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

NOTICES

This material is provided to the US Federal Aviation Administration under Contract No. 697DCK-22-C-00263.

Export Classification: EAR 5E002.a

EXPORT CONTROLLED - This information is subject to the Export Administration Regulations (EAR) pursuant to 15 C.F.R. Parts 730-774. Transfer of this technology by any means to a non-U.S. Person, whether in the United States or abroad without the proper U.S. government authorization is strictly prohibited. Violations of the EAR may be subject to both criminal and administrative penalties under the Export Control reform Act of 2018 (50 U.S.C. §§ 4801-4852).

© 2023 by Honeywell International Inc. All rights reserved.



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



Northern Plains UAS Test Site Grand Forks, ND

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

DOCUMENT REVISION LOG

TRADEMARK DISCLAIMER

All product and company names used in this document are trademarksTM or registered[®] trademarks of their respective owners. Trademark symbols are included on the first instance of the product or company name and are implied for all other instances that do not include the trademark symbol.

Table of Contents

1	INTROD	UCTION	4
	1.1 Pur	oose	4
	1.2 Sco	pe	4
	1.3 Doc	ument Overview	4
	1.4 Terr	ns and Abbreviations	5
	1.4.1	Acronyms	5
	1.4.2	Terminology	8
	1.5 App	licable Reference Documents	8
	1.5.1	Industry – RTCA	8
	1.5.2	Industry – NIST	9
	1.5.3	Industry – International Telecommunication Union (ITU)	9
	1.5.4	Industry – Internet Request for Comment (RFC)	9
	1.5.5	Project Documents	9
2	SYSTEM	I UNDER TEST CONFIGURATION	. 10
	2.1 Flig	ht Test Configuration	. 10
	2.1.1	Airborne System	. 10
	2.1.2	Ground System	. 12
	2.2 Flig	ht Test Component Summary	. 13
3	INSPEC	TION AND TEST REPORTING APPROACH	. 14
	3.1 Res	ult Reporting	. 14
	3.2 Res	ult Definitions	. 14
4	INSPEC	FION RESULTS	. 15
	4.1 Res	ults of Common Inspection Procedures	. 15
	4.1.1	IP_CM_001 – Crypto-Module Configuration	. 15
	4.1.2		0.00
		IP_CM_002 – User Data and Status Report Performance during All Flight Pha	202
		IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15	202
5	TEST RE	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 SULTS	. 19
5	TEST RE 5.1 Flig	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 CSULTS ht Test Results	. 19 . 19
5	TEST RF 5.1 Flig 5.1.1	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 CSULTS	. 19 . 19 . 19 . 19
5	TEST RF 5.1 Flig 5.1.1 5.1.2	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 CSULTS	. 19 . 19 . 19 . 19 . 22
5	TEST RF 5.1 Flig 5.1.1 5.1.2 5.1.3	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 SULTS	. 19 . 19 . 19 . 19 . 22 . 26
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 SULTS	. 19 . 19 . 19 . 22 . 26 . 30
5	TEST RF 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 CSULTS	. 19 . 19 . 19 . 22 . 26 . 30 . 33
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 SULTS	. 19 . 19 . 19 . 22 . 26 . 30 . 33 . 37
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6 5.1.7	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 CSULTS	. 19 . 19 . 19 . 22 . 26 . 30 . 33 . 37 . 40
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6 5.1.7 5.1.8 5.1.8	 IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 CSULTS	. 19 . 19 . 19 . 22 . 26 . 30 . 33 . 37 . 40 . 43
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6 5.1.7 5.1.8 5.1.9	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 SULTS	. 19 . 19 . 19 . 22 . 26 . 30 . 33 . 37 . 40 . 43 . 46
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6 5.1.7 5.1.8 5.1.9 5.1.10	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 CSULTS	. 19 . 19 . 19 . 22 . 26 . 30 . 33 . 37 . 40 . 43 . 46 . 49
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6 5.1.7 5.1.8 5.1.9 5.1.10 5.1.11	 IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 CSULTS	. 19 . 19 . 22 . 26 . 30 . 33 . 37 . 40 . 43 . 46 . 49 . 52
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6 5.1.7 5.1.8 5.1.9 5.1.10 5.1.11 5.1.12	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 SULTS	. 19 . 19 . 19 . 22 . 26 . 30 . 33 . 37 . 40 . 43 . 46 . 49 . 52 . 54
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6 5.1.7 5.1.8 5.1.9 5.1.10 5.1.11 5.1.12 5.1.13	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 SULTS	. 19 . 19 . 22 . 26 . 30 . 33 . 37 . 40 . 43 . 46 . 49 . 52 . 54 . 57
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6 5.1.7 5.1.8 5.1.9 5.1.10 5.1.11 5.1.12 5.1.13 5.1.14	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 SULTS	. 19 . 19 . 19 . 22 . 26 . 30 . 33 . 37 . 40 . 43 . 43 . 52 . 54 . 57 . 60
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6 5.1.7 5.1.8 5.1.9 5.1.10 5.1.11 5.1.12 5.1.13 5.1.14 5.1.15	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 SULTS	. 19 . 19 . 19 . 19 . 22 . 26 . 30 . 33 . 37 . 40 . 43 . 46 . 49 . 52 . 54 . 57 . 60 . 63
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6 5.1.7 5.1.8 5.1.9 5.1.10 5.1.11 5.1.12 5.1.13 5.1.14 5.1.15 5.1.16	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 SULTS	.19 .19 .19 .22 .26 .30 .33 .37 .40 .43 .46 .49 .52 .54 .57 .60 .63 .66
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6 5.1.7 5.1.8 5.1.9 5.1.10 5.1.11 5.1.12 5.1.13 5.1.14 5.1.15 5.1.16 5.1.17	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 SULTS	. 19 . 19 . 19 . 22 . 26 . 30 . 33 . 37 . 40 . 43 . 43 . 52 . 54 . 57 . 60 . 63 . 66
5	TEST RH 5.1 Flig 5.1.1 5.1.2 5.1.3 5.1.4 5.1.5 5.1.6 5.1.7 5.1.8 5.1.9 5.1.10 5.1.11 5.1.12 5.1.13 5.1.14 5.1.15 5.1.16 5.1.17 5.1.16 5.1.17 5.1.18	IP_CM_002 – User Data and Status Report Performance during All Flight Pha 15 SULTS	. 19 . 19 . 19 . 19 . 22 . 26 . 30 . 33 . 37 . 40 . 43 . 43 . 43 . 43 . 52 . 54 . 57 . 60 . 63 . 66 . 68

<i>J.2</i> 010	und Test Results	75
5.2.1	Ground-based Tests – 1-of-2	75
5.2.2	Ground-based Tests – 2-of-2	79
5.3 Lin	K Switchover Timing Analysis	
6 SUMMA	RY AND RECOMMENDATIONS	
6.1 Sun	nmary	
6.1.1	APNT with Honeywell Vision Aided Navigation (VAN)	
6.2 Rec	ommendations and Lessons Learned	
6.2.1	Program Management Lessons Learned	
6.2.2	Recommendations and Lessons Learned for Future Flight Tests	
6.2.3	Software Improvements to the C2 Application	
6.2.4	Software Development Considerations	
6.2.5	C-Band Connection and Link Lessons Learned	
6.2.6	C2 Link Routing Approach	
6.2.7	Honeywell VAN Recommendations	
A. EXPECT	ED RESULTS	
A.1 Cor	nmon Test Procedures	
A.1.1	TP_CM_001 - Control Plane and User Plane Traffic Mutual Authentication	on with
User Plan	ne Traffic Access Control Allowed	
A.1.2	TP_CM_002 - User Plane Traffic Mutual Authentication with UA Access	s to the
CS Denie	2d	102
A.1.3	TP_CM_003 – User Plane Traffic Mutual Authentication with CS Access	s to the
UA Deni	ed	106
A.1.4	TP_CM_004 – User Data Exchanges with Encryption	110
A.1.5	TP_CM_005 – User Data Exchanges without Encryption	114
A.1.6	TP CM 006 – User Data and Control Message Exchange with interruptic	∩n <
TET	118	511 5
ТЕТ А.1.7	118 TP CM 007 – Control Message Exchanges with Encryption	123
TET A.1.7 A.1.8	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption	123
TET A.1.7 A.1.8 A.1.9	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET	123 125 126
TET A.1.7 A.1.8 A.1.9 A.1.10	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery	123 125 126 133
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination	123 125 126 133 139
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination ect-Specific Test Procedures	123 125 126 133 139 144
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination rect-Specific Test Procedures TP_C2_001 – Flying Out of C-Band Range	123 125 126 133 139 144 144
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination iect-Specific Test Procedures TP_C2_001 – Flying Out of C-Band Range TP_C2_003 – C2 Link Loss and Recovery	123 125 126 133 139 144 144 155
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 A.2.2 TP	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination ect-Specific Test Procedures TP_C2_001 – Flying Out of C-Band Range TP_C2_003 – C2 Link Loss and Recovery C2_004 Link Switchovers	123 125 126 133 139 144 144 155 160
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 TP B. INSPEC	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination iect-Specific Test Procedures TP_C2_001 – Flying Out of C-Band Range TP_C2_003 – C2 Link Loss and Recovery C2_004 Link Switchovers FION RESULTS – UAS C2 LINK SYSTEM SECURITY	123 125 126 133 139 144 144 155 160 168
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 A.2.2 TP B. INSPEC B.1 Cry	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination ect-Specific Test Procedures TP_C2_001 – Flying Out of C-Band Range TP_C2_003 – C2 Link Loss and Recovery C2_004 Link Switchovers TION RESULTS – UAS C2 LINK SYSTEM SECURITY ptographic Configuration Inspection	123 125 126 133 139 144 144 155 160 168 169
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 TP B. INSPEC B.1 Cry B.1.1	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination iect-Specific Test Procedures TP_C2_001 – Flying Out of C-Band Range TP_C2_003 – C2 Link Loss and Recovery C2_004 Link Switchovers TION RESULTS – UAS C2 LINK SYSTEM SECURITY ptographic Configuration Inspection Cryptographic Library Characteristics	123 125 126 133 139 144 144 155 160 168 169
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 TP B. INSPEC B.1 Cry B.1.1 B.1.2	 118 TP_CM_007 – Control Message Exchanges with Encryption	123 125 126 133 139 139 144 144 155 160 168 169 169 170
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 TP B. INSPEC B.1 Cry B.1.1 B.1.2 B.1.3	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination ject-Specific Test Procedures TP_C2_001 – Flying Out of C-Band Range TP_C2_003 – C2 Link Loss and Recovery C2_004 Link Switchovers TION RESULTS – UAS C2 LINK SYSTEM SECURITY ptographic Configuration Inspection Cryptographic Library Characteristics Cryptographic Library Build Application Configurations	123 125 126 133 139 144 144 144 155 160 168 169 169 170 170
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 TP B. INSPEC B.1 Cry B.1.1 B.1.2 B.1.3 B.2 Sec	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination ject-Specific Test Procedures TP_C2_001 – Flying Out of C-Band Range TP_C2_003 – C2 Link Loss and Recovery C2_004 Link Switchovers FION RESULTS – UAS C2 LINK SYSTEM SECURITY ptographic Configuration Inspection Cryptographic Library Characteristics Cryptographic Library Build Application Configurations urity Requirement Inspection	123 125 126 133 139 144 144 155 160 168 169 169 170 170 171
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 TP B. INSPEC B.1 Cry B.1.1 B.1.2 B.1.3 B.2 Sec B.2.1	118 TP_CM_000 - Control Message Exchanges with Encryption TP_CM_008 - Control Message Exchanges without Encryption TP_CM_009 - Link Switchover < TET TP_CM_010 - Link Switchover > TET with Link Recovery TP_CM_011 - Control Plane and User Plane Traffic Link Termination ject-Specific Test Procedures TP_C2_001 - Flying Out of C-Band Range TP_C2_003 - C2 Link Loss and Recovery C2_004 Link Switchovers FION RESULTS - UAS C2 LINK SYSTEM SECURITY ptographic Configuration Inspection Cryptographic Library Characteristics Cryptographic Library Build Application Configurations rity Requirement Inspection SER-01 / SER-08 Compliance	123 125 126 133 139 139 144 144 144 155 160 168 169 169 170 170 171 171
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 A.2.2 TP B. INSPEC B.1 Cry B.1.1 B.1.2 B.1.3 B.2 Sec B.2.1 B.2.2	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination ject-Specific Test Procedures TP_C2_001 – Flying Out of C-Band Range TP_C2_003 – C2 Link Loss and Recovery C2_004 Link Switchovers FION RESULTS – UAS C2 LINK SYSTEM SECURITY ptographic Configuration Inspection Cryptographic Library Characteristics Cryptographic Library Build Application Configurations urity Requirement Inspection SER-01 / SER-08 Compliance SER-02 / SER-09 and SER-03 / SER-10 Compliance	123 125 126 133 139 144 144 155 160 168 169 170 170 171 172
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 TP B. INSPEC B.1 Cry B.1.1 B.1.2 B.1.3 B.2 Sec B.2.1 B.2.2 B.2.3	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination ject-Specific Test Procedures TP_C2_001 – Flying Out of C-Band Range TP_C2_003 – C2 Link Loss and Recovery C2_004 Link Switchovers FION RESULTS – UAS C2 LINK SYSTEM SECURITY ptographic Configuration Inspection Cryptographic Library Build Application Configurations urity Requirement Inspection SER-01 / SER-08 Compliance SER-04 / SER-11 Compliance	123 125 126 133 139 144 144 155 160 168 169 170 171 172 172
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 TP B. INSPEC B.1 Cry B.1.1 B.1.2 B.1.3 B.2 Sec B.2.1 B.2.2 B.2.3 B.2.4	118 TP_CM_007 – Control Message Exchanges with Encryption TP_CM_008 – Control Message Exchanges without Encryption TP_CM_009 – Link Switchover < TET TP_CM_010 – Link Switchover > TET with Link Recovery TP_CM_011 – Control Plane and User Plane Traffic Link Termination ject-Specific Test Procedures TP_C2_001 – Flying Out of C-Band Range TP_C2_003 – C2 Link Loss and Recovery C2_004 Link Switchovers FION RESULTS – UAS C2 LINK SYSTEM SECURITY ptographic Configuration Inspection Cryptographic Library Characteristics Cryptographic Library Build Application Configurations urity Requirement Inspection SER-01 / SER-08 Compliance SER-04 / SER-11 Compliance SER-05 / SER-12 Compliance	123 125 126 133 139 144 144 155 160 168 169 170 171 171 172 173
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 A.2.2 TP B. INSPEC B.1 Cry B.1.1 B.1.2 B.1.3 B.2 Sec B.2.1 B.2.2 B.2.3 B.2.4 C. INSPEC	118 TP_CM_007 - Control Message Exchanges with Encryption	123 125 126 133 139 144 144 155 160 168 169 170 171 172 172 173 22CSP-
TET A.1.7 A.1.8 A.1.9 A.1.10 A.1.11 A.2 Pro A.2.1 A.2.2 Pro A.2.1 A.2.2 TP B. INSPEC B.1 Cry B.1.1 B.1.2 B.1.3 B.2 Sec B.2.1 B.2.2 B.2.3 B.2.4 C. INSPEC TO-CS COM	 TP_CM_000 - Control Message Exchanges with Encryption	123 125 126 133 139 144 144 155 160 168 169 170 171 172 172 173 22CSP- 175

C.1.1	Cryptographic Characteristics	
C.1.2	VPN Configuration	
C.2 Sec	Purity Requirement Inspection	
C.2.1	SER-01 / SER-08 Compliance	
C.2.2	SER-02 / SER-09 and SER-03 / SER-10 Compliance	
C.2.3	SER-04 / SER-11 Compliance	
C.2.4	SER-05 / SER-12 Compliance	
	-	

Table of Figures

Figure 2-1. Airborne System Configuration for C2 System on Alta-X drone 1	0
Figure 2-2. Alta-X drone Configured for C2 System 1	1
Figure 2-3. Airborne System Configuration for VAN System on Cessna1	2
Figure 2-4. Ground System Configuration	2
Figure 5-1. Itasca Flight 1 Path	2
Figure 5-2. Itasca Flight 1 Performance	3
Figure 5-3. Itasca Flight 2 Path	4
Figure 5-4. Itasca Flight 2 Performance	4
Figure 5-5. Average Switchover Times, measured at the UA	5
Figure 6-1. C-Band data path from UA to CS. Using uAvionix SkyLine (top), and without	
SkyLine (bottom)	3
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	4
antenna	5
Figure C-1: WireGuard VPN Software Configuration (Satcom Link) 17	6

List of Tables

Table 2-1. SUT Component Summary	13
Table 3-1. Result Definitions	14
Table 4-1. Average Link Latency per flight for 006-C2	17
Table 4-2. User Plane Message delivery rate per flight for 006-C2	17
Table 5-1. Lost Link Events for C2 Flight #1	22
Table 5-2. Lost Link Events for C2 Flight #2	25
Table 5-3. Lost Link Events for C2 Flight #3	29
Table 5-4. Lost Link Events for C2 Flight #4	33
Table 5-5. Lost Link Events for C2 Flight #6	39
Table 5-6. Lost Link Events for C2 Flight #7	42
Table 5-7. Manual Commanded Switchovers for C2 Flight #8	45
Table 5-8. Lost Link Events for C2 Flight #8	45
Table 5-9. Lost Link Events for C2 Flight #9	48
Table 5-10. Lost Link Events for C2 Flight #14	51
Table 5-11. Lost Link Events for C2 Flight #15	53
Table 5-12. Manually Commanded Switchovers C2 Flight #16	56
Table 5-13. Lost Link Events for C2 Flight #16	56
Table 5-14. Lost Link Events for C2 Flight #17	59
Table 5-15. Manually Commanded Switchovers for C2 Flight #10	62

62
65
67
67
70
70
85
87
88

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 visionaided 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			
СМ	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			
	Inertial Measurement Unit			
IP ID: 1 / ID: 6	Inspection Procedure			
IPV4/IPV0	Internet Protocol Version 4 / Version 6			
	International Telecommunication Union			
KPI	Key Performance Indicator			
kte	Ky renormance indicator			
IMSE	Link Management and Security Function			
	Line of Sight			
LSMA	Local Storage and Management Application			
LTE	Long Term Evolution			
LTS	Long Term Support			
LWIR	Long Vavelength 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			
ТСР	Transport Control Protocol			
ТР	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.
	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-	
		<u>131Ar2.pdf</u>	
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 <u>https://www.itu.int/rec/T-REC-X.509-201910-I/en</u>	

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 machine¹ 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.

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	HW: Processor	Raspberry Pi 4B	e4:5f:01:05:42:9b	N/A	RPI #8
Link System	HW: Ethernet Switch	Netgear ProSafe Plus GS105E	N/A	N/A	
Under	HW: SATCOM Radio	Honeywell Versawave Satcom+5G	11	N/A	Engineering Prototype
Test	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	
	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	
C-Band Ground	HW: C-Band GRS Radio	uAvionix UAV-1006090-001	6200058	Firmware v0.4.12	GPS2 PadialD: 0x0100220020
Radios	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	
	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
CS C2 Link	SW: Operating System (VM)	Ubuntu 20.04 (Focal) Linux	N/A	20.04.6 LTS x86_64	Kernel: 5.15.0-72-generic
Under Test	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	

Table 2-1. SUT Component Summary

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 <u>not</u> 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.

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

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

	User Messages	User Messages	
	Sent	Received	Success Rate
Flight ID	(uplink + downlink)	(uplink + downlink)	(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%

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

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. 10:21 Arming (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
TP_C2_003A (Departure)	C2 Link Loss and Recovery	PASS	observed. 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 Ite 10:38 Status 2, LTE Up nominal
TP_C2_003A (Cruise)	C2 Link Loss and Recovery	PASS	 10.38 Status 2, ETE Op 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
TP_C2_003A (Arrival)	C2 Link Loss and Recovery	PASS	then Reenable 10:44 Status Secure Y/2 good. observed TET notification.
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.

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

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

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
			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
TP CM 001	Control / User Plane	PASS	up, C-Band down. nominal good
	authentication	1100	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
	User Data avalar and < MTU	DACC	stream, then UA.
II_CM_004A	User Data exchanges < WITU	LUDO	11.37 UA sellu II-1, lecu Iu-4, 11.38 switch 3 but link is down
			ISSUE/FRROR C-Band is down
TP C2 003A			11.38 set tet=3
(Begin)	C2 Link Loss and Recovery	PASS	11:30 UA status secure: $Y/2$ then
(2-8)			CS. Y/2 good.
			11:39 cleared for takeoff.
			11:39 disable links 1, 3.
TP C2 003A		DACC	11:40 ARMING / takeoff Flight #2.
(Takeoff)	C2 Link Loss and Recovery	PASS	11:40 disable link 2, waited 3 sec,
			then enable link 2.
TP C2 003A			11:41 50 ft. CS and UA status
(Departure)	C2 Link Loss and Recovery	PASS	secure, Y/2 both, good, 100ft.
(Departure)			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. 11:46 UA status secure: Y/1 good. 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.
TP_C2_003A (Arrival)	C2 Link Loss and Recovery	PASS	 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.
TP_C2_003A (Land)	C2 Link Loss and Recovery	PASS	11:52 hovering landing. 11:53 LANDED / ON GROUND / Disarmed. END OF FLIGHT 11:53 CS status secure: Y/2, then UA Y/2
TP_CM_011	Control / User Plane Termination	PASS	 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.

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.

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

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



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.
TP_C2_003A (Begin)	C2 Link Loss and Recovery	PASS	 12:34 UA Set TET -5 good. 12:35 Status Secure UA, then CS. both Y/2 LTE, good. 12:36 cleared for takeoff.
TP_C2_003A (Takeoff)	C2 Link Loss and Recovery	PASS	 12:36 disabled links 3, and 1, then 2. TAKEOFF / ARMING / flight #3. 12:36 disable 2. wait 3 seconds. enable link 2. 12:36 observed TET exceeded notification.
TP_C2_003A (Departure)	C2 Link Loss and Recovery	PASS	 12:37 Climbing 100 ft. 150 ft. 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 Ite. 12:44 Set tet =3 descending.
TP_C2_003A (Arrival)	C2 Link Loss and Recovery	PASS	 available. 200 ft. waiting 3 sec. then reenable link 2. 12:45 150 ft. UA Status secure then CS Y/2 TET Exceeded notification. 12:46 disable link 2 with no others available. 50 ft landing waiting 3
TP_C2_003A (Land)	C2 Link Loss and Recovery	PASS	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 12:48 stopping data stream from CS And UA
TP_CM_011	Control / User Plane Termination	PASS	 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.

TimeStamp	Flight Phase	Time offline (ms)	Prev Link	New Link	Note
I	8				
09/06/2023 12:36:32.760423	Takeoff	34,947	LTE	LTE	Total Link Loss Recovery
		-)			5
09/06/2023 12:38:58.386448	Cruise	34.218	LTE	LTE	Total Link Loss Recovery
		0 ., 0			
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
0,,00,2020 12.10101010500	Destein	55,011	212	212	
09/06/2023 12:46:18.855143	Landing	34,927	LTE	LTE	Total Link Loss Recovery
07/00/2025 12:10:10:055115	Lunanig	51,927	LIL	LIL	

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



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
D 1	D	D	
Procedure	Description	Result	Notes
			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,
TP_CM_001	Control / User Plane	PASS	with nominal. then UA. same good nominal.
	aumentication		2:48 UA Secure Start good session on LTE.
			2:49 CS Status secure: Y/2, then UA, Y/2 both good
			2:50 CS starting continuous data
			stream. then UA.
TP_CM_004A	User Data exchanges < MTU	PASS	2:51 UA send n=1, recd id=4
			2:51 UA Switch 3. from LTE to C-
			Band.
TP C2 003B			2:52 UA Y/3 status secure, good.
(Begin)	C2 Link Loss and Recovery	PASS	2:52 Set $TET = 3$ on both good.
(8)			2:52 UA SWITCH 2 from C-Band to LTE
			2:53 Status secure $Y/2$ on both.
			2:54 ARMING / TAKEOFF /
TP_C2_003B	C2 Link Loss and Recovery	PASS	Disabled links 1, 3, then 2. All links
(Takeoff)	, i i i i i i i i i i i i i i i i i i i		lost. enable link 2.
			2:55 Climbing status Y/2, on UA
			then CS 250 ft.
			2:56 Enable link -1. switch to link 1.
TP_C2_003B	C2 Link Loss and Pacovery	DASS	Satcom. disable link 2.
(Departure)	C2 LINK LOSS and Recovery	FASS	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 Ite 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
TP_C2_003B (Land)	C2 Link Loss and Recovery	PASS	 landing 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. thensecure STOP. Status: N/1 on both.3:10 send n=1, not recd. good.

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

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

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



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. 3:35 starting data streams, cs, then
TP_CM_004A	User Data exchanges < MTU	PASS	UA. 3:36 UA Send n=1, recd id=4. good. 3:37 SWITCHOVER to 3 C-Band.
TP_C2_003B (Begin)	C2 Link Loss and Recovery	PASS	 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, then3. waited 3 seconds. 50ft. enablelink 3
TP_C2_003B (Departure)	C2 Link Loss and Recovery	PASS	3:40 enable link 2. cruising altitude. 3:41 set tet =5

Draadura	Description	Dogult	Notes
rocedure	Description	Result	notes
			1 disable 2 weit 5 see
			disabled 2 anabled 2 waiting for
			disabled 2. enabled 5. waiting for
			2:44 on C Band secure analing 1
			5.44 on C-Band secure. enabling 1,
			2. $2 \cdot 14$ status V/2 Exceeded TET
			3.44 status 1/3. Exceeded 1E1.
			5.44 C5 Status 125. auto
			3.45 switch to 2 manually link is
TP C2 003P			5.45 Switch to 5 manually. This is
(Cruise)	C2 Link Loss and Recovery	FAIL	3.46 disable 3 auto switched to
(Cruise)			I TE
			3:46 Status V/2 then CS_same
			good
			3:47 enable C-Band-3 all links now
			3.47 status 3. UP nominal
			3:48 switch 3 from Ite 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			3:50 Switch 2. from LTE to C-Band.
(Arrival)	C2 Link Loss and Recovery	FAIL	3:50 disable 1, 2 clear to return to
· · ·			land.
			3:51 disable 3. descending. 200 ft.
			enable 3. 150 ft.
TP_C2_003B	C2 Link Loss and Pacavary	FAT	3:52 disable 3. wait 3 sec. enable 3
(Land)	C2 Link Loss and Recovery	FAIL	enable 2.
			3:53 LANDED / ON GROUND
			3:54 observed TET exceeded.
			3:54 status: Y/3 C-Band good.
	Control / User Plane		3:55 stopping data stream. good.
TP_CM_011	Termination	FAIL	3:55 Secure STOP.
			3:56 Status N/3 both good.
			3:56 send n=1, not recd.

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. 4:20 start continuous data stream.
TP_CM_004A	User Data exchanges < MTU	PASS	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
TP_C2_003B (Begin)	C2 Link Loss and Recovery	PASS	 is down. 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!! 4:36 disabled 1 first (accidentally), enable 1, disabled 2, disable 1. lost
TP_C2_003B (Land)	C2 Link Loss and Recovery	FAIL	track 4:38 hovering cleared to land LANDED // ON GROUND / Disarmed End of flight #6 (15 minute flight) 4:39 status secure shows wrong status. ISSUE/ERROR UA shows N/2, CS shows Y/3, GUI shows Satcom active
TP_CM_011	Control / User Plane Termination	FAIL	 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

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.

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

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



006-C2 Flight #6 - 09/06/2023

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
TP_CM_004A	User Data exchanges < MTU	PASS	 good. 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
TP_C2_003C (Begin)	C2 Link Loss and Recovery	PASS	same both good. 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
TP_C2_003C (Takeoff)	C2 Link Loss and Recovery	PASS	UP, C-Band down. 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. 5:15 UA status: Y/1 CS: Y/1 5:16 Set TET 3 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.
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.

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.

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

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



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 4:20 UA Switch 3 from LTE to C-
TP_C2_003C (Begin)	C2 Link Loss and Recovery	PASS	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
Troccurre	Description	Ittojuit	4:22 CS Status Y/3
			enable 2,
TP_C2_003C	C2 Link Loss and Recovery	DASS	4:22 UA status Y/3, observed TET
(Departure)	C2 Link Loss and Recovery	I AOO	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 1/2.
			C-Dalid is liaky eliable 1,2.
			TET exceeded
			4.25 CS Status 123: all un nominal
			SWITCH 3 from satcom to
			C-Band.
TP C2 003C			4:26 disable 3, switched auto to LTE
(Cruise)	C2 Link Loss and Recovery	PASS	- 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.
			4:51 Instructed to go to center and
			SWITCH 3
			4.31 Disable 1 2
			4:32 return to land
			4:32 Disable 3. wait 3 sec. enable 3.
TP_C2_003C	C2 Link Loss and Recovery	PASS	4:33 on C-Band, status sec. $Y/3$
(Arrival)	5		4:33 coming to land. disable 3 (only
			link), wait 3 enable C-Band. good.
TP_C2_003C	C2 Link Loss and Bosovany	DACC	4:33 CS Status Y/3, enable 2 good.
(Land)	C2 Link Loss and Recovery	radd	4:34 LANDED. ON GROUND.
			4:34 UA status secure $Y/3$.
			CS Status Y/3, then UA Y/3
TP CM 011	Control / User Plane	PASS	UA Stop data streams
	Termination		4:35 UA Secure stop
			CS Status N/3, UA same N/3.
			send n=1, not recd, good.

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

Time (CDT)	From	То	Flight Phase	Switchover time (ms)	TET	<tet< th=""></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
Trocedure	Description	Kesuit	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.
TP CM 001	Control / User Plane	PASS	good.
	authentication		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	C2 Link Loss and Recovery	PASS	set TET=3 UA then CS.
(Begin)	5		4:56 UA status: $Y/3$, then CS $Y/3$
			4:56 CS Status 123. all up nominal.
			4:5/ cleared for takeoff Flight 9,
TP_C2_003C	C2 Link Loss and Recovery	DASS	4.57 APMING / SPININING /
(Takeoff)	C2 Link Loss and Recovery		TAKEOFE disable 3 wait 3 sec
			enable 3 good
			4:58 CS Status Y/2. ISSUE/ERROR
			gui shows secure on 3, but status says
TP_C2_003C	C2 Link Loss and Recovery	PASS	Y/2.
(Departure)	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.
			5:00 CS Status Y/3.
			5:01 enable 1,2 while on C-Band.
			good.
			UA Status Y/3 good.
			CS Status 122 all up nominal
TP C2 003C			5.02 all links up disable 3 auto
(Cruise)	C2 Link Loss and Recovery	PASS	switchover to LTE_ISSUE/FRROR
(Cruise)			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.
			5:05 CS Status, Y/3, good.
			5:05 Set TET=3.
$1P_C2_003C$	C2 Link Loss and Recovery	PASS	5:05 Disable 1, 2. Return to land.
(Arrival)	<u>,</u>		5:05 disable 5. Wait 5 sec. enable 3,
			up gooa.

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.
TP_CM_011	Control / User Plane Termination	PASS	UA Status: Y/3. 5:08 Status secure Y/3, both. stopping data streams. UA Secure STOP. session gone. 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

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.

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

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



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
			6:33 - cs ua: N/2 6:34 ua send n=1 not recd good.
TP_CM_001	Control / User Plane authentication	PASS	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. PSSL 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.
TP_C2_001 (Land)	BVLOS, Flying out of C- Band range	PASS	6:44 ua ¥/3 cs: ¥/3 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.

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

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



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. cs Y/3
TP_C2_001 (Takeoff)	BVLOS, Flying out of C- Band range	PASS	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	

D	Description	D14	NT- 4
Procedure	Description	Kesult	INotes
			7:00 cs: Y/3, ua: Y/3
			set TET =5
			100 ft cruising.
			7:01 lost C-Band autoswitchover to
TD C2 001	DVI OS Elvino out of C		LTE. no tet exceeded good
IP_C2_001	By LOS, Flying out of C-	PASS	ua Y/2. cs Y/2
(Cruise)	Band range		RSSI -80 / -88
			RSSI -100 / -90.
			C-Band is gray/green
			7:02 cs: Y/2. ua Y/2
			7:03 return to land.
			switch 3. good.
TP C2 001	BVLOS, Flying out of C-		autoswitchover to LTE.
(Arrival)	Band range	PASS	7:05 ua: $Y/2$ there is a TET
`	6		exceeded notification. but not on CS.
TP C2 001	BVLOS, Flying out of C-	DACC	
(Land)	Band range	PASS	1:05 LANDED / ON GROUND.
`	e		7:06 cs Y/2 ua: Y/2 good.
			stop data stream.
TP CM 011	Control / User Plane	PASS	7:06 secure stop. good.
	Termination		cs N/2. ua N/2.
			ua send n=1 not recd good.

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.

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

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



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 9:37 start user data stream. cs then ua.
TP_CM_004A	User Data exchanges < MTU	PASS	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 Drone positioned over antenna dead
TP_C2_001 (Cruise)	BVLOS, Flying out of C- Band range	PASS	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 ftdescending9:47 reached box at 100 ft.es status 122 all un 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.

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.

Time (CDT)	From	То	Flight Phase	Switchover time (ms)	TET	<tet< th=""></tet<>
9:38	LTE	C-Band	surface	1,894	3,000	Y
9:47	LTE	C-Band	arrival	11,813	3,000	Ν

Table 5-12. Manually Commanded Switchovers 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

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



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	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.
11_011_001	authentication		good. ua secure start. up on LTE good. cs Y/2, ua: Y/2 good. 10:02 cs start continuous data stream, then ua. good.
TP_CM_004A	User Data exchanges < MTU	PASS	10:02 ua send n=1 recd id=4 good. 10:02 switch 3. from LTE to C-Band good.
TP_C2_001 (on ground)	BVLOS, Flying out of C- Band range	PASS	cs Y/3 10:03 set tet =3 ready for takeoff 10:03 ARMING / TAKEOFF
TP_C2_001 (Departure)	BVLOS, Flying out of C- Band range	PASS	 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. reached far position. C-Band shows
TP_C2_001 (Cruise)	BVLOS, Flying out of C- Band range	PASS	 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.

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.

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

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



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
	-		5:19 Secure Start session on LTE. all
TP_CM_001	Control / User Plane authentication	PASS	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
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 - ellum nominal.
TP_C2_004	C2 Switchovers	PASS	5.25 OA status 125. an up nominal.
(departure) 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.
TP_C2_004 (arrival)	C2 Switchovers	FAIL	UA Set TET =3 5:27 Return to land. UA switch 3 slooow to switch still on LTE. GOOD. 5:28 gui on 3. 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

Time (CDT)	From	То	Flight Phase	Switchover time (ms)	TET	<tet< th=""></tet<>
17:22	LTE	satcom	takeoff	2,594	5,000	Y
17:22	satcom	C-Band	departure	10,905	5,000	Ν
17:24	LTE	C-Band	cruise	1,666	5,000	Y
17:25	LTE	C-Band	cruise	19,871	5,000	Ν
17:25	C-Band	satcom	cruise	2,230	5,000	Y
17:26	satcom	LTE	cruise	10,766	5,000	Ν
17:27	LTE	C-Band	arrival	7,723	3,000	Ν
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 5-15. Manually Commanded Switchovers for C2 Flight #10

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
TP_CM_004A	User Data exchanges < MTU	PASS	set tet=3 5:42 status: Y/2. both good. 5:42 cleared for takeoff.
TP_C2_004 (on ground)	C2 Switchovers	PASS	5:44 ARMING / TAKEOFF switch 1. good. all up.
TP_C2_004 (departure)	C2 Switchovers	PASS	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.
TP_C2_004 (cruise)	C2 Switchovers	PASS	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.
TP_C2_004 (arrival)	C2 Switchovers	FAIL	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.
TP_CM_011	Control / User Plane Termination	PASS	ua stop data streams. 5:50 ua secure stop. ua N/1, cs: N/1 5:50 ua send n=1. not recd.

Time (CDT)	From	То	Flight Phase	Switchover time (ms)	TFT	<tft< th=""></tft<>
	110111	10	i iigiit i iidse	Switchover time (ms)	111	1111
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	Ν
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

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



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
TP_C2_004 (departure)	C2 Switchovers	PASS	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
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
TP_C2_004 (arrival)	C2 Switchovers	PASS	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 /
TP_CM_011	Control / User Plane Termination	PASS	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.

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

Time (CDT)	From	То	Flight Phase	Switchover time (ms)	TET	<tet< th=""></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
			6:12 starting flight 13
			cs N/2 ua N/2
			ua send n=1, not recd.
			all links green.
TP CM 001	Control / User Plane	DASS	cs status 125. an inks up nominal
	authentication		6:13 ua status 123 all links un
			nominal good.
			6:13 secure start. gui shows session
			on LTE.
			cs Y/2 ua: Y/2 both good.
			6:14 start continuous data stream.
TP_CM_004A	User Data exchanges < MTU	PASS	ua send $n=1$, recd $1d=10$.
TP C2 004			set $tet = 5$
(on ground)	C2 Switchovers	PASS	
			6:15 ua: Y/2 cs: Y/2
TP C2 004			6:16 ARMING / SPINNING /
(departure)	C2 Switchovers	PASS	TAKEOFF
			switch lua Y/1. 50 ft. cs: Y/1
			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.
TP_C2_004	C2 Switchovers	FAIL	set tet =5. 6:17 switch 3 up $V/3$ as: $V/3$
(cruise)	C2 Switchovers	rail	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.
			6.19 return to land command
			switch 3. good.
			ua Y/3 cs: Y/3
TP C2 004			switch 1. good.
(arrival)	C2 Switchovers	FAIL	ua: Y/1 cs: Y/1
			switch 2 TET exceeded
			6.20 switch 1 good
			LANDED / ON GROUND
			ua cs Y/1 *** NOTICED
			Satcom went down briefly, and
TP CM 011	Control / User Plane	PASS	exceeded TET??
	Termination		6:21 secure stop.
			cs: $IN/1$, ua $IN/1$ send $n=1$ not read good
			sena n=1 not reca good.

				-		
Time (CDT)	From	То	Flight Phase	Switchover time (ms)	TET	<tet< td=""></tet<>
18:16	LTE	satcom	takeoff	3,178	3,000	Y
18:16	satcom	C-Band	departure	10,951	3,000	Ν
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 5-20. Manually Commanded Switchovers for C2 Flight #13

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
TP_VN_002	VAN System Flight Procedure	PASS	9:10 – Camera Enabled 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

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.



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 – Carl S Enabled 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

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 \sim 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	
	User Data Exchanges without		10:30 TP-CM-005-a (less than
TP_CM_005A	Encryption, Payload Data	PASS	MTU)
	<mtu< td=""><td></td><td>send N=1, recd ID=10 good.</td></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. 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.
TP_CM_009	Link Switchover < TET	PASS	 switch 1. from ite 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.
TP_CM_011	Control Plane and User Plane Link Termination	FAIL	10:50 stop data streams. 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.

Procedure	Description	Result	Notes
Procedure TP_CM_003	Description User Plane Traffic Mutual Authentication with CS Access to the UA Denied	Result	Notes 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.
		FAIL	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).

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		11:04 configured for NULL
	Traffic Mutual		encryption.
	Authentication with User		11:05 cs: N/2, ua N/2
	Plane Traffic Access Control		11:06 cs status 123 all up nominal.
	Allowed		good. then ua. all up nominal.
		PASS	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	PASS	
	without Encryption		
TP_CM_005A	User Data Exchanges without		11:08 TP-CM-005-a
	Encryption, Payload Data	PASS	11:08 ua send n=1, recd 1d=24.
TD CM 005D	<miu User Dete Erschen des with est</miu 		good.
TP_CM_003B	User Data Exchanges without		from CS common de son UA > CS wie
	SMTU	PASS	SCP
	-M10		SCF 11.10 "TP CM 005B 2 tyt"
TP CM 000	Link Switchover < TET		11.10 II-CW-005D-2.1At $11.12 cs status 123 all un nominal$
			good then UA both good all up
			nominal good
			11.13 ua SWITCH 1 from LTE to
			Satcom, good
		PASS	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		11:15 TP-CM-011
	Link Termination		11:16 cs status Y/1, ua: Y/1.
		PASS	11:16 stopping user data streams.
		IAOO	ua secure stop. good.
			cs N/1, µa N/1

cs N/1, ua N/1 11:17 ua send n=1, not recd, good.

Draadura	Description	Docult	Notos
TP_CM_002	User Plane Traffic Mutual Authentication with UA Access to the CS Denied	Result	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.
TP_CM_003	User Plane Traffic Mutual Authentication with CS Access to the UA Denied	FAIL	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. 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)
		FAIL	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.

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-AAAAAAAAAAAAAAAAAAAAO00006
Sending user data message to peer
User Output: Sent 66 bytes.
```

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

	cs.main.sniffer.2023.09.08-09.54.40.pcapng						
Fil	e Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
	III 🖉 🐵 📙 🔤 💐 📽 🗢 🕾 🕾 🕢 📃 🚍 🔍 Q. Q. II						
	ipv6.addr == fd00:bbcc:dde0::a ipv6.addr == fd00:bbcc:dde0::f						
No.	Time Source Destination Protocol Length Info						
	90326 5206.4687408 fd00:bbcc:dde0::a fd00:bbcc:dde0::f UDP 71 3663	8 → 511	03 Le	en=3			
Ĺ	90367 5209.4689154 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2 171 Appl	ication	Data	a –			
	90368 5209.4690155 fd00:bbcc:dde0::a fd00:bbcc:dde0::f UDP 71 36638	8 → 511	03 Le	en=3			
<							
~	Frame 90367: 171 bytes on wire (1368 bits), 171 bytes cantured (1368 bits) on interface t	0000	45.0	0 00			
	Section number: 1	0010	0a 1	4 00			
	Interface id: 2 (tun2)	0020	dd e	0 00			
	Encapsulation type: Raw IP (7)	0030	dd e	0 00			
	Arcival Time: Sen 8, 2003 09:21:30 438127921 Pacific Davlight Time	0040	00 6	f 2d			
	[Time shift for this packet: 0.000000000 seconds]	0050	5a †	9 46			
	Ench Time: 1694190090.438127921 seconds	0000	4C ð 57 þ	9 08 9 9 0			
	[Time delta from previous captured frame: 0.286970946 seconds]	0080	fd 6	e a6			
	[Time delta from previous displayed frame: 3.000174556 seconds]	0090	75 c	a 55			
	[Time since reference or first frame: 5209.468915423 seconds]	00a0	29 9	9 f9			
	Frame Number: 90367						
	Frame Length: 171 bytes (1368 bits)						
	Capture Length: 171 hytes (1368 hits)						
	[Frame is marked: False]						
	[Frame is ignored: False]						
	[Prome is ignored, reast]						
	[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						

Step 17 fails.

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



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

Flight			Time				Switchover		<tet< th=""></tet<>
No	System	Date	(CDT)	From	То	Flight Phase	time (ms)	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	Ŷ
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	Ŷ
7	CS	6-Sep	17:14	LTE	satcom	cruise	2,341	5,000	Ŷ
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	Ŷ
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-Sen	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	Ŷ
0	CS	7 Sop	17:03	LTE	C Band	aruico	1 291	5,000	v

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

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	CS	7-Sep 7-Sep	17:22	satcom	C-Band 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	UA	7-Sep 7-Sep	17:25	C-Band	C-Band satcom	cruise	2 230	5,000	Y
10	CS	7-Sep	17:25	C-Band	satcom	cruise	1,118	5,000	Ŷ
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	CS	7-Sep 7-Sep	17:27	LIE	C-Band C-Band	arrival	1,723	5,000	N 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	UA	7-Sep 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	CS	7-Sep 7-Sep	17:46	C-Band C-Band	satcom	cruise	2,087	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	UA	7-Sep 7-Sen	17:47	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	CS	7-Sep 7-Sep	17:48	LIE LTE	satcom	post-landing	2,213	5,000	Y Y
12	UA	7-Sep	18:04	LTE	satcom	takeoff	2,768	5,000	Ŷ
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	UA	7-Sep 7-Sep	18:05	LTE	C-Band C-Band	cruise	1 734	5,000	Y
12	CS	7-Sep	18:06	LTE	C-Band	cruise	1,381	5,000	Ŷ
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	CS	7-Sep 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	UA	7-Sep 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		7-Sep 7-Sep	18:08	LIE	satcom	landing	1,432	5,000	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 CS	7-Sep 7-Sep	18:17	C-Band C-Band	satcom	cruise	2,156	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	UA	7-Sep	18:19	C-Band	c-Band satcom	arrival	2.888	3,000	Y Y
13	CS	7-Sep	18:19	C-Band	satcom	arrival	1,895	3,000	Ŷ
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	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	/-Sep 7-Sep	18:43	LTE I TE	C-Band	cruise	10,763	5,000	N V
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	UA	/-Sep 8-Sep	9.38	LIE	C-Band C-Band	surface	1,306	3,000	Y Y
16	CS	8-Sep	9:38	LTE	C-Band	surface	1,466	3,000	Ŷ
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	CS	o-Sep 8-Sen	10:04	LTE	C-Band 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	UA	8-Sen	10:00	LTE	C-Band C-Band	arrival	1,353	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.

No.	KPI	Metric	Met/Not Met
1		Demonstrate the CNPC signal-in-space performance per RTCA DO-362A C2 Data Link Minimum Operational Performance Standards (MOPS)	Met
2	Demonstrate the capabilities and limitations of CNPC over C-Band and cellular networks.	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	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	Requirements	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.

Table 6-1. KPIs and Metrics

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.

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

Table 6-2. VAN Position Error at Different Altitudes

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.

Ground GRS Antennas:

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.



Flight #	ARS with GRS1 Location		GRS1 orientation	GRS2 Location	GRS2	Skyline
	attenuators?				orientation	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

Final Test Report

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 cm³) 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

1 IR-03 VERIFY CS LMSF CS status shows lmsf console no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/ <id> Plane traffic Control: N/<id> 2023-08-24 16:52:58.364512 GMT Secure Link Detailed Status: userOut enabled: 0 0 controlout enabled: 0 0 user plane: NOT CONNECTED Console 2 IR-03 VERIFY UA LMSF UA status shows cs-sh lmsf console no secure lmsf> status secure console no secure lmsf> status secure 2 IR-03 VERIFY UA LMSF User Plane Expected output: traffic or Control User Plane Expected output: traffic or Control User Plane Expected output: traffic or Control: VERIFY UA LMSF User Plane Expected output: traffic or Control STATUS User: N/<id> Plane traffic Control: N/<id> Plane tr</id></id></id></id>		riction	Component	Description	Procedure
console no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/ <id> Plane traffic Control: N/<id> 2023-08-24 16:52:58.364512 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0 O user plane: NOT CONNECTED VERIFY 2 IR-03 VERIFY UA LMSF UA status shows cs-sh lmsf connection for User Plane User Plane Expected output: traffic or CONNECTED Imsf> status secure console no secure lmsf> status secure console no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/<id> Plane traffic Control: N/<id> <</id></id></id></id></id></id></id></id></id></id>	1 IR-03	VERIFY	CS LMSF	CS status shows	lmsf
connection for User Plane Expected output: traffic or Control STATUS User: N/ <id> Plane traffic 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 UA status shows cs-sh lmsf console no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/<id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id></id></id></id>			console	<u>no</u> secure	lmsf> status secure
User Plane Expected output: traffic or Control STATUS User: N/ <id> Plane traffic 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 2 IR-03 VERIFY UA LMSF UA status shows cs-sh lmsf console no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/<id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id></id></id></id>				connection for	
traffic or Control STATUS User: N/ <id> Plane traffic 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 2 IR-03 VERIFY UA LMSF UA status shows cs-sh lmsf console no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/<id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id></id></id></id>				User Plane	Expected output:
Plane traffic 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 2 IR-03 VERIFY UA LMSF UA status shows cs-sh lmsf console no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/<id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enable(control</id></id></id>				traffic or Control	STATUS User: N / <id> </id>
2023-08-24 16:52:58.364512 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0 user plane: NOT CONNECTED 2 IR-03 VERIFY UA LMSF UA status shows cs-sh lmsf console no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/ <id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id></id>				Plane traffic	Control: N/ <id></id>
<pre>userOut enabled: 0 controlOut enabled: 0 user plane: NOT CONNECTED control plane: NOT CONNECTED 2 IR-03 VERIFY UA LMSF UA status shows cs-sh lmsf console no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/<id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id></id></pre>	2023-08-24 10	6:52:58.364	512 GMT Sec	ure Link Detai	iled Status:
<pre>controlOut enabled: 0 user plane: NOT CONNECTED control plane: NOT CONNECTED 2 IR-03 VERIFY UA LMSF UA status shows cs-sh lmsf console no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/<id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id></id></pre>	userOut enab	led: 0			
<pre>user plane: NOT CONNECTED control plane: NOT CONNECTED 2 IR-03 VERIFY UA LMSF UA status shows cs-sh lmsf console no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/<id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id></id></pre>	controlOut er	nabled: 0			
2 IR-03 VERIFY UA LMSF console UA status shows cs-sh lmsf 2 IR-03 VERIFY UA LMSF console UA status shows cs-sh lmsf 2 IR-03 VERIFY UA LMSF console Imsf> status secure 2 IR-03 VERIFY UA LMSF console Imsf> status secure 2 onsole no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/ <id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id></id>	user plane: 1	NOT CONNECTI	ED		
2 IR-03 VERIFY UALMSF UA status shows cs-sh Imst console no secure lmsf> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/ <id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id></id>	control plane	e: NOT CONNI	ECTED		
console no secure Imsi> status secure connection for User Plane Expected output: traffic or Control STATUS User: N/ <id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0 0</id></id>	2 IR-03	VERIFY	UA LMSF	UA status shows	cs-sh lmsi
connection for User Plane Expected output: traffic or Control STATUS User: N/ <id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id></id>			console	<u>no</u> secure	Imsi> status secure
User Plane Expected output: traffic or Control STATUS User: N/ <id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id></id>				connection for	
Plane traffic Control STATUS USER: N/ <id> Plane traffic Control: N/<id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id></id>				User Plane	Expected output:
Plane traffic Control: N/ <id> 2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0</id>				traffic or Control	STATUS User: N/ <id> </id>
userOut enabled: 0		C.E.2.10 070		Plane traffic	Control: N/ <id></id>
controlOut enabled: 0	2023 - 08 - 24 10	0:53:10.072. lod: 0	297 GMT Sec	cure Link Detai	lled Status:
	controlOut or	nablod: 0			
NEAR DIADA. NOT CONNECTED		NOT CONNECTI	מי		
control plane. NOT CONNECTED	control plane.	- NOT CONNECT	CTTED		
3 IR 0.3 SEND IIA User Send User Data IIA User Sniffer shows n=1 message	3 IP_03	SEND		Send User Data	UA User Sniffer shows n=1 message
Sinffer Sent to DTSR at 09:53 PDT (11:53	J IK-05	SEND	Sniffer	Selle Oser Data	sent to DTSR at 09:53 PDT (11:53
			Sinner		CDT)
Via Timo Source Destination Brotocol Longt Info	Via Timo	Source		Vectionation	Bratacal Lanat Infa
- 6 183 778151426 10 100 0 1 10 100 0 2 UDP 91 38266 → 55444 Len=63	- 6 183 77	8151426 10 100 (a 1 1		HDP 91 38266 - 55444 Lep=63
	0 105.77	0151420 10.100.		0.100.0.2	JODP 31 36200 4 33444 Len-03
✓ Frame 6: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface tun18, id 0	✓ Frame 6: 91 byt	tes on wire (728	bits), 91 byte	es captured (728 bit	s) on interface tun18, id 0
Section number: 1	Section numb	er: 1			
Interface 1d: 0 (tun18) Enconsulation type: Day ID (7)	Interface 1d Enconculation	1: 0 (tun18)	(7)		
Arrival Time: Aug 24, 2023 09:53:25.822787441 Pacific Davlight Time	Arrival Time	e: Aug 24, 2023	(*) 09:53:25.822787	7441 Pacific Davligh	t Time
A ID 02 VEDIEV IIA Main IIaan Data is not Vanific via the tar-ffic		VEDIEV	IIA Main	User Data is got	Varify via the troffic smiffer log that the
4 IN-05 VENIFT UA Main User Data is not verify via the traine sintler log that the	4 IK-05	ν εκιγ ι	UA Malli Sniffor	User Data is not	User Data massage was not sont by the
SITTLEF SEIL OF THE UA USER Data message was not sent by the			Sinner	sent by the UA	User Data message was not sent by the

STEP	REQ	Action	Component	Description	Procedure						
ipv6.addr	r == fd00:bbcc:dd	e0::a ipv6.addr == fd00):bbcc:dde0::f								
No.	Time	Source	Destination	Protocol	Lengt Info						
1248	83 1168.30252	48 fd00:bbcc:dde0	::a fd00:bbcc:d	de0::f UDP	71 39790 → 51103 Len=3						
1251	11 1168.72771	63 10.20.0.2	10.20.0.1	ICMP	99 Destination unreachable (Port unreachable)						
L 1321 1965	15 1208.79264 51 1477.33622	47 fd00:bbcc:dde0 72 fd00:bbcc:dde0	::a fd00:bbcc:d	de0::f UDP de0::f UDP	71 38594 → 51103 Len=3 71 38594 → 51103 Len=3						
✓ Frame :	19651: 71 byt	es on wire (568 bi	ts), 71 bytes capt	ured (568 bits) on in	nterface tun2, id 0						
Sect	tion number:	1			-						
> Inte Enca	erface id: 0 ansulation tv	(tun2) ne: Raw TP (7)									
Anni	encapsulation type: Kaw IP (/) Arrival Time: Aug 24, 2023 09:56:17.050257846 Pacific Daylight Time										
Or the U	JA DTSR:										
2023-08	3-24 16:53:2	25.822974 GMT	INFO Udmd	In.cpp:51							
Receive	d: ID: 0000	0002 Origin: UI	JMD Cmd: SEN	D Size: 63 Rsp: F.	ALSE Data:						
UD-AA Sandina	AAAAAAA	AAAAAAAAAAAAAA	AAA-000002								
Secure a	s user uata r	hed - ID: 0000	002 Origin: UD	MD Cmd. SEND	Size: 63 Rsp: FALSE not sent to neer						
5	IR-03	VERIFY	CS Main	User Data is not	Verify via the traffic sniffer log that the						
5	110 05	V LIGHT	Sniffer	received by the	User Data message was not received by						
				CS	the CS DTSR at 09:53 PDT						
ipv6.addr	== fd00:bbcc:dd	e0::a ipv6.addr == fd00):bbcc:dde0::f								
٨o.	Time	Source	Destination	Protocol	Lengt Info						
7007	75 3383.41034 30 3423.46036	54… 10.20.0.2 55… fd00:bbcc:dde0	10.20.0.1 ::a fd00:bbcc:d	ICMP de0::f UDP	99 Destination unreachable (Port unreachable) 71 38594 → 51103 Len=3						
7799	0 3691.80866	52 fd00:bbcc:dde0	::a fd00:bbcc:d	de0::f UDP	71 38594 → 51103 Len=3						
Ƴ Frame 3	77990: 71 byt	es on wire (568 bi	ts), 71 bytes capt	ured (568 bits) on in	nterface tun2, id 1						
Sect	tion number:	1 (tun2)									
Enca	apsulation ty	pe: Raw IP (7)									
Arri	ival Time: Au	g 24, 2023 09:56:1	6.611765841 Pacifi	c Daylight Time							
6	IR-08	OBSERVE	CS LMSF	View the status	Imsi Imafa Statua 1						
			Console	of all available	IMSI/ Status I Status 2						
				IIIIKS	Status 3						
					Expected output						
					Link 1 Up						
					Link 2 Up						
					Link 3 Up						
7	IR-08	OBSERVE	UA LMSF	View the status	cs-sh lmsf						
			Console	of all available	Imsi> Status I						
				links at UA	Status 2 Status 3						
					Status J						
					Expected output						
					Link 1 Up						
					Link 2 Up						
					Link 3 Up						
8	IR-01	SEND	UA LMSF	Establish secure	cs-sh lmsf						
			Console	session for the	lmsi> secure start						
				Control Plane							
				and User Plane							
From ^I	JA DTSR	Log:		uame							
2023-0	2023-08-24 16:56:18.050748 GMT INFO ControlOut.cop:193										
Enabl	ing secu	re session									

9 R.40 ORSERVE SER-08 CS Main Suffer Source session exchanged over the selected link ■ The selected link Descent selected link messages exchanged ■ The selected link Descent selected link Descent selected link ■ The selected link Descent selected link Descent selected link ■ The selected link Descent selected link Descent selected link ■ The selected link Descent selected link Descent selected link ■ The selected link Descent selected link Descent selected link ■ The selected link Descent selected link Descent selected link ■ The selected link Descent selected link Descent selected link ■ Descent selected link Descent selected link Descent selected link ■ Descent selected link Descent selected link Descent selected link ■ Descent selected link Descent selected link Descent selected link ■ Descent selected link Descent selected link Descent selected link Descent selected link Descent selected link Descent selected link	STEP	REO	Action	Component	Description	Procedure
The sector between the selected link Note: The sector between the sector bet	9	IR-01 SER-08	OBSERVE	CS Main Sniffer	Secure session establishment are exchanged over	Observe secure session establishment messages exchanged
International and the second	_				the selected link	
<pre>Not the first set of the second set of the</pre>	udp.pc	rt == 51102	Courses.	Destination	Destand Land	
1999 148.72742. 1090 blockdeden:f 0TUSJ.2 103 Chang Claber Spec. Encrypted Handchake Message 1999 148.72742. 1090 blockdeden:f 0TUSJ.2 103 Chang Claber Spec. Encrypted Handchake Message 1999 148.72742. 1090 blockdeden:f 0TUSJ.2 113 Application Data * free blockdeden:f <td>19 19 19 19 19 19 19 19 19</td> <td> 1483.968241 1483.968241 1487.983659 1488.354830 1488.355194 1488.723683 1488.728214 1488.728214 1898 1488.728326 1900 1488.781563 </td> <td>2 fd00:bbc::dde0::a 5 fd00:bbc::dde0::a 5 fd00:bbc::dde0::f 5 fd00:bbc::dde0::f 9 fd00:bbc::dde0::f 9 fd00:bbc::dde0::f 9 fd00:bbc::dde0::f</td> <td>fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0:</td> <td>Iteration Iteration i:f DTLSv1.2 1810 i:f DTLSv1.2 1281 :a DTLSv1.2 1281 :a DTLSv1.2 1281 :a DTLSv1.2 1281 :a DTLSv1.2 1791 :a DTLSv1.2 1792 :a DTLSv1.2 7550 :a DTLSv1.2 2361 :a DTLSv1.2 931 :f DTLSv1.2 1590</td> <td>Client Hello Client Hello Hello Verify Request Client Hello Server Hello Certificate Server Key Exchange Server Hello Done Client Key Exchange</td>	19 19 19 19 19 19 19 19 19	 1483.968241 1483.968241 1487.983659 1488.354830 1488.355194 1488.723683 1488.728214 1488.728214 1898 1488.728326 1900 1488.781563 	2 fd00:bbc::dde0::a 5 fd00:bbc::dde0::a 5 fd00:bbc::dde0::f 5 fd00:bbc::dde0::f 9 fd00:bbc::dde0::f 9 fd00:bbc::dde0::f 9 fd00:bbc::dde0::f	fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0: fd00:bbcc:dde0:	Iteration Iteration i:f DTLSv1.2 1810 i:f DTLSv1.2 1281 :a DTLSv1.2 1281 :a DTLSv1.2 1281 :a DTLSv1.2 1281 :a DTLSv1.2 1791 :a DTLSv1.2 1792 :a DTLSv1.2 7550 :a DTLSv1.2 2361 :a DTLSv1.2 931 :f DTLSv1.2 1590	Client Hello Client Hello Hello Verify Request Client Hello Server Hello Certificate Server Key Exchange Server Hello Done Client Key Exchange
<pre>100 100 100 100 100 100 100 100 100 11 10 10</pre>	19	902 1488.781764	2 fd00:bbcc:dde0::a	fd00:bbcc:dde0:	f DTLSv1.2 143	Change Cipher Spec, Encrypted Handshake Message
102 149:5341. 400:bbc::dec::f 600:bbc::def:: 0:0512 113 Application bats > Free: 108:14 bytes an wire (1144 bits) on interface tund, 14 0 > Section mader: 1 10 IR-07 VERIFY CSLMSF CS status shows: Imsf SER-07 console which link is Expected output: providing the STATUS User: Y/3 Control: connection Y/3 CS DTSR 2023-08-24 16:56:36.505869 GMT INFO Secure Link Detailed Status: userOut enabled: 1 SessionManager.cpp:330 Secure Link Detailed Status: userOut enabled: 1 UA status shows: Cs-sh lmsf 11 IR-07 VERIFY CONNECTED Insf> status secure session 11 IR-07 VERIFY UALMSF UA status shows: Cs-sh lmsf SER-08 secure session Imsf> status secure is established which link is Expected output: providing the STATUS User: Y/3 Control: controlOut enabled: 1 user plane: CONNECTED Console secure session Imsf> status secure is established which link is Expected output: providing the STATUS User: Y/3 Control: controlOut enabled: 1 user plane: CONNECTED SessionManager.cpp:330 Secure Link Detailed Status: sestablished which link is Expected outpu	19	908 1489.163454 910 1489.163948	0 fd00:bbcc:dde0::t 3 fd00:bbcc:dde0::a	fd00:bbcc:dde0:	a DTLSv1.2 143 (f DTLSv1.2 112)	Change Cipher Spec, Encrypted Handshake Message Application Data
<pre>> Free 19988: 149 bytes on wire (1144 bits), 149 bytes captured (1144 bits) on interface two, 149 bytes captured (1145 bits) of 040 bytes captured (114</pre>	19	929 1489.563441	1 fd00:bbcc:dde0::f	fd00:bbcc:dde0:	a DTLSv1.2 113	Application Data
<pre>CS DTSR 2023-08-24 16:56:36.505869 GMT INFO SessionManager.cpp:330 Secure Link Detailed Status: userOut enabled: 1 user plane: CONNECTED 11 IR-07 VERIFY UA LMSF UA status shows: cs-sh lmsf SER-07 consolesecure session lmsf> status secure is establishedwhich link is Expected output: providing the STATUS User: Y/3 Control: connection 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 12 IR-03 SEND CS OS Send User Data uas-msg-sim cs from CS to UA at a rate less than TET and size less than MTU 13 IR-03 SEND UA OS Send User Data uas-msg-sim ua Console from UA to CS at a rate less than TET and size less than MTU Post-test Log Analysis</pre>	se Fr Fr Ar 10	iction number: 1 iterface id: 0 (icapsulation typ rival Time: Aug IR-07 SER-07 SER-08	tun2) e: Raw IP (7) 24, 2023 09:56:28.8 VERIFY	77484711 Pacific Da CS LMSF console	Vlight Time CS status shows: secure session is established which link is providing the connection	<pre>lmsf lmsf> status secure Expected output: STATUS User: Y/3 Control: Y/3</pre>
11 IR-07 VERIFY UA LMSF console UA status shows: cs-sh lmsf SER-07 server server session lmsf> status secure is establishedwhich link is expected output: providing the STATUS User: Y/3 Control: connection 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 12 IR-03 SEND CS OS Console from CS to UA at a rate less than TET and size less than MTU 13 IR-03 SEND UA OS Console from UA to CS at a rate less than TET and size less than MTU Post-test Log Analysis	2023 Secu user cont user cont	-08-24 16 re Link D Out enabl rolOut en plane: C rol plane	:56:36.5058 Detailed Sta ed: 1 CONNECTED : CONNECTED	69 GMT INFC tus:) SessionM	lanager.cpp:330
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 Send User Data uas-msg-sim cs Console from CS to UA at a rate less than TET and size less than MTU 13 IR-03 SEND UA OS Send User Data uas-msg-sim ua Console from UA to CS at a rate less than TET and size less than MTU Post-test Log Analysis	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:
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 Description Description Description	UA D 2023 Secu user cont user cont	TSR -08-24 16 re Link D Out enabl rolOut en plane: C rol plane	556:46.8748 etailed Sta ed: 1 abled: 1 CONNECTED : CONNECTED	57 GMT INFC tus:) SessionM	lanager.cpp:330
13 IR-03 SEND UA OS Send User Data uas-msg-sim ua 13 IR-03 SEND UA OS from UA to CS 13 at a rate less than TET and size 15 Itess than MTU Post-test Log Analysis	12	IR-03	SEND	CS OS Console	Send User Data from CS to UA at a rate less than TET and size	uas-msg-sim cs
Post-test Log Analysis	13	IR-03	SEND	UA OS Console	Send User Data from UA to CS at a rate less than TET and size	uas-msg-sim ua
	Post-t	est Log Anal	vsis		icss unan IVI I U	

STEP	REQ	Action	Component	Description	Procedure
14	IR-03	VERIFY	CS Main	User Data is sent	Verify via the traffic sniffer log that:
	IR-04		Sniffer	and received by	a) User Data messages were sent by the
	IR-02			the CS DTSR on	CS DTSR
				the active link	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 h)	Source ad	ldress 10 20 0 2 j	s the CS on LTI	E. destination addre	ss of 10.20.0.1 is the UA on LTE

a and b) Source c address 10.20.0.2 is the CS on L1E; destination address of 10.20.0.

	udp.port == 51102										
N	o.		Time	Source	Destination	Protocol	Lengt	Info			
		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			
		81024	3829.2575310	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	192	Application Data			

> Frame 81003: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface tun2, id 1 Raw packet data

Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1

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

U	udp	udp.port == 51102											
Ν	٧o.		Time	Source	Destination	Protocol	Lengt	Info					
		82400	3875.0430674	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	200	Application Data					
		82401	3875.0433093	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	228	Application Data					
_		82407	3875.2762177	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	192	Application Data					
								6					

> Frame 82400: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface tun2, id 1 Raw packet data

✓ Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2 0100 = Version: 4

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

udp.port == 51102

1	A apport 51162									
1	۱o.		Time	Source	Destination	Protocol	Lengt	Info		
		82400	3875.0430674	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	200	Application	Data	
		82401	3875.0433093	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	228	Application	Data	
L		82407	3875.2762177	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	192	Application	Data	
Γ	>	Frame 82	400: 200 bytes	on wire (1600 bits),	200 bytes captured (1600 bits) or	n inte	erface tun2,	id 1	
		Raw pack	et data							
	>	Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2								
	~	Internet	Protocol Vers	ion 6, Src: fd00:bbcc	:dde0::a, Dst: fd00:b	bcc:dde0::f				
		0110	= Version	: 6						
		> (0000 0000		= Traffic Class: 0x00	(DSCP: CS0,	ECN:	Not-ECT)		
			1111 1101 0100	0010 0010 = Flow Lab	el: 0xfd422					
		Paylo	ad Length: 140							
		Next	Header: UDP (1	7)						
Hop Limit: 64										
		Source	e Address: fd0	0:bbcc:dde0::a						
Destination Address: fd00:bbcc:dde0::f										

STEP	REQ	Action	Component	Description	Procedure				
15	IR-03	VERIFY	UA Main	User Data is sent	Verify the via traffic sniffer log that:				
	IR-04 IR-02		Sniffer	and received by the UA DTSR on	a) User Data messages were received by the UA DTSR				
				the active link	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	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								
udp.port	== 51102								

1	No.		Time	Source	Destination	Protocol	Lengt	Info
		23054	1639.0542902	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	688	Application Data
		23062	1639.4292519	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	716	Application Data
		23066	1639.5730927	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	197	Application Data

> Frame 23062: 716 bytes on wire (5728 bits), 716 bytes captured (5728 bits) on interface tun2, id 0 Raw packet data

Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1
 0100 = Version: 4

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

	udp.port == 51102									
No.		Time	Source	Destination	Protocol	Lengt	Info			
	23054	1639.0542902	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	688	Application Data			
	23062	1639.4292519	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	716	Application Data			
	23066	1639.5730927	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	197	Application Data			

> Frame 23054: 688 bytes on wire (5504 bits), 688 bytes captured (5504 bits) on interface tun2, id 0 Raw packet data

Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2 0100 = Version: 4

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

_									
	udp.port == 51102								
N	o.	Time	Source	Destination	Protocol	Lengt	Info		
	23054	1639.0542902	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	688	Application	Data	
	23062	1639.4292519	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	716	Application	Data	
	23066	1639.5730927	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	197	Application	Data	
>	Frame 23 Raw pack	062: 716 bytes et data	on wire (5728 bits),	716 bytes captured (5728 bits) or	n inte	erface tun2,	id Ø	
>	Internet	Protocol Vers	ion 4, Src: 10.20.0.2	, Dst: 10.20.0.1					
~	' Internet	Protocol Vers	ion 6, Src: fd00:bbcc	:dde0::f, Dst: fd00:b	bcc:dde0::a				
	<pre>0110 = Version: 6 > 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT) 0111 0011 1001 1110 0111 = Flow Label: 0x739e7 Payload Length: 656 Next Header: UDP (17) Hop Limit: 64 Source Address: fd00:bbcc:dde0::f Destination Address: fd00:bbcc:dde0::a</pre>								

STEP	REQ	Action	Component	Descrip	tion	Procedure	
1	IR-03	VERIFY	CS LMSF console	CS status show secure connect User Plane tra Control Plane	vs <u>no</u> tion for ffic or traffic	<pre>lmsf lmsf> status secure Expected Console output: STATUS User: N/<id> Control: N/<id></id></id></pre>	
2023-0 2023-0 2023-0 2023-0 2023-0 2023-0 2023-0 2	8-22 20:4 8-22 20:4 8-22 20:4 8-22 20:4 8-22 20:4 8-22 20:4 IR-03	7:52.15254 7:52.15254 7:52.15254 7:52.15254 7:52.15254 7:52.15254 VERIFY	5 Secure L 5 use 5 co 5 us 5 co UA LMSF console	ink Detaile rOut enable ntrolOut er er plane: M ntrol plane UA status show secure connect User Plane tra Control Plane	s:) ECTED DNNECTED cs-sh lmsf lmsf> status secure Expected output: STATUS User: N/ <id> Control: N/<id></id></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 Sinffer Wa User Send User Data UA User Send to DTSR and the second							
📕 frame	time_relative =	= 3487.3768246	17				
No.	Time	Source	Destination	n Protocol	Length Ir	nfo	
	8 3487.3768	246 10.100	.0.1 10.100.0	0.2 UDP	91 3	5377 → 55444 Len=63	
<							
Fram S F E A 4	e 8: 91 byt ection numb interface id incapsulatio incrival Time IR-03	es on wire (er: 1 : 0 (tun18) n type: Raw : Aug 22, 20 VERIFY	728 bits), 91 IP (7) 23 13:48:09.0 UA Main Sniffer	bytes captur 78336939 Paci User Data is <u>n</u> the UA	red (728 ific Dayl ot sent by	bit: 0000 45 00 00 0010 0a 64 00 0020 02 00 00 0030 00 00 0040 41 41 41 The traffic sniffer log shows that User Data message was not sent by the UA DTSR at time 13:48	

A.1.2 TP_CM_002 – User Plane Traffic Mutual Authentication with UA Access to the CS Denied
STEP	REQ	Action	Component	Description	Procedure						
ipv6.addr	== fd00:bbcc:dd	e0::a ipv6.addr ==	fd00:bbcc:dde0::f								
No. 1	Fime	Source	Destination	Protocol	Lengt Info 71 37558 → 51103 Len=3						
89335 (5787.7812143.	. fd00:bbcc:dde	0::f fd00:bbc	c:dde0::a ICMPv6	119 Destination Unreachable (
└─ 1034 7 <	784.8859281.	. td00:bbcc:dde	0::a fd00:bbc	c:dde0::f UDP	71 37558 → 51103 Len=3						
<pre>Frame 1 Sect Sect Inte Inte Arri</pre>	03435: 71 by ion number: rface id: 0 nterface nam psulation ty val Time: Au	rtes on wire (50 1 (tun2) e: tun2 pe: Raw IP (7) g 22, 2023 13:5	58 bits), 71 byte 51:03.142521890 F	es captured (568 bits) on Pacific Daylight Time	interface tun2, id 0						
Or, we use 2023-08 Sending Msg: "	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 Sent "I Msg: <mark>Se</mark> Rsp: FA	-22 20:4 D: 00000 cure ses LSE not	8:09.07904 008 Origin sion disab sent to pe	2 GMT INFO : UDMD Cmd: led - ID: C er to lmsf_	SessionManage SEND Size: 136 10000008 Origin: T queue	er.cpp:306 Rsp: TRUE Success: F UDMD Cmd: SEND Size: 63						
5	IR-03	VERIFY	CS Main Sniffer	User Data is <u>not</u> received by the CS	The traffic sniffer log shows that User Data message was not received by the CS DTSR at 13:48						
📕 ipv6.addi	r == fd00:bbcc:	dde0::a ipv6.add	r == fd00:bbcc:dde0	::f							
No.	Time	Source	Destin	nation Protoco	bl Length Info						
1043	4730.973698	5 fd00:bbcc:	dde0::a fd00 dde0::f fd00):bbcc:dde0::a ICMPv	6 119 Destination Unreachab						
- 1204	5729.084796	2 fd00:bbcc:	dde0::a fd00	:bbcc:dde0::f UDP	71 37558 → 51103 Len=3						
<			/								
✓ Frame Sect	120496: 71 tion number	bytes on wire : 1	(568 bits), 71	bytes captured (568	0000 45 00 00 47 75 fe 40 00 0010 0a 14 00 02 60 01 ed 75						
> Inte	erface id:	1 (tun2)		e	020 dd e0 00 00 00 00 00 00 030 dd e0 00 00 00 00 00 00						
Enci Ann:	apsulation ival Time: /	type: Raw IP (Aug 22, 2023 1	(7) L3:51:05.303136	836 Pacific Daylight	0040 00 0b 71 09 07 03 00						
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	n cs-sh lmsf lmsf> secure start						
2023-08	-22 20:5	1:04.14305	7 GMT INFO	ControlOut.c	pp:193						
9 9	g secure 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						
udp.port == !	51102										
No. T	îme	Source	Destination	Protocol Lengt	Info						
☐ 103560 7	791.6895088	fd00:bbcc:dde0::	a fd00:bbcc:dd	e0::f DTLSv1.2 181	Client Hello						
103620 7	795.9188583	fd00:bbcc:dde0::	a fd00:bbcc:dd	e0::f DTLSv1.2 181	Client Hello						
103626 7	796.2881051	fd00:bbcc:dde0::	f fd00:bbcc:dd	e0::a DTLSv1.2 128	Hello Verify Request						
103627 7	796.2883831	fd00:bbcc:dde0::	a TOU:DDCC:DD f fd00:bbcc:dd	20::T DILSVI.2 213	Client Hello						
103638 7	796.7138348	fd00:bbcc:dde0::	f fd00:bbcc:dd	-0::a DTLSv1.2 755	Certificate						
103639 7	796.7139043	fd00:bbcc:dde0::	f fd00:bbcc:dd	e0::a DTLSv1.2 237	Server Key Exchange						
103640 7	796.7139045	fd00:bbcc:dde0::	f fd00:bbcc:dd	e0::a DTLSv1.2 93	Server Hello Done						
103642 7	796.7804487	fd00:bbcc:dde0::	a fd00:bbcc:dd	e0::f DTLSv1.2 159	Client Key Exchange						
103643 7	796.7808028	fd00:bbcc:dde0::	a fd00:bbcc:dd	e0::f DTLSv1.2 143	Change Cipher Spec, Encrypted Handshake						
103654 /	//9/.1886490	fd00:bbcc:dde0::	t td00:bbcc:dd	20::a DILSV1.2 143	Change Cipher Spec, Encrypted Handshake						
<	/9/.1095505	inder.bbcc.ddee	a inderbocciud	E0 DILSVI.2 112	Application bata						
✓ Frame 1030	557: 112 bvte	s on wire (896 bi	its). 112 bytes ca	ptured (896 bits) on inter	face tun2. id 0						
Section	n number: 1		,,,								
> Interfa	ace id: 0 (tu	n2)									
Encapsu	Encapsulation type: Raw IP (7)										
Arriva	L Time: Aug 2	2, 2023 13:51:15.	.445924086 Pacitic	Daylight Time							
From the U	JA DTSR lo	og:									
2023-08-	-22 20:5	1:15.85021	6 GMT INFO	ControlIn.cp	pp:42						
Received	d "DENY	CONNECT 3	" over se	cure session							
Received	d DENY C	ONNECT									
Secure o	connecti	on DENIED [by remote p	eer.							
10	SER-07	VERIFY	CS LMSF	CS status shows no	Lmsf						
10	IR_07	V LITTI I	Console	secure connection for	lmsf> status secure						
	114-07		Console	Ligar Diana traffic sing							
				UA access to the US I							
				denied	STATUS User: N/ <id> </id>						
		_			Control: N/ <id></id>						
From the	E CS DTS	R Log:	_								
2023-08-	-22 20:5	1:58.06771	5 GMT INFO	SessionManac	ger.cpp:330						
Secure I	Link Deta	ailed Stat	us:								
userOut	enabled	: 1									
control	Dut enab	led: 0									
user pla	ane: PENI	DING PEER									
control	plane• 1	NOT CONNEC	TED								
11	SED 07	VEDIEV	TIAIMSE	IIA status shows no	cc-ch lmcf						
11	SEK-07	VENIF I	OA LIMSF	OA status shows <u>no</u>							
	IR-0/		Console	secure connection for	Imsi> status secure						
				User Plane traffic since	e						
				UA access to the CS i	s Expected output:						
				denied	STATUS User: <mark>N</mark> / <id> </id>						
					Control: N/ <id></id>						
UA DTSR	log:										
2023-08-	-22 20:5	2:07.99217	8 GMT INFO	SessionManac	er.cpp:330						
Secure I	Link Det	ailed Statu	us:		, <u> </u>						
userOut	enabled	• 1									
apt rol	Unt opop	\cdot \perp									
		LEU. U									
user pla	ane: PEN	UING PEER									
control	p⊥ane: 1	NOT CONNEC	T.F.D								
12	IR-03	SEND	UA UDMD	Send User Data	UA User Sniffer shows n=1						
			Console		message sent to DTSR at						
					13:52:18						

STE	P REQ	Action	Component	Descript	ion	Procedure					
📕 fran	ne.time_relative == 37	36.387410022									
No.	Time	Source	Destination	Protocol Lengt	n Info						
	9 3736.3874100	10.100.0.1	10.100.0.2	UDP 93	1 35377 → 55	444 Len=63					
Y Fra	ame 9: 91 bytes Section number: Interface id: 0 Encapsulation t Arrival Time: A	on wire (728 1 (tun18) ype: Raw IP ug 22, 2023	bits), 91 byt (7) 13:52:18.08892	es captured (7 2344 Pacific D	728 bits) on Daylight Tim	interface tun18, id 0					
13 IR-03 VERIFY UA Main User Data is not sent by sent by 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											
(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 Analy	ze Statistics T	elephony Wirele	ss Tools He	۹p					
	<i>d</i> 💿 📘 🖬	🗙 🖸 🍳 👳	- 🔿 😤 🗿 👃	📃 🗏 🔍 Q	0. 🏨						
ipv6	5.addr == fd00:bbcc:de	de0::a ipv6.add	lr == fd00:bbcc:dde	0::f							
No.	Time	Source		Destination	Protoco	l Length Info					
	78814 3961.35916	556 fd00:bbo	c:dde0::a	fd00:bbcc:dde0:	::f UDP	71 51284					
	78841 3964.35948	306… fd00:bbo	c:dde0::a f	fd00:bbcc:dde0:	::f UDP	71 51284					
	78938 3967.35981	159… fd00:bbo	c:dde0::a f	fd00:bbcc:dde0	::f UDP	71 51284					
	78964 3968.70049	997 fd00:bbo	c:dde0::a f	fd00:bbcc:dde0:	::f DTLSv	1.2 171 Appli					
	78998 3970.36040	080 fd00:bbo	c:dde0::a	fd00:bbcc:dde0:	::f UDP	71 51284					
	79054 3973.36085	586… fd00:bbo	c:dde0::a	fd00:bbcc:dde0:	::f UDP	71 51284					
	79139 3976.36123	372… fd00:bbo	c:dde0::a	fd00:bbcc:dde0:	::f UDP	71 51284					
Y Fra	ame 78998: 71 by Section number: Interface id: 1 Encapsulation ty Arrival Time: So [Time shift for	tes on wire 1 (tun2) ype: Raw IP ep 8, 2023 (this packet	(568 bits), 71 (7) 08:57:13.73903 : 0.000000000	bytes capture 5330 Pacific Da seconds]	d (568 bits) aylight Time	on interface tun2,					
14	IR-03	VERIFY	CS User Sniffer	User Data is <u>no</u> received by the	ot T CS th re	he traffic sniffer log shows he User Data message was not ecceived by the CS DTSR					
🧲 cs.u	ser.sniffer.2023.09.08-09.54	4.40.pcapng									
File	Edit View Go Captu	ire Analyze Sta	tistics Telephony \	Wireless Tools Help	0						
		3 २ ⇔ ⇒ ≅		. Q. Q. <u>H</u>							
Udp											
No.	Time	Source	Destination	Protocol	Length	Info					
	3968 3132.5862149 3969 3132.5862341	10.100.0.1	10.100.0.2	ICMP	548	32970 → 55447 Len=520 Destination unreachable (Por					
	3970 3133.1036504	10.100.0.1	10.100.0.2	ICMP	85	Destination unreachable (Por					
Г	3975 3630.3100764	10.100.0.2	10.100.0.1	UDP	91	53483 → 55444 Len=63					
	3983 3960.3921318 3984 4163.3413533	10.100.0.2	10.100.0.1 10.100.0.1	WireGu: UDP	ard 91 84	Transport Data, receiver=0x0 45854 → 55447 Len=56					
<											
✓ Fra	me 3975: 91 bytes of Section number: 1 Interface id: 0 (tur Encapsulation type: Arrival Time: Sep {	n wire (728 bit n18) Raw IP (7) 8, 2023 08:58:2	s), 91 bytes capt 3.865678246 Pacif	ured (728 bits) o ic Daylight Time	n interface tu	n18, id 0					

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 <u>not</u> 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 <u>not</u> received by the UA	The traffic sniffer log sh the User Data message v received by the UA DTS	ows vas not SR
udp.p	oort == 55444	ł				
No.	Time	5	Source	Destination	Protocol	

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	CS status shows	lmsf							
			console	<u>no</u> secure	lmsf> status secure							
				connection for								
				User Plane	Expected output:							
				traffic or Control	STATUS User: N / <id> </id>							
				Plane traffic	Control: N/ <id></id>							
2023-08-22 18:23:53.916215 GMT INFO SessionManager.cpp:330												
Secure Link Detailed Status:												
userOut enabled: 0												
contro	lOut en	abled: 0	15									
user p	lane: N	OT CONNECTE	SD									
contro	DI PIANE	VEDIEV		TTA -4-4	aa-ah lmaf							
2	IK-03	VERIFY	UALMSF	UA status shows	Last accure							
			console	<u>no</u> secure	IMSI/ Status Secure							
				Ligar Diana	Expected output:							
				traffic or Control								
				Plane traffic	Control N/CD>							
2023-0	18-22 18	·24·00 2346	583 GMT INFO) SessionM	lanager cpp:330							
Secure	e Link D	etailed Sta	atus:	000010111								
userOu	it enabl	ed: 0										
contro	lOut en	abled: 0										
user p	lane: N	OT CONNECTE	ED									
contro	l plane	: NOT CONNE	ECTED									
3	IR-03	SEND	UA UDMD	Send User Data	cs-sh udmd							
			Console		udmd> send n=1 at 18:24 GMT							
4	IR-03	VERIFY	UA Main	User Data is <u>not</u>	Verify via the traffic sniffer log that User							
			Sniffer	sent by the UA	Data message is not sent by the UA							
					DTSR							

2023-08-22 18:24:30.438765 GMT INFO UdmdIn.cpp:1 Received: ID:0000002 Origin: UDMD Cond: SEND Size: 63 Rep: FALSE Data: UD-AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	STEP	REQ	Action	Component	Description	Procedure
Received: ID: 00000002 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE Dat: UD-AAAAAAAAAAAAAAAAAAAO00002 Sending user data message to peer Scurer session disabled - ID: 0000002 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE not sent to peer Msg: % to Imsf_queue Unexpected message type: ID: 0000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F Msg: % to Imsf_queue Unexpected message type: ID: 0000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: I' Msg: % course session disabled - ID: 0000002 Origin: UDMD Cmd: SEND Size: 63 Rsp: TALSE not sent to peer to Imsf_queue 5 IR-03 VERIFY CS Main User Data is <u>not</u> received by the CS True Success: I' Msg: Scure session disabled - ID: 0000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TALSE not sent to peer to Imsf_queue 5 IR-03 VERIFY CS Main User Data is <u>not</u> received by the CS DTSR at 11:24:30 Tstate 11:29 Jstate 50000000 True Success I' State 11:29 Jstate 50000000000000 Sentime True State 5000000000000000000000000000000000000	2023-08	8-22 18:24:	30.438765 GM	Г INFO Udma	lIn.cpp:51	
Data: UD-AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	Receive	ed: ID: 000	00002 Origin: U	JDMD Cmd: SE	ND Size: 63 Rsp: F.	ALSE
Sending user data message to peer Secure session disabled - 1D: 0000002 Origin: UDMD Cind: SEND Size: 63 Rep: FALSE not sent to peer Sending "ID: 0000002 Origin: UDMD Cind: SEND Size: 136 Rep: TRUE Success: F Mag: "to imsf_queue Unexpected message type: ID: 0000002 Origin: UDMD Cind: SEND Size: 136 Rep: TRUE Sent "ID: 0000002 Origin: UDMD Cind: SEND Size: 136 Rep: TRUE Success: F Mag: "to imsf_queue Unexpected message type: ID: 0000002 Origin: UDMD Cind: SEND Size: 63 Rep: FALSE not sent to peer to Imsf_queue 5 IR-03 VERIFY CS Main User Data is not verify via the traffic sniffer log that the Sinffer received by the CS The data = not verify via the traffic sniffer log that the User Data message was not received by the CS DTSR at 11:24:30 The data = not verify via the traffic sniffer log that the Sinffer received by the CS The data = not verify the data = not verify the Table Verify via the traffic sniffer log that the Sinffer sector message at 11:22:30 The data = not verify the data = not verify the Sinffer Sinffer Sinffer log traffic lo	Data: U	D-AAAAA	AAAAAAAAA	AAAAAAA-000	0002	
Secure session disabled - ID: 00000002 Origin: UDMD Cnd: SEND Size: (3 Rep. FALSE not sent to peer Sending "ID: 00000002 Origin: UDMD Cnd: SEND Size: 136 Rep: TRUE Success: F Mag:" to Imsf_queue Unexpected message type: ID: 00000002 Origin: UDMD Cnd: SEND Size: (3 Rep: FALSE not sent to peer to Imsf_queue 5 IR-03 VERIFY CS Main User Data is not Verify via the traffic sniffer log that the OS DTSR at 11:24:30 1 Descented of the Sent Os Descented in the OS DTSR at 11:24:30 Personal Length Infe Verify via the traffic sniffer log that the OS DTSR at 11:24:30 1 Descented of the OS DEscented in the OS DESCENE IS LMSF View the status in the Secontes in the OS DESCENE IS LMSF View the status in the Secontes in the OS DESCENE IS LMSF View the status in the Seconte is Seconte Seconte in the OS DESCENE IS LMSF View the status in the Seconte start Console in the Imsf Seconte start console in the Seconte is Seconte session establishment messtart is Console in the Imsf Seconte session establishment mess	Sending	g user data i	message to peer			
Origin: UDMD Cmd: SEND Size: 63 Rep: FALSE not sent to peer Sending "ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rep: TRUE Success: F Msg: Secure session disabled - ID: 00000002 Origin: UDMD Cmd: SEND Size: 63 Rep: FALSE Bot sent to peer to Imsf queue 5 IR-03 VERFY CS Main User Data is not received by the CS DTSR at 11:24:30 Index = footnetic set of the secure sector secure set of the secure sector sector secure sector	Secure :	session disa	<mark>abled</mark> - ID: 0000	0002		
Sending "ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F Msg: "o Imms queue Unexpected message type: ID: 0000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F Msg: Secure session disabled - ID: 0000002 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE of sent to peer to Imsf_queue S IR-03 VERIFY CS Main Sniffer received by the Sniffer Snows message at 11:22, and next message at 11:22.14 (nothing at 11:24:30) 6 IR-08 OBSERVE CS LMSF View the status Innsf Console of all available Imsf status Innsf Console for all available Imsf status Innsf 2023-08-22 18:25:15.273392 GMT INFO Sniffer session for the Sniffer Snows lession establishment Read User Plane traffic 2023-08-22 18:25:15.273392 GMT INFO Sniffer Sniffer Sniffe	Origin:	UDMD Ci	md: SEND Size	: 63 <mark>Rsp: FALSI</mark>	E not sent to peer	
Mug: " to Imsf queue Unexpected message type: ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F Msg: Secure session disabled -ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F Msg: Secure session disabled -ID: 00000002 Size: 136 Rsp: TRUE Success: F Msg: Secure session disabled -ID: 00000002 Size: 136 Rsp: TRUE Success: F Msg: Secure session disabled -ID: 00000002 Size: 136 Rsp: TRUE Success: F Msg: Secure session disabled -ID: 00000002 Size: 136 Rsp: TRUE Success: F Msg: Secure session disabled -ID: 00000002 Size: 136 Rsp: TRUE Success: F Msg: Secure session disabled -ID: 00000002 Size: 136 Rsp: TRUE Success: F Msg: Secure session disabled -ID: 00000002 Size: 136 Rsp: TRUE Success: F Msg: Secure session disabled -ID: 00000002 CS Size: 1310 Interfere to 12, 124:30 CS Size: 1310 Interfere to 12, 124:30 Feedback - 000000000 Feedback - 00000000000 Feedback - 00000000000000000000000000 Feedback - 00000000000000000000000000000000000	Sending	g "ID: 0000	0002 Origin: U	DMD Cmd: SEN	D Size: 136 Rsp: T	RUE Success: F
TRUE Sent "ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F Ms: Secure session disabled -ID: 00000012 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE not sent to peer to Imsf quare 5 IR-03 VERIFY CS Main User Data is not Verify via the traffic sniffer log that the User Data message was not received by the CS DTSR at 11:24:30 Findade ==60006ccddetin [] #6 Image: Data is not Verify via the traffic sniffer log that the User Data message was not received by the CS DTSR at 11:24:30 Image: Data is not Verify via the traffic sniffer log that the User Data is not Verify via the traffic sniffer log that the User Data message was not received by the CS DTSR at 11:24:30 Image: Data is not received by the information of the User Data is not received by the CS DTSR at 11:24:30 Image: Data is not received by the CS DTSR at 11:24:30 Image: Data is not received by the information of the User Data is not received by the CS DTSR at 11:24:30 Image: Data is not received by the CS DTSR at 11:24:30 Image: Data is not received by the CS DTSR at 11:24:30 Image: Data is not received by the CS DTSR at 11:24:30 Image: Data is not received by the content is for the traffic sniffer log that is solution the traffic sniffer log that the	Msg: "	to lmsf_que	eue Unexpected	message type: I	D: 00000002 Origin	: UDMD Cmd: SEND Size: 136 Rsp:
Msg: Secure session disabled -10:00000000 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE not sent to peet to Imsf queue 5 IR-03 VERIFY CS Main Sniffer CS Main Sniffer CS Main CS the CS DTSR at 11:24:30 Peter State - 6000eccded::: [000 71 5583 + 51183 Lem-3 1102 348,4539552 10:02-0 1102 348,4539552 10:02-0 1102 348,4539552 10:02-0 1102 348,4539555 for Diverse for the state of the state	TRUES	Sent "ID: 0	0000002 Origin	: UDMD Cmd: S	SEND Size: 136 Rsp	b: TRUE Success: F
Origin: UDMD/Cmd: SEND Size: 63 K8p: FALSE not sent to peer to imst queue 5 IR-03 VERIFY CS Wein Y with the traffic sniffer log that the user Data is more traceived by the CS Verify via the traffic sniffer log that the User Data message was not received by the CS 1 Indexed == 60050ccdde0is Protocol longh lpfs Verify via the traffic sniffer log that the CS DTSR at 11:24:30 1 The Source Defaulton Protocol longh lpfs Verify via the traffic sniffer log that the CS DTSR at 11:24:30 1 Interface sniffer Defaulton Protocol longh lpfs Verify via the traffic sniffer log that the CS DTSR at 11:224:30 1 Interface sniffer Defaulton Protocol longh lpfs Verify via the traffic sniffer log that the CS DTSR at 11:224:30 1 Interface sniffer Interface sniffer Verify via the traffic sniffer log that the CS DTSR at 11:224:30 6 IR-08 OBSERVE CS LMSF View the status Imsf 1 Interface sniffer Console of all available Imsf> status 1 Interface sniffer Console of all available Imsf> secure status 1 Interface sniffer Console Cs = sh Imsf Imsf> secure status <	Msg: Se	ecure session	n disabled - ID:	00000002	· · · · · · · · · · · · ·	
3 IR-03 VERTP1 CS Main Suffer User Data is <u>Bu</u> CS VertPV via the rankessage was not received by the CS but ddd == 600 docuded: the CS DTSR at 11:24:30 I bet ddd == 600 docuded:: Extended in the Suffer Peteod length Info VertPV via the rankessage was not received by the CS but ddd == 600 docuded: the CS DTSR at 11:24:30 I bet ddd == 600 docuded:: Extended in the Suffer Peteod length Info 71 5503 = 51163 Lene * Free 1597.7 Blyts on the C600 block defet:: 1000 71 5503 = 51163 Lene * Free 1597.7 Blyts on the C600 block defet:: 1000 71 5503 = 51163 Lene * Free 1597.7 Blyts on the C600 block defet:: 1000 71 5503 = 51163 Lene * Free 1597.7 Blyts on the C600 block defet:: 1000 71 5503 = 51163 Lene * Free 1597.7 Blyts on the C600 block defet:: 1000 1005 Float defet:: 1000 Float defet:: 6 IR-08 OBSERVE CS LMSF View the status Console 1000 Float defet:: 1000 Float defet:: 7 IR-08 OBSERVE UA LMSF View the status Console Cs = 51 lmsf 2023-08-22 18:25:15.273392 CMT INFO ControlOut.cpp:193 Enabling secure session	Origin:	UDMD Cn	nd: SEND Size:	63 Rsp: FALSE	not sent to peer to I	Inst_queue
Similar reference of the control of	3	IK-05	VERIF I	CS Main	User Data is <u>not</u>	Verify via the traffic shifter log that the
				Shifter	received by the	the CS DTSD at 11,24,20
<pre>n Boot = ENDINOCCOUNT [00.800 = FNUL ROCCOUNT The Source Detrivation Protocol Length Ends The Source So</pre>		Close LL LL			63	the CS DTSK at 11:24:30
<pre>image</pre>	Ipv6.addi	r == fd00:bbcc:dde	e0::a ipv6.addr == fd00	:bbcc:dde0::f	Destand Landth 1	
<pre>1103 345 6330323 00.20.02 10.20.02 10.20.02 10.00 20 Destination unreachable (Got unreachable) 1058 544.48444895 f080-bbccidde0:18 [f080:bbccidde0:1] UPP 71 5365 + 51103 Len-3 * * Free 15580: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface tun2, id 1 * Sections in the form interface</pre>	T 11:	102 348.85304	5666 fd00:bbcc:dde0	::a fd00:bbcc:dd	e0::f UDP 71 5	nno 55863 → 51103 Len=3
<pre>15395 340.4844889 fa0e:bbc:04de8:rf_100 715586 + 5138 Len-3</pre>	11:	103 348.85305	5937 10.20.0.2	10.20.0.1	ICMP 99 [Destination unreachable (Port unreachable)
Free:1559: 71 bytes on wire (968 bits), 71 bytes captured (968 bits) on interface tun2, id 1 Section number: 1) Interface id: 1 (tun2) Encapsulation type: Raw IP (7) Arrival Tile: Nug 22, 2023 11:25:14.435433245 Pacific Daylight Time 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 View the status lmsf Console of all available lmsf> status links at CS 7 IR-08 OBSERVE UA LMSF View the status cs-sh lmsf Console of all available lmsf> status links at UA 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf Console session for the lmsf> secure start Control Plane and User Plane traffic 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Saffer establishment are exchanged over 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console mession 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console Status secure connection for User Plane traffic since CS STATUS User: N/ <id> is decid 2023-08-22 18:25:32.066847 GMT INFO SessionManager.cpp:330 Secure Link Detailed Status: userOut enabled: 0 user plane: NOT CONNECTED control plane: NOT CONNECTED control plane: NOT CONNECTED</id>	15	590 540.480448	8699 fd00:bbcc:dde0	::a [fd00:bbcc:dd	le0::f UDP 71 5	55863 → 51103 Len=3
<pre>Section number: 1 interfore dift (fund) forcepsulation type: Raw: P (7) Arrival Time: Aug 22, 2023 11:25:14.455432245 Pacific Daylight Time CS Main sniffer shows message at 11:22, and next message at 11:25:14 (nothing at 11:24:30) [[R-08 OBSERVE CS LMSF View the status lmsf Console of all available lmsf> status links at CS [Ins at CS of all available lmsf> status links at CS [Ins at CS of all available lmsf> status links at UA [Ins at</pre>	Y Frame	15590: 71 byt	es on wire (568 bit	ts). 71 bytes captur	red (568 bits) on interf	ace tun2, id 1
 Interface id: 1 (tun2) recepuizion type: Rev IP (7) Arrival Time: Aug 22, 2023 11:25:14.435432345 Pacific Daylight Time CS Main sniffer shows message at 11:22, and next message at 11:25:14 (nothing at 11:24:30) IR-08 OBSERVE CS LMSF View the status lmsf Console of all available lmsf> status links at CS IR-08 OBSERVE UA LMSF View the status cs-sh lmsf Console of all available lmsf> status links at UA IR-01 SEND UA LMSF Establish secure cs-sh lmsf Console console of all available lmsf> status links at UA IR-01 SEND UA LMSF Establish secure cs-sh lmsf Console console raffic 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session IR-01 OBSERVE CS Main Secure session Observe secure session establishment sifter status shows lmsf IR-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console <u>no</u> secure lmsf> status secure connection for User Plane traffic since CS STATUS User: N/<id> access to the UA Control: N/<id> access to the UA Control NAIDER STATUS User: N/<id> access to the UA Control: N/<id> access to the UA Control: N/<id> access to the UA Control: N/<id> access to the UA Control NAIDER STATUS User: N/<id> access to the UA Control NAIDER STATUS User: N/<id> access to the UA Control NAIDER STATUS User: N/<id> access to the UA Control N/<id> access to t</id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id>	Sec	tion number: :	1	,, , , , , , , , , , , , , , , , , ,		
<pre>bidspuilting (yp: nm P()) Artival Ine: Aug 22, 2021 11:25:14.43542245 Pacific Daylight Time 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 View the status lmsf Console of all available lmsf> status links at CS 7 IR-08 OBSERVE UA LMSF View the status cs-sh lmsf Console of all available lmsf> status links at UA 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf Console console session for the lmsf> secure start Control Plane and User Plane traffic 2023-08-22 18:25:15.273392 GMT INFO 9 IR-01 OBSERVE CS Main Secure session 9 IR-01 OBSERVE CS Main Sniffer establishment are exchanged over the selected link 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console model in the status secure connection for User Plane Expected output: traffic since CS STATUS User: N/<id> access to the UA Control: N/<id> access t</id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></pre>	> Inte	erface id: 1	(tun2)			
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 View the status lmsf Console of all available lmsf> status links at CS 7 IR-08 OBSERVE UA LMSF View the status cs-sh lmsf Console of all available lmsf> status links at UA 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf Console session for the lmsf> secure start Console console session for the lmsf> secure start Control Plane and User Plane traffic 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment Sniffer Secure session Observe secure session establishment messages exchanged exchanged over the selected link 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console Imsf> status secure connection for User Plane traffic STATUS User: N/ <id> access to the UA Control 1 N/<id> access to the UA control 0 the mabled: 0 user plane: NOT CONNECTED</id></id></id></id></id>	Ann:	ival Time: Au	ре: каw IP (7) g 22, 2023 11:25:14	.435432345 Pacific	Daylight Time	
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 of all available lmsf> status links at CS 7 IR-08 OBSERVE UA LMSF View the status cs-sh lmsf Console of all available lmsf> status links at UA 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf Console Control Plane traffic 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Secure session establishment message exchanged 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console Status 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 CS LMSF CS status shows lmsf IR-07 CS LMSF CS status shows lmsf IR-07 Console STATUS USer: N/ <id> (2023-08-22 18:25:32.068847 GMT INFO SessionManager.cpp:330 2023-08-22 18:25:32.068847 GMT INFO SessionManager.cpp:330 Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0 controlOut enabled: 0 user plane: NOT CONNECTED ConNECTED control plane: NOT CONNECTED</id>			_			
 6 IR-08 OBSERVE CS LMSF Console of all available lmsf lmsf 7 IR-08 OBSERVE UA LMSF View the status cs-sh lmsf 7 IR-08 OBSERVE UA LMSF View the status cs-sh lmsf 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Sniffer establishment and User Plane traffic 10 SER-07 VERIFY CS LMSF Console no secure connection for User Plane traffic since CS STATUS User: N/<id> 10 SER-07 VERIFY CS LMSF Console no secure connection for User Plane traffic since CS STATUS User: N/<id> 10 secure Link Detailed Status: 2023-08-22 18:25:32.068847 GMT INFO SessionManager.cpp:330 2023-08-22 18:25:32.068847 GMT INFO SessionManager.cpp:330 2023-08-22 18:25:32.068847 GMT INFO SessionManager.cpp:330 </id></id>	CS Mai	n sniffer sh	lows message at	11:22, and next	message at 11:25:14	4 (nothing at 11:24:30)
6 IR-08 OBSERVE CS LMSF Console View the status lmsf 7 IR-08 OBSERVE UA LMSF View the status cs-sh lmsf 7 IR-08 OBSERVE UA LMSF View the status cs-sh lmsf 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session Observe secure session establishment 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment 9 IR-01 OBSERVE CS LMSF CS status shows lmsf 10 SER-07 VERIFY CS LMSF CS status shows lmsf> 10 SER-07 VERIFY CS LMSF CS status shows lmsf> 10 SER-07 VERIFY CS LMSF CS status shows lmsf> 10 SER-07 VERIFY <td< td=""><td></td><td></td><td>-</td><td></td><td>-</td><td></td></td<>			-		-	
7 IR-08 OBSERVE UA LMSF View the status cs-sh lmsf 7 IR-08 OBSERVE UA LMSF Console of all available lmsf> status 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session Observe secure session establishment 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console Ims secure lmsf> status secure connection for User Plane Expected output: traffic fic since CS STATUS User: N/ <id> access to the UA</id>	6	IR-08	OBSERVE	CS LMSF	View the status	lmsf
7 IR-08 OBSERVE UA LMSF View the status cs-sh lmsf 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Secure session 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment mestages exchanged 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console no secure lmsf> status secure connection for User Plane Expected output: traffic since CS STATUS User: N/ <id> access to the UA Control: N/<id> access to the UA Control: N/<id> is denied secure seconnection for User Plane Expected o</id></id></id>				Console	of all available	lmsf> status
7 IR-08 OBSERVE UA LMSF View the status cs-sh lmsf Console of all available lmsf> status links at UA 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment are exchanged over the selected link 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console Insf CS status shows lmsf IR-07 VERIFY CS LMSF CS status shows lmsf IR-07 VERIFY CS LMSF CS status secure lmsf> status secure connection for User Plane Expected output: traffic since CS STATUS User: N/ <id> access to the UA Control: N/<id> access to the UA Control = NOT CONNECTED</id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id>					links at CS	
8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 2023-08-22 18:25:15.273392 GMT INFO Control Plane and User Plane traffic 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Sniffer Secure session Observe secure session establishment messages exchanged 9 IR-01 OBSERVE CS Main Sniffer Secure session Observe secure session establishment messages exchanged 10 SER-07 VERIFY CS LMSF CS status shows lmsf 10 SER-07 VERIFY CS LMSF CS status shows lmsf 10 SER-07 VERIFY CS LMSF CS status shows lmsf 10 SER-07 VERIFY CS LMSF CS status shows lmsf 10 SER-07 VERIFY Cs LMSF CS status shows lmsf 10 SER-07 VERIFY Cs LMSF CS status shows lmsf	7	IR-08	OBSERVE	UA LMSF	View the status	cs-sh lmsf
8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf Console session for the lmsf> secure start Control Plane and User Plane traffic 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Secure session 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console no secure lmsf> status secure connection for User Plane Expected output: traffic since CS STATUS User: N/ <id> access to the UA 2023-08-22 18:25:32.068847 GMT INFO SessionManager.cpp:330 Secure Link Detailed Status: userOut enabled: 0 user plane: NOT CONNECTED control plane: NOT CONNECTED control plane: NOT CONNECTED</id>				Console	of all available	lmsf> status
 8 IR-01 SEND UA LMSF Establish secure cs-sh lmsf Console session for the lmsf> secure start Control Plane and User Plane traffic 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment are messages exchanged exchanged over the selected link 10 SER-07 VERIFY CS LMSF CS status shows lmsf messages exchanged in the selected link 10 SER-07 VERIFY CS LMSF CS status shows lmsf is secure connection for User Plane Expected output: traffic since CS STATUS User: N/<id> access to the UA Control: N/<id> access to the UA control N/<id> a</id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id></id>					links at UA	
Console session for the lmsf> secure start Control Plane and User Plane traffic 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Sniffer establishment are messages exchanged exchanged over the selected link 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console no secure lmsf> status secure connection for User Plane Expected output: traffic since CS STATUS User: N/ <id> access to the UA Control: N/<id> access to the UA Control: N/<id> access to the UA Control: N/<id> secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0 user plane: NOT CONNECTED control plane: NOT CONNECTED</id></id></id></id>	8	IR-01	SEND	UA LMSF	Establish secure	cs-sh lmsf
Control Plane and User Plane traffic 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Sniffer establishment are messages exchanged exchanged over the selected link 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console no secure lmsf> status secure connection for User Plane Expected output: traffic since CS STATUS User: N/ <id> access to the UA Control: N/<id> access to the UA Control: N/<id> access to the UA Control: N/<id> userOut enabled: 0 user plane: NOT CONNECTED control plane: NOT CONNECTED</id></id></id></id>				Console	session for the	lmsf> secure start
and User Plane traffic 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment Sniffer establishment are messages exchanged exchanged over the selected link 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console no secure lmsf> status secure connection for User Plane Expected output: traffic since CS STATUS User: N/ <id> access to the UA Control: N/<id> access to the UA Control: N/<id> secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0 user plane: NOT CONNECTED control plane: NOT CONNECTED</id></id></id>					Control Plane	
traffic 2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment 10 SER-07 VERIFY CS LMSF CS status shows Imsf 10 SER-07 VERIFY CS LMSF CS status shows Imsf 10 SER-07 VERIFY CS LMSF CS status shows Imsf 11 IR-07 Console no secure Imsf> status secure 11 IR-07 Console Mosecure Imsf> status secure 12 User Plane Expected output: traffic since CS STATUS User: N/ <id> is denied 2023-08-22 18:25:32.068847 GMT INFO SessionManager.cpp:330 secure session session NOT CONNECTED Ouse</id>					and User Plane	
2023-08-22 18:25:15.273392 GMT INFO ControlOut.cpp:193 Enabling secure session 9 IR-01 OBSERVE CS Main Sniffer Status secure session observe secure session establishment 10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console no secure lmsf> status secure connection for User Plane Expected output: traffic since CS STATUS User: 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</id>					traffic	
 9 IR-01 OBSERVE CS Main Sniffer 10 SER-07 VERIFY CS LMSF IR-07 Console Console 10 SER Plane 2023-08-22 18:25:32.068847 GMT INFO Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0 user plane: NOT CONNECTED 	2023-	08-22-18	3:25:15.273	392 GMT INF	Control	Out.cpp:193
 9 IR-01 OBSERVE CS Main Secure session Observe secure session establishment messages exchanged 10 SER-07 VERIFY CS LMSF CS status shows lmsf like selected link 10 SER-07 VERIFY CS LMSF CS status shows lmsf like selected output: traffic since CS status secure connection for User Plane Expected output: traffic since CS STATUS User: N/<id> 10 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 </id>	Enabl	ing sect	are session	COM.	C ·	
Shiller establishment are messages exchanged exchanged over exchanged over the selected link Imsf IR-07 CS LMSF CS status shows Imsf IR-07 Console no secure Imsf> User Plane Expected output: traffic since CS STATUS User: N/ <id> Imsf> 2023-08-22 18:25:32.068847 GMT INFO SessionManager.cpp:330 Secure Link Detailed Status: userOut enabled: 0 output: user plane: NOT CONNECTED control plane: control plane: NOT CONNECTED Expected output:</id>	9	IK-01	OBSERVE	CS Main	Secure session	Observe secure session establishment
10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console no secure lmsf> status secure connection for User Plane Expected output: traffic since CS STATUS User: N/ <id> access to the UA Control: N/<id> is denied 2023-08-22 18:25:32.068847 GMT INFO SessionManager.cpp:330 Secure Link Detailed Status: userOut enabled: 0 output user plane: NOT CONNECTED control plane:</id></id>				Sniffer	establishment are	messages exchanged
10 SER-07 VERIFY CS LMSF CS status shows lmsf IR-07 Console no secure lmsf> status secure connection for User Plane Expected output: traffic since CS STATUS User: N/ <id> access to the UA Control: N/<id> is denied 2023-08-22 18:25:32.068847 GMT INFO Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0 user plane: NOT CONNECTED control plane: NOT CONNECTED</id></id>					the selected link	
IR-07 Console no secure lms1 IR-07 Console no secure lms5> status secure connection for User Plane Expected output: traffic since CS STATUS User: N/ <id> access to the UA Control: N/<id> access to the UA Control: N/<id> is denied 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</id></id></id>	10	SED 07	VEDIEV	CS I MSE	CS status shows	lmsf
<pre>INTERPORT CONNECTED Console Indiscult Interport Secure Secure connection for User Plane Expected output: traffic since CS STATUS User: N/<id> access to the UA Control: N/<id> is denied 2023-08-22 18:25:32.068847 GMT INFO SessionManager.cpp:330 Secure Link Detailed Status: userOut enabled: 0 user plane: NOT CONNECTED control plane: NOT CONNECTED</id></id></pre>	10	JR_07	VENIT I	Console		lmsf> status secure
User Plane Expected output: traffic since CS STATUS User: N/ <id> access to the UA Control: N/<id> is denied 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</id></id>		111-07		Console	connection for	imbi/ bedeub beedie
traffic since CS STATUS User: N/ <id> access to the UA Control: N/<id> is denied 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</id></id>					User Plane	Expected output:
access to the UA Control: N/ <id> is denied 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</id>					traffic since CS	STATUS User: $N/\langle ID \rangle$
is denied 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					access to the $U\Delta$	Control $\cdot N < TD >$
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					is denied	
Secure Link Detailed Status: userOut enabled: 0 controlOut enabled: 0 user plane: NOT CONNECTED control plane: NOT CONNECTED	2023-	08-22 18	3:25:32.068	847 GMT INF	0 SessionN	Manager.cpp:330
userOut enabled: 0 controlOut enabled: 0 user plane: NOT CONNECTED control plane: NOT CONNECTED	Secur	e Link D	Detailed St	atus:		
controlOut enabled: 0 user plane: NOT CONNECTED control plane: NOT CONNECTED	userO	ut enabl	Led: 0	· · · · ·		
user plane: NOT CONNECTED control plane: NOT CONNECTED	contro	olOut er	nabled: 0			
control plane: NOT CONNECTED	user 1	plane: N	NOT CONNECT	ED		
	contr	ol plane	e: NOT CONN	ECTED		

STEP	REQ	Action	Component	Description	Procedure
11	SER-07	VERIFY	UA LMSF	UA status shows	cs-sh lmsf
	IR-07		Console	<u>no</u> secure	lmsf> status secure
				connection for	
				User Plane	Expected output:
				traffic since CS	STATUS User: N/ <id> Control: N//ID> </id>
				is depied	concrot. N/ <ib <="" td=""></ib>
2023-	08-22 18	:25:37.654	528 GMT INF() Session	Manager.cop:330
Secur	e Link D	etailed Sta	atus:		14114901.0pp.000
user0	ut enabl	ed: 0			
contr	olOut en	abled: 0			
user j	plane: N	OT CONNECT	ED		
contr	ol plane	: NOT CONNE	ECTED		
12	IR-03	SEND	CS UDMD	Send User Data	udmd
_			Console		udmd> send n=1
📕 frame.	time_relative ==	246.453790129			
No.	Time	Source	Destinatio	n Protoco	l Length Info
1	3 246.453790	129 10.100.0.2	10.100.	0.1 UDP	91 36483 → 55444 Len=63
<					
Y Frame	e 13: 91 byt	es on wire (728	bits), 91 bytes	captured (728 bits	0000 45 00 00 5b 91 e4 40 00 40 0010 0a 64 00 01 8e 83 d8 94 00
> Ir	terface id:	0 (tun18)			0020 02 00 00 00 00 00 00 00
Er	capsulation	type: Raw IP (7	7)		0030 00 00 00 00 00 00 00 00 00
Ar	rival Time:	Aug 22, 2023 11	1:25:46.811794320	Pacific Daylight	0050 41 41 41 41 41 41 41 41 41 41 0050 41 41 41 2d 30 30 30 30 30
CS Us	er sniff	er shows UI	DMD message	at 11:25:46 B	PDT
13	IR-03	VERIFY	CS Main	User Data is <u>not</u>	The traffic sniffer log shows that User
			Sniffer	sent by the CS	Data message was not sent by the CS
0000	00 00 10				DTSR at time 18:25:46 GMT
2023-	U8-22 18 wod. TD.	:25:46.8118	837 GMT INFO	Cmd. SEND S	pp:si
Datai	иеа. тр. ир-дадад		22222-000003) CIIIQ: SEND SI	IZE. 03 KSP. FALSE
Sendi	ng user	data messa	ne to peer	<u>-</u>	
Secur	e sessio	n disabled	- ID: 00000	0002 Origin: U	JDMD Cmd: SEND Size: 63 Rsp:
FALSE	not sen	t to peer		···- · j ·	
Sendi	ng "ID:	00000002 01	rigin: UDMD	Cmd: SEND Siz	ze: 136 Rsp: TRUE Success: F
Msg:	" to lms	f_queue			
Sent	"ID: 000	00002 Orig:	in: UDMD Cmo	d: SEND Size:	136 Rsp: TRUE Success: F
Msg:	Secure s	ession disa	abled - ID:	00000002 Oric	gin: UDMD Cmd: SEND Size: 63
Rsp:	FALSE no	t sent to p	peer to lmst	f_queue	
14	IR-03	VERIFY	UA User	User Data is <u>not</u>	Verity via the traffic sniffer log that that
			Sniffer Log	received by the	no User Data message was received by
				UA	ine UA DISK

STEP	R	EQ	Actio	on	Component	Description		Procedure		
Examp with so	ole from	m test o: 10.100.0	n Sept 8').2.	th . CS s	ent n=1 at 9:24:	21; UA User Sniffer	r shows no m	essages received at t	hat time	
📕 ua	.user.sn	iffer.2023	.09.08-09.	50.59.pc	apng					
File	Edit \	View G	o Captu	ire An	alyze Statistics	Telephony Wireless	Tools Help)		
	6		💿 🗙 🕻) ୍	🗢 🔿 🗟 🖗 :	J 📃 📃 🔍 Q	Q. 🏨			
📙 udp										
No.		Time		Source		Destination	Protocol	Length Info		
	5107 5108	5376.8	397254 403578	10.100).0.1).0.1	10.100.0.2	UDP	91 3482 91 3482	(3 → 5 (3 → 5	
L	5109	5625.9	449502	10.100).0.1	10.100.0.2	UDP	91 3482	13 → 5	
<										
Y Fra	ame 51	09: 91	bvtes o	n wire	(728 bits), 9	1 bytes captured (728 bits) o	n interface tun18.	000	
	Secti	on numb	er: 1						001	
>	Inter	face id	: 0 (tu	n18) Bow T	. (7)				003	
	Arriv	al Time	: Sep a	каш 1 8, 2023	3 09:24:50.354	049834 Pacific Day	light Time		004	
	[Time	shift	for this	s packe	et: 0.00000000	0 seconds]	0		1005	
	Epoch	Time:	1694190	290.354	1049834 second	5	d-1			
[lime delta from previous captured frame: 108.004592440 seconds] [Time delta from previous displayed frame: 108.004592440 seconds]										
	[Time	since	referen	ce or f	first frame: 5	525.944950290 seco	nds]			
	Frame	Number	: 5109	haa (7)						
	Captu	Lengtn re Leng	: 91 by th: 91 l	tes (72 bytes ((728 bits)					
	[Fram	e is ma	rked: Fa	alse]	(,					
	[Fram	e is ig	nored: 1	False]						
	[Prot	ocols 1 ring Ru	n trame le Name	: raw:: : UDPl	Lp:udp:dataj					
	[Colo	ring Ru	le Stri	ng: udp	o]					
Rav	v pack	et data								
Ƴ Int	ternet	Protoc	ol Vers	ion 4,	Src: 10.100.0	.1, Dst: 10.100.0.	2			
15	IR	R-03	SEND		UA UDMD Console	Send User Data	udmd udmd> se	nd n=1		
16	IR	R-03	VERIFY	Y	UA Main	User Data is not	Notification	that User Data can	10t be	
					Sniffer	sent by the UA	sent from th	e UA DTSR		
2023	-08-2	22 18: • • • • • •	:25:57	.4421	90 GMT INF) UdmdIn.c	pp:51			
Data	•UD-7	: ID: AAAAAZ	AAAAA	004 C AAAAA	AAAA-00000	U CHIQ: SEND SI 4	12e: 03 R	sp: FALSE		
Send	ing ι	user c	lata m	essag	e to peer	-				
Secu	re se	essior	n disa	bled	- ID: 0000	0004 Origin: U	JDMD Cmd:	SEND Size: 63	8 Rsp:	
FALS: Send	E not ing '	t sent "TD• (to p	<mark>eer</mark> 04 Or	idin. IIDMD	Cmd. SEND Siz	20. 136 RG	an. TRUE Succe	vee. L	
Msq:	" to	o lmsf	gueu	e e	igin. Obhb	CIIIC. SEND SIZ	.e. 100 K	sp. inor succe	:55. F	
Sent	"ID	: 0000	00004	Origi	n: UDMD Cm	d: SEND Size:	136 Rsp:	TRUE Success:	F	
Msg:	Seci	are se	ession	disa	bled - ID:	00000004 Orig	gin: UDMD	Cmd: SEND Siz	:e: 63	
кsp: 17	FALS ID	SE not	, sent VERIEV	το p Z	CSUser	L_queue User Data is not	Verify via t	he traffic sniffer log	that no	
1/	IN	. 05	V LIXII' I	L	Sniffer	received by the	User Data n	nessage was receive	d by the	
						CS	CS DTSR o	r UDMD	2	

STEP	REQ	Action	Component	Description				Procedure
, udp								
No.	Time	Source	Destination	Protocol	Length	Info		
	13 246.453790129	10.100.0.2	10.100.0.1	UDP	91	36483	→ 55444	Len=63
Г	14 677.276722211	10.100.0.2	10.100.0.1	UDP	68	60159	→ 55444	Len=40
L	20 862.619209385	10.100.0.2	10.100.0.1	UDP	91	60159	→ 55444	Len=63
<								
Y Fra	me 14: 68 bytes (on wire (544	bits), 68 bytes capture	d (544 bits) or	n inter	face t	tun18. id	10
	Section number: 1	L Ì		· · · ·				
>	Interface id: 0 ((tun18)						
	Encapsulation typ	e: Raw IP (7)					
	Arrival Time: Aug	3 22, 2023 1	1:32:57.634726402 Pacifi	c Daylight Time				

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	Send a User Data	udmd					
			Console	less than MTU	udmd> send n=1					
				size						
UA DT:	SR									
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-AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA										
Sendi	ng user	data messag	ge to peer							
User (Output:	Sent 66 byt	ces.							
Buffe	r Conter	nts: [054200	040000002	000000040000	007f 000003f0000000					
00000	000fa107	455 0000005	5442d4141	41414141414	141 41414141414141					
414120	d3030303	3400]								
Sent	"USER_DA	TA.REQ	66							
2	IR-09b	VERIFY	CS Main	User Data <	Verify via the traffic sniffer log that					
			Sniffer	MTU does not require segmentation	User Data was not segmented					

STE	EP REQ	Act	tion	Compone	ent	Description	n		Pro	ocedure	e
🔳 ip	ov6.addr == fd00:bbcc	:dde0::a	ipv6.addr =	= fd00:bbcc:do	de0::f						
No.	Time	5	Source		Destinat	on	Prot	ocol	Lengt Info		
	78263 3703.636	7066 1	fd00:bbcc:	dde0::f	fd00:b	bcc:dde0::a	DTL	Sv1.2	113 Appl	ication	Data
	79696 3767.174	2560 1	fd00:bbcc:	dde0::a	fd00:b	bcc:dde0::f	DTL	Sv1.2	171 Appl:	ication	Data
	81003 3828 257	4532 1	Ed00.hhcc.	dde0f	fd00.h	hcc:dde0::a	DTI	Sv1 2	224 Annl	ication	Data
> F	rame 79696: 171	bytes (on wire (1	1368 bits),	171 by	rtes captured	(1368	3 bits) o	on interface	e tun2,	id 1
F	Naw packet data										
~ 1	internet Protocol	. Versi	on 4, Src:	10.20.0.1	, Dst:	10.20.0.2					
	0100 = Ve	rsion:	4								
	0101 = He	ader Le	ength: 20	bytes (5)							
	> Differentiated	Servi	ces Field:	0x00 (DSC	P: CS0,	ECN: Not-ECT	r)				
	Total Length:	171									
	Identification	: 0xde	54 (56916)	-							
	> 010 = F1	ags: 0	x2, Don't	fragment							
	0 0000 0000	0000 :	= Fragment	: Offset: 0							
	Time to Live: 255										
	Header Checksu	(41) m· 0v8	8aa [valid	lation dica	bled]						
	Header Checksum: 0x88aa [validation disabled]										
		• 10 20	a a 1	Tited]							
	Destination Ad	dress:	10.20.0.2	,							
\sim 1	internet Protocol	Versi	on 6. Src:	fd00:bbcc	:dde0::	a. Dst: fd00	: bbcc :	dde0::f			
	0110 = Ve	rsion:	6			.,					
	> 0000 0000				= Traff	ic Class: 0x0	00 (DS	CP: CS0.	ECN: Not-E	ECT)	
	1111 1101	0100	0010 0010	= Flow Lab	el: 0xf	d422				1	
	Payload Length	: 111									
	Next Header: U	DP (17))								
	Hop Limit: 64										
	Source Address	: fd00	:bbcc:dde0)::a							
	Destination Ad	dress:	fd00:bbcc	::dde0::f							
> L	lser Datagram Pro	tocol,	Src Port:	46466, Ds	t Port:	51102					
× 0	atagram Transpor	rt Laye	r Security	/							
	 DTLSv1.2 Recor 	d Layei	r: Applica	tion Data	Protoco	l: Applicatio	on Dat	a			
	Content Typ	e: App]	lication D	ata (23)							
	Version: DT	LS 1.2	(0xfefd)								
	Epoch: 1		_								
	Sequence Nu	mber: 2	2								
	Length: 90		den Beber	adaccrc		44 - 42 0.02 45 -	67440	000-000-	-01407014-4		52-02400400-
	Encrypted A	ppiicat	cion Data:	009068856	u2005TT	010036092/050	.17400	092e280a	C9140/01401	oadaød3	12000490400C
3	SER-04	VERIF	FY	UA Main	τ	Jser Data sen	t is	Verify	via the traf	fic sniff	fer log that the
				Sniffer	e	ncrypted		content	of the Use	r Data r	nessage sent
						J 1		cannot	be discerne	- ed	0
								Juinot			
U U	dp.port == 51102										
No	Time	Sol	urce	De	etination	Dr	otocol	Long	t Info		

No. Time Source Destination Protocol Lengt Infi 19929 1489.5634411 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2 113 App 21170 1552.1051299 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2 171 App 22327 1613 6457667 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2 224 App > Frame 21170: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interfa Raw packet data Bate Bate Bate Bate Bate Bate	b blication Data blication Data blication Data blication Data ce tun2 id 0						
19929 1489.5634411 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2 113 App 21170 1552.1051299 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2 171 App 22327 1613 6457667 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2 224 App > Frame 21170: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interfa Raw packet data	plication Data plication Data plication Data						
21170 1552.1051299 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2 171 App 22327 1613 6457667 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2 224 App > Frame 21170: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interfa Raw packet data	plication Data						
> 22327 1613 6457667 fd00:bbcc:dde0:f fd00:bbcc:dde0:e DTLSv1 2 224 Apv > Frame 21170: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interfa Raw packet data	lication Data						
> Frame 21170: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interfa Raw packet data	ce tun2 id 0						
Raw packet data	ice conzy zo o						
> 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							
✓ Datagram Transport Layer Security							
✓ DTLSv1.2 Record Layer: Application Data Protocol: Application Data							
Content Type: Application Data (23)							
Version: DTLS 1.2 (0xfefd)							
Epoch: 1							
Sequence Number: 2	Sequence Number: 2						
Length: 90							
Encrypted Application Data: 0d966aa56d28d5ffd1cd3ec927d5cf74d0092e280ac91407014	ef6ada0d3f3b08490400c						
UA Main sniffer shows application data is encrypted							
4 SER-04 VERIFY CS Main User Data Verify via t	he traffic sniffer log that						

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
ipv6.addr == fd00:bbc	::dde0::a ipv6.addr	== fd00:bbcc:dde0::f			
No. Time	Source	Destinat	ion Proto	ocol	Lengt Info
78263 3703.63	57066… fd00:bbc	c:dde0::f fd00:b	bcc:dde0::a DTLS	5v1.2	113 Application Data
79696 3767.174	42560 fd00:bbc	c:dde0::a fd00:b	bcc:dde0::f DTLS	5v1.2	171 Application Data
81003 3828 25	74532 ±d00•hhc		hccidde0iia DTLS	5v1 2	224 Application Data
Prame 79696: 171 Paw packet data	bytes on wire	(1368 Dits), 1/1 D	tes captured (1368	DITS)	on interface tunz, id i
> Internet Protoco	l Version 4. Sr	c: 10.20.0.1. Dst:	10.20.0.2		
> Internet Protoco	l Version 6, Sr	c: fd00:bbcc:dde0:	a, Dst: fd00:bbcc:	dde0::f	
> User Datagram Pr	otocol, Src Por	t: 46466, Dst Port	51102		
Ƴ Datagram Transpo	rt Layer Securi	ty			
✓ DTLSv1.2 Reco	rd Layer: Appli	cation Data Protoco	ol: Application Data	a	
Content Ty	e: Application	Data (23)			
Version: D	LS 1.2 (Øxtetd)			
Sequence N	mber: 2				
Length: 90					
Encrypted /	Application Dat	a: 0d966aa56d28d5f1	d1cd3ec927d5cf74d00	092e280	ac91407014ef6ada0d3f3b08490400c
CS Main Sniffer sł	iows application	on data is encrypte	d		
Post-test Log Anal	ysis				
5 SER-02	VERIFY	CS and UA	User Data	a)	Compare the CS DTSR log with
SER-04		DTSR Live	received matches		source data on the UA to show the
		Log	User Data sent		the sent and received contents ar
			which indicates		the same
			the message was	b)	Compare the UA DTSR log with
			accepted as	,	the source data on the CS to sho
			authentic.		that the sent and received conten
					are the same.
JA DTSR					
2023-08-24 16	5:57:31.81	8437 GMT INF() UdmdIn.	cpp:	51
Sending user	data mess	age to peer	•••••••••••••••••••••••••••••••••••••••	opp.	
User Output.	Sent 66 b	vtes			
Buffer Conter	$1 + s \cdot [05/2]$		000000000000000000000000000000000000000	0007	£ 000003£0000000
	163. [0342	0004000000002	1111111111111	л 1 л 1 л 1	
4141222020203	2020 2400	1			4141414141414141
414120303030.	5050 5400]			
CS DI SK			· ·· ·		4.2
2023-08-24 10):)/:31.9/	/438 GMT INF(userin.	cpp:	43
Keceived "USE	JK_DATA.RE				0 00000000 107455
		UUU4UUUUUU/f	0000003±000	00000	U UUUUUUUUIA10/455
00000055442d4	4141 4141	414141414141	41414141414	1414	1 41412d30303030303 34

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	Send a User Data	cs-rft <filename> <local< th=""></local<></filename>
			Console	greater than	filename>
				MTU size	
2	IR-09b	VERIFY	UA Main	User Data >	Verify via the traffic sniffer log that
			Sniffer	MTU is	User Data was segmented
				segmented	

S	ТЕР	REQ	Action	Compor	nent	t Description			Procedure
	ipv6.addr	== fd00:bbcc:dde0::	a ipv6.addr ==	fd00:bbcc:dde	0::f				
No). 	Time	Source	0	Destination		Protocol	Length	Info
	3815	2 2301.7844058	fd00:bbcc:d	lde0::f f	fd00:bbcc:	dde0::a	DTLSv1.2	228	Application Data
	3815	5 2301.7879238	fd00:bbcc:d	lde0::a f	fd00:bbcc:	dde0::f	IPv6	1420	IPv6 fragment (of
	3815	6 2301.7879671	fd00:bbcc:d	lde0::a f	fd00:bbcc:	dde0::f	DTLSv1.2	296	Application Data
	3815	7 2301.8091817	fd00:bbcc:d	lde0::a f	fd00:bbcc:	dde0::f	IPv6	1420	IPv6 fragment (of
	3815	8 2301.8092256	fd00:bbcc:d	lde0::a f	fd00:bbcc:	dde0::f	DTLSv1.2	296	Application Data
	3816	0 2301.8710348	fd00:bbcc:d	lde0::a f	fd00:bbcc:	dde0::f	IPv6	1420	IPv6 fragment (of
	3816	1 2301.8711460	fd00:bbcc:d	lde0::a f	fd00:bbcc:	dde0::f	DTLSv1.2	296	Application Data
	3816	8 2301.9358867	fd00:bbcc:d	lde0::a f	fd00:bbcc:	dde0::f	IPv6	1420	IPv6 fragment (of
	3817	0 2301.9359322	fd00:bbcc:d	lde0::a f	fd00:bbcc:	dde0::f	DTLSv1.2	296	Application Data
	3817	1 2302.0008402	fd00:bbcc:d	lde0::a f	fd00:bbcc:	dde0::f	IPv6	1420	IPv6 fragment (of
	3817	2 2302.0009685	fd00:bbcc:d	lde0::a f	fd00:bbcc:	dde0::f	DTLSv1.2	296	Application Data
	3817	3 2302.0654244	fd00:bbcc:d	lde0::a f	fd00:bbcc:	dde0::f	IPv6	1420	IPv6 fragment (of
	3817	4 2302.0655010	fd00:bbcc:d	lde0::a f	fd00:bbcc:	dde0::f	DTLSv1.2	296	Application Data
	3817	6 2302.1185340	fd00:bbcc:d	lde0::f f	fd00:bbcc:	dde0::a	DTLSv1.2	716	Application Data
1	2017	0 0000 1760011	£100.66	4-0.12	CJ00.66	11-02	Thur	1400	TD./ former / f
~	Frame 38155: 1420 bytes on wire (11360 bits), 1420 bytes captured (11360 bits) Section number: 1 Interface id: 1 (tun1) Encapsulation type: Raw IP (7) Arrival Time: Aug 24, 2023 10:10:01.501954484 Pacific Daylight Time [Time shift for this packet: 0.00000000 seconds] Epoch Time: 1692897001.501954484 seconds [Time delta from previous captured frame: 0.003652668 seconds] [Time delta from previous displayed frame: 0.003517967 seconds] [Time since reference or first frame: 2301.787923865 seconds] Frame Number: 38155 Frame Length: 1420 bytes (11360 bits) Capture Length: 1420 bytes (11360 bits) [Frame is marked: False]						d (11360 bi t Time] s]	0040 9 0050 0 0060 e 0070 9 0080 3 0090 6 0080 9 0080 9 0080 9 0080 9 0080 9 0080 8 0000 8 0000 8 0000 8 0000 8 0000 6 0000 8 0000 8 0000 8 0000 8 0000 8 0000 8 0000 8 0000 8 0000 8 0000 9 0000 8 0000 9 0000 8 0000 8 00000 8 0000 8 00000 8 00000 8 0000 8 00000 8 00000 8 00000000	a d8 29 7b pee eb c 1 00 00 00 00 01 4 0 00 00 01 7 2a 39 6 9 9 c1 fd 91 c6 6 e bc b0 4e 8f 22 f 2 5c 8d b3 ac 53 e e 2b 9e 5e 2c aff f 2 f 6 f0 66 9a 2f 7f 2 3d e5 91 52 48 5 3 d4 e5 69 32 f8 5 5 91 52 9b 25 49 e 1 aa 0c 99 15 f f 6 ad 2 1 4 b5 6a 7db
	[Pro	tocols in frame	: raw:ip:ip	/6:ipv6.frag	ghdr:data]			0150 d	7 57 15 cb 35 8e 2
	Raw pac	ket data						0170 1	5 00 00 01 00 09 a f f5 dd 7e 60 a6 f
>	Interne	t Protocol Vers	ion 4, Src:	10.10.0.1,	Dst: 10.1	0.0.2		0180 0	c 79 15 0d c3 7h 4
~	Interne	t Protocol Vers	ion 6, Src:	fd00:bbcc:	dde0::a, [)st: fd00:b	bcc:dde0::f	0190 1	f b5 28 97 13 <u>c4</u> 1

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 Ma	ain sniffer lo	og snapshot in	step 2 shows me	ssage is encrypted.	
4	SER-04	VERIFY	CS Main	User Data	Verify via the traffic sniffer log that the
			Sniffer	received is	content of the User Data message

sniffer log that the content of the User Data message received cannot be discerned

encrypted

STEP	REQ	Action	Compo	onent	Descrip	tion			Proce	dure	•
📕 ipv6.add	dr == fd00:bbcc:dde0	::a ipv6.addr ==	fd00:bbcc:dd	le0::f							
No.	Time	Source		Destination		Protocol	Lengt	Info			
992	259 4517.9471030	fd00:bbcc:d	de0::a	fd00:bbcc	:dde0::f	IPv6	1420	IPv6 fr	agment	: (off	=0 mc
• 992	260 4517.9631206	fd00:bbcc:d	lde0::a	fd00:bbcc	:dde0::f	DTLSv1.2	296	Applica	ation D	Jata	
992	265 4518.0500565	fd00:bbcc:d	lde0::a	fd00:bbcc	:dde0::f	IPv6	1420	IPv6 fr	agment	: (off	=0 mc
992	266 4518.0501321	fd00:bbcc:d	lde0::f	fd00:bbcc	:dde0::a	DTLSv1.2	192	Applica	ation D	ata	
992	267 4518.0698521	fd00:bbcc:d	lde0::a	fd00:bbcc	:dde0::f	DTLSv1.2	296	Applica	ation D	ata	
992	268 4518.1290478	fd00:bbcc:d	de0::a	fd00:bbcc	:dde0::f	IPv6	1420	IPv6 fr	agment	: (off	=0 mc
992	09 4518.1495935	fd00:bbcc:d	lde0::a	fd00:bbcc	:dde0::f	DTLSv1.2	296	Applica	ation D	ata	
992	271 4518.2097929	fd00:bbcc:d	lde0::a	fd00:bbcc	:dde0::f	IPv6	296	IPv6 fr	ragment	: (off	=1352
992	72 4518.2098051	fd00:bbcc:d	lde0::a	fd00:bbcc	:dde0::f	DTLSv1.2	1420	Applica	ation D	ata	
992	89 4518.2341292	fd00:bbcc:d	lde0::f	fd00:bbcc	:dde0::a	DTLSv1.2	192	Applica	ation D	ata	
992	90 4518.3294265	fd00:bbcc:d	de0::a	fd00:bbcc	:dde0::f	IPv6	296	IPv6 fr	ragment	: (off	=1352
<											
✓ Frame	99259: 1420 byt	tes on wire (1	L1360 bits), 1420 by	tes captur	ed (11360 bit	0000	45 00	05 8c	1e 67	40 (
Sec	tion number: 1		,	,,,			0010	0a 0a	00 02	60 00)e7 {
> Int	erface id: 0 (t	:un1)					0020	dd e0	00 00	00 00	00 (
Enc	apsulation type	: Raw IP (7)					0030	dd e0	00 00	00 00	00 (
Ann	ival Time: Aug	24, 2023 10:1	0:02.75020	03684 Paci	fic Davlig	ht Time	0040	9a d8	29 7b	be et	o c7 s
Гті	me shift for th	is packet: 0.	000000000	seconds]	, ,		0050	00 10 e6 da	69 07	20 00	66 1
Epo	ch Time: 169289	7002.75020368	4 seconds				0070	99 99	c1 fd	2a a: 91 ci	5 65 1
Гті	me delta from p	previous captu	red frame:	: 0.096363	616 second	s1	0080	3e bc	b0 4e	8f 22	2 f2 5
Î TI	me delta from p	revious displ	laved frame	e: 0.38248	9697 secon	ds1	0090	62 5c	8d b3	ac 53	3 e1 4
Гті	me since refere	ence or first	frame: 451	17.9471030	91 seconds	1	00a0	0e 2b	9e 5e	2c at	f f2 9
Fra	me Number: 9925	9				·	00b0	96 fØ	e6 9a	2f 71	F 21 🕻
Fra	me Length: 1420) bytes (11360) bits)				00c0	83 d4	e5 b9	16 ea	a 2c e
Car	ture Length: 14	20 bytes (113	60 bits)				00d0	ec 72	56 69	32 18	3 53 5
[Er	ame is marked:	Falsel	,				0000	C5 91	52 90	25 45	ee (
[Fr	ame is ignored:	Falsel					0100	e7 60	h7 4h	6d 24	14
[Pr	[Protocols in frame: rawin:inv6:inv6 fraghdr:data]							44 b5	6a 7d	ba f4	1 1b a
Raw pa	cket data				1		0120	56 45	73 07	36 dl	0 14 0
> Interr	Thermet Protocol Version 4 Spc: 10 10 0 1 Dct: 10 10 0 2								39 bd	4c do	ad (
> Interr	Thernet Protocol Version 6, Src: 10.10.0.1, DSC: 10.10.0.2 Internet Protocol Version 6, Src: fd00:bbcc:dde0::a Dct: fd00:bbcc:dde0:.f							75 be	e 88 4		
> Data (A Data (1252 hutas)								25 1		
CS Main	sniffer shows	messages an	e encrypt	ted							
Post-test	t Log Analysis	-									
5	SER-02 VI	ERIFY	UA and	ICS U	Jser Data	Co	mpare	e the re	eceive	d Us	er Data

- SER-04
- Content Directory
- User Data sent which indicates the message was accepted as authentic.

Compare the received User Data file received matches 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, $PA\overline{Y}LO\overline{A}D DATA < MTU$

Procedure:

STEP	REQ	Action	Component	Description	Procedure			
1	IR-09b	SEND	UA UDMD	Send User Data less	cs-sh			
			Console	than MTU size	udmd> send n=1			
UA DTSE	UA DTSR							
2023-09	9-08 16:	08:27.122	2153 GMT INF	O UdmdIn.cpp:	51			
Receive	ed: ID:	0000024	Origin: UDM	D Cmd: SEND Size:	63 Rsp: FALSE			
Data: [Data: UD-AAAAAAAAAAAAAAAAAAAAAAO00024							
Sending user data message to peer								
User Output: Sent 66 bytes.								

STEP	REQ	Action	Component	Description	Proced	lure		
2	IR-09b	VERIFY	CS Main	User Data < MTU	J Verify via the traffi	c sniffer log that		
			Sniffer	does not require	User Data was not s	segmented		
🧲 cs.main.s	niffer.2023.09.0	8-09.54.40.pcapng		segmentation				
File Edit	View Go C	apture Analyze	Statistics Telephony	Wireless Tools Help				
	۱ 📙 💽	रे 🖸 🍳 🗢 🔿	2 🕅 🕹 📃 📃	0,0,0,1				
ipv6.addr =	= fd00:bbcc:dde	e0::a ipv6.addr ==	fd00:bbcc:dde0::f					
lo.	Time	Source	Destination	Protocol	Length Info			
76809	4425.875348	39 fd00:bbcc:d	de0::a fd00:bbc	::dde0::f DTLSv1.2	2 167 Application Data			
76819	4425.951922	20 fd00:bbcc:d	de0::f fd00:bbco	::dde0::a DTLSv1.2	2 193 Application Data			
> Frame 76	809: 167 by	tes on wire (13	36 bits), 167 byte	s captured (1336 bit	s) on interface tun2, id 2			
Raw pack	et data		,, ,,		,			
✓ Internet 0100	Protocol Vers:	ersion 4, Src: ion: 4	10.20.0.1, Dst: 10	.20.0.2				
	0101 = Heade	er Length: 20 b	ytes (5)					
> Diffe Total	Length: 167	ervices Field: 7	0x00 (DSCP: CS0, E	CN: Not-ECT)				
Ident	ification: (0x0089 (137)						
> 010.	= Flag: 0000 0000 00	s: 0x2, Don't f 000 = Fragment	ragment Offset: 0					
Time	to Live: 25	5						
Proto Heade	col: IPv6 (4 r Checksum:	∔1) 0x667a [valida	tion disabled]					
[Head	er checksum	status: Unveri	fied]					
Sourc Desti	e Address: 1 nation Addre	10.20.0.1 ess: 10.20.0.2						
✓ Internet	Protocol V	ersion 6, Src:	fd00:bbcc:dde0::a,	Dst: fd00:bbcc:dde0	::f			
>	= Vers: 0000 0000	Lon: 6	= Traffic	Class: 0x00 (DSCP: 0	CS0, ECN: Not-ECT)			
	1111 0111 11	111 0101 1010 =	Flow Label: 0xf7f	5a	- ,			
Paylo Next	ad Length: 1 Header: UDP	(17)						
Hop L	imit: 64							
Sourc Desti	e Address: 1 nation Addre	ss: fd00:bbcc:dde0:	:a dde0::f					
> User Dat	agram Proto	col, Src Port:	59299, Dst Port: 5	1102				
 Datagram Data (66 	i Iransport i i bytes)	Layer Security						
Data:	05420018000	00002000000040	000007f0000003f000	0000000000000fd40635	500000055			
[Leng	th: 66]							
3	SER-02	VERIEV	CS and UA	User Data receive	d Verify the received	User Data		
5	SER-02	V LIXII ^I I	DTSR Live	matches User Data	ta message has the sar	ne contents as		
			Log	sent	the one that was ser	nt		
CS DTSF	٤		-					
2023-09-	08 16:08:2	6.844668 GM	T DEBUG Inp	utMessage.cpp:161				
Received	66 bytes o	f data from U	ser Input					
User Inpu	User Input: Expected message size is 66 bytes User Input Buffer Contents: [05/200180000002, 000000/0000007f, 0000002f00000000							
00000000)fd406355	00000055442	2d4141 4141414	141414141 41414	14141414141 41412d30303	303032 3400]		
Processin	g USER_I	DATA.REQ						
Sent "ID:	00000024	Origin: DTSI	R-UA Cmd: SEN	D Size: 63 Rsp: FA	ALSE Data:			
UD-AAA	AAAAAA	AAAAAAA	<mark>4AAA-000024</mark> " 1	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.
 cs.main.sniffer.2023.09.08-09.54.40.pcapng

File	Edit View Go Capture Ana	alyze Statistics Telephony	Wireless Tools Help					
	🔳 🔬 💿 📙 🛅 🔀 🕒 🤍 <	⇔ ⇒ 🕾 🗿 🕹 📃 📃	0,0,0,1					
, ip	v6.addr == fd00:bbcc:dde0::a ipv6.ad	ddr == fd00:bbcc:dde0::f						
No.	Time Source	Destination	Protocol	Length Ir	Info			
	76784 4424.4072371 fd00:bb	bcc:dde0::a fd00:bbcc	:dde0::f DTLSv1.	2 248 A	Application Data	а		
	76791 4424.8538607… fd00:bl	bcc:dde0::a fd00:bbcc	:dde0::f DTLSv1.	2 196 A	Application Data	а		
	76792 4424.8548712 fd00:bl	bcc:dde0::f fd00:bbcc	:dde0::a DTLSv1.	2 224 A	Application Data	а		
	76809 4425.8753489 fd00:bl	bcc:dde0::a fd00:bbcc	:dde0::f DTLSv1.	2 167 A	Application Data	а		
	76819 4425.9519220 fd00:bl	bcc:dde0::f fd00:bbcc	:dde0::a DTLSv1.	2 193 A	Application Data	а		
	76843 4426.3281031 fd00:bl	bcc:dde0::a fd00:bbcc	:dde0::f DTLSv1.	2 221 A	Application Data	а		
<	70052 4400 0407200 £300.bl	L	. 1 DTIC.A		·]:t: D-t-	-		
> F R > I > U V 0 V	<pre>rame 76809: 167 bytes on wir aw packet data nternet Protocol Version 4, : nternet Protocol Version 6, : ser Datagram Protocol, Src P atagram Transport Layer Secu </pre> <pre>/ DTLSV1.2 Record Layer: Application Version: DTLS 1.2 (0xfet Epoch: 1 Sequence Number: 70 Length: 86 Encrypted Application Data ata (66 bytes) Data: 054200180000000200004 [Length: 66]</pre>	<pre>re (1336 bits), 167 bytes Src: 10.20.0.1, Dst: 10. Src: fd00:bbcc:dde0::a, Port: 59299, Dst Port: 51 urity lication Data Protocol: on Data (23) fd) ata: 0542001800000002000 000040000007f0000003f0000</pre>	captured (1336 bit 20.0.2 Dst: fd00:bbcc:dde0 102 Application Data 0000040000007f0000000	s) on interfac :::f 3f00000000000000000000000000000000	:e tun2, id 2	0000 0010 0020 0030 0040	05 42 00 00 00 00 41 41 34 00	00 18 00 3f 00 55 41 41

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

STEP	REQ	Action	Component	De	scription			Procedu	re		
🧲 cs.main.sniff	er.2023.09.08-09.54.40.	pcapng	-		-						×
File Edit Vie	w Go Capture A	nalyze Statistics Tele	hony Wireless Tools	Help							
		. ← → ∞ 주 ₺ .									
udp.port==51	102									× →	• +
No. Ti	me	Source	Destination		Protocol	Length	Info				
46789 2	508.036104135	fd00:bbcc:dde	0::f fd00:bbcc	:dde0::a	DTLSv1.2	712	Applicat	ion Data			
46790 2	508.079719203	fd00:bbcc:dde	0::f fd00:bbcc	:dde0::a	DTLSv1.2	193	Applicat	ion Data			
46791 2	508.149179187	fd00:bbcc:dde	0::a fd00:bbcc	:dde0::f	DTLSv1.2	216	Applicat	ion Data			
46792 2	508.150677091	fd00:bbcc:dde	0::f fd00:bbcc	:dde0::a	DTLSv1.2	300	Applicat	ion Data			
46795 2	508.456275062	fd00:bbcc:dde	0::a fd00:bbcc	:dde0::f	DTLSv1.2	221	Applicat	ion Data			
46799 2	508.526878090	fd00:bbcc:dde	0::a fd00:bbcc	:dde0::f	DTLSv1.2	1112	Applicat	ion Data			
46800 2	508.569391994	fd00:bbcc:dde	0::f fd00:bbcc	:dde0::a	DTLSv1.2	188	Applicat	ion Data			
46813 2	508.947524638	fd00:bbcc:dde	0::a fd00:bbcc	:dde0::f	DTLSv1.2	232	Applicat	ion Data			
46814 2	508.948963159	fd00:bbcc:dde	0::f fd00:bbcc	:dde0::a	DTLSv1.2	188	Applicat	ion Data			
46816 2	508.949925179	fd00:bbcc:dde	0::f fd00:bbcc	:dde0::a	DTLSv1.2	324	Applicat	ion Data			
46821 2	509.315421185	fd00:bbcc:dde	0::a fd00:bbcc	:dde0::†	DTLSv1.2	260	Applicat	ion Data			
46822 2	509.316606526	fd00:bbcc:dde	0::t td00:bbcc	:dde0::a	DTLSv1.2	224	Applicat	ion Data			
46825 2	509.693582565	fd00:bbcc:dde	0::a fd00:bbcc	:dde0::t	DILSv1.2	248	Applicat	ion Data			
46826 2	509.694/08235	fd00:bbcc:dde	0::t td00:bbcc	:dde0::a	DILSV1.2	224	Applicat	ion Data			
46839 2	510.034186646		ev::a Td00:bbcc	:dde0::T	DILSV1.2	196	Applicat	ion Data			
✓ Frame 46	799: 1112 bvt	es on wire (889	6 bits), 1112 by	tes captur	ed (8896	0000 45	00 04 58	6a 72 40 00	ff 29 f8	df 0	a 14
Sectio	n number: 1					0010 0 a	14 00 02	. 60 02 2a c6	04 1c 11	40 f	d 00 b
> Interf	ace id: 2 (tu	n2)				0020 dd	e0 00 00	00 00 00 00	00 00 00	0a f	d 00
Encaps	ulation type:	Raw IP (7)				0030 dd	e0 00 00	00 00 00 00	00 00 00	0f d	6 8e
Arriva	1 Time: Sep	8, 2023 10:36:2	9.496090588 Cent	ral Daylig	ght Time	0040 04	1c 6b 23	8 17 fe fd 00	01 00 00	00 0	0 01
[Time	shift for thi	s packet: 0.000	000000 seconds]			0050 07	05 73 03	6 d3 01 00 00	02 00 00	00 0	d 00
Epoch	Time: 1694187	389.496090588 s	econds			0000 71 0070 7 1	00 00 00 00 00 00	45 00 03 d0	90 98 40	00 0	0 0e 0 06
[Time	delta from pr	evious captured	frame: -0.04254	10207 secor	nds]	0080 0a	64 00 01	0a 64 00 02	00 16 c1	9e 4	3 13
[Time	delta from pr	evious displaye	d frame: 0.07060	3028 secor	nds]	0090 4 d	ac 86 b9	80 18 01 f5	1f 7f 00	00 0	1 01
[Time	since referen	ce or first fra	me: 2508.5268780	90 seconds	5]	00a0 <mark>16</mark>	46 43 be	8b 09 75 53	49 9f 60	04 a	6 46
Frame	Number: 46799					00b0 <mark>30</mark>	0b 33 ce	5 f2 01 00 ac	1b dc 8f	38 d	e 23
Frame	Length: 1112	bytes (8896 bit	s)			00c0 03	c5 4e 2c	: ba d3 05 cd	fa fd b0	13 2	3 48
Captur	e Length: 111	2 bytes (8896 b	its)			00d0 80	0b 4e 5b	03 eb t4 96	05 80 d6	a2 4	b 96
[Frame	is marked: F	alse]				00e0 62 00f0 1f	99 IT 50	: 75 da T4 94 : 82 24 63 50	3T 1/ 1C	80 8	5 05
[Frame	is ignored:	False]				0100 de		58 a5 d6 6c	d4 46 3f	ha 2	7 66
[Proto	cols in frame	: raw:ip:ipv6:u	dp:dtls:data]			0110 60	46 e6 60	d2 7a aa 8e	a3 d7 68	35 8	f 31
[Color	ing Rule Name	: UDP]				0120 b3	12 e7 d6	5 c1 4c 0f ba	05 38 c1	32 1	e e9
[Color	ing Rule Stri	ng: udp]				0130 13	c5 85 0f	⁼ d9 cd 57 6c	dc 41 de	e9 e	c 35
Raw pack	et data					0140 <mark>9</mark> e	48 42 58	3 4a 93 87 ef	60 36 42	15 9	c 54
> Internet	Protocol Ver	sion 4, Src: 10	.20.0.1, Dst: 10	.20.0.2		0150 de) 52 6t 10) ab 2d 21 cb	eb 9e be	71 d	a f5
> Internet	Protocol Ver	sion 6, Src: fd	00:bbcc:dde0::a,	Dst: fd00	bbcc:dde	0150 93	0C 30 70	0 DZ 59 D5 11	e2 D0 e7	TE 2	2 06
> User Dat	agram Protoco	1, Src Port: 54	926, Dst Port: 5	1102		0180 bf	e4 cd_28	75 42 bf 96	b1 66 34	d0 5	d 62
Datagram	Transport La	yer Security	Data Da 1 - 1	A	- Det	0190 53	e5 <u>81 c7</u>	79 f4 ae bf	f2 <u>5b</u> <u>9e</u>	f7_d	7 77
DILSV1	∠ Kecord Lay	er: Application	Data Protocol:	Applicatio	on Data	01a0 <mark>f</mark> 1	77 fb 1c	27 93 6b 3d	90 2d b6	f8 9	4 f7
Data (10	asfanadanion	0020000000040000	0075000000500700	000000000000000000000000000000000000000	008 ff 71	01b0 34	c8 e4 fc	l b4 b8 7e d9	e3 ec 09	24 5	9 b8
[Longt	b. 10111	002000000000000000000000000000000000000	007100000100308	000000000000000000000000000000000000000	000e11/1/	01c0 e9	26 57 cc	6b 25 d3 7f	07 cb 66	65 5	0 a9
Lengt						<					>
<					>	Frame (1112 b	ytes) Decry	pted DTLS (1011 bytes)			

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

STE	P REG	Q A	ction	Compon	ent	Descrip
Text f	ile sent an	d receive	d matches.			
(П) Т	P-CM-005B	Notepad		_	_	×
Eile	Edit Earna	- View	Liele			
File	Ealt Form	at view	негр			
Some	awesome	text ne	ere			
Some	awesome	text ne	ere			
Some	awesome	text ne	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ne			
Somo	awesome	toxt he	ne			
Some	awesome	tovt he	ne			
Some	awesome	tovt he	ne			
Some	awesome	text he	re			
Some	awesome	text he	re			
Some	awesome	text he	re			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	ere			
Some	awesome	text he	re			*
In 11	Col 26	100%	Unix (LE)		UTE-8	

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

STEP	REQ	Action	Component	Description	Procedure
1	REQ	Action VERIFY	Component CS Main Sniffer	Description Control Messages are sent and User Data messages are received over the active link	 Procedure 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

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

	udp.port =:	= 51102					
No		Time	Source	Destination	Protocol	Lengt	Info
	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
	81024	3829.2575310	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	192	Application Data
~	Enome 91	002, 224 butos	an wine (1702 bits)	224 butos contuned	(1702 bits) or		unface tural id 1
	Frame of	005: 224 Dytes	on wire (1792 bits),	224 bytes captured	(1/95 DIC2) O	1 THE	riace cunz, iu i
	Raw pack	et data					
\sim	Internet	Protocol Vers	ion 4, Src: 10.20.0.2	, Dst: 10.20.0.1			

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).

	udp.port ==	= 51101					
No.		Time	Source	Destination	Protocol	Length	Info
	8714	620.938628597	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	109	Application Data
	10552	703.643603710	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	110	Application Data
	10637	704.688272858	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	108	Application Data
	10670	706.014371961	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	109	Application Data
>	Frame 10	552: 110 bytes	on wire (880 bits),	110 bytes captured	(880 bits) on	interface	e tun2, id 1 0000

```
Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
0100 .... = Version: 4
```

VERIFY

2	

UA Main Sniffer Control Messages are sent and User Data messages are received over the active link Verify via the traffic sniffer log that:

0020

0030

9949

- 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

STEPREQActionComponentDescriptionProcedureSource 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).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.dde0f	fd00.bbcc.dde0	DTLSv1_2	224	Application [lata
>	Frame 21	170: 171 bytes	on wire (1368 bits),	171 bytes captured (1368 bits) or	inte	erface tun2, i	id 0
	Raw pack	et data						
>	Internet	Protocol Vers	ion 4, Src: 10.20.0.1	, Dst: 10.20.0.2				
>	Internet	Protocol Vers	ion 6, Src: fd00:bbcc	:dde0::a, Dst: fd00:b	bcc:dde0::f			
>	User Dat	agram Protocol	, Src Port: 46466, Ds	t Port: 51102				
~	Datagram	Transport Lay	er Security					
	DTLSv:	L.2 Record Lay	er: Application Data	Protocol: Application	Data			
	Cor	ntent Type: App	olication Data (23)					
	Ver	sion: DTLS 1.2	2 (0xfefd)					
	Epo	och: 1						
	Sec	uence Number:	2					
	Ler	ngth: 90						
	End	rypted Applica	ation Data: 0d966aa56	d28d5ffd1cd3ec927d5cf	74d0092e280ac	91407	014ef6ada0d3f	3b08490400c

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)

	udp.port =:	= 51101								
No.		Time	Source		Destinat	ion	Protocol	Length	Info	
	8714	620.93862859	7 fd00:bbcc	:dde0::f	fd00:b	bcc:dde0::a	DTLSv1.2	109	Application	Data
	10552	703.64360371	0 fd00:bbcc	:dde0::a	fd00:b	bcc:dde0::f	DTLSv1.2	110	Application	Data
	10637	704.68827285	8 fd00:bbcc	:dde0::a	fd00:b	bcc:dde0::f	DTLSv1.2	108	Application	Data
	10670	706.01437196	1 fd00:bbcc	:dde0::f	fd00:b	bcc:dde0::a	DTLSv1.2	109	Application	Data
>	Frame 87 Raw pack	'14: 109 bytes et data	on wire (8	72 bits), 1	.09 byte	es captured (87	2 bits) on in	nterface	tun2, id 1	0000 0010
\sim	Internet	: Protocol Ver	sion 4, Src	: 10.20.0.2	, Dst:	10.20.0.1				0020
	0100	= Versio	n: 4							0040
		0101 = Header	Length: 20	bytes (5)						0050
	3	IR-10 IN IR-10 VE	/OKE RIFY	CS OS Co UA or CS LMSF Co	nsole	Interrupt the Secure Connection between UA & CS DTSR for a time < TET CS status show secure session is established the same lin is providing th connection after the interruption	disab enabl z a vs: lmsf on lmsf> k Expecta e STATU er Contr n	ole_lir e_lin statu ed output US User col: Y/	hk <id></id>	•
Se us co us cc	cure L erOut ntrolO er pla ntrol	ink Detai enabled: out enable ne: CONNE plane: CO	led Stat 1 d: 1 CTED NNECTED	us:		Ĩ				

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 receivedc) all Control Messages sent are received

STEP	REQ	Act	ion	Co	mponer	ıt	Description		Procedu	re	
The UA	Main	Sniffer	shows	the	user	data	messages	are	sent/received	for	the
entiret	ty of	the inte	errupt	ion †	time.						

		ua.main	.sniffe	r.2023.	08.23-17	7.16.27	.pcapng													
F	ile	Edit	View	Go	Captu	ire A	nalyze	Statisti	cs T	Telephony	w	ireless	Tools	Help						
1	7				· 💌 🛛	0	-	. 🖘 7	2 J		E G		11							
	N		•	010					r <u>v</u>				- 112							
L	u	dp.port	== 511	.02																
No) .		Time	2		Source	2			Destinatio	n		Prot	ocol	L	.ength	Info			
		1072	0 838	.9107	722116	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		712	Appl	icati	on	Data
		1072	3 838	.9956	546266	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		193	Appl	icati	on	Data
		1072	5 838	.9973	334414	fd00	:bbcc:	dde0::a		fd00:bb	cc:d	de0::f	DTL	Sv1.2		221	App1	icati	on	Data
		1073	3 839	.4723	348171	fd00	:bbcc:	dde0::a		fd00:bb	cc:d	de0::f	DTL	Sv1.2		196	App1	icati	on	Data
		1074	0 839	.8184	182853	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		224	App1	icati	on	Data
		1074	7 840	.0284	121748	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		193	Appl	icati	on	Data
		1074	8 840	.0296	591889	fd00	:bbcc:	dde0::a		fd00:bb	cc:d	de0::f	DTL	Sv1.2		221	Appl	icati	on	Data
		1075	8 840	.4729	954434	fd00	:bbcc:	dde0::a		fd00:bb	cc:d	de0::f	DTL	Sv1.2		684	App1	icati	on	Data
		1076	8 840	.8413	337170	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		712	App1	icati	on	Data
		1077	0 841	.0701	150506	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		193	App1	icati	on	Data
		1077	3 841	.0718	393245	fd00	:bbcc:	dde0::a		fd00:bb	cc:d	de0::f	DTL	Sv1.2		221	App1	icati	on	Data
		1078	1 841	.4728	356473	fd00	:bbcc:	dde0::a		fd00:bb	cc:d	de0::f	DTL	Sv1.2		196	Appl	icati	on	Data
		1079	1 841	.8843	343811	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		224	Appl	icati	on	Data
		1079	7 842	.0447	725672	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		193	Appl	icati	on	Data
		1079	9 842	.0465	510420	fd00	:bbcc:	dde0::a		fd00:bb	cc:d	de0::f	DTL	Sv1.2		221	Appl	icati	on	Data
		1080	7 842	.4732	271834	fd00	:bbcc:	dde0::a		fd00:bb	cc:d	de0::f	DTL	Sv1.2		684	Appl	icati	on	Data
		1081	5 842	.8482	285220	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		712	App1	icati	on	Data
		1082	2 843	.0935	523306	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		193	App1	icati	on	Data
		1082	4 843	.0949	910964	fd00	:bbcc:	dde0::a		fd00:bb	cc:d	de0::f	DTL	Sv1.2		221	App1	icati	on	Data
		1083	3 843	.4736	507839	fd00	:bbcc:	dde0::a		fd00:bb	cc:d	de0::f	DTL	Sv1.2		196	App1	icati	on	Data
		1083	9 843	.8879	915736	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		224	App1	icati	on	Data
		1085	0 844	.0213	377318	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		193	App1	icati	on	Data
		1085	1 844	.0229	998983	fd00	:bbcc:	dde0::a		fd00:bb	cc:d	de0::f	DTL	Sv1.2		221	App1	icati	on	Data
		1086	0 844	.4740	030706	fd00	:bbcc:	dde0::a		fd00:bb	cc:d	de0::f	DTL	Sv1.2		684	App1	icati	on	Data
		1086	9 844	.9296	559297	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		712	App1	icati	on	Data
		1087	4 845	.0567	727342	fd00	:bbcc:	dde0::f		fd00:bb	cc:d	de0::a	DTL	Sv1.2		193	App1	icati	on	Data
~	F	rame 1	.0607:	684	bytes	on w	ire (5	472 bit	s),	684 byt	es d	apture	1 (547)	2 bits)	on	interfa	ice t	un2,	id	0
		Sect	ion n	umber	r: 1															
	3	> Inte	rface	id:	0 (tu	n2)														
		Enca	psula	tion	type:	Raw	IP (7)													
		Arri	val T	ime:	Aug 2	3, 20	23 15:	30:26.0	6282	2739 Pa	cifi	c Dayl:	ight Ti	me						
I										-	-	-								

Control plane messages continue for the length of the interruption.

_										
ļ	udp	udp.port == 51101								
N	o.		Time	Source	Destination	Protocol	Length	Info		
		9003	773.087642673	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	104	Application	Data	
		9006	773.089357449	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	105	Application	Data	
		15140	1004.4345410	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	104	Application	Data	
		15142	1004.4357019	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	105	Application	Data	
		15152	1004.7197434	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	106	Application	Data	
~	/ Fra	ame 90	06: 105 bytes	on wire (840 bits), 1	05 bytes captured (84	0 bits) on ir	nterface	tun2, id 0	6	
		Sectio	on number: 1						6	
	>	Inter	face id: 0 (tu	n2)					e	
		Encap	sulation type:	Raw IP (7)					0	
		Arriva	al Time: Aug 2	3, 2023 15:29:24.6803	17510 Pacific Dayligh	t Time				
		F # 2		!+- 0 00000000					E E	

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 interruptionc) 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	СМ	007 -	Control	Message	Exchan	ges with	Encry	ption
-------	----	----	-------	---------	---------	--------	----------	-------	-------

STEP	REO	Action	Component	Description	n	Proc	edure	
1	IR OOL	OBSERVE	CS DTSP	Status Deports or		View the periodic	Status Deports	
1	IIX-090	ODSERVE	CS DISK	Status Reports at	C		Status Reports	
			Inspect Log	being sent		from the UA		
2	IR-09b	VERIFY	CS Main	Control Message	<	Verify via the traff	fic sniffer log that	t
			Sniffer	MTU does not re	anire	segmentation does	not occur	
			Shiriter	sagmantation	quite	segmentation does	novocui	
				segmentation				
🦲 cs.main	.sniffer.2023.09.08-09	9.54.40.pcapng					- 🗆	
File Edit	View Go Capt	ure Analyze Statistics	s Telephony Wireless	Tools Help				
	🖲 📙 🛅 🗙 🛛	🔓 । ९ 👄 🔿 🗟 👔	👃 📃 🗏 🔍 Q (₹.₩				
udp.port	== 51101							
No.	Time	Source	Destination	Protocol Length	Info			
793	75 402.337580106	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2 213	Client He	110		
798	39 402.781539095	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2 159	Client Ke	y Exchange		
799	92 402.781539223	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2 143	Change Ci	pher Spec, Encrypted Handsh	nake Message	
800	01 403.144295163	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2 108	Applicati	on Data		
94	78 486.266207646	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2 110	Applicati	on Data		
118	+7 400.114052407 21 576 734578977	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSV1.2 100	Applicati	on Data		
1220	0 507 041102007	fd@@.bbcc.ddo@	fd00.bbcc.ddo0.if	DTI 5/1 2 110	Applicati	on Data		
<								
> Frame #	8001: 108 bytes	on wire (864 bits),	, 108 bytes captured	(864 bits) on interface	0000 4	5 00 00 6c 6d 00 40 00 ff	29 fa 3d 0a 1	
Raw pa	cket data				0010 0	a 14 00 02 60 0a 27 26 00 den nn nn nn nn nn nn nn	30 11 40 TO 0 00 00 0a fd 0	
> Intern	et Protocol Vers	ion 4, Src: 10.20.0	0.1, Dst: 10.20.0.2	0.bbcc.dde0.f	0030 d	d e0 00 00 00 00 00 00 00	00 00 0f d3 1	
0110	0 = Version	: 6		0.00000.0000.11	0040 0	0 30 46 b6 17 fe fd 00 01	00 00 00 00 0	
>	. 0000 0000		. = Traffic Class: @	x00 (DSCP: CS0, ECN: No	t 0050 b	580 33 0C C0 39 DT 53 5a f c4 3d 4a 1e 1a ad 7d 26	3C CD 5e ee t 8e b9 7d	
	. 1010 0010 0111	0010 1011 = Flow L	abel: 0xa272b					
Pay:	load Length: 48							
Next	t Header: UDP (1	.7)						
нор	Limit: 64	0.bbcc.dde0e						
Dest	tination Address	: fd00:bbcc:dde0::f						
Ƴ User Da	atagram Protocol	, Src Port: 54032,	Dst Port: 51101					
Sour	rce Port: 54032							
Dest	tination Port: 5	1101						
Leng	gth: 48							
[Che	cksum: 0x4606 [u acksum Status: II	nverified]						
[Sti	ream index: 621	inter if ieug						
> [Tir	nestamps]							
UDP	payload (40 byt	es)						
✓ Datagra	am Transport Lay	ver Security						
Y DTL	5v1.2 Record Lay	er: Application Dat	a Protocol: Applicat	ion Data				
	ersion: DTLS 1	2 (0xfefd)						
E	Epoch: 1	- (
2	equence Number:	1						

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

Length: 27 Encrypted Application Data: 80330cc039bf535a3ccb5eee6b4ee1bfc43d4a1e1aad7d268eb

STEP	REQ	Action	Component	D	escription			Procedure	
3	SER-09	VERIFY	UA and CS	Control	Message	Coi	npare th	e two sniffer logs to	
-	SER-11		Main	received	1 matches	ver	ifv the re	eceived Control Messa	αe
	SER-11		Su iffann	Cantural		VCI.	41		ge L-4
			Shifters	Control	Message se	ent nas	the same	e contents as the one ti	nat
				which in	ndicates the	was	s sent		
				message	e was accept	ted			
				as authe	entic				
📕 ua.n	nain.sniffer.2023.09.	08-09.50.59.pcapng		us uume				_	
File Fo	lit View Go (Capture Analyze	Statistics Telephony	Wireless To	ools Help				
	a 💿 📙 🖬 🕻	X 🖾 S ⇔ ⇔	± A 4 = =		TT				
udp.p	ort == 51101								
No.	Time	Source	Destination		Protocol	Length Info	1		
140.	8612 620 140923	089 fd00.bbcc.d	de0f fd00.bbcc	· dde0 · · a	DTI Sv1 2	237 Sen	ver Kev Fi	vchange	
	8614 620.140923	126 fd00:bbcc:d	de0::f fd00:bbcc	:dde0::a	DTI Sv1.2	93 Ser	ver Hello	Done	
	8617 620.172074	283 fd00:bbcc:d	de0::a fd00:bbcc	:dde0::f	DTLSv1.2	159 Cli	ent Key E	xchange	
	8619 620.172372	324 fd00:bbcc:d	de0::a fd00:bbcc	:dde0::f	DTLSv1.2	143 Cha	nge Cipher	r Spec, Encrypted Har	
	8657 620.533769	484 fd00:bbcc:d	de0::f fd00:bbco	:dde0::a	DTLSv1.2	143 Cha	nge Cipher	r Spec, Encrypted Har	
	8662 620.534909	488 fd00:bbcc:d	de0::a fd00:bbcc	::dde0::f	DTLSv1.2	108 App	lication [Data	
	8714 620.938628	597 fd00:bbcc:d	de0::f fd00:bbcc	:dde0::a	DTLSv1.2	109 App	lication [Data	
1	0552 703.643603	710 fd00:bbcc:d	de0::a fd00:bbcc	::dde0::f	DTLSv1.2	110 App	lication [Data	
1	0637 704.688272	858 fd00:bbcc:d	de0::a fd00:bbcc	::dde0::f	DTLSv1.2	108 App	lication [Data	
<									
Enam	e 8662 · 108 but	tes on wire (864	hits) 108 hytes	cantured (S	64 hits) on i	nterface tur	0000 45	00 00 5c 5d 00 40 0	
Raw	nacket data	103 011 WILE (004	DICS), 100 Dyces (capcarea (e	,04 DICS) 0/1 I	incernace cui	0010 0a	14 00 02 60 0a 27 2	
> Inte	rnet Protocol \	/ersion 4. Src:	10.20.0.1. Dst: 10	.20.0.2			0020 dd	e0 00 00 00 00 00 0	
✓ Inte	rnet Protocol \	/ersion 6, Src:	fd00:bbcc:dde0::a,	Dst: fd00:	bbcc:dde0::f		0030 dd	l e0 00 00 00 00 00 0	
0	110 = Vers	ion: 6	,				0040 00	1 30 2d b7 17 fe fd 0	
> .	0000 0000 .		= Traffic	Class: 0x0	0 (DSCP: CS0,	ECN: Not-EC	0050 1b	7 80 33 0C C0 39 DT 5	
	1010 0010 0	111 0010 1011 =	Flow Label: 0xa272	2b			0000 01		
P	ayload Length:	48							
N	ext Header: UDP	P (17)							
н	op Limit: 64								
S	ource Address:	fd00:bbcc:dde0:	:a						
D	estination Addr	ess: fd00:bbcc:	dde0::f						
✓ User	Datagram Proto	ocol, Src Port:	54032, Dst Port: 5	1101					
S	ource Port: 540	32							
D	estination Port	:: 51101							
L	ength: 48								
C	hecksum: 0x2db7	[unverified]							
Ļ	Checksum Status	: Unverified]							
Ļ	Stream index: 2	[6]							
× L	limestampsj	h							
V Doto	op payload (40	Lavan Socurity							
	TISV1 2 Pecoed	Laver: Applicat	ion Data Protocol:	Applicatio	n Data				
	Content Type:	Application Da	ton baca Prococol.	Applicatio	ar baca				
	Version: DTLS	1.2 (0xfefd)	(2)						
	Epoch: 1	((((((((()))))))))))))))))))))))))							
	Sequence Numb	er: 1							
	Length: 27								
	Encrypted App	lication Data:	80330cc039bf535a3cc	:b5eee6b4ee	1bfc43d4a1e1a	ad7d268eb97d			
		0 1 . 1							

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 Mai	n sniffer lo	g shows appli	cation data is en	crypted.						
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	CS Main sniffer log shows application data is encrypted.									

STEP	REQ	Action	Component	Description	Procedure						
1	IR-09b	OBSERVE	CS DTSR	Status Reports are	View the periodic Status Reports from						
			Inspect Log	being sent	the UA						
2	IR-09b	VERIFY	CS Main	Control Message <	Verify via the traffic sniffer log that:						
	IR-02		Sniffer	MTU does not	a) message segmentation does not						
				require	occur for messages < MTU						
				segmentation	b) Control Messages include unique						
					IP source and destination						
					addresses that uniquely identify						
	the UA and CS										
CS Mair	n Sniffer log	shows control	messages are no	ot segmented (length is	s 105).						

A.1.8 TP_CM_008 – Control Message Exchanges without Encryption

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.

	cs.main.sniffer.2023.08.23-16.54.55.pcapng								
Fil	e Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help								
π	udp.port == 51101								
No.	Time Source Destination Protocol Leno	ith Info							
	45640 2067.5564434 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2	104 Application Data							
	45642 2067.5445687 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2	106 Application Data							
	45645 2067.9024776 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2	105 Application Data							
<	F3303 3308 036366 1300.LL	101 1000000							
*	<pre>Frame 45645: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on inte Section number: 1 > Interface id: 1 (tun2) Encapsulation type: Raw IP (7) Arrival Time: Aug 23, 2023 15:29:24.431983056 Pacific Daylight Time [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1692829764.431983056 seconds [Time delta from previous captured frame: 0.076488834 seconds] [Time delta from previous displayed frame: 0.357908845 seconds] [Time since reference or first frame: 2067.902477613 seconds] Frame Number: 45645 Frame Length: 105 bytes (840 bits) Capture Length: 105 bytes (840 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: raw:ip:ipv6:udp:dtls:data] [Coloring Rule Name: UDP] [Coloring Rule String: udp]</pre>	0000 45 00 00 69 ff 0010 0a 14 00 02 60 0020 dd e0 00 00 00 0030 dd e0 00 00 00 0040 00 2d be bc 17 0050 18 09 04 00 11 0060 4d 489 f3 c9 11							
> > > > >	<pre>[Protocols in Trame: raw:lp:lpv6:udp:dtls:data] [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: 45543, Dst Port: 51101 '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: 4 Length: 24 Encrypted Application Data: 09040001618f8ed9fcb5e2d7e2efef4d4d89f3c997ca59 'Data (4 bytes) Data: 09040001 [Length: 4]</pre>								

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.

	udp.port == 51101								
No	. Time	Source	Destination	Protocol	Length	Info			
	9003 773.087642673	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	104	Application	Data		
	9006 773.089357449	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	105	Application	Data		
	15140 1004.4345410	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	104	Application	Data		
	15142 1004.4357019	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	105	Application	Data		
	15152 1004.7197434	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	106	Application	Data		
	Frame 9006: 105 bytes	on wire (840 hits)	105 bytes cantured (8	40 hits) on i	nterface	tun2 id 0	000	00 09 04 00 01	
ľ.	Raw packet data	on wire (040 bits),	105 bytes captarea (c	40 5103/ 01/ 1	incer ruce	cunz, 10 0			
~	Internet Protocol Vers	sion 4. Src: 10.20.0.	1. Dst: 10.20.0.2						
	0100 = Version	1: 4	-,						
	0101 = Header	Length: 20 bytes (5)							
	> Differentiated Serv	vices Field: 0x00 (DS	CP: CS0. ECN: Not-ECT)					
	Total Length: 105			/					
	Identification: 0xf	fa5 (65445)							
	> 010 = Flags:	0x2. Don't fragment							
	0 0000 0000 0000) = Fragment Offset:	0						
	Time to Live: 255		-						
	Protocol: IPv6 (41)								
	Header Checksum: Øx	679b [validation dis	abledl						
	[Header checksum st	atus: Unverified]	,						
	Source Address: 10.	20.0.1							
	Destination Address	: 10.20.0.2							
~	Internet Protocol Vers	sion 6, Src: fd00:bbc	c:dde0::a, Dst: fd00:	bbcc:dde0::f					
	0110 = Version	1: 6	·····, ·····						
	> 0000 0000		= Traffic Class: 0x0	0 (DSCP: CS0.	ECN: No	t-ECT)			
	1010 0011 0110	0001 1001 = Flow La	bel: 0xa3619	. (,					
	Pavload Length: 45								
	Next Header: UDP (1	.7)							
	Hop Limit: 64								
	Source Address: fd0	0:bbcc:dde0::a							
	Destination Address	: fd00:bbcc:dde0::f							
>	User Datagram Protocol	l, Src Port: 45543, D	st Port: 51101						
~	Datagram Transport Lay	ver Security							
	✓ DTLSv1.2 Record Lay	ver: Application Data	Protocol: Applicatio	n Data					
	Content Type: Ap	plication Data (23)							
	Version: DTLS 1.	2 (0xfefd)							
	Epoch: 1								
	Sequence Number:	4							
	Length: 24								
	Encrypted Applic	ation Data: 09040001	618f8ed9fcb5e2d7e2efe	f4d4d89f3c997	ca5910				
~	Data (4 bytes)								
	Data: 09040001								
	[Length: 4]								

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.

STE P	REQ	Action	Component	t Description			Procedure
1	IR-04	VERIFY	CS Main Sniffer	Verify that User Data is sent over the active link	Veri User CS v Con	fy via Data via the nectio	the traffic sniffer log that the Messages are only sent by the link supporting the active
udp.p	oort == 51102						
lo. 15	Time	Source 855911 fd00:bb	occ:dde0::a	Destination fd00:bbcc:dde0::f fd00:bbcc:dde0:.f	Protocol DTLSv1	.2	Lengt Info 225 Application Data
15 15 15	2930 7970.5 2935 7970.7 2967 7971.0	340795 fd00:bl 352021 fd00:bl 846989 fd00:bl	<pre>>cc:dde0::f >cc:dde0::f >cc:dde0::f</pre>	fd00:bbcc:dde0::a fd00:bbcc:dde0::a fd00:bbcc:dde0::f	DTLSv1 DTLSv1 DTLSv1	.2 .2 .2	716 Application Data 197 Application Data 225 Application Data
: > Fran Raw	ne 152935: : packet data	197 bytes on wi	re (1576 bits),	197 bytes captured	(1576	0000 0010	45 00 00 c5 49 36 40 00 0a 14 00 01 60 07 e7 ae
<pre>> Inte > Inte > User > Data</pre>	ernet Protoc ernet Protoc Datagram F agram Transp	col Version 4, 5 col Version 6, 5 Protocol, Src P port Layer Secu	Src: 10.20.0.2, Src: fd00:bbcc: ort: 51102, Dst rity	Dst: 10.20.0.1 dde0::f, Dst: fd00:b Port: 45687	bcc:dd	0020 0030 0040 0050 0060 0060	dd e0 00 00 00 00 00 00 00 dd e0 00 00 00 00 00 00 00 89 2e 10 17 fe fd 00 74 75 d7 2e 51 e5 9e f9 02 af ec fb 4b fd b1 ff 6e 33 06 40 eb 7b c8 8c
Messa 2	ages from th IR-04	e CS are sent fr VERIFY	om 10.20.0.2, v UA Main Sniffer	which is LTE. Verify that User Data is received over the active link	Veri User by th activ	fy via Data ne UA ve Cor	the traffic sniffer log that the Messages are only received via the link supporting the nuection
udp	.port == 51102	2					
No.	Time 18708 2375 18717 2376 18726 2376 18730 2376	Source .6387582 fd00: .0768821 fd00: .4365354 fd00: .6360755 fd00:	bbcc:dde0::a bbcc:dde0::a bbcc:dde0::f bbcc:dde0::f	Destination fd00:bbcc:dde0::f fd00:bbcc:dde0::f fd00:bbcc:dde0::a fd00:bbcc:dde0::a	Proto DTL DTL DTL DTL	ocol Sv1.2 Sv1.2 Sv1.2 Sv1.2 Sv1.2	Length Info 225 Application Data 688 Application Data 716 Application Data 197 Application Data
> Fra Rav > Int > Int	ame 18726: v packet da ternet Prot ternet Prot	716 bytes on wi ta ocol Version 4, ocol Version 6,	ire (5728 bits) , Src: 10.20.0. , Src: fd00:bbc	, 716 bytes capture 2, Dst: 10.20.0.1 :c:dde0::f, Dst: fd0	d (5728 0:bbcc:	bits) on interface tun2, id 0
Messa	ages receive	d by the UA ha	ve destination 1	0.20.0.1, which is LT	E.		
3	IR-08	OBSERVE	CS LMSF Console	View the status of all available links	lms lms	f f> s	tatus
4	IR-08	OBSERVE	UA LMSF Console	View the status of all available links	cs- lms	sh l f> s	msf status
5	IR-05	SEND	CS LMSF Console	Issue Switchover command for the desired alternate link	lms lms	f f> s	witch 1
2023	-08-24 1	8:07:56.27	9090 GMT IN	IFO Control	Out.c	pp:2	294
6	IR-06	OBSERVE	UA DTSR Live Log	Observe the Switchover and note the Switchover Time	Veri Swit	fy the chove	e start and end timestamps of the er.
7	IR-06	OBSERVE	CS DTSR Live Log	Observe the Switchover and note the Switchover Time	Veri the S	fy the Switch	e start and end timestamps of nover.

Final Test Report

STE	REQ	Action	Component	Description	Procedure
P 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	<pre>cs-sh lmsf lmsf> status secure Expected output: STATUS User: Y/1 Control: Y/1 <u>No</u> indication that the interruption was greater than TET</pre>
2023-0 userOu contro user p contro	8-24 18 t enabl lOut en lane: C l plane	:08:08.8279 ed: 1 abled: 1 ONNECTED : CONNECTEI	965 GMT INFC	Secure Link	Detailed Status:
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	<pre>lmsf lmsf> status secure Expected output: STATUS User: Y/1 Control: Y/1 No indication that the interruption was greater than TET</pre>
2023-0 userOu contro user p	8-24 18 t enabl lOut en lane: C	:08:17.8606 ed: 1 abled: 1 ONNECTED	522 GMT INFC	Secure Link	Detailed Status:
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

S	TE I D	REQ	Ac	tion	Component	t	Description		Procedure	
	P									
	udp.port ==	= 51102								
No.		Time		Source		Destina	ition	Protocol	Lengt Info	
	153765	7996.	8549922	fd00:bbc	c:dde0::a	fd00:	bbcc:dde0::f	DTLSv1.2	225 Application Data	a
	153782	7997.7	7454497	fd00:bbc	c:dde0::f	fd00:	bbcc:dde0::a	DTLSv1.2	197 Application Data	а
	153783	7997.	7519058	fd00:bbc	c:dde0::a	fd00:	bbcc:dde0::f	DTLSv1.2	688 Application Data	а
<										
\sim	Frame 15	3782:	197 byte	s on wire	(1576 bits)	, 197	bytes captured	(1576 bits)	on interface tun1, id	0
	Sectio	on num	ber: 1							
	> Inter	face i	d: 0 (tu	n1)						
	Encap	sulati	on type:	Raw IP (7)					
	Arriva	al Tim	e: Aug 24	4, 2023 1	1:08:02.5485	50339	Pacific Daylight	t Time		
	[Time	shift	for this	s packet:	0.00000000	secon	ds]			
	Epoch	Time:	16929004	482.54855	0339 seconds		-			
	[Time	delta	from pre	evious ca	ptured frame	: 0.13	0245917 seconds	1		
	[Time	delta	from pre	evious di	splayed fram	e: 0.8	90457517 second	s]		
	[Time	since	referen	ce or fir	st frame: 79	97.745	449746 seconds]	-		
	Frame	Numbe	r: 15378	2			-			
	Frame	Lengt	h: 197 by	vtes (157	6 bits)					
	Captu	re Len	gth: 197	bytes (1	576 bits)					
	[Frame	e is m	arked: Fa	alsel	,					
	Frame	e is i	gnored: H	Falsel						
	Prote	ocols	in frame	: raw:ip:	ipv6:udp:dtl	sl				
	Colo	ring R	ule Name	: UDP1		-				
	[Colo	ring R	ule Stri	ng: udpl						
	Raw pack	et dat	a	.0						
>	Internet	Proto	col Vers	ion 4. Sr	c: 10.10.0.2	, Dst:	10.10.0.1			
>	Internet	Proto	col Vers	ion 6, Sr	c: fd00:bbcc	:dde0:	:f, Dst: fd00:b	bcc:dde0::a		
>	User Dat	agram	Protocol	, Src Por	t: 51102, Ds	t Port	: 45687			
>	Datagram	Trans	port Lav	er Securi	ty					
Sou	arce addr	ess is	10.10.0.2	which is	the CS on SA	ATCO	M.			

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

c) addresses are unique across paths over networked A/G links and over point-to-point A/G links

ST	E REQ	Actio	on Component	Description	cription Procedure	
P U	dp.port == 51102					
No.	Time 19614 2405. 19624 2405. 19625 2405. 19625 2405. 19625 2405. Trame 19614: 7 Section num Interface i Encapsulati Arrival Tim [Time shift Epoch Time: [Time delta [Time delta [Time delta [Time since Frame Numbe Frame Lengt Capture Len [Frame is m [Frame is m [Frame is i [Protocols [Coloring R aw packet dat	S 3378456 f 8871169 f 88871169 f 8885858 f 16 bytes o ber: 1 d: 1 (tun1 on type: R e: Aug 24, for this 169290049 from prev from prev from prev from prev reference r: 19614 h: 716 byt gth: 716 byt gth: 716 byt gth: 716 b arked: Fal gnored: Fa in frame: ule Name: ule String	Source d00:bbcc:dde0::f d00:bbcc:dde0::f d00:bbcc:dde0::a on wire (5728 bits), 1) Raw IP (7) , 2023 11:08:10.7493 packet: 0.00000000 00.749388783 seconds /ious captured frame /ious displayed frame /ious displayed frame 240 ces (5728 bits) bytes (5728 bits) lse] alse] raw:ip:ipv6:udp:dtl UDP] g: udp]	Destination fd00:bbcc:dde0::a fd00:bbcc:dde0::f 716 bytes captured 88783 Pacific Daylig seconds] : 0.210649411 second e: 0.255732518 seconds s5.337845666 seconds	Protocol DTLSv1.2 DTLSv1.2 (5728 bits) (5728 bits) (s] ds]	Length Info 716 Application Data 197 Application Data 225 Application Data on interface tun1, id 1
> I > U Dest	nternet Proto nternet Proto ser Datagram atagram Trans ination addres	col Versio Protocol, s is 10.10.0	on 4, Src: 10.10.0.2 on 6, Src: fd00:bbcc Src Port: 51102, Ds Cacunity 0.1 which is the UA c	, DST: 10.10.0.1 :dde0::f, Dst: fd00: t Port: 45687 on SATCOM.	bbcc:dde0::a	
12	2 IR-20	VERIFY	UA DTSR Live Log and UA Main Sniffer	Verify the appropriate Control Messages were exchanged while maintaining not breaking the secure	Verify via th a) the Co approp Layer b) the sec (i.e., m header errors	he traffic sniffer logs that: ntrol Messages are the vriate messages for a Network Switchover ure connection is maintained tessages with a DTLS record are observed, and no DTLS are logged)

secure connection

2023-08-24 18:07:56.279071 GMT INFOControlOut.cpp:291Sent "SWITCHOVER_REQUEST.REQ 521" 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.REQ3" across secure connectionReceived "CONNECT.REQ3" over secure sessionSent "CONNECT.CNF4Accepted" across secure connection

STE P	REQ	Action	Component	Description	Procedure
2023-08-24 18:07:56.142660 G Received "SWITCHOVER_RE 2023-08-24 18:07:56.153734 G Successful switchover to LinkIr Name: Satellite01 Address: 10.1 Peer: 10.10.0.1 Status: Link Up			CS DTSR Live Log T INFO Contro UEST.REQ 5 T INFO LinkIn p: 1 Type: Satellite .0.2 Adapter: tun1	Verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection dIn.cpp:42 2 1" over secure secure fo.cpp:343	 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)
Sent "CC Received Sent "CC 14	DNNECT.R I "CONNE DNNECT.C IR-21	EQ 3 CT.REQ CNF 4 VERIFY	" across secure co 3 " over secure Accepted" across UA DTSR Live Log	onnection e session s secure connection 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.

	udp.port == 51101									
No		Time	Source	Destination	Protocol	Lengt Info				
	153634	7991.9559860	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	109 App]	lication	Data		
	153664	7993.1559191	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	109 App]	lication	Data		
	159530	8174.3251472	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	108 App]	lication	Data		
<										
× < >	Frame 15 Section Internet Encapy Arriva [Time Epoch [Time [Time [Time Frame Captur [Frame [Frame [Frame [Frame [Prota [Coloo] Raw pack Internet User Dat	3634: 109 byte on number: 1 face id: 0 (tu sulation type: al Time: Aug 2 shift for thi Time: 1692900 delta from pr delta from pr since referen Number: 15363 Length: 109 b re Length: 100 b re Le	s on wire (872 bits), n1) Raw IP (7) 4, 2023 11:07:56.7590 5 packet: 0.000000000 476.759086648 seconds evious captured frame evious displayed fram ce or first frame: 79 4 ytes (872 bits) bytes (872 bits) alse] False] : raw:ip:ipv6:udp:dtl : UDP] ng: udp] ion 4, Src: 10.10.0.2 ion 6, Src: fd00:bbcc . Src Port: 51101. DS	109 bytes captured 86648 Pacific Daylig seconds] 0 0000273303 second 0 000027300 second 0 000020000000000000000000000000000000	(872 bits) on nt Time s] ds]]	interface	tun1, i	d 0		
	USER Dat	agram Protocol	, SIC POIC: 51101, DS	C FUIL: 30435						

STE P	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.

	udp	udp.port == 51101								
No			Time	Source	Destination	Protocol	Length	Info		
		19190	2392.1246320	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	109	Application	Dat	
		24455	2573.5066450	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	110	Application	Dat	
<		24468	2573.5814338	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTI Sv1.2	108	Annlication	Dat	

Frame 19190: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface tun1, id 1
 Section number: 1
 > Interface id: 1 (tun1)

```
Encapsulation type: Raw IP (7)
  Arrival Time: Aug 24, 2023 11:07:57.536175173 Pacific Daylight Time
   [Time shift for this packet: 0.00000000 seconds]
   Epoch Time: 1692900477.536175173 seconds
   [Time delta from previous captured frame: 0.044663801 seconds]
   [Time delta from previous displayed frame: 0.557941330 seconds]
   [Time since reference or first frame: 2392.124632056 seconds]
   Frame Number: 19190
   Frame Length: 109 bytes (872 bits)
   Capture Length: 109 bytes (872 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: 10.10.0.2, Dst: 10.10.0.1

```
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dde0::a
```

```
> User Datagram Protocol, Src Port: 51101, Dst Port: 38435
```

```
> Datagram Transport Layer Security
```

16	IR-06	VERIFY	CS DTS Live Lo	R Verify the g 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 DTS	SR:				
2023-08 CS DTS	-24 18:07 R:	:56.977766 GN	AT INFO	SessionManager.cpp:477	SWITCH completed in 699 ms
2023-08	-24 18:07	:56.758932 GN	AT INFO	SessionManager.cpp:477	SWITCH completed in 616 ms

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					
Verifica	tion looks	the same as step	1 of TP_CM_0	09; 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					
Verifica	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	View the status of	cs-sh lmsf					
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					
1	IR-05	INVOKE	CS OS Console	"	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	<pre>cs-sh lmsf lmsf> status secure Expected output: STATUS User: Y/<id> Control: Y/<id> Indication that interruption was greater than TET</id></id></pre>					

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

Final Test Report

STEP	REQ	Action	Component	Description	Procedure
2023-09-06 19:55:02.831204 GN Secure Link Detailed Status: userOut enabled: 1 controlOut enabled: 1 user plane: CONNECTED control plane: CONNECTED		2.831204 GMT ed Status: 1 CCTED NECTED	,		
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	<pre>lmsf lmsf> status secure Expected output: STATUS User: Y/<id> Control: Y/<id> Indication that interruption was greater than TET</id></id></pre>
2023-09- Secure L userOut of controlO user plan control p	-06 19:55:1 ink Detaile enabled: 1 ut enabled: he: CONNE blane: CON	2.591624 GMT ed Status: 1 CCTED NECTED			
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 veri	ification ste	en looks the sam	ne as step 10 of '	TP CM 009: not rep	eating 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 veri	fication ster	p looks the same	e as step 11 of T	P CM 009: not repe	point-to-point A/G links eating 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: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	3
Switchover Innitiator Task: sent CONNECT_REQ over link 3	
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	3
Switchover Innitiator Task: sent CONNECT_REQ over link 1	
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	3
Switchover Innitiator Task: sent CONNECT_REQ over link 2	
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	3
Switchover Innitiator Task: sent CONNECT_REQ over link 3	
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	3
Switchover Innitiator Task: sent CONNECT_REQ over link 1	
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	3
Switchover Innitiator Task: sent CONNECT_REQ over link 2	
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	3
Switchover Innitiator Task: sent CONNECT_REQ over link 3	
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	3
Switchover Innitiator Task: sent CONNECT_REQ over link 1	
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	3
Switchover Innitiator Task: sent CONNECT REQ over link 2	
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	3
Switchover Innitiator Task: sent CONNECT REQ over link 3	
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	3
Switchover Innitiator Task: sent CONNECT REQ over link 1	
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	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	REO	Action	Component	Description		Procedure
ua.main	.sniffer.2023.09.06	-14.34.55.pcapng	Component	Description		Troccurre
File Edit	View Go Ca	pture Analyze S	tatistics Telephony Wire	less Tools Help		
	🛞 📙 🔚 🗙	🕞 🔍 👄 🖦 I	🕾 🕢 I 📃 🔳 🕀	e e II		
	- E1101	• • •		•••		
	51101	-		D 1 1	1 11 T.C.	
No.	1 Ime	Source	Destination	Protocol	Length Info	**
2600	5 1189 724377	4 fd00:bbcc:dde	eo::a fd00:bbcc:dde	0::T DILSV1.2	100 Application Da	ta ta
2615	1 1192.765799	1 fd00:bbcc:dde	0::a fd00:bbcc:dde	0::f DTLSv1.2	108 Application Da	ta
2615	7 1193.168312	3 10.20.0.2	10.20.0.1	ICMP	136 Destination un	reachable (Port unreachable)
2617	7 1195.811371	6… fd00:bbcc:dde	0::a fd00:bbcc:dde	0::f DTLSv1.2	108 Application Da	ta
2628	7 1198.851130	7… fd00:bbcc:dde	e0::a fd00:bbcc:dde	0::f DTLSv1.2	108 Application Da	ta
2633	7 1201.927293	9… fd00:bbcc:dde	0::a fd00:bbcc:dde	0::f DTLSv1.2	108 Application Da	ta
2639	3 1202.294001	8 10.20.0.2	10.20.0.1	ICMP	136 Destination un	reachable (Port unreachable)
2646	3 1204.968135	5 fd00:bbcc:dde	e0::a fd00:bbcc:dde	0::f DTLSv1.2	108 Application Da	ta
2648	7 1208.027849 5 1211 080512	8… Td00:bbcc:dde	e0::a Td00:bbcc:dde	0::T DILSV1.2	108 Application Da	ta +>
2659	2 1211.009312	1 fd00:bbcc:dde	0f fd00.bbcc.dde	0a DTLSV1.2	100 Application Da	ta
2826	6 1277.018047	6 fd00:bbcc:dde	0::a fd00:bbcc:dde	0::f DTLSv1.2	110 Application Da	ta
2829	2 1278.062682	1 fd00:bbcc:dde	e0::a fd00:bbcc:dde	0::f DTLSv1.2	108 Application Da	ta
2832	3 1279.876524	7… fd00:bbcc:dde	e0::f fd00:bbcc:dde	0::a DTLSv1.2	109 Application Da	ta
3215	2 1437.492166	9… fd00:bbcc:dde	e0::a fd00:bbcc:dde	0::f DTLSv1.2	108 Application Da	ta
<						
Ƴ Frame 2	26151: 108 byt	es on wire (864	bits), 108 bytes capt	ured (864 bits) on	interface to 0000 45 0	00 00 6c d9 bf 40 00 ff 29 8
Sect	ion number: 1				0010 0a 1	14 00 02 60 0d d2 e6 00 30 1
> Inte	rface id: 1 (tun2)			0020 dd e	
Enca	psulation typ	e: Raw IP (7)			0040 00	30 2d b7 17 fe fd 00 01 00 0
Arri	val Time: Sep	6, 2023 12:54	:52.255277120 Pacific	Daylight Time	0050 1b d	:3 1a 0e 92 b3 b3 4d 78 46 d
[1m	e shitt for t	nis packet: 0.00	seconds		0060 c5 c	17 f2 80 19 11 19 16 c0 6c 1
[Tim	n fille. 10940 Ne delta from	previous canture	ed frame: -0 04228093	seconds]		
ſTim	e delta from	previous display	/ed frame: 3.041421783	seconds]		
[Tim	e since refer	ence or first fi	rame: 1192.765799186 s	econds]		
Fram	e Number: 261	51		-		
Fram	e Length: 108	bytes (864 bits	5)			
Capt	ure Length: 1	08 bytes (864 b:	its)			
[Fra	me is marked:	False]				
[Fra	me is ignored	: Falsej	ude.d+1e1			
[[[0]	oring Pule Na	me: raw:ip:ipvo: me: IDD]	acisj			
[Co1	oring Rule St	ring: udpl				
Raw pac	ket data					
> Interne	t Protocol Ve	rsion 4, Src: 10	0.20.0.1, Dst: 10.20.0	0.2		
> Interne	et Protocol Ve	rsion 6, Src: f	d00:bbcc:dde0::a, Dst	fd00:bbcc:dde0::f		
> User Da	tagram Protoc	ol, Src Port: 5	7810, Dst Port: 51101			
> Datagra	m Transport L	ayer Security				
16	IR-20	VERIFY	CS DTSR	Verify the	Verify via live	e log that:
			Live Log	appropriate	a) the Contr	ol Messages are the

16	IR-20	VERIFY	CS DTSR	Verify the	Ve	rify via live log that:
			Live Log	appropriate	a)	the Control Messages are the
				Control Messages		appropriate messages for a Network
				were exchanged		Layer Switchover based on the
				while maintaining		messages
				not breaking the	b)	the secure connection is maintained
				secure connection		(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 3 CONTROL PLANE: CONNECT.REQ 3 Processing suceeded. 3 CONTROL PLANE: CONNECT.REQ 3 Processing suceeded. 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		on C	ompone	ent D	Description				Procedure						
	cs.main	.sniffer.202	3.09.06-14.35	.45.pcapng											
Fi	e Edit	View G	o Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help						
		•	🗟 🗙 🔂	ې 🗢 🖻	» ≊ 👔	& ■		Q. 🎹							
	udp.port	== 51101					-								
_		Time	Source	ce		Destination		Protoc	col	Length	Info				
	22965	1144.433	3162 fd00	:bbcc:dde	:0::a	fd00:bbcc	:dde0::f	DTLS	v1.2	1	08 App	licati	Lon	Data	1
	23007	1146.387	1420 fd00	bbcc:dde:	e0::a	fd00:bbcc	:dde0::f	DTLS	v1.2	1	08 App	licati	Lon	Data	1
	23008	1146.387	1686 10.2	20.0.2		10.20.0.1		ICMP		1	36 Des	tinati	Lon	unre	achal
	23069	1149.531	9225 10.3	30.0.2	0	10.30.0.1	. dd. Q f	ICMP	4.0	1	50 Des	tinati	Lon	unre	achal
	230/6	1149.531	9014 TOOU 2243 - Edoo):bbcc:dde	20::a	fd00:bbcc	:dde0::T	DTLS	V1.2	1	08 App 08 App	licati	Lon	Data	
	23130	1155.546	2243 1000 9247 fd00):bbcc:dde	0::a	fd00:bbcc	:dde0::f	DTLS	v1.2	1	08 App 08 App	licati	Lon	Data	
	23225	1155.546	9676 10.2	20.0.2		10.20.0.1		ICMP		1	36 Des	tinati	ion	unre	achal
	23356	1159.600	8086 10.3	30.0.2		10.30.0.1		ICMP		1	50 Des	tinati	Lon	unre	achal
	23359	1159.600	7030 fd00	bbcc:dde):bbcc:dde	e0::a	fd00:bbcc	:dde0::f	DTLS	v1.2	1	08 App	licati	ion	Data	1
	23416	1162.042	4587 fd00):bbcc:dde	e0::a	fd00:bbcc	:dde0::f	DTLS	v1.2	1	08 App	licati	Lon	Data	
	23418	1162.042	4868. 10.1 0112 fd00	l0.0.2		10.10.0.1	uddo@uuf	DTLS	U1 0	1	50 Des	tinati licoti	Lon	Unre	achat
	23462	1164.713	9115 Tube 8708 fd00	hbcc:dde	-0::f	fd00:bbcc	:dde0::a	DTLS	v1.2	1	00 App 09 Ann	licati	ion	Data	
	24876	1230.624	8111 fd00):bbcc:dde	:0::a	fd00:bbcc	:dde0::f	DTLS	v1.2	1	10 App	licati	Lon	Data	
r.															
,	Ename (3007.10	8 hytes or	wire (80	54 hite)	108 byte	s canture	1 (864	hite)	on inte	0000	45.0	0 0	0 6c	d9 h
	Sect	tion numb	er: 1	1 WIIC (0	JA DICS)	, 100 bycc	s captare	4 (004	DICS	on ince	0010	0a 1	40	0 02	60 0
	> Inte	erface id	: 2 (tun2))							0020	dd e	0 0	0 00	00 0
	Enca	apsulatio	n type: Ra	aw IP (7)							0030	dd e	00	0 00 d 1-	00 0
	Anni	ival Time	: Sep 6,	2023 12:5	54:52.42	2426110 Pa	cific Dayl	light T	ime		0050	1b c	31	a Øe	92 b
	[Tin	ne shift	for this p	oacket: 0.	.0000000	00 seconds]				0060	c5 d	7 f	2 80	19 1
	Epoc	ch Time:	1694030092	2.42242611	L0 second	ls 0.0014									
[Time delta from previous captured frame: 0.201496985 seconds]															
[Time delta from previous displayed frame: 1.953825825 seconds] [Time since reference or first frame: 1146 387142035 seconds]															
	Frame Number: 23007														
	Fran	ne Length	: 108 byte	es (864 bi	its)										
	Capt	ture Leng	th: 108 by	/tes (864	bits)										
	[Fra	ame is ma	rked: Fals	se]											
[Frame is ignored: False]															
[Protocols in frame: raw:ip:ipv6:udp:dtis]															
	[Co]	loring Ru	le String:	udpl											
	Raw pa	cket data													
>	Interne	et Protoc	ol Version	n 4, Src:	10.20.0	.1, Dst: 1	0.20.0.2								
>	Interne	et Protoc	ol Versior	n 6, Src:	fd00:bb	cc:dde0::a	, Dst: fd	00:bbcc	:dde0:	::f					
2	User Da	atagram P	rotocol, 9	Src Port:	57810, 1	Ost Port:	51101								
2	Datagra	am Iransp	ort Layer	Security											
				_											
	17	IR-21	VERIFY	ť U.	A Main	Veri	y User Da	ata V	/erify	via the t	ratific	sniffer	log	g tha	t:
Snifter and Control a) User Data and Control a)							and Co	ontrol	Me	ssag	es				
						Mess	ages are		be	gin to be	excha	inged	ove	er the	e new
						excn	anged ove	i d h	L11	uk messar	as flow	1 01/0*	the	orio	inal
						stop	over the o	ld D	lin	hessage k	-5 1100		une	ong	mai

link

The verification for this step looks the same as step 15 from TP_CM_009; not repeating for conciseness.
REQ	Action	Component	Description	Procedure
IR-21	VERIFY	CS Main	Verify User Data	Verify via the traffic sniffer log that:
		Sniffer	and Control	a) User Data and Control Messages
			Messages are	begin to be exchanged over the new
			exchanged over	Link
			the new link and	b) no messages flow over the original
			stop over the old	link
			link	
fication for	this step looks	the same as step	16 from TP_CM_0	09; not repeating for conciseness.
IR-06	VERIFY	CS DTSR	Verify the	Verify the Switchover time is greater
		Live Logs	Switchover Time	than TET for a Scheduled MbB
			is greater than the	Switchover
			TET for a	
			Scheduled MbB	
			Switchover	
R:				
	REQ IR-21 fication for IR-06	REQActionIR-21VERIFYfication for this step looksIR-06VERIFY	REQActionComponentIR-21VERIFYCS Main SnifferSnifferSnifferfication for this step looks the same as step IR-06VERIFYCS DTSR Live Logs	REQActionComponentDescriptionIR-21VERIFYCS MainVerify User DataSnifferand ControlMessages areexchanged overthe new link andstop over the oldlinklinkfication for this step looks the same as step16 from TP_CM_0IR-06VERIFYCS DTSRVerify theLive LogsSwitchover Timeis greater than theTET for aScheduled MbBSwitchover

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 Us	Jser Plane Traffic Link Terminat	tion
-----------------------------------------	----------------------------------	------

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	<pre>lmsf lmsf> status secure Expected output: STATUS User: Y/<id> Control: Y/<id></id></id></pre>			
2023-08	8-24 18	15:02.8805	90 GMT Secui	re Link Detail	ed Status:			
userOut control user pl control	c enable Out ena ane: Co plane	ed: 1 abled: 1 DNNECTED : CONNECTED						
2	IR-07	VERIFY	UA LMSF console	UA status shows: secure session is established which link is providing the	<pre>cs-sh lmsf lmsf> status secure Expected output: STATUS User: Y/<id> Control + Y/(ID> </id></pre>			
connection 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</id>								
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			

STE	P I	REQ A	ction	Componer	nt Description		Procedure
📕 uc	dp.port =:	= 51102					
No.		Time	Source		Destination	Protocol	Lengt Info
	164930	8354.9033019	fd00:bbc	c:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	197 Application Data
	164935	8355.2507989	fd00:bbc	c:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	225 Application Data
	164944	8355.6915448	fd00:bbc	c:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	200 Application Data
	164945	8355.6923926	fd00:bbc	c:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	228 Application Data
	164951	8355.9039894	fd00:bbc	c:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	197 Application Data
Y F	rame 16	4945: 228 byte	es on wire	e (1824 bits)	, 228 bytes captured	(1824 bits)	on interface tun2, id 1
	Secti	on number: 1					
>	Inter	face id: 1 (tu	in2)				
	Encap	sulation type:	Raw IP (7)			
	Arriv	al Time: Aug 2	4, 2023 1	1:14:00.4954	93267 Pacific Daylig	ght Time	
	[Time	shift for thi	s packet:	0.00000000	seconds]		
	Epoch	Time: 1692900	840.49549	3267 seconds			
	[Time	delta from pr	evious ca	ptured frame	: 0.000847823 second	ls]	
	[Time	delta from pr	evious di	splayed fram	e: 0.000847823 secor	ids]	
	[Time	since referen	ice or fir	st frame: 83	55.692392674 seconds	;]	
	Frame	Number: 16494	5			-	
	Frame	Length: 228 b	ytes (182	4 bits)			
	Captu	re Length: 228	bytes (1	824 bits)			
	[Fram	e is marked: F	alse]				
	[Fram	e is ignored:	False]				
	[Prot	ocols in frame	: raw:ip:	ipv6:udp:dtl	s]		
	[Colo	ring Rule Name	UDP1				
	[Colo	ring Rule Stri	.ng: udp]				
R	aw pack	et data	0 13				
> 1	nternet	Protocol Vers	ion 4, Sr	c: 10.20.0.2	, Dst: 10.20.0.1		
> 1	nternet	Protocol Vers	ion 6, Sr	c: fd00:bbcc	:dde0::f, Dst: fd00	bbcc:dde0::a	
> 0	ser Dat	agram Protocol	, Src Por	t: 51102, Ds	t Port: 45687		
> D	atagram	Transport Lay	ver Securi	tv			
				1			

Source 10.20.0.2 is the CS on LTE

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

STEP	REQ	Action	Componer	nt Description		Procedure
udp.por	t == 51102					
No.	Time	Source	0	Destination F	Protocol Length	Info
294	441 2754.63	23237 fd00:bbc	c:dde0::f f	d00:bbcc:dde0::a	TLSv1.2 716	Application Data
294	446 2754.79	18463 fd00:bbc	c:dde0::f f	fd00:bbcc:dde0::a [DTLSv1.2 197	Application Data
294	448 2754.79	26903 fd00:bbc	c:dde0::a f	fd00:bbcc:dde0::f [0TLSv1.2 225	Application Data
294	456 2755.20	00159… fd00:bbc	c:dde0::a f	fd00:bbcc:dde0::f	DTLSv1.2 200	Application Data
294	464 2755.55	67013 fd00:bbc	c:dde0::f f	fd00:bbcc:dde0::a [DTLSv1.2 228	Application Data
294	472 2755.78	88555 fd00:bbc	c:dde0::f f	fd00:bbcc:dde0::a [TLSv1.2 197	Application Data
<		Clock L				11 11 51
✓ Frame See > Int End Arti [T: Epd [T: [T: [T: [T: Fra Fra Cap [Fra [Fra [Fra [Fra [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fra] [Fr	29446: 197 ction numbe terface id: capsulation rival Time: ime shift f poch Time: 1 ime delta f ime delta f ime delta f ime since r ame Number: ame Length rame is mar rame is ign rotocols in ploring Rul acket data net Protoco Datagram Pr	7 bytes on wire r: 1 0 (tun2) 1 type: Raw IP (Aug 24, 2023 1 for this packet: .692900840.20338 from previous dai rom previous di reference or fir 29446 197 bytes (157 th: 197 bytes (157 th: 19	<pre>(1576 bits), : 7) 1:14:00.203385 0.00000000 s 9510 seconds ptured frame: splayed frame: st frame: 2754 6 bits) 576 bits) ipv6:udp:dtls] c: 10.20.0.2, c: fd00:bbcc:ct t: 51102. Dst</pre>	<pre>197 bytes captured (1) 9510 Pacific Daylight seconds] 0.000071824 seconds] 4.791846393 seconds] Dst: 10.20.0.1 dde0::f, Dst: fd00:bbb Port: 45687</pre>	576 bits) on inter Time] cc:dde0::a	face tun2, id 0
Destinati 5	on address IR-11	10.20.0.1 is UA SEND	A on LTE. CS LMSF	Terminate the secure Control Plane traffic and User Plane traffic	lmsf>secu	re stop
6	IR-07 IR-11	VERIFY	CS LMSF console	connection CS status shows <u>no</u> secure connection for User Plane traffic or Control Plane	lmsf lmsf> stat c Expected outp STATUS Use	cus secure ut: er: N/ <id> </id>
2023-0 userOu contro	8-24 18 t enabl lOut en	:15:23.6482 ed: 0 abled: 0	267 GMT IN	traffic FO Secure L	Control: 1 ink Detailed	N/ <id> Status:</id>
user p	⊥ane: N	. NOT CONNECTE				
contro	⊥ p⊥ane	: NOT CONNE	LCTED	·		-
7	IR-07 IR-11	VERIFY	UA LMSF console	UA status shows <u>no</u> secure connection for User Plane traffic or Control Plane traffic	cs-sh Imsf lmsf> stat c Expected outp STATUS Use Control: 1	ut: ut: er: N/ <id> N/<id></id></id>
2023-0	8-24 18	:15:32.3079)58 GMT Se	cure Link Deta	iled Status:	
userOu	t enabl	ed: 0				
contro	10ut en	abled. O				
		ANTECH. V	רי			
contro	Lane: N	• NOT CONNECTE				
contro	⊥ p⊥ane	. NOT CONNE	UC I ED			

STEP	REQ	Action	Component	Description	n	Procedure
8	IR-04	SEND	UA UDMD	Send User Dat	ta (cs-sh udmd
			Console		I	udmd> send n=1 at 11:15
						PDT
9		VERIFY	UA User	UDMD sent a	.]	From the traffic sniffer, verify the User
			Sniffer	User Data]	Data message is sent from the UDMD
				message to DTSR	1	to the DTSR
Apply	a display filter «	<ctrl-></ctrl->				
No.	Time	Source	Destinati	ion	Protocol	Lengt Info
	3008 1132.024	6077 10.100.0.1	10.100	.0.2	UDP	548 39980 → 55447 Len=520
Ŀ.	3009 1132.460	2272 10.100.0.1	10.100	.0.2	UDP	91 45821 → 55444 Len=63
	3010 1133.024	8095 10.100.0.1	10.100	.0.2	UDP	60 39980 → 55447 Len=32
Ƴ Fram	e 3009: 91 by	tes on wire (728	bits), 91 bytes	captured (728 l	bits) o	n interface tun18, id 0
S	ection number	.: 1				
> 1	nterface id:	0 (tun18)				
E	ncapsulation	type: Raw IP (7)				
A	rrival Time:	Aug 24, 2023 11:	15:41.066441501 P	acific Daylight	t Time	
10	IR-04	VERIFY	UA Main	User Data and	l '	Verify via the traffic sniffer log that
	IR-11		Sniffer	Control	1	User Data and Control messages are
				Messages are	not 1	not sent by UA
				transmitted by	7	
				the UA DTSR	_	
2023-	-08-24 18	:15:41.0665	31 GMT INFO	UdmdIr	n.cpp	:51
Rece	ived: ID:	00000014 0	rigin: UDMD	Cmd: SEND	Size	: 63 Rsp: FALSE Data:
UD-AA	АААААААА	АААААААААА-	000014			-
Secui	re sessio	n disabled	- ID: 000000)14 Origin	: UDM	ID Cmd: SEND Size: 63 Rsp:
FALSE	E not sen	t to peer t	o lmsf queue	9		L
		1				
11	IR-04	VERIFY	CS Main	User Data and	l '	Verify via the traffic sniffer log that the
	IR-11		Sniffer	Control	1	User Data and Control messages were
				Messages are	not i	not received
				received by C	S	
				DTSR		

STEP REQ A			EQ Ac	Action Component Description						P	roce	dure	e					
(, u	dp.port ==	= 51101															
	No. Time Source Destination Protoco								Protocol		Leng	t Info						
1		159563	8175.0461908	fd00:bbc	c:dde0::a	fd@	0:bbcc:dde0::	f	DTLSv1	.2	10	9 Арр	lica	tio	n Da	ata		
1	L	167338	8431.8503511	fd00:bbc	c:dde0::a	fde	0:bbcc:dde0::	f	DTLSv1	.2	10	8 App	lica	tio	n Da	ata		
1		178806	9092.4116864	fd00:bbc	c:dde0::a	fd0	0:bbcc:dde0::	f	DTLSv1	.2	18	1 Cli	ent	Hel	lo			
1		178889	9096.5820597	fd00:bbc	c:dde0::a	fd0	0:bbcc:dde0::	f	DTLSv1	.2	18	1 Cli	ent	Hel	lo			
L		178890 9096.5822334… fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv						DTLSv1	.2	12	8 Hel	lo V	eri	fy I	Requ	uest	:	
L		178905	9096.9402166	fd00:bbc	c:dde0::a	fde	0:bbcc:dde0::	f	DTLSv1	.2	21	3 Cli	ent	Hel	lo			
L		178906	9096 9403233	fd00.hhr	c.dde0f	fdø	0. hhcc.dde0.	a	DTI Sv1	2	17	9 Ser	ver	Hel'	10			
ŀ	<																	
Γ	∽ F	rame 16	7338: 108 byte	s on wire	e (864 bits), 108	8 bytes captur	ed (864 bi	0000	45	00 00) 6c	ce	b5	40	00	ff
L		Sectio	on number: 1							0010	0a	14 00	02	60	0b	fb	d1	96
L	3	> Inter	face id: 1 (tu	n2)						0020	dd	e0 00	00	00	00	00	00	00
1	Encapsulation type: Raw IP (7)									0030	dd	e0 00	00	00	60 4-	60 4 J	00	00
	Arrival Time: Aug 24, 2023 11:15:16.653451760 Pacific Daylight Tim								t Time	0040	16	1d h	: aT / 10	1/ 5h	те hd	TO d5	00 02	br
l	[Time shift for this packet: 0.000000000 seconds]									0050	70	e7 a6	35	9h	e6	e1	5f	a1

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.

	udp.port == 51102											
No.		Time	Source	Destination	Protocol		Lengt	Info				
	167320	8431.8069070	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1	.2	200	App1:	icat	ion [Data	1
L	167321	8431.8076929	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1	.2	228	App1:	icat	lon [Data	1
	178941	9098.0920842	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1	.2	181	Clie	nt He	ello		
	179019	9102.2306968	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1	.2	181	Clie	nt He	2 11 0		
<												
~	Frame 16	7321: 228 byte	s on wire (1824 bits	s), 228 bytes captured	(1824	0000	45 0	0 00	e4 3	5 cb	40	00
	Secti	on number: 1				0010	0a 1	4 00	01 6	0 07	e7	ae
	> Inter	face id: 1 (tu	n2)			0020	dd e	0 00	00 0	0 00	00	00
	Encap	sulation type:	Raw TP (7)			0030	dd e	0 00	00 0	0 00	00	00
	Anning] Times Ave 24, 2022 44:45:46 (10702560 Desifie Devilient Time						00 a	8 2e	2f 1	.7 fe	fd	00
	ALLIN	ar Time: Aug 24	4, 2023 11:15:10.010	0/95500 Pacific Daylign	ic ilme	0050	93 7	5 d7	2e 5	1 e5	9e	fd

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	·15·16 664	1426 GMT INF	0 ImsfIn c	nn•129
Recei Forwa to co Secur Sent Disab	ved ID: rding II ntrol_pl e Stop r "USER_DI ling sec	00000016 (0: 00000016 ane seceived fr SCONNECT.F	Drigin: LMSF 5 Origin: LM com LMSF - n REQ 3 on	Cmd: SECURE S SF Cmd: SECURE otifying peer " across secur	ize: 40 Rsp: FALSE Arg: 0 Size: 40 Rsp: FALSE Arg: 0 e connection
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	8-24 18:1	5:16.6536	21 GMT INFO		
Receive	ed "USER_	DISCONNEC'	T.REQ 3	" over secure	session
Disabl	ing secur	e 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	CS status shows secure session is established on C-Band	lmsf lmsf> status secure
			Log		Expected output: STATUS User: Y/3 Control: Y/3
2023-09 userOut control user pl control	-08 15: enable Out ena ane: CC plane	01:42.65550 ed: 1 abled: 1 DNNECTED : CONNECTED	9 GMT S	ecure Link Detail	ed Status:
3	1	INVOKE	UA and CS LMSF Consoles	Change TET to surface/departure /arrival value	<pre>lmsf> set_tet 3 cs-sh lmsf lmsf> set tet 3</pre>
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

STE	Р	RE	Q	A	Actio	n	Comp	onen	t	De	scri	ption			Proce	dure
🧲 cs.n	nain.sr	hiffer.2	023.09.0)8-09.5	54.40.p	ocapng										
File	Edit	View	Go	Captu	ure A	Analyze	Statistic	s Te	lephony	Wii	reless	Tools	Help			
		0	010	🗙 🕻	<u></u>	(() 🗟 👔	<u>.</u>		Ð	Q	Q. 🎹				
udp.	port =	= 5110	12													
	Tir	ne		Sou	urce			Destin	nation			Protoc	ol	Length	Info	
95	60 48	38.648	309938	1 fd@	00:bb	cc:dde@)::f	fd00	:bbcc:	dde0:	:a	DTLS	1.2	20	8 Applica	tion Data
96	20 49	0.514	450674	7 fd	00:bb	cc:dde@)::a	fd00	:bbcc:o	dde0:	:f	DTLS	1.2	23	6 Applica	tion Data
96	21 49	0.648	387489	8 fd0	00:bb	cc:dde@)::f	fd00	:bbcc:c	dde0:	:a	DTLS	1.2	19	7 Applica	tion Data
<				• •												
✓ Fra	me 90 Secti Inter Encap Arriv [Time Epoch [Time Frame Captu [Fram [Fram [Fram [Fram [Fram [Fram [Fram [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold [Cold	521: : 521: : face face sulat val T: shith Time control control to to to to to to to to to to	197 by imber: id: 0 tion t ime: S ft for ta fro ta	rtes (1 (turype: ep { this impre- impre- impre- ierend 621 .97 by 197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197 .197	on wi n3) Raw 8, 20 s pac 371.6 eviou eviou ce or ytes byte alse] False : raw : UDP ng: u	<pre>re (15) IP (7) 23 08:0 ket: 0. 1808739 s captu s displ first (1576 k s (1576] :ip:ipv] dp]</pre>	<pre>/6 bits /2:51.6 .000000 /6 seco ured fr layed f frame: /its) /6:udp:</pre>), 19 18087 000 s nds ame: rame: 490. dtls]	7 byte: 396 Pac econds 0.13436 0.1343 6488748	cific] 58151 866815 5998 s	: Day . sec 1 se econ	d (1570 light 1 onds] conds] ds]	5 bits) Time	on int	erface tur	13, id 0
✓ Int	ernet	t Prot	tocol	Vers:	ion 4	, Src:	10.30.	0.2,	Dst: 10	0.30.	0.1					
				0.00	• •			a b								

Ipv4 address shows 10.30.0.2 which indicates C-Band. VERIFY

Sniffer

5 IR-04	
---------	--

User Data is received UA Main 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	Componen	t Description	Procedure
🚄 ua.maii	in.sniffer.2023.0	9.08-09.50.59.pcapr	ng		
File Edit	t View Go	Capture Analy	ze Statistics Te	ephony Wireless Tools	Help
	1 🔘 📘 💼	🗙 🖸 🤇 🗢	🔿 🗟 🚹 🕹	📑 🖲 २, २, 🖽	
udp.por	rt == 51102				
No.	Time	Source	De	estination Prote	ocol Length Info
100	681 707.3741	70929 fd00:bbc	c:dde0::f fo	100:bbcc:dde0::a DTL	Sv1.2 208 Application Data
100	686 707.3749	81460 fd00:bbc	c:dde0::a fo	100:bbcc:dde0::f DTL	Sv1.2 236 Application Data
< 100	693 708.1849	11851 #d00:bbc	c:dde0::a to	100:bbcc:dde0::f DTL	Sv1.2 688 Application Data
✓ Frame	10681: 208	bytes on wire	(1664 bits), 2	08 bytes captured (1664	bits) on interface tun3, id 0
Sec	ction number	·: 1	(,, -		,
> Int	terface id:	0 (tun3)			
End	capsulation	type: Raw IP (7)		
An	rival Time:	Sep 8, 2023 0	8:02:50.752798	215 Pacific Daylight Ti	me
LT:	ime shift fo	or this packet:	0.000000000 s	econdsj	
сро Гт-	ime delta fr	000 previous ca	ozio seconds ntured frame: 4	1,933648193 seconds]	
[T	ime delta fr	om previous di	splayed frame:	1.189271251 seconds]	
[Т	ime since re	ference or fir	st frame: 707.	374170929 seconds]	
Fra	ame Number:	10681		-	
Fra	ame Length:	208 bytes (166	4 bits)		
Cap	pture Length	n: 208 bytes (1	.664 bits)		
[Fi	rame is mark	(ed: False]			
[Fi	rame is igno	fored: Falsej	invConderd+1-1		
[P]	oloring Pule	Trame: raw:1p: Name: UDD]	ipv6:uap:atisj		
[CC	oloring Rule	String: udpl			
Raw p	acket data				
> Inter	net Protocol	l Version 4, Sr	c: 10.30.0.2,	Dst: 10.30.0.1	
pv4 add	dress shows	10.30.0.2 whic	h indicates C-I	Band.	
6		WAIT	Pilot	Perform takeoff,	Per Test Card
				navigate aircraft to	C-
				Band coverage area	l
				Northwest of Build	ing
7		MONITOR	Skyline	Monitor the C-Ban	d Monitor the C-Band signal
			-	signal	strength via Skyline
8		INVOKE	UA and CS	Once at cruise, cha	nge lmsf> set tet 5
·			LMSF	TET to cruise value	e (5 cs-sh lmsf
			Consoles	seconds)	` lmsf> set tet 5
9		WAIT	Pilot	Pilot navigates out	of Maneuvers drone to southeas
-				C-Band coverage	of building
10		MONITOR	Skyline	Monitor the C-Ran	d Monitor the C-Band signal st
			Skyllic	signal	via Skyline
10				Sigilai	via Skynne
10		OBSEDVE	Skyling	Once aircraft is	Monitor the DSSI of the C D
11		OBSERVE	Skyline	Once aircraft is	Monitor the RSSI of the C-B
11		OBSERVE	Skyline	Once aircraft is directly above the	Monitor the RSSI of the C-B connection via the Skyline G
11		OBSERVE	Skyline	Once aircraft is directly above the GRS, observe the	Monitor the RSSI of the C-B connection via the Skyline G noting the lowest RSSI occur the south side of build
11		OBSERVE	Skyline	Once aircraft is directly above the GRS, observe the RSSI of C-Band	Monitor the RSSI of the C-B connection via the Skyline G noting the lowest RSSI occur the south side of building
11		OBSERVE	Skyline	Once aircraft is directly above the GRS, observe the RSSI of C-Band connection has	Monitor the RSSI of the C-B connection via the Skyline G noting the lowest RSSI occur the south side of building

STEP REQ Action Component Description Procedure 12 IR-05 VERIFY CS LMSF CS status shows: lmsf ...secure session is lmsf> status secure IR-07 Console and IR-10 DTSR Live established Expected output: Log ... that the link has STATUS User: Y/2 | changed to the LTE ... that the secure Control: Y/2 connection is maintained following No indication that the interruption the interruption was greater than TET ... the CS DTSR did not indicate an interruption exceeding 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. cs.main.sniffer.2023.09.08-09.54.40.pcapng File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help ◢ ■ ∅ ⑧ 📙 🗟 🕱 🗳 ۹ ⇔ ⇔ 🕾 🗿 🛃 🚍 ۹ ۹ ۹ ۹ 🏨 dp.port == 51101 Time No. Source Destination Protocol Length Info 109 Application Data 13580 648.174909146 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2 108 Application Data 14484 681.752463738 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2 14487 681.753330703 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2 109 Application Data AFOTOTES FLOOLLESS JLOOLS DTLC...1 < Frame 14484: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface tun2, id 2 Section number: 1 > Interface id: 2 (tun2) Encapsulation type: Raw IP (7) Arrival Time: Sep 8, 2023 08:06:02.721676236 Pacific Daylight Time [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1694185562.721676236 seconds [Time delta from previous captured frame: 0.017725084 seconds] [Time delta from previous displayed frame: 33.577554592 seconds] [Time since reference or first frame: 681.752463738 seconds] Frame Number: 14484 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 0100 Manada and A

STEP	REQ	Action	Component	Description	Procedure
13	IR-05 IR-07 IR-10	VERIFY	UA LMSF Console and DTSR Live	CS status shows: secure session is established	lmsf lmsf> status secure
			Log	that the link has changed to the LTE that the secure	Expected output: STATUS User: Y/2 Control: Y/2
				maintained following the interruption the CS DTSR did	\underline{No} indication that the interruption was greater than TET
				interruption exceeding TET	
2023-09 switch Initiat	-08 15: command	06:01.49001 L. st-link swit	6 GMT Lost	link for secure	connection. Sending
CONTROL sent CO	PLANE: NNECT_F	>[080300]C EQ over lin	CONNECT.REQ	3	
CONTROL Receive	PLANE: d CONNE	CONNECT.CN CT.CNF.	IF 4 Accept	ted[09040001]<<<	2000 mg
Control	nlane	messages ch	ange inv4 a	address from C-Ba	nd to LTE and messages
remain	on same	port 51101		luaress from c-ba.	na co hill, and messages
dua.main.	sniffer.2023. View Go	09.08-09.50.59.pcapn	ig Statistics Telev	nhony Wireless Tools He	ln
The Lun					h.

á		1	9 📙 🔚 🗙 🕻	🕽 🍳 🗢 🗢 🗟 🗿 🕗	<u> </u>							
	udp.	udp.port == 51101										
N	o.		Time	Source	Destination	Protocol	Length	Info				
		14405	865.980158676	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	109	Application	Data			
		15083	899.156949318	fd00:bbcc:dde0::a	fd00:bbcc:dde0::f	DTLSv1.2	108	Application	Data			
		15108	899.528980857	fd00:bbcc:dde0::f	fd00:bbcc:dde0::a	DTLSv1.2	109	Application	Data			
<												
				1 (000 111)				. 0000	45 00			

~	Frame 15083: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface tur	0000	45 00
	Section number: 1	0010	0a 14
	> Interface id: 1 (tun2)	0020	dd e0
	Encapsulation type: Raw IP (7)	0030	dd e0
	Arrival Time: Sep 8, 2023 08:06:02.535576604 Pacific Daylight Time	0040	16 00
	[Time shift for this packet: 0.000000000 seconds]	0050	10 80
	Epoch Time: 1694185562.535576604 seconds	0000	10 52
	[Time delta from previous captured frame: -0.000474275 seconds]		
	[Time delta from previous displayed frame: 33.126790642 seconds]		
	[Time since reference or first frame: 899.156949318 seconds]		
	Frame Number: 15083		
	Frame Length: 108 bytes (864 bits)		
	Canture Length: 108 butes (864 bits)		
	[Forme is marked: Folse]		
	[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		
-			

STEP	REO	Action	Component	Descrip	otion		Procedure	e
14	IR-04	VERIFY	CS Main Sniffer	ain User Data is sent over r the active link (LTE)		Verify via that the Us only sent to supporting	the traffic si ser Data Mes to the UA via g the active Q	niffer log ssages are a the link Connection
User pl	ane mes	sages chan	ge from C-B	and to LTH	E IP add	resses.	2	
🚄 cs.main.s	niffer.2023.0	9.08-09.54.40.pcapn	9					
File Edit	View Go	Capture Analy	ze Statistics Tele	phony Wireless	Tools Help)		
	۱	े 🔀 🖸 । ९ 🗢	🔿 🕾 🗿 🕹 📑		Q. 🎹			
udp.port	== 51102							
1	ïme	Source	Destinat	ion	Protocol	Length	Info	
14452 6	81.297665	216 fd00:bbcc:d	de0::a fd00:b	bcc:dde0::f	DTLSv1.2	200	Application	Data
14453 6	81.297683	626 10.30.0.2	10.30.	.0.1	ICMP	228	Destination	unreachab.
14534 6	82.738399	789 fd00:bbcc:d	de0::f fd00:b	bcc:dde0::a	DTLSv1.2	192	Application	Data
<								
Frame : Sect Sect Enca Arri [Tin Epoc [Tin [Tin [Tin Fram Capt	(4534: 192 ion numbe rface id: upsulation val Time: he shift fr the shift fr the delta f he delta f he since r he Number: he Length: ture Length:	bytes on wire r: 1 2 (tun2) type: Raw IP (Sep 8, 2023 0 or this packet: 694185563.70761 rom previous ca rom previous di eference or fir 14534 192 bytes (153 h: 192 bytes (1	(1536 bits), 19, 8:06:03.70761228 0.00000000 sec 2287 seconds ptured frame: -0 splayed frame: 1 st frame: 682.73 6 bits) 536 bits)	2 bytes captur 37 Pacific Day 50nds] 0.071142248 se 0.440716163 se 08399789 secon	ed (1536 bi light Time conds] conds] ds]	ts) on inte	rrace tun2,	10 2
[Fra [Fra [Pro [Co] [Co] Raw pao V Interne	ame is mar ame is ign otocols in loring Rul loring Rul cket data et Protoco	ked: False] ored: False] frame: raw:ip: e Name: UDP] e String: udp] l Version 4, Sr	ipv6:udp:dtls] c: 10.20.0.2, D:	st: 10.20.0.1				
15	IR-04	VERIFY	UA Main Sniffer	User Data is over the activ (LTE)	received ve link	Verify via that the Us only recei supporting	the traffic si ser Data Mes ved via the li g the active C	niffer log ssages are ink Connection

S	ТЕР	R	EQ	Ac	tion	Componer	nt	Description	on		Pr	ocedu	re	
Us	er <mark>ua.m</mark>	plane nain.sniff	e mes <mark>er.2023.0</mark>	sages) <mark>9.08-09.</mark>	change 50.59.pcapng	e from C I	-Band	to LTE	IP add	resses	3.			
File	e Ed	lit Viev	w Go	Captur	e Analyze	Statistics	Telephony	Wireless	Tools H	elp				
		60	010	🗙 🖸	ء 🗢) 😤 🖗 🖉		େଇ୍େ ୍ େ	1 🏛					
	udp.p	ort == 51	1102											
No.		Tir	ne	5	Source		Destinatio	ı	Protoc	ol	Length	Info		
	1	5046 89	8.2015	04260 1	fd00:bbcc:	dde0::a	fd00:bb	cc:dde0::f	DTLS	/1.2	200	Appli	cation	Data
	1	5133 90 5165 90	0.2020	40849 1 00248 1	d00:bbcc:	dde0::a dde0::f	fd00:bb	cc:dde0::t	DTLS	/1.2	688	Appli	cation	Data
<	1	5105 50	0.5270	00240 1	000.00000.	0000.11	1000.00		DIES	/1.2	192	Арртт	cación	Data
~	Sime Sime Sime Sime Sime Sime Sime Sime	e 1513: ection nterfac ncapsul rrival Time sh poch Ti Time de Time de Time de Time si rame Nu rame Le apture Frame i Protocco Colorir Colorir	s: 688 number te id: lation Time: nift fo ime: 16 elta fr elta fr ince re umber: ength: Length is mark is igno ols in ng Rule ng Rule	bytes : 1 1 (tun? type: F Sep 8 r this 9418556 om prev om prev ference 15133 688 byt : 688 byt :	on wire (5 2) Raw IP (7) , 2023 08: packet: 0 53.5806681 vious capt vious disp e or first tes (5504 bytes (550 lse] alse] raw:ip:ip UDP] g: udp]	06:03.5806 0.000000000 35 seconds ured frame layed frame frame: 90 bits) 4 bits) v6:udp:dtl	688 byt 68135 Pa seconds :: 0.3012 e: 2.000 0.202040	es capture cific Dayl:] 12200 secon 536589 second: 849 second:	a (5504 ight Timo nds] onds] s]	e	Interf	ace t	0000 0010 0020 0040 0050 0050 0050 0050 0050 005	45 00 0a 14 dd e0 02 74 5f 33 19 ab b0 c8 03 7e 62 14 96 9f 8c 4c e2 14 96 9f 8c 4c ee e1 a0 c8 83 64 c7 fb 55 28 57 cc
>	Raw Inte	packet rnet Pi	data rotocol	Versi	on 4, Src:	10.20.0.1	, Dst: 1	0.20.0.2					0140 0150 0160	2b 06 f6 a5 47 Af
	16			WAIT	- ']	Pilot	Pilo to la west	t navigates nding area t side of bu	aircraft on ilding	Per Tes	st Card		0100	47 01
	17			MONI	TOR	Skyline	Mor C-B	C-Band co itor the inc and signal	verage	Monito strengtl	r the C- h via Sk	Band vline	signal	
	18	IR	-08	OBSE	RVE	CS LMSF Console	Stati the o alter avai	us indicatio current link nate links a lable	ons for and are	Lmsf lmsf> lmsf> lmsf> Expector Link Link Link	stat stat stat ed Resu 1 Up 2 Up 3 Up	us 1 us 2 us 3 lts:		
	19	IF	R-05	SEND		CS LMSF Console	Whi Swi to C	le cruising, chover cor -Band	, issue nmand	lmsf lmsf>	swite	ch 3		

STEP REQ Component Description Action Procedure 20 IR-05 VERIFY UA LMSF UA status shows: cs-sh lmsf lmsf> status secure IR-07 Console and ... secure session is IR-10 DTSR Live established ... that the link has Expected output: Log changed to C-Band STATUS User: Y/3 | ... that the secure Control: Y/3 connection is maintained following No indication that the interruption the interruption was greater than TET ... the UA DTSR did not indicate an interruption exceeding 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 21 IR-05 VERIFY CS LMSF CS status shows: lmsf IR-07 ... secure session is lmsf> status secure Console and IR-10 DTSR Live established Expected output: Log ... that the link has STATUS User: Y/3 | changed to C-Band Control: Y/3 ... that the secure connection is maintained following No indication that the interruption the interruption was greater than TET ... the CS DTSR did not indicate an interruption exceeding 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 22 WAIT Pilot Pilot begins descent Per Test Card and lands the aircraft 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 24	n for this s IR-04 IR-18 IR-19c	step is the same a VERIFY	s Step 14 where UA Main Sniffer	e the ip addresses are union For all switchovers, verify that: messages are exchanged over the active link addresses are unique	 que after each switchover. 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
25	I for this s	tep 1s identical to	UA DTSR Live Log	the ip addresses are unic For all switchovers, verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	 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	Componen	t Des	cription		Pr	ocedu	re	
Contro	l plane	e messages c	hange ipv	4 address	from	C-Band	to LTE,	and	no n	ew
DTLS h	andshał	kes are requ	ired.							
🚄 ua.mai	n.sniffer.202	3.09.08-09.50.59.pca	ong							
File Edit	View G	o Capture Analy	ze Statistics	Telephony Wir	eless Too	ols Help				
	•	🛅 🔀 🔄 <	🔿 😤 🚹 🕗	2 📃 📃 🔍	Q Q 1					
udp.port	== 51101									
No.	Time	Source		Destination		Protocol	Length	Info		
144	05 865.98	0158676 fd00:bbc	c:dde0::f	fd00:bbcc:dd	:0::a	DTLSv1.2	109	Appli	cation	Data
150	83 899.15	6949318 fd00:bbc	c:dde0::a	fd00:bbcc:dd	20::f	DTLSv1.2	108	Appli	cation	Data
151	08 899.52	8980857 fd00:bbc	c:dde0::f	fd00:bbcc:dd	:0::a	DTLSv1.2	109	Appli	cation	Data
<pre>> Frame Sec > Int Enc Arr [Ti Epo [Ti [Ti [Ti Fra Fra Cap [Fr [Fr [Co [Co Raw pa > Intern</pre>	15083: 10 tion numb erface id apsulatio ival Time me shift ch Time: me delta me delta me delta me since me Number me Length ture Leng ame is ma ame is ig otocols i loring Ru loring Ru loring Ru cket data et Protoc	<pre>18 bytes on wire er: 1 : 1 (tun2) n type: Raw IP (: Sep 8, 2023 G for this packet: 1694185562.53557 from previous ca from previous da reference or fir : 15083 : 108 bytes (864 th: 108 bytes (864 th: 108 bytes (864 th</pre>	(864 bits), : (7) 0.000000000 6604 seconds ptured frame: splayed frame: st frame: 899 bits) 664 bits) ipv6:udp:dtls c: 10.20.0.1 c: fd00:bbcc	108 bytes cap 76604 Pacific seconds] : -0.00047427 2: 33.1767906 0.156949318 so 5] 5] , Dst: 10.20. :dde0::a, Dst	Dayligh 5 second 42 secon 2conds] 0.2 : fd00:b	364 bits) o t Time ls] lds]	n interface	e tur	0000 0010 0020 0030 0040 0050 0060	45 00 0a 14 dd e0 00 30 1b 80 1b 52
26	IR-20	VERIFY	CS DTSR	For all sw	vitchover	rs, Vei	rify via the	live lo	g that:	

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)

STE	P	REQ	Action	Component	Descript	tion	Procedure
CS.I	main.si	niffer.2023.0	9.08-09.54.40.pcapng				
File	Edit	View Go	Capture Analyze	Statistics Telepho	ny Wireless Too	ols Help	
			• 🗷 🖬 🤇 🤍 •	⇒ ≃ r ⊻ _	_ ચ્ચ્ચ	£	
	p.port =	= 51101	-				
No.	1358	Time 2 648 174	Source 909146 fd00:bbcc:	dde0f fd00.l	tion bbcc:dde0::a	Protocol DTL Sv1 2	Length Info
	1448	4 681.752	463738 fd00:bbcc:	dde0::a fd00:l	bbcc:dde0::f	DTLSv1.2	108 Application Data
	1448	7 681.753	330703 fd00:bbcc:	dde0::f fd00:	bcc:dde0::a	DTLSv1.2	109 Application Data
<	1545	705 450	707757 £300.66	11-0.1- £100.1		DTI C. 1 D	110 41: 0
Y Fr	ame 1	4484: 108	bytes on wire (8	364 bits), 108 by	tes captured (8	64 bits) o	n interface tun2, id 2
	Sect	ion numbe	r: 1				
>	Inte	rface id:	2 (tun2)				
	Arri	val Time:	Sep 8, 2023 08:	06:02.721676236	Pacific Daylight	t Time	
	[Time	e shift f	or this packet: 0	.000000000 secon	ds]		
	Epoc	h Time: 1	694185562.7216762	36 seconds			
	Tim	e delta f e delta f	rom previous capt rom previous disr	ured trame: 0.01	7725084 seconds] ds]	
	[Tim	e since r	eference or first	frame: 681.7524	63738 seconds]	1	
	Fram	e Number:	14484				
	Frame	e Length:	108 bytes (864 b	oits)			
	[Frai	me is mar	ked: False]	(DICS)			
	[Frai	me is ign	ored: False]				
	[Pro	tocols in	<pre>frame: raw:ip:ip</pre>	v6:udp:dtls]			
		oring Rul	e Name: UDPj e String: udpl				
Ra	w pac	ket data	e string, dobl				
⊻ In	terne	t Protoco	l Version 4, Src:	10.20.0.1, Dst:	10.20.0.2		
Cont	rol	plane	messages c	hange ipv4	address fr	om C-Ba	nd to LTE, and no new
DTLS	ha ba	ndshak	es are requ	ired.			
27		IR-21	VERIFY	UA Main	For all switch	overs,	Verify via the traffic sniffer lo
				Sniffer	verify User D	ata and	that:
					Control Messa	ages are	a) User Data and Control
					exchanged ov	er the	Messages begin to be
					new link and s	stop over	exchanged over the new L
					the old link		b) no messages flow over the
c	1	1 1		6.4 1	. 1.		original link
Same	log	theck as	step 25, where no	one of the applic	ation data mess	ages are a	ddressed to the old link.
28		IK-21	VERIFY	CS Main	For all switch	overs,	verify via the traffic shifter log
				Shifter	Control Mose		ulai:
					control Messa	ages are	a) User Data and Control Massages bagin to be
					exchanged ov	er the	exchanged over the new L
					the old link	stop over	b) no messages flow over the
							original link
Same	امع د	heck as s	ten 26 where no	ne of the applica	tion data messa	ages are a	dressed to the old link
20111C 29	1050	IR-06	VERIFY	UA and CS	For all switch	overs	Verify the Switchover time is
		00	*	DTSR Live	verify the Swi	tchover	than TET for a Scheduled Mbl
				Logs	Time is less th	nan the	Switchover
				0-	TET for a Sch	eduled	
					MbB Switcho	ver	
CS E	TSR	:					
SWII	CH	comple	ted in 1368	ms. Switc	hover TET	set at	5000 ms.
		-					
UA D	TSR	:					
SWII	CH	comple	ted in 1783	ms. Switc	hover 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	Change TET to	lmsf> set_tet 3
			LMSF	surface/departure	cs-sh lmsf
			Consoles	/arrival value	lmsf> set_tet 3
2	IR-05	VERIFY	UA LMSF	UA status shows:	cs-sh lmsf
	IR-07		Console	secure session is	lmsf> status secure
				established	
				that the link has been	Expected output:
				re-established	STATUS User: Y/3
					Control: Y/3
3	IR-05	VERIFY	CS LMSF	CS status shows:	lmsf
	IR-07		Console	secure session is	lmsf> status secure
				established	
				that the link has been	Expected output:
				re-established	STATUS User: Y/3
					Control: Y/3
4	IR-05	SEND	UA LMSF	Issue Switchover	cs-sh lmsf
			Console	command for the desired	lmsf> switch 2
				link (LTE)	
5	IR-05	VERIFY	UA LMSF	UA status shows:	cs-sh lmsf
	IR-07		Console	secure session is	lmsf> status secure
				established	
				that the link has been	Expected output:
				re-established	STATUS User: Y/2
					Control: Y/2
6	IR-05	VERIFY	CS LMSF	CS status shows:	lmsf
	IR-07		Console	secure session is	lmsf> status secure
				established	
				that the link has been	Expected output:
				re-established	STATUS User: Y/2
_					Control: Y/2
7	IR-04	VERIFY	CS Main	User Data is sent over	Verify via the traffic sniffer log that
			Sniffer	the active link; User	the User Data Messages are only
				Data is received over the	sent & received via the link
				active link (LTE)	supporting the active Connection
8	IR-04	VERIFY	UA Main	User Data is received	Verify via the traffic sniffer log that
			Sniffer	over the active link;	the User Data Messages are only
				User Data is sent over	received via the link supporting the
0			D ¹	the active link (LTE)	active Connection
9		WAIT	Pilot	Pilot initiates the takeoff	Per Test Card
10		INVOKE	CS US	while taking off,	disable_link l
			Console	simulate active link	disable_link 3
				(L I E) is lost and other	UISADIE_IINK Z
				links are unavailable	
11		WATT	CS	Wait at least 2 second-	Wait 2 geoonds
11		WALL	Operator	for TET to pass	wan 5 seconds
			Operator	TOT TET TO Pass	

STEP	REO	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
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	Control: Y/2 lmsf lmsf> status secure Expected output: STATUS User: Y/2 Control: Y/2
15 16	IR-08	OBSERVE WAIT	UA LMSF Console Pilot	Status indication that TET has been exceeded Aircraft reaches cruising	Observe TET exceeded notification
17		INVOKE	UA and CS	altitude Change TET to cruise	lmsf> set_tet 5
18		INVOKE	LMSF Consoles CS OS Console	value While cruising, simulate active link (LTE) is lost and other links are	<pre>cs-sh lmsf lmsf> set_tet 5 disable_link 2</pre>
19		WAIT	CS Operator	Wait at least 5 seconds	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
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	Control: Y/2 lmsf lmsf> status secure Expected output: STATUS User: Y/2 Control: Y/2
23	IR-08	OBSERVE	UA LMSF	Status indication that	Observe TET exceeded notification
24		INVOKE	CS OS Console	Enable Satcom and C- Band	enable_link 1 enable_link 3

			-		
STEP 25	REQ IR-08	Action OBSERVE	Component CS LMSF Console	Description Status indications for the current link and alternate links are available	ProcedureLmsflmsf> status 1lmsf> status 2lmsf> 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	cs-sh lmsf lmsf> status secure
				that the link has been re-established on C- Band	Expected output: STATUS User: Y/3 Control: Y/3
28	IR-05	VERIFY	CS LMSF	CS status shows:	lmsf
20	IR-07		Console	secure session is established	lmsf> status secure
				that the link has been re-established on C-	Expected output: STATUS User: Y/3
29		INVOKE	CS OS Console	Simulate the previously active link is available again. (This could take	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	<u>No</u> 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	UA status shows: secure session is established	cs-sh lmsf lmsf> status secure
			Log	that the link has changed to the specified link that the secure	Expected output: STATUS User: Y/2 Control: Y/2
				connection is maintained following the interruption the UA DTSR did not	<u>No</u> indication that the interruption was greater than TET
				Indicate an interruption exceeding TET	

STEP	REO	Action	Component	Description	Procedure
34	IR-05	VERIFY	CS LMSF	CS status shows:	lmsf
-	IR-07 IR-10		Console and DTSR Live	secure session is established	lmsf> status secure
			Log	that the link has	Expected output:
			8	changed to the specified	STATUS User: Y/2
				link that the secure	Control: Y/2
				connection is	No indication that the interruption
				maintained following the interruption	was greater than TET
				the CS DTSR did not indicate an interruption	
	ID 04			exceeding TET	
35	IR-04	VERIFY	CS Main Sniffer	User Data is sent over the active link; User	Verify via the traffic sniffer log that the User Data Messages are only
				Data is received over the	sent & received via the link
36	IR-04	VERIFY	UA Main	User Data is received	Verify via the traffic sniffer log that
			Sniffer	over the active link; User Data is sent over	the User Data Messages are only received via the link supporting the
				the active link (LTE)	active Connection
37		INVOKE	CS OS Console	While cruising, simulate backup links satcom and	disable_link 1 disable link 3
			Compose	C-Band are lost.	_
38		WAIT	Pilot	Pilot begins descent	Radio pilot to begin descent
20		INWOKE	UA and CS	phase Change TET to	lmsf> set tet 3
39		INVOKE	LMSF	approach value, 3	cs-sh lmsf
40		NUOVE	Consoles	seconds	<pre>lmsf> set_tet 3 disable link 2</pre>
40		INVOKE	CS US Console	simulate active link	disable_link 2
			combole	(LTE) is lost and other	
			~~	links are unavailable	
41		WAIT	CS Operator	Wait to exceed TET	Wait 3 seconds
42		INVOKE	CS OS	While in descent,	enable_link 2
			Console	simulate the previously	
				and other links are	
				unavailable. (This could	
13	ID 05	VEDIEV	IIA I MSE	take several seconds)	cs-sh lmsf
43	IR-05 IR-07	VENIT I	Console	secure session is	lmsf> status secure
				that the link has been	Expected output:
				re-established	STATUS User: Y/2
44	IR-05	VERIEY	CS LMSF	CS status shows.	Control: Y/2 lmsf
с т	IR-07		Console	secure session is	lmsf> status secure
				that the link has been	Expected output:
				re-established	STATUS User: Y/2 Control: Y/2
45	IR-08	OBSERVE	UA LMSF	Status indication that	Observe TET exceeded notification
	00		Console	TET is exceeded	when LTE was down

Final Test Report

OTER	DEO	A	C (D	
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	VERIFY	UA LMSF	UA status shows:	cs-sh lmsf
	IR-07		Console	secure session is established	lmsf> status secure
				that the link has been	Expected output:
				re-established on LTE	STATUS User: Y/2
					Control: Y/2
51	IR-05	VERIFY	CS LMSF	CS status shows:	lmsf
	IR-07		Console	secure session is established	lmsf> status secure
				that the link has been	Expected output:
				re-established on LTE	STATUS User: Y/ <id> Control: Y/<id></id></id>
52	IR-08	OBSERVE	UA LMSF Console	Status indication that TET is exceeded	Observe TET exceeded notification when LTE was down
Post-flig	ght analys	is			
53	IR-04	VERIFY	CS Main	For every switchover,	Verify via the traffic sniffer log that:
	IR-18		Sniffer	verify that:	a) User Data and Control
	IR-19c			messages flow over	messages are exchanged over
	IR-21			the new link	the new Link (the active connection)
				over the original link addresses are unique	b) no messages flow over the original link
				L	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	Change TET to	lmsf> set_tet 3
			LMSF	surface/departure	cs-sh lmsf
2	ID 05		Consoles	/arrival value	Imsi> set_tet 3
2	IK-05 IR-07	VERIFY	UA LMSF Consolo	UA status shows:	CS-SH IMSI
	IK-07		Collisole	established	Inst/ Status Secure
				that the link has	Expected output:
				been re-established	STATUS User: Y/3 Control:
					Ү/З
3	IR-05	VERIFY	CS LMSF	CS status shows:	lmsf
	IR-07		Console	secure session is	lmsf> status secure
				established	Expected output:
				been re-established	STATUS User: Y/3 Control:
				been re-established	Y/3
4	IR-05	SEND	UA LMSF	Issue Switchover	cs-sh lmsf
			Console	command for the	lmsf> switch 2
				desired link (LTE)	
5	IR-05	VERIFY	UA LMSF	UA status shows:	cs-sh lmsf
	IR-07		Console	secure session is	Imsi> status secure
				that the link has	Expected output:
				been re-established	STATUS User: Y/2 Control:
					Y/2
6	IR-05	VERIFY	CS LMSF	CS status shows:	lmsf
	IR-07		Console	secure session is	lmsf> status secure
				established	
				that the link has	Expected output:
				been re-established	Y/2
7		WAIT	Pilot	Initiate Takeoff	Per Test Card
8	IR-05	SEND	UA LMSF	While the aircraft is	cs-sh lmsf
			Console	climbing, switch	lmsf> switch 1
0	ID 05			from LTE to satcom	as sh lmaf
9	IK-05 IR-07	VERIFY	UA LMSF Console	UA status shows:	CS-SH IMSI lmsf> status secure
	IK-07		Collisole	established	insi/ Status Sceure
				that the link has	Expected output:
				been re-established	STATUS User: Y/1 Control:
					Y/1
10	IR-05	VERIFY	CS LMSF	CS status shows:	lmsf
	IR-07		Console	secure session is	Imsi> status secure
				that the link has	Expected output:
				been re-established	STATUS User: Y/1 Control:
					Y/1
11	IR-05	SEND	UA LMSF	While the aircraft is	cs-sh lmsf
			Console	climbing, switch	lmsf> switch 3
				trom satcom to C-	
12	IR_05	VEDIEV	IIA I MSE	Band UA status shows:	cs-sh lmsf
12	IR-05 IR-07	V LIXIT I	Console	secure session is	lmsf> status secure
			20110010	established	
				that the link has	Expected output:
				been re-established	STATUS User: Y/3 Control:
					Y/3

STEP	REO	Action	Component	Description	Procedure
13	IR-05	VERIFY	CS LMSF	CS status shows:	lmsf
	IR-07		Console	secure session is established that the link has been re-established	<pre>lmsf> status secure Expected output: STATUS User: Y/3 Control: Y/3</pre>
14	IR-08	OBSER VE	CS LMSF Console	View the status of all available links	<pre>175 lmsf lmsf> Status 1 Status 2 Status 3</pre>
					Expected output Link 1 Up Link 2 Up Link 3 Up
15	IR-08	OBSER VE	UA LMSF Console	Issue command "status" to view the status of all	cs-sh lmsf lmsf> Status 1 Status 2
				available links	Status 3 Expected output Link 1 Up Link 2 Up Link 3 Up
16		WAIT	Pilot	Aircraft reaches	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	<pre>cs-sh lmsf lmsf> status secure Expected output: STATUS User: Y/3 Control: y/3</pre>
20	IR-05 IR-07	VERIFY	CS LMSF Console	CS status shows: secure session is established that the link has	Insf Imsf> status secure Expected output:
				been re-established	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	<pre>cs-sh lmsf lmsf> status secure Expected output: STATUS User: Y/1 Control: Y/1</pre>
25	IR-05 IR-07	VERIFY	CS LMSF Console	CS status shows: secure session is established that the link has been re-established	<pre>lmsf lmsf> status secure Expected output: STATUS User: Y/1 Control: y/1</pre>
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:
28	IR-05 IR-07	VERIFY	CS LMSF Console	CS status shows: secure session is established that the link has been re-established	<pre>Y/2 lmsf lmsf> status secure Expected output: STATUS User: Y/2 Control: </pre>
29	IR-08	OBSER VE	CS LMSF Console	View the status of all available links	<pre>1/2 lmsf lmsf> Status 1 Status 2 Status 3</pre>
					Expected output Link 1 Up Link 2 Up Link 3 Up

Use or disclosure of this data is subject to the restrictions on the title page of this document.

STEP	REO	Action	Component	Description	Procedure
30	IR-08	OBSER VE	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	<pre>lmsf> set_tet 3 cs-sh lmsf lmsf> set tet 3</pre>
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:
35	IR-05 IR-07	VERIFY	CS LMSF Console	CS status shows: secure session is established that the link has been re-established	<pre>Y/3 Imsf Imsf> status secure Expected output: STATUS User: Y/3 Control:</pre>
36	IR-05	SEND	UA LMSF Console	While the aircraft is descending, switch from C-Band to satcom	Y/3 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:
38	IR-05 IR-07	VERIFY	CS LMSF Console	CS status shows: secure session is established that the link has been re-established	Y/1 lmsf lmsf> status secure Expected output: STATUS User: Y/1 Control:
39	IR-05	SEND	UA LMSF Console	While descending, switch from satcom	Y/1 cs-sh lmsf lmsf> switch 2
40	IR-05 IR-07	VERIFY	UA LMSF Console	UA status shows: secure session is established	cs-sh lmsf lmsf> status secure
				that the link has been re-established	Expected output: STATUS User: Y/2 Control: Y/2

STED	DEU	Action	Component	Description	Drogoduro
41	IR-05	VERIEV	CSLMSF	CS status shows	lmsf
-11	IR-07	VERII I	Console	secure session is established	lmsf> status secure
				that the link has been re-established	Expected output: STATUS User: Y/2 Control: Y/2
42	IR-05	SEND	UA LMSF Console	While the aircraft is descending, switch	cs-sh lmsf lmsf> switch 1
43	IR-05 IR-07	VERIFY	UA LMSF Console	UA status shows: secure session is established	cs-sh lmsf lmsf> status secure
				that the link has been re-established	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	lmsf lmsf> status secure
				that the link has been re-established	Expected output: STATUS User: Y/1 Control: Y/1
45		WAIT	Pilot	Aircraft lands	Per Test Card
Post-flig	ht analysi	s			
46	IR-06	OBSER VE	UA DTSR Live Log	Observe the Switchover and note the Switchover	Verify the start and end timestamps of the Switchovers.
47	IR-06	OBSER VE	CS DTSR Live Log	Observe the Switchover and note the Switchover	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	<u>No</u> 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	<u>No</u> indications that the interruptions from switchovers were greater than TET
50	IR-04, IR-18 IR-19c	VERIFY	CS Main Sniffer	exceeding TET 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	REO	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.

	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	IP_CM_001A , Step 1
SER-08	The UAS C2 Link security system shall provide mutual peer entity authentication of C2 Control Plane traffic between the UA and CS.	64 bits or equivalent MOC.	1P_CM_001
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-	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.	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_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	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,	FIPS PUB. 198-1 with an authentication tag of at least 64 bits or equivalent MOC.	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	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.	MOC.	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-	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.	scale quantum computers, when available, will threaten the security of NIST-approved public key algorithms.	IP_CM_001A , Step 1

Table B 1 Seem	rity Doquiromont	with an INSDE	CTION or VEL	DIEV Tost Ston
Table B-1 – Secul	rity Requirements	S WITH AN INSPE	CITON OF VER	AIF Y Test Step

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 (<u>Certificate #3389</u>) 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.

Algorithm	Use	Characteristics	Relies on	NIST	NIST
_				Reference	CAVP
AES	Encryption/decryption	Key Sizes: 128, 192, 256 Modes:	DRBG	FIPS 197	<u>5446</u>
CVL (KAS)	Key agreement	<u>Curves</u> : P-256, P-384, P-521	ECDSA, DRBG, SHS	SP 800-56A	<u>1891</u>
DRBG	Random bit generation	SHA-256-based	SHS	SP 800-90A	<u>2131</u>
ECDSA	Key generation Key verification Signature generation Signature verification	<u>Curves</u> : P-256, P-384, P-521 <u>Hash</u> : SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHS, DRBG	FIPS 186-4	<u>1451</u>
KDF	Key Derivation Function	Mode: HMAC-based pseudo- random function (PRF) <u>Hash</u> : SHA-256 or SHA-384	HMAC, SHS	SP 800-56C	Note 1
HMAC	Message authentication code generation and verification	Mode: Hashed Message Authentication Code <u>Hash</u> : 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	<u>4365</u>
Note 1: The yendor (wolfSSI) affirms conformance of this function to NIST SP 800-56C. This KDF is approved					

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

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.

<pre>#!/bin/bash RC=0 WORKING_DIR="." OPTIONS="\enable-ipv6 \enable-fips=v2 \enable-opensslextra \enable-certgen \enable-certreq \enable-ccshamir \enable-eccshamir \enable-eccustcurves \enable-eccustcurves \enable-eccustcurves \enable-eccmcrypt \enable-aslas \enable-dlls_mtu \enable-aes \</pre>	Configuration summary for wol * Installation prefix: * System type: * Host CPU: * C Compiler: * AES: * AES-CBC: * AES-GCM: * AES-CCM: * AES-CTR: * DES3: * NULL Cipher: * SHA-224: * SHA-384: * SHA-512: * keygen: * certgen: * certgen: * certreq: * Hash DRBG: * PWDBASED:	fssl version 4.4.0 /usr/local pc-linux-gnu x86_64 gcc yes yes yes yes yes yes yes yes yes yes	
enable-dtls \ enable-dtls-mtu \	* certgen: * certreq:	yes yes	
enable-tls13 \ enable-aes \ enable-asp \	* Hash DRBG: * PWDBASED: * HKDF.	yes yes	
enable-testcert \ enable-nullcipher \	* X9.63 KDF: * DH:	yes yes	
enable-x963kdf"	* DH Default Parameters: * ECC: * ECC Custom Curves * ECC ENCRYPT:	yes yes yes yes	
	* DTLS: * TLS v1.3: * Supported Elliptic Curves:	yes yes yes	
A. Config.sh Build File	* 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.

<u>Note</u>: The cipher suites are registered on the <u>IANA web site</u>, 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 $--enable-aes \land$ 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 \land 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 $--enable-aes \land$ 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).

NIST SP 800-131A, Rev.2		Compliance			
	Requirement(s)	wolfSSL	UA and CS Prototype Implementation		
Section – Algorithm		Library per			
		Table 4-13	Configuration	Configuration	
2 – Encryption and	AES per NIST FIPS 197				
Decryption using	• 128, 192, or 256-bit keys	Y	Y	Not applicable –	
Block Cipher Algorithms	Approved mode of operation per NIST SP 800-38 series	AES	AES-256-GCM	NULL encryption	
3 – Digital Signature	 DSA per NIST FIPS 186-4 		Y	Y	
	• ECDSA len(n) >= 224	Y ECDSA	ECDSA using P-521 curve and SHA-512 (Note 1)	ECDSA using P-521 curve and SHA-512 (Note 1)	
4 – Random Bit	DRBG per SP 800-90A	Y			
Generation		DRBG	Y	Y	
	Hash_DRBG or	Y	Hash_DRBG using	Hash_DRBG using	
	HMAC_DRBG using any hash per NIST FIPS 180	SHS	SHA-256	SHA-250	
5 – Key Agreement using Diffie-Hellman	 Diffie-Hellman per NIST SP900-56A 	v	Y	Y	
(DH)	• DH >= 112 bits of security		ECDH-E using P-256	ECDH-E using P-521	
	(i.e., len(n) >= 224).		(Note 1)	(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	HMAC per FIPS 198 or	Y	Y	Y	
a Crypto-graphic Key	CMAC per SP 800-38B plus AES-128 per FIPS 197	KDF	HMAC-SHA-384	HMAC-SHA-256	

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

NIST SP 800-131A, Rev.2		Compliance		
Section Algerithm	Requirement(s)	wolfSSL Crypto	UA and CS Prototype Implementation (reference Section 4.5.1.3)	
Section – Algorithm		Library per Table 4-13	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-06².
- 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-ofscope 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 <code>Noise_IKpsk2_25519_ChaChaPoly_BLAKE2s</code>. 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.

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

Table C-1 – WireGuard Cryptographic Algorithms

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 = cOkrVrL11dUE+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:

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,		

Table C-2	– Compliance	with NIS	ST SP	800-56A
	Compnance	*****		000 001

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 <u>IANA web</u> 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.

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	

Table B-3 –	Compliance	with	NIST SP	800-13	1A, I	Rev. 2
	r			000 -0	, -	

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.