	IR-05	SEND	UA LMSF Console	While the aircraft is climbing, switch from LTE to satcom	`cs-sh lmsf` `lmsf> switch 1`

9	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/1 | Control: Y/1`

10	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/1 | Control: Y/1`

11	IR-05	SEND	UA LMSF Console	While the aircraft is climbing, switch from satcom to C-Band	`cs-sh lmsf` `lmsf> switch 3`

12	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

STEP	REQ	Action	Component	Description	Procedure

13	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

14	IR-08	OBSERVE	CS LMSF Console	View the status of all available links	`lmsf`
					`lmsf> Status 1`
					`Status 2`
					`Status 3`
					
					Expected output
					`Link 1 Up`
					`Link 2 Up`
					`Link 3 Up`

15	IR-08	OBSERVE	UA LMSF Console	Issue command "status" to view the status of all available links	`cs-sh lmsf`
					`lmsf> Status 1`
					`Status 2`
					`Status 3`
					
					Expected output
					`Link 1 Up`
					`Link 2 Up`
					`Link 3 Up`

16		WAIT	Pilot	Aircraft reaches cruising altitude	Per Test Card

17		INVOKE	UA and CS LMSF Consoles	Change TET to cruise value	`lmsf> set_tet 5`
					`cs-sh lmsf`
					`lmsf> set_tet 5`

18	IR-05	SEND	UA LMSF Console	While the aircraft is cruising, switch from LTE to C-Band	`cs-sh lmsf` `lmsf> switch 3`

19	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

20	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

21	IR-04 IR-18 IR-19c	VERIFY	CS Main Sniffer	On the CS, verify: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data messages are sent to the UA only via the C-Band link supporting the active connection b) all exchanged messages include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links

STEP	REQ	Action	Component	Description	Procedure
22	IR-04 IR-18 IR-19c	VERIFY	UA Main Sniffer	On the UA, verify: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data Messages are received by the UA only via the Satcom link supporting the active connection b) all exchanged messages include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links
23	IR-05	SEND	UA LMSF Console	While the aircraft is cruising, switch from C-Band to satcom	`cs-sh lmsf` `lmsf> switch 1`

24	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/1 | Control: Y/1`

25	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/1 | Control: Y/1`

26	IR-05	SEND	UA LMSF Console	While cruising, switch from satcom to LTE	`cs-sh lmsf` `lmsf> switch 2`

27	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

28	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

29	IR-08	OBSERVE	CS LMSF Console	View the status of all available links	`lmsf`
					`lmsf> Status 1`
					`Status 2`
					`Status 3`
					
					Expected output
					`Link 1 Up`
					`Link 2 Up`
					`Link 3 Up`

STEP	REQ	Action	Component	Description	Procedure

30	IR-08	OBSERVE	UA LMSF Console	Issue command "status" to view the status of all available links	`cs-sh lmsf`
					`lmsf> Status 1`
					`Status 2`
					`Status 3`
					
					Expected output
					`Link 1 Up`
					`Link 2 Up`
					`Link 3 Up`

31		INVOKE	UA & CS LMSF Console	Change the TET to approach value	`lmsf> set_tet 3`
					`cs-sh lmsf`
					`lmsf> set_tet 3`

32		WAIT	Pilot	Aircraft commences descent	Per Test Card
33	IR-05	SEND	UA LMSF Console	While the aircraft is descending, switch from LTE to C-Band	`cs-sh lmsf` `lmsf> switch 3`

34	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

35	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

36	IR-05	SEND	UA LMSF Console	While the aircraft is descending, switch from C-Band to satcom	`cs-sh lmsf` `lmsf> switch 1`

37	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/1 | Control: Y/1`

38	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/1 | Control: Y/1`

39	IR-05	SEND	UA LMSF Console	While descending, switch from satcom to LTE	`cs-sh lmsf` `lmsf> switch 2`

40	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

STEP	REQ	Action	Component	Description	Procedure

41	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/2 | Control: Y/2`

42	IR-05	SEND	UA LMSF Console	While the aircraft is descending, switch from LTE to satcom	`cs-sh lmsf` `lmsf> switch 1`

43	IR-05
	IR-07
		VERIFY	UA LMSF Console	UA status shows:
				…secure session is established
				…that the link has been re-established
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/1 | Control: Y/1`

44	IR-05
	IR-07
		VERIFY	CS LMSF Console	CS status shows:
				…secure session is established
				…that the link has been re-established
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/1 | Control: Y/1`

45		WAIT	Pilot	Aircraft lands	Per Test Card
Post-flight analysis					
46	IR-06	OBSERVE	UA DTSR Live Log	Observe the Switchover and note the Switchover Time	Verify the start and end timestamps of the Switchovers.
47	IR-06	OBSERVE	CS DTSR Live Log	Observe the Switchover and note the Switchover Time	Verify the start and end timestamps of the Switchovers.
48	IR-10	VERIFY	UA LMSF Console and DTSR Live Log	UA status shows: …the UA DTSR did not indicate an interruption exceeding TET	No indications that the interruptions from switchovers were greater than TET
49	IR-10	VERIFY	CS LMSF Console and DTSR Live Log	CS status shows: …the CS DTSR did not indicate an interruption exceeding TET	No indications that the interruptions from switchovers were greater than TET
50	IR-04, IR-18 IR-19c	VERIFY	CS Main Sniffer	On the CS, verify: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data messages were sent to the UA only via the link supporting the active connection b) all exchanged messages include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links

STEP	REQ	Action	Component	Description	Procedure
51	IR-04, IR-18 IR-19c	VERIFY	UA Main Sniffer	On the UA, verify: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data Messages were received by the UA only via the link supporting the active connection b) all exchanged messages include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links
52	IR-20	VERIFY	UA DTSR Live Log	Verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	Verify via the live log that: a) the Control Messages are the appropriate messages for a Network Layer Switchover b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)
53	IR-20	VERIFY	CS DTSR Live Log	Verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	Verify via the live log that: a) the Control Messages are the appropriate messages for a Network Layer Switchover b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)
54	IR-21	VERIFY	UA Main Sniffer	Verify User Data and Control Messages are exchanged over the new link and stop over the old link	Verify via the traffic sniffer log that: a) User Data and Control Messages begin to be exchanged over the new Link b) no messages flow over the original link
55	IR-21	VERIFY	CS Main Sniffer	Verify User Data and Control Messages are exchanged over the new link and stop over the old link	Verify via the traffic sniffer log that: a) User Data and Control Messages begin to be exchanged over the new Link b) no messages flow over the original link
60	IR-06	VERIFY	CS DTSR Live Log	For all switchovers, verify the Switchover Time is less than the TET for a Scheduled MbB Switchover	Verify the Switchover time is less than TET for a Scheduled MbB Switchover

B. INSPECTION RESULTS – UAS C2 LINK SYSTEM SECURITY

The following table summarizes the MASPS security requirements for which the Detailed Test Procedures [DTP] include an INSPECTION and/or VERIFY test step as a means to show compliance with the MOC in [DO-377A] for the UAS C2 Link System security. Note that the table includes pairs of requirements, e.g., SER-01 and SER-08, where the same MOC and inspection test step action are applicable to the respective security requirements for User Plane traffic and Control Plane traffic exchanged between the UA DTSR and the CS DTSR.

Table B-1 – Security Requirements with an INSPECTION or VERIFY Test Step

DO-377A			[DTP]
Req. No:	**Requirement**	**Means of Compliance (MOC)**	**Test Procedure and Test Step**
SER-01	The UAS C2 Link security system **shall** provide mutual peer entity authentication of C2 User Plane traffic between the UA and CS.	FIPS 140-2 Annex D key establishment and authentication tag of at least 64 bits or equivalent MOC.	**IP_CM_001A**, Step 1 **TP_CM_001**
SER-08	The UAS C2 Link security system **shall** provide mutual peer entity authentication of C2 Control Plane traffic between the UA and CS.		
SER-02	The UAS C2 Link security system **shall** provide data origin authentication of C2 User Plane traffic between the UA and CS.	AES Counter with CBC-MAC (CCM) per NIST SP 800-38C, or AES Galois Counter Mode (GCM) per NIST SP 800-38D, or Keyed-Hash Message Authentication Code (HMAC) per FIPS PUB. 198-1 with an authentication tag of at least 64 bits or equivalent MOC.	**IP_CM_001A,** Step 1 **TP_CM_005A**, Step 4
SER-09	The UAS C2 Link security system **shall** provide data origin authentication of C2 Control Plane traffic between the UA and CS.		**IP_CM_001A,** Step 1 **TP_CM_008**, Step 3
SER-03	The UAS C2 Link System security **shall** provide data integrity and anti-replay protection fir C2 User Plane traffic between the UA and CS,	AES-CCM per NIST SP 800-38C, or AES-GCM per NIST SP 800-38D, or HMAC per FIPS PUB. 198-1 with an authentication tag of at least 64 bits or equivalent MOC.	**IP_CM_001A,** Step 1 **TP_CM_005A**, Step 4
SER-10	The UAS C2 Link System security **shall** provide data integrity and anti-replay protection fir C2 Control Plane traffic between the UA and CS,		**IP_CM_001A,** Step 1 **TP_CM_008**, Step 3
SER-04	The UAS C2 Link security system **shall** provide confidentiality of sensitive C2 User Plane traffic between the UA and CS.	AES-CCM per NIST SP 800-38C, or AES-GCM per NIST SP 800-38D or equivalent MOC.	**IP_CM_001A**, Step 1 **TP_CM_004**
SER-11	The UAS C2 Link security system **shall** provide confidentiality of sensitive C2 Control Plane traffic between the UA and CS.		**IP_CM_001A**, Step 1 **TP_CM_007**
SER-05	The UAS C2 Link security system **shall** use cryptographic algorithms, with algorithm strength and key length sufficient to protect C2 User Plane traffic between the UA and CS for the duration of a flight.	Meet algorithm strength and key length requirements of NIST SP 800-131A, Rev. 2, or equivalent MOC. SP 800-131A recognizes that large-scale quantum computers, when available, will threaten the security of NIST-approved public key algorithms.	**IP_CM_001A**, Step 1
SER-12	The UAS CS C2 Link security system **shall** use cryptographic algorithms with algorithm strength and key length sufficient to protect C2 Control Plane traffic between the UA and CS.		**IP_CM_001A**, Step 1

Section B.1 summarizes the cryptographic configuration including the key characteristics of the selected cryptographic library, the cryptographic library build used for the validation tests, and the application configurations (cipher suites) used for the validation tests. Section B.2 references the cryptographic configuration and provide the inspection results for each of the requirement pairs identified in Table B-1.

B.1 CRYPTOGRAPHIC CONFIGURATION INSPECTION

B.1.1 Cryptographic Library Characteristics

The UA and CS systems under test leverage the commercial off-the-shelf (COTS) wolfSSL cryptographic library (version 4.4), which supports industry-standard Transport Layer Security (TLS, up to the current version 1.3) and Datagram Transport Layer Security (DTLS, version 1.2) protocols. The UA and CS systems use the DTLS protocol since UDP/IP was selected for the transport/network layers.

The wolfSSL library includes the wolfCrypt library, which provides the underlying cryptographic algorithms used by the TLS/DTLS protocols. The version of wolfSSL selected for this project includes a wolfCrypt library that has been FIPS 140-2 certified (Certificate #3389) under the NIST Crypto Module Validation Program (CMVP). In addition, the individual wolfCrypt cryptographic algorithm implementations have been certified under NIST Crypto Algorithm Validation Program (CAVP), as summarized in the following table.

Table B-2 – wolfCrypt Cryptographic Algorithms and associated NIST CAVP Certificates

Algorithm	Use	Characteristics	Relies on	NIST Reference	NIST CAVP
AES	Encryption/decryption	Key Sizes: 128, 192, 256 Modes: —CBC, CTR, ECB (SP 800-38A) —CMAC (SP 800-38B) —CCM (SP 800-38C) —GCM, GMAC (SP 800-38D) Tag Length: 96, 104, 112, 120, 128	DRBG	FIPS 197	5446
CVL (KAS)	Key agreement	Curves: P-256, P-384, P-521	ECDSA, DRBG, SHS	SP 800-56A	1891
DRBG	Random bit generation	SHA-256-based	SHS	SP 800-90A	2131
ECDSA	Key generation Key verification Signature generation Signature verification	Curves: P-256, P-384, P-521 Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHS, DRBG	FIPS 186-4	1451
KDF	Key Derivation Function	Mode: HMAC-based pseudo-random function (PRF) Hash: SHA-256 or SHA-384	HMAC, SHS	SP 800-56C	Note 1
HMAC	Message authentication code generation and verification	Mode: Hashed Message Authentication Code Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHS	FIPS 198	3604
SHS	Message digest generation	Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	None	FIPS 180	4365
Note 1: The vendor (wolfSSL) affirms conformance of this function to NIST SP 800-56C. This KDF is approved for use within an approved key establishment scheme but the CMVP does not currently provide CAVP component testing. [REF-3389SP]					

Certificate #3389 and the associated CAVP certificates cover operating environments (i.e., operating system plus computing platform) that are similar to the UA operating environment (i.e., Ubuntu Linux running on an ARM v8 processor) and the CS operating environment (i.e., Ubuntu Linux running on an Intel CPU). As documented previously in the [SRS], formal FIPS validation per SER-06 / SER-13 is out-of-scope of this project. However, the information presented in this section is intended to show that there is a path to FIPS validation for future production UA and CS systems using existing COTS crypto libraries.

B.1.2 Cryptographic Library Build

Panel A in the following figure lists the contents of the Config.sh file, which enables option settings for the wolfSSL cryptographic library build. Panel B is a configuration summary output file that was generated by the wolfSSL library at the time of build for the UA and CS. Since the same cryptographic build file is used for both the UA and the CS, the configuration summaries are identical for both systems.

```
#!/bin/bash
RC=0
WORKING_DIR="."
OPTIONS="\
--enable-ipv6 \
--enable-harden \
--enable-fips=v2 \
--enable-opensslextra \
--enable-keygen \
--enable-certgen \
--enable-certreq \
--enable-supportedcurves \
--enable-eccshamir \
--enable-ecc \
--enable-ecccustcurves \
--enable-eccencrypt \
--enable-sha384 \
--enable-dtls \
--enable-dtls-mtu \
--enable-tls13 \
--enable-aes \
--enable-asn \
--enable-testcert \
--enable-nullcipher \
--enable-x963kdf"
```

A. Config.sh Build File

```
Configuration summary for wolfssl version 4.4.0
*  Installation prefix:        /usr/local
*  System type:                pc-linux-gnu
*  Host CPU:                   x86_64
*  C Compiler:                 gcc
*  AES:                        yes
*  AES-CBC:                    yes
*  AES-GCM:                    yes
*  AES-CCM:                    yes
*  AES-CTR:                    yes
*  DES3:                       yes
*  NULL Cipher:                yes
*  SHA:                        yes
*  SHA-224:                    yes
*  SHA-384:                    yes
*  SHA-512:                    yes
*  keygen:                     yes
*  certgen:                    yes
*  certreq:                    yes
*  Hash DRBG:                  yes
*  PWDBASED:                   yes
*  HKDF:                       yes
*  X9.63 KDF:                  yes
*  DH:                         yes
*  DH Default Parameters:      yes
*  ECC:                        yes
*  ECC Custom Curves           yes
*  ECC_ENCRYPT:                yes
*  DTLS:                       yes
*  TLS v1.3:                   yes
*  Supported Elliptic Curves:  yes
*  Extended Master Secret:     yes
```

B. Configuration Summary Output

B-1 – wolfSSL Cryptographic Library Build

These figures will be referenced as necessary in the detailed inspection results in Section B.3.

B.1.3 Application Configurations

Two UA and CS DTSR application configurations were employed to support tests of the UAS C2 security requirements:

- **AEAD Configuration** – Uses the cipher suite `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x2C)`. This configuration, which uses AES in the GCM operating mode with 256-bit keys, was used to demonstrate compliance with the confidentiality requirements in SER-04 and SER-11.
- **NULL Configuration** – Uses the cipher suite `TLS_ECDHE_ECDSA_WITH_NULL_SHA (0xC0, 0x06)`. This configuration, which uses the NULL confidentiality algorithm (i.e., no encryption), was used to demonstration compliance with all SER requirements with the exception of the confidentiality requirements in SER-04 and SER-11.

  Note: The cipher suites are registered on the IANA web site, and the pair of hexadecimal values shown above in parentheses are an index into the table of registered values.

With the exception of the confidentiality algorithm (AES vs. NULL) and the hash function (SHA384 vs. SHA), the other algorithms in the cipher suites are identical (i.e., TLS, ECDHE, ECDSA). When using the AEAD Configuration, the AES_256_GCM algorithm provides authenticated encryption, which simultaneously provides both confidentiality and authenticity of the data. Since the AEAD algorithm performs authentication-then-encryption (i.e., the authentication tag is computed first, then both the plaintext data and the authentication tag are encrypted), the encrypted authentication tag cannot be observed directly (i.e., from a "black box" test perspective) in message exchanges. Therefore, the NULL Configuration was employed for validating the security requirements (e.g., SER-01/SER-08) where observing the authentication tag/length is specified in the means of compliance.

B.2 SECURITY REQUIREMENT INSPECTION

B.2.1 SER-01 / SER-08 Compliance

The MOC for SER-01/SER-08 references NIST FIPS 140-2 Annex D [REF-140-2], which specifies approved key establishment techniques. The listed techniques include NIST SP 800-56A [REF-56A], Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. Section 10 of NIST SP 800-56A states that an implementation claiming conformance must show use of:

- Elliptic Curve (EC) cryptography plus use of a NIST-recommended elliptic curve.
- Approved key agreement scheme
- Approved hash function
- Approved random bit generation
- Approved key generation scheme
- Approved key derivation function
- A MAC tag length greater than or equal to 64 bits (for all elliptic curve sizes and domain parameters).

The cipher suites for both the AEAD and NULL application configurations specify Elliptic Curve Diffie-Hellman Ephemeral (ECDHE), which is an approved key agreement scheme per NIST SP 800-56A, and the detailed DTLS logs identify the selected elliptic curves (secp521r1 for the NULL Configuration and secp256r1 for the AEAD Configuration), which meet the NIST SP 800-131A Rev.2 minimum length/strength requirements. Per Section B.1.1, the FIPS-validated wolfSSL wolfCrypt library implements the CVL Key Agreement Scheme (KAS) per NIST SP 800-56A and was certified under the NIST CAVP (certificate number 1891). The CVL KAS also uses an approved hash (SHS) per NIST FIPS 180, approved random bit generation (DRBG) per NIST SP 800-90A, key pair generation per NIST FIPS 186-4, and HMAC-based key derivation function per NIST SP 800-56C. In addition, conformance of CVL KAS with NIST SP 800-56A means that the resulting MAC tag is greater than or equal to 64 bits.

Result = PASS: This inspection demonstrates that the cryptographic module implements a key establishment scheme and associated MAC tag that are compliant with NIST FIPS 140-2 Appendix D and the key establishment technique specified in NIST SP 800-56A.

B.2.2 SER-02 / SER-09 and SER-03 / SER-10 Compliance

B.2.2.1 AEAD APPLICATION CONFIGURATION

Per Section B.1.1, the FIPS-validated wolfSSL wolfCrypt library supports the AES algorithm in accordance with NIST FIPS 197 operating in the AES-GCM mode per NIST SP 800-38D. Key lengths of 128, 192, and 256 bits are supported, and the registered cipher suite (`TLS_ECDHE_ECDSA_WITH_`**`AES_256_GCM`**`_SHA384`) invokes the use of AES-GCM with 256-bit keys.

As shown in Panel A of the figure in B.1.2, the build file includes the `--enable-aes \` option, and the configuration summary shown in Panel B confirms that the AES algorithm and the AES-GCM mode of operation are configured in the UA and CS builds. The AES-GCM mode produces a non-truncated 128-bit (16 byte) authentication tag.

Result = **PASS**: This inspection demonstrates that the cryptographic module was configured for AES with an approved symmetric key block cipher mode (AES-GCM per NIST SP 800-38D), which produces a non-truncated 128-bit (16 byte) authentication tag that is compliant with the MOC for SER-02 / SER-09 and SER-03 / SER-10.

B.2.2.2 NULL APPLICATION CONFIGURATION

Per Section B.1.1, the FIPS-validated wolfSSL wolfCrypt library supports the Hashed Message Authentication (HMAC) function in accordance with NIST FIPS 198 with an underlying Secure Hash Standard (SHS) algorithm in accordance with NIST FIPS 180.

As shown in Panel A of the figure in B.1.2, the build file includes the `--enable-nullcipher \` option, and the configuration summary shown in Panel B confirms that the NULL Cipher is configured in the UA and CS builds. The registered NULL cipher suite (`TLS_ECDHE_ECDSA_WITH_`**`NULL_SHA`**) invokes the use of HMAC with the SHA-1 hash algorithm, which produces a non-truncated 160-bit (20-byte) authentication tag.

Result = **PASS**: This inspection demonstrates that the cryptographic module was configured for HMAC-SHA1 per NIST FIPS 198 and produces a 160-bit tag, which is compliant with the MOC for SER-02/SER-09 and SER-03/SER-10.

B.2.3 SER-04 / SER-11 Compliance

The tests procedures used to validate the SER-04 and SER-11 confidentiality requirement used the AEAD Configuration. In this configuration, the registered cipher suite (`TLS_ECDHE_ECDSA_WITH_`**`AES_256_GCM`**`_SHA384`) invokes the AES algorithm operating in the GCM mode with 256-bit keys.

Per Section B.1.1, the FIPS-validated wolfSSL wolfCrypt library supports the AES algorithm in accordance with NIST FIPS 197 operating in the AES-GCM mode per NIST SP 800-38D. Key lengths of 128, 192, and 256 bits are supported, and the selected cipher suite (`TLS_ECDHE_ECDSA_WITH_`**`AES_256_GCM`**`_SHA384`) invokes the use of AES-GCM with 256-bit keys.

As shown in Panel A of the figure in B.1.2, the build file includes the `--enable-aes \` option, and the configuration summary shown in Panel B confirms that the AES algorithm and the AES-GCM mode of operation are configured in the UA and CS builds.

Result = **PASS**: This inspection demonstrates that the cryptographic module was configured for AES using an approved symmetric key block cipher mode (AES-GCM per NIST SP 800-38D), which is compliant with the MOC for SER-04 / SER-11.

B.2.4 SER-05 / SER-12 Compliance

This section summarizes UA and CS cryptographic module compliance with the algorithm, strength, and key length requirements per NIST SP 800-131A, Rev. 2. In the following table, the first two columns enumerate the algorithm-specific requirements contained in the NIST document. The remaining columns summarize compliance, including:

- **wolfSSL Crypto Library** – A yes (Y) or no (N) compliance indication and a pointer to the algorithm row in Table 4-13 that provides specific details and NIST CAVP certificates.
- **UA and CS Prototype Implementation** – A yes (Y) or no (N) compliance indication and the specific algorithm, mode, key length used in the prototype for each of the two application configurations (AEAD, NULL).

Table B-3 – Compliance with NIST SP 800-131A, Rev. 2

NIST SP 800-131A, Rev.2		Compliance		
Section – Algorithm	Requirement(s)	wolfSSL Crypto Library per Table 4-13	UA and CS Prototype Implementation (reference Section 4.5.1.3)	
			AEAD Configuration	NULL Configuration
2 – Encryption and Decryption using Block Cipher Algorithms	• AES per NIST FIPS 197 • 128, 192, or 256-bit keys • Approved mode of operation per NIST SP 800-38 series	**Y** AES	**Y** AES-256-GCM	**Not applicable** – NULL encryption
3 – Digital Signature	• DSA per NIST FIPS 186-4 • ECDSA len(n) >= 224	**Y** ECDSA	**Y** ECDSA using P-521 curve and SHA-512 (**Note 1**)	**Y** ECDSA using P-521 curve and SHA-512 (**Note 1**)
4 – Random Bit Generation	• DRBG per SP 800-90A	**Y** DRBG	**Y** Hash_DRBG using SHA-256	**Y** Hash_DRBG using SHA-256
	• Hash_DRBG or HMAC_DRBG using any hash per NIST FIPS 180	**Y** SHS		
5 – Key Agreement using Diffie-Hellman (DH)	• Diffie-Hellman per NIST SP900-56A • DH >= 112 bits of security (i.e., len(n) >= 224).	**Y** CVL (KAS)	**Y** ECDH-E using P-256 curve (**Note 1**)	**Y** ECDH-E using P-521 curve (**Note 1**)
6 – Key Agreement using RSA			**Not applicable** – UA and CS prototypes use Diffie-Hellman key agreement in lieu of RSA; refer to previous row.	
7 – Key Wrapping			**Not applicable** – Key wrapping not required for the UA and CS prototype implementations.	
8 – Deriving Additional Keys from a Crypto-graphic Key	• HMAC per FIPS 198 or • CMAC per SP 800-38B plus AES-128 per FIPS 197	**Y** KDF	**Y** HMAC-SHA-384	**Y** HMAC-SHA-256

NIST SP 800-131A, Rev.2		Compliance		
Section – Algorithm	**Requirement(s)**	**wolfSSL Crypto Library per Table 4-13**	**UA and CS Prototype Implementation (reference Section 4.5.1.3)**	
			AEAD Configuration	**NULL Configuration**
	• Key derivation key >= 112 bits		(**Note 2**)	(**Note 2**)
9 – Hash Functions	• Secure hash algorithm per NIST FIPS 180 • SHA-224, -256, -384, -512 acceptable	**Y** SHS	**Y** SHA-256 (DRBG) SHA-384 (KDF) SHA-512 (ECDSA)	**Y** SHA-1 (HMAC, **Note 3**) SHA-256 (DRBG, KDF) SHA-512 (ECDSA)
10 – Message Authentication Codes	• HMAC per FIPS 198; or • CMAC per SP 800-38B plus AES-128 per FIPS 197; or • GMAC per SP 800-38D plus AES-128 per FIPS 197; or • KMAC per SP 800-185 plus SHA3 per FIPS 202	Y GCM/GMAC plus AES	**Y** AES-256-GCM	Not applicable
		Y HMAC	Not applicable	**Y** HMAC-SHA1-160 (**Note 3**)

NOTES:

1. For each case, the selected curve meets the NIST SP 800-131A Rev.2 minimum length/strength requirements.
2. Per RFC 5246 [REF-5246], TLS v1.2 specifies the use of an HMAC-based pseudo-random function with SHA-256, unless a stronger hash is specified, to generate symmetric keys for message authentication and confidentiality.
3. Per NIST SP 800-131A Rev.2, any approved hash algorithm per NIST FIPS 180-4, which includes SHA-1, may be used for HMAC as long as the key size is greater than 112 bits.

Result = **PASS**: This inspection demonstrates that the cryptographic module was configured to use algorithms with strength and key length requirements per NIST SP-800-131A, Rev. 2 in compliance with the MOC for SER-05 / SER-12.

C. INSPECTION RESULTS – VPN FOR PROTECTING THE UA-TO-C2CSP AND C2CSP-TO-CS COMMUNICATION LINKS

The UA and CS systems under test implement a VPN that provides protections to satisfy the following DO-377A MASPS security requirements:

- **SER-14** (User Plane traffic) – Air/ground network connection between the CS and C2CSP secured in accordance with SER-01 through SER-06[2].
- **SER-15** (User Plane traffic) – Air/ground network connection between the UA and C2CSP secured in accordance with SER-01 through SER-06.
- **SER-16** (Control Plane traffic) – Air/ground network connection between the CS and C2CSP secured in accordance with SER-08 through SER-13.
- **SER-17** (Control Plane traffic) – Air/ground network connection between the UA and C2CSP secured in accordance with SER-08 through SER-13.

As documented previously in the [SRS], formal FIPS validation per SER-06 / SER-13 is out-of-scope of this project. Therefore, the inspection of SER-14 / SER-15 requirements considers only SER-01 through SER-05, and the inspection of SER-16 / SER-17 considers only SER-08 through SER-12. As described previously in Appendix B of this report, the inspection examines pairs of requirements, e.g., SER-01 and SER-08, where the security requirements for User Plane traffic and Control Plane traffic specify the same MOC. Refer to Table B-1 in Appendix B of this report for the requirement text and MOCs for the applicable security requirements.

Section C.1 summarizes the cryptographic characteristics of the selected VPN, and Section C.2 provide the inspection results for each of the requirement pairs identified previously in Table B-1.

C.1 CRYPTOGRAPHIC CONFIGURATION INSPECTION

C.1.1 Cryptographic Characteristics

The UA and CS systems under test leverage the commercial off-the-shelf (COTS) WireGuard® VPN software to protect both User Plane and Control Plane traffic exchanged between the UA and CS via the UA-to-C2CSP and C2CSP-to-CS communication links. WireGuard VPN is open source software (i.e., GLPv2 license similar to OpenVPN) that employs start-of-the-art cryptography as described in a WireGuard whitepaper [WG-VPN]. Many commercial VPN service providers leverage WireGuard as the underlying VPN protocol; the list of service providers include NordVPN®, Surfshark®, ProtonVPN, VyprVPN™, MozillaVPN®, and dozens more.

The WireGuard VPN implementation uses the single cipher suite `Noise_IKpsk2_25519_ChaChaPoly_BLAKE2s`. Although the underlying crypto-algorithms used by WireGurad are not certified under the NIST Crypto Algorithm Validation Program (CAVP), the algorithms are specified in industry-standard Internet RFCs, as summarized in the following table:

[2] For User Plane traffic, the SER-14 / SER-15 requirements in DO-377A specify compliance with SER-01 through SER-07. In feedback provided previously to the FAA and RTCA SC-228, Honeywell proposed removing the reference to SER-07 since it not practical for air-ground and ground-ground network connections to enforce access controls between the UA and CS C2 Link Management Systems. This proposal was accepted and the draft DO-377B MASPS removes SER-07 from SER-14 / SER-15, which now specify compliance with SER-01 through SER-06.

Table C-1 – WireGuard Cryptographic Algorithms

Algorithm	Use	Characteristics	Standard
ChaCha20-Poly1305	Encryption/decryption with Authentication	Key Size: 256 bits Mode: AEAD Tag Length: 128 bits	RFC 8439
ECDH	Key Agreement	Curve: Curve25519 (256-bit key)	RFC 8418 (ECDH) RFC 7748 (curve)
KDF	Key Derivation Function	Mode: HMAC-based Hash: BLAKE2	RFC 5869
HMAC	Message authentication code generation and verification	Mode: Hashed Message Authentication Code Hash: BLAKE2	RFC 2104
Hash	Message digest generation	Hash: BLAKE2	RFC 7693

C.1.2 VPN Configuration

Figure 0-1 shows the server configuration used during test flights for the WireGuard VPN software.

```
[Interface]
Address = 10.10.0.2/24
ListenPort = 1191
PrivateKey = cOkrVrL1ldUE+pW999LMZyv17B8pzPLGcGiovWVMAU0=

[Peer]
PublicKey = hfgyu5/i4ShDqNpVV58Xz0jWeejW6utqNzTM5HizxBk=
AllowedIPs = 10.10.0.1/32
```

Figure C-1: WireGuard VPN Software Configuration (Satcom Link)

C.2 SECURITY REQUIREMENT INSPECTION

C.2.1 SER-01 / SER-08 Compliance

The MOC for SER-01/SER-08 references NIST FIPS 140-2 Annex D [REF-140-2], which specifies approved key establishment techniques. The listed techniques include NIST SP 800-56A [REF-56A], Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. In the following table, the leftmost column summarizes the requirements that must be met to claim conformance with Section 10 of NIST SP 800-56A, and the rightmost columns indicate WireGuard VPN compliance, with support comments as necessary:

Table C-2 – Compliance with NIST SP 800-56A

NIST SP 800-56A	Compliance	
Requirement	WireGuard VPN	Comments
Elliptic Curve (EC) cryptography plus use of a NIST-recommended elliptic curve	Y	WireGuard VPN uses Elliptic Curve Cryptography with Curve25519, which is a NIST-recommended curve per SP800-186. Curve25519 uses a 256-bit key which provideS 128 bits of security, similar to the secp256r1 curve that is used for the C2 Link System (DTSR-to=DTSR) security.
Approved key agreement scheme	Y	WireGuard VPN uses ECDH for key agreement,

NIST SP 800-56A	Compliance	
Requirement	WireGuard VPN	Comments
Approved hash function	N	WireGuard VPN uses the BLAKE2 algorithm as the underlying hash function. The BLAKE2 algorithm is not a NIST-approved hash algorithm; HOWEVER, it was one of the top 5 finalists out of a field of 51 entrants for the NIST hash competition.
Approved random bit generation	N	WireGuard uses the Noise framework for random bit generation, which relies on the /dev/random and /dev/urandom devices under Linux (Ubuntu and Raspberry PI OS). The kernel uses a ChaCha20-based cryptographic pseudorandom number generator that is not NIST-approved.
Approved key derivation function	N	WiredGuard VPN uses an HMAC-based key derivation function per RFC 5869, but the underlying BLAKE2 hash algorithm is no a NIST-approved algorithm.
A MAC tag length greater than or equal to 64 bits (for all elliptic curve sizes and domain parameters)	Y	WireGuard VPN generates HMAC tags that are 128 bits in length, which exceeds the 64-bit requirement,

Result = **PARTIAL**: This inspection shows that WireGuard is partially compliant with the key establishment scheme and associated MAC tag requirements in NIST FIPS 140-2 Appendix D. Refer to the Result in Section C.2.4 for additional considerations.

C.2.2 SER-02 / SER-09 and SER-03 / SER-10 Compliance

Per Section B.1.1, the WireGuard VPN implementation uses the ChaCha20 encryption algorithm with Poly1305 authenticator to provide authenticated encryption with associated data (AEAD). The encryption key size is 256 bits, which provides 128 bits of security, the same as AES256. ChaCha20-Poly1305 produces a non-truncated 128-bit (16 byte) authentication tag, which is the same length as the tag produced by AES256 operating in GCM mode.

Note that the ChaCha20 and Poly1305 algorithms are specified in cipher suites (e.g., `TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256` registered on the IANA web site) for use with TLS v1.2 or DTLS v1.2 (or later versions) per RFC 7905. This demonstrates industry confidence in the security robustness of these algorithms.

Result = **PASS**: This inspection demonstrates that the WireGuard VPN implementation uses an AEAD mode and produces a non-truncated 128-bit (16 byte) authentication tag that satisfies the MOC equivalency for SER-02 / SER-09 and SER-03 / SER-10.

C.2.3 SER-04 / SER-11 Compliance

The MOC for SER-04 / SER-11 specify AES-CCM or AES-GCM, both of which provide AEAD, as an acceptable MOC. As reported in Appendix B in this report, the C2 Link System (DTSR-to-DTSR) security implementation uses AES-GCM with 256-bit keys, which provides 128 bits of security.

Similarly, the WireGuard VPN implementation uses the ChaCha20 encryption algorithm with Poly1305 authenticator to provide AEAD. The encryption key size is 256 bits, which provides 128 bits of security, the same as AES256. ChaCha20-Poly1305 produces a non-truncated 128-bit (16 byte) authentication tag, which is the same length as the tag produced by AES256 operating in GCM mode. As noted in the previous section, the ChaCha20 and Poly1305 algorithms are specified for use with TLS/DTLS.

Result = **PASS**: This inspection demonstrates that the WireGuard VPN implementation uses an authenticated encryption mode that provides data confidentiality with 128 bits of security and that satisfies the MOC equivalency for SER-04 / SER-11.

C.2.4 SER-05 / SER-12 Compliance

This section summarizes WireGuard VPN compliance with the algorithm, strength, and key length requirements per NIST SP 800-131A, Rev. 2. In the following table, the first two columns enumerate the algorithm-specific requirements contained in the NIST document, the last two columns indicate WireGuard VPN compliance, with support comments as necessary.

Table B-3 – Compliance with NIST SP 800-131A, Rev. 2

NIST SP 800-131A, Rev.2		Compliance	
Section – Algorithm	**Requirement(s)**	**WireGuard VPN**	**Comments**
2 – Encryption and Decryption using Block Cipher Algorithms	• AES per NIST FIPS 197	N	WireGuarf VPN uses the ChaCha20 algorithm, which is used by industry but which is not a NIST-approved algorithm.
	• 128, 192, or 256-bit keys	Y 256 bits	WireGuard VPN uses the ChaCha20 algorithm with 256-bit keys which provides 128 bits of security.
	• Approved mode of operation per NIST SP 800-38 series	N	WireGuard VPN uses the ChaCha20 algorithm with Poly1305 to provide authenticated encryption per industry standards (RFC 8439); however, it does not use a NIST-approved mode of operation.
3 – Digital Signature	• DSA per NIST FIPS 186-4 • ECDSA len(n) >= 224	Not applicable	WireGuard VPN protocol does not use digital signatures,
4 – Random Bit Generation	• DRBG per SP 800-90A • Hash_DRBG or HMAC_DRBG using any hash per NIST FIPS 180	N	Wireguard VPN software relies on the /dev/urandom and /dev/random virtual devices for random bit generation under Linux. These devices implement a ChaCha20-based cryptographic

NIST SP 800-131A, Rev.2		Compliance	
Section – Algorithm	**Requirement(s)**	**WireGuard VPN**	**Comments**
			pseudorandom number generator which is not NIST-approved.
5 – Key Agreement using Diffie-Hellman (DH)	• Diffie-Hellman per NIST SP900-56A • DH >= 112 bits of security (i.e., len(n) >= 224).	**Y** ECDH using Curve25519	WiredGuard VPN uses Curve25519, which is a NIST-recommended curve per SP800-186. The curve uses a 256-bit key that provides 128 bits of security.
6 – Key Agreement using RSA		**Note Applicable**	WireGuard VPN use Diffie-Hellman key agreement in lieu of RSA; refer to previous row.
7 – Key Wrapping		**Not Applicable**	WireGuard VPN does not use key wrapping.
8 – Deriving Additional Keys from a Crypto-graphic Key	• HMAC per FIPS 198 or • CMAC per SP 800-38B plus AES-128 per FIPS 197	**N** HMAC-BLAKE2	WireGuard VPN uses the BLAKE2 algorithm as the underlying hash function for HMAC computation. Refer to comment for "9 – Hash functions"
	• Key derivation key >= 112 bits	Y 256 bits	
9 – Hash Functions	• Secure hash algorithm per NIST FIPS 180 • SHA-224, -256, -384, -512 acceptable	**N** BLAKE2	WireGuard VPN uses the BLAKE2 algorithm as the underlying hash function. The BLAKE2 algorithm is not a NIST-approved hash algorithm; HOWEVER, it was one of the top 5 finalists out of a field of 51 entrants.for the NIST hash competition.
10 – Message Authentication Codes	• HMAC per FIPS 198; or • CMAC per SP 800-38B plus AES-128 per FIPS 197; or • GMAC per SP 800-38D plus AES-128 per FIPS 197; or • KMAC per SP 800-185 plus SHA3 per FIPS 202	**N** ChaCha20-Poly1305	WireGuard VPN uses the ChaCha20 algorithm with Poly1305 to provide authenticated encryption per industry standards (RFC 8439); however, it does not use a NIST-approved mode of operation.

Result = **PARTIAL**: This inspection shows that the industry standard algorithms used by WireGuard provide security strength and key lengths that are equivalent to the NIST-approved algorithms specified in NIST SP-800-131A, Rev. 2. HOWEVER, the underlying cryptographic algorithms themselves are not NIST-approved. Although the inspection results for SER-05 / SER-12 do not show full compliance with the MOC, other factors should be considered:

- As noted previously, WireGuard VPN has been adopted widely by commercial VPN service providers.
- WireGuard VPN has been subjected to independent cryptographic proof [INRIA], which analyzed the entire protocol and concluded that the protocol is cryptographically safe and achieves stated security goals of secrecy, forward secrecy, mutual authentication, session uniqueness, and resistance to denial of service attacks.
- Although OpenVPN and OpenSSL support NIST-approved algorithms, their code sizes are large (~400K lines of code) since they support multiple protocols (TLS, DTLS), many cipher suites (RSA-based, ECC-based), and many configuration options. By comparison, since WireGuard VPN is a focused solution, its code size is significantly (~100x) smaller, which offers a number of advantages: minimizes the attack surface, simplifies setup/configuration (i.e., less opportunity for mistakes), and improves performance (which is a key consideration for UAS C2 communications).
- The C2 Link System (DTSR-to-DTSR) security uses DTLS and a cipher suite that relies on NIST-approved algorithms, and the VPN uses the WireGuard VPN protocol and industry-standard algorithms. Together they provide two layers of security for exchanges between the UA and the CS. Having protocol and crypto-algorithm diversity mitigates the risk of both layers of security being compromised at the same time. In other words, there is still one layer of protection if the protocol/algorithms for the other layer are broken.

This page intentionally left blank.