Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

# Functional Failure Mode, Effects and Criticality Analysis of Spacecraft Autonomous Collision Avoidance Systems

**Tomás Costa Pinho**
Université de Toulouse
**Antonio Vinicius Diniz Merladet**
diniz.merladet@tum.de
Technical University of Munich
**Chiara Manfletti**
Technical University of Munich
**Daniel Rondon Pleffken**
Embry-Riddle Aeronautical University
**Carlos Henrique Netto Lahoz**
Aeronautics Institute of Technology (ITA)

**Research Article**

**Keywords:** collision avoidance, spacecraft autonomy, failure modes, criticality analysis, traffic coordination

**Posted Date:** August 20th, 2026

**DOI:** https://doi.org/10.21203/rs.3.rs-10608970/v1

**License:** This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

**Additional Declarations:** No competing interests reported.

## Abstract

Autonomous collision-avoidance systems can reduce dependence on immediate ground intervention, but they also create a distributed safety function whose performance depends on tracking, conjunction assessment, communications, onboard sensing and computing, autonomous decision-making, maneuver planning, and propulsion. This study applies a tailored functional Failure Mode, Effects and Criticality Analysis to a representative end-to-end architecture for autonomous spacecraft collision avoidance. The system boundary was defined through functions across the ground and spacecraft segments. Failure modes were derived from functional deviations and assessed in terms of effects, causes, baseline detection provisions, and recommended risk controls. Because mission-specific failure rates and calibrated diagnostic-coverage data were unavailable, the study uses a qualitative priority index based on relative severity, occurrence, and detectability rankings rather than a quantitative European Cooperation for Space Standardization (ECSS) criticality number. The rankings are engineering judgments for comparative prioritization; they are not operational statistics or independently validated quantitative risk estimates. The completed analysis contains 127 failure modes with baseline risk priority number (RPN) values. The highest RPN cases include a false-negative maneuver decision, false-negative input validation, an incorrect collision-probability output, delayed tracking and conjunction information, late onboard measurements, unusable navigation data, false-negative autonomous reconfiguration, erroneous resource-state reporting, and constraint-violating maneuver plans. High-severity modes are also screened independently of RPN. Cross-cutting findings concern information provenance and integrity, deadline assurance, validation asymmetry, authority coordination, resource and actuation assurance, and achieved-state verification. Recommendations address heterogeneous redundancy, calibration and health monitoring, conservative uncertainty treatment, independent decision checks, validated degraded modes, resource margins, and post-maneuver verification.

## 1 Introduction

# 1.1 Motivation

The expansion of government, commercial, and scientific space activities has increased the number of human-made objects in Earth orbit. The growth includes active payloads, rocket bodies, mission-related objects, and fragmentation debris. ESA catalogue statistics [1] establish the operational environment in which collision-avoidance systems must function to avoid the conjunction of space objects.

Space debris comprises human-made objects that no longer perform a useful function, including inactive spacecraft, spent launch-vehicle stages, and fragments produced by break-ups, erosion, and collisions. The population that can be routinely tracked is only a subset of the total environment; smaller fragments remain numerous and can still threaten spacecraft because orbital relative velocities are high [2]. The increasing object population raises both the frequency of conjunction screening and the operational burden associated with assessing and resolving alerts.

The long-term concern is not limited to current traffic. Collision fragments can increase the population and thereby create additional collision opportunities, a feedback mechanism commonly associated with the Kessler syndrome. Long-term environment studies indicate that cumulative collisions in low Earth orbit can continue to increase even under restrictive future-launch assumptions [3]. The United Nations University assessment likewise characterizes cascading debris growth as a potential orbital risk tipping point [4].

The accidental collision between Iridium 33 and Kosmos 2251 on February 10, 2009 demonstrated the consequences of an unmitigated conjunction between intact spacecraft. The satellites collided at approximately 11.7 km/s, near 776

km altitude, and generated more than 2,300 trackable fragments [5]. Such events threaten spacecraft safety, mission viability, and the long-term use of orbital regions.

Collision prediction and avoidance therefore form a safety-critical operational chain. A failure can originate in observation, orbit determination, data exchange, conjunction assessment, decision-making, planning, command execution, spacecraft state estimation, or propulsion. A safety assessment must consider the distributed chain rather than only the onboard decision algorithm.

## 1.2 Research Overview

Traditional collision-avoidance operations rely substantially on ground organizations to obtain tracking data, assess conjunctions, coordinate with other operators, authorize maneuvers, and command the spacecraft. Ground involvement remains important, but communication outages, decision latency, data-quality uncertainty, and short response windows can limit timely intervention. ACAS concepts address these limitations by combining ground information with onboard sensing, computing, decision logic, maneuver planning, and actuation.

An ACAS can evaluate conjunction information, determine whether a CAM is required, generate a feasible plan, and execute or recommend the maneuver according to the assigned authority and operational concept. Autonomous decision-planning has been investigated as a means to improve responsiveness and preserve mission objectives under time constraints [6]. Autonomy does not eliminate risk; it redistributes authority and creates new dependencies on software, data, timing, and interaction design.

Rigorous hazard analysis, simulation, verification, validation, and operational testing are therefore required. The safety objective is not only to reduce the likelihood of component failures, but also to prevent unsafe decisions, delayed actions, invalid messages, contradictory coordination, resource exhaustion, and maneuvers that create new conjunctions or violate mission constraints.

This study uses functional FMECA to identify and prioritize ways in which the distributed ACAS operation can fail. The Reliability Analysis Center guide describes FMECA as a structured means of connecting functions or items with failure modes, effects, causes, criticality, detection, and corrective action [7]. MIL-STD-1629A codified procedures for performing and documenting the analysis [8]. A later literature review summarized implementation practices and recurring application issues [9]. IEC 60812 formalized general planning, tailoring, documentation, and maintenance requirements for FMEA/FMECA [10]. ECSS-Q-ST-30-02C established the corresponding space-product-assurance framework [11].

The analysis has four main objectives: define a representative ACAS functional architecture; identify failure modes and their effects, causes, detection provisions, and risk controls; assess the value and limitations of FMECA for a highly interconnected autonomous operation; and propose recommendations and mitigation constraints. The output is intended to support spacecraft developers, operators, mission planners, traffic coordinators, safety engineers, software teams, approval authorities, and systems engineers.

The full function decomposition (Table S1) and complete FMECA (Tables S2a–S2d) are provided in the Supplementary Material, while this article presents the methodological narrative, illustrative tables, results, recommendations, and methodological assessment.

The specific novelty of this study is the end-to-end, cross-segment application of a tailored functional FMECA to ACAS as a distributed operational capability. Rather than examining only an onboard algorithm or a single spacecraft subsystem, the analysis links ground tracking, conjunction assessment, communications, onboard sensing and

computing, autonomous decision and maneuver planning, propulsion execution, and post-maneuver feedback within one traceable failure-mode baseline. This structure makes propagation across ground-space interfaces explicit and translates the results into reusable assurance priorities.

## 2 ACAS Operational Context

# 2.1 ACAS Operations

ACAS concepts seek to maintain spacecraft safety and mission continuity in increasingly congested orbital environments by responding to conjunction events with reduced dependence on immediate human intervention. They combine ground-based observation and coordination with onboard state estimation, collision-risk processing, decision-making, maneuver planning, and propulsion [6].

The term ACAS in this paper denotes the operational capability rather than a single hardware unit. The capability extends across external tracking services, conjunction-assessment providers, the spacecraft operator and ground system, communication links, spacecraft sensors and computers, autonomous processing modules, and the propulsion chain. The implementation and allocation can vary by mission; the functions and interfaces, rather than a specific product architecture, define the FMECA boundary.

Autonomous operation becomes particularly relevant when communication disruptions, ground-processing delays, or short times to closest approach prevent a conventional decision cycle. The system must nevertheless remain coordinated with external actors, maintain traceable data provenance, respect mission and regulatory constraints, and provide recoverable degraded modes.

# 2.2 Situational Awareness

Space situational awareness supplies observations, catalogues, orbit estimates, covariance information, and environmental context needed to screen for close approaches. Ground radar and optical networks observe object position, velocity, and related parameters, while orbit-determination and data-fusion processes maintain estimates that can be used for conjunction assessment [12].

The quality of the resulting assessment depends on coverage, observation geometry, calibration, time synchronization, object identification, force models, covariance realism, and the consistency of data from multiple sources. Gaps, delays, or underestimated uncertainty can produce missed conjunctions; excessive uncertainty or false tracks can generate unnecessary alerts and maneuvers.

Environmental information can also affect orbit prediction and spacecraft health. Space-weather conditions influence atmospheric density, drag, charging, radiation exposure, communication, and sensor performance. Relevant environmental data can therefore inform model selection, uncertainty treatment, and protective spacecraft responses [12].

# 2.3 Standards Context

International standards provide a technical framework for collision avoidance and coordination. ISO 23705:2026 specifies workflows and technical requirements for perceiving, evaluating, and avoiding collisions among orbiting

objects, including data requirements, probability or consequence estimation, and guidance for executing avoidance maneuvers [13].

For an autonomous implementation, the relevant implications include defined operational responsibilities, documented risk-mitigation strategies, exchange of ephemeris and conjunction data, coordination of maneuver intentions, explicit treatment of data quality, and controlled decision criteria. The standard does not remove the need for mission-specific validation of models, thresholds, and authority allocation.

ISO/FDIS 9490 is under development at stage 50.20 [14]. The Final Draft International Standard addresses Space Traffic Coordination as a broader cooperative framework for planning, harmonization, information sharing, and synchronization of space activities. Its emphasis on interoperability, transparency, procedures, responsibilities, coordination, and data exchange is directly relevant to the interfaces surrounding an ACAS.

## 2.4 Navigation Data Messages

CCSDS Navigation Data Messages (NDMs) form an umbrella family of distinct message standards for exchanging orbit, tracking, conjunction, and attitude information [15]. ODM, CDM, TDM, and ADM are not interchangeable labels; each message type has its own content and operational semantics. Standardization supports interoperability, automated validation, metadata traceability, consistent units, and controlled parsing across organizations and software implementations.

Orbit Data Messages include the Orbit Parameter Message, which communicates a state vector or orbital elements at an epoch; the Orbit Ephemeris Message, which communicates time-tagged state vectors; and the Orbit Comprehensive Message, which supports richer metadata, covariance, and modeling information [16]. These products can support orbit propagation and conjunction screening when their time systems, reference frames, units, object identities, and uncertainty data are correctly interpreted.

The Conjunction Data Message communicates predicted encounter information between assessment providers and spacecraft operators. Relevant content includes object identifiers, time of closest approach, miss distance, relative state information, covariance data, probability of collision where applicable, and assessment metadata [17]. A CDM must be treated as a time-sensitive assessment product rather than an unconditional command to maneuver.

The Tracking Data Message communicates observations such as range, range rate, Doppler, and angular measurements [18]. These data are inputs to orbit determination; they are not interchangeable with a CDM. Failure to preserve message type, source, units, timing, or object association can propagate incorrect states into later decisions.

The Attitude Data Message communicates spacecraft attitude information [19]. An ADM is not a maneuver-intent message. Cooperative maneuver coordination requires a defined message or service that explicitly represents intent, constraints, identity, validity, and timing.

For larger products or stored files, protocols such as the CCSDS File Delivery Protocol provide acknowledged delivery, transaction management, and fault handling across intermittent links [20]. Their applicability depends on the latency and message-size requirements of the specific collision-avoidance function.

## 2.5 Space Traffic Coordination

Space traffic coordination involves cooperative planning, data exchange, and synchronization among operators and service providers to reduce collision and interference risk. The present environment is distributed across governmental, commercial, and collaborative organizations rather than controlled by a single global authority [21].

Tracking and conjunction services may use public catalogues, bilateral exchanges, operator ephemerides, commercial observations, and collaborative platforms. This diversity can broaden coverage and resilience, but it also creates differences in formats, update rates, quality metrics, thresholds, and operational procedures.

National and regional initiatives increasingly treat orbital sustainability and coordination as policy priorities [22]. Analyses of the current environment emphasize that knowing where objects are is insufficient; operators also need timely, trusted, and mutually understood information about planned maneuvers, responsibilities, and response expectations [23].

The FMECA therefore includes ground tracking, conjunction assessment, and ground control as functional blocks rather than treating them as fixed external assumptions. Their failures can deprive the autonomous spacecraft of valid inputs, produce contradictory assessments, delay decisions, or prevent coordination with other actors.

## 2.6 Method Selection

The research reviewed HAZOP, FRAM, FTA, FMEA/FMECA, and STPA before selecting the method. The selection was based on the study objective, available information, desired traceability, and project constraints.

HAZOP uses guide words and multidisciplinary examination to identify deviations from intended operation. IEC 61882 provides guidance on study definition, preparation, examination sessions, documentation, and follow-up [24]. The method was not selected because the project required a function-by-function worksheet and explicit prioritization.

FRAM emphasizes functional variability and resonance, while STPA examines unsafe control actions, control flaws, and interactions that can produce losses even when components have not failed. Comparative research shows that FMEA, HAZOP, FRAM, and STPA generate different but overlapping findings because they model systems and causation differently [25].

FTA is a deductive method that decomposes a defined top event into contributing conditions. FMEA/FMECA is inductive and proceeds from functions or items toward effects. Comparative literature indicates that the techniques differ in traceability, level of decomposition, and ability to connect causes with implementation details [26].

A previous ACAS study used STPA to develop safety recommendations for the same general operational problem [27]. FMECA was deliberately selected to provide a complementary bottom-up view and a ranked worksheet. Case-study evidence confirms that FMEA and STPA identify different categories of findings: FMEA is closely tied to architecture and failure modes, while STPA is stronger for unsafe interactions, software/control behavior, and systemic causal factors [28].

FMECA was therefore considered suitable for the ACAS operational analysis. Its strengths are systematic coverage, traceability from function to control, and support for design-assurance prioritization. Its weaknesses include analyst dependence, potentially large worksheets, limited treatment of emergent interactions and organizational factors, and sensitivity to the selected ranking method.

## 2.7 FMECA Basis

FMEA is an inductive analysis that identifies how functions, hardware, software, processes, human actions, or their interfaces can fail and examines the resulting local and global effects. FMECA extends FMEA by classifying or prioritizing failure modes according to defined criticality criteria. In the ECSS framework, failure-mode criticality combines severity with likelihood or probability of occurrence [11]. IEC 60812 also recognizes tailored priority methods, including RPN-based approaches, when their purpose and limitations are defined [10].

The space-specific ECSS standard distinguishes functional, hardware, and process FMECA. A functional FMECA analyzes functions rather than the items used to implement them; hardware FMECA addresses physical implementation; process FMECA addresses activities such as manufacturing, integration, test, or operations [11]. This study uses the functional approach because the architecture is representative and not tied to a detailed flight design.

The workflow was tailored from established guidance rather than presented as a verbatim implementation of one standard. The Reliability Analysis Center guide informed the general FMECA structure [7]. MIL-STD-1629A informed the traditional procedural sequence [8]. IEC 60812 informed the tailored priority and documentation provisions [10]. ECSS-Q-ST-30-02C informed the space-specific functional FMECA basis [11]. The historical NASA procedure provided an additional aerospace reference for the analysis workflow [29]. The core sequence is:

1. Define the analysis purpose, decision use, system boundary, mission interval, operational modes, assumptions, exclusions, functional hierarchy, and ranking rules.

2. Construct a functional architecture showing information, decision, authority, resource, actuation, and feedback interfaces.

3. Identify credible functional deviations, including omission, delay, corruption, intermittency, premature or unintended action, failure to stop, degraded output, and failure of validation or recovery.

4. Determine the functional and end effects, plausible causes and enabling conditions, and the baseline detection or compensating provisions for each failure mode.

5. Assign severity from the worst credible end effect, assign a relative occurrence rank from the causal exposure and baseline assumptions, assign detectability from the likelihood of timely detection, and calculate the baseline RPN.

6. Screen critical-severity modes independently of RPN, develop preventive, detective, compensating, or mitigating controls, and repeat the analysis when the design, operational concept, or evidence changes.

The process is iterative. New causal information can change a failure-mode definition; new baseline detection logic can change the detectability ranking; and design changes can introduce or remove dependencies. Recommended controls do not reduce the baseline RPN until they are allocated, implemented, verified, and validated. The worksheet should therefore be maintained as configuration-controlled assurance evidence rather than treated as a one-time calculation.

The resulting analysis is coherent with the functional FMECA framework, but it is deliberately tailored. The study uses a representative operational architecture, a consolidated effects field, qualitative relative occurrence rankings, and an RPN-based priority index. It does not claim a failure-rate-based ECSS criticality number, a complete item-level design FMECA, a formal single-point-failure list, or closed residual risk.

# 3 FMECA Application

# 3.1 Scope

The system boundary represents the distributed operation required to assess, decide, plan, and execute an autonomous collision-avoidance response. It is not a reliability model of a single product. The boundary includes selected ground and spacecraft functions whose outputs are necessary for the ACAS mission.

The mission of the representative ACAS is to assess and mitigate conjunction events while preserving spacecraft safety, mission continuity, and applicable coordination obligations. The FMECA examines the ways in which the involved functions can fail to support that mission.

The representative baseline primarily addresses uncrewed spacecraft. The severity scale includes potential loss of life only as a tailoring provision for crewed applications and does not assume this consequence for every ACAS implementation.

The analyzed operational interval begins with the availability of tracking or conjunction information and continues through assessment, ground or autonomous decision, CAM planning, command or authorization, maneuver execution, and post-maneuver confirmation. Nominal and degraded operation are considered. Launch, re-entry, manufacturing, assembly, deliberate debris-removal missions, and detailed cybersecurity attack analysis are outside the primary boundary.

The baseline is a representative distributed capability, not a specific certified design. Each row therefore states a functional deviation and generic causal mechanisms. Hardware or software faults are included only when they explain the functional failure; implementation-specific component failure rates, diagnostic coverage, and redundancy independence are not assumed.

The “S”, “O”, and “D” rankings describe this baseline before the recommended controls are implemented. Severity is assigned from the worst credible end effect within the stated assumptions. “O” is a relative occurrence rank, not a numerical probability. “D” represents the difficulty of detecting the condition in time using only the baseline provisions listed in the row; a high “D” value means poorer timely detectability.

The ground segment includes ground-based tracking, conjunction assessment, and the ground control center. Ground-based tracking covers radar, optical, and other observation services that produce measurements and orbit information. Conjunction assessment processes the available states and uncertainties to identify close approaches and communicate assessment products. Ground control monitors the spacecraft, validates information, coordinates with external actors, and retains the authority allocated by the operational concept.

The spacecraft segment includes onboard communications, the onboard computer, navigation and attitude sensors, environmental and health sensors, the ACAS processing, decision, and maneuver-planning modules, and the propulsion chain. The propulsion chain comprises the control unit, fuel and power resources, thrusters, and performance feedback.

Other spacecraft and debris are external entities. Debris is non-cooperative and is represented through tracking and conjunction information. Other spacecraft may be non-cooperative or cooperative; cooperative coordination requires a defined and validated exchange of intent or maneuver data.

The analysis identifies 34 functions. They include observation and tracking-data delivery; conjunction computation and delivery; spacecraft monitoring, ground decision, command transmission, and data relay; ground-space and inter-spacecraft communications; RFI mitigation; onboard power conversion, telecommand processing, reconfiguration,

and telemetry formatting; navigation, environmental, and health measurement; propulsion-plan validation, thrust-vector and resource allocation, command dispatch, fuel and power provision, thruster execution, performance reporting; and ACAS input gathering, validation, collision-probability calculation, maneuver decision, and CAM generation.

Table 1 presents the propulsion-chain functional decomposition that supports systematic failure-mode generation without implying a specific hardware design.

Table 1
Functional description of the propulsion chain

| Functional block | Function |
|---|---|
| Propulsion control unit | Receive and validate the CAM plan |
| Propulsion control unit | Compute thrust vector and resource allocation |
| Propulsion control unit | Dispatch propulsion commands |
| Fuel and power resources | Provide fuel and electrical power |
| Fuel and power resources | Monitor fuel and power state |
| Thrusters | Execute thrust commands |
| Thrusters | Report propulsion performance |

## 3.2 Architecture

The functional architecture proposed is shown in Fig. 1. It represents ground-based tracking and conjunction assessment, ground control, ground-space and inter-spacecraft communication, onboard sensing and computing, the ACAS processing, decision, and maneuver-planning chain, and the propulsion resources and actuation path. The figure defines the research boundary; message applicability and normalized terminology are interpreted according to Sections 2.3 and 2.4 and the functional decomposition in Table S1 of the Supplementary Material.

In Fig. 1, NDM identifies the CCSDS navigation-message family, while the parenthetical labels identify representative specific message types. ADM carries spacecraft attitude data and does not communicate maneuver intent; maneuver intention requires a separately defined and validated coordination exchange.

The diagram supports effect tracing across levels of indenture. For example, a delayed tracking message can propagate through conjunction assessment to a late decision; an invalid sensor state can contaminate the collision-probability calculation; and propulsion underperformance can invalidate the achieved post-maneuver trajectory unless feedback is independently verified.

## 3.3 Failure Modes

Failure modes were generated as paths in which a defined function could fail to provide its intended output, timing, authority, or state transition. Standard functional-deviation categories included no output, incomplete or degraded output, incorrect or inconsistent output, delayed output, premature action, repeated or unintended action, failure to cease, and failure of validation, detection, isolation, or recovery.

Hardware faults, software defects, environmental stresses, timing and synchronization errors, communication failures, protocol mismatches, configuration errors, human or organizational actions, and upstream data problems were considered where relevant. Failure modes were included when they were within the defined boundary,

operationally distinguishable, and capable of affecting an ACAS function or its assurance. Duplicate formulations were consolidated. The set is systematic for the stated scope but is not claimed to be exhaustive for every spacecraft implementation.

Human and organizational actions are included only as contributing conditions where they can affect a defined function. The study does not constitute a formal human-reliability analysis or an organizational safety assessment.

The process produced 127 failure modes. The complete analysis is provided in Tables S2a–S2d of the Supplementary Material. Table 2 presents examples for onboard-computer functions.

Table 2
Onboard-computer functions and identified failure modes

| Function | Failure modes |
|---|---|
| Convert and regulate electrical power | No power output; incorrect or out-of-range output; unstable power |
| Process telecommands | No decryption; command not decoded; command decoded incorrectly; command decoded too late; false-positive validation; false-negative validation; telecommand lost; telecommand executed twice; telecommand sent to the wrong subsystem |
| Perform autonomous reconfiguration | False-negative reconfiguration; false-positive reconfiguration; inadequate reconfiguration |
| Format telemetry packets | Packet not generated; temporally inconsistent packet generated; invalid packet generated |

# 3.4 Effects and Severity

Effects were considered at the affected function and at the higher operational or mission level. Relevant outcomes include loss or degradation of conjunction assessment, false-positive or false-negative alerts, loss of coordination, delayed decisions, unsafe or unnecessary maneuvers, constraint violations, resource depletion, loss of maneuverability, mission degradation, and increased collision risk. The worksheet uses one consolidated effects field; a design-specific FMECA should separate local, next-higher-level, system, and mission effects when required.

Severity is based on the worst credible end effect of the individual failure mode within the defined architecture and operating assumptions, not merely on the local symptom. A rank of 10 is reserved for modes that can directly leave a credible collision unmitigated or contribute to catastrophic loss; ranks 8–9 denote serious or critical effects that remain conditional on the encounter, available alternatives, or subsequent barriers.

Effects were written to distinguish data rejection from acceptance of invalid data. A malformed message that is rejected can reduce availability or consume time; the same message, if accepted, can corrupt the state estimate or decision. Similarly, a false-positive environmental alert can unnecessarily degrade the spacecraft, while a false-negative alert can permit damage or data corruption to progress. Table 3 presents examples of effects for environmental-monitoring failure modes.

Table 3
Effects of environmental-monitoring failure modes

| Failure mode | Consolidated effects |
|---|---|
| No measurement | Critical exposure (radiation spikes, thermal extremes) goes unnoticed, leading to data corruption and component degradation/failure. Degraded situational awareness and decisions. |
| False-negative environmental anomaly | Critical exposure goes unnoticed, leading to data corruption and component degradation/failure. Degraded situational awareness and decisions. |
| False-positive environmental anomaly | A nominal environmental condition is reported as hazardous. Protective modes, duty-cycle reductions, or sensor inhibitions can be activated unnecessarily, consuming resources and reducing mission or ACAS availability; repeated false alarms can also impair operator response. |
| Late measurement | Environmental information becomes available after its latest useful time, delaying protective action and degrading the validity of state estimation or autonomous decisions. |

## 3.5 Causes and Occurrence

Cause analysis considered initiating faults and enabling conditions. Examples include loss of power, sensor degradation, calibration drift, observation gaps, channel congestion, message corruption, outdated ephemerides, reference-frame mismatch, time desynchronization, model or covariance error, numerical instability, software defects, inadequate thresholds, missing constraints, resource-estimation error, valve or thruster faults, and incomplete coordination. Representative ground decision and planning examples are listed in Table 4.

The analysis does not assume that a listed cause is statistically independent. Common power, timing, software, environmental, and data sources can create correlated failures across multiple functions. Common-cause treatment is therefore a required extension in a mission-specific analysis.

Occurrence rankings compare the causal exposure of the failure modes within the conceptual architecture. They consider the number and plausibility of initiating mechanisms, operating and environmental exposure, architecture, and assumed baseline controls. They are not frequencies, probabilities, or predictions of in-service occurrence. The exact qualitative anchors are provided in Table S3 of the Supplementary Material.

Table 4
Causes associated with ground decision and maneuver-planning failure modes

| Failure mode | Causes and enabling conditions |
|---|---|
| Failure to react upon anomaly | Operator inaction. Alert fatigue. Missing procedures. Fault in response logic. |
| No CAM plan generated | Algorithm error. Software crash. Incomplete input data. Human inaction. |
| Delayed CAM plan generated | Inefficient algorithm. Processing overload. Suboptimal task prioritization. Slow hardware. |
| Incomplete or incorrect CAM plan generated | Incomplete input data. Outdated ephemerides. Missing mission constraints. Incorrect planning algorithm. |
| CAM plan creates new conjunction risk | Small screening volume. Outdated ephemerides. Maneuver intention not shared. Poor communication. |
| CAM plan violates mission objectives | Incorrect, incomplete or old constraints that do not reflect reality. Configuration errors (on constraint priority or safety margins). Coverage gaps. |

## 3.6 Detection and Detectability

Baseline detection provisions identify a failure before the unsafe effect becomes irreversible or provide evidence needed to diagnose and recover from it. Provisions include message-integrity and conformance checks, source and object-identity validation, timestamp and age limits, cross-source comparison, filter residuals, reasonableness checks, health monitoring, watchdogs, acknowledgement and timeout logic, telemetry trends, independent computation, pre-execution simulation, post-maneuver orbit determination, and periodic tests or audits. Propulsion-performance reporting examples are listed in Table 5.

Detection must be timely. A condition that is eventually detected only after the decision or maneuver window has closed does not provide effective risk control. D therefore ranks the difficulty of timely detection by the baseline provisions documented in the row. Recommended controls are prospective and are not used to justify the current D rank or baseline RPN.

Table 5
Baseline detection provisions for propulsion-performance reporting failures

| Failure mode | Baseline detection provisions |
|---|---|
| No propulsion-performance report generated | Timeout alarm on expected report. Health monitoring (heartbeat loss). Cross-check with other sources (IMUs detected thrust). |
| Invalid/incorrect report sent | Integrity and conformance checks (CRC/ECC, format validation). Plausibility checks (range, rate of change). Timestamp validation. Cross-check with other sources. Redundant sensors disagreement. |

## 3.7 Priority Logic

A qualitative priority-ranking stage was selected because mission-specific failure-rate data, calibrated diagnostic coverage, and an approved program criticality matrix were unavailable. Each failure mode received relative severity, occurrence, and detectability rankings from 1 to 10. The rankings support comparison within this dataset; they are not absolute probabilities, certification thresholds, or a quantitative ECSS criticality number.

The ranking logic was tailored to ACAS operational consequences. Tables 6–8 provide the compact banded scales for the FMECA classification, while Table S3 of the Supplementary Material provides explicit integer anchors and application rules:

Higher “S” means a more severe end effect,

Higher “O” means greater relative occurrence, and

Higher “D” means poorer timely detectability.

Table 6
Severity ranking scale used for the ACAS FMECA

| Rank | Operational interpretation – Severity “S” |
|---|---|
| 1–2 | Negligible to minor local effect; essential collision-avoidance capability and margins are preserved. |
| 3–5 | Limited to moderate degradation, rework, workload, or resource loss; collision-avoidance capability remains available. |
| 6–7 | Significant or major degradation, partial loss of a supporting function, or materially reduced margins and maneuver options. |
| 8–9 | Serious or critical effect that can remove a required barrier, corrupt a key output, create an unsafe state, or leave a conjunction insufficiently controlled. |
| 10 | Catastrophic end effect that can directly leave a credible collision unmitigated or contribute to loss of spacecraft or mission; for crewed applications, potential loss of life. |

Table 7
Relative occurrence ranking scale used for the ACAS FMECA

| Rank | Operational interpretation – Occurrence “O” |
|---|---|
| 1 | Exceptional within the conceptual architecture and stated operating assumptions. |
| 2–3 | Very remote to remote relative occurrence. |
| 4–6 | Occasional to moderately frequent relative occurrence. |
| 7–9 | Frequent to near-certain relative occurrence without additional control. |
| 10 | Expected or continuous in the baseline design or operating environment. |

Table 8
Detectability ranking scale used for the ACAS FMECA

| Rank | Operational interpretation – Detectability “D” |
|---|---|
| 1–2 | Almost certain or very high likelihood of timely detection before the unsafe effect develops. |
| 3–4 | High to moderate-high likelihood of timely detection. |
| 5–7 | Moderate to low likelihood of timely detection; indication can be indirect or delayed. |
| 8–9 | Very low or mainly post-event detectability. |
| 10 | No credible timely detection before the end effect. |

The Risk Priority Number was calculated as:

$$RPN = S \times O \times D \quad (1)$$

The baseline RPN is formula-driven for every row in the dataset. The RPN is a comparative priority index, but multiplication of ordinal scales can create non-unique combinations and apparent precision. It is therefore interpreted with the component scores: all modes with $S \geq 9$ are screened as priority candidates irrespective of RPN, after which RPN and D support ordering and allocation of further review. Values of 120 or 144 are descriptive dataset groupings, not acceptance criteria. Ranking stability should be tested when expert assessments or design assumptions change [30].

Tables 9 and 10 summarize the rankings, effects, causes, and baseline detection provisions for the four thruster-execution failure modes. The required-propulsion-unavailable entry has S = 10, O = 3, D = 3, and baseline RPN = 90. The component rankings remain visible beside the product.

Table 9
Current priority rankings for thruster-execution failure modes

| Failure mode | S | O | D | Baseline RPN |
|---|---|---|---|---|
| Required propulsion unavailable | 10 | 3 | 3 | 90 |
| Incorrect propulsion | 9 | 3 | 4 | 108 |
| Degraded or incomplete propulsion | 8 | 4 | 4 | 128 |
| Unstable propulsion | 9 | 3 | 4 | 108 |

Table 10
Effects, causes, and baseline detection provisions for thruster-execution failure modes

| Failure mode | Consolidated effects | Causes and baseline detection |
|---|---|---|
| Required propulsion unavailable | The propulsion authority required for the planned CAM is unavailable. The spacecraft may become underactuated or unable to achieve the commanded trajectory change, leaving the conjunction unmitigated and potentially causing loss of mission. | Causes: Loss of required propellant feed, ignition, valve actuation, electrical power, thermal conditioning, or a sufficient set of healthy thrusters; upstream resource failure; or hardware damage and blockage. Detection: Compare commanded and achieved acceleration or velocity change; monitor ignition, pressure, flow, temperature, valve state, and power; use start-timeout alarms and pre-burn readiness checks. |
| Incorrect propulsion | Thrust is produced with an incorrect direction, magnitude, timing, or duration. The achieved trajectory deviates from the CAM plan, can require corrective burns, and can leave the original conjunction unmitigated or create a secondary conjunction. | Causes: Thruster misalignment (mount shift assembly, thermal bowing). Wrong thruster fired (configuration errors, or misinterpretation due to corruption). Asymmetrical propellant delivery. Upstream failure in sensors or the control unit (sensor drift, contamination from exhaust). Component (nozzle) damage or degradation (thermal expansion). Detection: Discrepancy in expected values and real values from navigation sensors and thruster sensors. |
| Degraded or incomplete propulsion | Thrusters fire but produce less thrust than commanded, or the burn ends prematurely. CAMs are only partially executed, leaving residual collision risks. This can cause mission degradation and resource waste for corrective maneuvers. | Causes: Partial blockage in propellant lines due to ice or contamination. Valve actuators fault (degraded response, only opening partially). Fuel leakage or insufficient upstream pressure. Thruster wear or damage (erosion, nozzle cracks). Premature cutoff due to faulty sensor signal (false alarm), component fault or software fault. Detection: Discrepancy between commanded thrust and thruster performance. Discrepancy between commands and actual navigation data. Health monitoring alarms. |
| Unstable propulsion | Thrust oscillates during the burn, causing attitude disturbance, maneuver error, additional resource use, and increased structural loading. Collision-avoidance effectiveness can be reduced and a corrective maneuver may be required. | Causes: Gas entrainment, pressure-control fluctuation, propellant slosh, valve or regulator cycling, combustion or discharge instability, component wear, control-loop instability, or coupling with mission-specific structural modes. Detection: Fluctuations, oscillations or cycling in readings like velocity/acceleration, pressure in lines/chamber, temperature in thruster. Guidance, navigation, and control (GNC) alarms. Perform short pre-maneuver verifications if resources allow. |

# 3.8 Controls and Reassessment

Recommended risk-control measures were developed after considering the failure effects, causes, baseline detection provisions, severity, and comparative priority. Measures can prevent the initiating condition, detect or isolate it, compensate for degraded performance, restrict authority, provide independent confirmation, preserve safe margins, or reduce the consequence of an unavoidable failure. Selected environmental-monitoring examples are summarized in Table 11.

Recommendations were written as design or assurance objectives rather than universal technology prescriptions. A technique is included only when it is applicable to the mission architecture, environment, timing, and failure mechanism. For example, in-flight bias estimation and multi-sensor fusion are appropriate for spacecraft IMUs, while zero-velocity updates developed for terrestrial pedestrian or vehicle navigation are not generally applicable in orbital flight; the zero-velocity update (ZUPT) source is therefore cited as a rejected analogy rather than as an ACAS control [31].

No residual RPN is reported. Residual scoring would imply that the controls have been allocated to a specific design, implemented, verified, validated, and shown to provide the assumed independence and diagnostic coverage. A project application should record the action owner, verification method, status, evidence, and approved residual disposition.

After implementing any individual recommendation or combination of recommendations, the modified system should undergo a formal change-impact reassessment before the action is closed or residual risk is accepted. The reassessment should update the controlled architecture, interfaces, assumptions, functions, failure modes, effects, causes, baseline controls, S/O/D rankings, and verification evidence. FMECA should then be complemented by STPA or another interaction-focused method to determine whether the change introduces new hazards, unsafe control actions, loss scenarios, interface incompatibilities, common-cause or dependent failures, cybersecurity weaknesses, degraded-mode conflicts, or conflicts among recommendations. The affected integration level should then be reverified and revalidated through appropriate regression, interface, operational-scenario, and secondary-conjunction testing before residual risk is reassessed and the recommendation is formally closed.

Table 11
Recommended controls for environmental-monitoring failure modes

| Failure mode | Recommended risk-control measures |
|---|---|
| No measurement | Use an adaptive sampling strategy, independent power and data paths, and appropriately diverse environmental sensors, such as radiation, temperature, and charging monitors. Provide shielding and conservative degraded-mode logic. |
| False-negative environmental anomaly | Perform periodic calibration and threshold reviews using representative environments. Use overlapping coverage and conservative conflict handling when independent sources disagree. |
| False-positive environmental anomaly | Use independent or diverse sensor confirmation, persistence and hysteresis, contextual thresholds, calibration and self-test, and operator confirmation only for costly protective actions when time and workload permit. |
| Late measurement | Define maximum data age, allocate time-critical processing priority, adapt sampling when conditions change, and bound filtering delay. Use independent environmental indications where justified. |

# 4 Results

# 4.1 Overall Profile

The worksheet contains 127 failure modes with baseline RPN values from 18 to 180. The median is 100, the first quartile is 84, and the third quartile is 128. Forty-eight entries have RPN values of at least 120, 19 have values of at least 144, 60 have severity rankings of at least 9, and 23 have detectability rankings of at least 5. The 60 modes with $S \geq 9$ remain priority candidates irrespective of their RPN. Figure 2 shows the complete RPN distribution.

The distribution supports relative prioritization but should not be interpreted as a probability distribution. Several distinct combinations of S, O, and D produce the same RPN. High-severity failures can receive moderate RPN values when they are considered remote or readily detected, while less catastrophic failures can rank higher when they are relatively frequent and difficult to identify in time.

## 4.2 Highest RPN Modes

The highest-ranked failure mode is a false-negative decision by the ACAS decision module (ID 121), with S = 10, O = 3, D = 6, and RPN = 180. A required maneuver is not authorized, leaving the conjunction unmitigated. The ranking reflects catastrophic potential combined with moderate detection difficulty.

False-negative input validation (ID 116) and incorrect collision-probability output (ID 118) each have RPN = 162. Both can contaminate later decisions without producing an obvious component failure. Delayed tracking information (ID 5), delayed conjunction computation or delivery (IDs 12 and 14), and late environmental or health measurements (IDs 85 and 89) have RPN = 160 because the information may become unusable after the latest decision time.

Additional high-priority entries include incorrect conjunction data (ID 9), incomplete conjunction data (ID 11), telecommand-decoding failure (ID 64), false-negative autonomous reconfiguration (ID 72), unusable inertial measurement (ID 80), incorrect thrust-vector computation (ID 93), incorrect resource-state reporting (ID 105), false-positive maneuver decisions (ID 120), and maneuver plans that violate constraints (ID 126). Figure 3 summarizes the highest-ranked entries.

The lowest baseline RPN is assigned to loss of radioisotope power generation, if such a source is used (ID 102), with S = 9, O = 1, D = 2, and RPN = 18, because the selected baseline assumes that loss of electrical output would be directly observable through power telemetry and health monitoring. These are relative engineering judgments rather than a statistical failure-rate estimate. The row remains conditional because most collision-avoidance spacecraft do not use radioisotope power.

## 4.3 Functional Patterns

Onboard sensors have the highest block median RPN (135), followed by the ACAS decision module (132). Ground-based tracking and conjunction assessment are tied at a median of 120. The pattern reflects the sensitivity of collision avoidance to data quality, timeliness, model validity, and the authority to authorize or reject a maneuver. It does not imply that every implementation will have the same ranking.

Ground tracking and conjunction assessment are dominated by coverage, calibration, fusion, time, data-format, and delivery failures. Ground control adds monitoring, procedural, command, and coordination failures. Onboard communications add link, interface, protocol, and RFI failures. The OBC and sensor blocks add state-estimation, validation, reconfiguration, power-conversion, and health-monitoring failures. The propulsion chain adds plan validation, resource estimation, command allocation, thrust execution, and feedback failures.

The results demonstrate that ACAS risk is information-centric and time-dependent. A valid message delivered too late can be as ineffective as a missing message. A physically healthy subsystem can contribute to an unsafe decision if its output is incorrectly associated, formatted, timestamped, modeled, or interpreted.

## 4.4 Cross-Cutting Findings

A thematic synthesis of the complete worksheet identified six recurring findings that cut across the functional blocks. These themes do not create additional scores or frequency categories; they summarize mechanisms and assurance needs that recur across the 127 failure-mode rows. Table 12 consolidates the findings.

Table 12
Cross-cutting findings derived from the complete ACAS FMECA

| Cross-cutting finding | Recurrent manifestations | General assurance implication |
|---|---|---|
| **Information integrity and provenance** | Wrong source or object association; corrupted, incomplete, or invalid messages; reference-frame, unit, covariance, configuration, or data-age errors. | Validate source, identity, format, frame, units, covariance, version, completeness, and age before operational use, while preserving provenance through the decision chain. |
| **Time and deadline assurance** | Delayed tracking, conjunction products, onboard measurements, commands, decisions, and maneuver plans; valid information arriving after its latest useful time. | Define synchronized time services, latency budgets, latest-useful times, processing priorities, timeout and escalation logic, and bounded-age fallback data. |
| **Validation and decision asymmetry** | False-negative validation or maneuver decisions can leave a threat unmitigated; false-positive outcomes can cause unnecessary maneuvers, resource use, and secondary risk. | Use calibrated thresholds, independent checks, explicit disagreement handling, hysteresis or commitment logic, and conservative treatment of uncertainty without adopting an unconditional maneuver default. |
| **Authority and coordination** | Conflicting or unclear ground and onboard decisions; incomplete maneuver-intent exchange; loss of coordination among operators, service providers, and spacecraft. | Define authority modes and transitions, authenticated coordination exchanges, degraded-mode decision rules, and traceable records of responsibility and decision state. |
| **Resource and actuation assurance** | Incorrect resource-state estimates; infeasible plans; thrust-vector, allocation, command, or execution errors; unavailable, degraded, or unstable propulsion. | Perform pre-execution feasibility and readiness checks, preserve margins, use independent resource-state evidence where justified, verify controllability, and compare commanded with achieved performance. |
| **Recovery and achieved-state verification** | False-negative or inadequate reconfiguration; missing performance feedback; recovery to an unsafe configuration; absent or delayed post-maneuver confirmation. | Validate reconfiguration and degraded modes, monitor health and performance independently, confirm the achieved orbit after the maneuver, and reassess changes before closing residual risk. |

Across the themes, the principal result is that ACAS safety depends not only on the correctness of an onboard decision algorithm, but also on maintaining trustworthy and timely information through authority transitions and on verifying that the commanded maneuver produced the intended state. False-negative and delayed modes recur among the highest priorities because they can preserve apparently nominal hardware while eliminating the remaining decision or maneuver window.

# 5 Discussion

## 5.1 Ground Segment

Ground tracking should use diverse observations and transparent source-quality management to reduce blind periods, calibration errors, and single-source dominance. Multi-star-tracker detection research illustrates one possible approach to diversified space-object observation [32]. Reconfigurable optical-system research provides another possible approach to space-object tracking [33]. The mission applicability and maturity of either approach must be assessed. Data-fusion methods can support cross-source consistency, provenance, and confidence management [34].

Tracking and conjunction services should monitor end-to-end latency, message age, object identity, reference frames, units, covariance, and source history. Critical products should have defined latest-useful times and escalation logic. QoS policies may prioritize time-critical data, but the prioritization policy must not starve lower-ranked observations that are necessary to maintain catalogue quality.

Inter-agency simulation, coordinated exercises, and agreed communication channels can improve readiness for unusual encounters. The ground segment should also maintain validated fallback methods for incomplete data, but a simplified model or last valid state must have a bounded age, increasing uncertainty, and clearly defined applicability.

## 5.2 Ground Control

Ground control requires trained operators, concise procedures, decision-support tools, periodic drills, audits, and post-maneuver reviews. Early data requests and command preparation can preserve time margin, but premature commitment can create new risks if the conjunction state changes.

Ground systems should cross-check onboard state against independent tracking and expected maneuver effects. When communication or information quality is poor, the operational concept must define which decisions remain autonomous, which require human confirmation, and which trigger conservative degraded modes.

Human confirmation is not a universal mitigation. It is effective only when communication, workload, competence, and decision time permit. The system should not rely on an operator as an unmodeled last barrier; the human role, information requirements, authority, and response time must be explicitly designed and verified.

## 5.3 Communications

Communications assurance should combine link margin, appropriate error detection and correction, message conformance, integrity and authenticity checks, sequence and timestamp validation, and redundant paths where justified. Research on multiple-cell upsets informs the selection of error-correction techniques for space electronics [35]. Research on short LDPC-coded space messages informs the design of coding sequences under short-message constraints [36]. The selected scheme must match the link, latency, and implementation constraints.

Critical information may be retransmitted or transferred through acknowledged file-delivery services where the latency budget permits. Automatic retries require limits to prevent congestion or stale-message acceptance. Software and interface versions must remain controlled across ground and flight systems.

RFI should be monitored and coordinated across entities. Frequency changes, timing changes, beam steering, and alternative links can mitigate interference, but an uncoordinated mitigation can create new interference or disrupt the data needed for collision avoidance. Radiation-induced upsets in onboard electronics are a separate physical mechanism and should not be mislabeled as RFI.

## 5.4 Computing and Sensors

The OBC should provide protected memory, controlled configuration, health monitoring, watchdogs, time services, and validated reconfiguration logic. The central role of onboard computers in data handling and subsystem coordination makes common power, timing, and software failures particularly important [37].

Autonomous reconfiguration should be tested against representative fault, timing, and degraded-data scenarios. A false-negative trigger can leave a failed configuration active; a false-positive trigger can unnecessarily remove healthy capability. The target safe configuration and the criteria for returning to normal operation must be defined.

Navigation and attitude sensors require calibration, residual monitoring, saturation handling, thermal control, radiation and vibration protection, and cross-checking among independent modalities. Range and Doppler ambiguities are well-known in radar systems, but terrestrial weather-radar techniques are not direct validation for spacecraft tracking [38].

Environmental and health sensors should use adaptive sampling only within validated bounds. Dynamic thermal-control concepts demonstrate that spacecraft thermal management can be actively adapted, but such research does not replace mission-specific sensor and protection design [39]. Maximum data age, filtering delay, and alarm persistence should be explicit safety parameters.

## 5.5 Propulsion and Resources

Propulsion controls should validate the CAM plan, compute thrust and resource allocations with current models, dispatch commands to the correct devices, verify readiness, and compare achieved motion with the expected trajectory. Research on autonomous thruster-failure recovery shows that some actuator failures can be accommodated by reconfiguration [40]. Formation-flying guidance research likewise demonstrates compensation strategies for actuator faults [41]. In both cases, controllability and performance depend on the remaining actuator geometry and available resources.

Short verification pulses may support calibration when they are operationally safe and when their trajectory effect is included in the assessment. They should not be treated as a general requirement because time, fuel, and secondary-conjunction constraints may preclude them.

Resource management should preserve fuel and power reserves, use independent sensing or estimation where justified, and account for uncertainty in consumption. Zero-boil-off research can inform long-duration cryogenic systems, but it applies only to compatible propellant architectures [42]. Solar-array contingency design should consider deployment and pointing failures documented in spacecraft mechanisms experience [43].

Fuel-cell architectures require reactant, water, pressure, and thermal management, together with leak isolation and reserve power. Multi-stack fuel-cell research provides evidence on redundancy architecture and energy management [44]. Aerospace regenerative fuel-cell research identifies fluidic-component design and management challenges [45]. Hydrogen quality requirements can use ISO 14687:2025 [46].

POGO is a coupled structural-propulsion instability associated mainly with launch vehicles and high-thrust liquid propulsion. The NASA design criteria provide historical propulsion-assurance evidence, but POGO accumulators are not a general control for low-thrust on-orbit collision-avoidance systems [47].

## 5.6 ACAS Logic

ACAS processing should validate source, identity, format, units, reference frame, timestamp, covariance, completeness, and plausibility before accepting data. Suspect sources can be isolated or down-weighted through a

controlled source-quality policy. Validation criteria should be audited to detect permissive thresholds that admit bad data and restrictive thresholds that reject valid data.

Collision-probability models should be tested across representative encounter geometries, covariance conditions, coordinate transformations, numerical tolerances, and out-of-scope scenarios. Independent or simplified calculations can provide cross-checks, but disagreement requires an explicit decision process rather than automatic averaging.

Although the representative function is named “compute collision probability” for traceability to the selected architecture, the assessment is not restricted to a single probability-of-collision threshold. Mission implementations may combine probability, miss distance, consequence, uncertainty, maneuverability, or other validated risk metrics, provided their applicability domain and decision logic are explicitly defined.

Decision logic should represent data quality and uncertainty, use hysteresis or commitment windows where appropriate, and prevent repeated oscillation between maneuver and no-maneuver states. A false-negative decision is the highest-ranked failure; however, defaulting automatically to a maneuver is not safe because the proposed maneuver can be infeasible, violate constraints, consume critical resources, or create a secondary conjunction.

Every authorized plan should therefore pass feasibility, resource, attitude, communications, mission-constraint, and secondary-conjunction checks. Prevalidated maneuver templates can reduce planning time, but templates require configuration control and must be updated for the current spacecraft state and environment.

Post-maneuver verification should use independent navigation or tracking evidence to confirm achieved state and update later conjunction assessments. The system should retain logs of inputs, validation decisions, model versions, thresholds, authority transitions, commands, telemetry, and achieved trajectory to support investigation and continuous improvement.

## 5.7 Adjacent Measures

The research surveys broader space-debris and collision-consequence measures, including shielding, spacecraft orientation, active debris deflection, and debris-removal or deceleration concepts [48]. These measures address debris prevention, remediation, or consequence reduction rather than the functional reliability of ACAS.

They are therefore not treated as controls for the identified ACAS failure modes. Shielding and robust orientation can reduce damage from small particles, but they do not replace avoidance of trackable collision threats. Active interaction with debris introduces fragmentation, targeting, authority, and mission risks that require a separate system-safety and legal assessment.

## 5.8 Method Assessment

The completed analysis is structured as a research-level tailored functional FMECA. It provides traceability from a controlled functional boundary through failure modes, effects, causes, baseline detection provisions, S/O/D rankings, baseline RPN, and recommended controls. The worksheet can support design reviews, verification planning, test-case selection, operational procedures, identification of candidate critical functions and failure modes, and allocation of additional engineering attention.

Accordingly, recommendations should be managed as configuration-controlled system changes rather than isolated worksheet actions. Closure requires confirmation that the implemented change remains compatible with adjacent recommendations and does not create new interaction, interface, common-cause, cybersecurity, or degraded-mode risks.

A mission-specific application should use explicit completion criteria, peer review, configuration control, and consistency checks across all rows.

The principal tailoring differences from a design-specific ECSS FMECA are explicit: effects are consolidated rather than separated into local and successive higher levels; O is a relative rank rather than a failure probability; the priority index includes detectability; single-point and common-cause failures are not closed systematically; and recommended controls have no verified residual score. These limitations do not invalidate the research objective, but they prevent the research from being used as final certification or qualification evidence, without further specific application.

FMECA can become large and time-consuming for interconnected systems. Decomposition improves manageability but can obscure dependencies and interactions. Common causes, feedback loops, timing, adaptive behavior, conflicting control actions, and organizational influences are not naturally represented by a linear row-based model.

The qualitative RPN adds a prioritization mechanism but does not create quantitative risk. Ordinal multiplication can conceal different S/O/D profiles, and a high severity should remain visible even when a low occurrence or detection rank reduces the product. The ranking should be accompanied by the component scores, severity-led screening, sensitivity analysis, and expert rationale.

STPA is suited to unsafe interactions, control authority, process-model flaws, and losses that occur without component failure. The FMECA and prior STPA analyses are therefore complementary rather than competing. A method-comparison study consolidates this conclusion across FMECA, HAZOP, and STPA [49].

## 5.9 Limitations

The system architecture is representative and does not model a specific spacecraft, orbit, propulsion technology, operator, traffic-coordination service, mission phase set, or control-authority allocation. Failure modes, effects, ratings, and controls must be tailored before use on a real mission.

Occurrence and detection rankings are engineering judgments rather than estimates derived from operational statistics. The RPN values support internal comparison only. No claim is made that the ranking predicts accident probability or satisfies a regulatory acceptance criterion.

The analysis does not fully model common-cause failure, cybersecurity attack paths, human and organizational behavior, software control interactions, dynamic reconfiguration, or the temporal evolution of a conjunction. These topics require complementary methods and scenario-based validation.

# 6 Conclusions

This study applied functional FMECA to an end-to-end autonomous collision-avoidance operation. The analysis defined 34 functions and identified 127 failure modes spanning ground tracking, conjunction assessment, ground control, communications, onboard computing and sensing, autonomous processing and decision-making, maneuver planning, propulsion resources, actuation, and feedback.

The baseline RPN values range from 18 to 180. The leading priorities are associated with false-negative maneuver decisions, acceptance of invalid inputs, incorrect collision-probability outputs, delayed information, unusable navigation or health data, false-negative reconfiguration, resource-state errors, and unsafe maneuver plans. The cross-cutting findings emphasize information provenance and integrity, data age and deadline control, validation asymmetry,

authority coordination, resource and actuation assurance, and independent confirmation of the achieved maneuver state.

Recommended controls include diverse and graded information sources, message conformance and authenticity checks, deadline monitoring, calibration and health monitoring, independent computation, controlled degraded modes, conservative uncertainty treatment, robust decision logic, validated templates, propulsion and resource margins, and post-maneuver confirmation.

FMECA provides useful traceability and comparative prioritization for design and operational assurance. The analysis is methodologically coherent for its stated exploratory purpose because the scope, ground rules, baseline, ranking logic, control status, and limitations are explicit. Its limitations remain significant for autonomous collision avoidance: the method is analyst-dependent, largely static, weak in representing interactions and organizational control, and sensitive to ordinal ranking choices. It should therefore be maintained iteratively and combined with STPA, scenario analysis, simulation, quantitative reliability data, common-cause analysis, and independent multidisciplinary review.

## Abbreviations

**ACAS** Autonomous Collision Avoidance System

**ADM** Attitude Data Message

**CAM** Collision-Avoidance Maneuver

**CCSDS** Consultative Committee for Space Data Systems

**CDM** Conjunction Data Message

**CRC** Cyclic Redundancy Check

**ECC** Error-Correction Code

**FMEA** Failure Mode and Effects Analysis

**FMECA** Failure Mode, Effects and Criticality Analysis

**FRAM** Functional Resonance Analysis Method

**FTA** Fault Tree Analysis

**HAZOP** Hazard and Operability Study

**IMU** Inertial Measurement Unit

**ISO** International Organization for Standardization

**NDM** Navigation Data Message

**OBC** Onboard Computer

**ODM** Orbit Data Message

**QoS** Quality of Service

| | |
|---|---|
| **RFI** | Radio-Frequency Interference |
| **RPN** | Risk Priority Number |
| **STC** | Space Traffic Coordination |
| **STPA** | System-Theoretic Process Analysis |
| TDM | Tracking Data Message |

## Declarations

Funding

No funding was received for conducting this study.

Competing interests

The authors have no relevant financial or non-financial interests to disclose.

Author contributions

**Tomás Costa Pinho:** conceptualization, investigation, methodology, formal analysis, data curation, visualization, and writing—original draft. **Antonio Vinicius Diniz Merladet:** conceptualization, methodology, data curation, supervision, validation, project administration, and writing—original draft. **Chiara Manfletti:** supervision, validation, and writing—review and editing. Daniel Rondon Pleffken: methodology, validation, and writing—review and editing. **Carlos Henrique Netto Lahoz:** methodology, supervision, validation, and writing—review and editing.

Data availability

The data supporting this study are provided in the article and supplementary material. Additional information used in the analysis is available from the public sources listed in the references.

## References

1. European Space Agency: Space Environment Statistics: space debris by the numbers. ESA Space Debris User Portal (2026). https://sdup.esoc.esa.int/discosweb/statistics/.
2. National Aeronautics and Space Administration: Orbital debris frequently asked questions. NASA Orbital Debris Program Office. https://orbitaldebris.jsc.nasa.gov/faq/.
3. Muelhaupt, T.J., Sorge, M.E., Morin, J., Wilson, R.S.: Space traffic management in the new space era. Journal of Space Safety Engineering 6(2), 80-87 (2019). https://doi.org/10.1016/j.jsse.2019.05.007
4. Eberle, C., Sebesvari, Z.: Technical report: Space debris. In: Interconnected Disaster Risks 2023: Risk Tipping Points. United Nations University Institute for Environment and Human Security, Bonn (2023). https://doi.org/10.53324/YIKU7602
5. European Space Agency: About space debris. ESA Space Safety. https://www.esa.int/Space_Safety/Space_Debris/About_space_debris.
6. Bourriez, N., Loizeau, A., Abdin, A.F.: Spacecraft autonomous decision-planning for collision avoidance: a reinforcement learning-based approach. In: 74th International Astronautical Congress, Baku, Azerbaijan (2023),

Paper IAC-23-A6.7.6.x76800. https://arxiv.org/abs/2310.18966

7. Borgovini, R., Pemberton, S., Rossi, M.: Failure mode, effects, and criticality analysis (FMECA). Report CRTA-FMECA. Reliability Analysis Center, Rome, NY (1993). https://apps.dtic.mil/sti/pdfs/ADA278508.pdf
8. U.S. Department of Defense: MIL-STD-1629A: Procedures for performing a failure mode, effects, and criticality analysis. Revision A, 24 November 1980; canceled 4 August 1998 with no superseding document. Department of Defense, Washington, DC (1980). https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=37027
9. Sharma, K.D., Srivastava, S.: Failure mode and effect analysis implementation: a literature review. Journal of Advance Research in Aeronautics and Space Science 5(1-2), 1-17 (2018)
10. International Electrotechnical Commission: IEC 60812:2018 Failure modes and effects analysis (FMEA and FMECA), 3rd edn. IEC, Geneva (2018). https://webstore.iec.ch/en/publication/26359
11. European Cooperation for Space Standardization: ECSS-Q-ST-30-02C: Failure modes, effects (and criticality) analysis (FMEA/FMECA). ECSS, Noordwijk (2009), reconfirmed 14 June 2023. https://ecss.nl/standard/ecss-q-st-30-02c-failure-modes-effects-and-criticality-analysis-fmeafmeca/
12. Lal, B., Balakrishnan, A., Caldwell, B.M., Buenconsejo, R.S., Carioscia, S.A.: Global trends in space situational awareness (SSA) and space traffic management (STM). Report D-9074. IDA Science and Technology Policy Institute, Washington, DC (2018). https://apps.dtic.mil/sti/pdfs/AD1123106.pdf
13. International Organization for Standardization: ISO 23705:2026 Space systems - Identifying, evaluating and avoiding collisions between orbiting objects, 1st edn. ISO, Geneva (2026). https://www.iso.org/standard/87556.html
14. International Organization for Standardization: ISO/FDIS 9490 Space systems - Space Traffic Coordination (STC). Final Draft International Standard, stage 50.20. ISO, Geneva (2026). https://www.iso.org/standard/83500.html
15. Consultative Committee for Space Data Systems: Navigation Data Messages Overview. CCSDS 500.2-G-3. CCSDS, Washington, DC (2023). https://ccsds.org/Pubs/500x2g3.pdf
16. Consultative Committee for Space Data Systems: Orbit Data Messages. CCSDS 502.0-B-3. CCSDS, Washington, DC (2023). https://ccsds.org/Pubs/502x0b3e1.pdf
17. Consultative Committee for Space Data Systems: Conjunction Data Message. CCSDS 508.0-B-1, incorporating Technical Corrigendum 2 (October 2021). CCSDS, Washington, DC (2013). https://ccsds.org/Pubs/508x0b1e2c2.pdf
18. Consultative Committee for Space Data Systems: Tracking Data Message. CCSDS 503.0-B-2, incorporating Technical Corrigendum 1 (October 2021). CCSDS, Washington, DC (2020). https://ccsds.org/Pubs/503x0b2c1.pdf
19. Consultative Committee for Space Data Systems: Attitude Data Messages. CCSDS 504.0-B-2. CCSDS, Washington, DC (2024). https://ccsds.org/Pubs/504x0b2.pdf
20. Consultative Committee for Space Data Systems: CCSDS File Delivery Protocol (CFDP). CCSDS 727.0-B-5. CCSDS, Washington, DC (2020). https://ccsds.org/Pubs/727x0b5e1.pdf
21. Reed, H., Tsamis, N., Dailey, N.: Space sustainability and traffic management requires trusted space stakeholder coordination. In: Advanced Maui Optical and Space Surveillance Technologies Conference, Wailea, Hawaii (2023). https://doi.org/10.64861/MVHC2799
22. Shields, R.: Space sustainability as a national priority in the United States. Journal of Space Safety Engineering 9(4), 481-487 (2022). https://doi.org/10.1016/j.jsse.2022.08.002
23. Sadat, M., Siegel, J.: Space traffic management: time for action. Issue brief. Atlantic Council, Forward Defense, Washington, DC (2022). https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/space-traffic-

management-time-for-action/

24. International Electrotechnical Commission: IEC 61882:2016 Hazard and operability studies (HAZOP studies) - Application guide, 2nd edn. IEC, Geneva (2016). https://webstore.iec.ch/en/publication/24321
25. Sun, L., Li, Y.F., Zio, E.: Comparison of the HAZOP, FMEA, FRAM, and STPA methods for the hazard analysis of automatic emergency brake systems. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering 8(3), 031104 (2022). https://doi.org/10.1115/1.4051940
26. Yu, S., Yang, Q., Liu, J., Pan, M.: A comparison of FMEA, AFMEA and FTA. In: 2011 9th International Conference on Reliability, Maintainability and Safety, pp. 954-960 (2011). https://doi.org/10.1109/ICRMS.2011.5979423
27. Merladet, A.V.D., Jouisse, M., Moreira, G., Silveira, R.D.M., Lahoz, C.H.N., Manfletti, C.: Recommendations for the operation of autonomous collision avoidance systems through STPA application. Presented at the MIT STAMP Workshop 2025, Cambridge, MA (2025). https://psas.scripts.mit.edu/home/2025-stamp-workshop-program/
28. Sulaman, S.M., Beer, A., Felderer, M., Höst, M.: Comparison of the FMEA and STPA safety analysis methods - a case study. Software Quality Journal 27(1), 349-387 (2019). https://doi.org/10.1007/s11219-017-9396-0
29. National Aeronautics and Space Administration: Procedure for failure mode, effects, and criticality analysis (FMECA). NASA RA-006-013-1A; NASA-TM-X-65227. NASA, Washington, DC (1966). https://ntrs.nasa.gov/citations/19700076494
30. Bowles, J.B.: An assessment of RPN prioritization in a failure modes effects and criticality analysis. In: Annual Reliability and Maintainability Symposium, pp. 380-386 (2003). https://doi.org/10.1109/RAMS.2003.1182019
31. Suresh, R.P., Sridhar, V., Pramod, J., Talasila, V.: Zero Velocity Potential Update (ZUPT) as a correction technique. In: 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages, pp. 1-8 (2018). https://doi.org/10.1109/IoT-SIU.2018.8519902
32. Liu, M., Wang, H., Yi, H., Xue, Y., Wen, D., Wang, F., Shen, Y., Pan, Y.: Space debris detection and positioning technology based on multiple star trackers. Applied Sciences 12(7), 3593 (2022). https://doi.org/10.3390/app12073593
33. Haritonova, D., Zarins, A., Rubans, A.: Reconfigurable optical system for space object tracking. Latvian Journal of Physics and Technical Sciences 62(4), 3-13 (2025). https://doi.org/10.2478/lpts-2025-0025
34. Oltrogge, D., Kerr, E., Biswas, S.K., Lozano, J.M., Lucken, R., Mulholland, M., et al.: Space traffic management: data fusion. Acta Astronautica 230, 131-138 (2025). https://doi.org/10.1016/j.actaastro.2024.08.056
35. Gracia-Morán, J., Saiz-Adalid, L.J., Gil-Tomás, D., Gil-Vicente, P.J.: Improving error correction codes for multiple-cell upsets in space applications. IEEE Transactions on Very Large Scale Integration Systems 26(10), 2132-2142 (2018). https://doi.org/10.1109/TVLSI.2018.2837220
36. Battaglioni, M., Andrews, K., Giuliani, R., Marinelli, F., Chiaraluce, F., Baldi, M.: Design and analysis of the tail sequence for short LDPC-coded space communications. IEEE Transactions on Aerospace and Electronic Systems 61(6), 16938-16952 (2025). https://doi.org/10.1109/TAES.2025.3599498
37. European Space Agency: Onboard computers and data handling. ESA Space Engineering and Technology. https://www.esa.int/Enabling_Support/Space_Engineering_Technology/Onboard_Computers_and_Data_Handling.
38. Mahapatra, P.R., Zrnić, D.S., Eilts, M.D.: Strategies for mitigating range and Doppler ambiguities in the WSR-88D. NOAA National Severe Storms Laboratory, Norman, OK (1994). https://www.nssl.noaa.gov/publications/rv-ambiguity/Strategies_For_Mitigating_Range_And_Doppler_In_WSR88D.pdf
39. Peng, Y., Wu, J., Ni, J., Li, X., Li, L., Zhao, B., Li, M., Pei, G.: Magnetic-controlled dynamic radiative cooling and solar heating for advanced space thermal management. Carbon Neutrality 4, 23 (2025). https://doi.org/10.1007/s43979-025-00137-8

40. Pong, C.M.: Autonomous thruster failure recovery for underactuated spacecraft. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA (2010). http://hdl.handle.net/1721.1/62491
41. dos Santos, W.G., Mason, P., Stoneking, E.T., Sarli, B.V.: Reconfigurable guidance strategy for compensating actuator faults in spacecraft formation flying. Journal of Guidance, Control, and Dynamics 48(2), 282-296 (2025). https://doi.org/10.2514/1.G008087
42. National Aeronautics and Space Administration: Zero boil-off tank experiments to enable long-duration space exploration. NASA Science Mission Directorate (2024). https://science.nasa.gov/science-research/science-enabling-technology/zero-boil-off-tank-experiments-to-enable-long-duration-space-exploration/.
43. Rivera, A., Stewart, A.: Study of spacecraft deployables failures. In: 19th European Space Mechanisms and Tribology Symposium, online (2021). NASA NTRS 20210020397. https://ntrs.nasa.gov/citations/20210020397
44. Qiu, Y., Zeng, T., Zhang, C., Wang, G., Wang, Y., Hu, Z., Yan, M., Wei, Z.: Progress and challenges in multi-stack fuel cell system for high power applications: architecture and energy management. Green Energy and Intelligent Transportation 2(2), 100068 (2023). https://doi.org/10.1016/j.geits.2023.100068
45. Smith, P.J., Zhong, Z., Cain, K.P., Cashman, J.L., Debelak, B.W., Gilligan, R.P., et al.: Aerospace regenerative fuel cell fluidic component design challenges. NASA/TM-20210024659. NASA Glenn Research Center, Cleveland, OH (2022). https://ntrs.nasa.gov/citations/20210024659
46. International Organization for Standardization: ISO 14687:2025 Hydrogen fuel quality - Product specification, 2nd edn. ISO, Geneva (2025). https://www.iso.org/standard/82660.html
47. Rubin, S.: Prevention of coupled structure-propulsion instability (POGO). NASA SP-8055. National Aeronautics and Space Administration, Washington, DC (1970). https://ntrs.nasa.gov/citations/19710016604
48. Leal Filho, W., Abubakar, I.R., Hunt, J.D., Dinis, M.A.P.: Managing space debris: risks, mitigation measures, and sustainability challenges. Sustainable Futures 10, 100849 (2025). https://doi.org/10.1016/j.sftr.2025.100849
49. Merladet, A.V.D., Lahoz, C.H.N., Manfletti, C., Pinho, T.C., Rodrigues, J.P.S., Silveira, R.D.M., et al.: Comparison of hazard analysis methods for autonomous collision avoidance systems in the space sector. In: Socha, V., Hanakova, L. (eds.) Proceedings of the 25th International Conference on New Trends in Civil Aviation, NTCA 2026, pp. 343-355. Czech Technical University in Prague, Prague (2026). https://doi.org/10.23919/NTCA68808.2026.11524134

## Figures

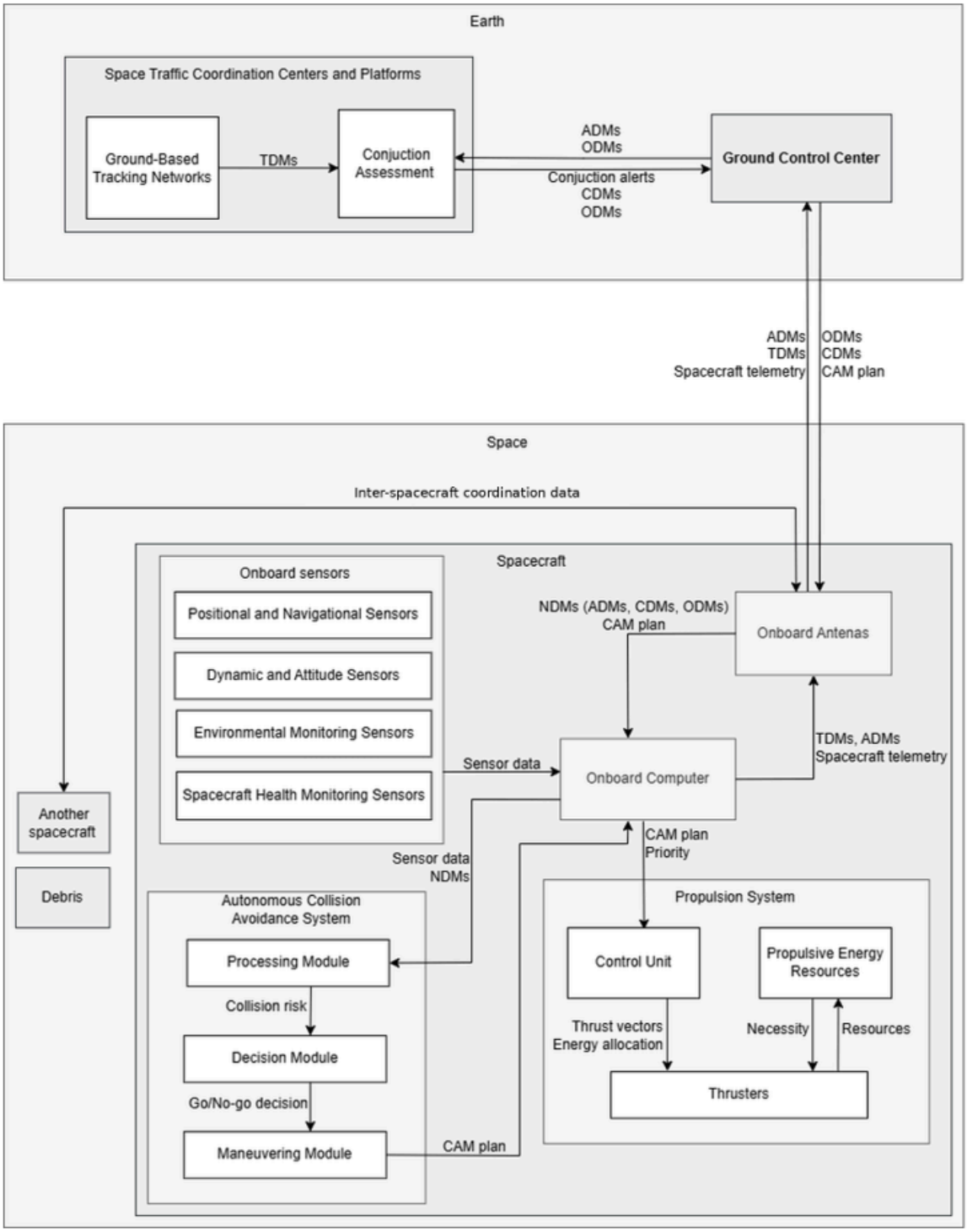



**Figure 1**

Functional block diagram illustrating the operation of ACAS

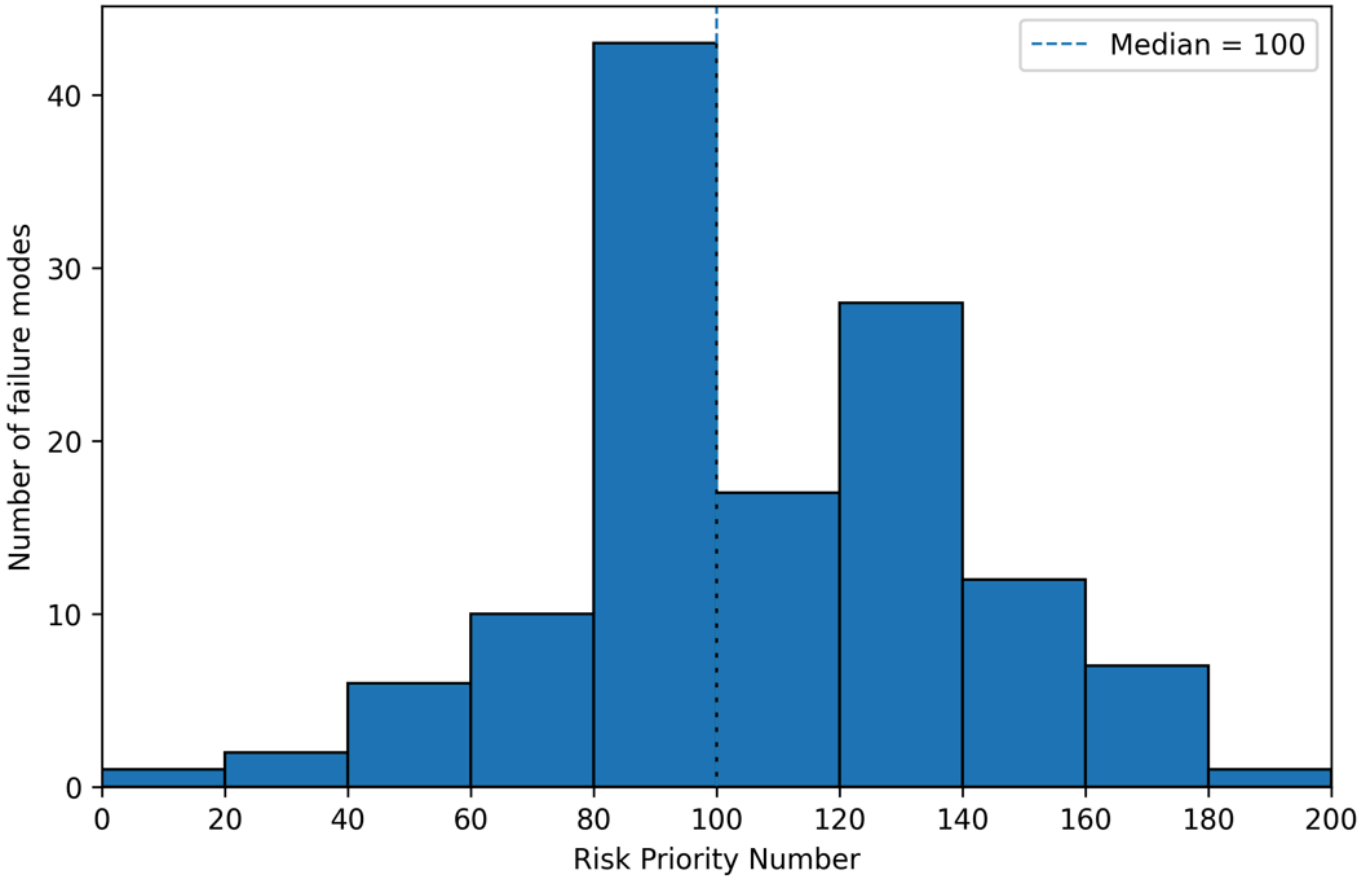



**Figure 2**

Distribution of baseline RPN values for the 127 failure modes

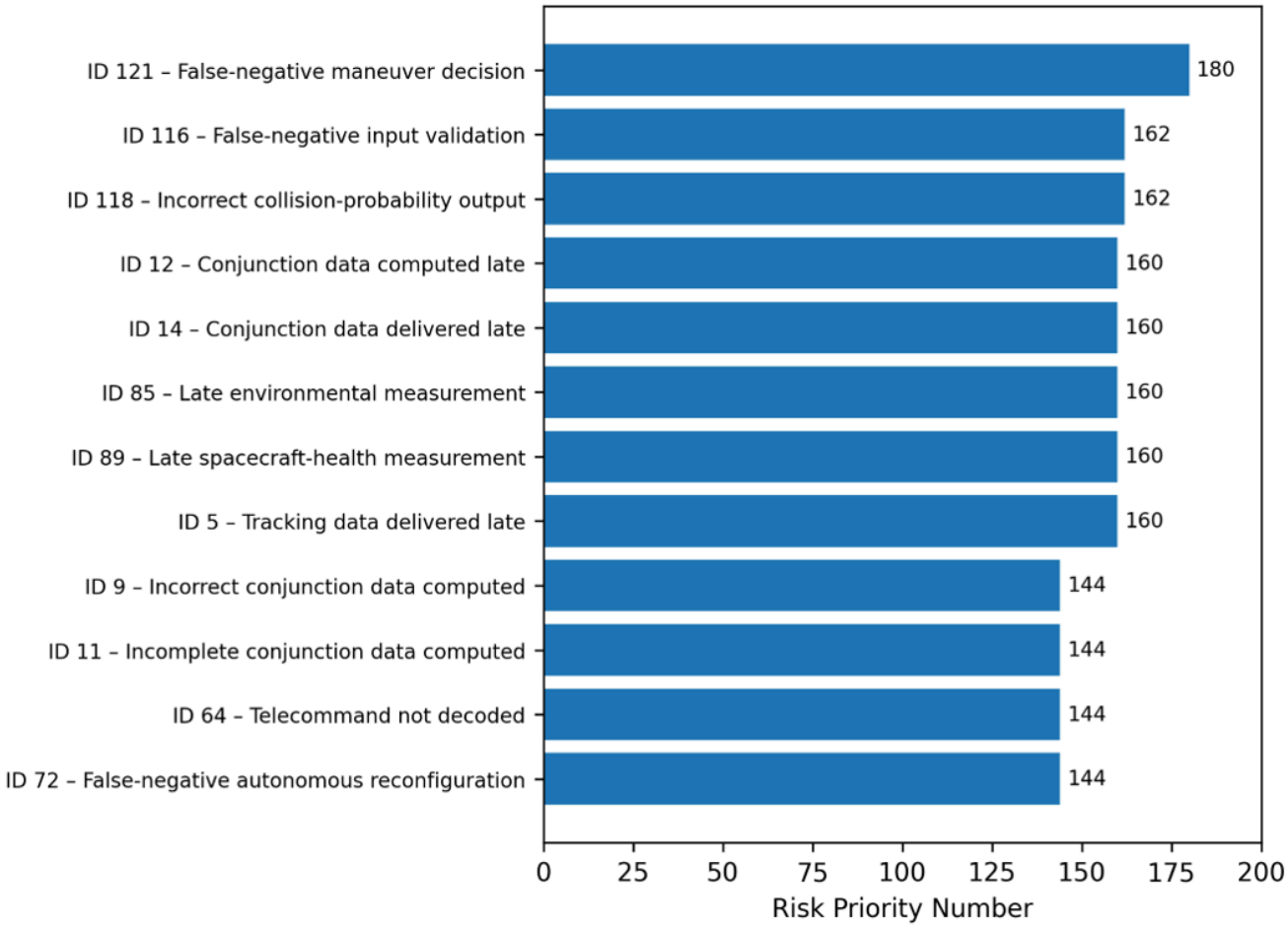



**Figure 3**

Highest baseline RPN failure modes in the FMECA dataset

## Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- ACASFMECACEASSupplementaryMaterialSubmission1.docx