EVALUATION AND POTENTIAL DESIGN MITIGATIONS TO ADDRESS CHANGES IN RCC 319-19

Martin Fette, Eric Myers, Jeff Wright
Raytheon Technologies
Tucson, AZ 85757

ABSTRACT

The Range Commanders Council (RCC) Range Safety Group updated the Flight Termination Systems (FTS) Commonality Standard 319 in July 2019, which incorporated numerous changes from the previous September 2014 version in both FTS performance and test requirements, chapters 3 and 4. Additionally, significant changes to safety software validation, autonomous FTS, and guidance on using automotive grade parts were added. After providing an overview of FTS and RCC 319, Raytheon Missile Systems Subject Matter Experts will discuss and summarize the most impactful changes of the 2019 release of RCC 319 with proposed actions and high-level implementation concepts.

KEYWORDS

Flight Termination Systems, Range Safety, Autonomous, RCC 319

INTRODUCTION

Flight Termination Systems (FTS) involve close coordination with multiple engineering disciplines, program leadership and Range Safety. Every element of the system design, build and test must adhere to the requirements defined in the Range Commanders Council - Flight Termination System Commonality Standard (RCC 319). Range safety requires approval authority at every stage of the FTS design, from requirement definition to test, to ensure that the design demonstrates an overall reliability of 0.999 with 95% confidence. A flight termination system is one of three subsystems, which are collectively referred to as a flight safety system (FSS – see Figure 1 for both a generic tone-based FTS and a generic autonomous FTS). This paper will focus on the most significant changes to design and test requirements for FTS components – with a focus on autonomous FTS requirements - in the 2019 release.

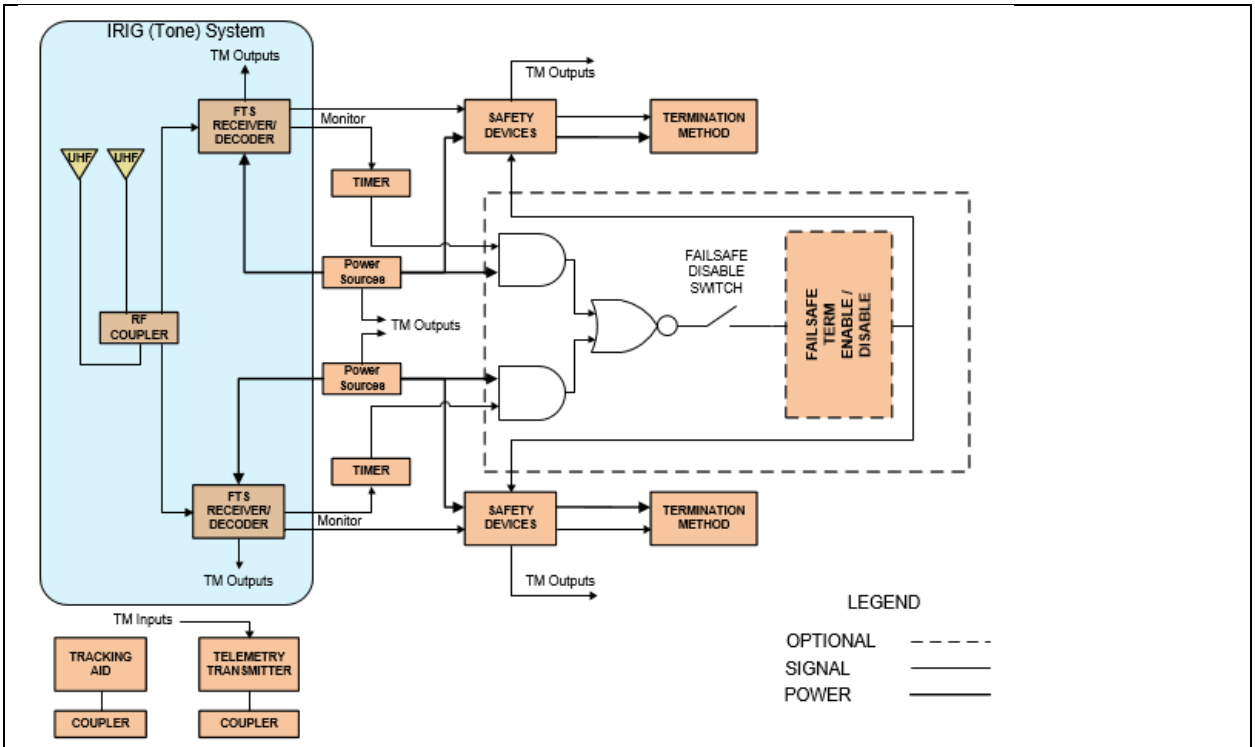

Figure 1 - Generic Flight Safety System (Extracted/Redrawn from RCC 319-19 Figure 1-1)

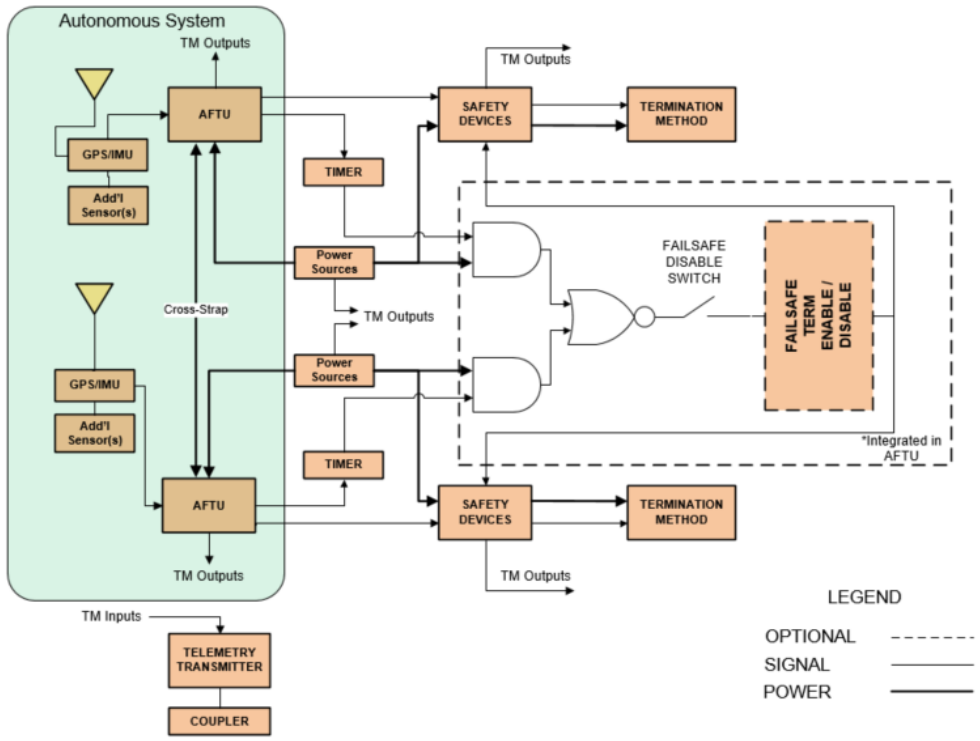

Figure 2 - Generic Autonomous Flight Safety System (Extrapolated from RCC 319-19 Figure 1-1)

The RCC 319 standard is organized by chapters, each with a specific focus (reference Table 1). Note that chapters 3 and 4 contain the majority of the design and test requirements, and specific attention to changes between the 2014 and 2019 releases focuses on these chapters.

The first chapter of RCC 319 focuses on scope/background material of range safety system development, along with a description of the overall programmatics of getting a flight certification for an FTS. This chapter also introduces the topic of tailoring, or modification of the requirements presented in the remaining chapters. More detail on the exact process of tailoring is presented in chapter 2 of RCC 319.

Chapter 3 presents detailed performance requirements for all the components that make up a flight termination system. Detailed requirements are given for each type of FTS technology, such as antennas, batteries, energetics and others – covering the majority of technologies fielded in prior FTS designs. This chapter typically contains the majority of the tailoring focus in order to align the overall document with the FTS being developed.

Chapter 4 details the specific testing requirements for each FTS component type. This chapter is also tailored, based on the final design and overall predicted environments of the flight test vehicle. Testing requirements for each environmental type (such as acceleration, shock, vibration, temperature exposure, etc.) is covered in this chapter. Specific test matrices for each FTS component are defined in RCC 319 and each incorporates an appropriate test margin (MPE multiplier, as defined in chapter 4 of RCC 319), for predicted environments (i.e., shock, vibration, acceleration, etc.) The resulting tailoring is used to create the acceptance and qualification test plans and procedures.

Chapters 5 and 6 refer to field test specific requirements – covering both for pre-flight range certification testing as well as detail on the test equipment used to support the flight mission itself. These chapters are not as commonly tailored, as the specific detail on how the flight safety system will be tested in the field is usually contained in the certification test procedure and flight CONOPS.

The remaining chapters are focused on documentation requirements, including the required analysis, test reports and final Flight Termination System Report detail that will require range safety approval before a flight certification is issued. Once an FTS design is finalized, formal range safety approval is required for all qualification test plans and procedures.

Table 1- RCC 319 Major Sections

Chapter 1 – Introduction and Overview	Chapter 8 - Documentation
Chapter 2 – Tailoring Guide	Appendix A - Safety Software Requirements
Chapter 3 - System Performance Requirements	Appendix B - Electronics Part Procurement Req
Chapter 4 - Component Testing	Appendix C - Electronics Derating Requirements
Chapter 5 - Prelaunch Test and Launch Requirements	Appendix D - Planning Guide to using RCC319
Chapter 6 - Ground support Design Requirements	Appendix E-G: Glossary, citations and references
Chapter 7 - FTS Analysis	

HIGH LEVEL SUMMARY OF CHANGES FROM PREVIOUS RELEASE

The RMD team reviewed all changes to the RCC 319-14 document using document comparison tools built in MSWord. Although the 2019 release of RCC 319 contained changes in most sections of the document (including significant changes to the appendices), the focus of this paper is on changes to the design and test portions of this standard (chapters 3-4 and Appendix A) – leaving the changes to the remaining chapters and appendices to a future paper.

Although a significant number of changes were due to minor formatting updates (acronyms, abbreviations, and spelling corrections – minor findings), there was a significant amount of new/revised material added to the 2019 revision (significant findings) that the team has reviewed and assessed for this paper. The assessment summary is detailed in Table 2, with the column identifiers as defined above.

Table 2- RCC 319 Changes Summary

RCC 319 Chapter	Minor Findings	Significant Findings	Total Identified
Chapter 3	117	103	220
Chapter 4	50	50	100
Appendix A	Complete re-write from 2014 material		

Evaluation of the identified document changes has resulted in a subjective categorization – based on overall impact to flight termination system designs. One such area focuses on the updates to autonomous flight termination systems (AFTS/AFSS) and the associated changes to both design and test requirements to support this technology. Although AFTS was described in the previous (2014) release of RCC 319, the updates include in the 2019 release are significant, and are summarized in the following sections.

CHANGE DETAIL WITH FOCUS ON AUTONOMOUS FTS

As opposed to the traditional RF command link architecture, an Autonomous Flight Safety System (AFSS) uses vehicle trajectory, on-board tracking data, and pre-designated decision termination criteria to determine if a test vehicle should be terminated. An AFSS replaces the Command Receivers (FTRs) and UHF antennas in a traditional FTS design with redundant AFTUs (Autonomous Flight Termination Unit) and dedicated, independent tracking sources. Tracking systems and components that support the AFTS function are required to meet range commonality standards RCC 324 and RCC 319.

An Autonomous Flight Termination System (AFTS) uses on-board decision-making capabilities to terminate a mission when the vehicle performance violates predetermined parameters. An AFTS includes all the associated software, hardware, and subsystems (such as GPS receivers, GPS antennas, batteries, and Inertial Navigation Systems) required to make the flight termination decision (versus the traditional, ‘human-in-the-loop’ FTS.) It is important to note that an autonomous FTS system does not replace the fuzing or termination devices that are used in a traditional FTS.

At a high level, the change from a traditional FTS to an autonomous system replaces the flight termination receivers and associated UHF antennas with a 'decision engine' or Autonomous Flight Termination Unit (AFTU, see Figure 1.) All the remaining FTS components are retained.

The overall benefits of an autonomous FTS are clear, especially for applications with significantly large range allocation requirements (footprint or mission 'corridor'.) Autonomous FTS specifically allow for the elimination (or significant reduction) of permanent ground-based range safety assets (with a corresponding savings in operational costs) and a significant increase the number of potential launch sites and corridors. As mentioned earlier, the 2014 release of RCC 319 included requirements for autonomous FTS component design and test; however, the 2019 release augmented these requirements significantly. Some examples of these changes include:

Section 3.5.3 (AFTS) added specific reference to a new software/firmware verification requirement – specifically the changes incorporated into Appendix A of the standard (Safety Software Requirements). Specific updates to Appendix A will be covered in a later section, but in summary, the range now requires a more detailed evaluation of the source code used, independent validation/verification requirements and testing capabilities. These changes, while applicable to any programmable logic FTS component, are especially critical for autonomous systems, given the complexity/dependency on the decision engine and embedded wrapper logic.

Section 3.2.7 (Ability to Test) was significantly changed for AFTS systems, specifically defining detail for how the system would use simulated tracking sources (trajectory data) to verify the overall performance of the autonomous system, in a pre-launch verification – also allowing trajectory data to be injected directly into the AFTS vs using RF hoods only. This section also covers new rules for re-testing the AFTS should connections between any 'voting candidates' be disturbed after the end-to-end test was completed. Previously, only the FTS components directly involved in the termination action (FTS 'fire-chain') were held to this requirement.
Section 3.5 (Failsafe) was also updated for AFTS specific configurations, specifically with requirements for failsafe termination on memory corruption of configuration files, executable software, or AFTS Mission Data Load (MDL.)

RCC 319 Chapter 4 (Component Testing) included some additional requirements for autonomous systems that will be covered in more detail later in this paper, but from a design point-of-view, section 4.19.2.1 now requires that all functionality of an AFTS controller (AFTU) be verified during acceptance and qualification testing – not just the functions that are required to support a specific mission. This change will likely result in a significant schedule impact to the overall acceptance and qualification programs – but is certainly dependent on the functionality of the AFTU itself.

Additionally, in 4.19.2 (Terminate Decision Criteria), the RSOs added clarification that the AFTU shall initiate a terminate output when at least half of the tracking sources violates terminate criteria. Previously, the requirement was for a terminate event when only one tracking source reported error. This change is viewed as an improvement to the overall mission assurance position, as now a majority of tracking sources would need to agree with a mission deviation as opposed to a single, failed component.

The team also identified a new requirement for ground-based AFSS and specifically requiring that a termination command be issued when ground-transmission RF quality degrades below an acceptable reliability level. There was not a specific reference to ground-based Flight Safety Systems in the previous revision of 319, but if such a unit were being specifically developed – a new requirement that initiates the autonomous termination on RF quality would seem analogous to the FTR failsafe parameters in section 3.5.2

Additionally, the team's investigation showed that the previous requirement for the AFTS to initiate the termination event on erratic vehicle behavior, and specifically requiring testing of the AFTS using 90-degree turns and tumbling events has been removed. It is uncertain why the instability requirement was removed from required testing, but the team surmises that the earlier requirement was of specific concern to overall mission assurance due to increased probability of AFTS activation.

CHANGE DETAIL FOR SAFETY SOFTWARE REQUIREMENTS

As previously mentioned, another area where significant changes have been made are to software (SW) and firmware (FW) requirements throughout.
Section 3.2.8 (safety-critical Software and Firmware): Key takeaways include the following. FTS SW and FW shall conform to a tailored version of Appendix A (covered later) or other standard approved by Range Safety. Single point failures must be eliminated as well as hidden features. SW/FW must complete Independent Validation and Verification (IV&V) per an approved plan prior to formal production. Finally, design and analyses must account for hardware (HW) induced software failures (e.g., bit flip in memory)

Section 5.3.6.1 (Flight Mission Data Load Validation): AFTS was covered earlier, but safety software/firmware requirements are specifically referenced in this section. This section requires a comprehensive test of the Mission Data Load (MDL) unique to a specific mission to validate that it performs in accordance with (IAW) a Software Requirement Specification for both nominal and failure scenarios. All scenarios must be approved by Range Safety and be statistically significant. This can be done by Software-in-the-loop (SIL) simulation, hardware-in-the-loop (HWIL) simulation or end-to-end test. The MDL must be validated by two independent organizations.
Section 7.8 (Software and Firmware): Updates were made to SW/FW analysis as well in this section, which again calls out compliance to Appendix A and requires any computing system, as well as SW and FW to be analyzed when performing a safety critical function. Specific analyses referenced include a SW Hazard Analysis. This is where HW induced SW failures would be investigated as well as out-of-specification values and potential cascading effects. The remaining significant changes in the SW/FW area are documented in Appendix A. Updated requirements to pay particular attention to are noted below.

Section A.3.1 (Partitioning): The potential implications to reduction of requirements by complying with this section cannot be overstated. This section states that if the system developer implements a partitioned system compliant to a Range Safety approved partitioning standard, then the SW will comply with all subsequent requirements in sections A.3, A.4, and A.5. The example standard given is the Aeronautical Radio Incorporated (ARINC) 653, *Avionics Application*

Software Standard Interface. Specific and detailed requirements are document in subsections, but generally fall into three partitioning categories: Safety-critical, support-critical, and non-critical.
Section A.3.2 (Human-computer Interface): "Human-computer interface for an airborne FTS should not exist". Additional requirements are imposed if this type of system is implemented, including Human Factors Engineering and other SW behavioral requirements.

Section A.4.1 (Range Safety Life Cycle Approval): A software life cycle process must be defined, approved by Range Safety, and followed throughout a program. This includes periodic reviews and consideration for Development, Operations, Maintenance, Audit, Configuration Management, Joint Review, Documentation, Quality Assurance, Verification and Validation (V&V), Managerial, Improvement and Training processes. General Operation, Failure Detection, Computation, Data Integrity and other documentation requirements are also tightly controlled, some of which are highlighted below.

Section A.4.5 (Data Integrity Requirements): These requirements read very much like Systems Security Engineering requirements, where experience has shown that there is potential here for significant cost and schedule impact.

Section A.4.6 (Software Design and Implementation Requirements): Range Safety will be part of all SW design peer reviews and will approve the overall design, including the coding standard used, with input from an IV&V contractors analysis results.

Section A.4.7 (Testing Requirements): A test plan must be created and approved by Range Safety. Failure Corrective Action procedures will be documented in a Configuration Management Plan.
Section A.4.8 (COTS Requirements): Also, to be documented in the Configuration Management Plan and are subject to the Hazard analysis. Re-used software is treated as new software. Use of COTS SW in a safety critical application must be approved by Range Safety.

Section A.4.9 (Programming Language Requirements): Programming language shall be approved by Range Safety. When mixing legacy SW with newly developed SW a hazard analysis must be performed. Translators or compilers must have a certificate of validation to a recognized national or international standard or shall be assessed to establish its fitness for purpose.
Section A.4.10 (IV&V Assessment Requirements): An independent third party, i.e., not part of the developer's company or its subsidiaries unless approved, is required to perform an assessment and report to Range Safety.

Section A.4.11 (Documentation Requirements): A multitude of new documents are now required to satisfy the safety firmware/software submittal process. See Table A-1 below for specific details.

Table A-1. Safety-critical Software Documentation Listing
System Software Documentation
Software Life Cycle Process Standard
Software Assurance Standard†
Software Project Management Plan†
Human Factors Engineering Standard/Plan†
Software Development Documentation
Software Configuration Management Plan†
Software Quality Assurance Plan†
Software Development Plan
SDD
Software Coding Standards
Requirements Documentation
Software Requirements Specification
Selection Documentation
Host Computer System Validation‡
Power Up and Restart Safe State Conditions‡
Software Partitioning Methods‡
Communication Methods for Software (between partitions and with external links)‡
Programming Language Selection Assessment (if applicable)‡
Safety-Critical System Events‡
Identification of Critical Data Values‡
Software Metrics (Complexity, Size, etc.)§
COTS Component Validation‡
Assessment (IV&V) Documentation
Assessment (IV&V) Process Plan
Evaluation Reports
Anomaly Reports
Test Documentation
Test Plan
Test Procedures
Test Report
Support Documentation
User Documentation and Procedures
Operations and Maintenance Plan
† Recommend including as part of the software development plan.
‡ Recommend including as part of the SDD or software requirements specification.
§ Recommend including within the Software Coding Standard.

Most, if not all, of these significant SW/FW changes have the potential to significantly increase program cost and schedule scope, unless tailored and managed appropriately. Appendix A (in and

of itself) went from 6 pages (21 'shall' statements) in RCC 319-14 to 25 pages (251 'shall' statements) in RCC 319-19. Even then, each of these changes need to be considered and planned for early with Range Safety collaboration as a high frequency recurring activity.

CHANGE DETAIL WITH FOCUS ON DESIGN VALIDATION

After comparative inspection, the latest 2019 release of RCC 319 continues to strengthen and clarify the environmental system evaluation and required testing for a certified flight termination system. This is evident by the dominance of Chapter 4 and is the largest portion of the document. In the environmental/validation sections, there are several clarifications and test re-ordering that appear relatively straightforward and can be characterized as general document cleanup. There are also several updates that have the potential to significantly 'increase scope' when comparing previous revisions and maturation. Some examples of considerable revision updates include (but are not limited to):

Section 3.3.2 (Maximum Predicted Environmental (MPE) Uncertainty Margin): For vehicles with less than three flights of measured environmental data history, an additional 11 Degrees C of thermal margin has been added. With the introduction of this requirement, new developments hoping to leverage existing, mature components may have new challenges attempting to retain component grandfathering (which may never have been tested to similar qualification levels.)
In addition, with vehicles predicting severe thermal environments, and required electronics component thermal de-rating, it is possible that significant, additional work scope be required to redesign the component and or mounting structure. A component with acceptable (however minimal) margin that was acceptable in RCC 319-14 may not be directly acceptable in RCC 319-19.

Section 4.14.5 (Transportation Shock): Most changes are likely cleanup from the previous revision. The latest version introduces a commercial package drop height of 48" onto a concrete surface. Previous revisions mention drop testing without specific requirements, likely left to the tailoring agent to define and approve final test parameters. The team evaluated that this modification was a clarification only.

Similar to the MPE discussion earlier, previous mature components may have different requirements and possible expanded testing scope and or redesign may be required to satisfy these updates. These changes do not necessarily affect energetic components, as there has been long established testing requirements for ordnance items in previous revisions of RCC 319.

Section 4.15.6 (Temperature/Humidity Altitude Testing): Changes in this section were also deemed to be 'for clarification only.' Specifically, a new ambient temperature step was added to "Return the chamber to ambient humidity". Although highly design dependent, this addition is not deemed to be a significant stressing step in the process. The 'return to ambient' humidity step will likely drive additional test time to "bake out" the chamber and is highly dependent on the test apparatus and unit being tested.

Section 4.36 (Table 4-85, Shock and Vibration Isolator Qualification Test Requirements): This section added specific stand-alone requirements for operating environment tests. The team concluded that these changes were most likely made as clarifications and document cleanup. Specifically, that the isolator can now be tested at the system level with parent FTS components. However, if tested separately, this section still requires environmental testing at the isolator component level. Additionally, 4.36.4 added significant detail regarding characterization testing. This change was also evaluated as 'no impact' for new designs, however, component reuse from the previous RCC 319 revision could likely require additional testing and/or tailoring to comply if interpreted or tailored differently.

CONCLUSION AND SUMMARY

Each update to RCC319 ensures that 'lessons learned' from current flight test experiments – especially those that were designated as safety related - are made available for future flight test programs. As flight test programs become more complex, the technology requirements for the flight safety systems also increases. This increased complexity is also reflected in subsequent releases of RCC 319.

Design teams for flight safety systems must ensure that a detailed review and analysis of each update to RCC 319 is completed as soon as that document is made available. Thorough understanding of these modifications will benefit the team in both the requirement tailoring and the overall design phases of the program.