DEPARTMENT OF THE AIR FORCE
UNITED STATES SPACE FORCE
SPACE LAUNCH DELTA 30

Autonomous Flight Termination System (AFTS) Certification Roadmap

---

Elisa Casazza*, Safety Assessment Flight Termination Engineer SLD 30*

Peyton Kramilch, *Safety Assessment Intern SLD 30*

Table of Contents

CHAPTER 1

SCOPE

How does one prepare an autonomous flight termination system for use at Space Launch Delta 30? Autonomous flight systems consist of ordnance, signal transfer lines, tracking sources like GPS or IMUs, and other support equipment. Autonomous flight termination units head up the entire system—housing the flight criteria which governs a vehicle's flight. Autonomous flight termination systems boast of a seamless partnership between software and hardware solutions. This begs the question, how does SLD 30 work with the Range User to ensure a highly reliable system that will safeguard the public in case of a catastrophic failure? This certification roadmap will initially provide a technical background for elements of the autonomous flight termination system. Then, it will answer three key questions. First, how does the hardware of an autonomous flight termination system become compliant to vital safety requirements? Second, how does the software of an autonomous flight termination system become compliant to safety requirements? And finally, after flight hardware and flight software is integrated, what kind of system and subsystem level tests must a Range User pass before launch? This document will establish the roadmap for developing, testing, and ensuring safety compliance for an autonomous flight termination system at Space Launch Delta 30.

CHAPTER 2

POLICIES AND STANDARDS FOR SYSTEM APPROVAL

2.0 INTRODUCTION TO AUTONOMOUS FLIGHT TERMINATION SYSTEMS

As per the memorandum from the Department of the Air Force (DAF) regarding Autonomous Flight Termination System Implementation (dated 28 August 2023), Range Users must transition to an autonomous flight termination system by 1 October 2025. While Vandenberg Space Launch Delta 30 can still support launches that use traditional flight termination systems, developments in technology have enabled Range Users to implement a new high-fidelity autonomous flight termination system instead. The autonomous system utilizes onboard sensors, processing systems, and programmed safety criteria to ensure proper termination of the vehicle's flight when its safety criteria is violated. This autonomous system removes humans from making real-time vehicle destruct or non-destruct decisions. The autonomous flight termination system's health and status data is still relayed for the Range's situational awareness.

2.1 DESIGN CONSIDERATIONS-REDUNDANCY

The autonomous flight termination system must protect against single points of failure within its hardware and software. Hardware redundancy safeguards against single points of failure; therefore, two autonomous flight termination systems will be installed on the vehicle. To protect the flight software from errors, rigorous software development and certification processes, monitored by Independent Verification & Validation organizations, are implemented to ensure functionality and seamless performance of the flight software within the autonomous flight termination unit.

2.2 REQUIREMENT DOCUMENTATION AND STANDARDS

2.2.1 SSCMAN 91-710 – Space Systems Command Manual, the Range Safety User Requirements–This document has seven comprehensive volumes. Each volume addresses a specific aspect of safety during design, development, and day of launch activities. The System Safety Portal (https://www.vandenberg.spaceforce.mil/Range/RangeSafety/) outlines the more tcompliance process for the SSCMAN 91-710. Volumes 2 and 4 are applicable to autonomous flight termination systems; therefore, a summary of their contents is provided.

Volume 2's requirements detail specific Preliminary Flight Data Package and Final Flight Data Package content. Content ranges from formatting and frequency of data needed, nominal trajectory and off-nominal trajectory variations, and mission-specific deliverables. The Preliminary Flight Data Package must be submitted to the Flight Analysts within Launch Safety (SELF) as soon as possible. The Flight Analysts will use the Preliminary Flight Data Package to determine if an autonomous flight termination system is necessary or not for a Range User's specific application. The Final Flight Data Package will be submitted to the Flight Analysts after the preliminary one's review. See document SEAE-FTS-013 for the Flight Data Package on the FTS Portal.

Volume 4, Airborne Flight Safety System Design, Test, and Documentation Requirements provides specific requirements for United States Space Force Ranges that supplement, override, or clarify RCC 319 requirements.

2.2.2 RCC 319 – The Range Commanders Council Flight Termination Systems Commonality Standard is a set of design and testing requirements with which Range Users must comply. It contains safety requirements for both autonomous and commanded flight termination systems. The RCC 319 is designed to be customizable to a Range User's specific application. Range Safety has the final authority on disposition and interpretation of requirements.

2.2.3 RCC 324 – The Global Positioning and Inertial Measurements Range Safety Tracking Systems Commonality Standard provides common requirements for performance and verification for airborne Range Tracking Systems, including Global Positioning Systems and Inertial Measurement Units.

NOTE: Safety critical means that if the system or component were to fail, the vehicle could not destruct properly. For autonomous flight termination systems, radio frequency downlink components are no longer safety-critical items because telemetered data from the vehicle is only used for situational awareness. While radio frequency downlink components are no longer safety-critical items, they still a required service for launch following the means of compliance for SSCMAN 91-701 section 6.10.1.3.1.

2.3 TAILORING BASICS

Tailoring is a concept used for safety standards found in the RCC 319, RCC 324, and SSCMAN 91-710. Tailoring means that a launch program can work with their launch range to customize safety requirements for their launch vehicle.

To tailor a document, the following steps are taken:

a. Requirements that do not have relation to or bearing on the affected system are deleted.
b. New requirements/rewritten existing requirements are developed for any new technologies or unique applications.
c. Requirements can be tailorable if there is an equivalent level of safety available. Rationale must be documented.
d. Tailoring sessions will take place with the Range User's assigned safety engineer. Once initial requirement drafts are formed, these drafts will be sent up to management for review. This is an iterative process until all comments and concerns are addressed.
e. Once the review process is complete, the Chief of Safety will sign the tailored document. The document is then routed to other signatories.
f. If a Range User cannot meet a requirement, a non-conformance is written. Non-conformances will be evaluated for approval by the appropriate SLD 30 authorities.

See the FTS Portal (https://www.vandenberg.spaceforce.mil/Range/Flight-Termination-System/) document SEAE-FTS-008 Tailoring Example for a tailoring visual. RCC 319's Chapter 2 offers an additional, authoritative look at tailoring. Remember, the Preliminary Flight Data Package (document SEAE-FTS-013) should be completed prior to tailoring. The Preliminary Flight Data Package will be used to determine if a program needs a flight termination system or not. It is vital to send it in as soon as possible. It will be provided to Flight Analysis within Launch Safety (SELF) here at SLD 30 Range Safety.

CHAPTER 3

RANGE POINTS OF CONTACT

3.0 SPACE LAUNCH DELTA 30—Military bases will have safety departments such as weapons, occupational, or aviation. Sites hosting launch pads will have an additional department that handles the following launch safety requirements: SSCMAN 91-710, RCC 319, and RCC 324. Launch Delta 30 is divided into six subsections, which are elucidated in the "Safety Office Subsection Responsibilities" document on the FTS Portal. Space Launch Delta 30 has three primary offices pertaining to the test and evaluation of an autonomous flight termination system.

3.1 SEAE – Safety Assessment FTS Engineering (SEAE) is responsible for the design and testing of the autonomous flight termination system, range tracking system, and the telemetry data transmitting system. SEAE ensures the reliability and effectiveness of these systems to safeguard the public and government assets in the event of a launch vehicle anomaly. SEAE is the point of contact for SSCMAN 91-710 Volume 4, RCC 319, and RCC 324.

3.2 SELF – Flight Analysis within Launch Safety (SELF) is the range safety office responsible for developing the mission rules that ensure that an anomalous vehicle is terminated when flight constraints are violated. SELF will develop the digital version of the mission rules, while working with the Range User to ensure an error-free solution. SELF requires a number of deliverables from the Range User prior to launch. SELF is the point of contact for SSCMAN 91-710 Volume 2. SELF uses a Range User's Preliminary Flight Data Package to determine whether a Range User's application will need a termination system. It is vital they receive the Preliminary Flight Data Package as soon as possible.

3.3 SELR – Risk Analysis within Launch Safety (SELR) develops processes, data, and criteria to evaluate launch risks. This section conducts special studies to analyze hazards, risks, potential launch logistics issues relating to risk, and actions to mitigate risk. Related to autonomous flight termination systems, SELR provides day of launch risk analysis to ensure public risk criteria is met for both commercial and government launches. SELR is the POC for SSCMAN 91-710 Volume 2 Attachment 4. They also abide by RCC 319.

CHAPTER 4

TEST AND EVALUATION OF FLIGHT SOFTWARE

4.0 INTRODUCTION

This chapter will elucidate how the software of an autonomous flight termination system becomes compliant with safety requirements. Section 4.1 will provide a technical overview of the software and configuration data used by the Autonomous Flight Termination Unit (AFTU), the primary in-flight decision maker. Section 4.2 will discuss flight software testing, validation, and certification. Appendix B of the RCC 319 contains all requirements for safety critical and non-safety critical software utilized by the launch vehicle and its autonomous flight termination system.

4.1 AFTU FLIGHT SOFTWARE TECHNICAL OVERVIEW

Flight software will be defined as the software that runs on and through the AFTU. It consists of an MDL, CASS, and the Wrapper. The MDL, CASS, and the Wrapper engage with one another on the autonomous flight termination unit during flight to evaluate whether a flight is nominal or not.

4.1.1 MDL – A Mission Data Load (MDL) is a set of mission rules developed by Range Safety and the Range User that defines safety-driven constraints during flight that the launch vehicle needs to abide by. The MDL is uploaded into the AFTU prior to launch and is validated by Range Safety and the Range User. This chapter will provide a technical background for mission rules and the MDL. For an operational timeline, and a closer look at SLD 30's interpretation of the RCC 319 tailoring that governs the MDL Validation Campaign, please see SEAE-FTS-OO3 "Mission Data Load Validation Campaign Timelines & Requirement Overview" on the FTS Portal.

4.1.1.1 <u>Mission Rules</u> – Mission Rules are flight constraints derived by both Range Safety and the Range User to comply with Federal, State, County, and local regulations, and mitigate safety risk to people, property, and the environment. The rules are written by Range Safety and the Range User in a text file using an Extensible Markup Language (XML). The syntax is defined in Range Safety Operations Markup Language (rsoML) Schema Definition. The schema compartmentalizes the Mission Rules into 13 different categories: Mission, User Defines, Settings, Commands, Sensors, Atmospheric Regions, Flight Events, Reference Frames, Boundaries, Tables, Mission Rules, and Stream Sets. Note, defining every section may not be necessary to a specific mission. More information can be found on the FTS Portal document SEAE-FTS-011 "CASS and CHERRY Introduction". See Reference page for link.

4.1.1.2 <u>MDL Creation</u> – When the Mission Rules and XML file write-up are satisfactory to Range Safety and the Range User, the file can be converted to a new text file with a format compatible for flight, called a MDL file. This is accomplished using the MDL Tool (See Section 4.2.2.1 to learn more about MDL Tool).

4.1.2 CASS – The Core Autonomous Safety Software (CASS) is the core software used by an AFTU to provide safety critical [analysis] during the flight.

4.1.2.1 There are three operation releases (OR) available. Descriptions of each OR is as follows:

a. OR1 – Certified in July 2015. Important features in OR1 include vacuum Instantaneous Impact Point (IIP) estimate, reference frame, wrapper responsibilities, and usage of static flight boundaries and gates.
b. OR2 – Certified in August 2018. Important updates in OR2 include dynamic boundaries, a new template rule structure, improved voting system, separation of rules and command decisions, reference frames, and the ability to define data items.
c. OR3 – Certified in July 2022. Important updates in OR3 include drag and wind-corrected IIP estimate, real-time boundary-dependent Green Time estimate, User defined vehicle sensor, and enhanced computational efficiency.

4.1.2.2 CASS Function – CASS uses the contents of the MDL to create data structures necessary to perform algorithmic computations, evaluate expressions, and assess decision logic with respect to what the Mission Rules define. By initializing CASS Flight Software with the MDL, the safety script is produced in memory to be executed periodically during the flight. The safety script determines if the vehicle is safe to continue flight or should be terminated. Each invocation of the safety script uses ingested tracking sensor and flight computer data describing the state of the rocket (e.g., position, velocity). The result of the safety script depends on commands defined in the MDL—Flight Termination, End of Safety Responsibility, Green Time Violations, etc.

4.1.3 Wrapper –

As Software Safety Engineer, Jeffrey Cherry states,

> "The CASS Flight Software is a passive computational element that has no capability to interact with external devices. Another software element, known as the Wrapper, is required to connect the CASS Flight Software computational element with the real-world. The Wrapper provides the MDL contents to the CASS Flight Software by retrieving the MDL file from on-board storage (e.g., RAM) or as input from an external communication link (e.g., serial or network) and storing the MDL contents in RAM. The Wrapper is responsible for gathering input from all tracking sensors and the host vehicle before periodically invoking the safety script in the CASS Flight Software. After completion of script processing, the Wrapper then has the vital responsibility to initiate physical actions in response to commands. Finally, the Wrapper has the responsibility to monitor processing within the AFTU and the CASS Flight Software computational element and then send the health and status data to the host vehicle for outgoing telemetry transmission to ground receiving sites."

The Wrapper software is developed by the Range User's AFTU Development Team. See Section 4.2.1 for more information about procedures and responsibility allocations for testing the Wrapper.

4.1.4 AFTU in Flight– A day of launch scenario is provided to demonstrate the interaction between the Flight Software and the autonomous flight termination unit:

> Day of launch operations begin by turning the AFTUs on. The Mission Data Load (MDL) is then inserted into the AFTU and undergoes a Cyclic Redundancy Cycle (CRC) and checksum verification to ensure the inserted MDL is the correct and certified version. More information about CRC and checksum validation can be found in Section 4.2.3 of this paper. Once the certified MDL is confirmed, it is used to initialize CASS Flight Software.
>
> Throughout the flight, the following operations repeat continuously until the autonomous flight termination unit reaches the end of Range Safety's responsibility in flight: On-board tracking sensors measure the vehicle's current state (e.g., position, velocity) and relays the data to the AFTUs. Each AFTU receives data from the tracking sensors and flight computer, and the Wrapper is accepting the incoming data. The Wrapper synchronizes the data to the same time base and periodically calls the CASS Flight Software using the latest set of data. CASS executes the safety script using the ingested data. Upon the completion of the safety script, the Wrapper sends telemetry and safety data to the flight computer for transmission to ground receiving stations
>
> In summary, the Wrapper will pull vehicle performance data from vehicle sensors, format that data to be ingested by CASS, and then send the vehicle performance data to CASS. CASS will compare the vehicle performance data to the criteria provided by the MDL. If performance criteria found in the MDL is violated, CASS will recommend a destruct to the Wrapper. The Wrapper will receive that destruct recommendation and initiate the ordnance chain. Sometimes CASS will not recommend destruct right away, instead it will wait a pre-determined period of time to see if the erroneous condition will recover. If it corrects itself, CASS will continue to rule process nominally.

4.2 FLIGHT SOFTWARE TESTING, VALIDATION, AND CERTIFICATION

The Wrapper, CASS Flight Software, and MDL undergo efforts to be tested, validated, and certified for use. Once each element is proven to meet safety requirements, they are all run through test cases to ensure proper functionality and execution.

4.2.1 Wrapper – Testing the Wrapper is an independent effort completed by the Range User's AFTU Development Team. RCC 319 Appendix A, titled "Safety Software Requirements," pertains specifically to the testing and certification of Flight Safety Software. The AFTU developer must certify the software before the AFTU can be used as a safety device.

4.2.2 CASS – The CASS Flight Software is already certified, see Section 4.1.2. Upon acquisition, CASS is ready for use by the Range User. The CASS and CHERRY Tool distributions provide five free tools that are utilities necessary to certify the MDL and ensure that the Mission Rules are IAW Range Safety requirements. A brief explanation of each tool and its purpose is below.

4.2.2.1 MDL Tool – The Mission Data Load Tool (MDL Tool) reads Mission Rules XML files, performs a number of checks and validations, and generates the MDL file.

4.2.2.2 CASS DDSim – The CASS Data Driven Simulation Tool (CASS DDSim) uses the MDL file and an input simulation directives file to invoke the safety script and saves data items after each invocation for post-simulation evaluation. The simulation outputs a Formatted TM file, Message file, Stream Data file, and Point Data file.

4.2.2.3 CASS MCSim – The CASS Monte Carlo Simulation Tool (CASS MCSim) uses the MDL and numerous simulated trajectories to produce an end state for the simulated flight (e.g., safe flight or flight terminated), and other utilities. This allows for extensive analysis of the Mission Rules to be conducted since a significant amount of varying flight scenarios were simulated.

4.2.2.4 CASS FFSim – The CASS Fast Simulation Tool (CASS FFSim) functions alongside CASS MCSim to optimize execution speed when running a high volume of simulations.

4.2.2.5 CHERRY Tool – Software Safety Engineer, Jeff Cherry describes,

> "A special utility, the CHERRY Tool, provides users with an interactive environment to convert Mission Rule XML files to MDL files, accept a nominal flight trajectory and produce simulated tracking sensor data, execute simulations using the MDL file and the simulated tracking sensor data, and evaluate results from each simulation or export data for use by a Geographical Information System (GIS) tool."

4.2.3 MDL Validation – Developing and validating the MDL is a multi-step process with rigorous testing. As discussed in Section 4.1.1, the first draft of the Mission Rules is created by the host Range to generate a basic set of Mission Rules and ensure compliance with regulations and successful translation into an MDL file. To create the MDL, the Range needs Range Users to provide a Preliminary Flight Data Package to the Flight Analysts in Launch Safety (SELF) as soon as possible. Deliverables that may be contained in the Preliminary Flight Data Package are as follows:

a. Numerous flight scenarios, including the nominal trajectory, three-sigma trajectories (e.g., exceptional performance, low performance), and failure trajectories. Refer to SCCMAN 91-710 V2 for more information about required flight criteria. This shall be provided by the Launch Provider.
b. Vehicle performance and structural breakup models. This shall be provided by the Launch Provider.
c. Tracking sensor information and mention of vehicle data used by the AFTUs. This shall be provided by the Launch Provider and AFTU vendor.
d. FTS operational timing internal delays. This shall be provided by the Launch Provider and AFTU vendor.
e. Constraints imposed by the AFTUs, including the CASS Operational Release number upon which their safety application is based. This shall be provided by the AFTU vendor.

The first draft of the Mission Rules should be run through CASS Utilities such as CHERRY Tool or CASS DDSim. These simulations will generate a second draft of the Mission Rules by providing insight into the shortcomings of the first draft. Off-nominal trajectories are used to verify that safety violations are detected and the flight properly terminated when expected.

The second draft of the Mission Rules should be run through CASS Utilities such as CASS MCSim. These simulations will generate the third draft of the Mission Rules. This stage of Mission Rules is often referred to as the "Safety Draft," since CASS MCSim computes a statistically significant number of off-nominal trajectories to ensure satisfaction of safety criteria.

The Safety Draft Mission Rules XML file is sent to the Range User for additional hardware and software testing to validate the Mission Rules. This stage in the testing process ensures a version of the Mission Rules that maintains safety and mission assurance objectives under realistic fault scenarios. These simulations should use higher fidelity simulated tracking sensor and vehicle data. Unlike the testing done by Range Safety, the Range User will test the Mission Rules using their own developed Wrapper via applications provided by the AFTU vendor.

Notably, modifications made to the Safety Draft Mission Rules upon being tested by the Range User requires re-running CASS MCSim and further testing by the Range User. This process will repeat with each iteration of the Mission Rules until the simulations yield successful results with identical Mission Rules XML files and bit-wise identical MDL files. Once completed, the Mission Rules XML file and corresponding MDL file are considered validated for flight.

Software Safety Engineer, Jeff Cherry states,

> "Proper configuration control is necessary by both the host Range and the Launch Provider during MDL validation. Mission Rules file changes can be tracked via comments in the Mission Rules XML file and using the file revision string, which is a string copied from the XML file to the MDL file. The file revision string can be checked pre-flight to aid in validating that the correct MDL version will be used for flight."

The confirmation procedures are the CRC and checksum verifications. CRC and checksum function as a digital footprint to confirm the correct version of the MDL is inserted in the AFTS.

4.3 SOFTWARE IN THE LOOP (SIL)

4.3.1 Software Testing Methods – Prior to launch, Flight Safety Software (MDL, CASS, Wrapper) is tested to meet requirements in three distinct ways. It undergoes Software In the Loop (SIL), Hardware In the Loop (HIL), and an End to End test (the final Autonomous Flight Termination System check out prior to launch). Combined Testing. See document SEAE-FTS-004 "Mission Data Load Validation Campaign Test Cases Minimum" on the FTS portal for a visual to see which test cases are used during Software in the Loop (SIL) vs Hardware In the Loop (HIL) vs an End to End test. Next, a brief description of Software in the Loop (SIL), Hardware in the Loop (HIL), and an End to End test will be given.

Software in the Loop testing occurs when flight software is run through simulated flight scenarios in a desktop simulation. These simulations, or test cases, are launch simulations performed to ensure that CASS, the Wrapper, and the MDL work together harmoniously in nominal and non-nominal flight conditions. Multiple in-flight events are tested to demonstrate that CASS, the Wrapper and the MDL will together initiate a terminate output when any of the flight criteria in the MDL is violated and will not initiate a terminate output under any other condition. The Mission Rules XML file and MDL file will undergo flight simulations in CASS MCSim. The purpose of the Software in the Loop test is to build confidence that the MDL is accurate and reliable before insertion in the autonomous flight termination unit. More on SLD 30's interpretation of SIL requirements can be found in document SEAE-FTS-003 'Mission Data Load Validation Timeline & Requirement Overview" on the FTS Portal.

Once Software in the Loop testing is completed, the MDL should be in its final state. A Hardware in the Loop test will run CASS, the finalized Wrapper, and final MDL on a flight like set up of the autonomous flight termination system. The End to End test will run CASS, the finalized Wrapper, and the final MDL on the actual autonomous flight termination system installed on the vehicle. Chapter 6, entitled "Pre-Launch Combined Testing" offers more detail on the Hardware in the Loop testing and End to End testing.

CHAPTER 5

TEST AND EVALUATION OF FLIGHT HARDWARE

5.0 INTRODUCTION TO FLIGHT HARDWARE

This chapter will elucidate how the software of an autonomous flight termination system becomes compliant with safety requirements. Section 5.1 will provide a flight hardware technical overview. Section 5.2 will explore hardware component testing. Section 5.3 will focus on system and subsystem pre-flight testing. Section 5.4 will discuss test troubleshooting and analysis.

5.1 FLIGHT HARDWARE TECHNICAL OVERVIEW

For those unfamiliar with autonomous flight termination systems, they contain a myriad of flight hardware. Some examples include autonomous flight termination units (AFTU), harnessing, lanyard pull initiators, batteries, ordnance, explosive transfer lines, GPS, and IMUs. The hardware functions together to terminate the launch vehicle when necessary. To ensure high reliability in hostile operating environments, extensive testing is required.

5.2 FLIGHT HARDWARE COMPONENT TESTING

5.2.1 Acceptance Testing– Acceptance testing screens for component workmanship defects by subjecting it to environments that the component would see in flight. Such tests may include thermal cycle, thermal vacuum, sinusoidal vibration, random vibration, acoustic vibration, tensile loads, and occasionally thermal shock. Each component will have a test table in the RCC 324 or RCC 319 that is tailorable for a Range User's specific application.

All components installed on the launch vehicle must undergo acceptance testing, unless the component is single use, such as ordnance. A single-use component is tested for workmanship defects via Lot Acceptance Testing (LAT). LAT testing is performed at qualification environmental levels.

RCC 319 Section 4.12 details the general acceptance test requirements and procedures, not specific to a component. It includes requirements pertaining to items such as test set up and data review. One thing to note, sometimes Lot Acceptance Testing is also referred to as ELAT—Environmental Lot Acceptance Testing.

5.2.2 Qualification Testing– Qualification testing demonstrates the robustness of the design of the component by exposing it to the environmental levels with a margin above that which it would see during flight. The purpose of additional margin is to account for launch vehicle failure environments, flight to flight variability, and unit to unit production variability. Qualification testing demonstrates that the FTS components will function. Components need to pass all required acceptance tests before undergoing qualification environmental tests.

Individual units having undergone qualification testing are not permitted to be installed on the vehicle. Qualification tests encompass non-operating environments to extreme operating environments, each being potentially catastrophically strenuous on the component. After a successful qualification test, a design is considered to have met all its safety requirements on the component level. Once one unit of a design has gone through acceptance and qualification testing, other units of the same design will only undergo acceptance testing to screen for manufacturing defects before installation on the launch vehicle.

RCC 319 Section 4.13 details general qualification testing and analysis requirements. RCC 319 Section 4.14 details qualification non-operating environments test types, procedures, and requirements. RCC 319 Section 4.15 details qualification operating environments test types, procedures, and requirements. RCC 324 has similar requirements for range tracking system components.

5.3 SYSTEM AND SUBSYSTEM PRE-FLIGHT TESTING

The autonomous flight termination system must be tested once installed on the launch vehicle from the individual component to the entire system. This is to ensure the component, sub-system, and whole system will perform as required during pre-launch countdown and vehicle flight.

5.3.1 Pre-Flight Component Tests – Component verification tests are performed pre-installation to ensure the expected performance is achieved—i.e., that no defects occurred in the shipping, handling, or storage process since acceptance test certification. Each test yields results that identify either aligning data to the acceptance test, or anomalous or out-of-family results. These tests must be conducted as close to the launch day as possible and are valid for 180 days.

5.3.2 Pre-Launch Sub-System and System Tests – After components are installed on the vehicle, sub-system and system level tests are conducted to confirm that there are zero discrepancies in data that may indicate concerns for flight reliability. Sub-system tests and checkouts may be performed mid-installation or after full system assembly.

End to End (E2E) testing is the final, combined flight software and flight hardware checkout prior to launch. End to End testing occurs as close to the day of launch as possible on internal vehicle power, typically three days prior to flight. E2E tests the autonomous flight termination system's flight configuration. Ordnance final connections are not made during the E2E test; they are connected afterward. Ordnance load simulators or inert Low Energy Exploding Foil Initiators (LEEFI) are used as a replacement during the E2E test. They function to measure the ordnance pulse outputs and verify proper amplitude and pulse width. More on End to End tests in Chapter 6, Section 4 of this paper.

5.3.3 References – Chapter 5 in RCC 319 details pre-launch testing procedures and requirements for components, sub-systems, and the FTS system. Section 5.2 details Pre-Flight Component Tests. Section 5.3 details Pre-Launch Sub-System and System level tests, including E2E testing.

5.4 TROUBLESHOOTING AND NON-CONFORMANCES

In the event of an autonomous flight termination system test failure or anomaly, a Range Safety representative must be informed verbally or electronically within one day.

5.4.1 Test Failure Examples – Examples of a test failure or an anomaly includes the following:

a. A Range Safety test objective is failed
b. Any test result that indicates an out-of-family condition compared to other test results regardless of whether it satisfies other test criteria
c. Any unexpected change in the performance occurring at any time during testing
d. Examinations that show any defects that could adversely affect the performance
e. Anomalies in amplitude in a measured performance parameter, inadvertent outputs, or any sign that a part is stressed beyond its design limit even if the component passes the final functional test.

The configuration must not be adjusted when a failure or anomaly occurs. It must be frozen, with zero invasive troubleshooting or corrective action occurring prior to Range Safety approval. Range Safety has the prerogative to participate in failure analysis, determination of root cause, and corrective action. Failure investigation plans and written failure analysis must be submitted to Range Safety for review and approval. These documents identify causes of the failure, isolate the failure to the smallest replaceable item, and detail approaches to resolve the failure.

5.4.2 Governing Requirements for Failure Analyses – Section 4.4 and 4.5 in RCC 319 detail timelines, procedures, and requirements for actions to take following a failure and anomaly during Acceptance or Qualification testing. Section 5.1 in RCC 319 also details timelines, procedures, and requirements for actions to take following failure and anomaly incidences, but for the component, sub-system, and system testing. This differs from the procedures for Acceptance and Qualification testing because the testing described in Chapter 5 is typically performed on components and systems installed on the launch vehicle.

CHAPTER 6

PRE-LAUNCH COMBINED TESTING

6.0 INTRODUCTION TO SYSTEM AND SUBSYSTEM LEVEL TESTS

Finally, once compliant flight hardware and flight software becomes integrated, system and subsystem level tests must be passed by the launch vehicle before launch. There are two main tests required by the RCC 319 that ensure that the autonomous flight termination system's software and hardware are configured correctly for launch. Section 6.1 will discuss the Hardware in the Loop test. Section 6.2 will discuss the End to End Test. While this chapter discuss the two final system tests prior to launch, Chapter 5 of the RCC 319 contains a closer look at the subsystem tests and component certification prior to launch.

6.1 HARDWARE IN THE LOOP (HIL)

In brief, Hardware in the Loop test occurs when the finalized flight software (final MDL, Wrapper, and CASS), running on flight-like hardware, is put through a predetermined number of test cases. The flight like hardware consists of an exact replica of the entire autonomous flight termination system, including AFTU, electronic safe and arm devices, harnessing, simulated ordnance loads, and even the piece parts of components. The purpose of this test is to ensure that flight-like hardware responds correctly to the MDL, Wrapper, and CASS. The test setup for HIL testing must be approved by SLD 30 prior to use. For an in-depth look at SLD 30's interpretation of the safety requirements pertaining to Hardware in the Loop testing, see document SEAE-FTS-003 "Mission Data Load Validation Campaign Timeline and Requirement Overview" on the FTS Portal. See document SEAE-FTS-004 "Mission Data Load Validation Campaign Test Cases TEMPLATE" on the FTS portal for a visual to see which test cases are used during Software in the Loop (SIL) vs Hardware In the Loop (HIL) vs an End to End test.

6.2 END TO END TEST (E2E)

The End to End test will run CASS, the finalized Wrapper, and the final MDL on the actual autonomous flight termination system installed on the vehicle on the launch pad. The purpose of this test is to ensure that the flight hardware and software interact harmoniously prior to flight. The flight hardware shall be tested in the exact configuration it will fly in, except that the ordnance is replaced with a simulated load. After the End to End test, the Range User will perform final ordnance connections. The autonomous flight termination system is then configuration controlled by Range Safety. Essentially, the End to End test is the final autonomous flight termination system checkout that confirms that the interaction between the actual flight hardware and software functions as expected and continues to meet its safety requirements.

See document SEAE-FTS0—4 "Mission Data Load Validation Campaign Test Cases TEMPLATE" on the FTS portal for a visual to see which test cases are an End to End test. For SLD 30's interpretation of End to End safety requirements, see document SEAE-FTS-003

"Mission Data Load Validation Campaign Timeline and Requirement Overview" on the FTS Portal.

CHAPTER 7—ACRONYMS

AFTS – Autonomous Flight Termination System

AFTU – Autonomous Flight Termination Unit

CASS – Core Autonomous Safety Software

CHERRY – CASS Hazard Evaluation Readiness Review Analysis

DIU – Data Interface Unit

ESAD – Electronic Safe-and-Arm Device

E2E – End-to-End

FDP – Flight Data Package

FPA – Flight Plan Approval

FTS – Flight Termination System

GFE – Government Furnished Equipment

GIS – Geographical Information System

GPS – Global Positioning System

HIL – Hardware in the Loop

IIP – Instantaneous Impact Point

IMU – Inertial Measurement Unit

IV&V – Independent Verification and Validation

LAT – Lot Acceptance Testing

MDL – Mission Data Load

MPE – Maximum Predicted Environment

RF – Radio Frequency

rsoML – Range Safety Operations Markup Language

RSS – Range Safety System

RTS – Range Tracking Systems

SE – Safety Engineering

SEAE – Safety Assessment FTS Engineering

SELF – Launch Safety Engineering, Flight Analysis

SELR – Launch Safety Engineering, Risk Analysis

SLD – Space Launch Delta

SSC – Space Systems Command

SIL – Software in the-Loop

TDTS – Telemetry Data Transmitting System

XML – Extensible Markup Language