



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

SYSTEMS ENGINEERING CAPSTONE REPORT

**COMMAND AND CONTROL OF UNMANNED SYSTEMS
FOR EMISSIONS CONTROL EXPEDITIONARY
ADVANCED BASE OPERATIONS**

by

Matthew A. Grant, Matthew G. Hunter,
Kathleen Nuzzo, and Eric A. Toth

September 2023

Advisor:
Co-Advisor:

Britta Hale
Douglas L. Van Bossuyt

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE September 2023	3. REPORT TYPE AND DATES COVERED Systems Engineering Capstone Report		
4. TITLE AND SUBTITLE COMMAND AND CONTROL OF UNMANNED SYSTEMS FOR EMISSIONS CONTROL EXPEDITIONARY ADVANCED BASE OPERATIONS			5. FUNDING NUMBERS	
6. AUTHOR(S) Matthew A. Grant, Matthew G. Hunter, Kathleen Nuzzo, and Eric A. Toth				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) As the Department of the Navy transitions to Distributed Maritime Operations, there is a need to develop new systems, techniques, and procedures to limit the warfighter's exposure to an enemy. One of the most prevalent forms of exposure is the radio frequency (RF) footprint generated from the use of command and control (C2) equipment. This research analyzes the warfighter exposure risk created by operating unmanned systems (UxS) in Expeditionary Advanced Base Operations (EABO). To analyze the RF footprint of UxS operations, research is conducted to determine how C2 occurs between the UxS and the operator and how the transmitted data is protected against cyberattacks through security protocols and methods. The research is leveraged to develop a Concept of Operations (CONOPS) and scenarios to investigate how RF footprint changes as the level of UxS autonomy is varied. The CONOPS and scenarios are implemented in a modeling and simulation environment to examine the impact of UxS autonomy level and the security protocol used to protect the C2 link. The simulation results are then analyzed to determine the level of warfighter exposure and cyberattack risks for operating a UxS in EABO and identify a recommended balance between autonomy and situational awareness.				
14. SUBJECT TERMS security protocols, command and control, C2, encryption, authentication, DMO, EABO			15. NUMBER OF PAGES 181	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**COMMAND AND CONTROL OF UNMANNED SYSTEMS FOR EMISSIONS
CONTROL EXPEDITIONARY ADVANCED BASE OPERATIONS**

Matthew A. Grant, Matthew G. Hunter, Kathleen Nuzzo, and Eric A. Toth

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

**NAVAL POSTGRADUATE SCHOOL
September 2023**

Lead Editor: Kathleen Nuzzo

Reviewed by:

Britta Hale
Advisor

Douglas L. Van Bossuyt
Co-Advisor

Accepted by:

Oleg A. Yakimenko
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As the Department of the Navy transitions to Distributed Maritime Operations, there is a need to develop new systems, techniques, and procedures to limit the warfighter's exposure to an enemy. One of the most prevalent forms of exposure is the radio frequency (RF) footprint generated from the use of command and control (C2) equipment. This research analyzes the warfighter exposure risk created by operating unmanned systems (UxS) in Expeditionary Advanced Base Operations (EABO). To analyze the RF footprint of UxS operations, research is conducted to determine how C2 occurs between the UxS and the operator and how the transmitted data is protected against cyberattacks through security protocols and methods. The research is leveraged to develop a Concept of Operations (CONOPS) and scenarios to investigate how RF footprint changes as the level of UxS autonomy is varied. The CONOPS and scenarios are implemented in a modeling and simulation environment to examine the impact of UxS autonomy level and the security protocol used to protect the C2 link. The simulation results are then analyzed to determine the level of warfighter exposure and cyberattack risks for operating a UxS in EABO and identify a recommended balance between autonomy and situational awareness.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT AND OBJECTIVES	3
B.	TECHNICAL APPROACH.....	4
1.	Problem Definition.....	5
2.	Model Development and Simulation	6
3.	Risk Analysis	7
4.	Recommended Solutions	8
C.	DELIVERABLES	8
D.	CHAPTER SUMMARY.....	8
E.	SUMMARY OF CHAPTERS.....	8
II.	PROBLEM DEFINITION	11
A.	STAKEHOLDER ANALYSIS	11
1.	Topic Sponsor.....	13
2.	NRP	13
3.	NPS.....	14
4.	Naval and Marine Warfighters.....	14
5.	DON.....	14
6.	Program Offices	14
7.	Defense Contractors.....	15
B.	SCOPE	15
1.	Assumptions.....	15
2.	Constraints.....	16
C.	ASSESSMENT OF CURRENT CAPABILITIES	17
1.	Communication Links	17
2.	Open Systems Interconnection Model	18
3.	Cyber and Electronic Warfare Attacks	19
4.	Security Protocols and Methods	19
D.	CONCEPT OF OPERATIONS AND SCENARIOS.....	25
1.	Percent Autonomy Scenarios	27
2.	Triggered Event for C2	33
E.	UXS OPERATIONAL RISKS.....	35
F.	CHAPTER SUMMARY.....	36
III.	MODELING AND SIMULATION	37
A.	MODEL REQUIREMENTS.....	37

1.	Variable Inputs.....	37
2.	Desired Output.....	38
B.	MODEL PARAMETERS	39
1.	Constants	39
2.	Data Transmission Packet Size.....	41
3.	Mission Data Types.....	42
C.	MODEL DEVELOPMENT	47
1.	TLS Percent Autonomy Model Details	47
2.	TLS Triggered Event Model.....	54
3.	Denial-of-Service Model	58
D.	MODEL VERIFICATION	61
1.	MLS Overhead Verification.....	61
2.	TLS Overhead and Handshake Verification	63
3.	Model Verification	65
E.	SUMMARY OF MODEL ASSUMPTIONS.....	66
1.	Definition of Autonomy	66
2.	Handshake and Key Exchange Frequency	67
3.	Channel Overhead is Excluded.....	67
4.	MLS and PSK Operate in Broadcast Mode	67
5.	DoS Attack Timing	68
F.	SIMULATION AND RESULTS	69
1.	Percent Autonomy Model Without DoS Attack.....	69
2.	Percent Autonomy Model with DoS Attack	72
3.	Triggered Event Model.....	78
G.	CHAPTER SUMMARY.....	85
IV.	RISK ANALYSIS.....	87
A.	RISK DEFINITION.....	87
1.	Likelihood	87
2.	Impact	90
B.	RISK ASSESSMENT	92
1.	Likelihood Assessment.....	92
2.	Impact Assessment.....	97
3.	Risk Assessment	100
C.	RISK ANALYSIS.....	105
1.	Impact of Variables.....	105
2.	Trade Space Analysis.....	111
D.	CHAPTER SUMMARY.....	117

V.	CONCLUSIONS AND RECOMMENDATIONS.....	119
A.	CONCLUSIONS	119
B.	RECOMMENDATIONS FOR UXS OPERATIONS IN DMO/ EABO ENVIRONMENTS	120
C.	RECOMMENDATIONS FOR FUTURE RESEARCH.....	123
	APPENDIX A. MLS MODEL DETAILS.....	127
A.	MLS PERCENT AUTONOMY MODEL DETAILS.....	127
1.	MLS C2 and Autonomous Operation Timing.....	130
2.	MLS C2 Data Transmission.....	130
3.	MLS Recorded Video Transmission	131
4.	MLS Live Video Transmission	132
B.	MLS TRIGGERED EVENT MODEL.....	133
1.	MLS Trigger Autonomous Operation and Triggering Event.....	136
2.	MLS Triggered Communications.....	136
	APPENDIX B. PSK MODEL DETAILS.....	139
A.	PSK PERCENT AUTONOMY MODEL DETAILS.....	139
1.	PSK C2 and Autonomous Operation Timing.....	142
2.	PSK C2 Data Transmission.....	142
3.	PSK Recorded Video Transmission	143
4.	PSK Live Video Transmission	144
B.	PSK TRIGGERED EVENT MODEL	145
1.	PSK Trigger Autonomous Operation And Triggering Event.....	148
2.	PSK Triggered Communications.....	148
	LIST OF REFERENCES	149
	INITIAL DISTRIBUTION LIST	153

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Autonomy Spectrum	3
Figure 2.	Three Phase Systems Engineering Approach	5
Figure 3.	Stakeholder Influence/Interest Matrix	13
Figure 4.	Basic UAS Wireless Communication Architecture.....	17
Figure 5.	OSI Model Layers.....	18
Figure 6.	TLS Three-Way Handshake for Establishing Connection.....	21
Figure 7.	CONOPS C2 of UxS in the DMO / EABO Environment	26
Figure 8.	Operational Scenario of UxS Operation Using Full C2.....	28
Figure 9.	Operational Scenario of UxS Operation Using Full Autonomy	30
Figure 10.	Operational Scenario of UxS Operation Using a Percent Split Between C2 and Autonomy	32
Figure 11.	Operational Scenario of UxS Operation Using a Trigger Event for C2.....	34
Figure 12.	Video Formats.....	43
Figure 13.	Video Transmission and Recording Timeline	46
Figure 14.	TLS Communication Sequence	48
Figure 15.	TLS Percent Autonomy Innoslate Model	49
Figure 16.	TLS Handshake (F.4.1.1).....	50
Figure 17.	TLS C2 Data Transmission Model (F.4.1.3)	52
Figure 18.	TLS Recorded Video Transmission (F.4.1.4).....	53
Figure 19.	TLS Live Video Transmission (F.4.1.5).....	54
Figure 20.	TLS Triggered Event Innoslate Model	56
Figure 21.	Triggered Communications and Data (F.3.1.4)	58
Figure 22.	Download Triggered Data (F.3.1.4.2).....	58

Figure 23.	DoS Timing Innoslate Model.....	59
Figure 24.	DoS Model Timing Output Used to Assess Impact on Mission Models.....	60
Figure 25.	MLS Wireshark Analysis.....	62
Figure 26.	TLS 1.3 Overhead and Handshake Verification	64
Figure 27.	Timing Diagram of a DoS Attack on the TLS 50% Autonomy Model	73
Figure 28.	Timing Diagram of a DoS Attack on the TLS 30% Autonomy Model	74
Figure 29.	Triggering Event Model Timing Results	79
Figure 30.	TLS Triggering Event Model Timing Results with a DoS Attack	82
Figure 31.	MLS and PSK Triggering Event Model Timing Results with a DoS Attack	83
Figure 32.	Geolocation of Forward Unit Risk Comparison	106
Figure 33.	Geolocation of UxS Risk Comparison.....	107
Figure 34.	DoS Risk Comparison.....	108
Figure 35.	Impersonation Risk Comparison.....	109
Figure 36.	UxS Operational Risks of 100% Autonomous Operations with a Triggered Event Trigger Event Causing Periodic Video Transmission without DoS Attacks	110
Figure 37.	UxS Operational Risks of 100% Autonomous Operation with a Trigger Event Trigger Event Causing Periodic Video Transmission with DoS Attacks	111
Figure 38.	TLS Percent Autonomy Baseline Scenario Risk without DoS Attacks Trade Space.....	113
Figure 39.	TLS Percent Autonomy DoS Scenario Risk with DoS Attacks Trade Space.....	114
Figure 40.	MLS Percent Autonomy Scenario with DoS Attacks Trade Space.....	115
Figure 41.	PSK Percent Autonomy Scenario with DoS Attacks Trade Space.....	116
Figure 42.	Decision Tree	122

Figure 43.	MLS Communication Timing Sequence	128
Figure 44.	MLS Percent Autonomy Model.....	129
Figure 45.	MLS C2 Data Transmission Model (F.4.2.3)	131
Figure 46.	MLS Recorded Video Transmission (F.4.2.4).....	132
Figure 47.	MLS Live Video Transmission (F.4.2.5).....	133
Figure 48.	MLS Triggered Event Model.....	135
Figure 49.	Download Triggered Data (F.3.2.4).....	137
Figure 50.	PSK Communication Timing Sequence	140
Figure 51.	PSK Percent Autonomy Model.....	141
Figure 52.	PSK C2 Data Transmission Model (F.4.3.3)	143
Figure 53.	PSK Recorded Video Transmission (F.4.3.4).....	144
Figure 54.	PSK Live Video Transmission (F.4.3.5).....	145
Figure 55.	PSK Triggered Event Model.....	147

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Stakeholders	12
Table 2.	Summary of Security Protocols and Methods Advantages and Disadvantages	24
Table 3.	UxS Operational Risk Matrix	35
Table 4.	Video Information.....	44
Table 5.	Sampling of Forward Unit C2 Total Data Transmission from Model Data without DoS Attacks for Verification	65
Table 6.	Data Transmitted (Approximated RF Footprint) During a Mission Without DoS Attacks – Varying Levels of Autonomy	71
Table 7.	Data Transmitted (Approximated RF Footprint) During a Mission with DoS Attacks – Varying Levels of Autonomy	75
Table 8.	Complete Packet Data Lost During a DoS Attack – Varying Levels of Autonomy	76
Table 9.	Percentage of Data Transmission Lost Due to a DoS Attack – Varying Levels of Autonomy	77
Table 10.	Total Data Transmitted (Approximated RF Footprint) During a Mission without DoS Attacks – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission.....	80
Table 11.	Total Data Transmitted (Approximated RF Footprint) During a Mission with DoS Attacks – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission	84
Table 12.	Data Transmission Lost During a DoS Attack – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission	84
Table 13.	Percentage of Data Transmitted During a DoS Attack – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission	85
Table 14.	Risk Assessment Matrix	87
Table 15.	Assessment Scale – Likelihood of Forward Unit Geolocation	88

Table 16.	Assessment Scale – Likelihood of UxS Geolocation	89
Table 17.	Assessment Scale – Likelihood of Data Transmission During a DoS Attack.....	89
Table 18.	Assessment Scale – Likelihood of Impersonation Threat.....	90
Table 19.	Impact of Threat Event Assessment Matrix.....	91
Table 20.	Likelihood Forward Unit Geolocation Based on RF Output – Varying Levels of Autonomy	93
Table 21.	Likelihood of UxS Geolocation Based on RF Output – Varying Levels of Autonomy	94
Table 22.	Likelihood of Forward Unit Geolocation Based on RF Output – 100% Autonomy with a Trigger Event Causing Periodic Video Transmission	95
Table 23.	Likelihood of UxS Geolocation Based on RF Output– 100% Autonomy with a Trigger Event Causing Periodic Video Transmission	95
Table 24.	Likelihood of Data Loss due to DoS Attack – Varying Levels of Autonomy	96
Table 25.	Likelihood of Data Loss Due to DoS Attack – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission	96
Table 26.	Likelihood of Impersonation – Varying Levels of Autonomy	97
Table 27.	Likelihood of Impersonation – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission	97
Table 28.	Geolocation Impact Values.....	98
Table 29.	DoS Attack Impact Values.....	98
Table 30.	Impersonation Attack Impact Values.....	99
Table 31.	Forward Unit Geolocation Risk Levels – Varying Levels of Autonomy	101
Table 32.	UxS Geolocation Risk Levels – Varying Levels of Autonomy.....	102
Table 33.	Data Transmission Loss During DoS Attack Risk Levels – Varying Levels of Autonomy	103

Table 34.	Impersonation Risk Levels – Varying Levels of Autonomy	104
Table 35.	Risk Levels – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission without DoS Attacks	104
Table 36.	Risk Levels – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission with DoS Attack.....	104

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AI	artificial intelligence
C2	command and control
CNPC	control and non-payload communications
COC	command operations center
CONOPS	concept of operations
DMO	Distributed Maritime Operations
DON	Department of the Navy
DoS	Denial-of-Service
EABO	Expeditionary Advanced Base Operations
EO	electro-optical
FHSS	frequency-hopping spread spectrum
GHz	gigahertz
GPS	Global Positioning System
HD	high definition
IPSec	Internet Protocol Security
IR	infrared
kB	kilobytes
kbps	kilobits per second
LWIR	long-wave infrared
MACSec	Media Access Control Security
MB	megabytes
Mbps	megabits per second
MBSE	model-based systems engineering
MLS	Messaging Layer Security
NDS	National Defense Strategy
NIST	National Institute of Standards and Technology
NRP	Naval Research Program

OSI	Open Systems Interconnection
PSK	Pre-Shared Key
RF	radio frequency
RGB	red, green, blue
RPO	relevant program office
SA	situational awareness
SP	special publication
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAS	unmanned aerial system
UxS	unmanned systems
WEZ	weapon engagement zone

EXECUTIVE SUMMARY

The Navy recognizes that unmanned systems (UxS) will play a critical role in the execution of Distributed Maritime Operations and Expeditionary Advanced Base Operations by “providing additional warfighting capability and capacity to augment the traditional combatant force, allowing the option to take on greater operational risk while maintaining a tactical and strategic advantage” (Department of the Navy 2021). Multiple geographically dispersed platforms, weapons, and sensors will be integrated to improve battlespace awareness and enable forces to mass combat power at times and places of their choosing. Integration of all these systems requires a substantial amount of command and control (C2) to maintain situational awareness by transmitting and receiving data across C2 systems that generates a radio frequency (RF) footprint that adversaries can use to geolocate and target friendly forces. The enemy can also conduct Denial-of-Service (DoS) and impersonation attacks. Utilizing autonomy for UxS operations reduces the risks of geolocation but limits C2 capabilities.

The scope of this project is to compare the different factors that contribute to the cybersecurity and RF footprint risks of using C2 of UxS in contested environments and provide recommended solutions to reduce risk. Specifically, the goal is to optimize and/or maintain security while simultaneously enhancing interoperability during operations. This is done by cross comparing various C2 security protocols and using predetermined time intervals or triggered events to transition from full C2 of the operator to full autonomy as depicted in Figure 1.

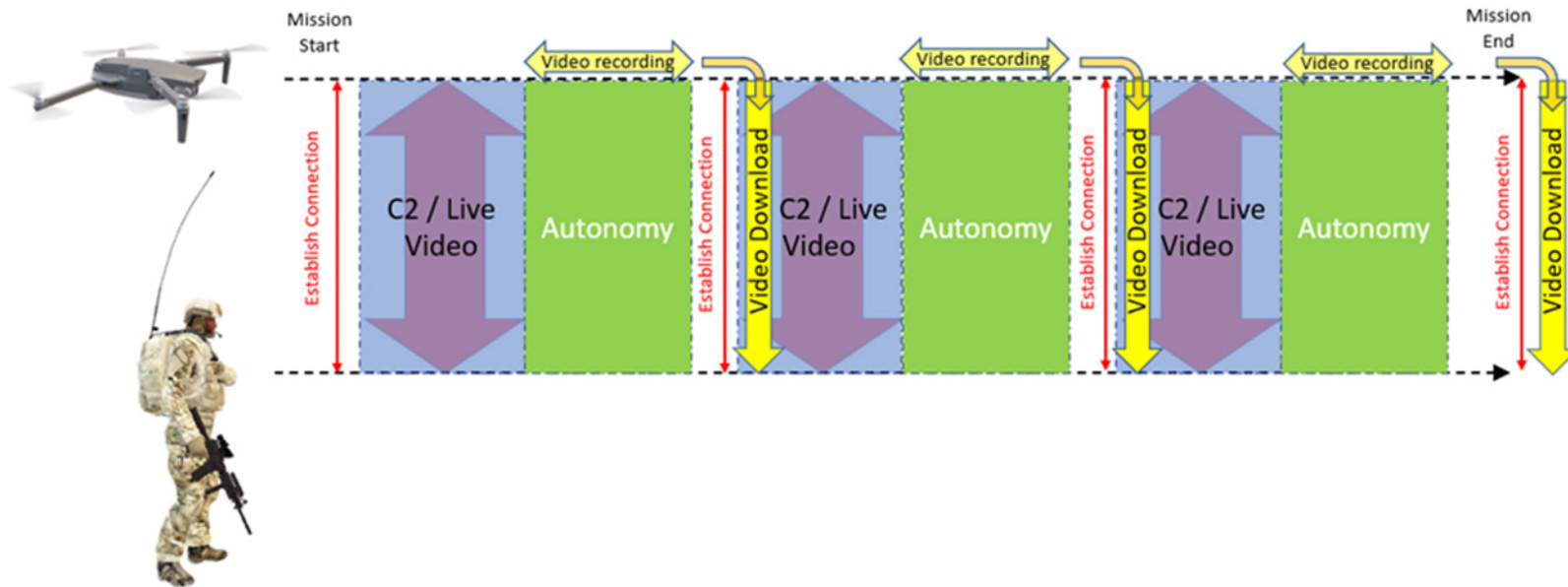


Figure 1. Operational Scenario of UxS Operation Using a Percent Split between C2 and Autonomy. The mission begins by establishing connection between the operator and the UxS. Initially, there is a continuous feed of C2 data from the operator to the UxS and live video from the UxS to the operator for a predetermined time interval indicated in blue. After the time interval ends, the connection between the operator and the UxS ends and the UxS operates autonomously while recording video for a predetermined length of time as indicated in green. Once the autonomy time interval is complete, the UxS reestablished connection with the operator who resumes C2 of the UxS and live video feed resumes while the recorded video is downloaded. This process repeats for the duration of the mission.

Modeling and simulation are used to determine the RF footprint risk for each autonomy scenario with each security protocol. The model takes the scenario type, file size, and security protocol as the main variable inputs to determine the resulting RF footprint, approximated as data transmission time. The file size of the data being transferred, especially the recorded video, is dependent on the duration the system operates in an autonomous mode. The longer the system operates autonomously, the larger the file size for recorded video to be downloaded to the forward unit's C2 station. This research models the Transport Layer Security (TLS), Messaging Layer Security (MLS), and Pre-shared Key (PSK) security protocols and methods as a sample across the space.

The model also injects DoS attacks to determine the effect of a DoS attack on the RF footprint with each security protocol and method. The results show a decrease in RF footprint as the level of autonomy is increased. The C2 protocols also affect the RF footprint with TLS resulting in the highest RF footprint and MLS resulting in the lowest RF footprint.

A risk analysis is performed using the modeling and simulation results to determine the level of geolocation, DoS, and impersonation risks. A trade-off space for risks and situational awareness is identified for each security protocol or method. Depending on mission needs, situational awareness can be sacrificed for an increase in autonomy to reduce risk. Figure 2 summarizes this trade-of space into a decision tree that can be used as a guideline for military leaders to determine what UxS set-up will best meet the mission's needs.

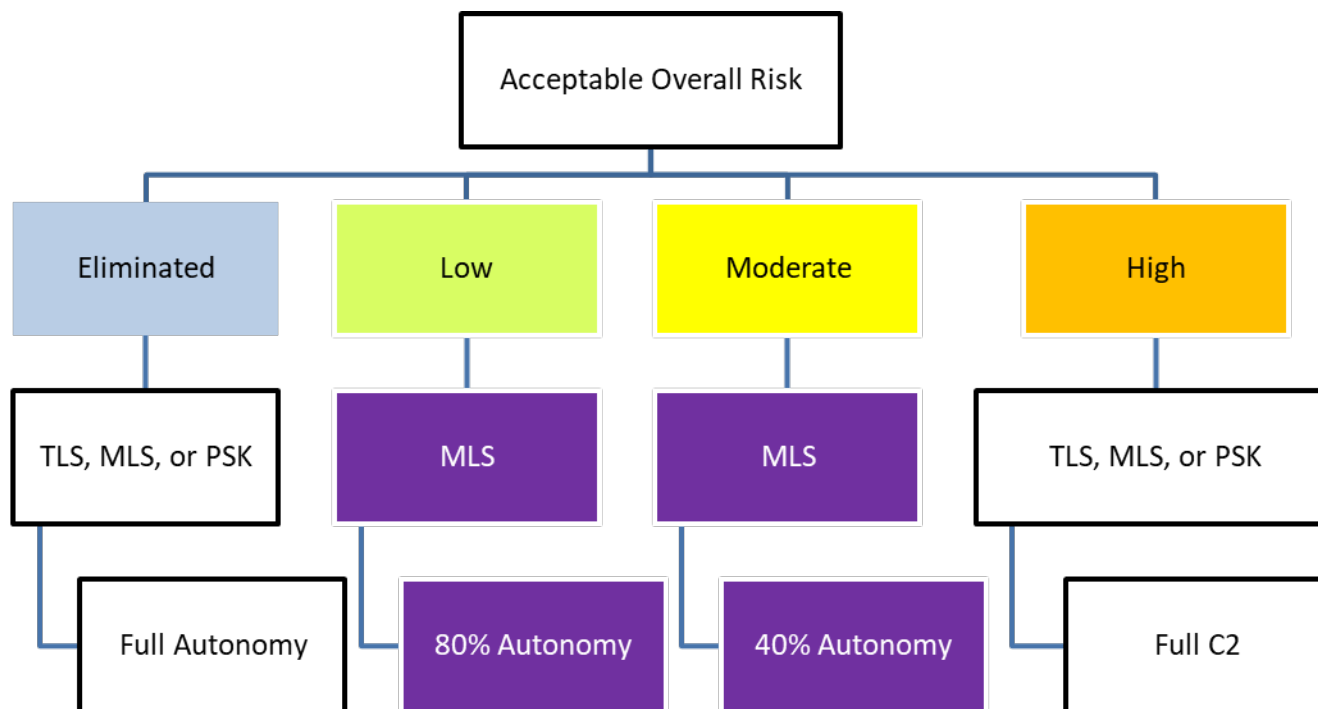


Figure 2. Decision Tree. If the acceptable risk level is moderate, MLS can be used with 40% autonomy to provide the maximum amount of situational awareness while remaining at moderate risk.

While this research focuses on security protocols, which helps to protect transmitted data, it is also necessary to protect the UxS itself. Future research should be focused on what counter UxS measures may be faced on the battlefield as well as existing UxS protection methods. This will allow for mitigation efforts to take place during the design of a semi-autonomous UxS system. Incorporating UxS protection measures during the design of UxS will be less expensive and more effective than trying to add the protection measures after the system is employed in the DMO/EABO environment.

References

Department of the Navy. 2021. *Unmanned Campaign Framework*. Washington, DC: Department of the Navy, 2021. https://www.navy.mil/Portals/1/Strategic/20210315%20Unmanned%20Campaign_Final_LowRes.pdf?ver=LtCZ-BPIWki6vCBTdgtDMA%3D%3D.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In 2021, the Department of the Navy (DON) released its Unmanned Campaign Framework in response to the 2018 National Defense Strategy (NDS) and the 2020 Tri-Service Maritime Strategy. The NDS identifies the central challenge to U.S. prosperity and security as “the reemergence of long-term, strategic competition by revisionist powers,” specifically China and Russia (Department of Defense 2018). These revisionist powers, along with other rogue regimes, are competing across all domains: air, land, sea, space, and cyberspace. The Tri-Service Maritime Strategy provides a strategy to remain competitive in all domains through the Distributed Maritime Operations (DMO) and Expeditionary Advanced Base Operations (EABO) concepts (U.S. Navy, U.S. Marine Corps, and U.S. Coast Guard 2020). The DON further specifies in its Unmanned Campaign Framework that unmanned systems (UxS) will play a critical role in the execution of DMO/EABO by “providing additional warfighting capability and capacity to augment the traditional combatant force, allowing the option to take on greater operational risk while maintaining a tactical and strategic advantage” (Department of the Navy 2021). The Unmanned Campaign Framework further states, “unmanned systems will increase lethality, capacity, survivability, operational tempo, deterrence, and operational readiness.”

DMO/EABO integrate multiple, geographically dispersed platforms, weapons, and sensors to improve battlespace awareness and enable forces to mass combat power at times and places of their choosing. Integrating all these systems requires a substantial amount of command and control (C2) to maintain situational awareness (SA) by transmitting and receiving data across systems generating a radio frequency (RF) footprint. RF footprints create an added challenge in the cyberspace, electromagnetic, and information environment domains. Adversaries can identify the RF footprint and use it to geolocate and target friendly forces. The enemy can also conduct Denial-of-Service (DoS) and impersonation cyberattacks. DoS attacks prevent C2 and can increase the RF footprint as devices try to reestablish C2. Impersonation attacks are used to gain access to the UxS and corrupt the data. The risks of these attacks are minimized through various

security protocols that encrypt and authenticate the data exchange between systems while the risks of RF footprint geolocation are minimized by utilizing autonomous UxS that require little to no C2 to operate.

The DON Unmanned Campaign Framework defines unmanned as “the physical removal or remote location of the human from the platform” (Department of the Navy, 2021). UxS operate on a spectrum of autonomy, defined as “the ability to adapt interactively to the dynamic maritime environment” (Department of the Navy, 2021). Figure 1 illustrates the autonomy spectrum and provides examples. UxS operating under low autonomy depend heavily on the human operator, requiring greater C2. Operating UxS at this end of the autonomy spectrum generates a large RF footprint. UxS operating under high autonomy requires little, if any C2, thus reducing the RF footprint. While reducing or eliminating the RF footprint is attractive, fully autonomous systems are not a solution to every mission. Some missions require the warfighter to maintain a high level of SA that is not provided by fully autonomous UxS operations. To determine the optimal level of autonomy for a given use case, a balance must be struck between the need to maintain SA and the need to limit the RF footprint. Furthermore, the type of C2 protocol used may affect survivability against cyberattacks as well as the potential for reducing the RF footprint.

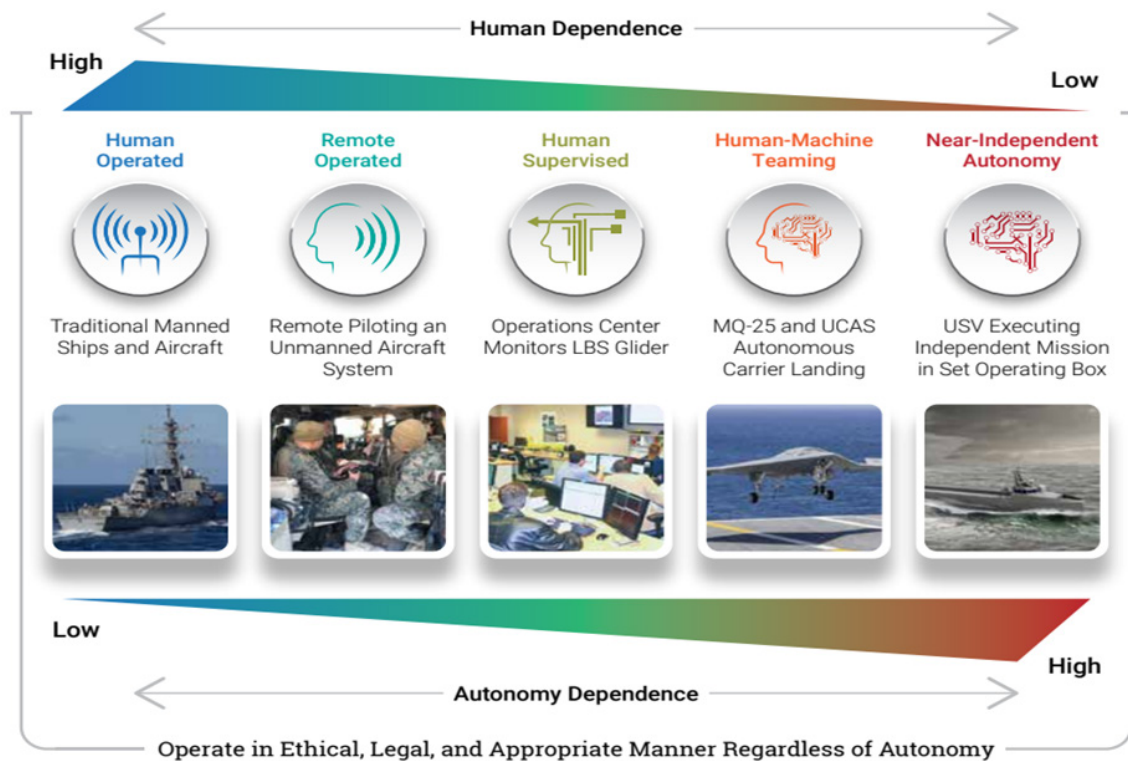


Figure 1. Autonomy Spectrum. Source: DON Unmanned Campaign Framework (2021).

A. PROBLEM STATEMENT AND OBJECTIVES

As the U.S. Department of the Navy implements DMO/EABO, the need for C2 increases. DMO/EABO enables increased battle space awareness and influence by transmitting and receiving data across multiple geographically dispersed platforms, sensors, and weapons. The challenge with DMO/EABO is maintaining sufficient SA through C2 while generating minimal or no RF footprint or other detectable activities that the enemy can use to locate the distributed forces. The goal of this research is to develop a concept of operations (CONOPS) and scenarios for operating UxS in the DMO/EABO environment. The scenarios examine varying levels of autonomy for UxS to determine the effect of autonomy on the RF footprint. Utilizing autonomous UxS reduces the RF footprint for C2 of those systems, but also reduces SA. This research analyzes the risks of each scenario and develops a decision tree to determine which security protocol and level of autonomy is recommended for a given use case.

This report addresses the following questions:

- How can C2 of UxS used in the DMO/EABO environment impact the RF footprint and risk of operators?
- How does UxS autonomy impact potential RF footprint and other risks to the operators?
- How can C2 and autonomy be balanced to improve RF footprint and overall risk while maintaining needed C2?
- How do C2 protocols affect the RF footprint and survivability against cyberattacks?

B. TECHNICAL APPROACH

The research team's approach to analyzing this problem space starts with research to determine the true problem based on information received from the stakeholders. Research of protocols currently utilized for UxS C2 in today's operational environment along with research on UxS autonomy and its effect on the ability to execute C2 is heavily used as the basis of developing the CONOPS and scenarios for using UxS in an EABO environment where a tradeoff between C2 and autonomy can be used to mitigate risks. After developing the CONOPS and scenarios, a risk analysis is performed using modeling and simulation to demonstrate tradeoff considerations between autonomy and C2 to determine the overall risk for varying scenarios.

A "Modified 3 Phase" systems engineering process is utilized throughout development of the project. This process is progressive and sequential but can loop back to earlier phases of the process, if necessary. Figure 2 shows the research team's systems engineering process flow and feedback process.

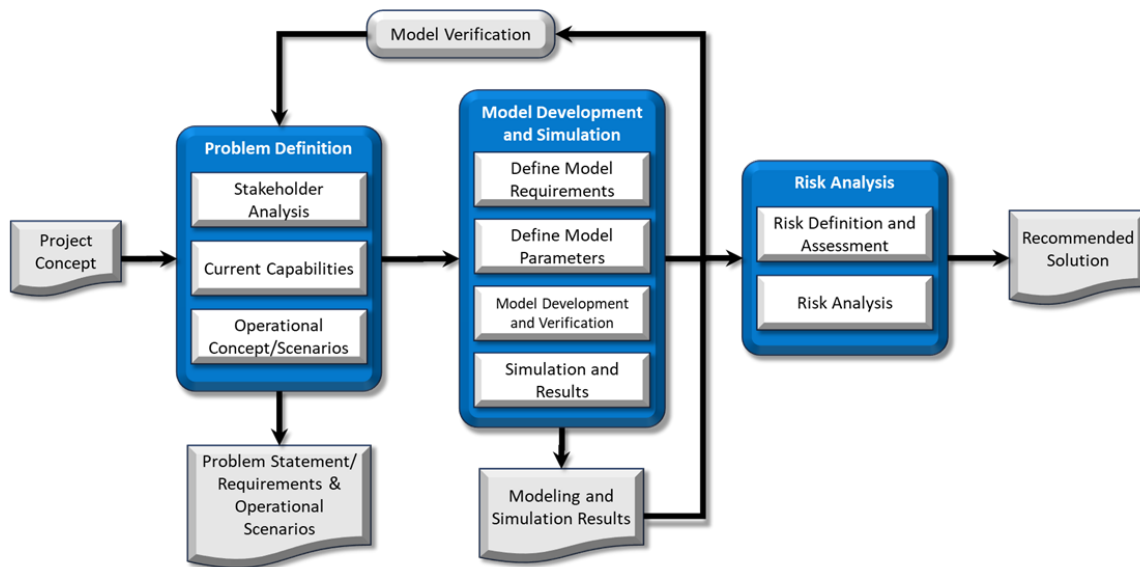


Figure 2. Three Phase Systems Engineering Approach. Adopted from Bones et al. (2018).

1. Problem Definition

An analysis of the stakeholder's initial problem statement is conducted to define the true problem that needs to be addressed. This analysis examines the stakeholders and their needs/desires and translates them into more specific system level requirements. This problem definition examines current operational capabilities, defines operational concepts, and conducts a functional analysis to determine the true problem statement and establish requirements for the project.

a. Stakeholder Identification and Analysis

This activity examines and identifies stakeholders that have a vested interest in the project and identifies their needs. The information obtained from this activity help shape the overall project and system evaluation requirements.

b. Current Capabilities

Determination of current capabilities sets a benchmark of performance for the research team and ensures evaluation of concepts are meaningful and not duplicative. The

current capabilities define the different variables that exist within the CONOPS and scenarios defined in the next step.

c. Operational Concept and Scenarios

This activity defines a top level CONOPS for UxS in the DMO/EABO environment. A series of scenarios are generated to examine the different type of UxS operations within the CONOPS. It is important to establish realistic CONOPS and scenarios to produce relevant information for the stakeholders.

2. Model Development and Simulation

This phase utilizes the CONOPS and scenarios from the Problem Definition Phase to develop a model architecture used to analyze the dangers of RF transmissions in a DMO/EABO environment. This phase consists of defining the model requirements, the various parameters used in the model, the model verification process, and the simulation method and results.

a. Define Model Requirements

This activity defines the purpose of the model and model's inputs and outputs. This activity is critical to the success of the overall risk evaluation. If the model is incorrectly defined, the output of the analysis is also incorrect.

b. Define Model Parameters

This activity defines the parameters, the constants, and assumptions, within which the model is developed. The parameters determine the method in which the model is developed.

c. Model Development and Verification

During this task, the model input requirements and parameters are used to build a working model that delivers an output. Model verification is a necessary process in which the model is checked for accuracy. A verified model ensures accurate simulation results and increases confidence and credibility to the analysis. Model development and

verification are iterative processes. As the model is developed, it is periodically verified by comparing the simulation data trends with the expected trends and then adjustments are made as necessary based on the verification. For example, the RF footprint is expected to decrease as the level of autonomy is increased. If the simulation results show a sudden increase in RF footprint as autonomy increases, the model is reexamined to determine the cause and identify errors in the model that need correction.

d. Simulation and Results

In this activity, the research team runs simulations of the verified model and reports the results. Multiple simulations are conducted to obtain results for each variable input to enable a comparison of results in the next phase.

3. Risk Analysis

This phase uses the simulation results to assess the risk of UxS operations in each scenario. This phase consists of defining risk, assessing the risk level of the simulation results, and analyzing the assessed risk levels to draw meaningful conclusions.

a. Risk Definition and Assessment

This activity details the definition of risk the research team uses for risk assessment. The risk definition determines the risk level of each simulated scenario. The assigned risk level enables comparison of scenarios for analysis.

b. Risk Analysis

In this activity, the risk levels of each simulated scenario are compared with one another to identify the effect of each variable. This comparison of variables enables the research team to draw conclusions and make recommendations on which set of variables to use in each scenario.

4. Recommended Solutions

From the outcome of the three phases described above, the research team identifies the set of variables that presents the least overall risk to the warfighting unit given a particular operational scenario.

C. DELIVERABLES

The main output of the project is a decision matrix the warfighter can use to determine which security protocol and level of UxS autonomy is recommended for the given mission and the anticipated operational threats. This decision matrix allows warfighters to mitigate the mission risks to the maximum extent possible while still completing the mission.

The deliverables for this project are the following:

- Capstone project report: “Command and Control of Unmanned Systems for Emissions Control Expeditionary Advanced Base Operations.”
- A model of the UxS operational scenarios developed in Innoslate and held at the Naval Postgraduate School (NPS) by the project advisors.

D. CHAPTER SUMMARY

Chapter I introduces the project by explaining the initial need behind the research and describes the project’s problem statement. The chapter details the technical approach and systems engineering process used to conduct the research and analysis leading to the project deliverables.

E. SUMMARY OF CHAPTERS

(1) Chapter I, Introduction

Chapter I introduces the problem and the systems engineering process used to deliver results.

(2) Chapter II, Problem Definition

Chapter II defines project scope, CONOPS, and scenarios. The chapter presents a summary of existing technologies available to solve the problem defined in Chapter I.

(3) Chapter III, Modeling and Simulation

Chapter III details development of the model used to simulate UxS operations under various operating conditions.

(4) Chapter IV, Risk Analysis

Chapter IV presents the results from the modeling and simulation from Chapter III and compiles the raw results into a meaningful analysis to form recommendations.

(5) Chapter V, Conclusions and Recommendations

Chapter V uses the analysis from Chapter IV to provide recommendations and draw conclusions to answer the questions posed in the problem statement.

THIS PAGE INTENTIONALLY LEFT BLANK

II. PROBLEM DEFINITION

This chapter identifies the problem stakeholder and defines the project scope. Current capabilities are assessed to aid the development of the CONOPS and scenarios for the project.

A. STAKEHOLDER ANALYSIS

The research team identified stakeholders that have a vested interest in the project and identified their interests and concerns as summarized in Table 1. Figure 3 shows a stakeholder power-interest grid used to prioritize stakeholder needs. Stakeholders with high influence and high interest are the highest priority.

Table 1. Stakeholders

Stakeholder	Type	Interests	Concerns
Topic Sponsor	Primary	Deeper knowledge of current abilities to direct future research/development research teams	Current project scope does not result in feasible set of solutions
Naval Research Program (NRP)	Primary	Timely high-quality research in line with the topic sponsor's interest	Research cost overruns, substandard quality, not in line with topic sponsor's interests
NPS	Primary	Timely high-quality research	Schedule overruns, substandard quality
Naval and Marine Warfighters	Secondary	Methods of UxS C2 that significantly lowers RF footprints	The associated cost and prospective interoperability with existing systems and operations
DON	Secondary	Solutions that provide the force with the most effective resources to conduct DMO/EABO operations	Cost and schedule overruns
Program Offices	Other	Fulfill the DON's vision for prospective solutions	Cost and schedule overruns, integrations details
Defense Contractors	Other	An awarded contract to create working low footprint C2 systems and UxS	Cost and schedule over-runs

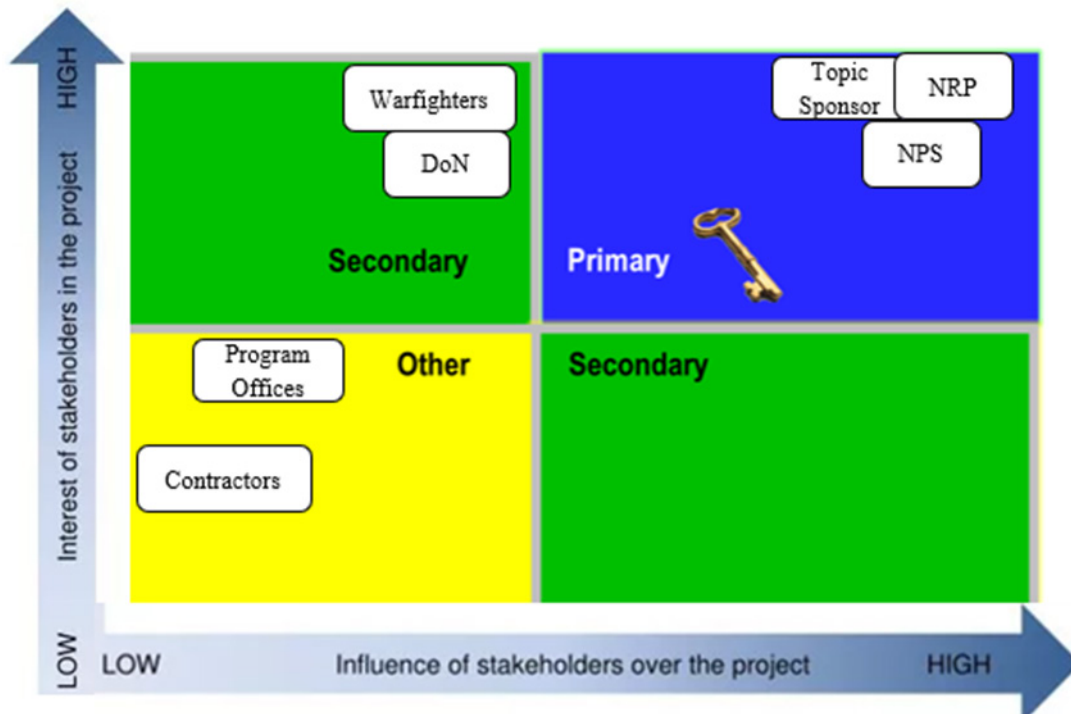


Figure 3. Stakeholder Influence/Interest Matrix

1. Topic Sponsor

The topic sponsor is a primary stakeholder and holds high interest in the project and has moderately high influence on the project. The topic sponsor is interested in understanding the risks of RF interference in a DMO/EABO environment and presented this topic to the NRP for approval and execution of topic research. The resulting research provides direction for future research. The topic sponsor is concerned about obtaining useful research in a timely manner.

2. NRP

The NRP is the primary stakeholder holding the most influence and interest on the project. The NRP is interested in high-quality research that benefits the DOD and is in line with a topic sponsor's interest. The NRP provides funding for the project so it can be executed. The NRP is concerned about obtaining useful research in a timely manner and within the allotted budget.

3. NPS

NPS is another primary stakeholder and has equal interest in the project as the project sponsor, but with slightly less influence. NPS is tasked with executing the project is interested in ensuring its students provide quality research that addresses the project sponsor's research goals. NPS is concerned with providing research in a timely manner and withing the budget allocated by the topic sponsor.

4. Naval and Marine Warfighters

The warfighter is a secondary stakeholder with a high interest in the project but has low influence. The warfighter is interested in obtaining improved equipment and operational procedures to fulfill their missions effectively and safely. The results of this project can increase warfighter safety in the DMO/EABO environment. Warfighters are concerned about system suitability and changes to operational procedures. Implementing the recommendations in this research will directly impact how the warfighter trains and operates, and impacts equipment needs.

5. DON

The DON is a secondary stakeholder with similar interest and influence on the project as the warfighter. The DON is interested in supplying the warfighter with improved equipment and operational procedures to complete missions more effectively while ensuring the safety of the warfighter. The DON is concerned with implementing the recommendations in this research in a cost effective and timely manner.

6. Program Offices

Program offices are other stakeholders with very low influence and moderate interest in the project. Program offices are tasked with implementing the recommendations in this research as directed by the DON. Program offices are concerned with implementing the recommendations in the cost and schedule parameters dictated by the DON.

7. Defense Contractors

Defense contractors are other stakeholders with the least interest and least influence on the project. Defense contractors are interested in the contract opportunities made available by the program offices implementing the recommendations of this research. Contract opportunities are opportunities for defense contractors to expand their business and collect additional revenue. Defense contractors are concerned with cost and schedule when submitting proposals for contract opportunities and executing the contract if awarded.

B. SCOPE

The scope of this project is to research and analyze the different factors that contribute to the cybersecurity and RF footprint risks of using C2 of UxS in contested DMO/EABO environments. The goal is to optimize and/or maintain security while simultaneously enhancing interoperability in the DMO/EABO by cross comparing various C2 security protocols in combination with different levels of UxS autonomy. The stakeholders are interested in balancing C2 and autonomy to reduce RF footprint risks and maintain SA to defend against various threats imposed on units in DMO/EABO.

The research team considers potential CONOPS and scenarios for DMO/EABO to frame and scope the balance between these factors to predict an optimized configuration for a given scenario by leveraging prior work on low-RF emission software distribution protocols for DMO/EABO updates and C2 protocol design & analysis research.

1. Assumptions

Assumptions play a critical role by establishing the underlying beliefs and statements that form the basis for the argument or plan. research team. These assumptions help define the boundaries of the project scope. All operations within DMO/EABO are considered.

- All protocols use National Security Agency (NSA) approved and Commercial Solutions for Classified compliant cipher suites for encryption and authentication.

- UxS have provisions to operate in a Global Positioning System (GPS)-denied areas.
- Although this report will focus solely on unmanned arial systems (UAS), the concepts explored within this report can be applied to unmanned ground vehicles, unmanned surface vehicles, and unmanned underwater vehicles.

2. Constraints

Constraints refer to the limitations or restrictions that impact a project, plan, or situation. These constraints define the boundaries within which actions and decisions must operate.

- This report focuses on group 1 small UAS controlled within the DMO/EABO, excluding larger drones controlled within the continental United States.
- There are many security protocols and methods available to encrypt and authenticate signals during UxS operations. Only Transport Layer Security (TLS) and Messaging Layer Security (MLS) protocols are assessed in this project as a sample across the space. Other protocols are not within the project scope and are not assessed.
- There are several means of providing C2 to UxS. Only C2 communication to be in scope for this project, other signal items such as GPS, are out of scope.
- The focus for this project is on C2 systems using RF only. Other means of C2 communication are out of scope.
- Although TLS and MLS can use Transmission Control Protocol (TCP) for connection and authentication, TCP overhead is excluded from the analysis as a common baseline. This research analyzes the specific protocols and methods detailed in the requirements.

C. ASSESSMENT OF CURRENT CAPABILITIES

This section provides an assessment of current capabilities related to the operation of UxS, RF footprint, and cybersecurity. These current capabilities provide insight into CONOPS and scenario development.

1. Communication Links

Generally, UxS have two basic types of communication links, a control and non-payload communications (CNPC) link and a data link (Zeng, Zhang, and Lim 2016). Information passed through the CNPC link includes C2 from the ground control station (operator) to the UxS, status report from the UxS to ground, and sense-and-avoid information among multiple UxS as depicted in Figure 4. Data links support mission-related communications such as video captured from the UxS camera.

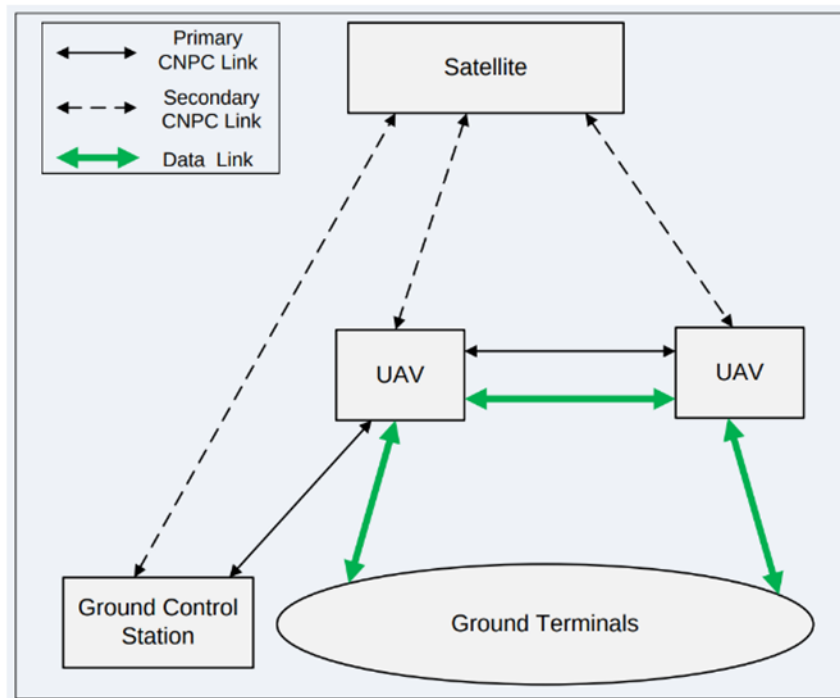


Figure 4. Basic UAS Wireless Communication Architecture. Source: Zeng, Zhang, and Lim (2016). UxS communicate with each other and the ground control station using CNPC and data links.

2. Open Systems Interconnection Model

The Open Systems Interconnection (OSI) model is a conceptual framework used to describe the communication process between different computer systems (Saxena 2014). It was developed by the International Organization for Standardization to provide a standard model for network communication that would allow different systems to communicate with each other (Saxena 2014). The OSI model consists of seven layers, each with a specific function and set of protocols that govern the communication between systems. Understanding the OSI model is important in network communication as it provides a common language and framework for network designers and engineers to build and troubleshoot complex network systems. The seven layers are presented in Figure 5.

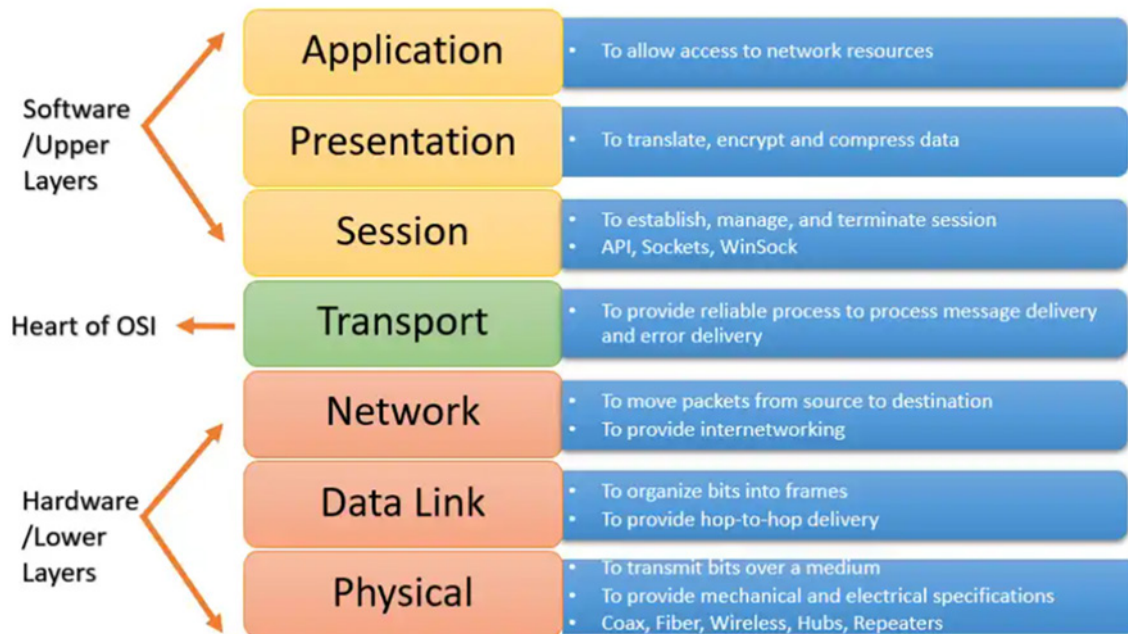


Figure 5. OSI Model Layers.. Source: Williams (2023). The OSI model layers are listed in order from the top down, starting with the application layer. A short description and purpose of each layer is presented to the right in the blue text boxes.

3. Cyber and Electronic Warfare Attacks

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800–30 defines a cyberattack as “an attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information” (2012). The type of cyberattacks examined in this work are impersonation attacks. In an impersonation (a.k.a. spoofing) attack, the attacker pretends to be an authentic user and gain access to the communication between devices (Barbeau, Hall, and Kranakis 2006). If successful, the impersonator gains access to network resources. The impersonator can use this access to corrupt and steal data and gain control of UxS.

Electronic warfare attacks “exploit and deny access to RF communications” (Poisel 2019, 1). The type of electronic warfare attack examined in this work are DoS attacks. In a DoS (a.k.a RF jamming) attack, the attacker “injects substantial amounts of electromagnetic energy, referred to as noise, into a receiving antenna” causing a break in the communication link between targeted assets (Thiessen, Van Bossuyt, and Hale 2022, 276). In UxS operations, DoS attacks prevent the UxS from receiving the necessary C2 information from the operator. A DoS attack also prevents the UxS from sending data back to the operator, reducing the operator’s SA.

4. Security Protocols and Methods

To secure the information exchange during UxS operations, a variety of security protocols and approaches are available. TLS, PSK, Internet Protocol Security (IPSec), Media Access Control Security (MACSec), and MLS are detailed in the following paragraphs. This work will specifically apply TLS, the PSK technique, and MLS, as MACSec and IPSec are both session-based protocols which follow similar handshake behavior as TLS for the purposes of this work.

a. Transport Layer Security

TLS is a session-based protocol that provides an encrypted and authenticated channel for sending data and receiving data between connected entities that is hardened against impersonation attacks but is susceptible to DoS (Leon and Britt 2022). Connection between the UAS (the client) and the control station (the server) is established through a three-way handshake, as shown in Figure 6. When groups of devices are connected, this handshake must occur for each connection, meaning the RF footprint increases linearly with each additional device to which an entity is connected. In a DoS attack, each time communications are interrupted, the handshake must occur again to establish a new connection. Repeated communication back and forth to reset a connection increases the RF footprint generated. A benefit of session-based protocols like TLS is their performance against a compromise. The loss of data during the compromise is limited to the session in which the compromise occurs (Dowling and Hale 2020). In other words, TLS provides a smaller vulnerability window than if a fixed key (PSK) is used. TLS operates at the transport layer by adding a security layer between the application layer (Layer 7) and the transport layer (Layer 4) (Microsoft 2023). After key establishment, the TLS protocol uses symmetric encryption to secure data transmitted between endpoints.

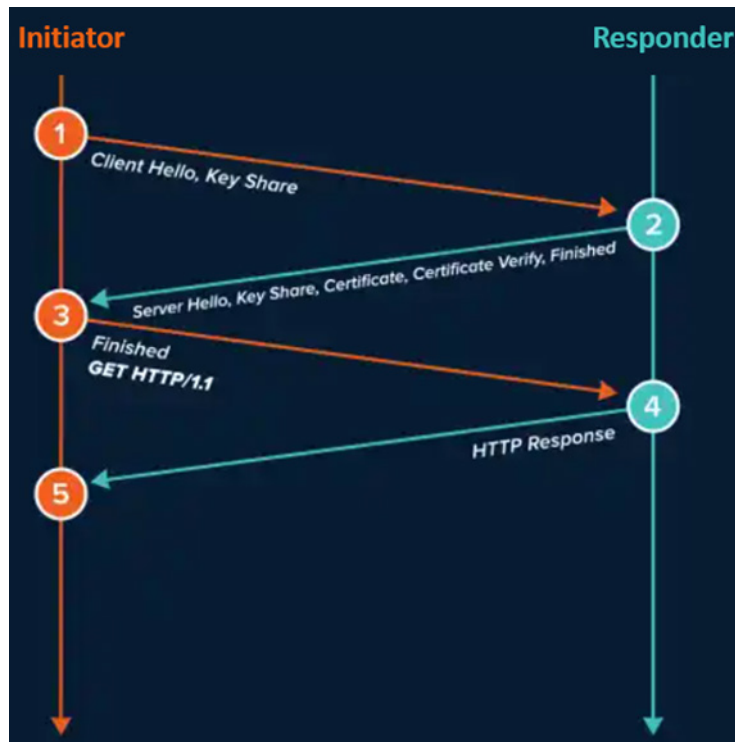


Figure 6. TLS Three-Way Handshake for Establishing Connection. Adopted from Singh (2018).

b. Pre-Shared Key

A PSK is a security establishment method in which a static key is distributed to the communicating entities before it is needed (Lewis 2022). In the DOD, this involves manual distribution of the keys via key loaders. This method will be referred to as “PSK” in this report. After a key transfer, encrypted data using the shared secret key can be sent across a channel (Lewis 2022). The benefit of using a PSK is that it eliminates the need to reinitiate a key exchange in the event of a DoS attack. Instead, the devices can resume communication as soon as the DoS attack ends. Utilizing a PSK eliminates the three-way handshake, resulting in a slightly lower RF footprint compared to TLS. The downside of using PSK is its susceptibility to compromise. Because the PSK is a static key, there is no fast and easy way to establish a new connection in the event of a compromise/impersonation attack, resulting in a complete loss of data as well as impersonation potential. To reset the connection, new crypto keys would need to be manually distributed and loaded onto all the devices which takes a lot of time, especially when

devices are located all over the world in the case of DMO/EABO. PSK can be used in various security protocols; its operation is typically at the data link layer of the OSI model.

c. Internet Protocol Security

IPSec is typically used to protect information shared at Layer 3 of the OSI model. IPSec uses the Internet Key Exchange (IKE) protocol to establish a shared key which is used for encryption/authentication of the IPSec datagrams as they are shared through the network (Lewis 2022). IPSec can operate in two modes: transport mode and tunnel mode. IPSec has similar advantages and disadvantages as the TLS method. Like in TLS, if the key is compromised, the connection is vulnerable to impersonation attacks. Another drawback of IPSec is the large overhead size that contributes to the RF footprint.

d. Media Access Control Security

MACSec is an IEEE 802.1AE standard for securing information exchanged between Ethernet connected devices (Lewis 2022). MACSec operates in the sub-layer of the data link Layer 2 in the OSI model. MACSec has similar protections and weaknesses against DoS and impersonation attacks as TLS and IPSec.

e. Messaging Layer Security

MLS is an asynchronous continuous key agreement protocol. By being asynchronous, MLS eliminates the need for constant, real-time connection between the communicating entities. The sender can send information at any time, and the receiver can process that information at any time, hence allowing for delayed routing. The MLS protocol is beneficial in a DoS attack as MLS does not require a handshake to reestablish the connection and so avoids the associated RF footprint and delays caused by reconnection in TLS. Because MLS is asynchronous and a continuous key agreement protocol, it eliminates the medium compromise windows present in TLS and long compromise windows in PSK. Instead, continuous key agreement protocols offer controllable short windows, dependent on adversarial action at the time of compromise. Security can be recovered if the adversary remains passive (Dowling and Hale 2021).

MLS is also beneficial when connecting multiple devices as it scales devices logarithmically as opposed to linearly like TLS (Britt, Leon, and Hale 2022). Scaling logarithmically reduces the amount of data that must be sent between devices compared to the data required when devices are connected one-to-one. MLS operates at the application layer (Layer 7) of the OSI model, where it provides a secure communication layer for group communications.

f. Summary of Security Protocols and Methods

Table 2 summarizes the advantages and disadvantages of the security protocols and methods examined in this research. Each security protocol and method operate at a specific layer within the OSI model and provides varying levels of protection against cyberattacks. Some protocols and methods rely on higher data overhead compared to others which generates a larger RF footprint.

Table 2. Summary of Security Protocols and Methods Advantages and Disadvantages

	TLS	PSK	IPSec	MACSec	MLS
OSI Model Layer	Transport Layer (Layer 4)	Data Link Layer (Layer 2)	Network Layer (Layer 3)	Data Link Layer (Layer 2)	Application Layer (Layer 7)
RF Footprint	High	Low	High	High	Medium
DoS Attack Survivability	Low	High	Low	Low	High
Impersonation Survivability	Medium	Low	Medium	Medium	High

D. CONCEPT OF OPERATIONS AND SCENARIOS

The CONOPS for C2 of UxS in the DMO/EABO environment is depicted in Figure 7. The Command Operation Center (COC) tasks the forward unit with a mission. Next, the forward unit deploys UxS to accomplish the mission, using C2 to maintain SA of the UxS and their surroundings. The unit also provides status updates to the COC throughout the mission. While the UxS are operating in DMO/EABO environments, they are subjected to enemy cyberattacks. The C2 signals used to communicate between the UxS, forward unit, and COC generate an RF footprint that can reveal their locations to the enemy.

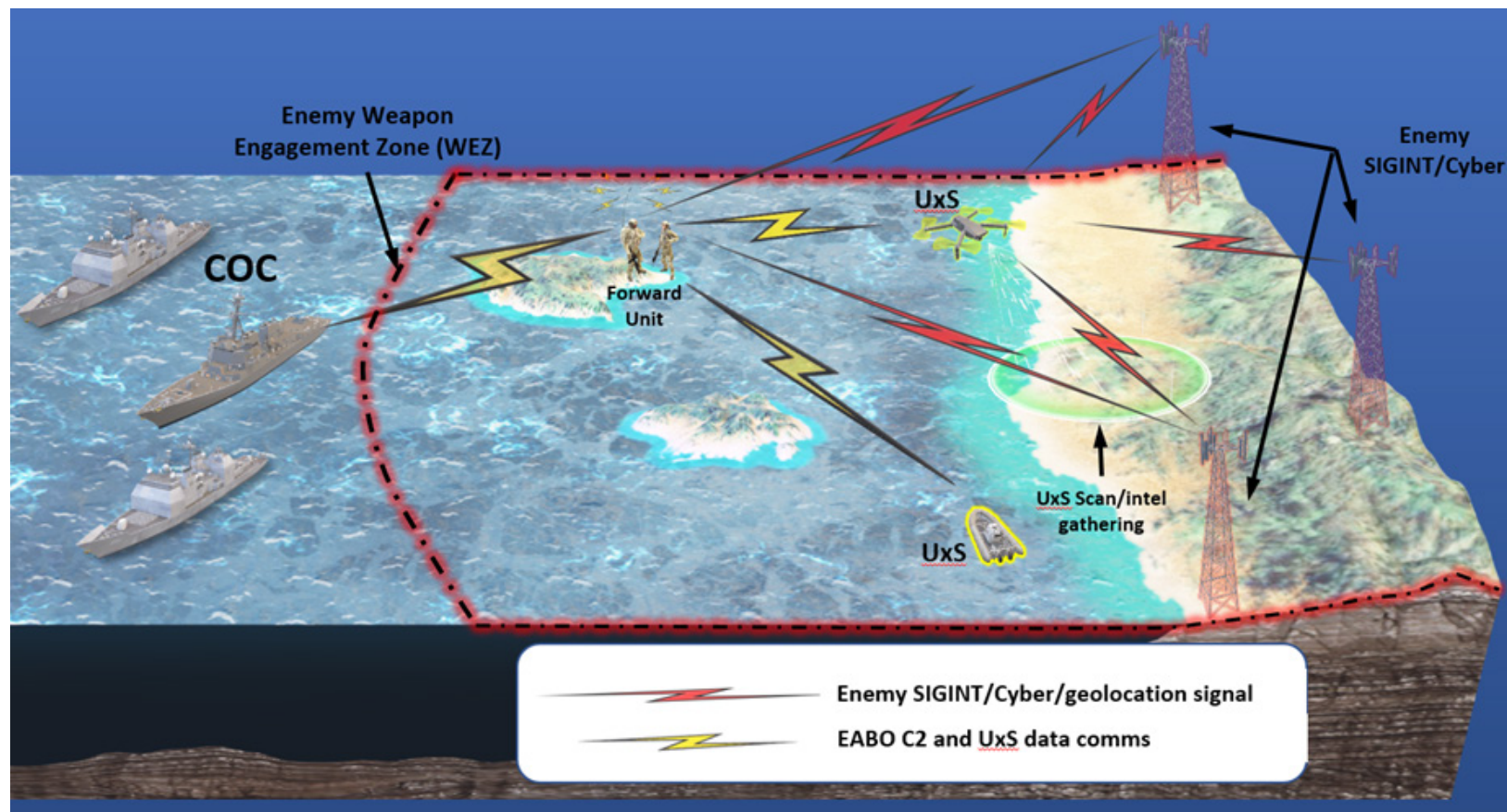


Figure 7. CONOPS C2 of UxS in the DMO / EABO Environment. The forward unit deploys to the enemy WEZ and operates UxS to complete the mission. The forward unit relays status updates to the COC to provide the COC with SA of the enemy WEZ. The enemy conducts cyberattacks against the UxS and forward unit.

There are many use cases in which the RF footprint needs to be reduced or eliminated, but the risk from operating fully autonomously without SA is too high. For example, any UxS equipped with a weapon needs to be operated under human supervision to ensure the weapon does not fire inadvertently or fire upon an incorrect target. In these use cases, a hybrid of C2 and autonomy may provide the best risk mitigation. In a hybrid scenario, the UxS can operate semi-autonomously while receiving and executing commands from the forward unit as needed. The UxS can transmit information back to the forward unit in predetermined time intervals or as determined by an artificial intelligence (AI) algorithm to provide the forward unit with some level of SA. A hybrid scenario reduces the amount of C2 required to support operations and the resulting RF footprint while maintaining some level of SA. The scenarios below explore different use cases within the autonomy spectrum that include the basic full C2 and fully autonomous use cases as well as two hybrid use cases. The use cases are grouped into two categories: percent autonomy and triggered event.

1. Percent Autonomy Scenarios

The following percent autonomy scenarios examine the full range of autonomy, from zero percent autonomy with full C2 to full autonomy with no C2. There are also use cases in between where the operator can choose to alternate between zero percent autonomy and 100 percent autonomy periodically during the mission.

a. Zero Percent Autonomy with Full C2

In a full C2 scenario, the UxS is tele-operated by an operator using an Xbox style controller. The CNPC and data links transmit information between the UxS and the forward unit continuously as shown in Figure 8. The unit receives live video feed from the UxS to maintain SA of the UxS' location and its proximity to obstacles and controls the UxS accordingly. While full C2 provides SA, it generates a large RF footprint.

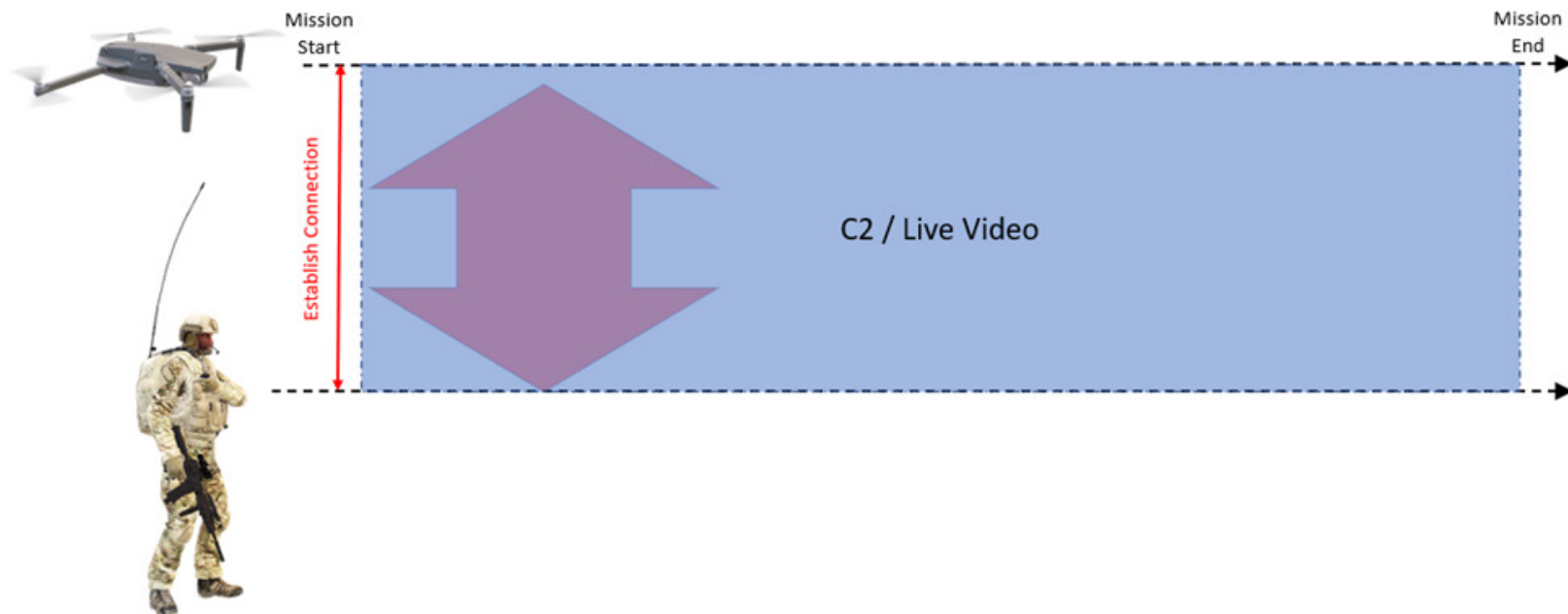


Figure 8. Operational Scenario of UxS Operation Using Full C2. The mission begins by establishing connection between the operator and the UxS. During the mission, there is a continuous feed of C2 data from the operator to the UxS and live video from the UxS to the operator. The C2 data and live video exchange is indicated in blue. The full C2 scenario provides the best SA, however, the continuous connection generates a large RF footprint exposing the operator and the UxS locations to the enemy.

Most UxS have fail safes in the event the C2 connection is lost. These fail safes ensure the UxS comes to a safe stop/landing and avoids obstacles. An example use case for this scenario is target acquisition and firing where a human operator needs full maritime domain awareness to command the UxS to fire upon a target.

b. Full Autonomy with no C2

A fully autonomous UxS performs tasks without human intervention or control. Instead of being controlled by a human operator, autonomous UxS are equipped with sensors to capture data and algorithms and decision-making systems that allow the UxS to carry out complex operations and navigate based on sensor data. By removing the human operator, the need to C2 and its corresponding RF footprint risk is eliminated. However, the lack of C2 means the unit will not have SA. This scenario is depicted in Figure 9.

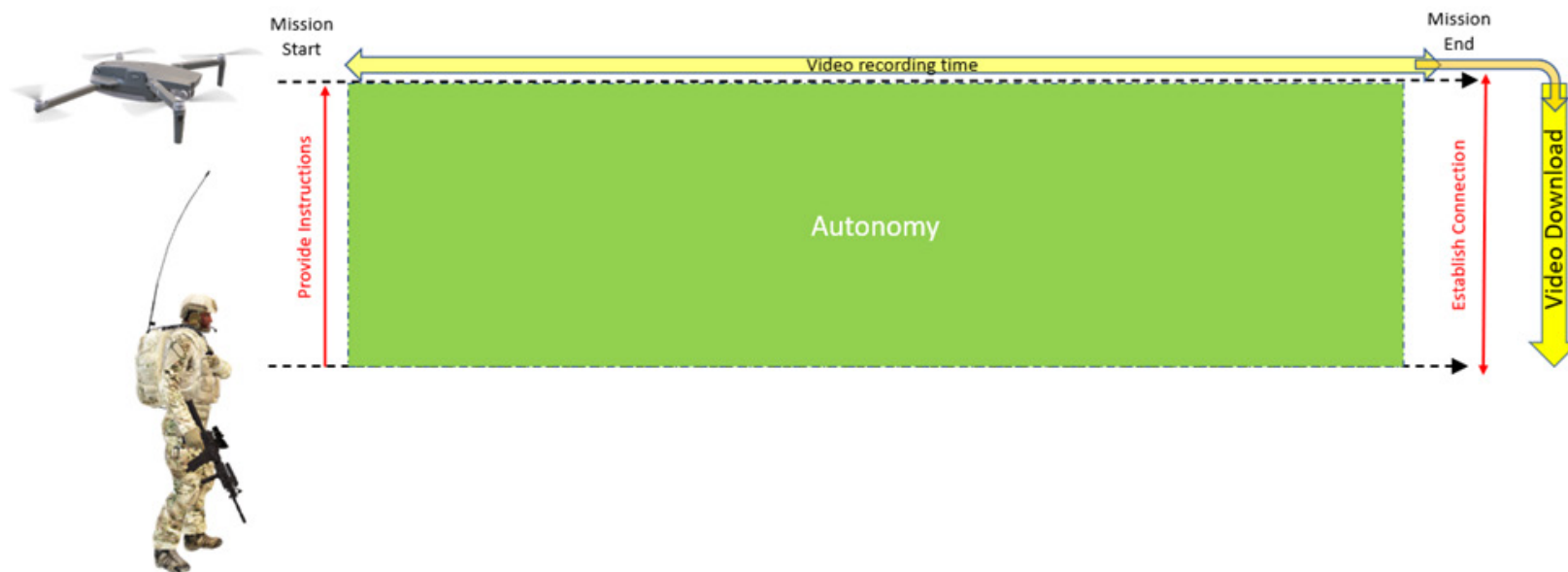


Figure 9. Operational Scenario of UxS Operation Using Full Autonomy. The mission begins when the operator provides instructions to the UxS. The UxS operates under full autonomy while recording video for the duration of the mission as indicated in green. When the UxS returns to the operator at the conclusion of the mission, a connection is established between the operator and the UxS (wired or wireless connection) to enable the recorded video to be downloaded from the UxS. This scenario eliminates the RF footprint but does not provide any SA to the operator during the mission.

An example use case of this scenario is a logistics UxS where its sole purpose is to deliver a payload between predetermined locations. The risk of not having maritime domain awareness depends on the value of the UxS and its payload.

c. Hybrid Percent Split Between C2 and Autonomy

One hybrid solution to balance the risks of C2 RF footprint and autonomy SA is to alternate between full C2 and full autonomy as shown in Figure 10. Before the start of the mission, the warfighter can determine what percentage of C2 is acceptable based on the RF footprint risk. The UxS is initially teleoperated while providing live video feed. After a period, the UxS operates autonomously. When the autonomy duration has ended, data is downloaded from the UxS to the forward unit and the operator resumes full control of the UxS. During this time, the operator can send the UxS new instructions to follow during the next autonomous period based on the data received.

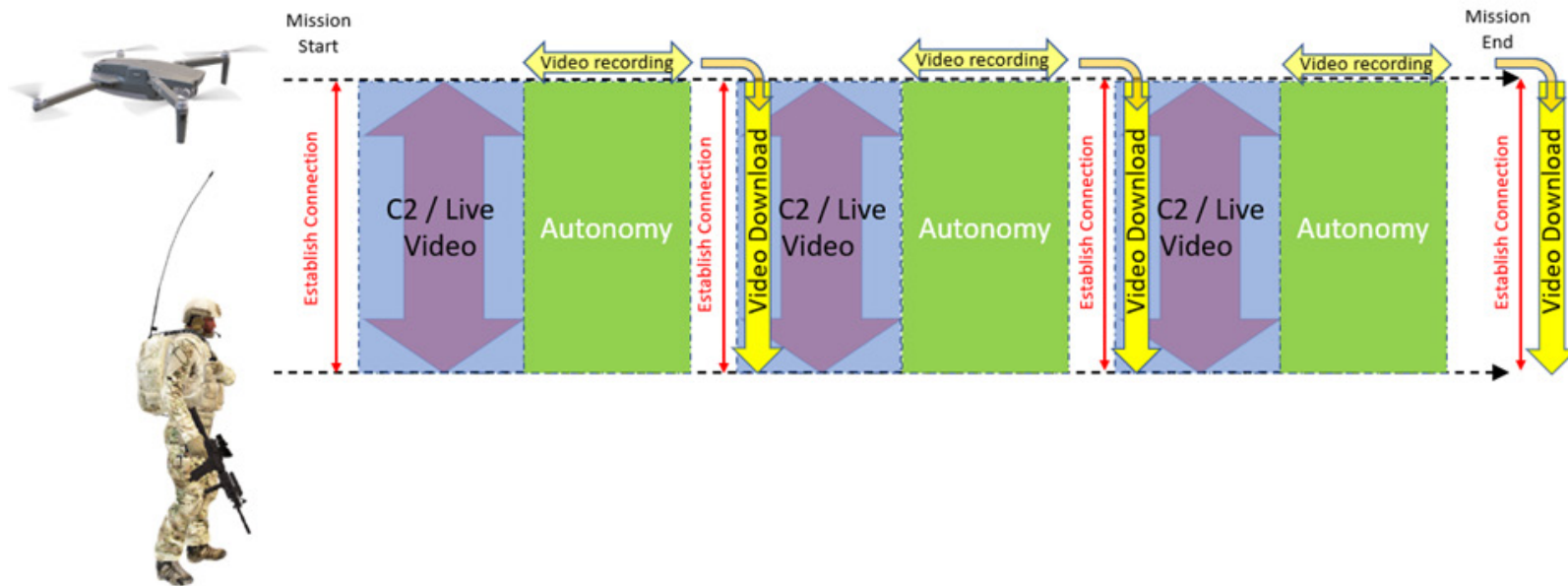


Figure 10. Operational Scenario of UxS Operation Using a Percent Split Between C2 and Autonomy. The mission begins by establishing connection between the operator and the UxS. Initially, there is a continuous feed of C2 data from the operator to the UxS and live video from the UxS to the operator for a predetermined time interval indicated in blue. After the time interval ends, the connection between the operator and the UxS ends and the UxS operates autonomously while recording video for a predetermined length of time as indicated in green. Once the autonomy time interval is complete, the UxS reestablishes connection with the operator who resumes C2 of the UxS and live video feed resumes while the recorded video is downloaded. This process repeats for the duration of the mission.

2. Triggered Event for C2

Another hybrid solution between C2 and autonomy is to designate a trigger. A trigger is something that causes the UxS to download its data to the operator. The forward unit can review that data and determine if the operator needs to take full control of the UxS. This scenario is depicted in Figure 11. The trigger could be the UxS arriving at a designated GPS coordinate, or something identified by an on-board AI system, such as image recognition of a target. This scenario could be useful in several applications. For example, in a use case where a weaponized UAS is used to seek out a target, the UAS can fly autonomously to the target to avoid generating an RF footprint that would reveal its location. Once the UAS reaches the target, the operator can assume control over the UAS to confirm the target and make the kill command.

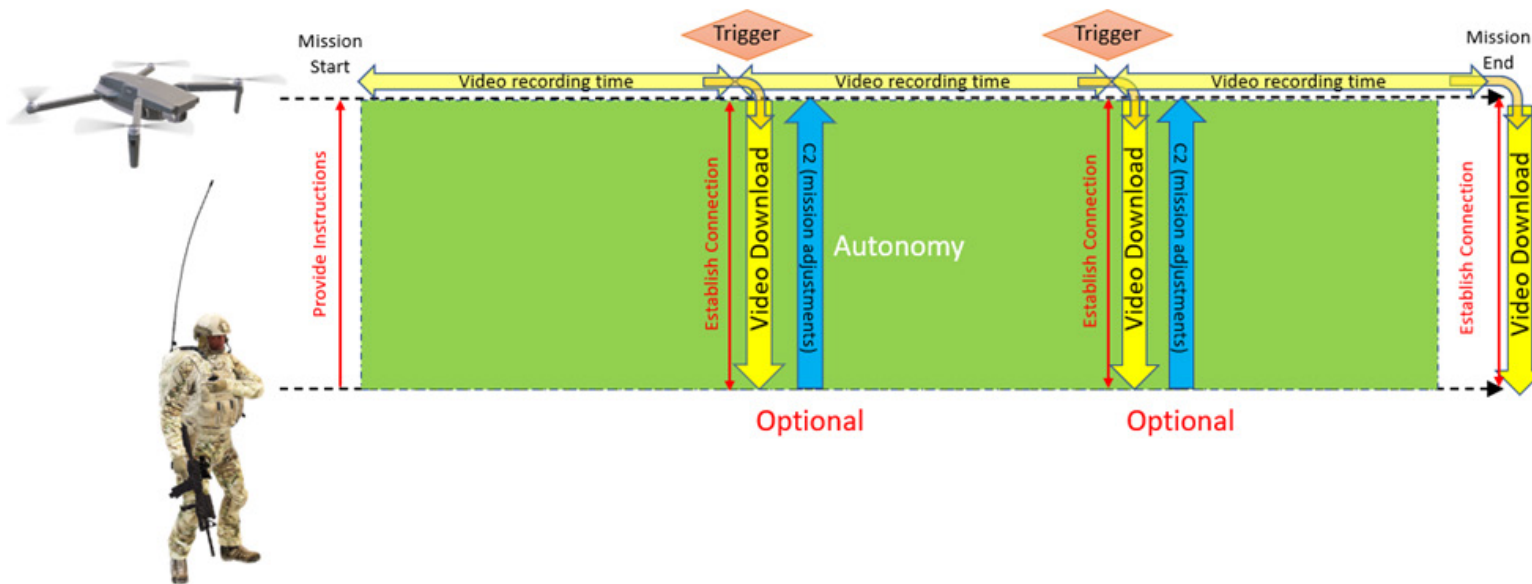


Figure 11. Operational Scenario of UxS Operation Using a Trigger Event for C2. The mission begins when the operator provides instructions to the UxS. The UxS operates under full autonomy while recording video for the duration of the mission as indicated in green. If the UxS detects a trigger during the mission, it establishes connection with the operator and the recorded video is downloaded for the operator to review. After reviewing, the operator has the option to assume C2 of the UxS or allow the UxS to resume autonomous operations. A trigger event can occur multiple times in a mission or might never occur. When the UxS returns to the operator at the conclusion of the mission, a connection is established between the operator and the UxS (wired or wireless connection) to enable the recorded video to be downloaded from the UxS. This scenario reduces the RF footprint while providing SA to the operator at critical moments.

E. UXS OPERATIONAL RISKS

There are several risks inherent to the operation of UxS in contested environments such as DMO/EABO. The primary risk of interest is enemy geolocation of the forward unit using the RF footprint generated during UxS operations. This research defines geolocation as “the problem of precise localization (or geolocation) of spatially separated sources emitting electromagnetic energy in the form of radio signals within a certain frequency bandwidth by observing their received signals at spatially separated sensors (or array elements) of the geolocation of RF signals system” (Progri 2011, 5). With this knowledge, the enemy can attack personnel, gain access to system networks, and potentially locate the COC and other forward units within the DMO/EABO. Geolocating the UxS is another concern. The enemy can locate the UxS and destroy it, capture data, and gain control of the UxS to use in a counterattack.

In addition to the primary geolocation risks, the research team examines the risk of cyberattacks. Each of the scenarios works with any security protocol or method. The combination of security protocol type and level of autonomy determines the RF footprint and the associated risks. A sample matrix of possible combinations is shown in Table 3.

Table 3. UxS Operational Risk Matrix

		Security Protocols and Methods			Risk
		TLS	PSK	MLS	
Level of Autonomy	Full C2	High	Medium	Medium	Geolocation
		High	Low	Low	DoS
		Medium	High	Low	Impersonation
	Hybrid	Medium	Medium	Medium	Geolocation
		Medium	Low	Low	DoS
		Medium	High	Low	Impersonation
	Full Autonomy	Low	Low	Low	Geolocation
		Low	Low	Low	DoS
		Low	Low	Low	Impersonation

F. CHAPTER SUMMARY

Chapter II defines the problem and sets the ground rule on the conduct of the project. It details the scope of work to be performed along with assumptions and constraints for conducting modeling and analysis for this project and examines the current capabilities employed today. Chapter II details the CONOPS and scenarios to examine in later chapters and sets their boundaries. It also details how the overall risk is assessed for each scenario to determine optimized solutions.

III. MODELING AND SIMULATION

Chapter III details the model architecture used to analyze the dangers of RF transmissions on the battlefield. The chapter defines the various parameters used in the model and describes the methods used to analyze the different protocols under consideration. Lastly, the chapter explains the model verification process and presents the simulation results.

A. MODEL REQUIREMENTS

Modeling and simulation are used to approximate the RF footprint created by each scenario and security protocol identified in Table 2. The model takes variable inputs to determine the resulting RF footprint.

1. Variable Inputs

Three main inputs are used for the model: scenario type, file size, and security protocol. CONOPS scenarios, as described in Chapter II Section D, are used as the operational blueprints for a variety of mission types. Several mission scenario types are developed to minimize risk during the mission. File size of the data being transferred, especially recorded video, is dependent on the scenario type and the duration the system is operating in an autonomous mode. The longer the system operates autonomously, the larger the file size for recorded video to be downloaded to the unit's C2 station. Security protocols are chosen from prior works/studies conducted on this subject/mission set. Focusing on a few specific protocols provides a sample across the space.

a. Scenario

The scenario input allows the user to select from the scenarios described in Chapter II, Section D. The percent autonomy can be set to any value between and including zero percent to 100 percent. Alternatively, the user can select the triggered event scenario. In the triggered event scenario, the model will run in an autonomous mode until a triggering event occurs. This triggering event is based on a probability that can be adjusted by the user of the model.

b. File Size

The model allows the user to manually input the size of the video file to be transmitted from the UxS based on the percentage of time the system will function in an autonomous verse C2 mode of operation in any given mission scenario. The video file size per unit of time is constant for all models, which is detailed further in Chapter III.B.1.c, but the unit of time for the recorded video is the driving factor for this variable.

c. Security Protocol

The user can select between three security protocols: TLS, PSK, and MLS. These protocols are selected because they exemplify basic differences in functionality among protocols available in the defense and private sectors and provide all the capabilities required for this type of system. Security protocols and methods provide confidentiality, data integrity, and authentication.

2. Desired Output

The purpose of these models is to simulate the RF footprint generated from each combination of inputs defined in Chapter III.A.1. For this research, the RF footprint is defined as the volume of C2 and video data transmitted by the forward unit's C2 system and UxS respectively. Although there are many factors that contribute to the overall RF footprint such as signal energy, type of waveforms used, and the portion of the electromagnetic spectrum used in transmission, this simplistic definition provides a rough approximation of the RF footprint to compare the results of using different security protocols for various mission types. The model simulates the RF footprint in three ways.

1. UxS RF footprint. The UxS RF footprint is approximated as the volume of live and recorded video data transmitted by the UxS. This approximation does not include the C2 data transmitted by the forward unit's C2 system. The UxS RF footprint is used to assess the risk of UxS geolocation and contributes to cyberattack vulnerability.

2. Forward Unit RF Footprint. Conversely, the forward unit RF footprint is approximated as the volume of C2 data transmitted by the forward unit's C2 system. It does not include the volume of video data transmitted by the UxS. The forward unit RF footprint is used to assess the risk of the enemy geolocating the forward unit and contributes to cyberattack vulnerability.
3. Total RF footprint. The total RF footprint includes both the UxS RF footprint and the forward unit RF footprint. The total RF footprint is used to compare the effects of the different inputs in the resulting RF footprint. It is also used to assess cyberattack risks.

B. MODEL PARAMETERS

1. Constants

There are several model parameters that remain constant regardless of the mission scenario and security protocol used. Constants have inherent, static properties that provide consistency to the model and simplify model simulation and computation. This section details the model's constants.

a. Total Mission Time

The Navy's Group 1 small UAS such as the RQ-12A Wasp IV and RQ-11B Raven have a runtime between 50 minutes and 3 hours (Naval Air Systems Command n.d.). A runtime of 100 minutes is set as a constant mission time for our model since it is a close approximation to the average runtime of Group 1 small UAS.

b. Step Size

The triggered event scenarios are the only models with a true step size construct. The step size, or amount of time the system takes to step through one full cycle of the model is set to a constant of one second. The smaller the step size, the more fidelity the model will have. This added fidelity increases the complexity of the model's simulation runs by requiring additional calculations, increasing required runtimes, and adding extra data to the output for examination. There is a point at which adding fidelity only adds

more work to the effort without producing the same increase in added benefits. The research team's choice of using a one second step provides the system model ample opportunity to detect a triggering event and start the process of transmitting the desired information back for further investigation and action if required. The models developed for this research are not overly complex; therefore, the team opted to choose higher fidelity in the models. If the models were more complex, further scrutiny of the step size would be warranted to balance fidelity with desired output and computational limitations. For these models to accomplish a 100-minute mission, they need to loop through this autonomous segment of the model 6000 times. Upon exiting the autonomous activity, the models enter the probabilistic trigger gate that is set to be triggered a certain percentage of times for the total mission. For the percent autonomy models, timing is set based on the desired percentage of time the system is to be used in an autonomous mode. Each model run for these scenarios requires input to the model depending on these factors.

c. Video File Size per Unit Time

Real world video files with the same resolution and recording times can vary in size due to the complexity of the scene content during the compression process. Details on the video and compression parameters for this model are detailed later in Section 3.b of this chapter. For consistency throughout all simulations, the file size of the recorded video is set to a standard 33 megabytes (MB) per minute (CircleHD 2019). This file size accounts for the video compression and is consistent with industry standards.

Video file size is determined by resolution, bit depth, and frame rate. Most Navy Group 1 small UAS are equipped with an electro-optical (EO) and infrared (IR) gimbal camera to provide visible and infrared imaging on the surrounding area for SA to the operator. The exact make and model of the EO/IR gimbal cameras used by the Navy are classified under Controlled Unclassified Information, which exceeds the classification of this report. This research leverages system specification of the USG-212 camera system from UAS components. The USG-212 is a commercially available camera system with similar applications to the Navy Group 1 small UAS. The USG-212 camera system delivers a 1920 x 1080 EO resolution and a 60 frame per second EO framerate (UAS

Components 2023). Since the EO/IR camera provides red, green, blue (RGB) imaging, the bit depth is determined to be 24-bits; 8 for red, 8 for green, and 8 for blue (Cornell University Library 2003).

d. Data Rate

In addition to file size, the model also relies on a constant data rate. Data rate is the number of bits processed per unit of time. UxS are commonly operated at a frequency of 2.4 gigahertz (GHz) (Yang et al. 2021, 1678). Higher frequencies offer faster video transmission, but their range is limited and can be severely affected by geographical features (911 Security 2023). A 2.4 GHz frequency can support multiple video transmission data rates; however, readily available hardware typically supports 100 megabits per second (Mbps) (Suntor 2023). One hundred Mbps provides a high enough data rate to allow for quick video downloads/transmission without falling prey to unreliable connections due to distance or geography.

2. Data Transmission Packet Size

Data is transmitted in application packets consisting of the C2 or video data and additional overhead determined by each protocol's specification such as cipher suite overhead and protocol options. The maximum packet size for TLS is 16 kilobytes (kB) (RFC 8446 2018). To reduce model complexity, 16 kB is used as the application data packet size for all models prior to the addition of the protocol overhead.

Data transmission packets are examined with a network analyzer tool and cross compared to their respective protocol specifications to establish and verify the model's parameters for data transmission are accurate and representative of real-world data. This verification process is detailed in Chapter III.D and identifies the TLS data packet overhead as 200 bytes and the MLS data packet overhead as 171 bytes. Due to limited resources, the PSK overhead is not verified. This research assumes PSK uses the same cipher suite as TLS, so the PSK overhead is set to 200 bytes.

3. Mission Data Types

As stated in Chapter II, UxS operations rely on two types of data links, CNPC link to exchange C2 information and a data link to exchange video and still image captures for SA. Details on the different data exchanges used in this model are provided in Chapter III.B.4 along with assumptions and rationale as to why certain parameters or values are used.

a. CNPC Data

CNPC data between the forward unit's C2 station and a UxS is typically small compared to other types of data being exchanged such as video. The effective tactical data rate between a C2 station and a Group 1 small UASs is between 27 and 100 kilobits per second (kbps) (Dinc, 2009). This model sets the data rate as a constant in the middle of those values at a rate of 50 kbps to stay on the conservative side.

b. Video

The intelligence data under consideration for this research is limited to video (live feed & recording downloads). Other intelligence data such as radiological detection could be considered but those are not as common and are not as taxing for transmission bandwidth requirements. Video data is commonly used for UxS operations.

(1) Video Data

For this model, the research team chooses to model the UxS with a standard full color High Definition (HD) camera with a resolution of 1920 x 1080, a bit depth of 24 (8 bits per red, green, and blue channels), and a standard frame rate of 30Hz. Other video format resolutions such as 4k are considered but the research team determines full HD cameras provide adequate resolution for this mission type, are commonly available, low power, and have relatively low bandwidth requirements compared to larger formats. A comparison of available video formats is presented in Figure 12. Other camera sensors are considered such as Long-Wave Infrared (LWIR) sensors which can be utilized for both day, night, and obscured (tactical smoke cover) operational scenarios. Many UxS systems have both camera types that are used in a "one or the other" configuration at any

given time, but since LWIR video only comes in mono-chrome format, a color camera of the same resolution produces larger file sizes for the same length of video therefore increasing bandwidth requirements for transmission. This research uses only full color HD data for ease of modeling and its higher potential to impact the overall RF footprint during operations.



Figure 12. Video Formats. Source: Typito (2020). Various video format resolutions considered for modeling to determine UxS data and bandwidth requirements for modeling and simulation.

(2) Video Compression

Video data consists of large amounts of data that need to be stored and transmitted. To reduce the storage size and ultimately the amount of data required to be transmitted from the UxS to the C2 station, the H.264 video compression standard is used for the model. H.264 is an industry standard with higher performance over other less efficient video compression standards such as MPEG-2. Compression ratios of up to 2000:1 are achievable with H.264 but at the detriment of video quality after decompression. Typical “lossless” compression ratios range from 2:1 to 20:1 and “lossy” ratios range from 20:1 to 2000:1 depending on scene content. This model uses a ratio of

25:1, which is on the conservative side of the lossy range. Table 4 presents a summary of the video data variables used for this model development.

Table 4. Video Information

UxS Video Information		
Video Data Variable	Value	Units
Resolution	1920 x 1080	Horizontal x Vertical pixels
Bit Depth	24	bits (8-Bit x RGB)
Frame Rate	30	Frame per second
Raw File Size	1492.992	Mbps
1 min of Raw Video	89579.52	Mbps
Compression Ratio	26:1	
Compressed File Size	57.4 7.4625	Mbps MB per second

(3) Live Video

For the identified operational scenarios, live video feed from the UxS to the forward unit's C2 station occurs 100% of the time while the UxS is linked and communicating with the C2 station. This operation is not necessarily required. The system could be controlled without live video feed. This research includes live video in the model to assess its contribution to RF footprint and SA.

Transmission of compressed live video feed requires a bandwidth of 57.4 Mbps as detailed in Table 4. The compressed live video feed bandwidth requirement is in addition to the bandwidths required for CNPC data transmission and the recorded video file download which occur simultaneously.

(4) Recorded Video

For each CONOPS scenario, video is recorded for the entire mission duration and stored internally to the UxS for download upon mission completion. During mission operations, only portions of the recorded video that occurred during autonomous operations are transmitted to the forward unit's C2 station upon the initial C2 connection after an autonomous action. The forward unit's C2 station records the live video

transmission when received thus reducing the amount of data required for transmission. This action results in a lower RF footprint and reduced bandwidth requirements. The recorded video file size is determined in the same way live video size is determined. The difference is the recorded video file is accumulated into a single file for the duration of the recording cycle. Figure 13 depicts the video transmission and recording timeline for a percent autonomy scenario.

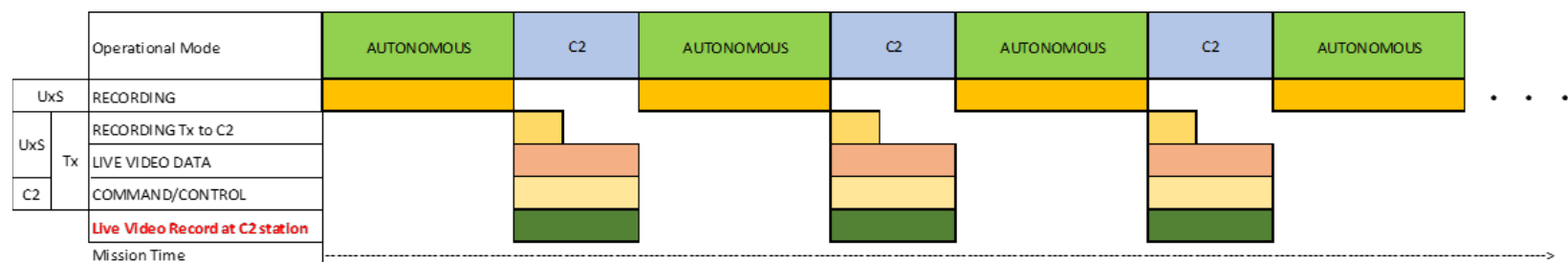


Figure 13. Video Transmission and Recording Timeline

C. MODEL DEVELOPMENT

The research team develops the models for this project in Innoslate model-based systems engineering (MBSE) tool developed by SPEC Innovations. Innoslate is a web-based tool and due to some of its limited capabilities, the research team elects to create several smaller models, one for each security protocol with variable autonomy, rather than making one large model with several security protocol and autonomy options. The initial models simulate scenarios 1a, 1b, and 1c previously defined in Chapter II. These models are referred to as percent autonomy models from herein. Scenario 2 is simulated using separate models, referred to as triggered event models. The development of the TLS percent autonomy models and TLS triggered event models is detailed in Chapters III.C.1 and III.C.2. Development of the MLS and PSK models are detailed in Appendix A and Appendix B respectively.

1. TLS Percent Autonomy Model Details

The top-level TLS percent autonomy model is shown in Figure 15. In this section, a description of each step of the model is presented and overall operations are explained. The standard flow of operations for the MLS and PSK percent autonomy models generally follow these same steps with the only difference being the security protocol. Data type, file & data size, transmission bitrate and mission timing are all the same.

While developing these models, the research team quickly realized simulation of a 100-minute mission that delves down to the byte level of transmission presents an issue. Simulations at that level result in extremely long runtimes that usually ended up crashing the Innoslate modeling tool and requires the research team to try again. To help alleviate this issue, the 100-minute mission model is broken down into 10-minute segments which can be adjusted afterwards to account for a full mission. Additionally, certain activities within the model are examined and adjusted to further reduce simulation runtime and computational requirements. The final adjustment to the model is to multiply the data transmission loop (block F.4.1.2 of Figure 15) by 100 to alleviate this issue. Figure 14 depicts the TLS communication timing sequence to illustrate the back-and-forth data transfer between the C2 unit and the UxS, it is a representation for how the model works.

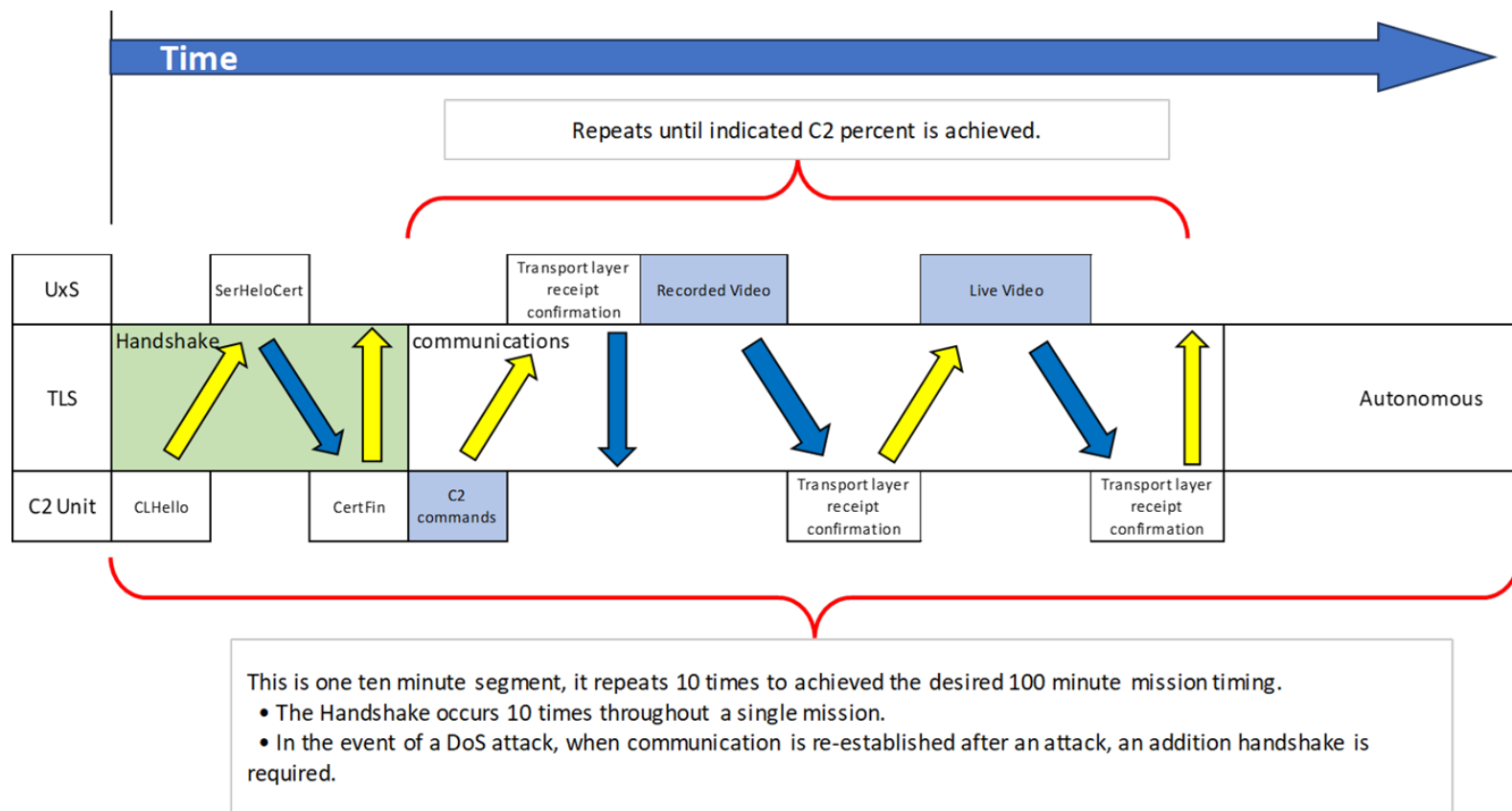


Figure 14. TLS Communication Sequence

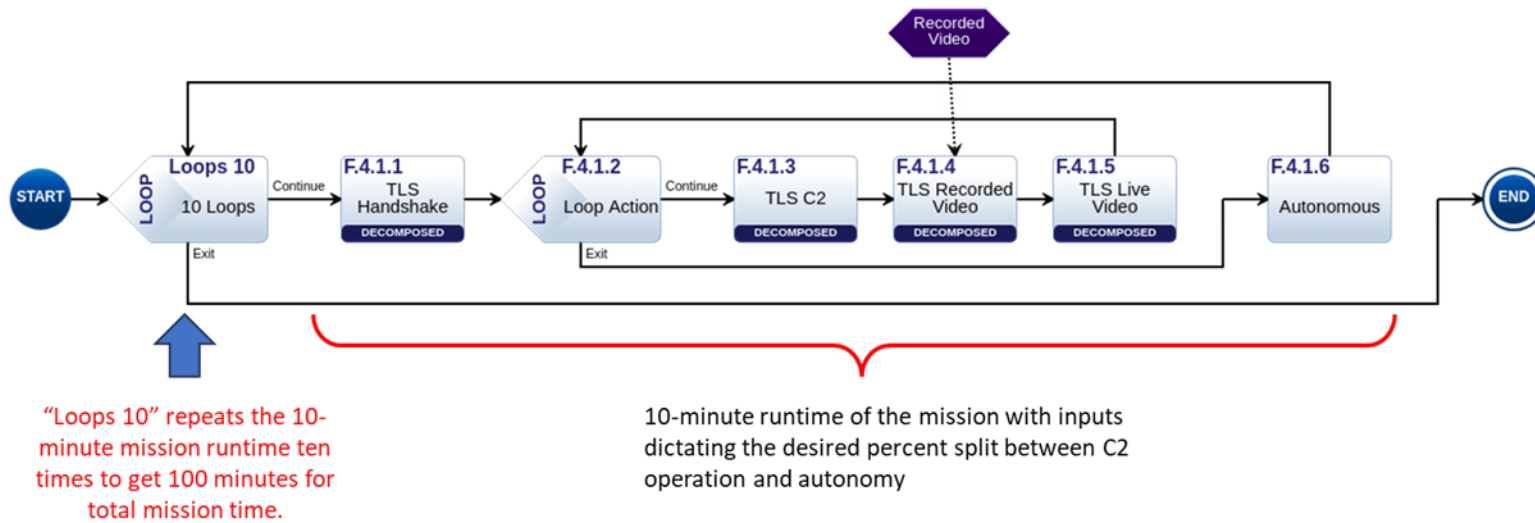


Figure 15. TLS Percent Autonomy Innoslate Model

a. ***TLS Handshake (F.4.1.1)***

The first action to occur is the “Handshake” (F.4.1.1) which establishes a secure communication pathway. The handshake occurs once at the beginning of every C2 to UxS initiation. The number of C2 to UxS initiations is determined by how many times the system cycles between C2 and Autonomous modes during mission operations. The number of cycles is predetermined by the percentage split of C2 to UxS operations provided by the user as input to the model. In this scenario, the C2 station transmits the appropriate “Client Hello, Key Share” signal to the UxS. Next, the UxS replies with the “Server Hello, Key Share, Certificate, and Finished” signal. Lastly, the C2 station transmits a signal authenticating and confirming the handshake integrity completing the handshake and allowing the model/simulation to progress to the next action block, the loop action, where data can be transmitted with security (RFC 8446 2018). The TLS Handshake action is depicted in Figure 16. Action block F.4.1.1.4 transmits the “Client Hello” portion of the handshake which is 571 bytes in size. Next, the UxS in block F.4.1.1.2 replies with a “Server Hello” message to the C2 unit, which is 1466 bytes in size. Lastly, the C2 unit (block F.4.1.1.5) authenticates the connection with a “Finished” message that is 52 bytes in size to establish a secured link. The number of bytes transmitted during the handshake is verified using Wireshark as detailed in Chapter III.D.2.

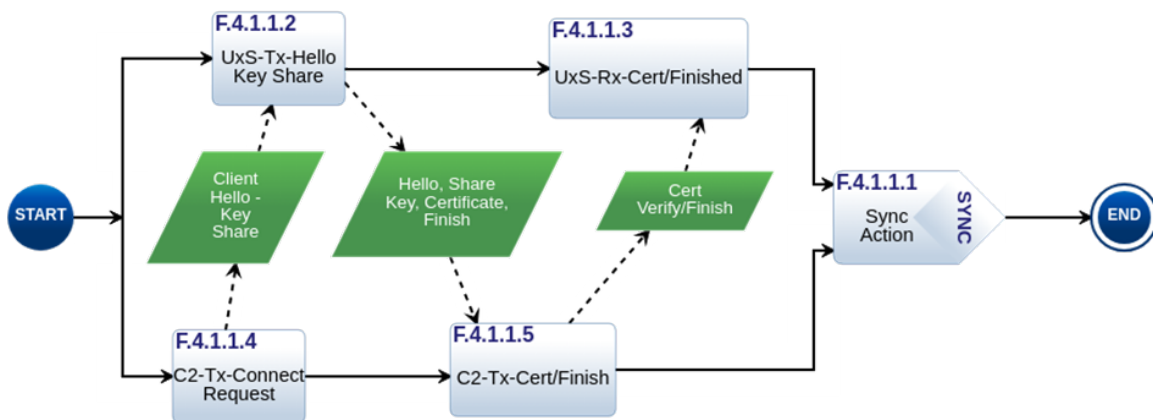


Figure 16. TLS Handshake (F.4.1.1)

b. TLS Command & Control and Autonomous Operation Timing

From Figure 15, the Loop Action (F.4.1.2) determines the length of time the UxS is controlled by the forward unit providing C2 to the UxS and receiving real time SA data from the UxS. Parameters internal to F.4.1.2 are manipulated to obtain the correct percentage balance between C2 and Autonomous operation for various model runs. Each action inside this loop block runs sequentially one time before looping back to repeat again and again until the predetermined C2 timing is satisfied for a particular simulation run. When the timing requirement is satisfied, the model leaves the loop, and the system enters the autonomous mode of operation. The actions and behaviors internal to the loop operation include: C2 data transmission, recorded video (download), and live video operations. These actions and behaviors are detailed in Chapters III.C.1.c through III.C.1.e.

c. TLS C2 data transmission

TLS C2 data transmission is represented in Figure 15 as F.4.1.3. Internal details on the actions that occur during this activity are shown in Figure 17. During this activity, the forward unit sends C2 command messages to the UxS to adjust UxS mission parameters and operational actions in real-time. Upon receiving the C2 command signal, the UxS returns an acknowledgement signal indicating the command was received correctly and that a resend of that same command signal is not necessary before exiting to the next operation. At this point, the model moves to the next operational block, transmission of recorded video from the UxS to the C2 station.

Since the C2 and live video signals require a constant data rate of information flow, 50 kbps and 57 Mbps respectively, while the recorded video can be sent at any rate until download is complete, this caused a problem in the model resulting in an inflated overhead count for the C2 signal. The C2 signal is very small compared to the video signals, to establish the correct bit rate for the C2 signal, each loop of data transfer only requires 14 bytes of actual C2 data compared to 16 kB for live video and roughly 11 kB for recorded video. This means that each 14-byte C2 packet gets an additional 200 bytes of overhead data that TLS requires grossly inflating the C2 transmission times. Since this

is not realistic or practical in real world applications, a scaling factor was applied to the C2 overhead signal resulting in one C2 data packet of 16 kB only requiring one overhead byte count of 200 bytes.

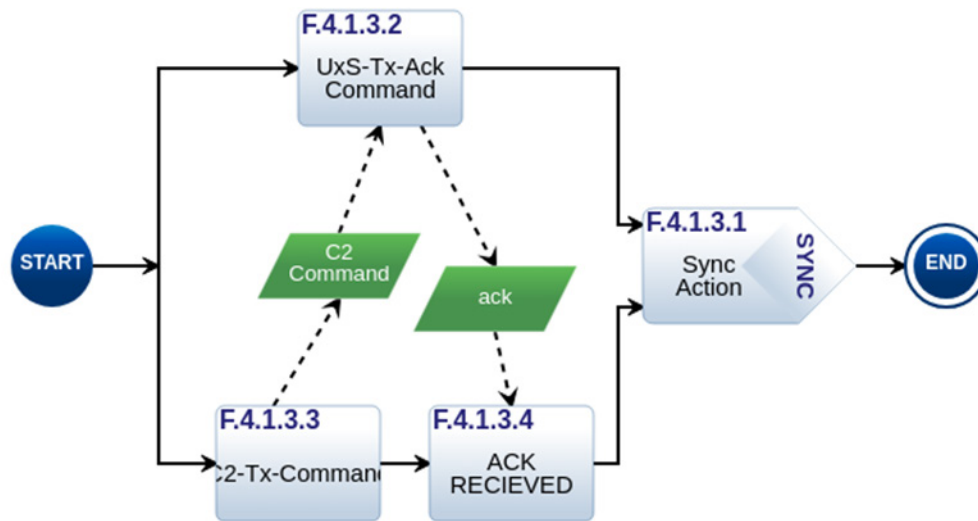


Figure 17. TLS C2 Data Transmission Model (F.4.1.3)

d. *TLS Recorded Video Transmission*

Figure 18 shows the recorded video transmission operation of the model. This operation is shown in Figure 15 as F.4.1.4. Video is recorded and transmitted for the autonomous duration of a mission. The recorded video file is represented as the purple “Recorded Video” resource block shown in Figure 18. The parameters of this resource block are set for each simulation and depend on the length of time the system operates in autonomous mode before C2 initiations during the mission. The model limits the number of C2 initiations to ten for every simulation for ease of implementation and minimal complexity. The input to the resource block is the predetermined file size in bytes. Each time the model cycles through this operation, a set number of bytes is subtracted from the resource block which is dependent on which communication/security protocol is used.

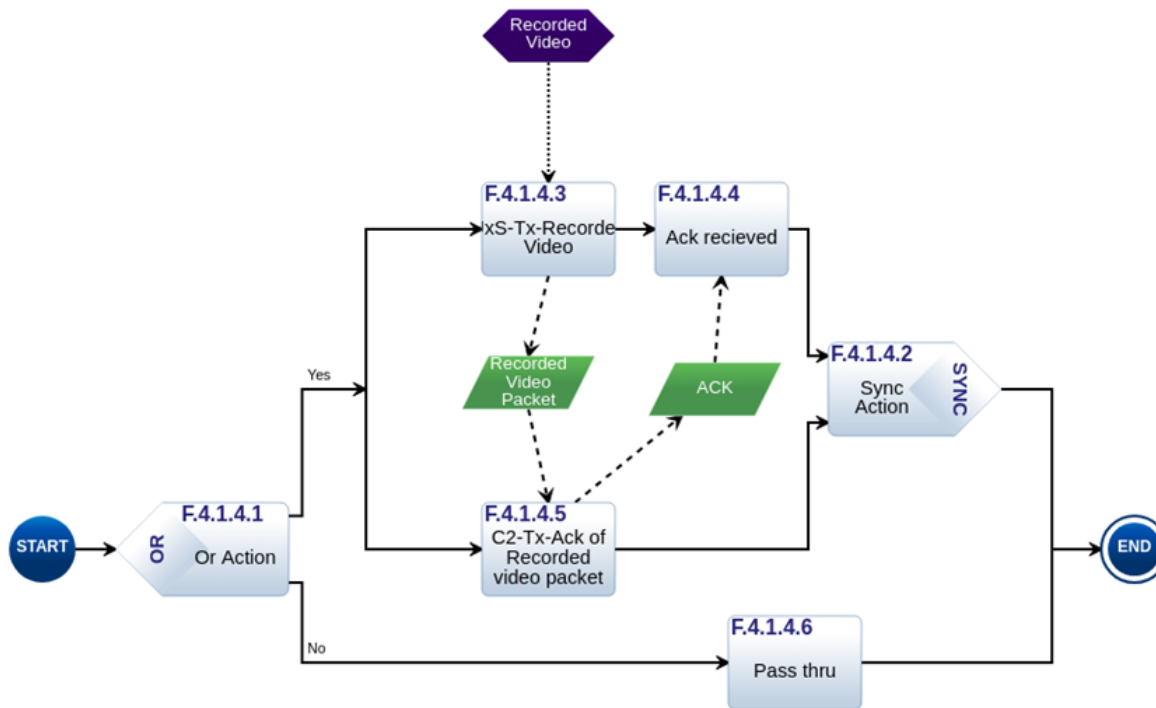


Figure 18. TLS Recorded Video Transmission (F.4.1.4)

Upon entry into this operation, if the recorded video file size is greater than zero, the “YES” path from the “OR” block (F.4.1.4.1) operator will be chosen. This path results in the UxS transmitting one packet of recorded video to the C2 personnel, then receiving an acknowledgement signal from the C2 station to confirm successful transmission before exiting the block for the next operation. After the video download is complete, any additional cycles through this operation will result in the “OR” block to choose the “NO” path (recorded video size =0) to skip further attempts to transmit data, eliminating this step from the rest of C2 control process.

e. *TLS Live Video Transmission*

Upon exiting the recorded video transmission operation (F.4.1.4), the system transmits one packet of real-time live video so the C2 personnel have SA while they’re linked and communicating with the UxS. Figure 19 shows the internal processes for this portion of the mode. This block runs for the entire time C2 personnel are communicating with the UxS. In this operation, live video is transmitted from the UxS to the forward

unit's C2 station which in turn sends an acknowledgement signal back to the UxS much like the recorded video transmission detailed in Chapter III.C.1.d. The live video bandwidth required for video of this resolution and bit depth is detailed in Table 4 and will remain constant, this will limit the bandwidth available for transmitting the recorded video file.

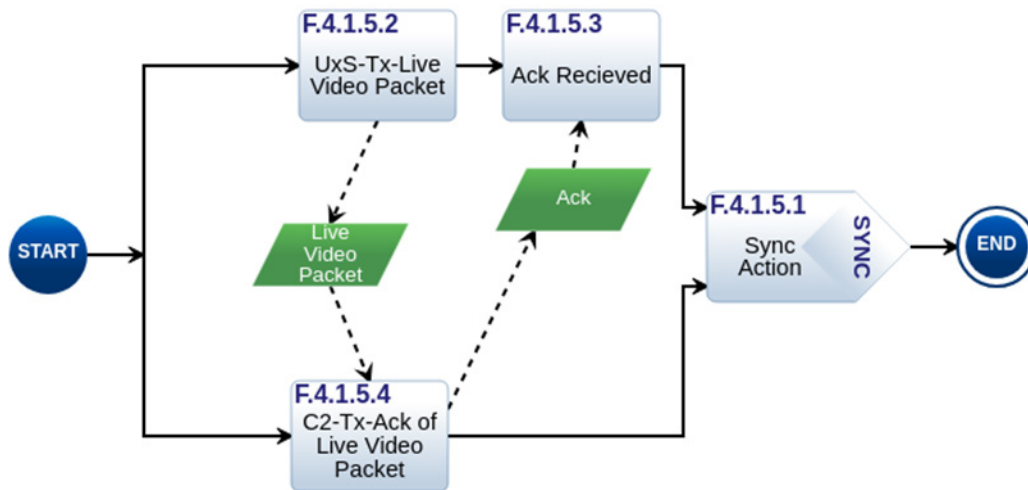


Figure 19. TLS Live Video Transmission (F.4.1.5)

Upon exiting this live video transmission block, the next operation depends on whether the system has met its time or percentage requirement for C2 operations. If it has, the system will move to autonomous operations next, if not, it will continue the loop until it does.

2. TLS Triggered Event Model

As detailed Chapter II.D.2, the “Triggered Event Model” is a scenario where either an object is identified by the UxS using some level of on-board AI, such as image recognition of a target, or when the UxS arrives at a designated GPS coordinate. The triggering artifact will cause the UxS to download data to the operator for evaluation to determine if the detected object is of operational interest and needs further investigation. If further inquiry is needed, C2 personnel can take full control of the UxS to do so.

To keep simulations comparable from one run to the next, the model does not exercise the further investigation pathway if a triggering event occurs. Figure 20 shows the top-level operational steps for this scenario.

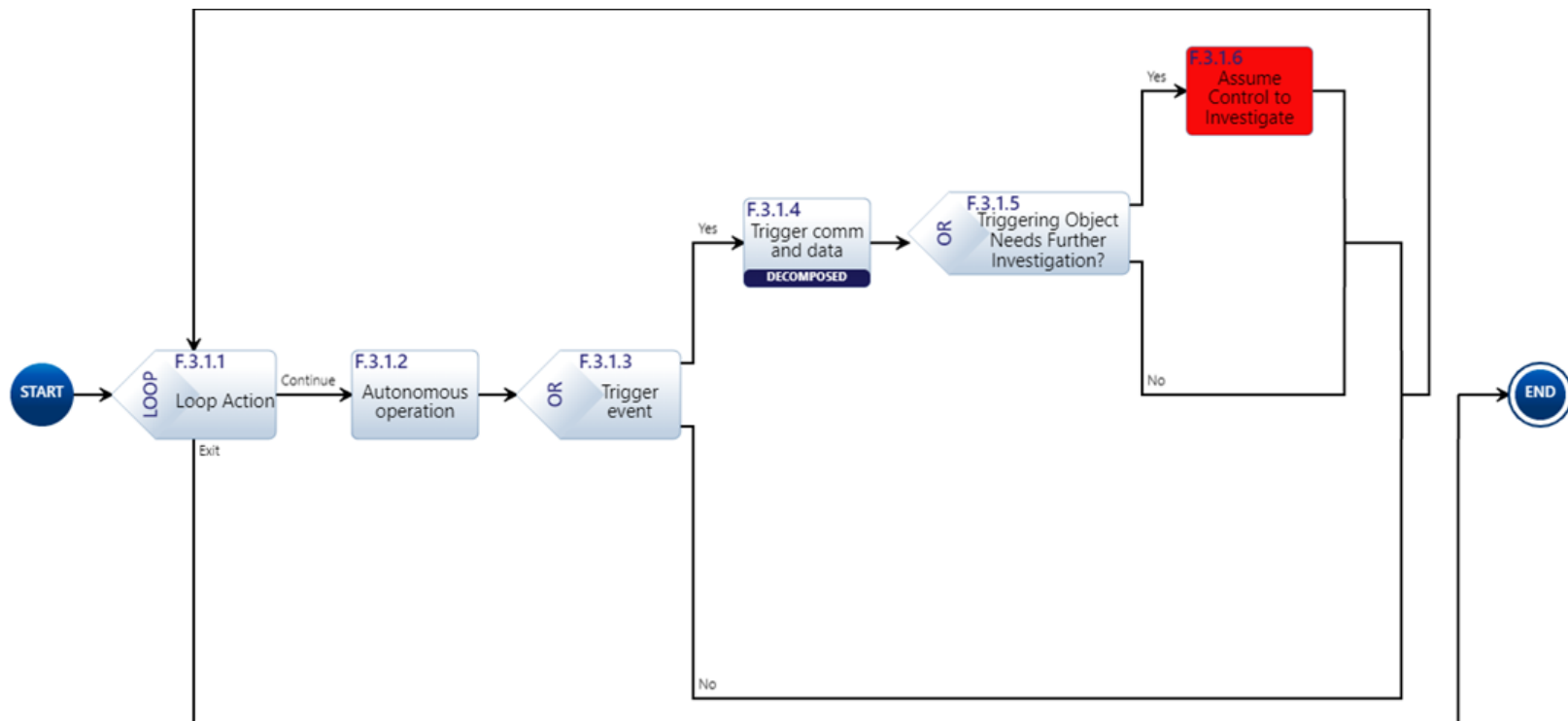


Figure 20. TLS Triggered Event Innoslate Model

a. TLS Trigger Autonomous Operation & Triggering Event

The autonomous operation shown in Figure 20 as block F.3.1.2 represents the time the UxS is operating in an autonomous mode that is free of any transmitted RF signals. The duration of this activity can be set to any value and is dependent on overall mission parameters. Block F.3.1.3 is a probabilistic determination on whether a triggering event occurs during the mission. This probability can be set anywhere between zero and one hundred percent depending on the expected threat level for any given mission. The research team chooses to use a probability that results in an average mission having ten triggered events. As detailed in the following section, each triggered event will result in three minutes of mission video to be transmitted back to the C2 personnel for evaluation and mission adjustment if it is deemed necessary. Ten triggering events was chosen by the research team as it will equate to a total of 30 minutes of mission video (equates to 990 MB of video data and 30% of the 100-minute mission time) to be sent back to the C2 team and limit the transmission time from the UxS to keep the approximate RF footprint low. The research team assessed this as a reasonable balance to compare the impacts of using these protocols in this scenario.

b. TLS Triggered Communications

In the event a triggering event occurs, the model enters the “Trigger Comm and Data” activity block shown as F.3.1.4 in Figure 20 and is decomposed into its smaller activities shown in Figure 21 and Figure 22. Once this activity is initiated, the TLS Handshake occurs to establish a secure communication channel. The TLS handshake, F.4.1.1, is the same activity detailed earlier in Chapter III.C.1.a. After successful completion of the handshake, the UxS proceeds to transmit the relevant data that caused the trigger for further examination by C2 personnel. For the purposes of this project and to keep consistency with each simulation, the research team chooses to make all the triggered downloads three minutes of recorded video. The rationale for three minutes is to help provide the time just before and after the triggered event to provide some context to the data. After download is complete, the C2 personnel have the option to take control or let the system continue to operate autonomously.

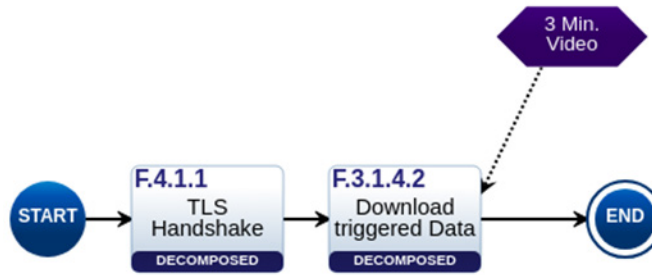


Figure 21. Triggered Communications and Data (F.3.1.4)

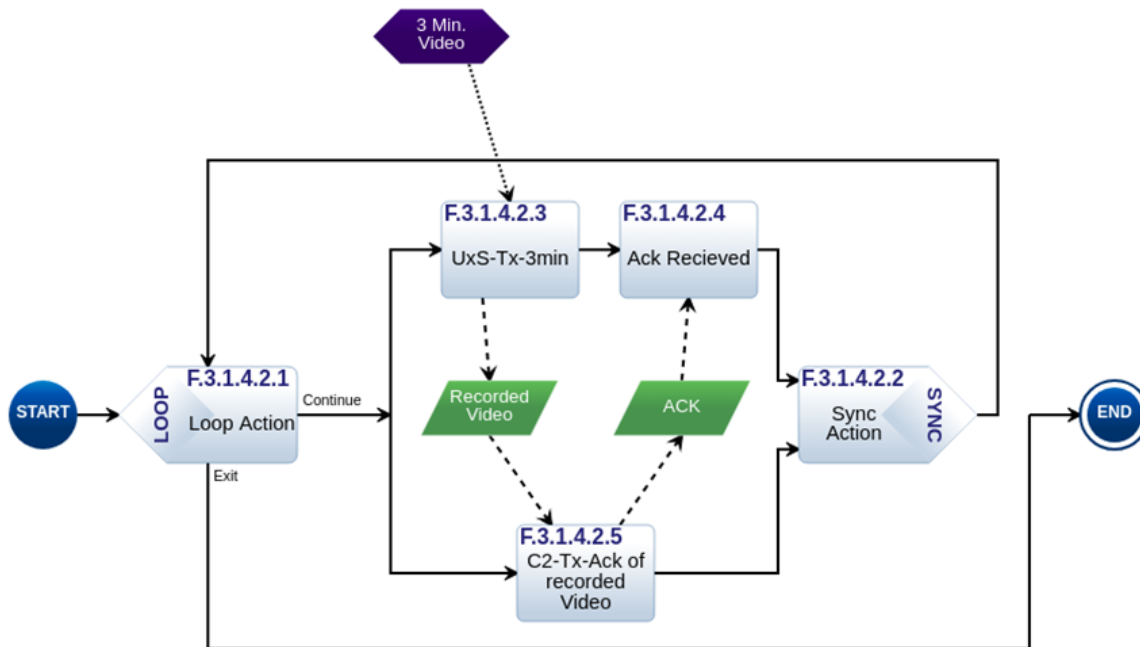


Figure 22. Download Triggered Data (F.3.1.4.2)

3. Denial-of-Service Model

To assess the impact of an adversary's DoS attack on the mission profiles, the research team develops a DoS model, shown in Figure 23, to randomly generate when an attack occurs and the duration of an attack during a typical 100-minute mission. Parameters are set in the model to adjust the probability of attack and the duration of each attack with a mean and standard deviation on timing. The parameters selected for the model produce an average of 6 attacks per 100-minute mission. An average of six attacks represents a highly contested scenario and provides a conservative analysis of risks. In

practice, the average number of attacks is likely lower. The duration of the attacks is assigned a normal distribution of five minute and a standard deviation of 30 seconds. There are two strategies of DoS attacks: long, prolonged attacks and frequent short attacks (Cook, 2023). Cloudflare, an information technology service management company, found that the average DoS in 2022 lasted 390 seconds (6.5 minutes) (Cook, 2023). A DoS attack duration of 5 minutes was selected for the model because it is a close approximation to the reported average DoS attack duration and is easily computed in our model which computes the RF footprint for a given mission scenario in 10-minute segments. Additionally, these models do not incorporate DoS mitigation techniques and procedures. Future research is recommended to conduct a sensitivity analysis and determine more appropriate values. The timing output of this model is shown in Figure 24 and is used on all the models to assess this attack scenario and to maintain an “apples to apples” comparison on the effects to the missions.

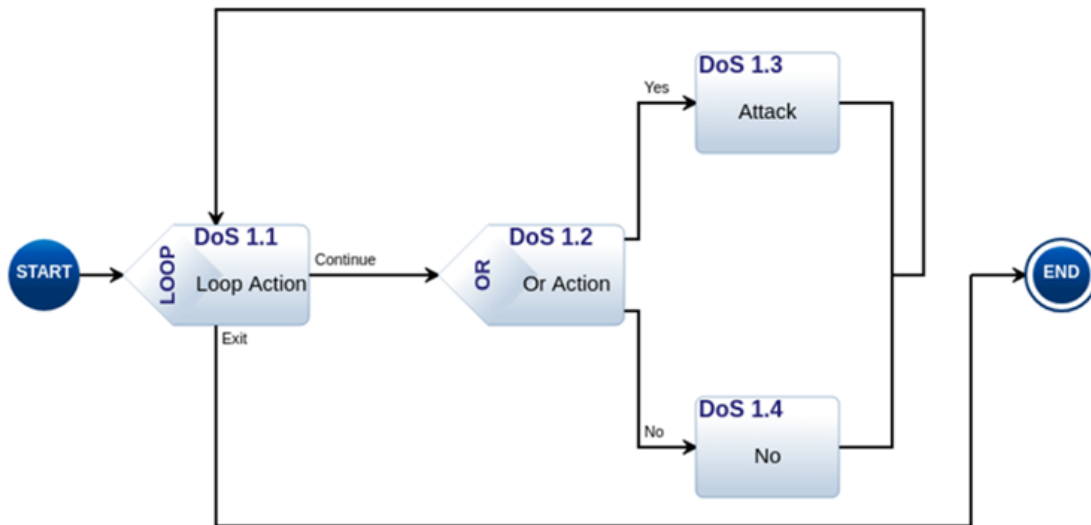


Figure 23. DoS Timing Innoslate Model

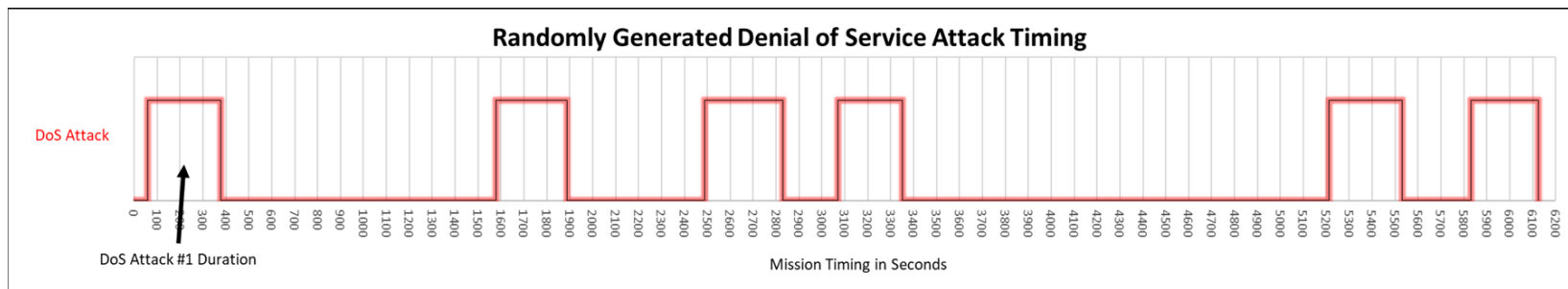


Figure 24. DoS Model Timing Output Used to Assess Impact on Mission Models

D. MODEL VERIFICATION

This section details the model verification process. By verifying the model, the research team ensures the model outputs are representative of real-world results. This research compares security using TLS, MLS, and PSK to encrypt data. Additional networking layers may be required for functionality and influence RF footprint, however these additional layers are not considered in this research to ensure an “apple-to-apples” comparison between the selected protocols and methods as a security approach. Wireshark is used to determine the data overhead required by the MLS and TLS protocols to transmit data. Of note, the implementation of MLS scanned on the network is not optimized nor does it include a delivery service; however, it provides a touchpoint for basic protocol comparison. Verification of the PSK data overhead requires additional tools and resources unavailable to the research team at the time of this research. For the purposes of this research, the PSK channel security overhead is assumed equivalent to the TLS overhead of 200 byte, such as when a PSK key is installed via a keyloader and used with a TLS record layer protocol. After verifying the protocol data packet overheads, the completed models are verified to ensure the results are accurate.

1. MLS Overhead Verification

This research leverages previous research from Andre Leon and Christopher Britt. To verify the correct overhead is applied, a chat environment using MLS protocol for security and implementation is created. The simulation environment consists of two virtual machines (VM) connected to the same wireless network and within the same subnet. Both virtual machines have Ubuntu 18.4 operating systems. One (1), 1885-byte plaintext message is sent from the server to the client and analyzed with Wireshark as shown in Figure 25. The results show that 171 bytes are added to the overall frame from the X25519 AES 128GCM SHA 256 Ed25519 cipher suite (Leon and Britt 2022). These additional 171 bytes are used as the packet overhead in the MLS models.

No.	Source	Destination	Protocol	Length	Info
1	10.0.2.8	10.0.2.15	TCP	74	47650 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1645144610 TSecr=0 WS=128
2	10.0.2.15	10.0.2.8	TCP	74	8080 → 47650 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3670533517 TSecr=1645144610 WS=128
3	10.0.2.8	10.0.2.15	TCP	66	47650 → 8080 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1645144610 TSecr=3670533517
4	10.0.2.15	10.0.2.8	TCP	2122	8080 → 47650 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2056 TSval=3670533518 TSecr=1645144610
5	10.0.2.8	10.0.2.15	TCP	66	47650 → 8080 [ACK] Seq=1 Ack=2057 Win=63488 Len=0 TSval=1645144611 TSecr=3670533518
6	10.0.2.8	10.0.2.15	TCP	309	47650 → 8080 [PSH, ACK] Seq=1 Ack=2057 Win=64128 Len=243 TSval=1645144612 TSecr=3670533518
7	10.0.2.15	10.0.2.8	TCP	66	8080 → 47650 [ACK] Seq=2057 Ack=244 Win=65152 Len=0 TSval=3670533519 TSecr=1645144612
8	10.0.2.15	10.0.2.8	TCP	934	8080 → 47650 [PSH, ACK] Seq=2057 Ack=244 Win=65152 Len=868 TSval=3670533523 TSecr=1645144612
9	10.0.2.8	10.0.2.15	TCP	66	47650 → 8080 [ACK] Seq=244 Ack=2925 Win=64128 Len=0 TSval=1645144616 TSecr=3670533523

Figure 25. MLS Wireshark Analysis

2. TLS Overhead and Handshake Verification

The research team utilizes Wireshark to examine the TLS 1.3 packets, specifically the Client Hello key exchange. Figure 26 shows the length of a 1466-byte packet. The TLS overhead is identified as 200 bytes and is comprised of the X25519 AES 128GCM SHA 256 Ed25519 cipher suite used in the key agreement and the packet header overhead. For the handshake, the “client hello” is identified as 571 bytes and the “server hello” is identified as 1466 bytes. Lastly, the “Finished” message size is identified as 66 bytes. The Client Hello and Server Hello varies and is dependent the on the supported cipher suites, TLS version, random data, supported extensions, and session ID.

No.	Source	Destination	Protocol	Length	Info
1	192.168.1.176	142.250.176.194	TCP	66	59938 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	142.250.176.194	192.168.1.176	TCP	66	443 → 59938 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
3	192.168.1.176	142.250.176.194	TCP	54	59938 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4	192.168.1.176	142.250.176.194	TLSv1.3	571	Client Hello
5	142.250.176.194	192.168.1.176	TCP	54	443 → 59938 [ACK] Seq=1 Ack=518 Win=66816 Len=0
6	142.250.176.194	192.168.1.176	TLSv1.3	1466	Server Hello, Change Cipher Spec
7	142.250.176.194	192.168.1.176	TCP	1466	443 → 59938 [PSH, ACK] Seq=1413 Ack=518 Win=66816 Len=1412 [TCP segment of a reassembled PDU]
8	192.168.1.176	142.250.176.194	TCP	54	59938 → 443 [ACK] Seq=518 Ack=2825 Win=131072 Len=0
9	142.250.176.194	192.168.1.176	TCP	1466	443 → 59938 [ACK] Seq=2825 Ack=518 Win=66816 Len=1412 [TCP segment of a reassembled PDU]
10	142.250.176.194	192.168.1.176	TLSv1.3	351	Application Data
11	192.168.1.176	142.250.176.194	TCP	54	59938 → 443 [ACK] Seq=518 Ack=4534 Win=131072 Len=0
12	192.168.1.176	142.250.176.194	TLSv1.3	118	Change Cipher Spec, Application Data
13	142.250.176.194	192.168.1.176	TLSv1.3	668	Application Data, Application Data
14	192.168.1.176	142.250.176.194	TCP	54	59938 → 443 [ACK] Seq=582 Ack=5148 Win=130560 Len=0

Figure 26. TLS 1.3 Overhead and Handshake Verification

3. Model Verification

TLS requires a handshake at the start of the mission to establish connection. As detailed in Chapter III.C, this handshake occurs a minimum of 10 times in the percent autonomy model. Additional occurrences of the handshake may occur because of a DoS attack. Each instance of the handshake adds to the total data transmitted during the mission. PSK relies on manual distribution of key prior to the start of the mission, eliminating the handshake. Since the PSK model has the same data packet overhead as the TLS model, but eliminates the handshake, the PSK model should result in a lower data transmission volume compared to the TLS model.

MLS relies on a continuous key agreement instead of a handshake like TLS. The frequency of key updates is set by the user. For this research, the MLS key update occurs at the beginning and end of each mission and is excluded from the model. Because the MLS key updated is excluded from the model and MLS requires a smaller data packet overhead than PSK, MLS is expected to have the lowest volume of data transmission.

The model results are examined to ensure these comparisons exist. Table 5 shows a small sampling of the model data examined during verification. TLS results in the highest volume of data transmission and MLS results in the lowest volume of data transmission as expected. An additional verification check includes making sure the data volume decreases as percent autonomy increases. The data in Table 5 follows this expected trend. The data transmitted is greatest at 0% autonomy and decreases for each subsequent row in the table.

Table 5. Sampling of Forward Unit C2 Total Data Transmission from Model Data without DoS Attacks for Verification

Percent of Mission Conducted in Autonomous Mode	TLS (MB)	PSK (MB)	MLS (MB)
30	26.854	26.847	26.573
40	23.026	23.020	22.781
50	19.185	19.170	18.975

E. SUMMARY OF MODEL ASSUMPTIONS

This section summarizes the assumptions made in model development that impact the results and analysis of this research. The results and analysis are only valid for scenarios matching these assumptions.

1. Definition of Autonomy

There are many ways in which to model autonomy. This research models a 100-minute mission as ten-minute intervals. Within each ten-minute interval, operations occur in C2 mode, autonomous mode, or a combination of both. In C2 mode, the UxS receives C2 signals from the operator that consists of low data rate control signals that are used for the physical maneuvers and operation of the UxS while the UxS transmits recorded and live video back to the C2 personnel. These operations occur in series as depicted in Figure 15. First, a C2 data packet (14 bytes excluding overhead) is transmitted from the C2 station to the UxS. Next, the UxS transmits a recorded video packet (11,300 bytes excluding overhead). Lastly, the UxS transmits a live video packet (16,000 bytes excluding overhead) before the process repeats with the next C2 data packet. In autonomous mode, the UxS records video. The recorded video is downloaded to the forward unit C2 station the next time the UxS enters C2 mode. For example, at 0% autonomy, operations occur in C2 mode for the full ten-minute interval and repeated for the subsequent intervals. Conversely, at 100% autonomy, operations occur in autonomous mode for the full ten-minute interval and repeated for the subsequent intervals. At intermediate levels of autonomy such as 50% autonomy, operations occur in C2 mode for 50% of the ten-minute segment of time (five minutes) before switching to autonomous mode for the remaining time of the interval. At 60% autonomy, operations occur in C2 mode for 40% of the ten-minute segment of time (4 minutes), before switching to autonomous mode for the remaining time of the interval. This alternation between C2 and autonomy occurs for each subsequent ten-minute interval throughout the total mission. The duration of C2 mode operations determines the number of C2 data packets and live video data packets exchanged. Operations at 50% autonomy will result

in increased C2 and live video data packets compared to operations at 60% autonomy which results in an increased number of recorded video packets.

2. Handshake and Key Exchange Frequency

The simulated RF footprint results and risk analysis contained in this research are impacted by the timing and frequency of the security protocol handshake or key exchange. UxS operations using TLS are modeled with a handshake occurring at the start of each ten-minute interval. PSK and MLS key exchanges and updates are assumed to occur prior to the start of each mission and are excluded from the model. The results and analysis do not reflect the additional RF footprint associated with implementing a more frequent MLS key update periodicity or the time and cost of manually loading keys for PSK. Implementing frequent MLS key updates would result in an increased RF footprint and higher risk compared to the results contained in this research.

3. Channel Overhead is Excluded

This research compares security using TLS, MLS, and PSK to encrypt data. Additional networking layers may be required for functionality and influence the RF footprint, such as transport layer TCP/User Datagram Protocol options; however these additional layers are not considered in this research to ensure an “apple-to-apples” comparison between the selected protocols and methods as a security approach. Transport layer or other layer protocols may be different for security option we consider. Additional networking layers could also increase the data packet overhead, thus increasing RF footprint and geolocation risks. Decision makers should consider the actual risks during operations to be potentially higher than the risks estimated in this research.

4. MLS and PSK Operate in Broadcast Mode

This research assumes MLS and PSK operate in a broadcast mode and do not require an acknowledgment from the recipient when transmitting data (i.e., the transport type and operator settings allow this). This means that during a DoS attack, MLS and PSK continue to transmit data even though the data is not received. There is no increase in RF footprint when operating with MLS and PSK in broadcast mode.

TLS does not support broadcast mode, and an acknowledgement is required since unreliable packet delivery would otherwise lead to protocol failure. During a DoS attack, the sender cannot receive an acknowledgment from the receiver. This causes the sender to attempt to reestablish connection until the DoS attack stops before continuing data transmission. Each attempt to reestablish connection results in an increase in RF footprint.

MLS and PSK have the option to acknowledge each data packet; however, analysis of this use case is not included in this research. It should be noted that using MLS or PSK with acknowledgements, if selected, would result in increased geolocation and DoS risks compared to the risk levels presented in this research.

5. DoS Attack Timing

The timing of DoS attacks impacts the resulting RF footprint for the TLS model. As detailed in Chapter III.E.1, the 100-minute mission is divided into ten-minute segments. Within each ten-minute segment, the UxS operated in C2 mode for a predetermined period, then switches to autonomous mode for the remainder of those ten minutes. Once the ten minutes have passed, the UxS switches back to C2 mode for the next ten-minute interval. Additionally, this research assumes DoS attacks follow a normal distribution of five minutes and a standard deviation of 30 seconds. These assumptions result in a high probability that there will be overlap between a DoS attack and C2 mode operations in which data is transmitted.

In the TLS model, the forward unit C2 station initiates a handshake each time the UxS switches from autonomous mode to C2 mode at the start of each 10-minute interval. If the attack occurs during this transition from autonomy to C2, the “Client Hello” sent from the C2 station is not received by the UxS. Subsequently, the C2 station will not receive a “Server Hello” from the UxS. The C2 station will continue to send repeated “Client Hello” messages to the DoS attack ends a “Server Hello” message is received. These repeated handshake attempts cause an increase in data transmission (RF footprint) from the forward unit C2 station. The PSK and MLS models are unaffected by DoS attack timing because this research assumes they operate in a broadcast mode as detailed

in Chapter III.E.4. In other words, the PSK and MLS models send data even if the data is not received.

If autonomy is modeled with longer time intervals of 30 minutes for example, the probability of overlap between a DoS attack and C2 mode operations would decrease as percent autonomy increases. The DoS attack would likely occur only during autonomous operations in which no data is transferred, so the likelihood of data loss would decrease.

Alternatively, a DoS attack could begin during C2 mode operations. In this instance, the DoS attack is likely to affect UxS transmission as the UxS transmits 16 kB of data per packet (excluding overhead) while the C2 station only transmits 14 bytes of data per packet (excluding overhead). The PSK and MLS models are unaffected by DoS attack timing because this research assumes they operate in a broadcast mode as detailed in Chapter III.E, however, the TLS model is affected. When a DoS attack occurs during UxS transmission using TLS, the UxS continues to resend the data packet until the attack ends. This causes an increase in the UxS data transmission. After the attack ends, a TLS handshake occurs to reestablish connection.

This research defines lost data as C2 and video data. For TLS, handshake data was excluded because it does not provide situational awareness or C2 to the forward unit.

F. SIMULATION AND RESULTS

This section presents the simulation results of both the percent autonomy and triggered event models with and without the DoS attacks as described in Chapter III.C.3. An analysis of these results and their effects on mission risks is provided in Chapter IV of this report.

1. Percent Autonomy Model Without DoS Attack

The percent autonomy models are simulated in the discrete simulator mode of Innoslate. As described in Chapter III.C.1, the 100-minute missions are divided into 10-minute sections for computational ease and simulation software limitations. For each iteration of the simulation, the percentage of time the system operated in C2 mode is increased by 10% starting at 10% and ending at 100%. Since these models simulate the

transfer of very large data sets, a multiplication factor of 100 was implemented for each loop of the UxS data transfer. This was due for two reasons, decreasing the time it takes each simulation to run, and to prevent the Innoslate web-based software from timing out during the simulation. The results of the simulations are presented in Table 6 where the values show the total amount of data transmitted, in MB that the C2 and UxS components are transmitting during the entire 100-minute mission. As detailed in Chapter III.D, the results follow the expected outcome for a mission containing no attacks.

Table 6. Data Transmitted (Approximated RF Footprint) During a Mission Without DoS Attacks – Varying Levels of Autonomy

Percent of Mission Conducted in Autonomous Mode	TLS		PSK		MLS	
	Forward Unit C2 (MB)	UxS Video (MB)	Forward Unit C2 (MB)	UxS Video (MB)	Forward Unit C2 (MB)	UxS Video (MB)
0	38.364	43837.215	38.358	43837.200	37.963	43386.793
10	34.530	39808.215	34.530	39808.200	34.157	39378.153
20	30.695	35751.515	30.689	35751.500	30.365	35373.913
30	26.854	31694.815	26.847	31694.800	26.573	31181.444
40	23.026	27654.315	23.020	27654.300	22.781	27377.204
50	19.185	23609.115	19.170	23609.100	18.975	23368.564
60	15.344	19552.415	15.337	19552.400	15.183	19364.324
70	11.516	15511.915	11.510	15511.900	11.390	15371.855
80	7.675	11455.215	7.669	11455.200	7.598	11367.615
90	3.848	7414.715	3.841	7414.700	3.792	7358.975
100	0.000	0.000	0.000	0.000	0.000	0.000

2. Percent Autonomy Model with DoS Attack

For the percent autonomy models, the DoS attack as described in Chapter III.C.3 is applied to each percent autonomy run to determine the effects of the attack on the overall mission transmission for each component of the system. For a system operating with the TLS protocol, if the DoS attack occurs during a time of communication between the UxS and the C2 unit, the transmission operation that is interrupted at the initiation of the attack is anticipated to continue transmission of that data until an acknowledgement signal can be received at which point the TLS handshake is reinitiated to continue any further communication. This activity increases the overall transmission between the UxS and C2 unit thus increasing the overall detectability and risk to the mission. This scenario is depicted in Figure 27 and Figure 28 showing the impact to data transmission for TLS during the 50% C2/autonomy split mission and 30% C2/autonomy split mission respectively. The asynchronous capability of the MLS and PSK protocols allow for communication of data without the need for an acknowledgement signal. This allows for the continuous flow of data even during a DoS attack with the main impact to the mission being no communication between the UxS and C2 unit, i.e., loss of control of the UxS and no SA during the periods of attack. Results of these attacks for each protocol are provided in Table 8 which shows the impact to transmitted data for the indicated mission. Table 9 shows the total amount of data lost during a DoS attack. This research defines data lost as the raw data and packet headers, excluding handshake or key exchange. Data transmitted during a DoS is lost and will never be seen by the forward unit, resulting in reduced SA.

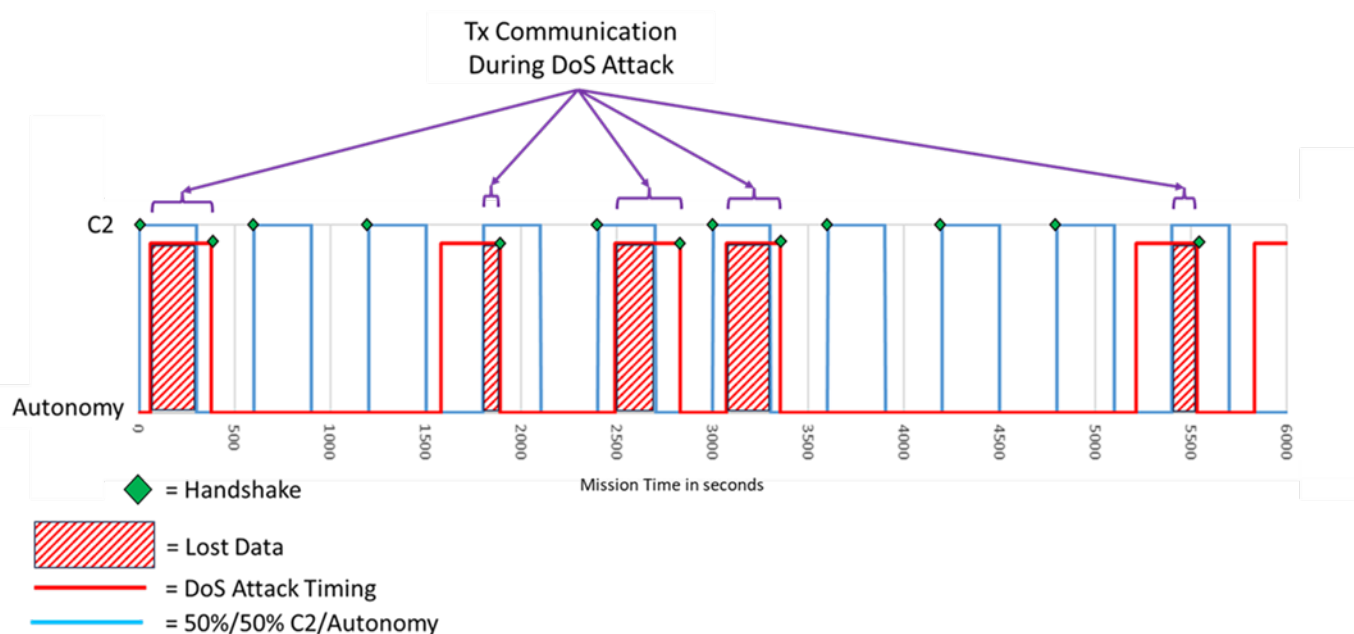


Figure 27. Timing Diagram of a DoS Attack on the TLS 50% Autonomy Model. A total of six DoS attacks occur during the 100 minute mission. Three DoS attacks occur during C2 mode in which the forward unit and UxS are transmitting C2 commands and video data. C2 data packets and video data packets are alternately transmitted for the duration of C2 mode operations. Depending on the exact timing of the DoS attack, either the C2 data packet transmission or the UxS data packet transmission is affected. As detailed in Chapter III.E.5, the UxS data transmission is more likely to be affected than the C2 data transmission because the UxS video data is greater in volume. The affected data packet attempts to resend repeatedly until an acknowledgement signal can be received. Once an acknowledgement signal is received, the TLS handshake is reinitiated to continue any further communication. Two DoS attacks begin during autonomous mode and extend into C2 mode. When this event occurs, the forward unit C2 system is unable to connect to the UxS during the attack. The C2 system attempts to complete the TLS handshake until the DoS attack is over. Repeated handshake attempts generate a significant increase in RF footprint. The last DoS attack occurs only during autonomous mode and has no impact since there is no data transmission in autonomous mode. This differs from actual protocol behavior in practice, where TLS timeouts and new handshakes make occur, etc.; however, for modeling purposes it provides a rough approximation to possible behavior.

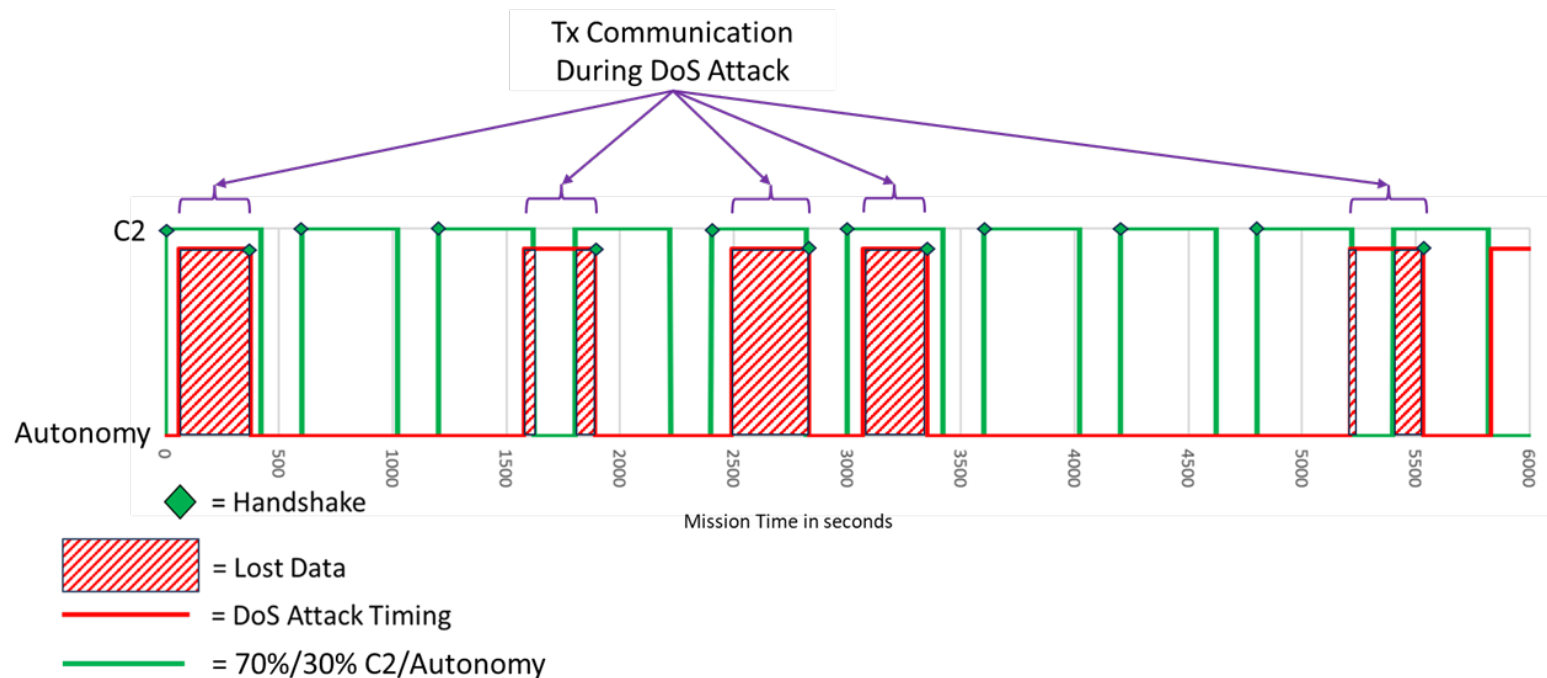


Figure 28. Timing Diagram of a DoS Attack on the TLS 30% Autonomy Model. A total of six DoS attacks occur during the 100 minute mission. Five DoS attacks occur during C2 mode in which the forward unit and UxS are transmitting C2 commands and video data. C2 data packets and video data packets are alternately transmitted for the duration of C2 mode operations. Depending on the exact timing of the DoS attack, either the C2 data packet transmission or the UxS data packet transmission is affected. As detailed in Chapter III.E.5, the UxS data transmission is more likely to be affected than the C2 data transmission because the UxS video data is greater in volume. The affected data packet attempts to resend repeatedly until an acknowledgement signal can be received. Once an acknowledgement signal is received, the TLS handshake is reinitiated to continue any further communication. The last DoS attack occurs only during autonomous mode and has no impact since there is no data transmission in autonomous mode. This differs from actual protocol behavior in practice, where TLS timeouts and new handshakes make occur, etc.; however, for modeling purposes it provides a rough approximation to possible behavior. The 30% autonomy mission shown in this figure has a shorter window of autonomous mode. This means it is less likely for a DoS attack to begin during autonomous mode and extend into C2 mode causing repeated handshake attempts and generating a significant increase in RF footprint as seen in the 50% autonomy mission depicted in Figure 27.

Table 7. Data Transmitted (Approximated RF Footprint) During a Mission with DoS Attacks – Varying Levels of Autonomy

Percent of Mission Conducted in Autonomous Mode	TLS		PSK		MLS	
	Forward Unit C2 (MB)	UxS Video (MB)	Forward Unit C2 (MB)	UxS Video (MB)	Forward Unit C2 (MB)	UxS Video (MB)
0	27.244	52868.260	38.358	43837.200	37.963	43386.793
10	24.561	50077.260	34.530	39808.200	34.157	39378.153
20	21.874	47272.900	30.689	35751.500	30.365	35373.913
30	19.173	42355.870	26.847	31694.800	26.573	31181.444
40	2769.402 ^a	31299.970	23.020	27654.300	22.781	27377.204
50	2779.309	28439.640	19.170	23609.100	18.975	23368.564
60	2789.266	25630.070	15.337	19552.400	15.183	19364.324
70	2765.984	22838.240	11.510	15511.900	11.390	15371.855
80	2776.017	20122.350	7.669	11455.200	7.598	11367.615
90	2753.054	9906.880	3.841	7414.700	3.792	7358.975
100	0.000	0.000	0.000	0.000	0.000	0.000

C2 data packets and video data packets are alternately transmitted for the duration of C2 mode operations. Depending on the exact timing of the DoS attack, either the C2 data packet transmission or the UxS data packet transmission is affected. As detailed in Chapter III.E.5, the UxS data transmission is more likely to be affected than the C2 data transmission because the UxS video data is greater in volume. The affected data packet attempts to resend repeatedly until an acknowledgement signal can be received. Once an acknowledgement signal is received, the TLS handshake is reinitiated to continue any further communication.

^aAs autonomy increases, the likelihood of a DoS attack occurring during the transition from autonomous operations to C2 operations increases. When this event occurs, the forward unit C2 system is unable to connect to the UxS during the attack. The C2 system attempts to complete the TLS handshake until the DoS attack is over. Repeated handshake attempts generate a significant increase in RF footprint accounting for the sudden increase in forward unit C2 data transmission at 40% autonomy. The spike in RF footprint does not always occur at 40% autonomy. The timing and frequency of DoS attacks are randomly generated within the model. Re-running the simulation results in a different distribution of DoS attacks during the mission, thus changing where the increase in RF footprint occurs within the autonomy spectrum defined in this research.

PSK and MLS do not require a handshake to reestablish connection after a DoS attack, therefore the data is the same as the model without DoS attacks. Only TLS model has increased data transmission due to DoS attack.

Table 8. Complete Packet Data Lost During a DoS Attack – Varying Levels of Autonomy

Percent of Mission Conducted in Autonomous Mode	TLS ^a		PSK		MLS	
	Forward Unit C2 (MB)	UxS Video (MB)	Forward Unit C2 (MB)	UxS Video (MB)	Forward Unit C2 (MB)	UxS Video (MB)
0	11.123	12718.623	11.136	12734.820	11.011	12590.741
10	9.979	11480.283	9.979	11480.288	9.864	11345.927
20	8.824	10228.303	8.823	10228.300	8.725	10111.696
30	7.684	8989.283	7.690	8997.380	7.605	8897.608
40	6.868	8118.003	6.866	8118.000	6.792	8035.310
50	5.769	6933.123	5.768	6933.120	5.707	6861.649
60	4.619	5686.003	4.618	5686.000	4.569	5629.035
70	3.467	4437.263	3.466	4437.260	3.431	4393.925
80	2.235	3096.183	2.248	3112.380	2.220	3077.222
90	0.770	1484.563	0.768	1484.560	0.758	1471.795
100	0.000	0.000	0.000	0.000	0.000	0.000

During a DoS attack, the receiver is overwhelmed through RF jamming by the attacker and cannot receive the data transmitted by the intended sender. The transmitted data is effectively “lost.”

The lost data presented includes the packet overhead.

^aTLS lost data includes C2 and video data. It does not include handshake data. Handshake data was excluded because it does not provide situational awareness or C2 to the forward unit.

Lost data transmission is converted to percentage of transmission lost for use in the risk analysis in Chapter IV. Percentage of transmission lost, P_{loss} , is calculated by the equation where X is the “Amount of Data Transmitted During a DoS Attack” and Y is “Amount of Data Transmitted During a Mission without DoS Attacks.” The values of “X” come from Table 6 and the values of “Y” come from Table 8. Table 9 shows the calculated percentages of lost transmission time.

$$P_{loss} = \frac{X(s)}{Y(s)} \times 100$$

Table 9. Percentage of Data Transmission Lost Due to a DoS Attack – Varying Levels of Autonomy

Percent of Mission Conducted in Autonomous Mode	TLS	PSK	MLS
0%	29%	29%	29%
10%	29%	29%	29%
20%	29%	29%	29%
30%	28%	28%	29%
40%	29%	29%	29%
50%	29%	29%	29%
60%	29%	29%	29%
70%	29%	29%	29%
80%	27%	27%	27%
90%	20%	20%	20%
100%	0%	0%	0%

The percentage of data transmission lost is consistent for all levels of autonomy. This is due to the way autonomy is defined in this research, as detailed in Chapter III.E.1. The 100-minute mission is divided into ten-minute segments. Within each ten-minute segment, the UxS operated in C2 mode for a predetermined period, then switches to autonomous mode for the remainder of those ten minutes. Once the ten minutes have passed, the UxS switches back to C2 mode for the next ten-minute interval. The result of this assumption, combined with our average DoS attack duration of 5 minutes, is a high probability that there will be overlap between a DoS attack and C2 mode operations in which data is transmitted.

If autonomy was modeled with longer time intervals of 30 minutes for example, the probability of overlap between a DoS attack and C2 mode operations would decrease as percent autonomy increases. The DoS attack would likely occur to only autonomous operations in which no data is transferred, so there would be no loss of data.

Note: Percentages shown in the table are rounded to the nearest integer.

3. Triggered Event Model

For the triggered event models, the research team simulates the models where ten triggering events occur during the mission to determine the overall data transmission from each component within this system. The research team then takes the output of these models and applies the DoS attack as detailed previously and applied it to the mission to determine its impact.

a. Triggered Event Model Without a DoS Attack

The triggered event simulations are initially run without DoS attacks. The results of these simulations are detailed in Figure 29 and Table 10 and represent the same type of data as the percent autonomy models. As can be seen in Table 10, the effect of the security protocol in the triggered event scenario is minimal. The amount of video data being transmitted is the same for all three triggered models with the only difference coming from the required acknowledgement signals for TLS and the differing overheads for each security protocol.

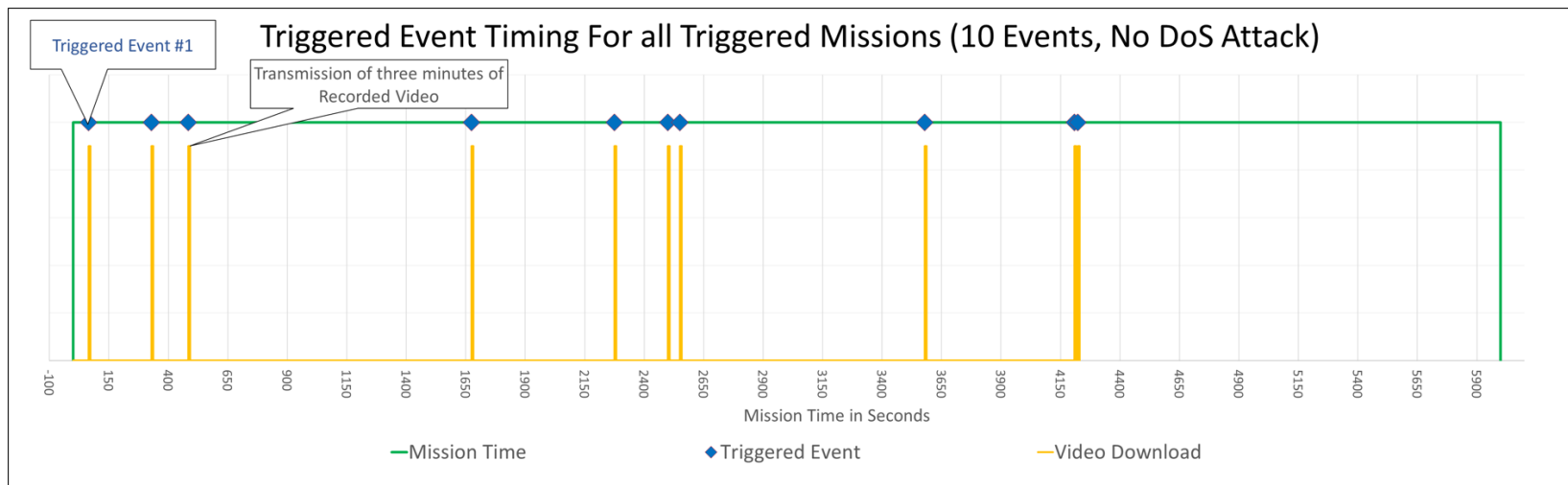


Figure 29. Triggering Event Model Timing Results

Table 10. Total Data Transmitted (Approximated RF Footprint) During a Mission without DoS Attacks – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission

	Data Transmitted (MB)
TLS – Forward Unit C2	0.015
TLS – UxS Video	1008.406
PSK – Forward Unit C2	0.000
PSK – UxS Video	1004.4
MLS – Forward Unit C2	0.000
MLS – UxS Video	1002.206

b. Triggered Event Model With a DoS Attack

Using the same triggered event model outputs from Chapter III.F.3.a, the research team applies the same DoS attack applied to the percent autonomy models to determine the overall effects the attack had on mission transmission times. The results of these simulations are detailed in Figure 30, Figure 31, Table 11, Table 12, and Table 13 for direct comparison to the same missions without an attack applied. This research assumes MLS and PSK operate in a broadcast mode as detailed in Chapter III.E.4, therefore an acknowledgement signal is not required to continue transmission of the next packet of recorded video to the C2 unit. In this situation, the data the UxS is trying to transmit will not be received by the C2 personnel and the data will be lost resulting in loss of SA. Loss of SA is the only impact for these protocols. Shown in the MLS and PSK triggering event model timing results, Figure 31, five of the ten triggered events will not be received by the C2 unit significantly degrading SA. For TLS, a DoS attack can result in both lost data and extra data transmission resulting in degraded SA and increased RF footprint. TLS does not support broadcast mode, and an acknowledgement is required since unreliable packet delivery would otherwise lead to protocol failure. During a DoS attack, the sender cannot receive an acknowledgment from the receiver. This causes the sender to attempt to reestablish connection until the DoS attack stops before continuing data transmission. Each attempt to reestablish connection results in an increase in RF footprint. Additionally, if another triggered event occurs within the same window of an attack, that

additional triggered data will be lost for the mission as well. This scenario occurs twice in the TLS Triggered model and can be seen in Figure 30. The first and third attacks overlap with two triggered events resulting in the UxS continuing to try to transmit data for the duration of the attack for the first triggered event while the second triggered events data is overlooked in the background resulting in its loss. The TLS model results in five of the ten triggered events data being lost as well as significantly more data transmission. Table 12 shows the volume of data transmitted during a DoS attack and Table 13 shows the percentage of lost data calculated using the equation on page 75.

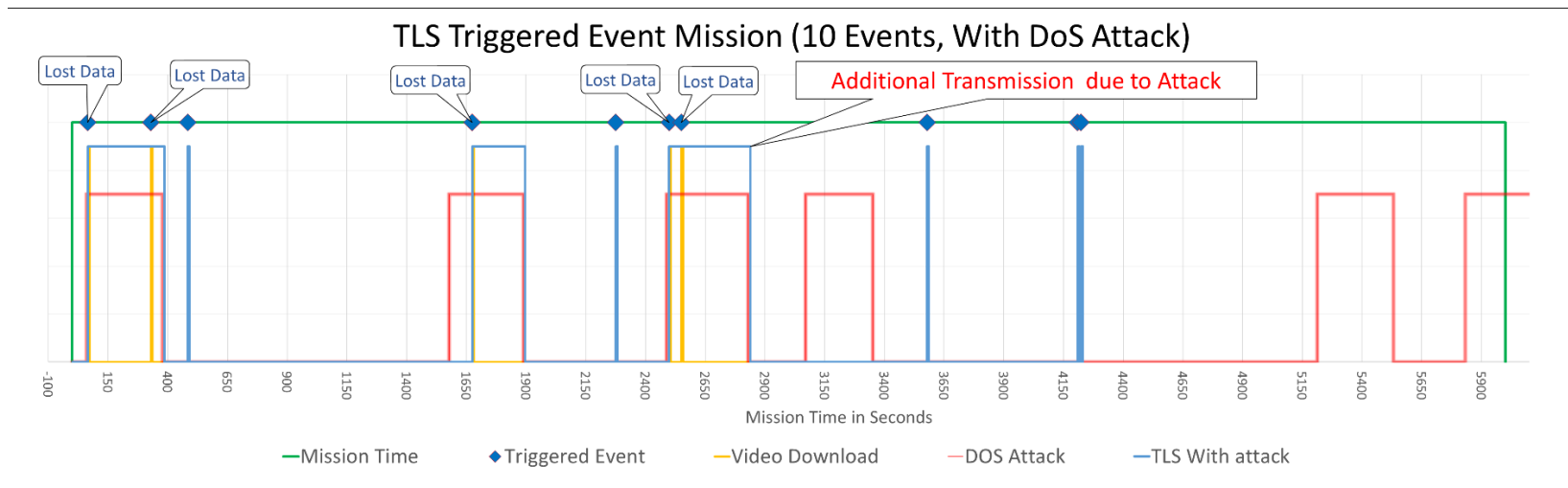


Figure 30. TLS Triggering Event Model Timing Results with a DoS Attack. The yellow lines represent the original “video download” segments from triggered event model without DoS attacks (Figure 28). The yellow lines indicate the video signals that are lost and will never be received by the C2 personnel. The blue line shows the additional RF transmission because of the DoS attack. This shows that with TLS, a DoS attack results in both a decrease in SA and an increase in RF footprint.

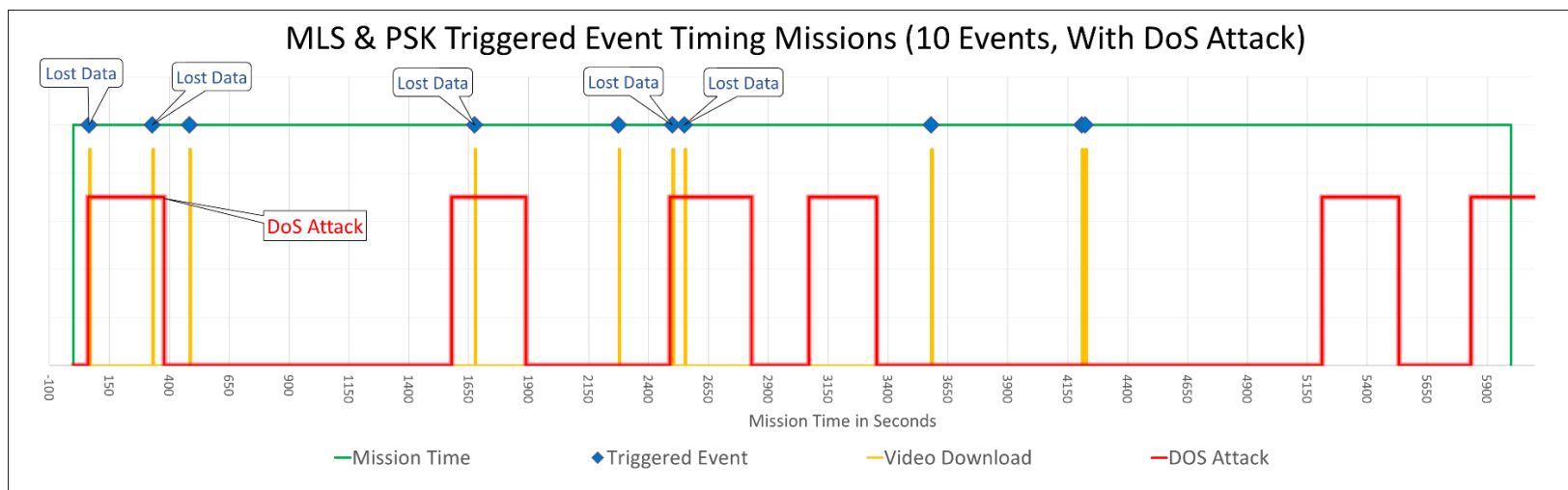


Figure 31. MLS and PSK Triggering Event Model Timing Results with a DoS Attack. The triggered events represented by the blue diamonds. If a trigger event occurs during a DoS attack, indicated by the red line, the transmitted data will be lost and never received by the forward unit. MLS and PSK operating in a broadcast mode as described in Chapter III.E.4, will only result in the loss of data (decreased SA) and no additional transmitted data is accumulated during these attacks as with TLS (no increase in RF footprint).

Table 11. Total Data Transmitted (Approximated RF Footprint) During a Mission with DoS Attacks – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission

	Data Transmitted (MB)
TLS – Forward Unit C2	0.01
TLS – UxS Video	11533.63
PSK – Forward Unit C2	0.00
PSK – UxS Video	1004.40
MLS – Forward Unit C2	0.00
MLS – UxS Video	1002.21

If the DoS attack occurs during a trigger event, the communication signal that is interrupted, the recorded video or live video signal from the UxS, that interrupted signal will continually try to be sent until receiving a confirmation message the data was received. Upon confirmation, a new TLS handshake occurs to ensure a secure link.

PSK and MLS do not require a handshake to reestablish connection after a DoS attack, therefore the data is the same as the model without DoS attacks. Only TLS model has increased data transmission due to DoS attack, since for PSK and MLS a retransmission is not performed (unless later requested).

Table 12. Data Transmission Lost During a DoS Attack – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission

	Data Lost (MB)
TLS – Forward Unit C2	0.01
TLS – UxS Video	504.2
PSK – Forward Unit C2	0.00
PSK – UxS Video	502.2
MLS – Forward Unit C2	0.00
MLS – UxS Video	501.3

During a DoS attack, the receiver is overwhelmed through RF jamming by the attacker and cannot receive the data transmitted by the intended sender. The transmitted data is effectively “lost.”

The lost data presented includes the packet overhead.

^aTLS lost data includes C2 and video data. It does not include handshake data. Handshake data was excluded because it does not provide situational awareness or C2 to the forward unit.

Table 13. Percentage of Data Transmitted During a DoS Attack – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission

	Percentage of Data Lost
TLS	50
PSK	50
MLS	50

Note: Percentages shown in the table are rounded to the nearest integer.

G. CHAPTER SUMMARY

This chapter identifies the model requirements and details the inputs, outputs, and constants. The development of the TLS percent split autonomy and trigger models are examined in detail while the MLS and PSK model development processes are contained in Appendix A and Appendix B. This chapter also examines the process in which the model is verified to ensure the model provides the desired outputs and that the output is accurate. Lastly, this chapter presents the simulation results. The next chapter, Chapter IV, analyzes the simulation results to answer the research questions presented in Chapter I.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RISK ANALYSIS

In Chapter II, the research team identified three risks inherent in the operation of UxS; geolocation, DoS, and impersonation attacks. Chapter IV explains the methods and reasoning behind the analysis of these three risks.

A. RISK DEFINITION

The NIST SP 800-30 defines risk as “a measure of the extent to which an entity is threatened by a potential circumstance or event” (2012). NIST SP 800-30 further defines risk as “a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” Table 14 shows the risk assessment matrix that assigned a risk level or Very High, High, Moderate, Low, and Very Low based on the likelihood and level of impact of the identified risk.

Table 14. Risk Assessment Matrix. Adapted from NIST (2012).

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Adverse Impact				
	Negligible	Limited	Serious	Severe	Catastrophic
Almost Certain	Very Low	Low	Moderate	High	Very High
Highly Likely	Very Low	Low	Moderate	High	Very High
Somewhat Likely	Very Low	Low	Moderate	Moderate	High
Unlikely	Very Low	Low	Low	Low	Moderate
Highly Unlikely	Very Low	Very Low	Very Low	Low	Low
Eliminated	Eliminated				

Risk values for Very High, High, Moderate, Low, and Very Low are the assessment of NIST (2012).

1. Likelihood

The likelihood of occurrence of a threat event is determined by combining “an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact” (NIST 2012).

This research defines the likelihood a threat event will have a negative impact based on the amount of time the UxS and/or forward unit is transmitting data as shown in Table 15 through Table 18 (NIST 2012). If the adversary initiates a threat event during a period where no data transmission occurs, there will be no negative impact. The adversary cannot successfully geolocate assets or personnel; or conduct successful cyberattacks if no transmission signal is present or expected by the C2 systems and UxS. Conversely, if there is a constant stream of data transmission throughout the mission, the adversary has a high likelihood of successfully geolocating personnel and assets and C2 systems and UxS are vulnerable to cyberattacks.

Table 15. Assessment Scale – Likelihood of Forward Unit Geolocation.
Adapted from NIST (2012)

Qualitative Values	Forward Unit C2 Data Transmitted (MB)	Description
Almost Certain	≥ 10000 MB	“If the threat event is initiated or occurs, it is almost certain to have adverse impacts.”
Highly Likely	≥ 1000 MB	“If the threat event is initiated or occurs, it is highly likely to have adverse impacts.”
Somewhat Likely	≥ 100 MB	“If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.”
Unlikely	≥ 10 MB	“If the threat event is initiated or occurs, it is unlikely to have adverse impacts.”
Highly Unlikely	> 0 MB	“If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.”
Eliminated	$= 0$ MB	The threat is not present .

The middle column, data transmitted, provides a semi-qualitative method for assigning a likelihood of threat initiation. A magnitude scale is used to assess the likelihood. For example, 20 MB of data transmission is assigned a qualitative value of “unlikely” while 20000 MB of data transmission is assigned a qualitative value of “almost certain.”

Table 16. Assessment Scale – Likelihood of UxS Geolocation. Adapted from NIST (2012).

Qualitative Values	UxS Video Data Transmitted (MB)	Description
Almost Certain	≥ 40000 MB	“If the threat event is initiated or occurs, it is almost certain to have adverse impacts.”
Highly Likely	≥ 30000 MB	“If the threat event is initiated or occurs, it is highly likely to have adverse impacts.”
Somewhat Likely	≥ 20000 MB	“If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.”
Unlikely	≥ 10000 MB	“If the threat event is initiated or occurs, it is unlikely to have adverse impacts.”
Highly Unlikely	> 0 MB	“If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.”
Eliminated	$= 0$ MB	The threat is not present .

The middle column, data transmitted, provides a semi-qualitative method for assigning a likelihood of threat initiation. The average quantity of UxS video data transmitted is between 20000 MB and 30000 MB. This average is assigned a qualitative value of “somewhat likely.” Other qualitative values are based on 10000 MB increments greater or lesser than the average. For example, 10000 MB of data transmission is assigned a qualitative value of “unlikely” while 40000 MB of data transmission is assigned a qualitative value of “almost certain.”

Table 17. Assessment Scale – Likelihood of Data Transmission During a DoS Attack. Adapted from NIST (2012).

Qualitative Values	Total Percent of Data Transmission Lost Due to DoS Attacks	Description
Almost Certain	$\geq 80\%$ of data is lost	“If the threat event is initiated or occurs, it is almost certain ” to result in lost data.
Highly Likely	$\geq 60\%$ of data is lost	“If the threat event is initiated or occurs, it is highly likely to” result in lost data.
Somewhat Likely	$\geq 40\%$ of data is lost	“If the threat event is initiated or occurs, it is somewhat likely to” result in lost data.
Unlikely	$\geq 20\%$ of data is lost	“If the threat event is initiated or occurs, it is unlikely to” result in lost data.
Highly Unlikely	$< 20\%$ of data is lost	“If the threat event is initiated or occurs, it is highly unlikely to” result in lost data.
Eliminated	0% of data is lost	The threat is not present .

The middle column, transmission time, provides a semi-qualitative method for assigning a likelihood of threat initiation. Five qualitative values are defined by equal intervals of 20%. For example, a 25% loss of data is assigned a qualitative value of “unlikely,” and a 45% data loss is assigned a qualitative value of “somewhat likely.”

Table 18. Assessment Scale – Likelihood of Impersonation Threat. Adapted from NIST (2012).

Qualitative Values	Data Link Present	Security Protocol/ Method	Description
Highly Likely	Yes	PSK	PSK is susceptible to impersonation attacks. “If the threat event is initiated or occurs, it is highly likely to” succeed.
Somewhat Likely	Yes	TLS	TLS provides moderate protection against impersonation attacks. “If the threat event is initiated or occurs, it is somewhat likely to” succeed.
Unlikely	Yes	MLS	MLS provides high protection against impersonation attacks. “If the threat event is initiated or occurs, it is unlikely to” succeed.
Eliminated	No	All	When operating in full autonomy, no data link is present, and an impersonation attack will not succeed. The threat is not present.

2. Impact

NIST defines the level of impact as “the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability” (2012). Table 19 is used to assess the level of impact of a threat event.

Table 19. Impact of Threat Event Assessment Matrix. Adapted from NIST (2012).

Qualitative Values	Description
Catastrophic	“The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.”
Severe	“The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.”
Serious	“The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.”
Limited	“The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.”
Negligible	“The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.”

B. RISK ASSESSMENT

The risk level for geolocation, DoS, and impersonation are determined for each scenario by identifying likelihood and negative impact for each risk. The research team uses DMO/EABO environment research and the modeling and simulation data from Chapter III to assess the risk of geolocating the UxS and the forward unit during UxS operations and the risks of DoS and impersonation attacks.

1. Likelihood Assessment

The likelihood a threat initiation will result in adverse impacts is assessed for each risk.

a. Likelihood of Geolocation

The likelihood a geolocation threat initiation is assessed using Table 15, Table 16, and the M&S results. The likelihood values for geolocation threat initiation are listed in Table 20 through Table 23 for the percent autonomy scenario and trigger event scenarios. This assessment assumes that PSK and MLS do not try to resend data in a broadcast mode without an acknowledgement from the receiver, and that an acknowledgement is not required. TLS always requires an acknowledgement, causing the likelihood of geolocation to increase as autonomy is increased during a DoS attack. If the operator chooses to require acknowledgements using PSK or MLS, the likelihood of geolocation would be greater than the likelihood presented in this research. In this alternative scenario, the PSK and MLS geolocation likelihoods would be similar to the TLS likelihood.

Table 20. Likelihood Forward Unit Geolocation Based on RF Output – Varying Levels of Autonomy

Percent of Mission Conducted in Autonomous Mode	Without DoS Attacks			With DoS Attacks ^a		
	TLS	PSK	MLS	TLS	PSK	MLS
0	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely
10	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely
20	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely
30	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely
40	Unlikely	Unlikely	Unlikely	Highly Likely	Unlikely	Unlikely
50	Unlikely	Unlikely	Unlikely	Highly Likely	Unlikely	Unlikely
60	Unlikely	Unlikely	Unlikely	Highly Likely	Unlikely	Unlikely
70	Unlikely	Unlikely	Unlikely	Highly Likely	Unlikely	Unlikely
80	Highly Unlikely	Highly Unlikely	Highly Unlikely	Highly Likely	Highly Unlikely	Highly Unlikely
90	Highly Unlikely	Highly Unlikely	Highly Unlikely	Highly Likely	Highly Unlikely	Highly Unlikely
100	Eliminated	Eliminated	Eliminated	Eliminated	Eliminated	Eliminated

^aTLS always requires an acknowledgement, causing the likelihood of geolocation to increase as autonomy is increased. An acknowledgement is optional when using PSK and MLS in a broadcast mode. This assessment assumes that PSK and MLS do not try to resend data in a broadcast mode without an acknowledgement from the receiver, and that an acknowledgement is not required. If the operator chooses to require acknowledgements using PSK or MLS, the likelihood would increase with increased autonomy, similar to the TLS likelihood presented in the table.

Table 21. Likelihood of UxS Geolocation Based on RF Output – Varying Levels of Autonomy

Percent of Mission Conducted in Autonomous Mode	Without DoS Attack			With DoS Attack ^a		
	TLS	PSK	MLS	TLS	PSK	MLS
0	Almost Certain	Almost Certain	Almost Certain	Almost Certain	Almost Certain	Almost Certain
10	Highly Likely	Highly Likely	Highly Likely	Almost Certain	Highly Likely	Highly Likely
20	Highly Likely	Highly Likely	Highly Likely	Almost Certain	Highly Likely	Highly Likely
30	Highly Likely	Highly Likely	Highly Likely	Almost Certain	Highly Likely	Highly Likely
40	Somewhat Likely	Somewhat Likely	Somewhat Likely	Highly Likely	Somewhat Likely	Somewhat Likely
50	Somewhat Likely	Somewhat Likely	Somewhat Likely	Somewhat Likely	Somewhat Likely	Somewhat Likely
60	Unlikely	Unlikely	Unlikely	Somewhat Likely	Unlikely	Unlikely
70	Unlikely	Unlikely	Unlikely	Somewhat Likely	Unlikely	Unlikely
80	Unlikely	Unlikely	Unlikely	Somewhat Likely	Unlikely	Unlikely
90	Highly Unlikely	Highly Unlikely	Highly Unlikely	Highly Unlikely	Highly Unlikely	Highly Unlikely
100	Eliminated	Eliminated	Eliminated	Eliminated	Eliminated	Eliminated

^aTLS always requires an acknowledgement, causing the likelihood of geolocation to increase as autonomy is increased. An acknowledgement is optional when using PSK and MLS in a broadcast mode. This assessment assumes that PSK and MLS do not try to resend data in a broadcast mode without an acknowledgement from the receiver, and that an acknowledgement is not required. If the operator chooses to require acknowledgements using PSK or MLS, the likelihood levels would be greater than those presented in this table.

Table 22. Likelihood of Forward Unit Geolocation Based on RF Output – 100% Autonomy with a Trigger Event Causing Periodic Video Transmission

	TLS	PSK	MLS
Without DoS Attack	Highly Unlikely	Eliminated	Eliminated
With DoS Attack	Highly Unlikely	Eliminated	Eliminated

Table 23. Likelihood of UxS Geolocation Based on RF Output– 100% Autonomy with a Trigger Event Causing Periodic Video Transmission

	TLS	PSK	MLS
Without DoS Attack	Highly Unlikely	Highly Unlikely	Highly Unlikely
With DoS Attack	Highly Unlikely	Highly Unlikely	Highly Unlikely

b. Likelihood of Lost Data Due to DoS Attack

The likelihood of a DoS threat initiation is assessed using Table 17 and the M&S results. The likelihood values for DoS threat initiation resulting in adverse impacts are listed in Table 24 and Table 25 for the percent autonomy scenario and trigger event scenarios.

Table 24. Likelihood of Data Loss due to DoS Attack – Varying Levels of Autonomy

Percent of Mission Conducted in Autonomous Mode	TLS	PSK	MLS
0	Unlikely	Unlikely	Unlikely
10	Unlikely	Unlikely	Unlikely
20	Unlikely	Unlikely	Unlikely
30	Unlikely	Unlikely	Unlikely
40	Unlikely	Unlikely	Unlikely
50	Unlikely	Unlikely	Unlikely
60	Unlikely	Unlikely	Unlikely
70	Unlikely	Unlikely	Unlikely
80	Unlikely	Unlikely	Unlikely
90	Unlikely	Unlikely	Unlikely
100	Eliminated	Eliminated	Eliminated

The percentage of data transmission lost is consistent for all levels of autonomy. This is due to the way autonomy is defined in this research, as detailed in Chapter III.E.1. The 100-minute mission is divided into ten-minute segments. Within each ten-minute segment, the UxS operated in C2 mode for a predetermined period, then switches to autonomous mode for the remainder of those ten minutes. Once the ten minutes have passed, the UxS switches back to C2 mode for the next ten-minute interval. The result of this assumption, combined with our average DoS attack duration of 5 minutes, is a high probability that there will be overlap between a DoS attack and C2 mode operations in which data is transmitted.

If autonomy was modeled with longer time intervals of 30 minutes for example, the probability of overlap between a DoS attack and C2 mode operations would decrease as percent autonomy increases. The DoS attack would likely occur only during autonomous operations in which no data is transferred, so the likelihood of data loss would decrease.

TLS lost data includes C2 and video data. It does not include handshake data. Handshake data was excluded because it does not provide situational awareness or C2 to the forward unit.

Table 25. Likelihood of Data Loss Due to DoS Attack – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission

TLS	PSK	MLS
Somewhat Likely	Somewhat Likely	Somewhat Likely

c. Likelihood of Successful Impersonation Attack

The likelihood of a successful impersonation attack is assessed using Table 18. The likelihood values for impersonation threat initiation resulting in adverse impacts are listed in Table 26 and Table 27 for the percent autonomy scenario and trigger event scenarios.

Table 26. Likelihood of Impersonation – Varying Levels of Autonomy

Percent of Mission Conducted in Autonomous Mode	TLS	PSK	MLS
0	Somewhat Likely	Highly Likely	Unlikely
10	Somewhat Likely	Highly Likely	Unlikely
20	Somewhat Likely	Highly Likely	Unlikely
30	Somewhat Likely	Highly Likely	Unlikely
40	Somewhat Likely	Highly Likely	Unlikely
50	Somewhat Likely	Highly Likely	Unlikely
60	Somewhat Likely	Highly Likely	Unlikely
70	Somewhat Likely	Highly Likely	Unlikely
80	Somewhat Likely	Highly Likely	Unlikely
90	Somewhat Likely	Highly Likely	Unlikely
100	Eliminated	Eliminated	Eliminated

Table 27. Likelihood of Impersonation – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission

TLS	PSK	MLS
Somewhat Likely	Highly Likely	Unlikely

2. Impact Assessment

The next step is to determine the impact using the definitions contained in Table 19. Table 28 through Table 30 list the impact levels for each risk and describe why those levels were selected.

Table 28. Geolocation Impact Values. Adapted from NIST (2012).

Risk	Protocol or Method	Impact	Description
Geolocate Unit	All	Catastrophic	If the adversary geolocates the unit, they can launch a physical attack that “could result in multiple severe or catastrophic effects on individuals.” A physical attack could lead to “loss of life or serious life-threatening injuries” to all members of the forward unit.
Geolocate UxS	All	Severe	If the adversary geolocates the UxS, they can capture or destroy the UxS causing “major damage to organizational assets.” The organization would suffer a monetary loss from losing the UxS and any data stored on the UxS.

Table 29. DoS Attack Impact Values. Adapted from NIST (2012).

Protocol or Method	Impact	Description
TLS	Serious	A DoS attack would prevent data transmission. The forward unit would temporarily lose SA of the UxS. Once the DoS attack stops, a TLS handshake would be performed. Following that, data transmission would resume. Data transmitted during the DoS attack would be lost. The mission can still be completed, but the extended interruption in data transmission would “significantly reduce” effectiveness.
MLS and PSK	Limited	A DoS attack would prevent data transmission. The forward unit would temporarily lose SA of the UxS. Once the DoS attack stops, data transmission would immediately resume. Data transmitted during the DoS attack would be lost. The mission can still be completed, but the temporary interruption in data transmission would reduce effectiveness.

Table 30. Impersonation Attack Impact Values. Adapted from NIST (2012).

Protocol or Method	Impact	Description
TLS	Serious	Assuming loss of session keys, an impersonation attack scope spans a single session, which may be in the order of ours. The result could be a “significant degradation in mission” forging of mission C2 messages or responses, and potentially subversion of mission success. Data confidentiality and authentication would also be lost or the duration of the session. The risk window is bounded by the session length.
PSK	Severe	Assuming a loss of session keys, an impersonation attack could last for the entire duration of the PSK lifespan causing “a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; result in major financial loss.” As such an attack may not be detected, the risk window is bounded by guidance time windows for manually distributing new keys.
MLS	Limited	Assuming loss of session keys, an impersonation attack could last a variable length of time, controllable by mission parameters or other decision-based automated settings. Such time windows may be significantly shorter than those in TLS. The result could be “degradation in mission,” forging of mission command and control messages or response, and potentially subversion of mission success. Data confidentiality and authenticity would also be lost for the duration of the time window. The risk window can be bounded as desired

While the model in this research assumes the MLS key update occurs just before each mission, these impact values capture normal differences in which more frequent MLS key updates occur during the mission to shorten the vulnerability window.

3. Risk Assessment

Finally, the risk level was determined using Table 14 to identify the resulting risk level for each combination of likelihood and impact. The resulting risk levels for geolocation, DoS, and impersonation are listed in Table 31 through Table 36. The risk levels presented in this research are impacted by the model assumptions stated in Chapter III.E. Decision makers should consider the potential for increased risk levels if these assumptions are not representative of the intended operations.

Table 31. Forward Unit Geolocation Risk Levels – Varying Levels of Autonomy

Percent of Mission Conducted in Autonomous Mode	Without DoS Attacks			With DoS Attacks ^a		
	TLS	PSK	MLS	TLS	PSK	MLS
0	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
10	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
20	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
30	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
40	Moderate	Moderate	Moderate	Very High	Moderate	Moderate
50	Moderate	Moderate	Moderate	Very High	Moderate	Moderate
60	Moderate	Moderate	Moderate	Very High	Moderate	Moderate
70	Moderate	Moderate	Moderate	Very High	Moderate	Moderate
80	Low	Low	Low	Very High	Low	Low
90	Low	Low	Low	Very High	Low	Low
100	Eliminated	Eliminated	Eliminated	Eliminated	Eliminated	Eliminated

^aTLS always requires an acknowledgement, causing the likelihood of geolocation to increase as autonomy is increased. An acknowledgement is optional when using PSK and MLS in a broadcast mode. This assessment assumes that PSK and MLS do not try to resend data in a broadcast mode without an acknowledgement from the receiver, and that an acknowledgement is not required. If the operator chooses to require acknowledgements using PSK or MLS, the likelihood levels would be greater than those presented in this table.

Table 32. UxS Geolocation Risk Levels – Varying Levels of Autonomy

Percent of Mission Conducted in Autonomous Mode	Without DoS Attacks			With DoS Attacks ^a		
	TLS	PSK	MLS	TLS	PSK	MLS
0	High	High	High	High	High	High
10	High	High	High	High	High	High
20	High	High	High	High	High	High
30	High	High	High	High	High	High
40	Moderate	Moderate	Moderate	High	Moderate	Moderate
50	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
60	Low	Low	Low	Moderate	Low	Low
70	Low	Low	Low	Moderate	Low	Low
80	Low	Low	Low	Moderate	Low	Low
90	Low	Low	Low	Low	Low	Low
100	Eliminated	Eliminated	Eliminated	Eliminated	Eliminated	Eliminated

^aTLS always requires an acknowledgement, causing the likelihood of geolocation to increase as autonomy is increased. An acknowledgement is optional when using PSK and MLS in a broadcast mode. This assessment assumes that PSK and MLS do not try to resend data in a broadcast mode without an acknowledgement from the receiver, and that an acknowledgement is not required. If the operator chooses to require acknowledgements using PSK or MLS, the likelihood levels would be greater than those presented in this table.

Table 33. Data Transmission Loss During DoS Attack Risk Levels – Varying Levels of Autonomy

Percent of Mission Conducted in Autonomous Mode	With DoS Attacks		
	TLS	PSK	MLS
0	Low	Low	Low
10	Low	Low	Low
20	Low	Low	Low
30	Low	Low	Low
40	Low	Low	Low
50	Low	Low	Low
60	Low	Low	Low
70	Low	Low	Low
80	Low	Low	Low
90	Low	Low	Low
100	Eliminated	Eliminated	Eliminated

The percentage of data transmission lost is consistent for all levels of autonomy. This is due to the way autonomy is defined in this research, as detailed in Chapter III.E.1. The 100-minute mission is divided into ten-minute segments. Within each ten-minute segment, the UxS operated in C2 mode for a predetermined period, then switches to autonomous mode for the remainder of those ten minutes. Once the ten minutes have passed, the UxS switches back to C2 mode for the next ten-minute interval. The result of this assumption, combined with our average DoS attack duration of 5 minutes, is a high probability that there will be overlap between a DoS attack and C2 mode operations in which data is transmitted.

If autonomy was modeled with longer time intervals of 30 minutes for example, the probability of overlap between a DoS attack and C2 mode operations would decrease as percent autonomy increases. The DoS attack would likely occur only during autonomous operations in which no data is transferred, so the risk of data loss would decrease.

Table 34. Impersonation Risk Levels – Varying Levels of Autonomy

Percent of Mission Conducted in Autonomous Mode	TLS	PSK	MLS
0	Moderate	High	Low
10	Moderate	High	Low
20	Moderate	High	Low
30	Moderate	High	Low
40	Moderate	High	Low
50	Moderate	High	Low
60	Moderate	High	Low
70	Moderate	High	Low
80	Moderate	High	Low
90	Moderate	High	Low
100	Eliminated	Eliminated	Eliminated

Table 35. Risk Levels – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission without DoS Attacks

	TLS	PSK	MLS
Geolocate Forward Unit	Low	Eliminated	Eliminated
Geolocate UxS	Low	Low	Low
Impersonation	Moderate	High	Low

Table 36. Risk Levels – 100% Autonomous Operations with a Trigger Event Causing Periodic Video Transmission with DoS Attack

	TLS	PSK	MLS
Geolocate Forward Unit	Low	Eliminated	Eliminated
Geolocate UxS	Low	Low	Low
DoS Data Los	Moderate	Low	Low
Impersonation	Moderate	High	Low

C. RISK ANALYSIS

The resulting risk levels are determined by the security protocol, the autonomy scenario, and the presence of DoS attacks. This section analyzes the effects of these variables on risk level. This section also examines the trade space of risks versus SA to develop a decision matrix to determine which combination of variables is suitable for a given use case.

1. Impact of Variables

Figure 32 through Figure 35 show the difference between the baseline model risks and DoS model risks for geolocation and cyberattacks. The figures are used to assess the survivability of the TLS, PSK, and MLS security protocols and methods against the geolocation and cyberattack risks. The figures also assess the impact of DoS attacks on the risk levels. A detailed assessment is provided in the figure captions.

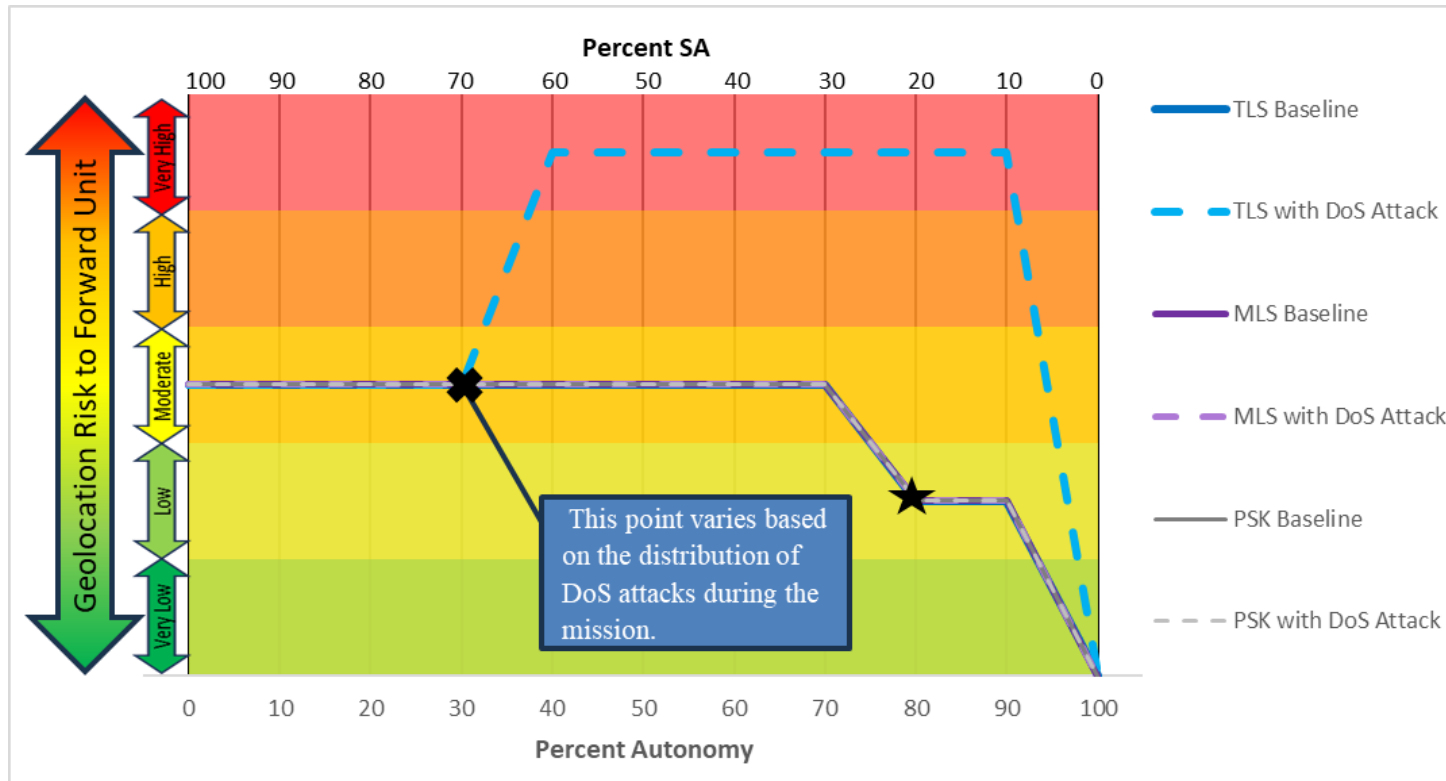


Figure 32. Geolocation of Forward Unit Risk Comparison. Except for TLS with DoS attacks, the risk of geolocating the forward unit is moderate for 0–70% autonomy and low for 80–90% autonomy. At 100% autonomy, the risk is eliminated. The TLS handshake causes a significant increase in data transmission following a DoS attack. This causes an increased risk. If DoS attacks are likely, it is recommended to use PSK or MLS to reduce risk. The spike in risk for TLS with DoS attacks does not always occur at 40% autonomy. The timing and frequency of DoS attacks are randomly generated within the model. Re-running the simulation results in a different distribution of DoS attacks during the mission, thus changing where the sudden increase in RF footprint occurs on the graph. Therefore, this point does not provide any insight. Instead, decision makers should consider the risk of geolocating the forward unit is unknown except at the extreme ends of the autonomy spectrum, 0% and 100% autonomy.

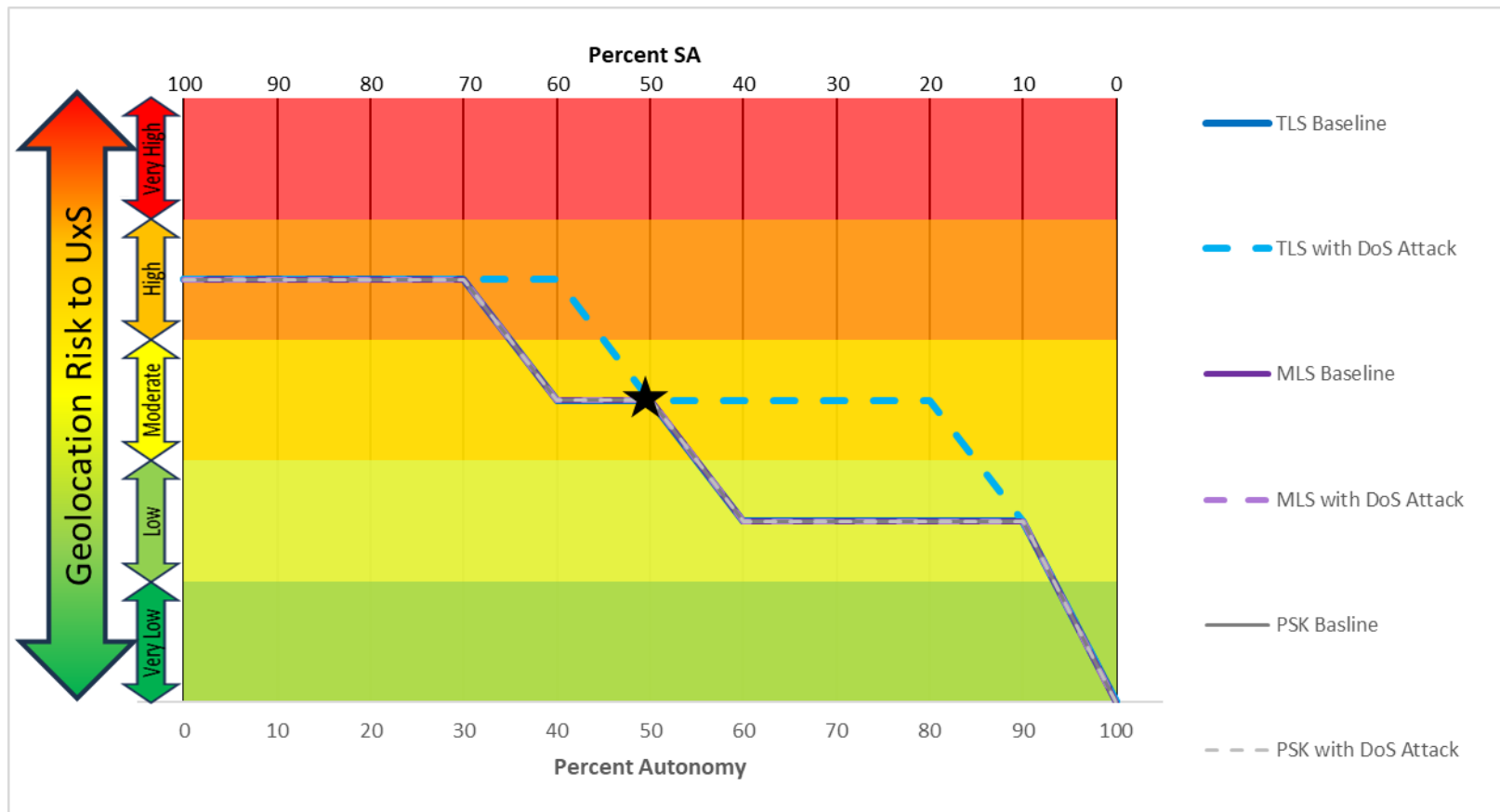


Figure 33. Geolocation of UxS Risk Comparison. Except for TLS with DoS attacks, the risk of geolocating the UxS is high for 0–30% autonomy and low for 60–90% autonomy. At 100% autonomy, the risk is eliminated. The TLS handshake causes a significant increase in data transmission following a DoS attack. This causes the risk to remain high for 30–40% autonomy and extends the range of autonomy for which the risk is moderate. If DoS attacks are likely, it is recommended to use PSK or MLS to reduce risk.

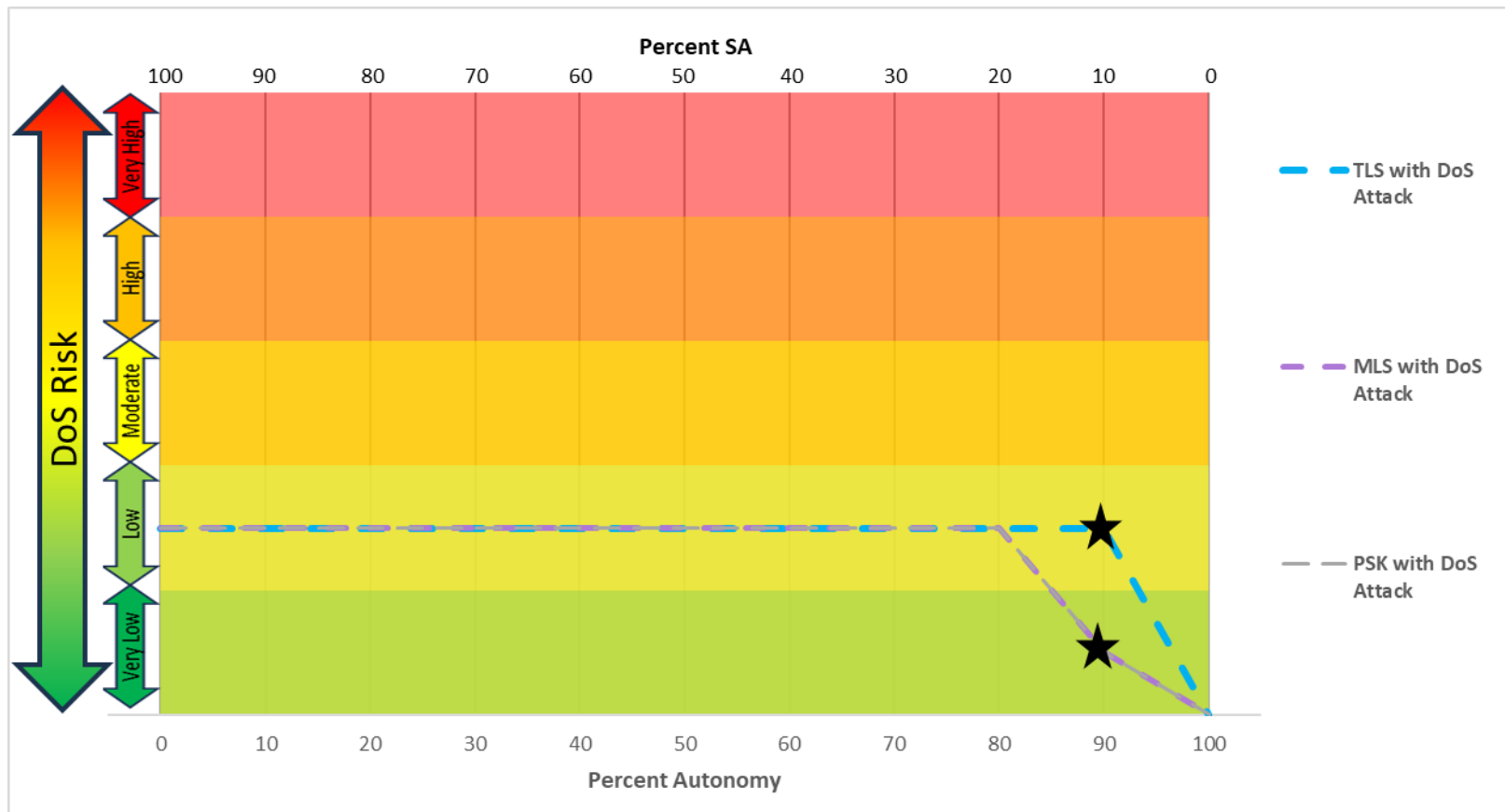


Figure 34. DoS Risk Comparison. The risk of a successful DoS attack preventing data transmission from the forward unit or UxS is low for 0–90% autonomy using TLS and PSK. Using MLS reduces the risk to very low at 90% autonomy. At 100% autonomy, the risk is eliminated.

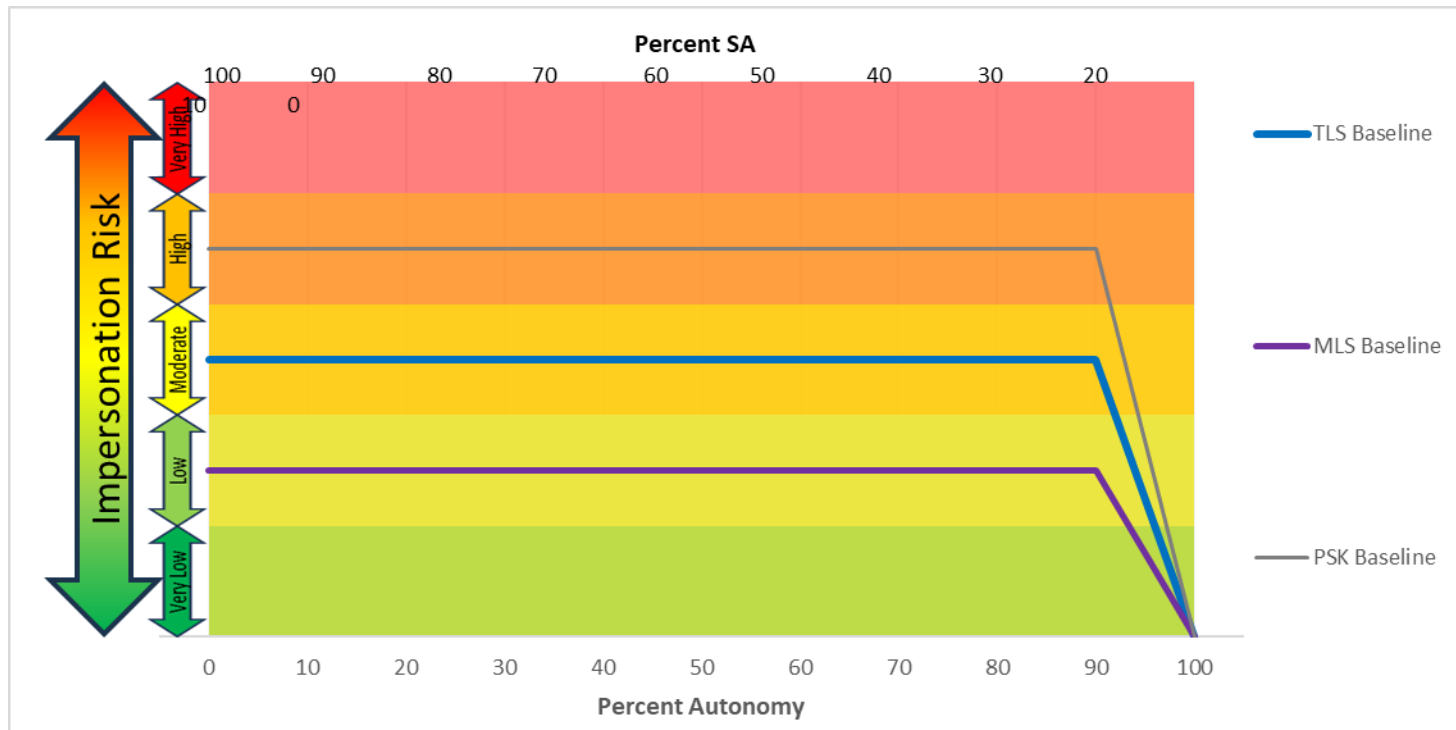


Figure 35. Impersonation Risk Comparison. The risk of a successful impersonation attack with MLS is low for all levels of autonomy up to 100% autonomy. MLS provides the shortest window of impersonation attack vulnerability of the three security protocols and methods assessed in this research because MLS allows adjustable key update frequencies. PSK has the largest impersonation attack vulnerability window, resulting in high risk. At 100% autonomy, the risk is eliminated as the UxS and forward unit are not expecting to receive commands or data. If the adversary attempts an impersonation attack during 100% autonomous operations, the UxS and forward unit will ignore the adversary. While the model in this research assumes the MLS key update occurs just before each mission (i.e., in MB transferred), this graph captures normal risk differences in which more frequent MLS key updates occur during the mission to shorten the vulnerability window.

Figure 36 and Figure 37 compare the operational risks of operating a UxS in a triggered event scenario. The risk of geolocating the unit is eliminated when using PSK or MLS due to their asynchronous capability. In this scenario, PSK and MLS do not require an acknowledgement signal from the forward unit when the UxS transmits data. This means the forward unit does not emit an RF footprint and remains hidden from the adversary. The risks of geolocation and impersonation are the same with or without a DoS attack. The risk of a DoS for MLS and PSK are low because they allow data transmission to resume immediately after the DoS attack. This risk of a DoS attack is moderate for TLS because TLS requires a handshake to reestablish connection, causing a longer delay in data transmission compared to MLS and PSK.

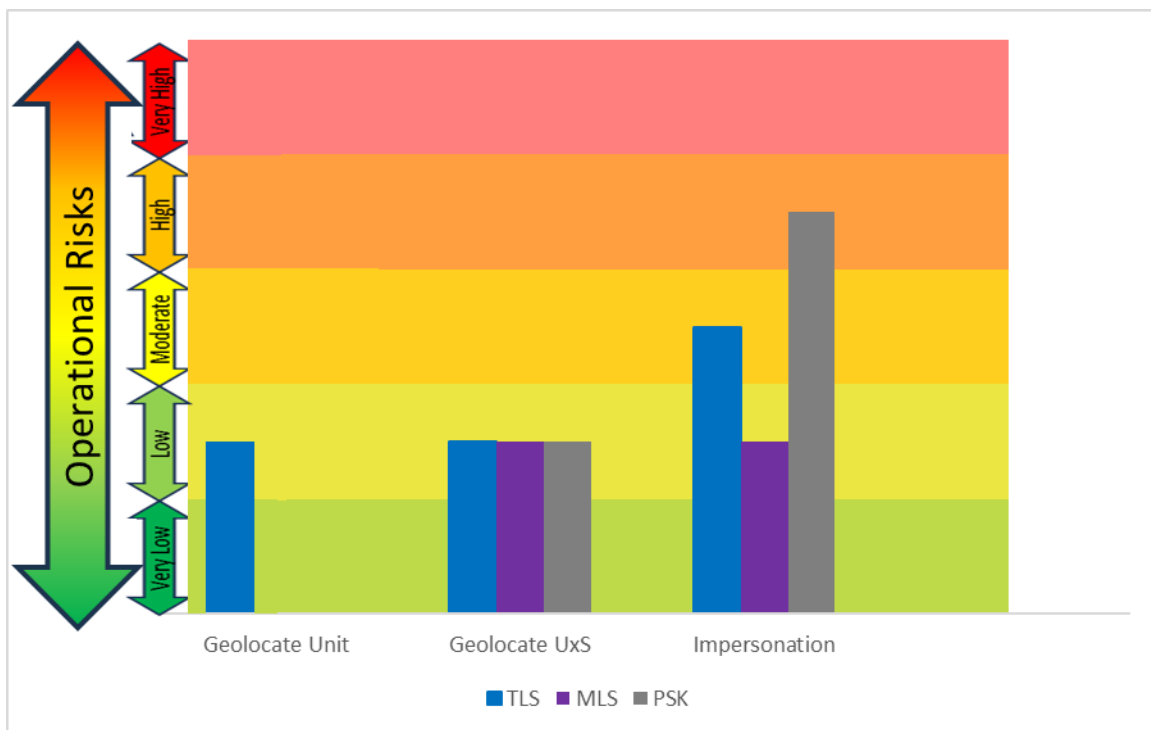


Figure 36. UxS Operational Risks of 100% Autonomous Operations with a Triggered Event Trigger Event Causing Periodic Video Transmission without DoS Attacks

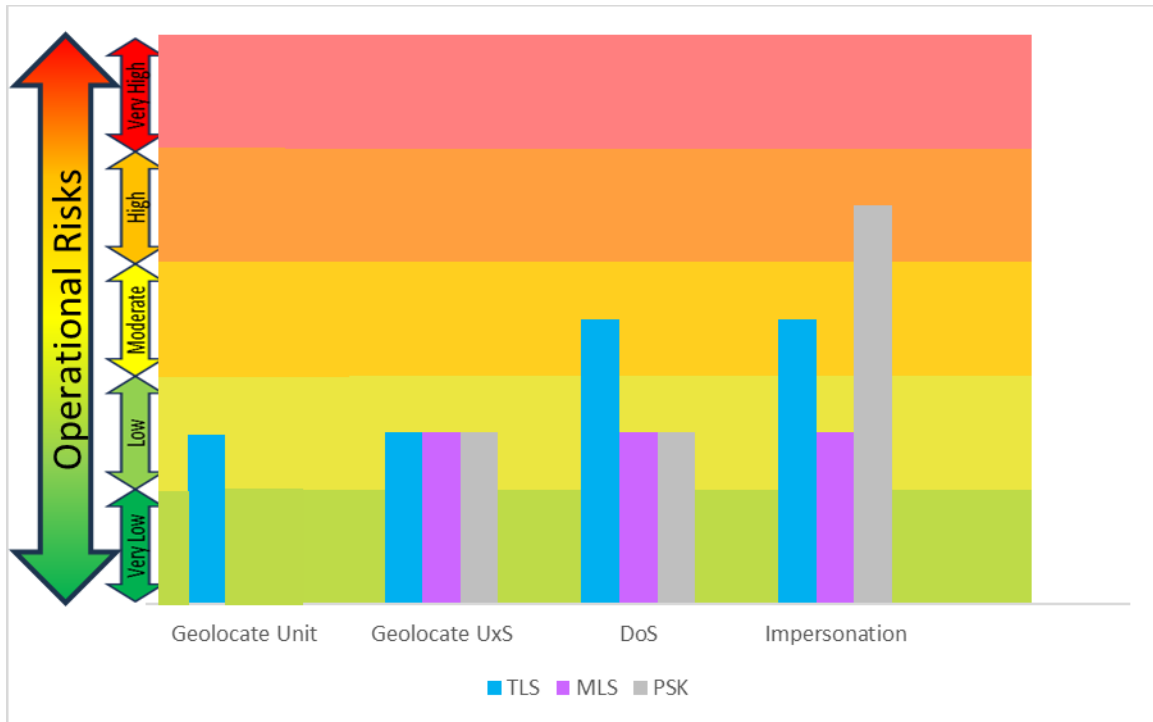


Figure 37. UxS Operational Risks of 100% Autonomous Operation with a Trigger Event Trigger Event Causing Periodic Video Transmission with DoS Attacks

2. Trade Space Analysis

To determine the best balance of RF risks and SA, the research team analyzes the graphs in Figure 38 through Figure 41. As established in Chapter IV.C.1, the geolocation and impersonation risks using MLS and PSK are unaffected by DoS attacks. Therefore, only the MLS and PSK scenarios with DoS are examined. The geolocation risks using TLS are affected by DoS attacks therefore TLS scenarios with and without DoS attacks are both examined. The risks of geolocation, DoS, and impersonation decrease in steps. For example, Figure 38 shows the risk of geolocating the UxS remains the same for 10%-30% autonomy. As autonomy increases, SA decreases. This means that an autonomy level of 30% provides the same level of UxS risk mitigation compared to 10% autonomy, but results in decreased SA. In other words, if a moderate risk of UxS geolocation is acceptable, it is preferable to use 10% autonomy to achieve the acceptable risk level while maintaining maximum SA. Another way to examine the trade space is to assess the

overall risk level. The overall risk is defined as the highest risk level for any operational risk. For example, Figure 41 shows the risks of geolocating the UxS and impersonation attacks as moderate for 0% autonomy. The risk of geolocating the UxS is high for 0% autonomy. Therefore, the overall risk for operations with 0% autonomy is high.

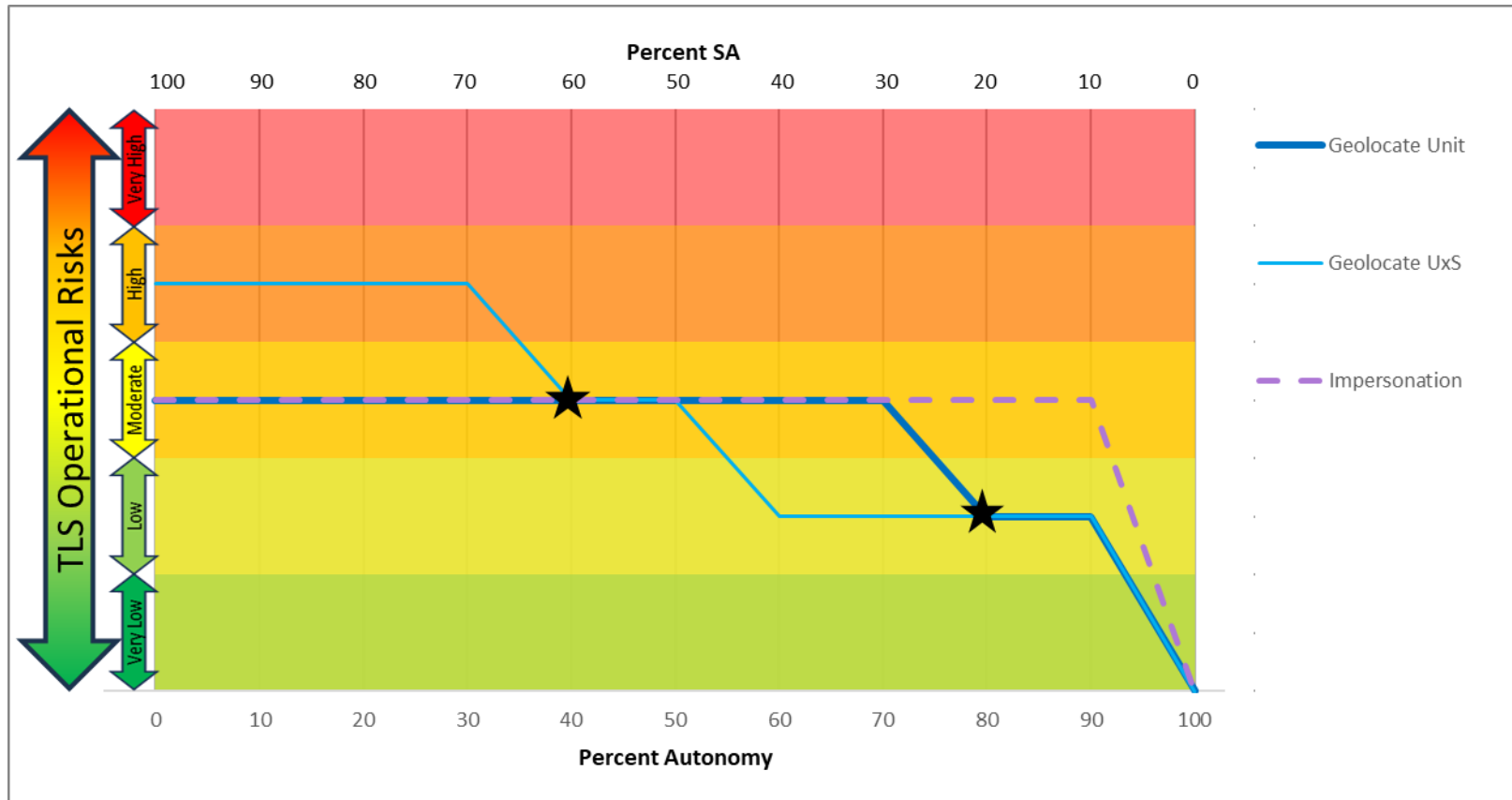


Figure 38. TLS Percent Autonomy Baseline Scenario Risk without DoS Attacks Trade Space. All operational risks are eliminated at 100% autonomy, however, the forward unit will not have any SA during the mission. If SA is desired, then the lowest achievable overall risk level is moderate. Using 80% autonomy will reduce the geolocations risk to low, however, the impersonation attack risk remains moderate. If the forward unit is willing to accept moderate risk, 40% autonomy can be utilized to maintain maximum SA.

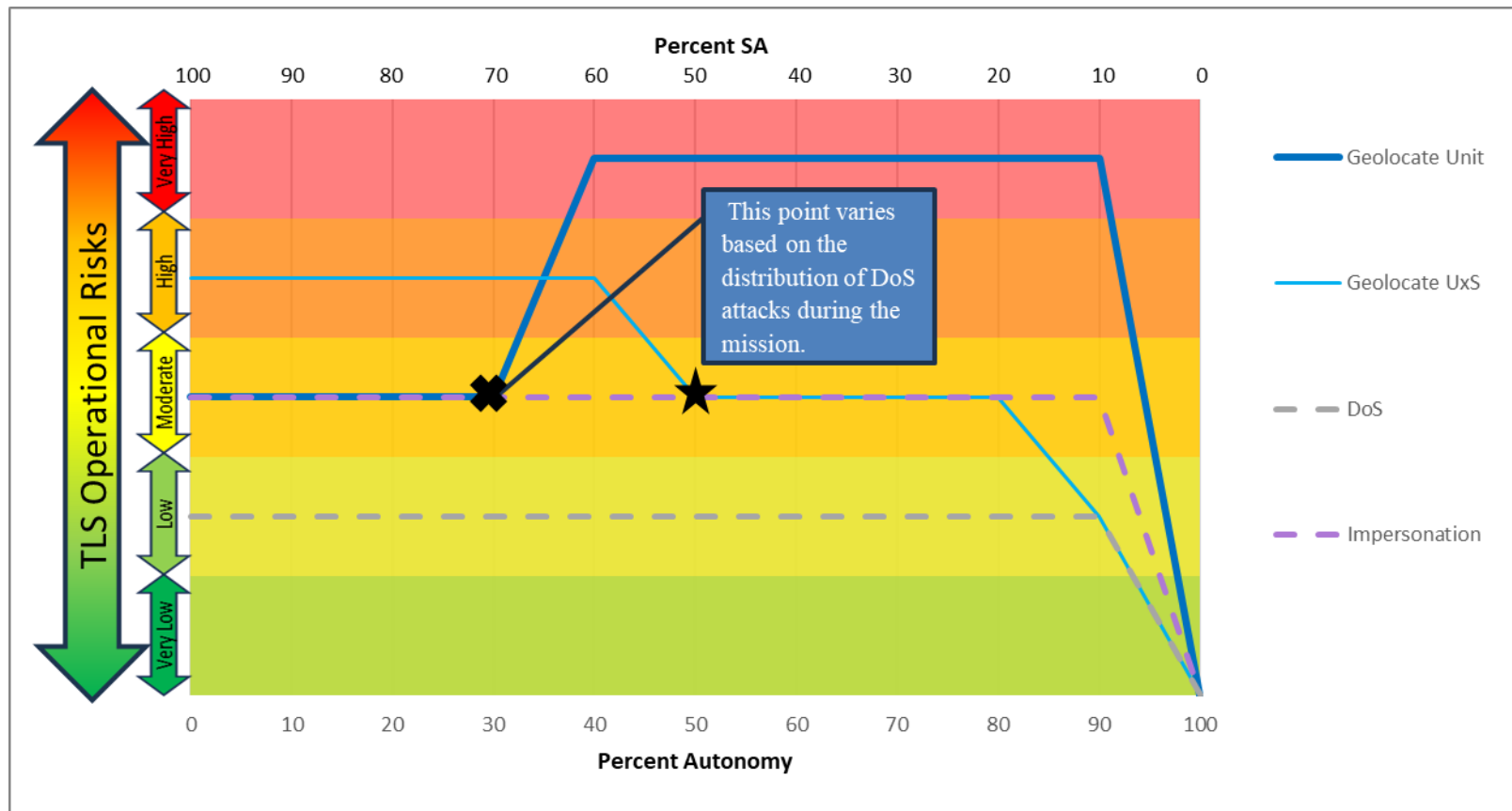


Figure 39. TLS Percent Autonomy DoS Scenario Risk with DoS Attacks Trade Space. The lowest achievable overall risk level is high without using full autonomy. Full autonomy is required to eliminate risk; therefore, the unit will not have SA during the mission. Full C2 (0% autonomy) should only be used if High risk is acceptable. The spike in risk for geolocation of the forward unit risk does not always occur at 40% autonomy. The timing and frequency of DoS attacks are randomly generated within the model. Re-running the simulation results in a different distribution of DoS attacks during the mission, thus changing where the sudden increase in RF footprint occurs on the graph. Therefore, this point does not provide any insight. Instead, decision makers should consider the risk of geolocating the forward unit is unknown except at the extreme ends of the autonomy spectrum, 0% and 100% autonomy. What this graph does show is that the other risks are reduced to moderate by using a minimum of 50% autonomy.

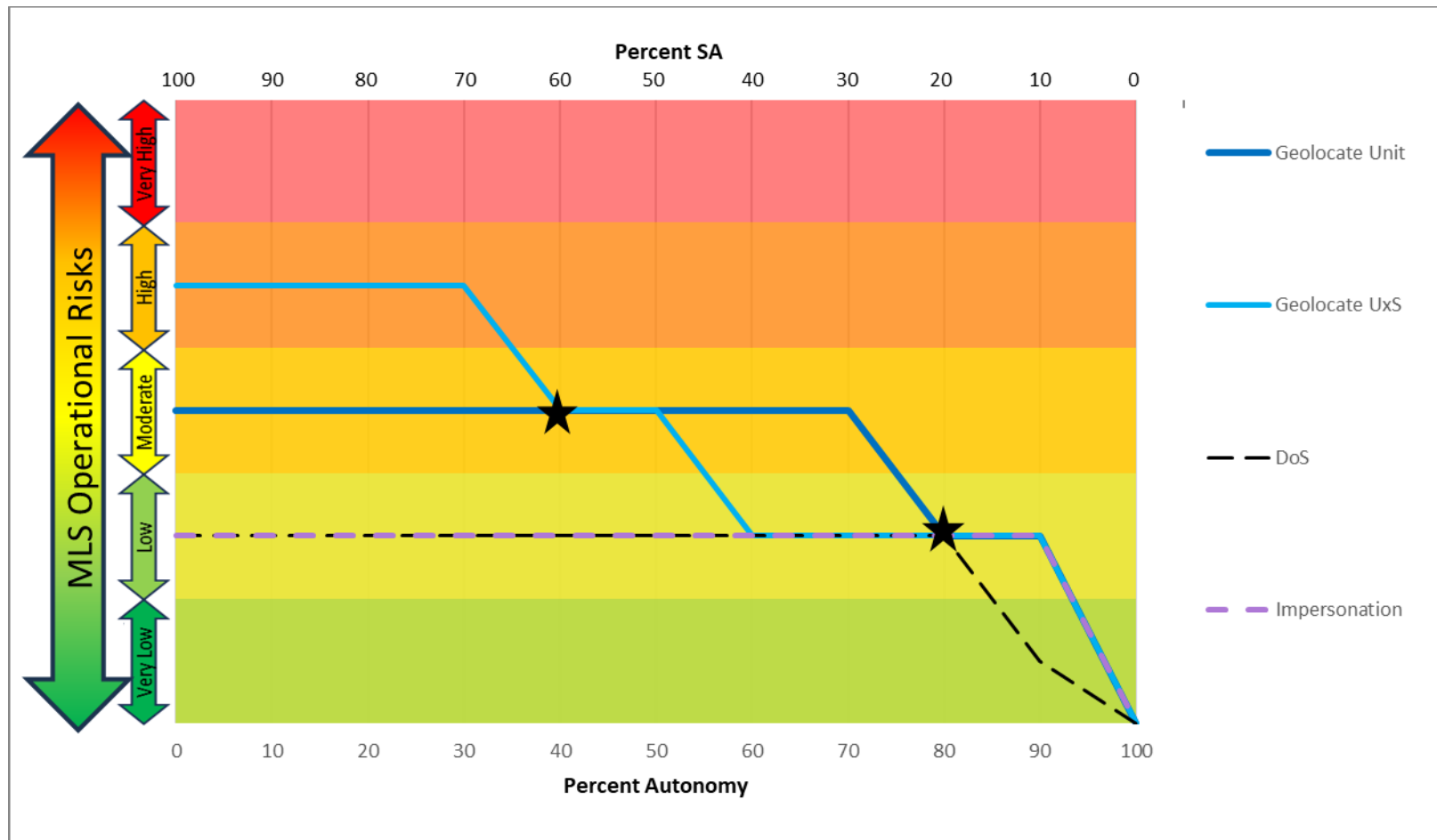


Figure 40. MLS Percent Autonomy Scenario with DoS Attacks Trade Space. The lowest achievable overall risk level is low without using full autonomy. Full autonomy is required to eliminate risk; therefore, the unit will not have SA during the mission. Using 80% autonomy will achieve low risk while providing maximum allowable SA for the desired risk level. If the forward unit is willing to accept moderate risk, 40% autonomy provides the most SA for moderate risk. Full C2 operation of the UxS results in high overall risk.

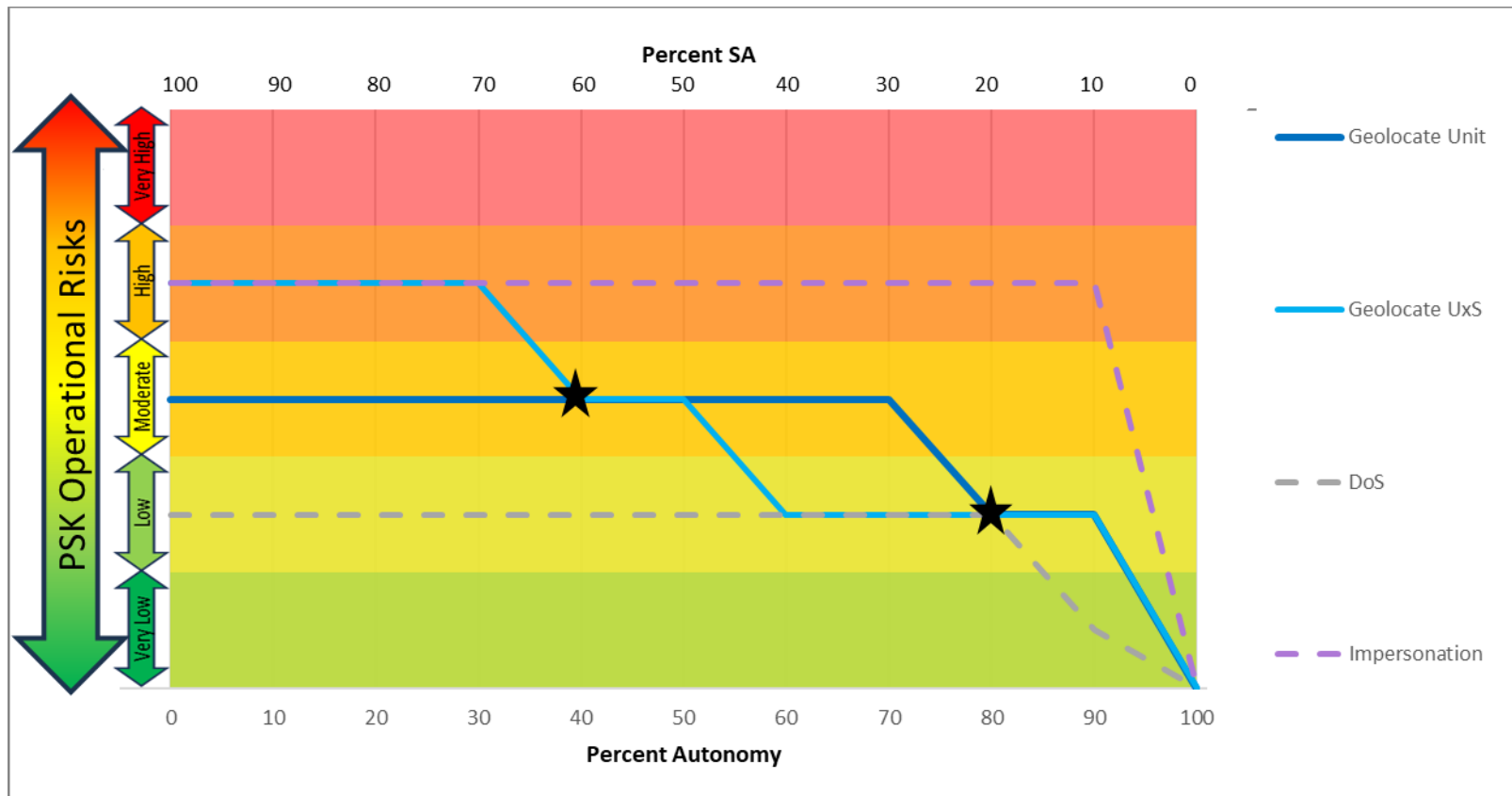


Figure 41. PSK Percent Autonomy Scenario with DoS Attacks Trade Space. The lowest achievable overall risk level is high due to PSK's low survivability against impersonation attacks. Full autonomy is required to eliminate risk; therefore, the unit will not have SA during the mission. If SA is required during a mission, 40% autonomy is recommended. Utilizing 40% autonomy reduces the geolocation risk to moderate while providing some SA, however, the impersonation attack risk remains high and can only be reduced or eliminated by using 100% autonomy or a different security protocol such as MLS. To reduce the geolocation risk to low, 80% autonomy is recommended, however, the overall risk remains high due to the impersonation attack risk level.

D. CHAPTER SUMMARY

Chapter IV defines RF risk that this report attempts to minimize and analyzes the model results. The results and analysis show how the security protocols and level of autonomy affect the operational risks of geolocation and cyberattacks. The research team analyzes the trade-offs between the autonomy, risks, and SA to develop a decision tree to aid unit commanders in selecting the best security protocol and level of autonomy for a given use case. The conclusions and decision tree are presented in Chapter V.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

This chapter summarizes the risk analysis conclusions and answers the research questions posed in Chapter I. The research team makes recommendations for the operation of UxS in a DMO/EABO environment to increase safety of personnel and mission success. The research team also recommends topics and questions for future study to further advance the findings of this report.

A. CONCLUSIONS

This report examines C2 of UxS using RF data links as detailed in Chapter II. During C2 of UxS an RF signal is emitted. If the adversary can confirm the presence of RF signals in their area of operations, then they know that our forces are nearby. Even if the adversary does not know what information is being transmitted, it is still possible to detect the signal and then locate the broadcasting location. This is a significant risk to not only the UxS equipment, but also the operators controlling it. The other risk during operations is the possibility of cyberattacks. To prevent the adversary from gathering, corrupting, or preventing the information being transmitted between the operator and the UxS, encryption and authentication is used. The different methods of data encryption and authentication create various added levels of RF footprint. Generally, the more security that a protocol provides, the greater the RF footprint. One thing that remains clear from the above research is that if the data link is active, then the adversary can listen, locate, and attack. This is an important consideration when conducting DMO/EABO operations because the friendly forces will often be secluded and closer to the adversary than in traditional warfare. In these types of missions, it might not be feasible to provide any type of assistance if the operators become compromised. That is why it is necessary to consider the above risk levels when choosing what type of equipment to use in DMO/EABO.

UxS autonomy is a valid means of reducing potential RF footprint and other risks to operators. As shown in the Chapter IV analysis, when the UxS runs in an autonomous state, the risk impact of creating an RF footprint is decreased. This is an important

consideration because there is no need to have an active traceable data link if it does not serve a useful purpose to the operators. The model and analysis show that a higher level of autonomy greatly decreases the amount of risk associated with the enemy being able to geolocate the UxS and its operators. While this is a good development in the DMO/EABO environment, there is a drawback. More autonomy will create a longer amount of time where the forward units do not have the most up to date SA. In the evaluated scenarios, the operators do not have a live video to see what is happening on the ground while the UxS is operating autonomously and recording video to send later.

The absence of SA poses a risk to the operators. This means that operators and commanders need to balance SA and RF footprint to provide the greatest level of UxS utility for the mission while limiting risks. The military often uses the phrase Mission, Enemy, Terrain, Troops available, Time, and Civilian Considerations. It is essentially a statement that military leadership uses during mission planning and execution that means some things can and will change. The idea is that instead of having one way of doing a task and only ever executing it that way; there should be considerations to help drive mission success. That is what needs to happen when balancing RF footprints with SA. Some missions and environments allow for greater autonomy than others, while some missions call for full SA. A decision needs to be made by military leaders and operators on how a specific mission should be executed to best serve the mission's needs and keep the operators out of harm's way. The trade space analysis in Chapter IV provides an example of how this might work.

B. RECOMMENDATIONS FOR UXS OPERATIONS IN DMO/EABO ENVIRONMENTS

Everyone identifies and characterizes risks in his or her own unique way. Each mission has a unique set of characteristics, parameters, threats, and importance. Any recommendations based off a risk analysis from an outside party should be taken with extreme caution. This section provides a decision tree based off the research conducted in this paper. One should keep in mind the narrow scope, assumptions, and constraints that bounded this research. There are multiple other factors that have not been considered in this research that may or may not affect mission risk. This decision tree should be built

upon with further research that is pertinent to this mission set and should only be used as an aid for an overall mission risk assessment by those with all the information for a particular mission.

To help unit commanders plan UxS missions in DMO/EABO environments, the research team proposes the decision tree presented in Figure 42. The decision tree enables unit commanders to determine which combination of UxS operational variables is best suited for an upcoming UxS mission. The decision tree presents a balance of autonomy to reduce the RF footprint risks while maintaining SA. For example, if the acceptable overall risk level is moderate and the mission and threat mirror the scenarios covered in this research, then 40% autonomy and the MLS protocol are recommended to maintain maximum SA at a moderate risk level.

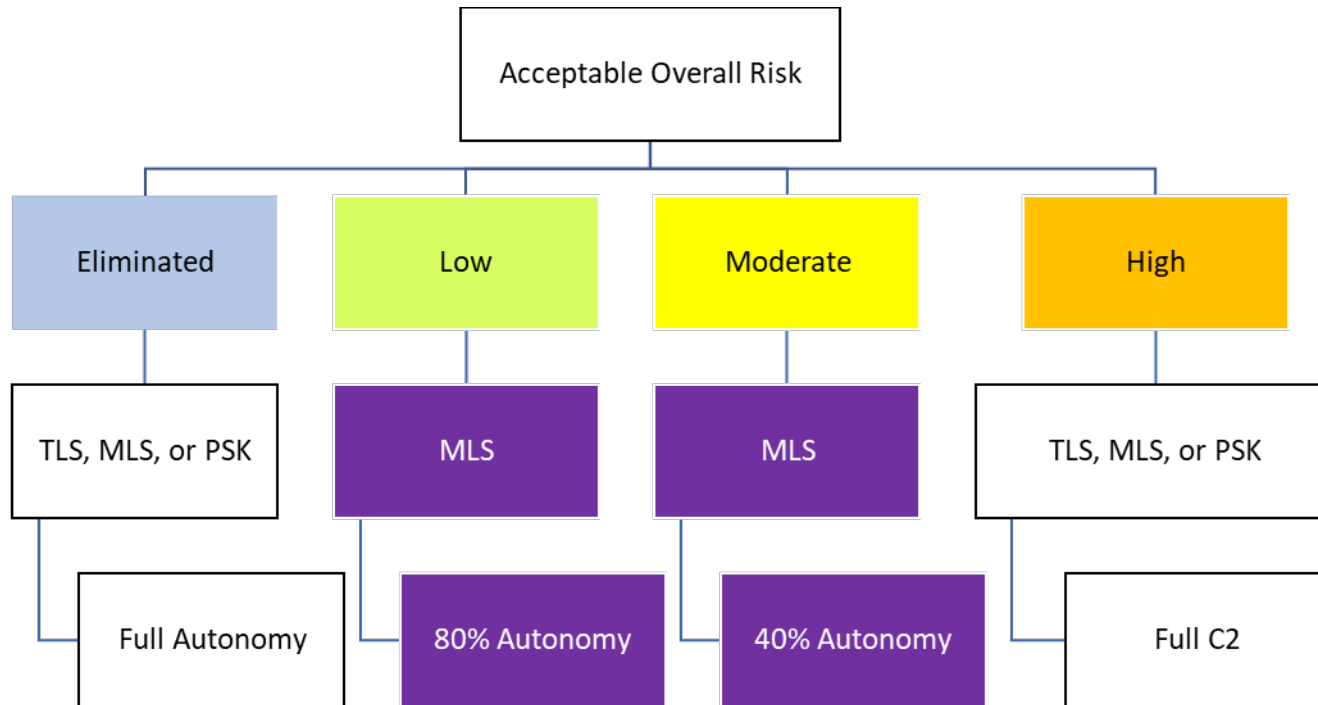


Figure 42. Decision Tree. If the acceptable risk level is moderate, MLS can be used with 40% autonomy to provide the maximum amount of situational awareness while remaining at moderate risk.

C. RECOMMENDATIONS FOR FUTURE RESEARCH

Operating a UxS in a swarm, where multiple UxS work together in a coordinated manner, can impact the RF footprint differently compared to operating an individual UxS. The increased communication activity and coordination among the UxS in a swarm can result in higher RF transmission and reception, potentially leading to a larger RF footprint. The collective RF emissions from multiple UxS operating in proximity can contribute to a more significant RF presence in the surrounding environment. Spectral congestion may occur if the swarm utilizes similar or overlapping frequency bands for communication, causing interference and reduced signal quality. Through collaborative spectrum management techniques, such as coordinating frequency channels or employing frequency hopping, the swarm can mitigate congestion and minimize the impact on the RF footprint. Mesh networking, commonly used in swarms, can extend the RF footprint by enabling multi-hop communication among UxS. Distributed data processing within the swarm may also increase RF communication due to data exchange and collaborative decision-making. Careful swarm management strategies and RF planning are essential to optimize the RF footprint and ensure efficient and reliable swarm operations.

Frequency-hopping spread spectrum (FHSS) is a wireless communication technique that involves rapidly changing frequencies in a predetermined pattern to transmit data over a wide frequency range. In FHSS, the available frequency spectrum is divided into narrowband channels, and the transmitter and receiver synchronize their hopping patterns (Techslang 2023). The transmitter hops from one frequency channel to another according to a predefined sequence, typically generated by a pseudorandom number generator or a predetermined pattern. This rapid frequency hopping offers several advantages. It enhances robustness against interference by allowing the system to avoid frequencies experiencing high levels of interference or noise (Techslang 2023). FHSS provides inherent security as the hopping pattern is known only to authorized devices, making it challenging for unauthorized users to intercept or disrupt the communication (Techslang 2023). Additionally, FHSS takes advantage of frequency diversity, spreading the signal across multiple frequencies to combat fading and multipath interference

(Techslang 2023). FHSS optimizes spectrum utilization, making efficient use of available frequency resources. FHSS spreads the transmitted signal over a wide range of frequencies by rapidly hopping between different frequency channels. This spreading effect reduces the power density at any given frequency, making the signal appear as low-level noise or interference. As a result, the RF footprint of FHSS is spread across a broader frequency range, reducing the likelihood of an attack and detection by adversaries.

One area of future research that needs to be explored is how to protect the UxS. While the connection protocol can help protect the data transmission, there are still plenty of counter UxS methods on the battlefield that will need to be mitigated. For example, if the mission is to conduct a reconnaissance of a certain enemy military installation, it is necessary to know what makes that installation unique and what type of counter UxS defense systems would be most effective (Tan, Van Bossuyt, and Hale 2021). Along with that concept, it is possible that some defense systems might have unforeseen flaws, such as interoperability (Hale and Van Bossuyt 2021). If the UxS operators can understand what possible defense systems they will face, they will be able to maximize their chance of mission success.

Understanding how to overcome the counter measures can lead to better mission success, but it is still necessary to protect the UxS itself. This implies that it is necessary to understand specific attack types that could affect the UxS and what the consequences would be on the mission. Since a lot of current military equipment is capable of being interconnected, there are many ways for the enemy to carry out a cyberattack. One way to mitigate these risks is to work the mitigation methods into the original design of the system (O'Halloran, Papakonstantinou, and Van Bossuyt 2018). Having these mitigation techniques included early in the design will likely lead to more successful mission operations and prevent expensive fixes later in the system life cycle.

Lastly, one of the goals of this research paper was to find possible ways to minimize a UxS RF footprint. While this team focused on how autonomy can decrease the footprint, there are other areas to consider. For example, how important is the UxS itself? Is it acceptable to have the actual UxS be exposed to the enemy if the operators are

well protected? The article “Securing Software Updates under Receiver Radio Frequency Geolocation Risk” explores how to minimize the RF footprint on the receiving end of radio transmissions to complete software downloads (Hayden, Sweeney, and Hale 2022). The idea of minimizing the receiving end could prove useful, as that is the UxS operators in this research team’s scenarios. If the operator geolocation risk can be mitigated or almost eliminated, then autonomy may not be necessary providing better SA for the ground forces.

The research team used Innoslate as the MBSE tool to model and simulate operational scenarios for this research. It was quickly determined partway through the research that Innoslate is somewhat limited in its flexibility in dealing with this type of simulation. For future research that builds upon this paper, the research team recommends using a different tool for increased fidelity and ease of use where multiple input variables are used.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. MLS MODEL DETAILS

This appendix details the development of the MLS percent autonomy models and MLS triggered event models.

A. MLS PERCENT AUTONOMY MODEL DETAILS

The top-level MLS percent autonomy model is shown in Figure 44. In this section, a description of each step of the model is presented and overall operations are explained.

While developing these models, the research team quickly realized simulation of a 100-minute mission that delves down to the byte level of transmission presents an issue. Simulations at that level result in extremely long runtimes that usually ended up crashing the Innoslate modeling tool and requires the research team to try again. To help alleviate this issue, the 100-minute mission model is broken down into 10-minute segments which can be adjusted afterwards to account for a full mission. Additionally, certain activities within the model are examined and adjusted to further reduce simulation runtime and computational requirements. The final adjustment to the model is to multiply the data transmission loop (block F.4.2.2 of Figure 44) by 100 to alleviate this issue. Figure 43 depicts the MLS communication timing sequence to illustrate the back-and-forth data transfer between the C2 unit and the UxS, it is a representation for how the model works.

MLS, unlike TLS, does not require a handshake to reestablish communications if contact has already occurred at a prior time. MLS does require periodic key updates to maintain effective communication security. Key update typically occurs on a frequency “of hours or days, and not milliseconds” (RFC 9420 2023). For this research, the MLS key update occurs at the beginning and end of each mission and is excluded from the model.

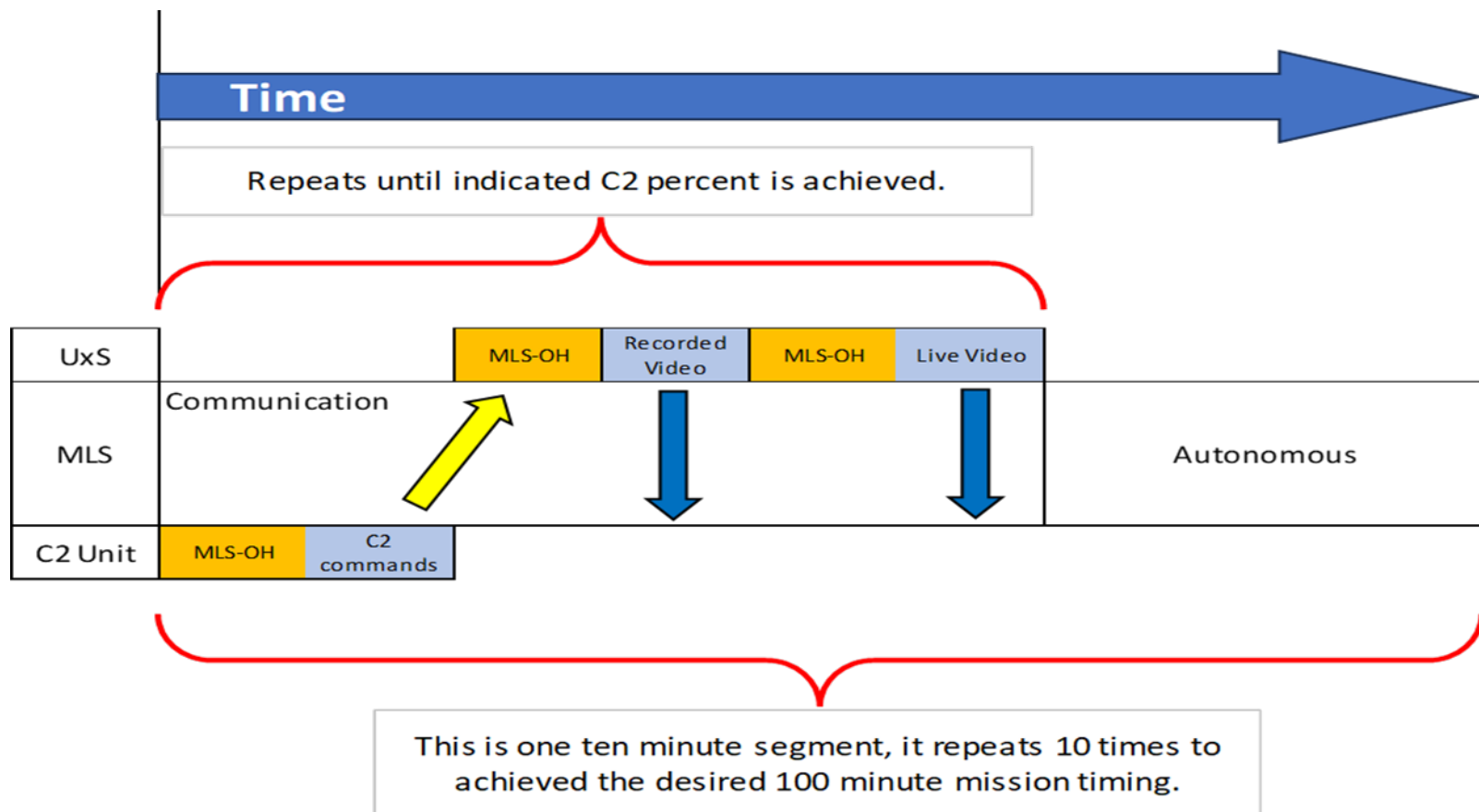


Figure 43. MLS Communication Timing Sequence

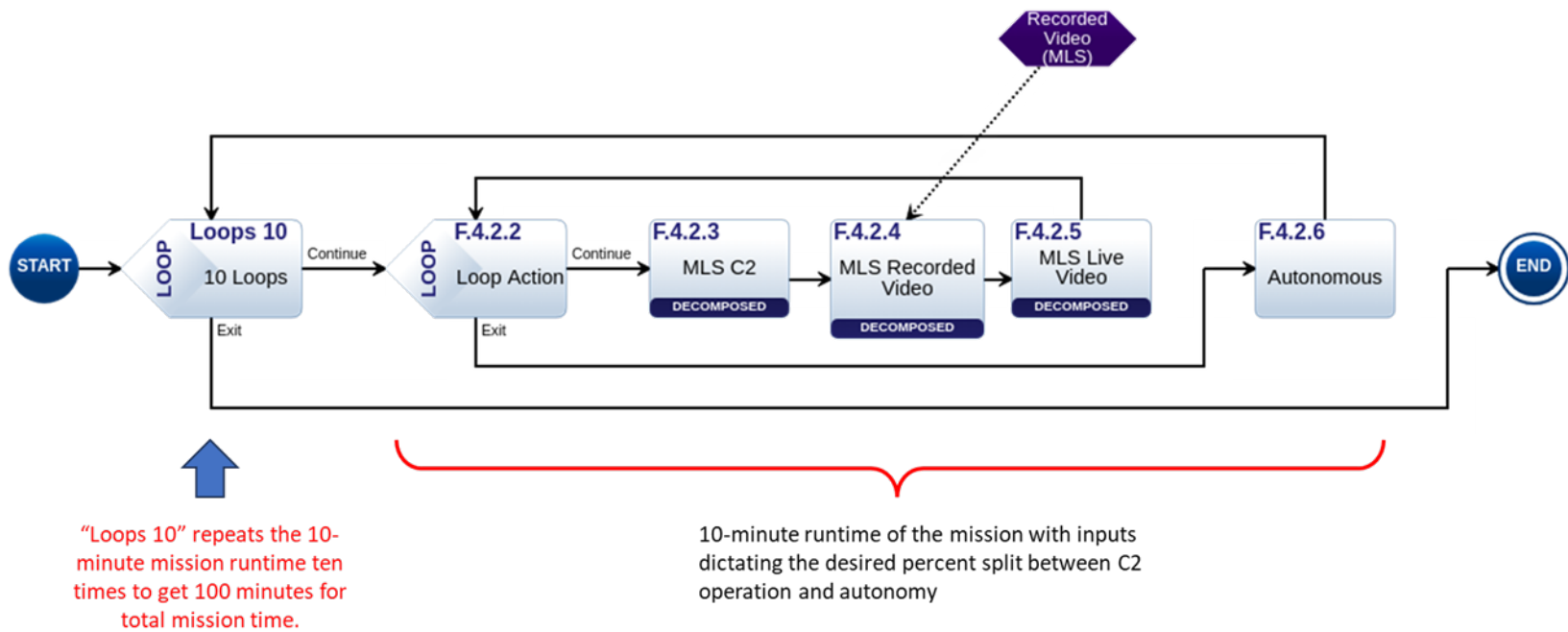


Figure 44. MLS Percent Autonomy Model

1. MLS C2 and Autonomous Operation Timing

From Figure 44, the Loop Action (F.4.2.2) determines the length of time the UxS is controlled by the forward unit providing C2 to the UxS and receiving real time SA data from the UxS. Parameters internal to F.4.2.2 are manipulated to obtain the correct percentage balance between C2 and Autonomous operation for model runs. Each action or block inside this loop runs sequentially one time before looping back to repeat again and again until the predetermined C2 timing is satisfied for a particular simulation run. When the timing requirement is satisfied, the model leaves the loop, and the system enters the autonomous mode of operation. The actions and behaviors internal to the loop operation include: C2 data transmission, recorded video (download), and live video operations. These actions and behaviors are detailed in Section A.A.2. through Section A.A.4.

2. MLS C2 Data Transmission

MLS C2 data transmission is represented in Figure 44 as F.4.2.3. Internal details on the actions that occur during this activity are shown in Figure 45. During this activity, the forward unit sends C2 command messages to the UxS to adjust UxS mission parameters and operational actions in real-time. MLS can operate in an asynchronous mode where an intended recipient of the signal does not have to be present to return an acknowledgement signal to indicate the data was received correctly before exiting to the next operation. This is a major difference between TLS and MLS and greatly affects the transmission of data in periods of interference or attacks. After the data is sent, an acknowledgement signal is not necessary and the model immediately moves to the next operational block, transmission of recorded video from the UxS to the C2 station.

Again, like with TLS, the C2 and live video signals require a constant data rate of information flow, 50 kbps and 57 Mbps respectively, while the recorded video can be sent at any rate until download is complete, this caused a problem in the model resulting in an inflated overhead count for the C2 signal. The C2 signal is very small compared to the video signals, to establish the correct bit rate for the C2 signal, each loop of data transfer only requires 14 bytes of actual C2 data compared to 16 kB for live video and

11.6 kB for recorded video. This means that each 14-byte C2 packet gets an additional 171 bytes of overhead data that MLS requires and grossly inflates the C2 transmission times. Since this is not realistic or practical in real world applications, a scaling factor was applied to the C2 overhead signal resulting in one C2 data packet of 16 kB only requiring one overhead byte count of 171 bytes. This maintains equality in the models for a fair comparison of the protocols.

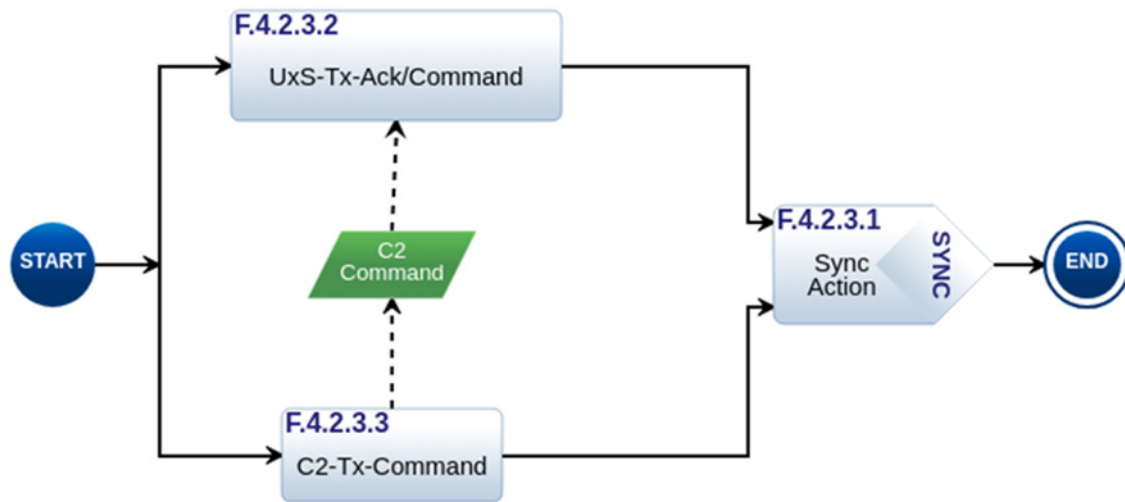


Figure 45. MLS C2 Data Transmission Model (F.4.2.3)

3. MLS Recorded Video Transmission

Figure 46 shows the recorded video transmission operation of the model. This operation is shown in Figure 44 as F.4.2.4. Like the TLS model described in Chapter III, video is recorded and transmitted for the autonomous duration of a mission. The recorded video file is represented as the purple “Recorded Video (MLS)” resource block shown in Figure 46. The parameters of this resource block are set for each simulation and depend on the length of time the system operates in autonomous mode before C2 initiations during the mission. The model limits the number of C2 initiations to ten for every simulation for ease of implementation and minimized complexity. The input to the resource block is the predetermined file size in bytes. Each time the model cycles through

this operation, a set number of bytes is subtracted from the resource block which is dependent on which communication/security protocol is used.

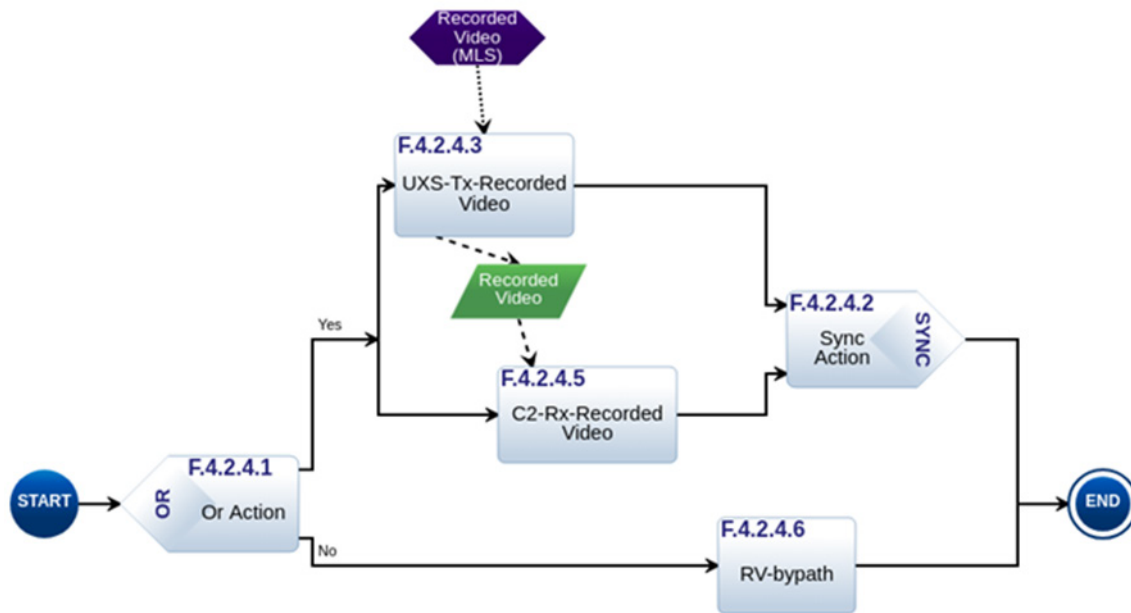


Figure 46. MLS Recorded Video Transmission (F.4.2.4)

Upon entry into this operation, if the recorded video file size is greater than zero, the “YES” path from the “OR” operator (F.4.2.4.1) will be chosen. This path results in the UxS transmitting one packet of recorded video to the C2 personnel and immediately exits the block for the next operation. After the video download is complete, the “OR” operation will choose the “NO” path (recorded video size =0) to skip further attempts to transmit data, eliminating this step from the rest of C2 control process.

4. MLS Live Video Transmission

Upon exiting the recorded video transmission operation (F.4.2.4), the system enters the MLS live video operation (F.4.2.5) to transmit one packet of real-time live video to the C2 personnel so they have SA while they’re linked and communicating with the UxS. Figure 47 shows the internal processes for this portion of the mode. This block runs for the entire time C2 personnel are communicating with the UxS. The live video

bandwidth required for video the chosen resolution and bit depth is detailed in Table 4 and is consistent in all the models, this limits the bandwidth available for transmitting the recorded video file and receiving C2 data.

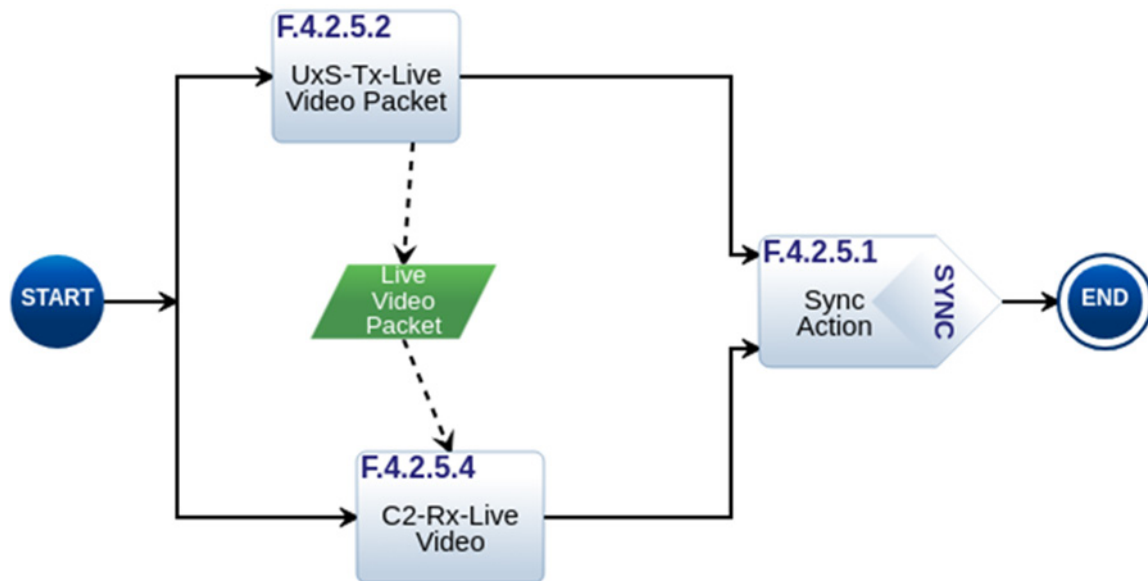


Figure 47. MLS Live Video Transmission (F.4.2.5)

Upon exiting this live video transmission block, the next operation depends on whether the system has met its time or percentage requirement for C2 operations. If it has, the system will move to autonomous operations next, if not, it will continue the loop until it does.

B. MLS TRIGGERED EVENT MODEL

As detailed Chapter II, Section D.2, the “Triggered Event Model” is a scenario where either an object is identified by the UxS using some level of on-board AI, such as image recognition of a target, or when the UxS arrives at a designated GPS coordinate. The triggering artifact will cause the UxS to download data to the operator for evaluation to determine if the detected object is of operational interest and needs further investigation. If further inquiry is needed, C2 personnel can take full control of the UxS to do so.

To keep simulations comparable from one run to the next, the model does not exercise the further investigation pathway (F.3.2.6) if a triggering event occurs. Figure 48 shows the top-level operational steps for this scenario.

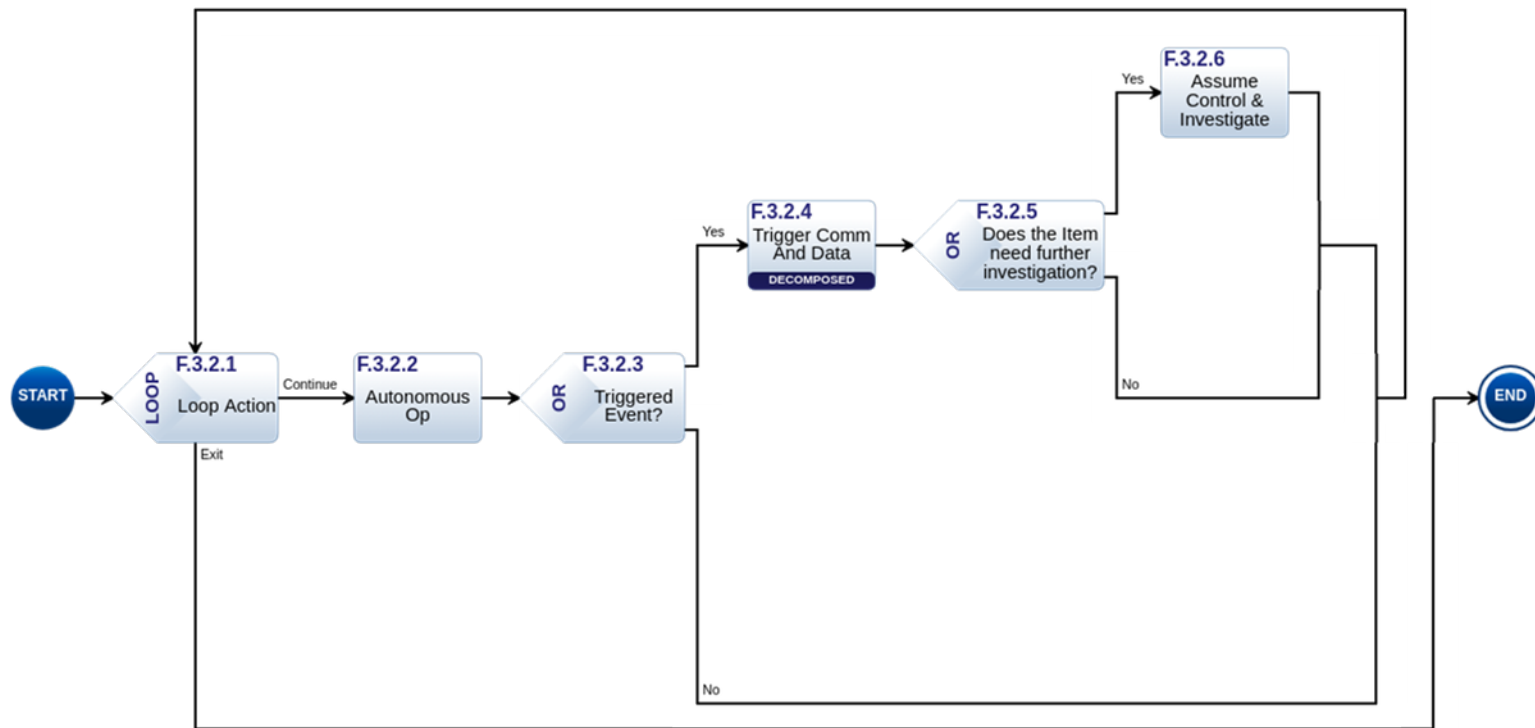


Figure 48. MLS Triggered Event Model

1. MLS Trigger Autonomous Operation and Triggering Event

The autonomous operation shown in Figure 48 as block F.3.2.2 represents the time the UxS is operating in an autonomous mode that is free of any transmitted RF signals. The duration of this activity can be set to any value and is dependent on overall mission parameters. Block F.3.2.3 is a probabilistic determination on whether a triggering event occurs during the mission. This probability can be set anywhere between zero and one hundred percent depending on the expected threat level for any given mission. For all the models, the research team chose to use a probability that results in an average mission having ten triggered events. As detailed in the TLS Model section, each triggered event will result in three minutes of mission video to be transmitted back to the C2 personnel for evaluation and mission adjustment if it is deemed necessary. Ten triggering events was again chosen by the research team as it will equate to a total of 30 minutes of mission video (30% of the 100-minute mission) to be sent back to the C2 team and limit the transmission time from the UxS to keep the approximate RF footprint low and keeping the models the same for comparison.

2. MLS Triggered Communications

In the event a triggering event occurs, the model enters the “Trigger Comm and Data” activity block shown as F.3.2.4 in Figure 48 and is decomposed into its smaller activities shown in Figure 49. Once this activity is initiated, the UxS proceeds to transmit the relevant data that caused the trigger for further examination by C2 personnel. For the purposes of this project and to keep consistency with each simulation, the research team chose to make all the triggered downloads three minutes of recorded video. The rationale for three minutes is to help provide the time just before and after the triggered event to provide some context to the data. After download is complete, the C2 personnel have the option to take control of the UxS to investigate the triggering activity or let the system continue to operate autonomously. In all the models, this investigation option is always set to “No” to remove it as a variable and maintain comparable outputs.

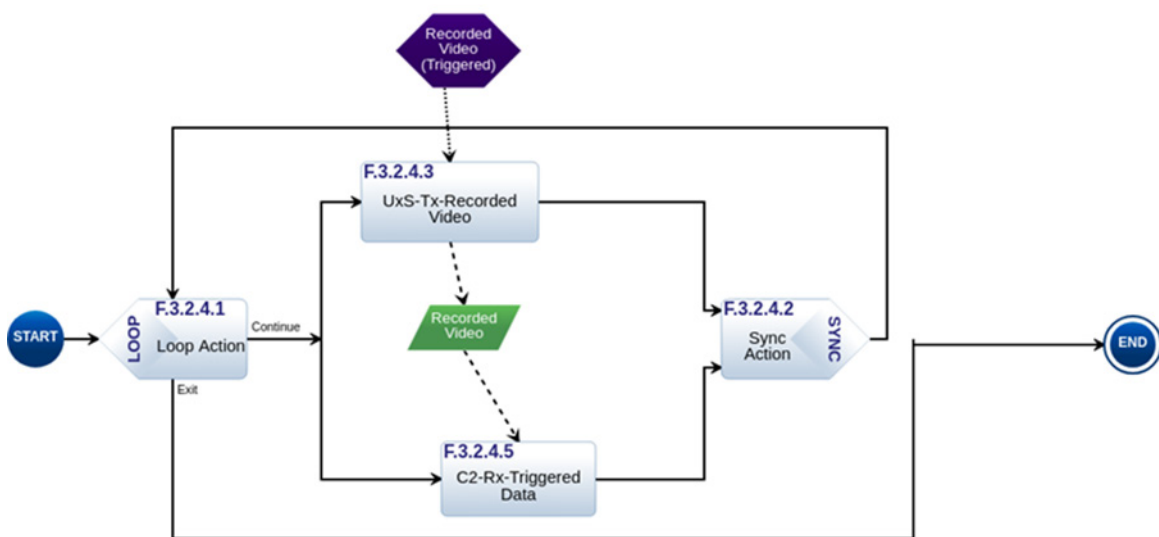


Figure 49. Download Triggered Data (F.3.2.4)

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. PSK MODEL DETAILS

This appendix details the development of the PSK percent autonomy models and PSK triggered event models.

A. PSK PERCENT AUTONOMY MODEL DETAILS

The top-level PSK percent autonomy model is shown in Figure 51. In this section, a description of each step of the PSK model is presented and overall operations are explained. PSK and MLS are very similar in functionality and their models are almost identical, the only difference being the slight difference in overhead during communication. Like MLS, the PSK handshake will occur before the mission since the keys need to be manually loaded onto the assets. Therefore, the model does not include a handshake.

Like the previous models, due to limitation in the simulation tool, the 100-minute mission model is broken down into 10-minute segments which can be adjusted afterwards to account for a full mission. Additionally, certain activities within the model were examined and adjusted to further reduce simulation runtime and computational requirements. The final adjustment to the model is to multiply the data transmission loop (block F.4.3.2 of Figure 51) by 100 to alleviate this issue. Figure 50 depicts the MLS communication timing sequence to illustrate the back-and-forth data transfer between the C2 unit and the UxS, it is a representation for how the model works.

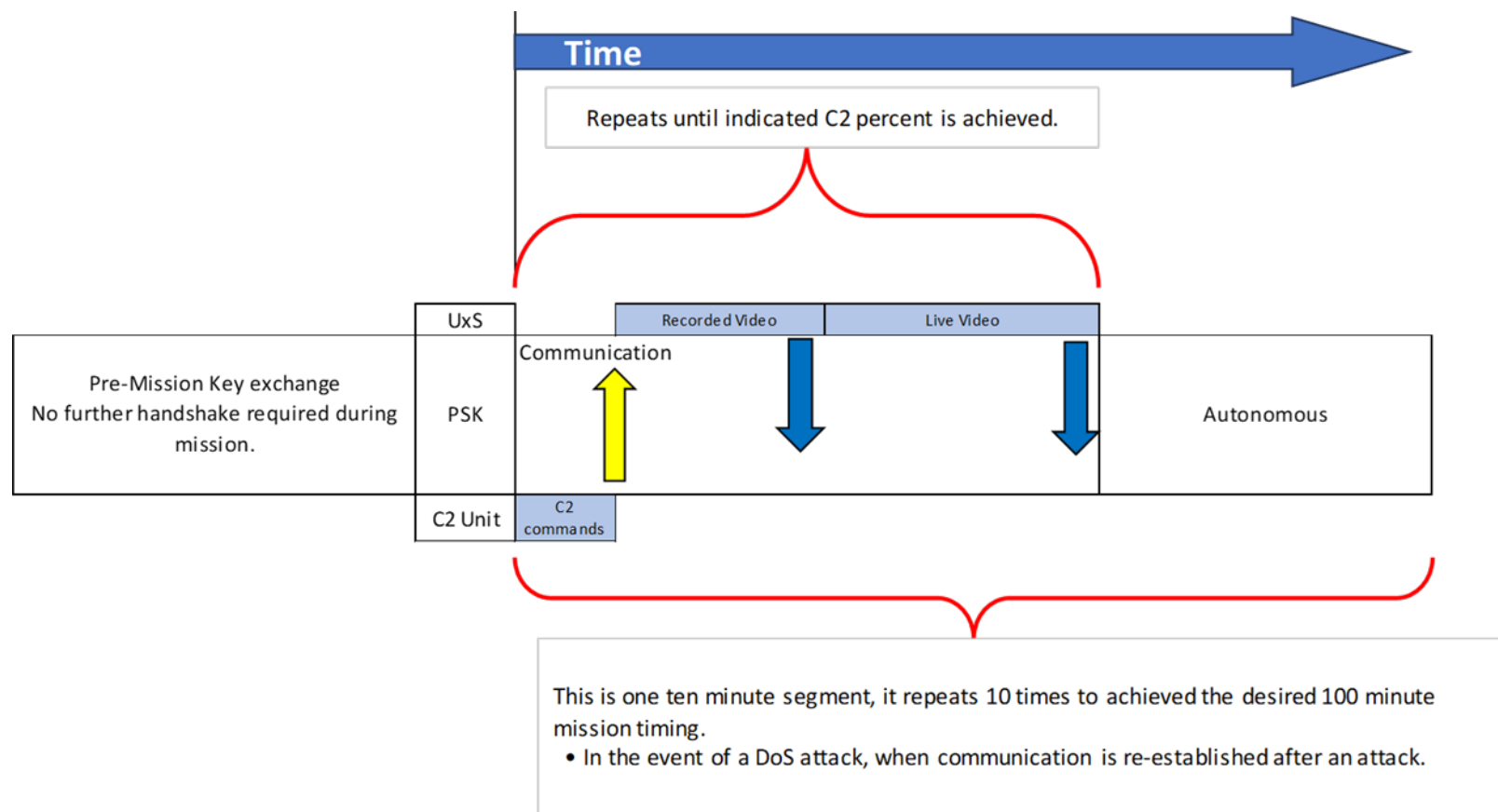


Figure 50. PSK Communication Timing Sequence

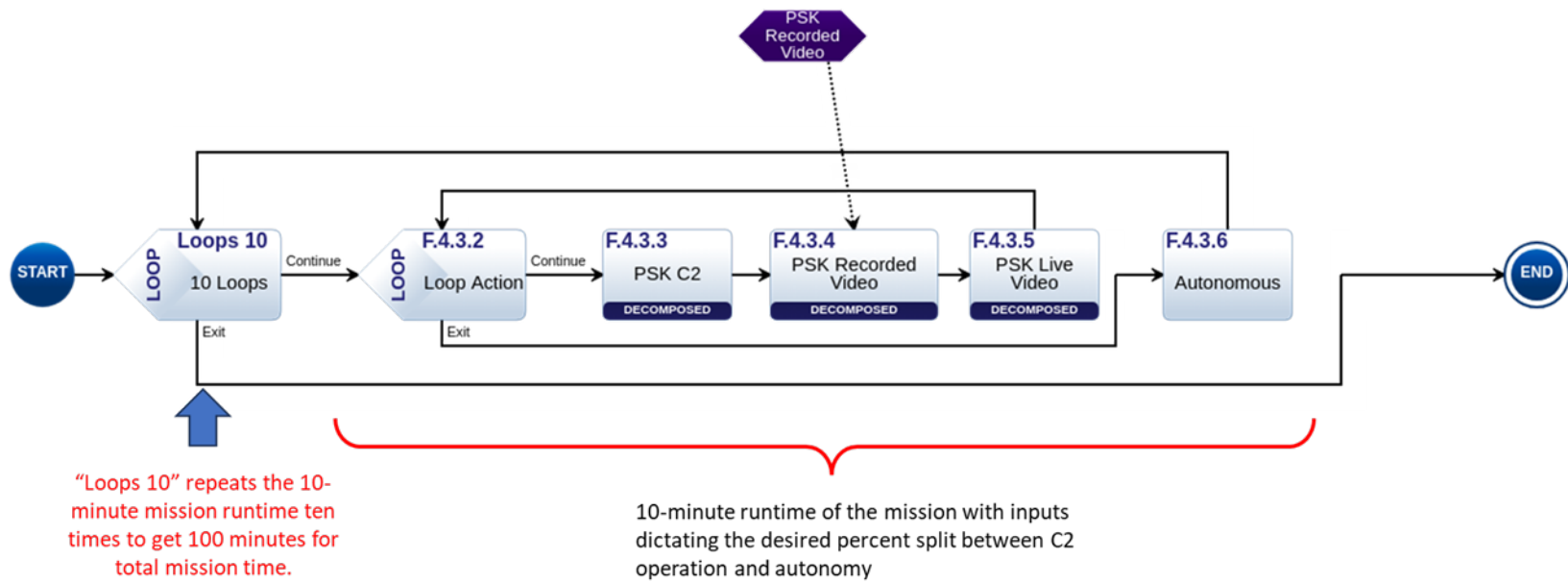


Figure 51. PSK Percent Autonomy Model

1. PSK C2 and Autonomous Operation Timing

From Figure 51, the Loop Action (F.4.3.2) determines the length of time the UxS is controlled by the forward unit providing C2 to the UxS and receiving real time SA data from the UxS. Parameters internal to F.4.3.2 are manipulated to obtain the correct percentage balance between C2 and Autonomous operation for model runs. Each action or block inside this loop runs sequentially one time before looping back to repeat again and again until the predetermined C2 timing is satisfied for a particular simulation run. When the timing requirement is satisfied, the model leaves the loop, and the system enters the autonomous mode of operation. The actions and behaviors internal to the loop operation include: C2 data transmission, recorded video (download), and live video operations. These actions and behaviors are detailed in Section B.A.2 through Section B.A.4.

2. PSK C2 Data Transmission

PSK C2 data transmission is represented in Figure 51 as F.4.3.3. Internal details on the actions that occur during this activity are shown in Figure 52. During this activity, the forward unit sends C2 command messages to the UxS to adjust UxS mission parameters and operational actions in real-time. PSK can operate in an asynchronous mode where an intended recipient of the signal being sent does not have to be present to return an acknowledgement signal to indicate the data was received correctly before exiting to the next operation. Like with MLS, this is a major difference between TLS and PSK and greatly affects the transmission of data in periods of interference or attacks. After the signal is sent, and acknowledgement signal is not necessary and the model immediately moves to the next operational block, transmission of recorded video from the UxS to the C2 station.

Again, like with TLS and MLS, the C2 and live video signals require a constant data rate of information flow, 50 kbps and 57 Mbps respectively, while the recorded video can be sent at any rate until download is complete, this caused a problem in the model resulting in an inflated overhead count for the C2 signal. Like the other scenarios, the C2 signal is very small compared to the video signals, to establish the correct bit rate

for the C2 signal, each loop of data transfer only requires 14 bytes of actual C2 data compared to 16 kB for live video and 11.3 kB for recorded video. This means that each 14-byte C2 packet gets an additional 200 bytes of overhead data that PSK requires and grossly inflates the C2 transmission times. Since this is not realistic or practical in real world applications, a scaling factor was applied to the C2 overhead signal resulting in one C2 data packet of 16 kB only requiring one overhead byte count of 200 bytes. This maintains equality in the models for a fair comparison of the protocols.

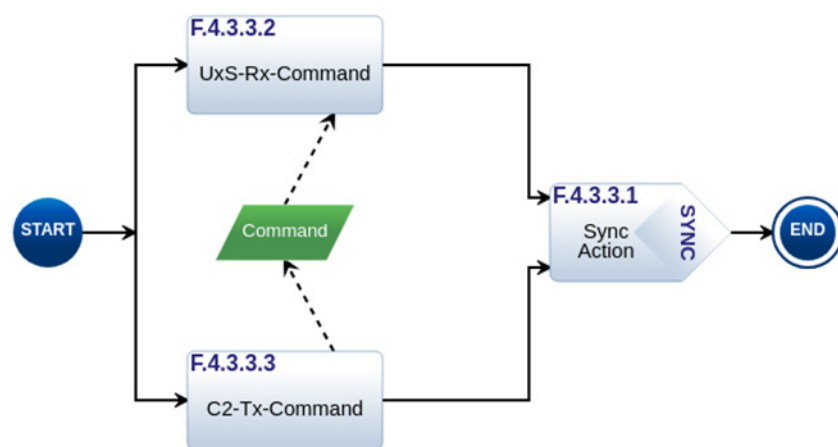


Figure 52. PSK C2 Data Transmission Model (F.4.3.3)

3. PSK Recorded Video Transmission

Figure 53 shows the recorded video transmission operation of the model. This operation is shown in Figure 51 as F.4.3.4. Like the TLS model described in Chapter III, video is recorded and transmitted for the autonomous duration of a mission. The recorded video file is represented as the purple “PSK Recorded Video” resource block shown in Figure 51. The parameters of this resource block are set for each simulation and depend on the length of time the system operates in autonomous mode before C2 initiations during the mission. The model limits the number of C2 initiations to ten for every simulation for ease of implementation and minimize complexity. The input to the resource block is the predetermined file size in bytes. Each time the model cycles through

this operation, a set number of bytes is subtracted from the resource block which is dependent on which communication/security protocol is used.

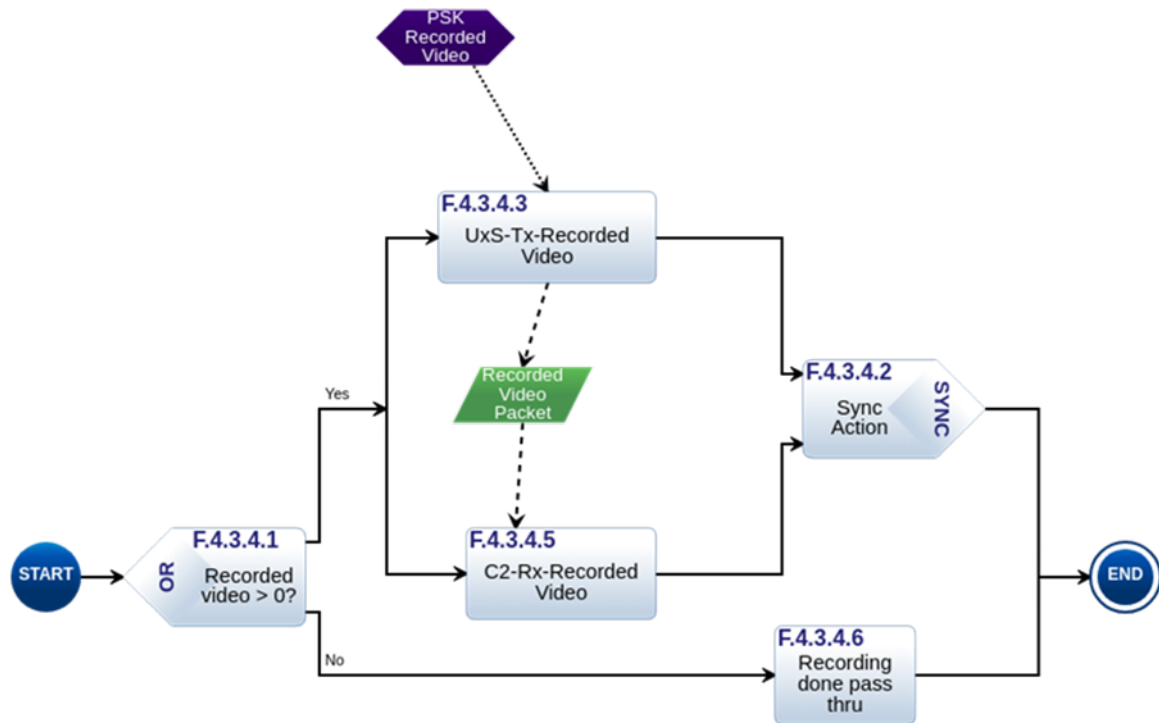


Figure 53. PSK Recorded Video Transmission (F.4.3.4)

Upon entry into this operation, if the recorded video file size is greater than zero, the “YES” path from the “OR” operator (F.4.3.4.1) will be chosen. This path results in the UxS transmitting one packet of recorded video to the C2 personnel before exiting the block for the next operation. After the video download is complete, the “OR” operation will choose the “NO” path (recorded video size =0) to skip further attempts to transmit data, eliminating this step from the rest of C2 control process.

4. PSK Live Video Transmission

Upon exiting the recorded video transmission operation (F.4.3.4), the system enters the PSK live video operation (F.4.3.5) to transmit one packet of real-time live video to the C2 personnel so they have SA while they’re linked and communicating with

the UxS. Figure 54 shows the internal processes for this portion of the mode. This block runs for the entire time C2 personnel are communicating with the UxS. The live video bandwidth required for video the chosen resolution and bit depth is detailed in Table 4 and is consistent in all the models, this limits the bandwidth available for transmitting the recorded video file and receiving C2 data.

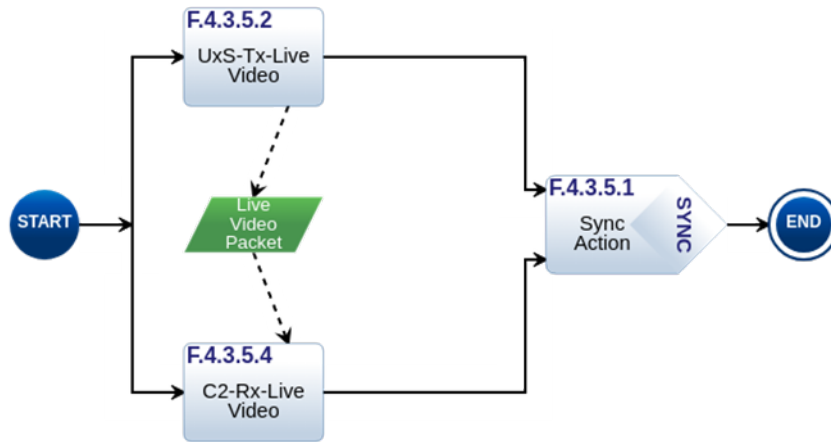


Figure 54. PSK Live Video Transmission (F.4.3.5)

Upon exiting this live video transmission block, the next operation depends on whether the system has met its time or percentage requirement for C2 operations. If it has, the system will move to autonomous operations next, if not, it will continue the loop until it does.

B. PSK TRIGGERED EVENT MODEL

As detailed Chapter II, Section D.2, the “Triggered Event Model” is a scenario where either an object is identified by the UxS using some level of on-board AI, such as image recognition of a target, or when the UxS arrives at a designated GPS coordinate. The triggering artifact will cause the UxS to download data to the operator for evaluation to determine if the detected object is of operational interest and needs further investigation. If further inquiry is needed, C2 personnel can take full control of the UxS to do so.

To keep simulations comparable from one run to the next, the model does not exercise the further investigation pathway (F.3.3.10) if a triggering event occurs. Figure 55 shows the top-level operational steps for this scenario.

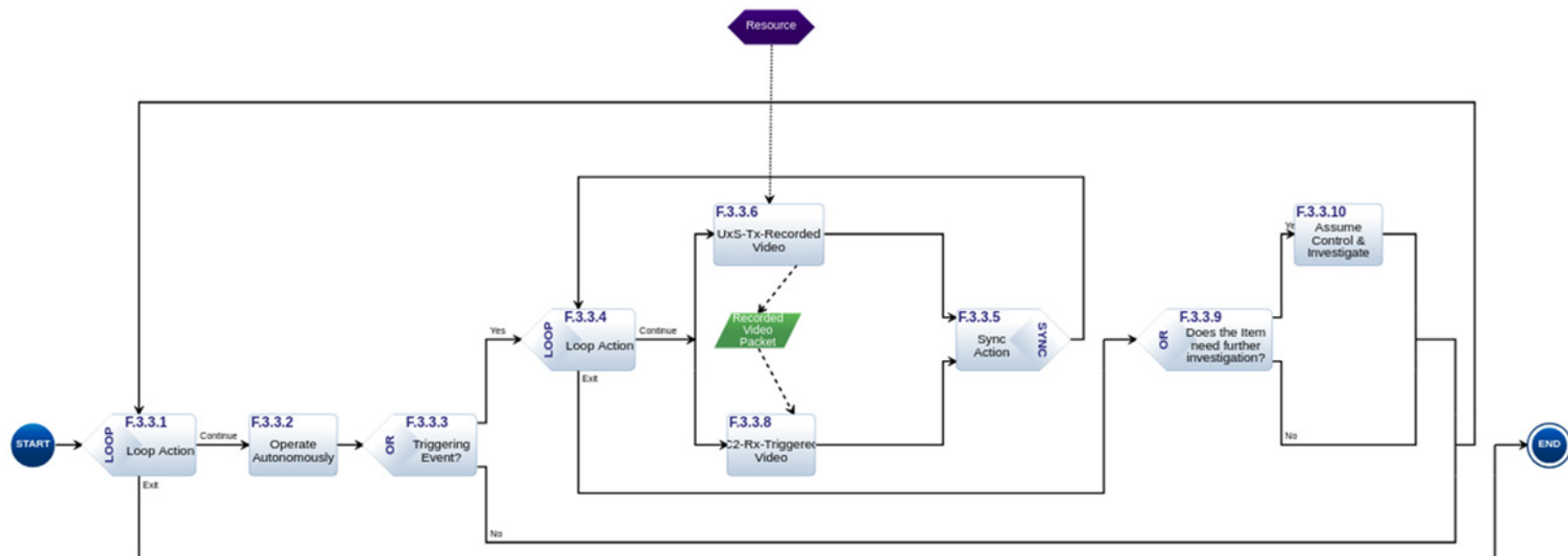


Figure 55. PSK Triggered Event Model

1. PSK Trigger Autonomous Operation And Triggering Event

The autonomous operation shown in Figure 55 as block F.3.3.2 represents the time the UxS is operating in an autonomous mode that is free of any transmitted RF signals. The duration of this activity can be set to any value and is dependent on overall mission parameters. Block F.3.3.3 is a probabilistic determination on whether a triggering event occurs during the mission and was chosen to be the same as the TLS and MLS models.

2. PSK Triggered Communications

In the event a triggering event occurs, the model enters the communication portion of the model starting at block F.3.3.4 of Figure 55. Once this activity is initiated, the UxS proceeds to transmit the relevant data that caused the trigger for further examination by C2 personnel. As with the other models, after a three-minute video is downloaded, the C2 personnel have the option to take control of the UxS to investigate the triggering activity or let the system continue to operate autonomously. In all the models, this investigation option is always set to “No” to remove it as a variable and maintain comparable outputs.

LIST OF REFERENCES

- 911 Security. 2023. "Drone Communication – Data Link." Accessed May 10, 2023. <https://www.911security.com/learn/airspace-security/drone-fundamentals/drone-communication-data-link>.
- Barbeau, Michel, Jyanthi Hall, and Evangelos Kranakis. 2006. "Detecting Impersonation Attacks in Future Wireless and Mobile Networks." In *Secure Mobile Ad-Hoc Networks and Sensors*, edited by Mike Burmester and Alec Yasinsac, 4074:80–95. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/11801412_8.
- Britt, Chris, Andre Leon, and Britta Hale. 2022. "C2 Superiority in an Era of Technological Competition." The Cyber Edge. September 30, 2022. <https://www.afcea.org/signal-media/cyber-edge/c2-superiority-era-technological-competition>.
- Bones, Michelle, Leonard Bunch, Ken Fisher, Stephanie Mara, Alex Stone. 2018. "Data Fusion Architecture for Undersea Warfare with Autonomous Underwater Vehicles." Capstone Project Report, Naval Postgraduate School. <https://hdl.handle.net/10945/59583>.
- CircleHD. 2019. "How to Accurately Calculate Video File Size (Plus: Bonus Glossary)." November 13, 2019. <https://www.circlehd.com/blog/how-to-calculate-video-file-size>.
- Cook, Sam. 2023. "20+ DDoS Attack Statistics and Facts for 2018–2023." Comparitech (blog). June 13, 2023. <https://www.comparitech.com/blog/information-security/ddos-statistics-facts/>.
- Cornell University Library. 2003. "Moving Theory into Practice Digital Imaging Tutorial." Accessed April 5, 2023. <http://preservationtutorial.library.cornell.edu/contents.html>.
- Department of Defense. 2018. *Summary of the 2018 National Defense Strategy of the United States of America*. Washington, DC: Department of Defense, 2018. <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
- Department of the Navy. 2021. *Unmanned Campaign Framework*. Washington, DC: Department of the Navy, 2021. https://www.navy.mil/Portals/1/Strategic/20210315%20Unmanned%20Campaign_Final_LowRes.pdf?ver=LtCZ-BPIWki6vCBTdgtDMA%3D%3D.

- Dinc, Mustafa. 2009. "Design considerations for military data link architecture in enabling integration of intelligent unmanned air vehicles (UAVs) with navy units." In NATO SCI Conference, Germany. 2009. https://www.researchgate.net/profile/Mustafa-Dinc-4/publication/323839640_Design_Considerations_for_Military_Data_Link_Architecture_in_Enabling_Integration_of_Intelligent_Unmanned_Air_Vehicles_UAVs_with_Navy_Units/links/5aaebc76a6fdcc1bc0bc743a/Design-Considerations-for-Military-Data-Link-Architecture-in-Enabling-Integration-of-Intelligent-Unmanned-Air-Vehicles-UAVs-with-Navy-Units.pdf.
- Dowling, Benjamin, and Britta Hale. 2020. "There Can Be No Compromise: The Necessity of Ratcheted Authentication in Secure Messaging." *Cryptology ePrint Archive*. June 5, 2020. <https://eprint.iacr.org/2020/541.pdf>.
- Dowling, Benjamin, and Britta Hale. 2021. "Secure Messaging Authentication against Active Man-in-the-Middle Attacks." In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, 54–70. Vienna, Austria: IEEE. <https://doi.org/10.1109/EuroSP51992.2021.00015>.
- Gupta, Brij, and Amrita Dahiya. 2021. *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures*. First edition. CRC Focus. Boca Raton London New York: CRC Press.
- Hale, Britta, and Douglas Van Bossuyt. 2021. "Counter-Unmanned Aerial Systems for the Navy and Marine Corps: Future Hardware Development Needs." Naval Research Program executive summary, Naval Postgraduate School. <https://calhoun.nps.edu/handle/10945/6979>.
- Hayden, Blake, Matthew Sweeney, and Britta Hale. 2022. "Securing Software Updates under Receiver Radio Frequency Geolocation Risk." In *MILCOM 2022 – 2022 IEEE Military Communications Conference (MILCOM)*, 643–48. Rockville, MD, USA: IEEE. <https://doi.org/10.1109/MILCOM55135.2022.10017775>.
- Leon, Andre and Christopher Britt. 2022. "UXS Authentication And Key Exchange Requirements For Multidomain Operation And Joint Interoperability." Master's thesis, Naval Postgraduate School. <https://calhoun.nps.edu/handle/10945/70738>.
- Lewis, Floyd. 2022. "Visual Modeling And Simulation Of Cryptographic Protocols Under Contested Environments." Master's thesis, Naval Postgraduate School. <https://hdl.handle.net/10945/71497>.
- Microsoft. 2023. "Transport Layer Security Protocol." August 1, 2023. <https://learn.microsoft.com/en-us/windows-server/security/tls/transport-layer-security-protocol>.

- National Institute of Standards and Technology. 2012. *Guide for Conducting Risk Assessments*. NIST Special Publication 800-30 Revision 1. Gaithersburg, MD: U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.
- Naval Air Systems Command. 2023. “Group 1 Small Unmanned Aircraft Systems.” Accessed April 4, 2023. <https://www.navair.navy.mil/product/Group-1-Small-Unmanned-Aircraft-Systems>.
- O’Halloran, Bryan M., Nikolaos Papakonstantinou, and Douglas L. Van Bossuyt. 2018. “Assessing the Consequence of Cyber and Physical Malicious Attacks in Complex, Cyber-Physical Systems During Early System Design.” In *2018 IEEE 16th International Conference on Industrial Informatics (INDIN)*, 733–40. Porto: IEEE. <https://doi.org/10.1109/INDIN.2018.8471937>.
- Poisel, Richard. 2019. *RF Electronics for Electronic Warfare*. Artech House Electronic Warfare Library. Boston, MA: Artech House. <https://ebookcentral.proquest.com/lib/ebook-nps/detail.action?docID=5988152&pq-origsite=primo>.
- Progni, Ilir. 2011. *Geolocation of RF Signals: Principles and Simulations*. New York, NY: Springer New York. <https://doi.org/10.1007/978-1-4419-7952-0>.
- RFC 8446. 2018. “RFC: 8446 The Transport Layer Security (TLS) Protocol Version 1.3.” IETF, August 2018. <https://ietf.org/rfc/rfc8446.txt>.
- RFC 9420. 2023. “The Messaging Layer Security (MLS) Protocol draft-ietf-mls-protocol-20.” IETF, 27 March 2023. <https://datatracker.ietf.org/doc/html/draft-ietf-mls-protocol-20>.
- Saxena, Piyush. 2014. “OSI Reference Model—A Seven Layered Architecture of OSI Model.” *International Journal of Research (IJR)* 1, no. 10 (2014): 1145–1156. <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=fde021097ce7440a44ecf61470778d72f99e307f>.
- Singh, Prabhnit. 2018. “Optimizing Web Performance with TLS 1.3.” Cisco. November 28, 2018. <https://www.thousandeyes.com/blog/optimizing-web-performance-tls-1-3>.
- Suntor. 2023. “Drone Video Transmitter Products.” Accessed May 10, 2023. <https://www.cofdm-transmitter.com/quality-12055165-5km-2-4ghz-wireless-cofdm-drone-video-transmitter-uav-video-transmission>.
- Tan, Choon Seng, Douglas L. Van Bossuyt, and Britta Hale. 2021. “System Analysis of Counter-Unmanned Aerial Systems Kill Chain in an Operational Environment” *Systems* 9, no. 4: 79. <https://doi.org/10.3390/systems9040079>.

- Techslang. 2023. “What Is the Frequency Hopping Spread Spectrum?” Accessed March 22, 2023. <https://www.techslang.com/definition/what-is-the-frequency-hopping-spread-spectrum/>.
- Thiessen, Christian, Douglas Van Bossuyt, Britta Hale. 2022. “Reducing Asymmetry in Countering Unmanned Aerial Systems.” In *Nineteenth Annual Acquisition Research Symposium* 273–287. <https://calhoun.nps.edu/bitstream/handle/10945/70340/SYM-AM-22-048.pdf?sequence=1&isAllowed=y>.
- Typito. 2022. “Video Resolutions: What they are, Different Types, and their Pixel Size” July 1, 2022. <https://typito.com/blog/video-resolutions/>.
- UAS Components. 2023. “USG-212 Camera System.” Accessed April 4, 2023. <https://res2.weblium.site/res/5cef7aaf06b46b0023146455/6113ced8e32264002157fc5f>.
- U.S. Navy, U.S. Marine Corps, and U.S. Coast Guard. 2020. *Advantage at Sea: Prevailing with Integrated All-Domain Naval Power*. <https://media.defense.gov/2020/Dec/16/2002553074/-1/-1/0/triservicestrategy.pdf>.
- Williams, Lawrence. 2023. “OSI Model Layers and Protocols in Computer Network.” July 22, 2023. <https://www.guru99.com/layers-of-osi-model.html>.
- Yang, S. Luo, Y. Miao, W. Ge, C. Sun, W. Luo, C. 2021. “RF Signal-Based UAV Detection and Mode Classification: A Joint Feature Engineering Generator and Multi-Channel Deep Neural Network Approach.” *Entropy* 2021 (23), 1678. <https://doi.org/10.3390/e23121678>.
- Zeng, Yong, Rui Zhang, and Teng Joon Lim. 2016. “Wireless Communications with Unmanned Aerial Vehicles: Opportunities and Challenges.” *IEEE Communications Magazine* 54 (5): 36–42. <https://doi.org/10.1109/MCOM.2016.7470933>.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Fort Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California



DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE