Recommendations for the operation of Autonomous Collision Avoidance Systems through STPA application

Capt. Antonio Vinicius **Diniz** Merladet

Dr. Carlos Lahoz; Dra. Chiara Manfletti; Morgane Jouisse; Col. Moreira; Capt. Silveira

MIT STAMP Workshop 2025



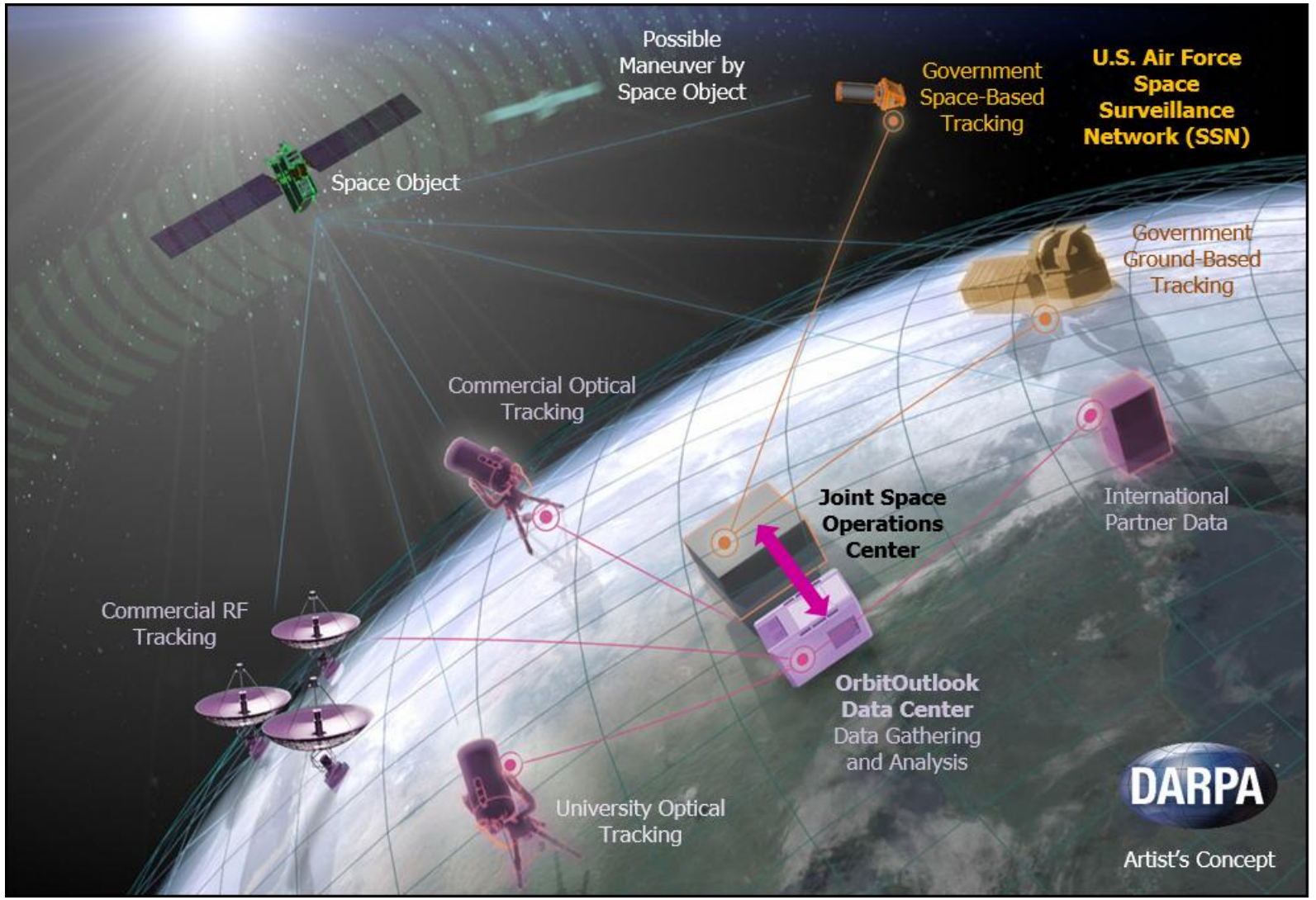
Objective

This analysis identifies hazards, unsafe control actions, and loss scenarios that may affect spacecraft safety, mission success, and the orbital environment. It proposes safety constraints and recommendations to support the design, operation, and regulatory framework of Autonomous Collision Avoidance Systems (ACAS), aiming for safer and more sustainable space operations.

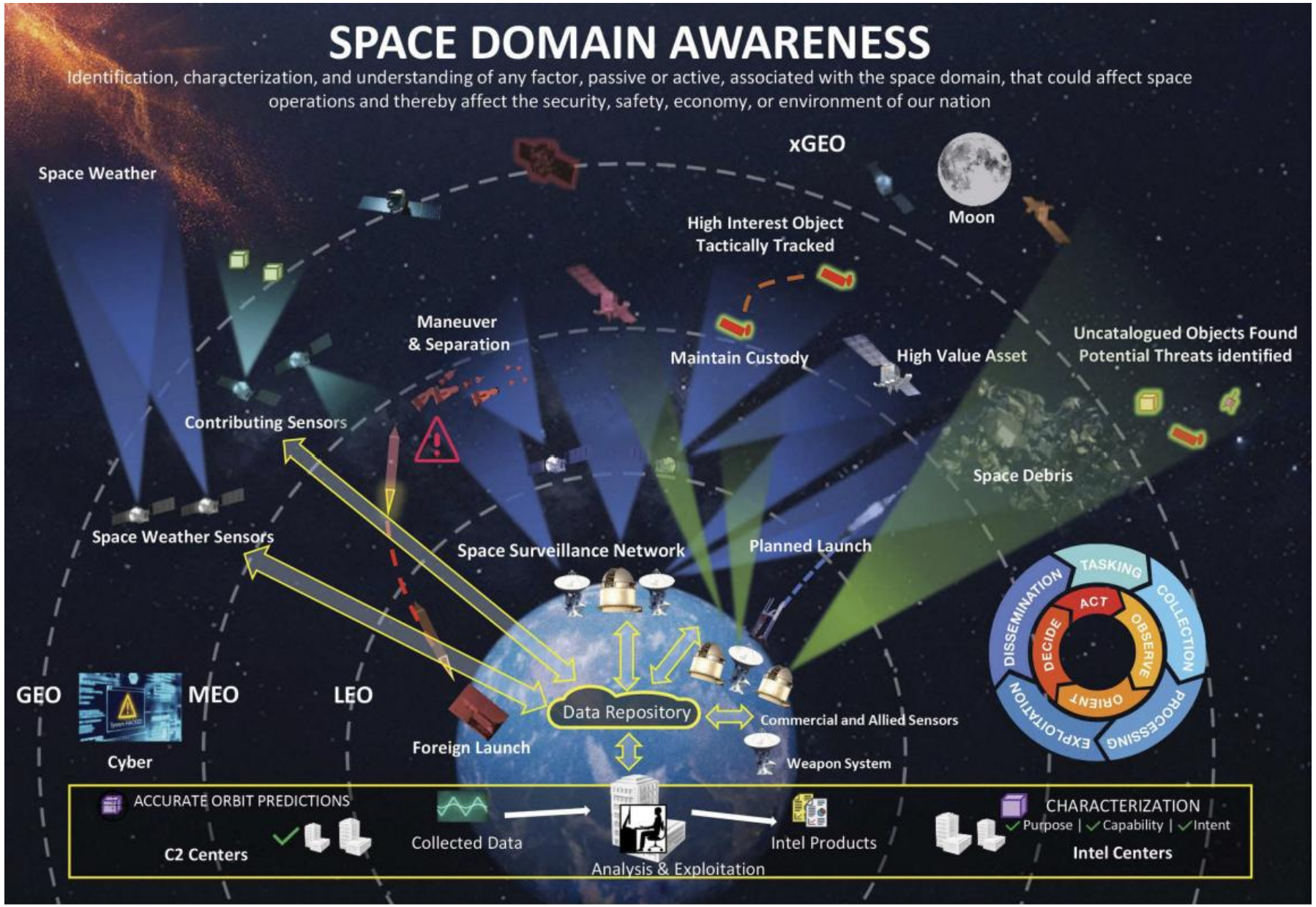
Headlines:

1) Introduction – Space Situational Awareness
2) Motivation – Accidents and Incidents with space objects
3) STAMP-STPA Results
4) Recommendations for Autonomous Collision Avoidance Systems
5) Applicability of the Results
6) Conclusions

Space Situational Awareness (SSA)

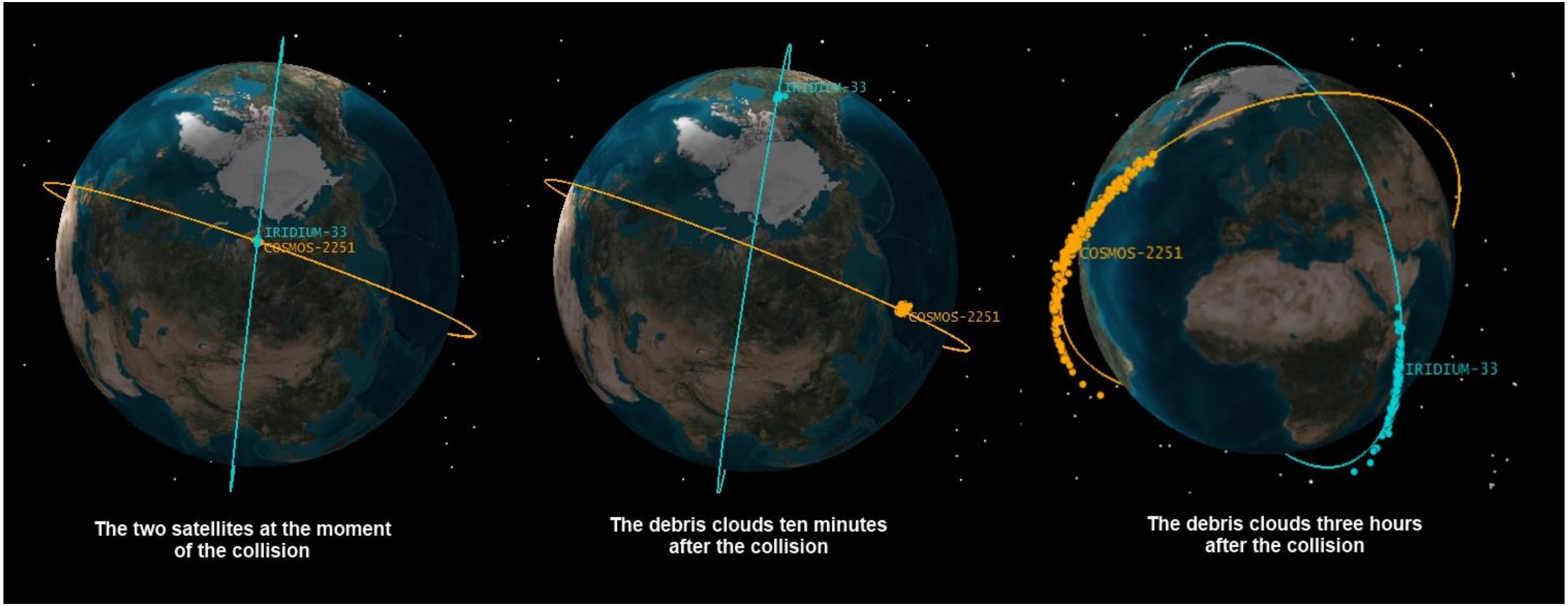


Source:
DARPA / US DoD



Source:
[COMSPOC]

Motivation – Incidents / Accidents

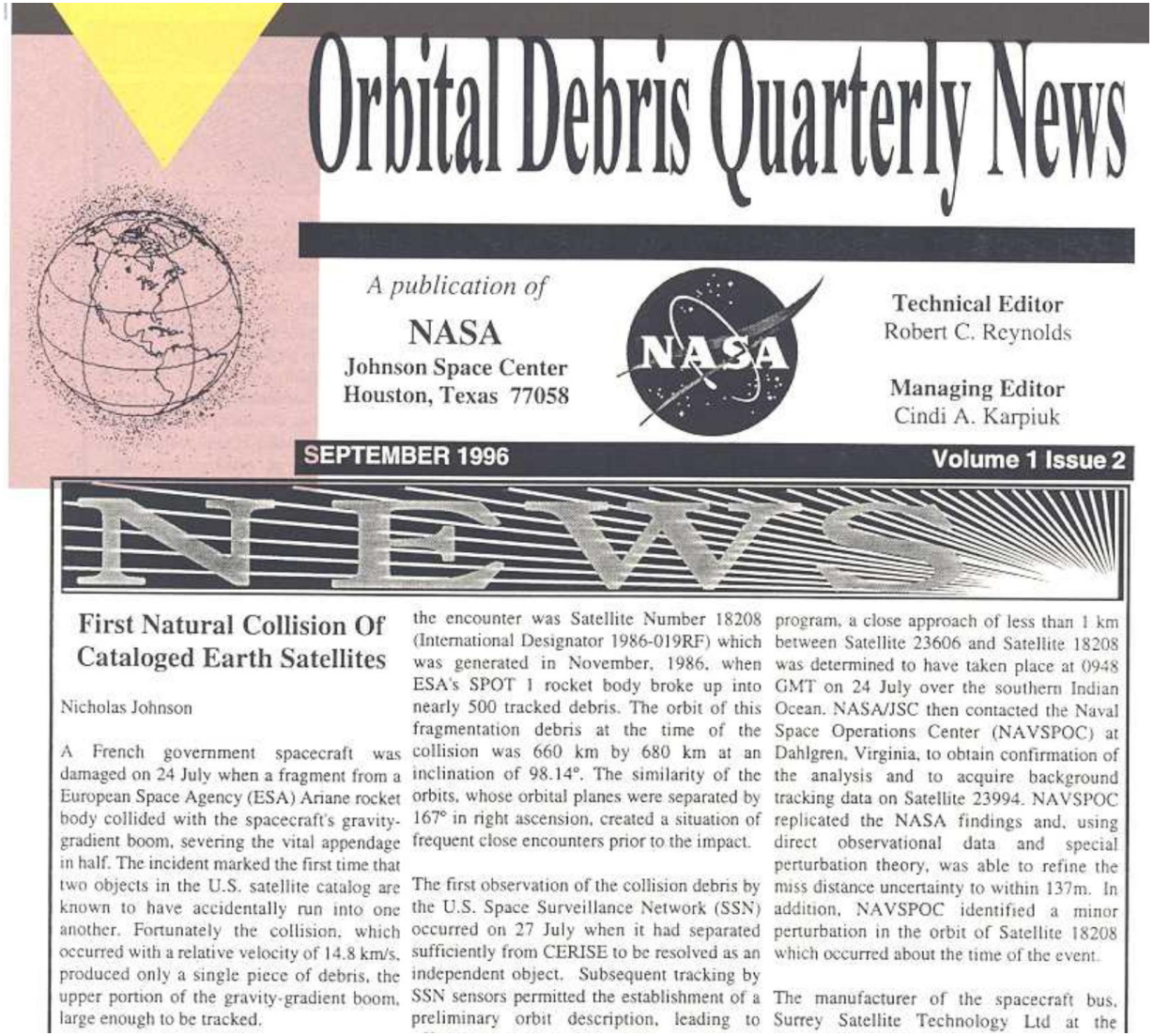


Iridium-33 vs. Cosmos-2251 collision — 10 Feb 2009

Active Iridium-33 collided with defunct Cosmos-2251 at 11.7 km/s. Both destroyed, generating over 2,000 trackable fragments, the first-ever satellite–satellite collision.

Source:
Secure World Foundation
Fact Sheet

Motivation – Incidents / Accidents



Orbital Debris Quarterly News

A publication of
NASA
Johnson Space Center
Houston, Texas 77058

Technical Editor
Robert C. Reynolds

Managing Editor
Cindi A. Karpiuk

SEPTEMBER 1996 Volume 1 Issue 2

NEWS

First Natural Collision Of Cataloged Earth Satellites

Nicholas Johnson

A French government spacecraft was damaged on 24 July when a fragment from a European Space Agency (ESA) Ariane rocket body collided with the spacecraft's gravity-gradient boom, severing the vital appendage in half. The incident marked the first time that two objects in the U.S. satellite catalog are known to have accidentally run into one another. Fortunately the collision, which occurred with a relative velocity of 14.8 km/s, produced only a single piece of debris, the upper portion of the gravity-gradient boom, large enough to be tracked.

the encounter was Satellite Number 18208 (International Designator 1986-019RF) which was generated in November, 1986, when ESA's SPOT 1 rocket body broke up into nearly 500 tracked debris. The orbit of this fragmentation debris at the time of the collision was 660 km by 680 km at an inclination of 98.14°. The similarity of the orbits, whose orbital planes were separated by 167° in right ascension, created a situation of frequent close encounters prior to the impact.

The first observation of the collision debris by the U.S. Space Surveillance Network (SSN) occurred on 27 July when it had separated sufficiently from CERISE to be resolved as an independent object. Subsequent tracking by SSN sensors permitted the establishment of a preliminary orbit description, leading to

program, a close approach of less than 1 km between Satellite 23606 and Satellite 18208 was determined to have taken place at 0948 GMT on 24 July over the southern Indian Ocean. NASA/JSC then contacted the Naval Space Operations Center (NAVSPOC) at Dahlgren, Virginia, to obtain confirmation of the analysis and to acquire background tracking data on Satellite 23994. NAVSPOC replicated the NASA findings and, using direct observational data and special perturbation theory, was able to refine the miss distance uncertainty to within 137m. In addition, NAVSPOC identified a minor perturbation in the orbit of Satellite 18208 which occurred about the time of the event.

The manufacturer of the spacecraft bus, Surrey Satellite Technology Ltd at the

CERISE collision — 24 Jul 1996

French CERISE satellite was struck by debris from an exploded Ariane H-10 upper stage, severing its stabilization boom. First confirmed case of cataloged debris hitting an operational satellite.

Source:
NASA
Orbital Debris Quarterly News

Motivation – Incidents / Accidents

NASA DART–MUBLCOM mishap — Apr 2005
NASA's DART autonomous spacecraft made unintended contact with MUBLCOM during a proximity demo due to navigation/software faults. The mission was ended prematurely.

Luch/Olymp-K proximity to Intelsat — Apr–Sep 2015
Russian satellite Luch (Olymp-K) repeatedly maneuvered close to commercial Intelsat satellites in GEO without coordination, raising concerns over proximity operations.

Sentinel-1A debris strike — Aug 2016
ESA's Sentinel-1A was hit on its solar array by a millimeter-sized particle, likely small debris or a meteoroid, causing a brief anomaly. First imaged strike of its kind.

ESA Aeolus vs. Starlink-44 near miss — Sep 2019
ESA maneuvered Aeolus to avoid a conjunction with Starlink-44 after coordination with SpaceX failed due to a paging issue. Demonstrated STM protocol gaps.

IRAS vs. GGSE-4 close pass — Jan 2020
Two derelict satellites (IRAS and GGSE-4) passed within ~47 m at 14.7 km/s. No collision occurred, but the event underscored catastrophic risks from dead satellites.

ISS debris avoidance maneuver — Sep 2020
The ISS conducted a reboost to avoid a conjunction with an unidentified object. Crew sheltered in Soyuz vehicles as precaution. Showed late-warning risks for human spaceflight.

Tiangong vs. Starlink near misses — Jul & Oct 2021
China reported two avoidance maneuvers by its Tiangong space station to prevent close approaches with Starlink satellites, filing an official complaint to the UN.

Chinese satellite near miss (~30 m) — May 2023
Chinese satellite came within ~30 m of a defunct Russian satellite. Extremely close approach, highlighting unmanaged collision risks.

Inoperative Russian satellite collision — Sep 2023
inactive Russian satellite collided with orbital debris, causing fragmentation. Example of ongoing vulnerability of debris spacecraft.

RESURS-P1 breakup — Jun 2024
Debris Russian satellite RESURS-P1 fragmented in orbit, creating hundreds of debris pieces. The ISS crew sheltered as a safety measure.

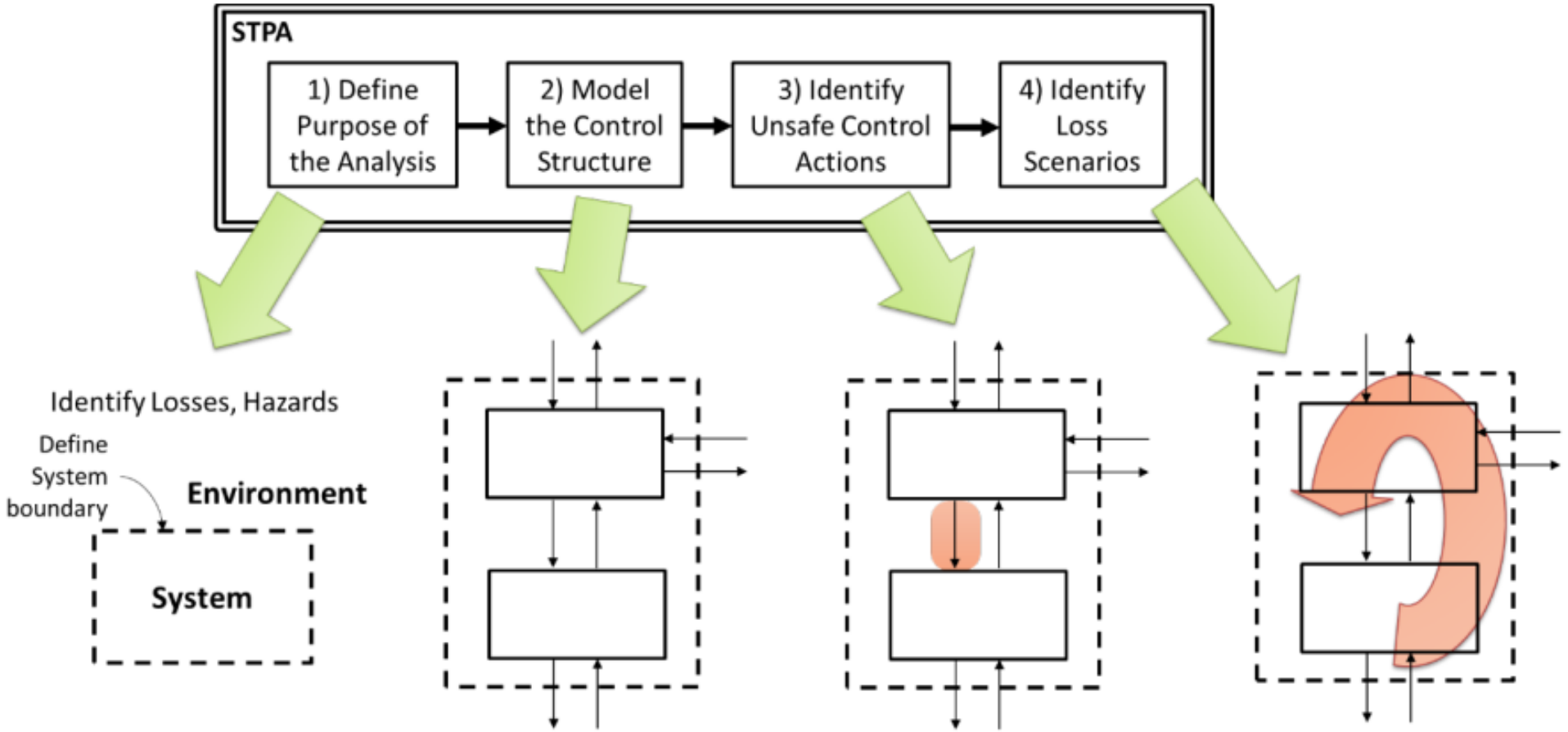
Motivation – Incidents / Accidents

ESA Space Environment Report 2025

- Increase in conjunction alerts and CAMs, especially in LEO.
- Growth of large constellations and debris from past collisions/fragmentations.
- Some operators receive hundreds of alerts daily, highlighting congestion.
- Lack of a centralized STM framework.

System-Theoretic Process Analysis (STPA)

In this study, were performed the procedures described in the [MIT STPA-Handbook]



STPA applied to Autonomous Collision Avoidance Systems

Identification of Losses (L)

L-1: Loss of life or injury to people

- Harm to operators in space due to collisions involving crewed spacecraft or human-occupied infrastructure.

L-2: Loss or damage to the analyzed spacecraft or mission

- Includes destruction, functional impairment, or the inability of the spacecraft to complete its intended mission (e.g., communication, research, observation).

L-3: Loss of or damage to other orbital assets or to the orbital environment

- Harm to third-party satellites, spacecraft, or orbital infrastructure caused by the actions or inactions of the analyzed spacecraft, including collisions.
- Creation of space debris or disruption to the sustainability of orbital operations, increasing risks for future missions.

L-4: Loss of reputation or financial impact for stakeholders

- Stakeholders, such as tracking networks, data providers, space traffic coordinators, spacecraft operators, and manufacturers, may face reputational harm or financial losses due to an incident involving the spacecraft, affecting trust, credibility, and opportunities for future collaborations or missions.

Main system-level Hazards

Identification of system-level Hazards (H)

H-1: The spacecraft is in a trajectory that violates safe separation limits. [L-1], [L-2], [L-3], [L-4]

H-2: The spacecraft's position and trajectory data are inaccurately assessed. [L-1], [L-2], [L-3], [L-4]

H-3: The spacecraft deviates from its assigned orbital space or boundaries. [L-2], [L-3], [L-4]

H-4: The spacecraft's maneuver plans create conditions that compromise mission objectives or lead to other conjunction risks. [L-1], [L-2], [L-3], [L-4]

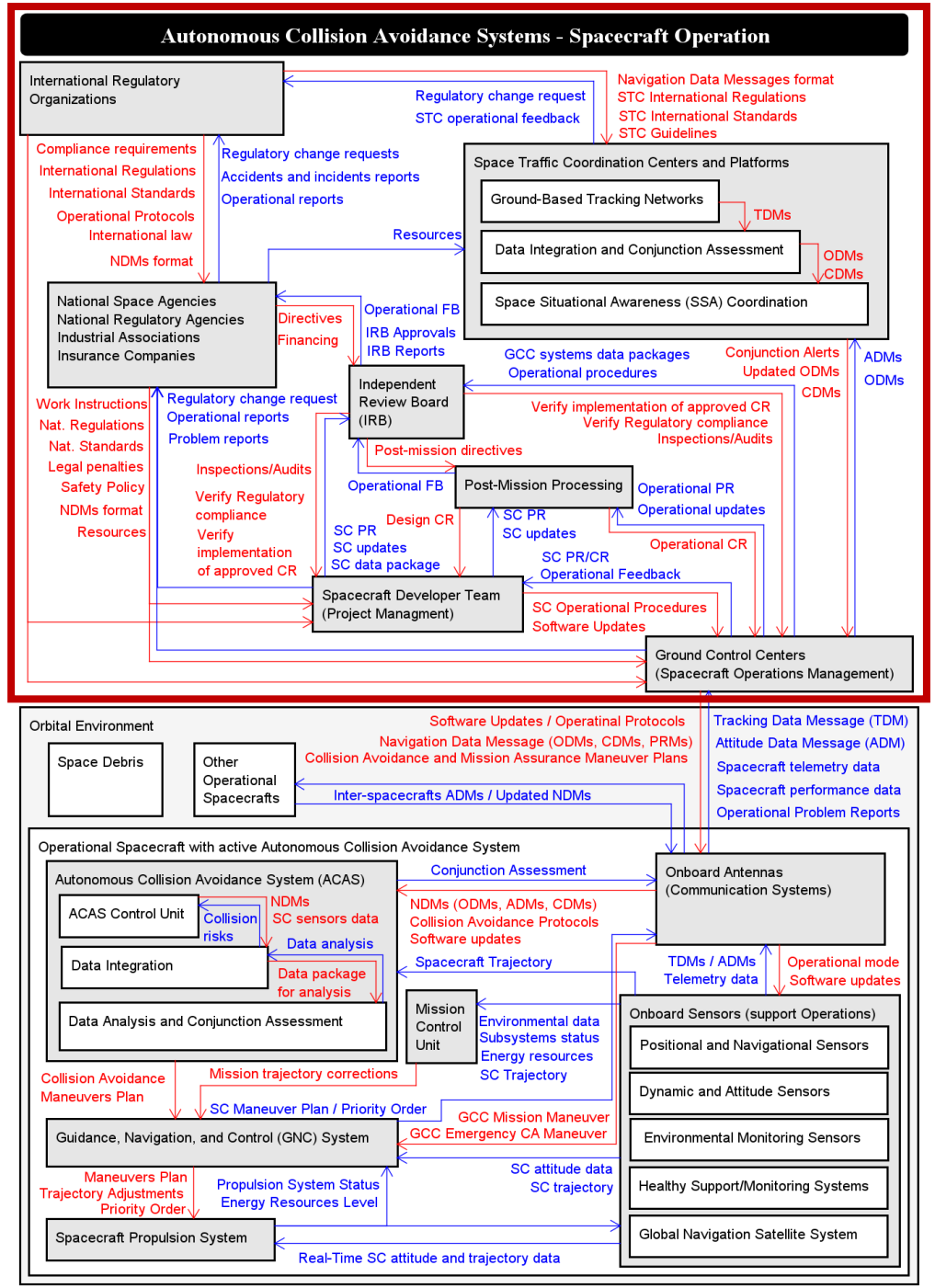
H-5: Propulsion fuel or energy reserves are consumed above operational limits. [L-2], [L-4]

H-6: Communications with ground control or other operators are interrupted, degraded, conflicting, or unresponsive. [L-1], [L-2], [L-3], [L-4]

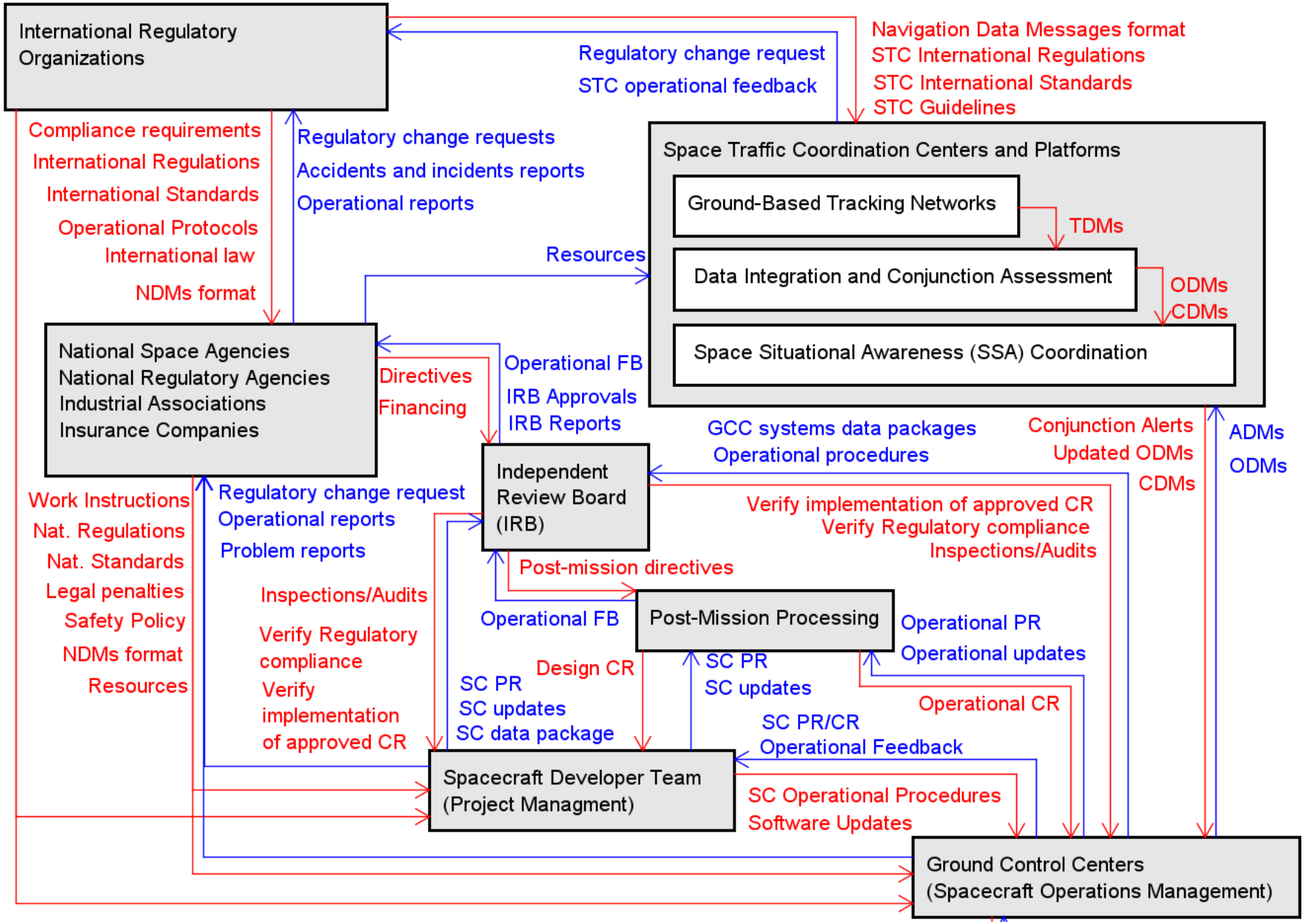
Refined Hazards and Safety Constraints

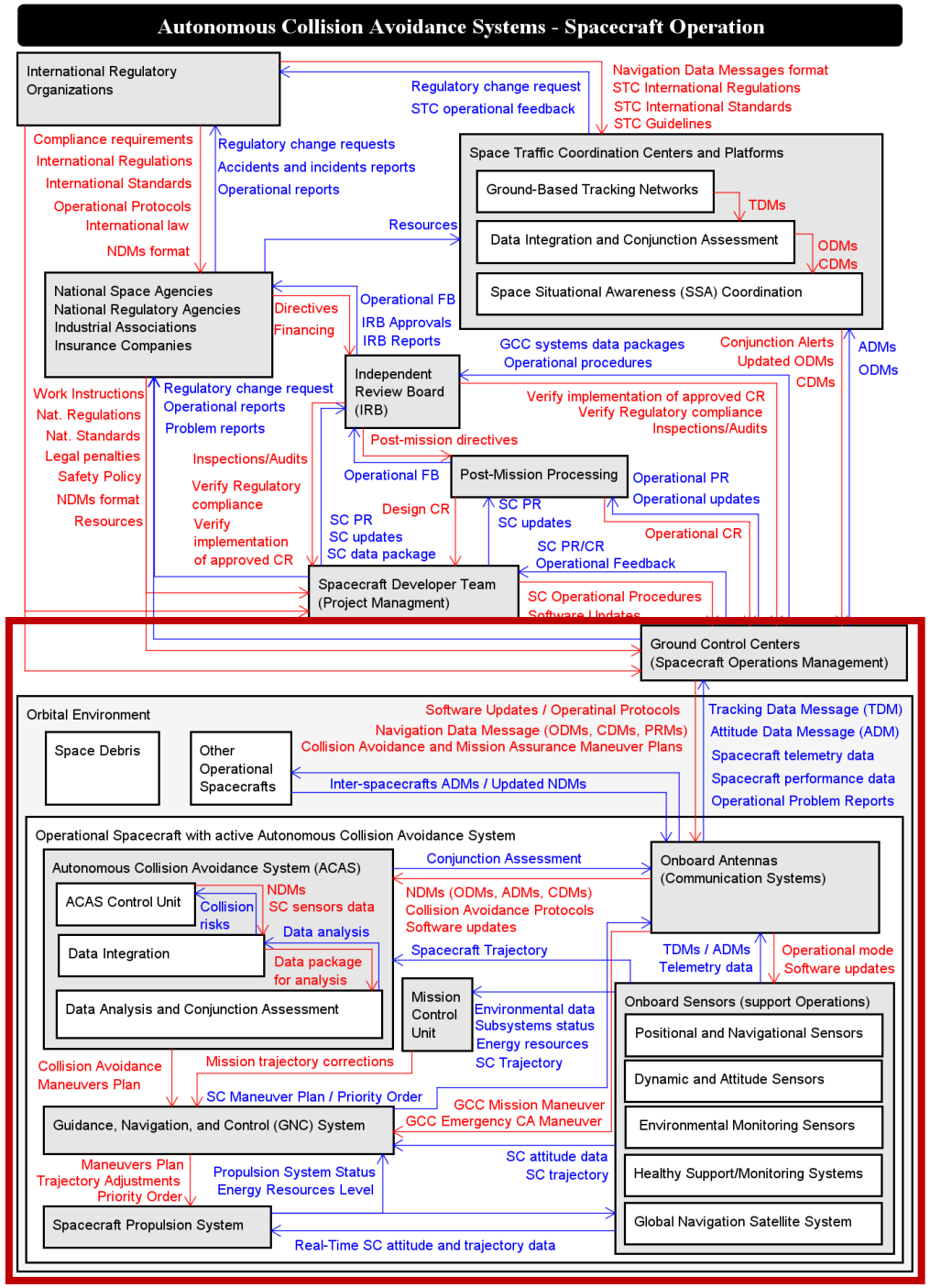
Identification of 79 Refined Hazards and 189 Safety Constraints

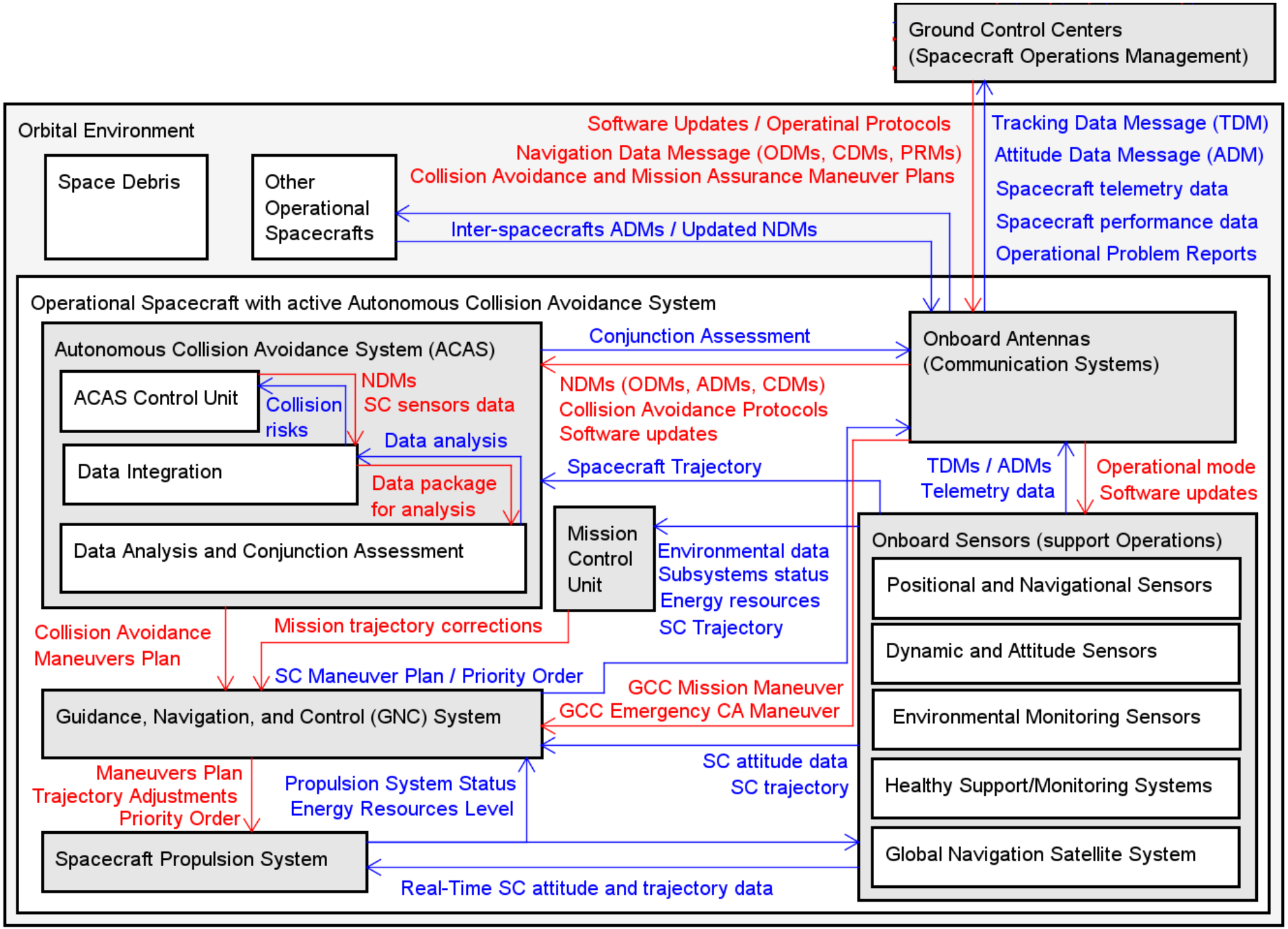
Hazard	Refined Hazards	System-Level Safety Constraints
[H-4]	**H-4.2: Maneuvers conflict with mission objectives.** [L-2], [L-4]	**SC-4.2.1:** Collision avoidance maneuver planning must align with predefined mission objectives and constraints. [H-4.2] **SC-4.2.2:** Collision Avoidance Systems must verify that proposed maneuvers do not violate mission-critical parameters. [H-4.2, H-4.9] **SC-4.2.3:** The spacecraft must assess and document any deviations from mission objectives due to collision avoidance priorities. [H-4.2, H-4.9] **SC-4.2.4:** Collision avoidance maneuvers must have priority over mission plans. [H-4.2, H-4.9]
	H-4.3: Maneuvers create conjunction risks with other objects. [L-1], [L-2], [L-3], [L-4]	**SC-4.3.1:** All maneuver plans must account for potential conjunction risks with nearby orbital objects. [H-4.3, H-4.7] **SC-4.3.2:** Collision Avoidance Systems must include secundary collision risk analysis as part of maneuver planning protocols. [H-4.3, H-4.9] **SC-4.3.3:** Collision Avoidance Systems must include post-maneuver analysis to evaluate residual conjunction risks and adjust trajectories if needed. [H-4.3, H-4.7] **SC-4.3.4:** Trajectory planning must consider an increased safety margins when involving crewed spacecraft or human-habited systems. [H-4.3]


Autonomous Collision Avoidance Systems - Spacecraft Operation
International Regulatory Organizations
Regulatory change request
STC operational feedback
Navigation Data Messages format
STC International Regulations
STC International Standards
STC Guidelines
Compliance requirements
International Regulations
International Standards
Operational Protocols
International law
NDMs format
Regulatory change requests
Accidents and incidents reports
Operational reports
Space Traffic Coordination Centers and Platforms
Ground-Based Tracking Networks
TDMs
Data Integration and Conjunction Assessment
ODMs
CDMs
Space Situational Awareness (SSA) Coordination
Resources
National Space Agencies
National Regulatory Agencies
Industrial Associations
Insurance Companies
Directives
Financing
Operational FB
IRB Approvals
IRB Reports
GCC systems data packages
Operational procedures
Conjunction Alerts
Updated ODMs
CDMs
ADMs
ODMs
Independent Review Board (IRB)
Work Instructions
Nat. Regulations
Nat. Standards
Legal penalties
Safety Policy
NDMs format
Resources
Regulatory change request
Operational reports
Problem reports
Verify implementation of approved CR
Verify Regulatory compliance
Inspections/Audits
Post-mission directives
Inspections/Audits
Verify Regulatory compliance
Verify implementation of approved CR
Operational FB
Post-Mission Processing
Operational PR
Operational updates
Design CR
SC PR
SC updates
SC data package
SC PR
SC updates
Operational CR
SC PR/CR
Operational Feedback
Spacecraft Developer Team (Project Managment)
SC Operational Procedures
Software Updates
Ground Control Centers (Spacecraft Operations Management)
Orbital Environment
Space Debris
Other Operational Spacecrafts
Software Updates / Operatinal Protocols
Navigation Data Message (ODMs, CDMs, PRMs)
Collision Avoidance and Mission Assurance Maneuver Plans
Inter-spacecrafts ADMs / Updated NDMs
Tracking Data Message (TDM)
Attitude Data Message (ADM)
Spacecraft telemetry data
Spacecraft performance data
Operational Problem Reports
Operational Spacecraft with active Autonomous Collision Avoidance System
Autonomous Collision Avoidance System (ACAS)
ACAS Control Unit
Collision risks
NDMs
SC sensors data
Data analysis
Data Integration
Data package for analysis
Data Analysis and Conjunction Assessment
Conjunction Assessment
NDMs (ODMs, ADMs, CDMs)
Collision Avoidance Protocols
Software updates
Onboard Antennas (Communication Systems)
Spacecraft Trajectory
TDMs / ADMs
Telemetry data
Operational mode
Software updates
Mission Control Unit
Environmental data
Subsystems status
Energy resources
SC Trajectory
Onboard Sensors (support Operations)
Positional and Navigational Sensors
Dynamic and Attitude Sensors
Environmental Monitoring Sensors
Healthy Support/Monitoring Systems
Global Navigation Satellite System
Collision Avoidance Maneuvers Plan
Mission trajectory corrections
SC Maneuver Plan / Priority Order
GCC Mission Maneuver
GCC Emergency CA Maneuver
Guidance, Navigation, and Control (GNC) System
SC attitude data
SC trajectory
Maneuvers Plan
Trajectory Adjustments
Priority Order
Propulsion System Status
Energy Resources Level
Spacecraft Propulsion System
Real-Time SC attitude and trajectory data

Autonomous Collision Avoidance Systems - Spacecraft Operation




Autonomous Collision Avoidance Systems - Spacecraft Operation
International Regulatory Organizations
Regulatory change request
STC operational feedback
Navigation Data Messages format
STC International Regulations
STC International Standards
STC Guidelines
Compliance requirements
International Regulations
International Standards
Operational Protocols
International law
NDMs format
Regulatory change requests
Accidents and incidents reports
Operational reports
Space Traffic Coordination Centers and Platforms
Ground-Based Tracking Networks
TDMs
Data Integration and Conjunction Assessment
ODMs
CDMs
Space Situational Awareness (SSA) Coordination
Resources
National Space Agencies
National Regulatory Agencies
Industrial Associations
Insurance Companies
Directives
Financing
Operational FB
IRB Approvals
IRB Reports
GCC systems data packages
Operational procedures
Conjunction Alerts
Updated ODMs
CDMs
ADMs
ODMs
Independent Review Board (IRB)
Work Instructions
Nat. Regulations
Nat. Standards
Legal penalties
Safety Policy
NDMs format
Resources
Regulatory change request
Operational reports
Problem reports
Verify implementation of approved CR
Verify Regulatory compliance
Inspections/Audits
Post-mission directives
Inspections/Audits
Verify Regulatory compliance
Verify implementation of approved CR
Operational FB
Post-Mission Processing
Operational PR
Operational updates
Design CR
SC PR
SC updates
SC data package
SC PR
SC updates
Operational CR
SC PR/CR
Operational Feedback
Spacecraft Developer Team (Project Managment)
SC Operational Procedures
Software Updates
Ground Control Centers (Spacecraft Operations Management)
Orbital Environment
Space Debris
Other Operational Spacecrafts
Software Updates / Operatinal Protocols
Navigation Data Message (ODMs, CDMs, PRMs)
Collision Avoidance and Mission Assurance Maneuver Plans
Inter-spacecrafts ADMs / Updated NDMs
Tracking Data Message (TDM)
Attitude Data Message (ADM)
Spacecraft telemetry data
Spacecraft performance data
Operational Problem Reports
Operational Spacecraft with active Autonomous Collision Avoidance System
Autonomous Collision Avoidance System (ACAS)
ACAS Control Unit
Collision risks
NDMs
SC sensors data
Data analysis
Data Integration
Data package for analysis
Data Analysis and Conjunction Assessment
Conjunction Assessment
NDMs (ODMs, ADMs, CDMs)
Collision Avoidance Protocols
Software updates
Onboard Antennas (Communication Systems)
Spacecraft Trajectory
TDMs / ADMs
Telemetry data
Operational mode
Software updates
Mission Control Unit
Environmental data
Subsystems status
Energy resources
SC Trajectory
Onboard Sensors (support Operations)
Positional and Navigational Sensors
Dynamic and Attitude Sensors
Environmental Monitoring Sensors
Healthy Support/Monitoring Systems
Global Navigation Satellite System
Collision Avoidance Maneuvers Plan
Mission trajectory corrections
SC Maneuver Plan / Priority Order
GCC Mission Maneuver
GCC Emergency CA Maneuver
Guidance, Navigation, and Control (GNC) System
SC attitude data
SC trajectory
Maneuvers Plan
Trajectory Adjustments
Priority Order
Propulsion System Status
Energy Resources Level
Spacecraft Propulsion System
Real-Time SC attitude and trajectory data

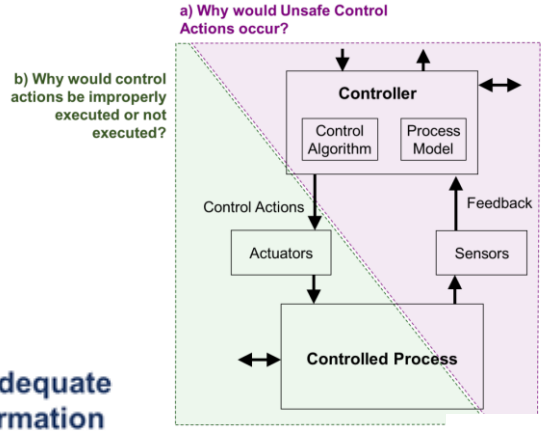

Ground Control Centers
(Spacecraft Operations Management)
Orbital Environment
Space Debris
Other
Operational
Spacecrafts
Software Updates / Operatinal Protocols
Navigation Data Message (ODMs, CDMs, PRMs)
Collision Avoidance and Mission Assurance Maneuver Plans
Inter-spacecrafts ADMs / Updated NDMs
Tracking Data Message (TDM)
Attitude Data Message (ADM)
Spacecraft telemetry data
Spacecraft performance data
Operational Problem Reports
Operational Spacecraft with active Autonomous Collision Avoidance System
Autonomous Collision Avoidance System (ACAS)
ACAS Control Unit
Collision
risks
NDMs
SC sensors data
Data Integration
Data analysis
Data package
for analysis
Data Analysis and Conjunction Assessment
Conjunction Assessment
NDMs (ODMs, ADMs, CDMs)
Collision Avoidance Protocols
Software updates
Onboard Antennas
(Communication Systems)
Spacecraft Trajectory
TDMs / ADMs
Telemetry data
Operational mode
Software updates
Mission
Control
Unit
Environmental data
Subsystems status
Energy resources
SC Trajectory
Onboard Sensors (support Operations)
Positional and Navigational Sensors
Dynamic and Attitude Sensors
Environmental Monitoring Sensors
Healthy Support/Monitoring Systems
Global Navigation Satellite System
Collision Avoidance
Maneuvers Plan
Mission trajectory corrections
SC Maneuver Plan / Priority Order
GCC Mission Maneuver
GCC Emergency CA Maneuver
Guidance, Navigation, and Control (GNC) System
SC attitude data
SC trajectory
Maneuvers Plan
Trajectory Adjustments
Priority Order
Propulsion System Status
Energy Resources Level
Spacecraft Propulsion System
Real-Time SC attitude and trajectory data

11 Control Actions Analyzed - 158 UCAs and SCs

Control Action (by ACAS)	Not Providing Leads to Hazard	Providing Leads to Hazard	Provided Too Soon, Too Late, Out of Order	Stopped Too Soon, Applied Too Long
Generate maneuver plans based on collision analysis.	**UCA-H.01**: ACAS does not generate maneuver plans for critical conjunctions detected in NDMs. [H-1.6, H-6.9]	**UCA-H.05**: ACAS generates maneuver plans using incomplete or inconsistent NDM data. [H-2.3, H-6.4]	**UCA-H.10**: ACAS generates maneuver plans too late for the spacecraft to respond effectively. [H-6.3, H-4.9]	**UCA-H.13**: ACAS stops generating maneuver plans too soon, before or during ongoing maneuvers on dynamic scenarios where other spacecrafts are also maneuvering with active propulsion systems. [H-4.10, H-6.3]

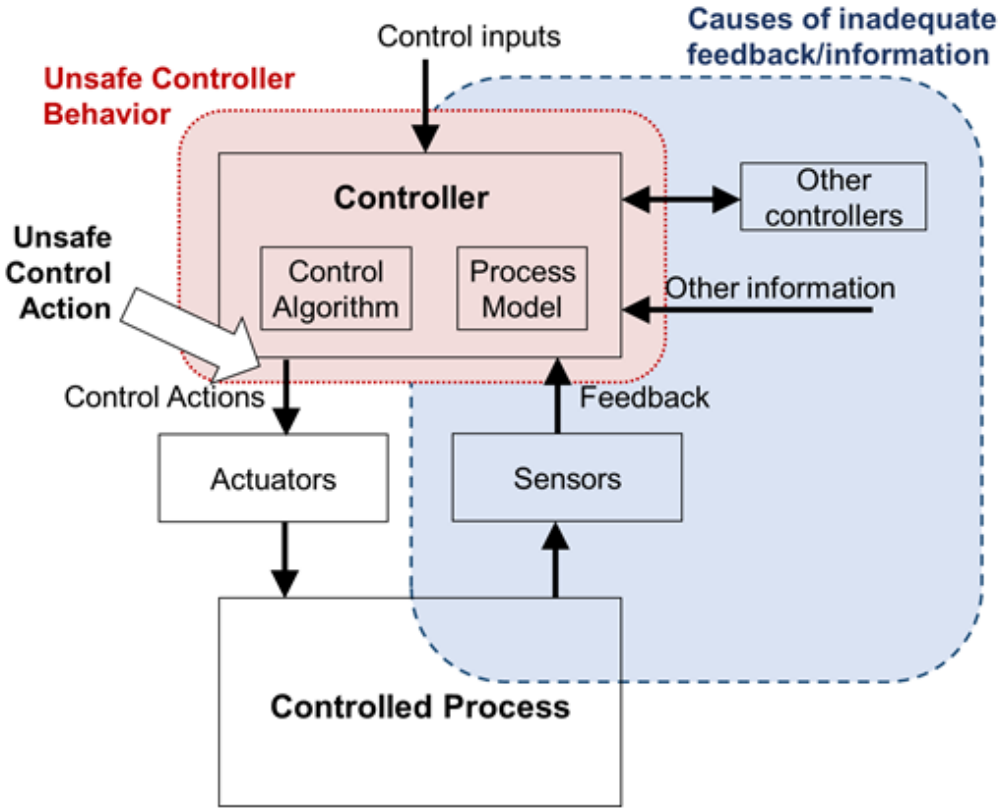
SC-H.01: ACAS must generate maneuver plans for critical conjunctions detected in NDMs.

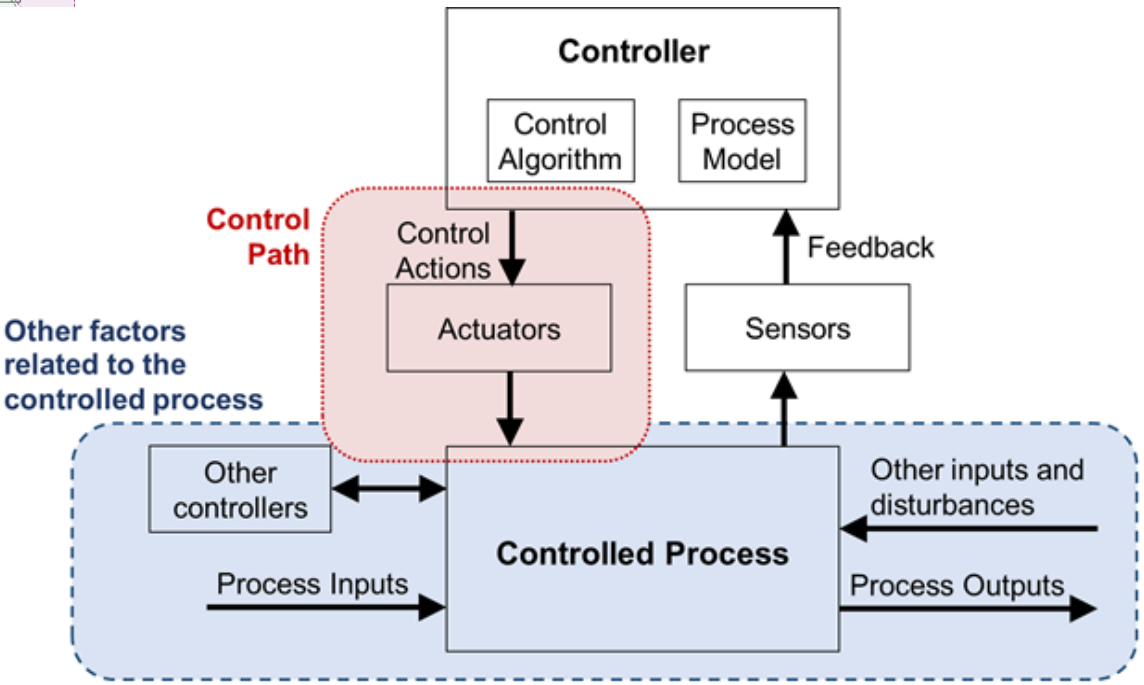
Identifying Loss Scenarios



a) Why would Unsafe Control Actions occur, leading to hazards?

b) Why would control actions be improperly executed or not executed, leading to hazards?





Source:
[STPA Handbook]

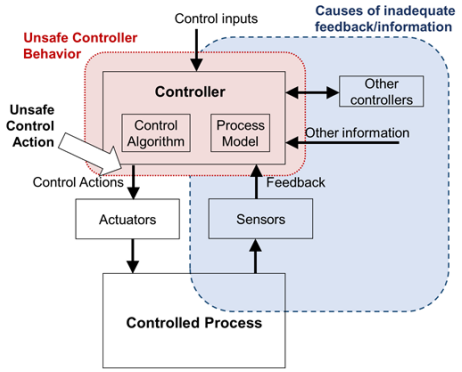
Loss Scenarios – Unsafe Control Actions

a) Why would Unsafe Control Actions occur, leading to hazards?

Suppose the occurrence of **UCA-H.05**:

- What are the causal factors that make the ACAS to generate maneuver plans using incomplete or inconsistent NDM data?

(70 LS identified for the 14 UCA-H's, 05 related with UCA-H.05)



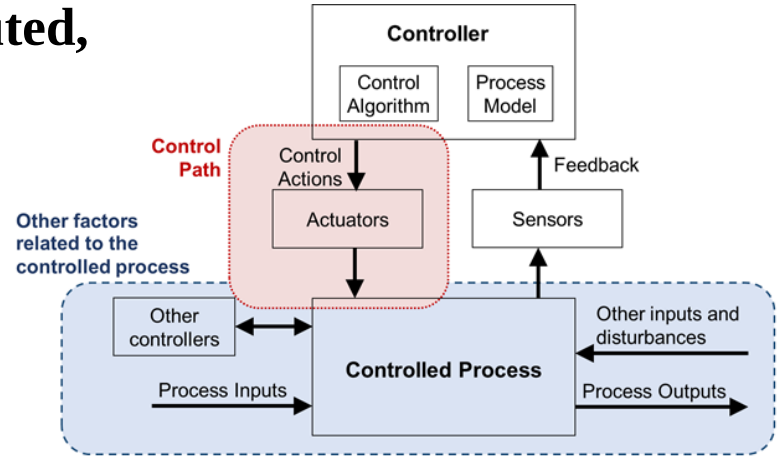
Loss Scenarios	Associated Causal Factors	Rationales
Unsafe Control Input - LS-H.05.03: Ground Centers provide incomplete or inconsistent NDMs, such as CDMs with outdated conjunction details or ODMs with missing trajectory data. This happens due to tracking sensor degradation, data corruption during transmission, or environmental interference. As a result, ACAS generates flawed maneuver plans, compromising orbital safety.	- Sensor degradation or calibration issues affecting NDM accuracy. - Data corruption during transmission from external tracking systems.	- Implement cross-check mechanisms for NDM validation. - Conduct regular calibration of external tracking systems for data accuracy.
Inadequate Process Model - LS-H.05.04: The ACAS process model assumes that incoming NDMs, such as CDMs and ODMs, are complete and consistent without verifying their accuracy. This assumption arises due to inadequate feedback validation mechanisms or delays in receiving telemetry updates. As a result, ACAS generates flawed maneuver plans, increasing collision risks and undermining mission safety.	- Lack of validation mechanisms for incoming NDM data. - Delayed or outdated telemetry updates from external systems.	- Develop automated validation protocols for incoming NDMs. - Verify that telemetry updates are synchronized and cross-checked in real-time.

Loss Scenarios – Execution of Control Actions

ACAS provides maneuver plans to avoid potential collision (07 LS)

b) Why would control actions be improperly executed or not executed, leading to hazards? Examples:

- Execute a maneuver if neither GCC nor ACAS sent it.
- Execute a different maneuver than commanded by GCC or ACAS.
- Do not execute a maneuver commanded by the GCC or ACAS.



Loss Scenarios	Associated Causal Factors	Rationales
Controlled Process – LS-H.CP.07: Ground control overrides the onboard ACAS maneuver plan with commands that do not address the immediate conjunction risks. This occurs due to procedural misalignment between the ground operators' decision-making processes and ACAS-generated recommendations. The spacecraft executes the ground commands, but the maneuver plans are less effective, increasing collision risks and resource inefficiencies.	- Ground command overrides are issued without considering ACAS-generated maneuver plans. - Procedural misalignment between ground operators and onboard systems.	- Synchronize ground operator commands with ACAS-generated maneuver plans during critical scenarios. - Implement safeguards to prioritize ACAS recommendations during high-risk collision events.

Recommendations for Autonomous Collision Avoidance Systems

Once identified the loss scenarios, **it is possible to associate safety recommendations (known as safety constraints in STPA approach, that can also be interpreted as requirements for system behavior) to avoid the occurrence of the identified loss scenarios or even to mitigate their consequences**.

Associated with the STPA results, **this work proposes 135 recommendations divided into 11 topics related** to Autonomous Collision Avoidance Systems, aiming to maintain operational safety and performance.

- **Data Validation and Integrity** — 07 recommendations
- **Communication Resilience** — 09 recommendations
- **Propulsion and Energy Management** — 07 recommendations
- **Space Situational Awareness (SSA) and Space Traffic Coordination (STC)** — 36 recommendations
- **Feedback and Logging Systems** — 08 recommendations
- **Verifications, Standards, and Compliance** — 16 recommendations
- **Human-Machine Interaction, Training, and Operator Readiness** — 06 recommendations
- **Fault Tolerance** — 09 recommendations
- **Implementation of Artificial Intelligence and Machine Learning** — 17 recommendations
- **Security and Cybersecurity Aspects** — 10 recommendations
- **Incident and Accident Response** — 10 recommendations

Recommendations for ACAS – SSA/STC

Recommendations for ACAS Operation	Associated Controllers	Correlation
R.52: The spacecraft should be capable of inhibiting its autonomous collision avoidance system in case a secondary object needs to take responsibility for the avoidance maneuver.	- Spacecraft (CT-06) - ACAS (CT-06.A)	[SC-4.6.1] [SC-4.6.2] [UCA-H.12] [LS-H.08.04]
R.57: In case a propulsive system malfunction or erroneous thrust is detected, external operators involved in the conjunction should be immediately informed (autonomous notification), especially when ACAS has taken responsibility for the avoidance maneuver.	- Spacecraft (CT-06) - ACAS (CT-06.A) - GCC (CT-04) - STCP (CT-03)	[SC-4.4.3] [SC-4.6.3] [SC-3.10.3] [LS-H.CP.04]
R.59: Enable spacecraft to autonomously share updated NDMs (e.g., CDMs, ODMs) received from ground control with other spacecraft that are either part of the same constellation, operated by the same Ground Control Center, or covered by a formal partnership between different operators. This decentralized dissemination reduces data propagation delays, improves localized space situational awareness, and supports coordinated avoidance strategies in congested orbital regions.	- Spacecraft (CT-06) - ACAS (CT-06.A) - GCC (CT-04) - STCP (CT-03) - Spacecraft Developer Team (CT-05)	[SC-4.4.1] [SC-2.0.2] [SC-2.0.6] [SC-4.7.1] [UCA-H.07] [LS-H.CP.03] [CR-04.01]

Recommendations for ACAS - Incident and Accident Response

Recommendations for ACAS Operation	Associated Controllers	STPA Correlation
R.127: Develop incident/accident response guidelines for ground control centers detailing step-by-step procedures to manage loss scenarios, operational anomalies, and system malfunctions.	- SC Operators (CT-04) - Ind. Review Board (CT-08)	[SC-2.0.7] [LS-H.CP.01] [CR-08.01]
R.130: Conduct post-incident investigation analysis on ACAS decision-making processes to identify root causes and improve the operation of Collision Avoidance Systems.	- Ind. Review Board (CT-08) - STCP (CT-03)	[CR-08.01] [H-2.10] [LS-H.05.05]
R.131: Create standardized reporting templates for operators to communicate incident details to relevant authorities promptly.	- SC Operators (CT-04) - Space ADM (CT-02)	[SC-6.9.3] [H-4.11] [CR-06.D.03]
R.134: Regularly simulate incident scenarios involving ACAS to evaluate system resilience and to train operators on best practices for accident/incident response.	- SC Operators (CT-04) - SC Developers (CT-05) - Ind. Review Board (CT-08)	[CR-05.05] [LS-H.08.05] [H-4.9]

Applicability of the results – Accident analysis

Overview / Summary	Causal Factors and Research Correlations	Preventive and Mitigation Measures
ESA Aeolus and Starlink-44 (2019) On 2 Sep 2019, ESA's **Aeolus** executed a unilateral CAM to avoid **Starlink-44** after a paging bug prevented SpaceX acknowledgment.	• Single-channel/email alert missed (**SC-4.4.1, SC-4.4.3**). • Different Pc models across operators caused inconsistent triggers (**SC-2.0.2, UCA-H.05**). • No shared execution window or responsibility protocol (**SC-4.3.1, UCA-H.10**). • No redundancy or fallback if comms failed (**SC-4.9.3, UCA-H.13**).	• Integrating automated notifications with fallback (**R.10**) would have ensured action even if the paging bug silenced one operator. • Harmonizing Pc thresholds with adaptive updates (**R.03**) could have aligned both operators' decision points. • Predefined maneuver responsibility protocols (**R.40**) could have specified who should act, avoiding last-minute unilateral action. • Unified maneuver execution timelines (**R.42**) would have reduced delay and given both parties a deterministic window for action. • Onboard autonomy to act under comms loss (**R.15**) could have secured safe default CAMs without waiting for GCC negotiation. • Reliable or redundant communication systems (**R.09**) could have prevented failures in alert transmission or reception. • Feedback loops for maneuver (**R.61**) could have caught the paging bug earlier and corrected the communication pathway.

Further Analysis

Extend STPA scope: Proceed the analysis for additional UCAs and controllers

Comparative hazard analysis: Contrast STPA results with FTA, FMEA, HAZOP, and others, to validate findings and highlight complementary insights.

Standards and regulations linkage: explore alignment of ACAS safety constraints with evolving frameworks such as ISO 24113, FAA Part 450, and international regulations.

Broader SSA/STC applications: apply STPA methodology to other domains of space situational awareness or space traffic coordination, such as Tracking of space objects, proximity operations, or constellation management.

Apply STPA to other space systems and operations: extend the methodology to space propulsion systems, launch operations, reentry operations, GNCS, spacecraft servicing, on-orbit assembly, and proximity operations.

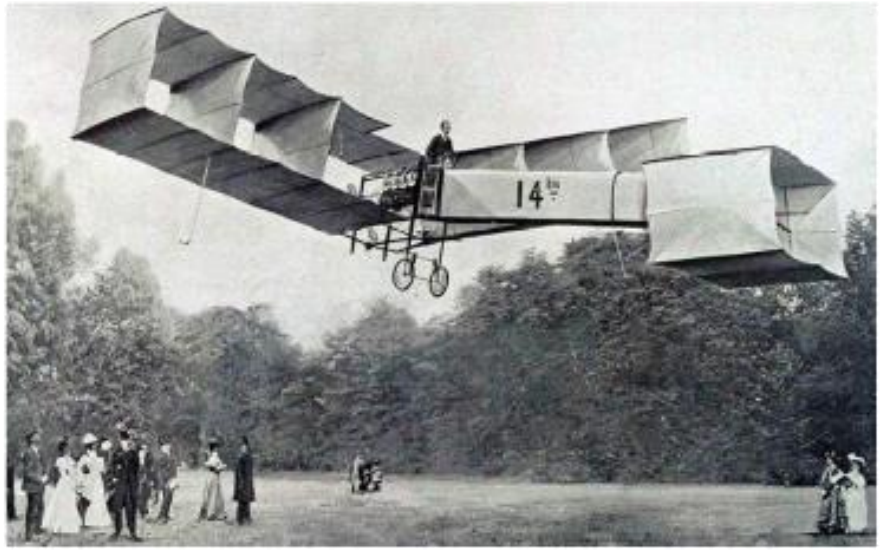
Conclusions

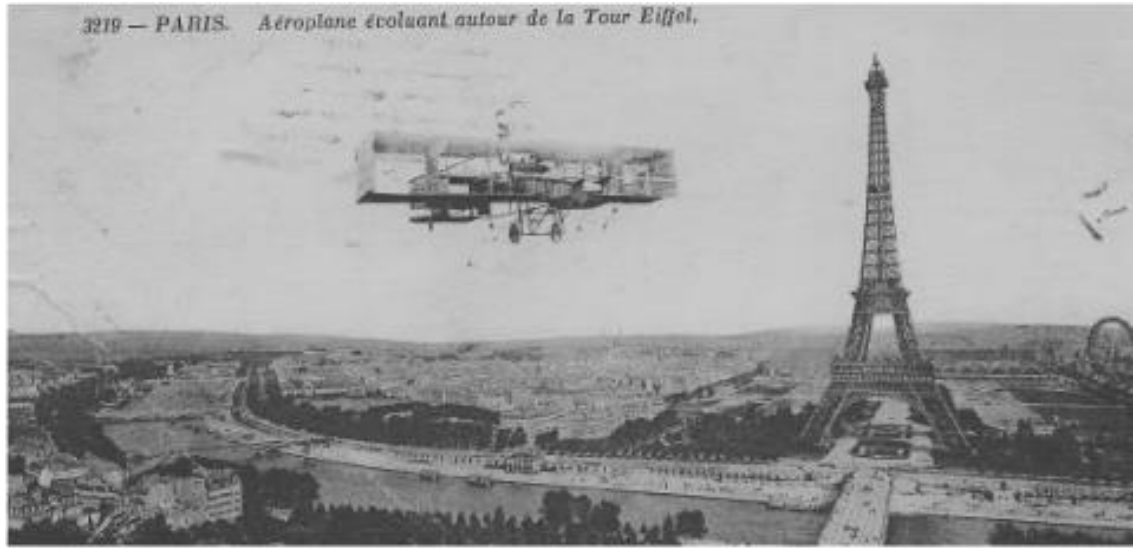
- Identified losses, hazards, UCAs, and loss scenarios, leading to the proposal of SCs and recommendations.
- Confirms the importance of robust communication, accurate data integration, and effective operational coordination.
- Highlighted vulnerabilities from environmental factors, communication delays, and data inaccuracies.
- Considerations included SSA data validation, trajectory planning refinements, verification processes, AI/ML algorithms, accident response, and improved coordination protocols.
- Recommendations intend to support developers, operators, mission planners, SSA coordinators, and regulators in refining designs, operations, and verifications/approvals.

The analysis proposes:

- **188 system-level constraints** (from hazards and subhazards)
- **158 controller safety constraints** (from unsafe control actions)
- **135 recommendations** (correlated with loss scenarios, causal factors, and other STPA results)







"Invent is to imagine what nobody thought; it is to believe what no one has sworn;
it is to risk what no one dared; is to accomplish what no one has tried.
Invent is transcend."

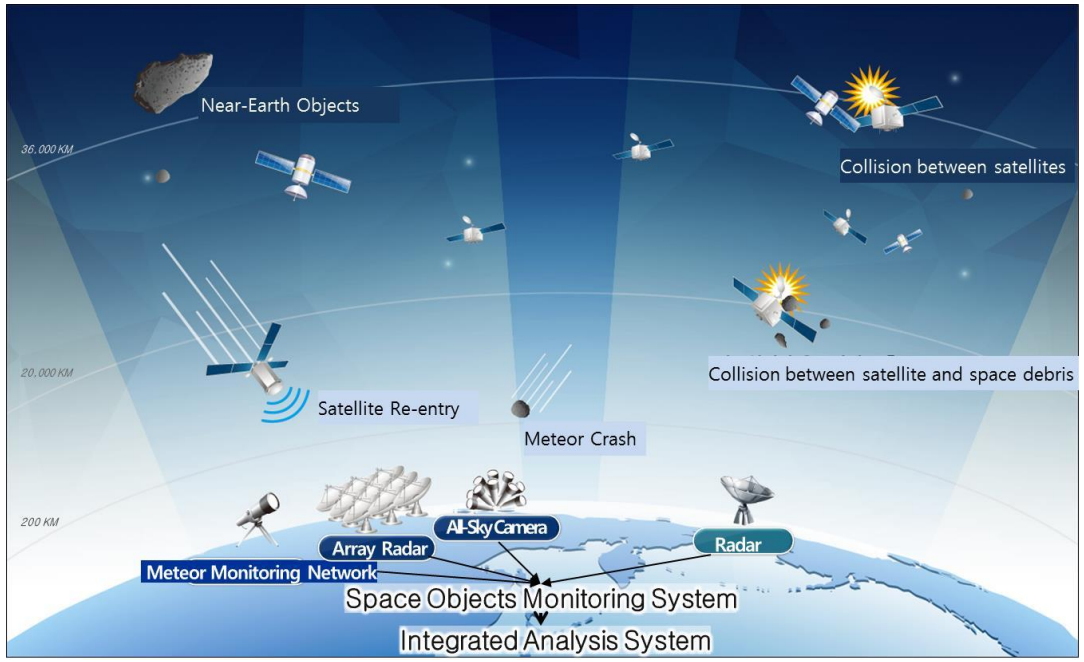
Alberto Santos Dumont

Capt Diniz – dinizavdm@fab.mil.br

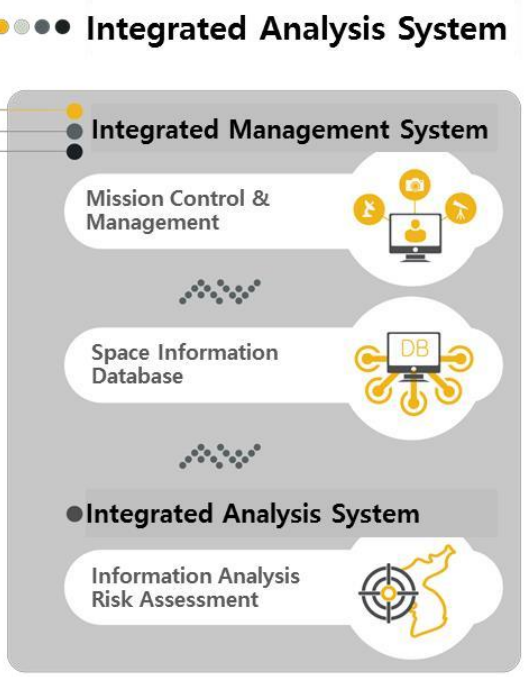
ADDITIONAL SLIDES

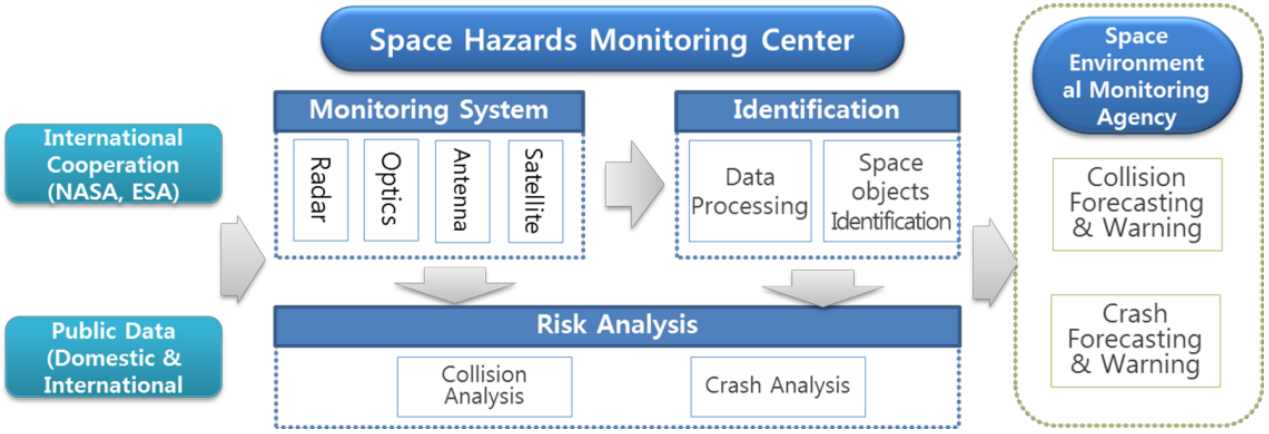
Questions and Answers

Space Traffic Coordination (STC)











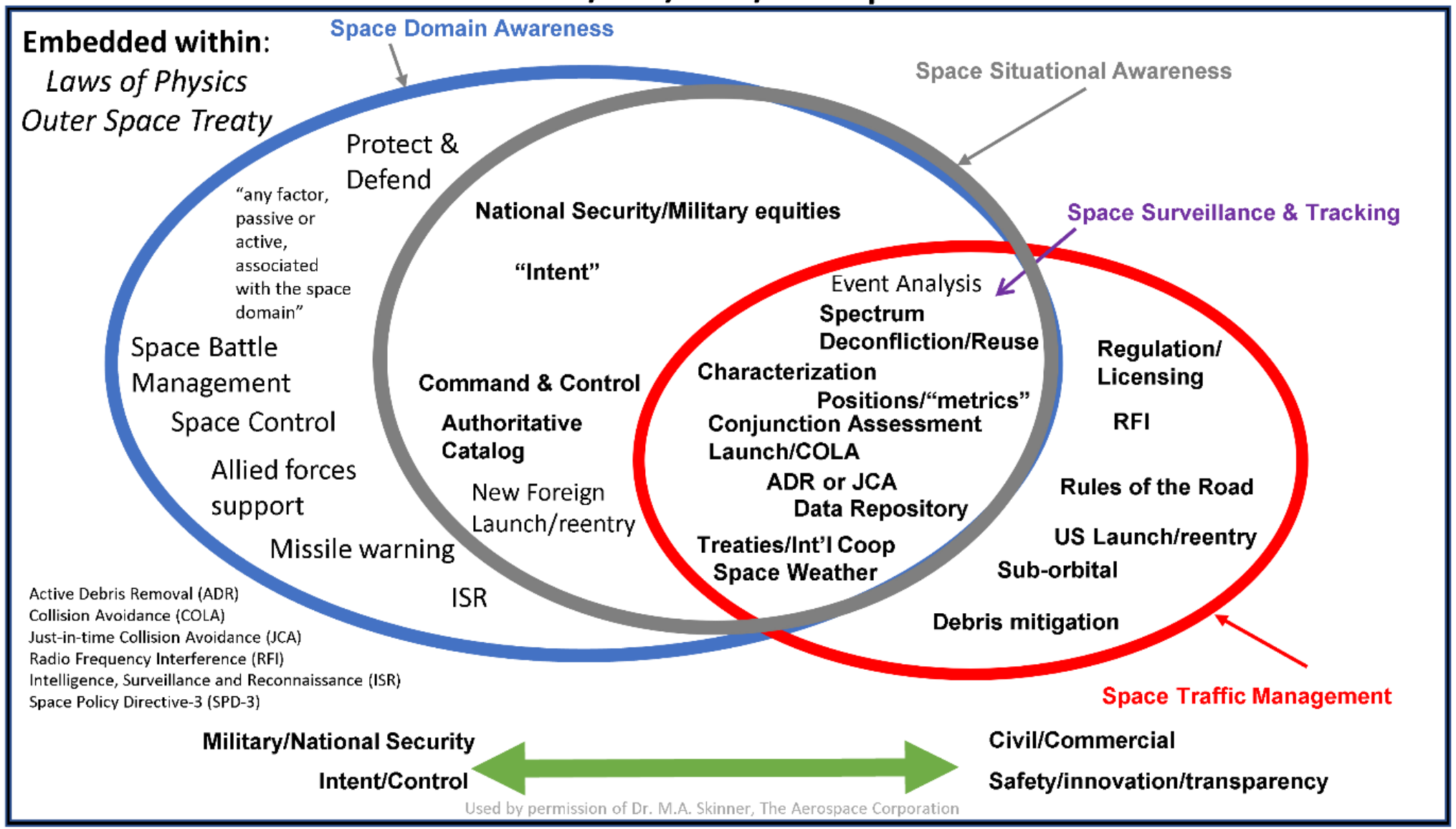


Source:

Space Situational Awareness Center

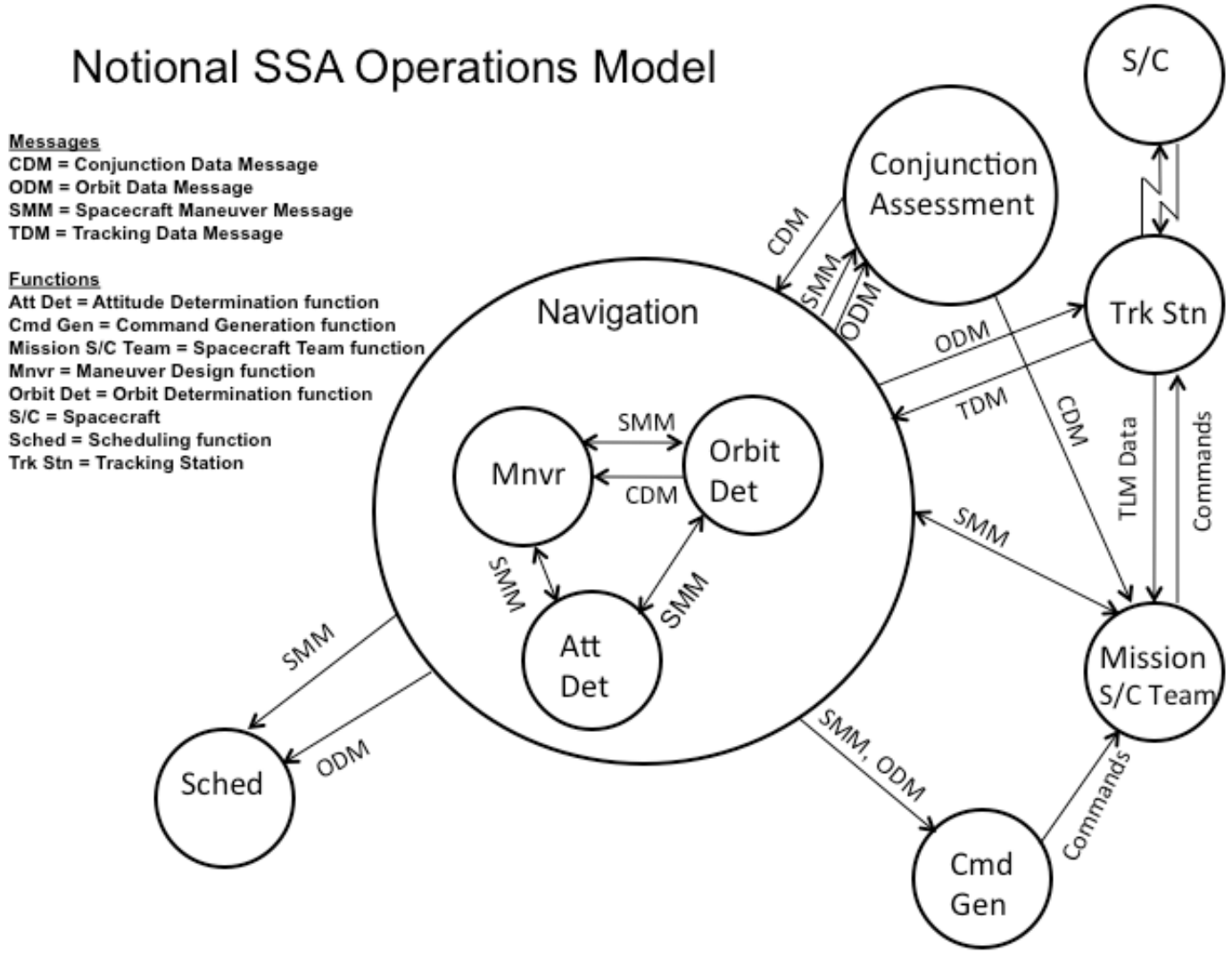
Korea Astronomy and Space Science Institute

SDA/SSA/STM/SST Equities



Source:
ISO CD3 9490
Space Traffic Coordination

CCSDS Data Messages for Space Situational Awareness



Source:

[Jet Propulsion Laboratory AIAA paper]

Motivation – Incidents / Accidents

Incident	Description	Relevance	Root cause / Causal factors	Sources
CERISE (CNES) and Ariane debris 24 Jul 1996	CNES's *CERISE* collided with a cataloged fragment from the SPOT-1 Ariane-1 upper stage, severing part of its stabilization boom.	First well-documented case of a functioning satellite damaged by known orbital debris.	The Ariane-1 upper stage that launched SPOT-1 (1986) had fragmented; one fragment intersected CERISE's orbit a decade later.	NASA Orbital Debris Quarterly News (ODQN) v2-1 (Orbital Debris Program Office) ESA/ESOC conference paper "Collision of CERISE with space debris" (ESA Proceedings Database)
NASA DART–MUBLCOM mishap 15 Apr 2005	NASA's DART autonomous rendezvous demo made unintended contact with MUBLCOM during approach; the mission was terminated.	Cautionary incident for autonomy in proximity ops and collision-avoidance logic.	Onboard navigation/software issues; limited ground intervention.	NASA "Overview of the DART Mishap Investigation Results"
Iridium-33 vs. Cosmos-2251 10 Feb 2009	Operational Iridium-33 collided with non-operational Cosmos-2251 at ~11.7 km/s, destroying both and generating a large debris cloud.	First satellite-satellite collision; major inflection point for STM practices.	No coordinated avoidance action; event occurred without a collision-avoidance maneuver.	NASA Orbital Debris Program Office v13-2 NASA Technical Reports Server "The Collision of Iridium-33 and Cosmos-2251"

Motivation – Incidents / Accidents

Incident	Description	Relevance	Root cause / Causal factors	Sources
ESA Aeolus vs. Starlink-44 02 Sep 2019	ESA maneuvered Aeolus off a predicted conjunction with Starlink-44; no collision occurred.	Exposed fragility of ad-hoc, email-based coordination and lack of binding protocols.	Reliance on manual coordination; absence (then) of standardized inter-operator procedures.	European Space Agency "ESA spacecraft dodges large constellation"
Luch/Olymp-K near Intelsat (GEO) Apr–Sep 2015	Russian Luch/Olymp-K maneuvered close to multiple Intelsat GEO satellites over months.	Signature case of unannounced proximity operations in GEO raising operator safety/coordination concerns.	Lack of transparency; no enforceable proximity-ops norms in GEO.	The Space Review technical history of the 2015 RPO sequence. Aerospace Security - CSIS "Unusual Behavior in GEO: Luch (Olymp-K)"
Sentinel-1A debris/micrometeoroid strike (ESA) 23 Aug 2016	ESA confirmed a millimetre-class particle struck a Sentinel-1A solar array; onboard images showed the mark; operations continued.	Direct, well-documented evidence of small-particle hazard to operational sats.	Likely sub-cm debris or meteoroid below tracking thresholds.	ESA mission note: Copernicus Sentinel-1A satellite hit by space particle. Copernicus/CLS incident report

Motivation – Incidents / Accidents

Incident	Description	Relevance	Root cause / Causal factors	Sources
IRAS vs. GGSE-4 (debris) 29 Jan 2020	Two non-maneuverable debris spacecraft (IRAS & GGSE-4) passed within tens of metres at ~14.7 km/s; no impact observed.	Highlights catastrophic risk from debris encounters where no CAM is possible.	Non-operational spacecraft with no propulsion; no active debris-removal regime or Collision Avoidance capability.	LeoLabs technical narrative (miss-distance estimates & timeline): Medium post. Space
ISS Debris Avoidance Maneuver — 22 Sep 2020	ISS executed a 150-second reboost to avoid a close pass with an unknown object; the crew followed procedures.	Shows real-time operational risk and late-warning challenges for human spaceflight.	Late conjunction warning; degraded debris environment in LEO.	NASA ISS Blog "Station Boosts Orbit to Avoid Space Debris" NASA ISS Blog "Station Crew Preps for Space Debris Avoidance Maneuver"
Tiangong vs. Starlink (China UN filing) 1 Jul & 21 Oct 2021	China reported to the UN two avoidance maneuvers by its space station to prevent close approaches with Starlink satellites.	First formal United Nations notification of conjunction risk with a commercial mega-constellation.	No global STM authority; reliance on operator judgement/notifications.	UNOOSA Note Verbale A/AC.105/1262

Motivation – Incidents / Accidents

Incident	Description	Relevance	Root cause / Causal factors	Sources
Chinese Satellite near-miss with debri Russian satellite May 2023	A Chinese satellite passed within ~30 m of a non-operational Russian satellite - No collision occurred.	Shows how conjunctions between active and defunct satellites can approach collision thresholds; prompted political debate in the UK about debris action.	Absence of coordinated space traffic management; no avoidance maneuver possible on the derelict.	Orbital Today "Space Debris Disaster averted by 30m"
Inoperational Russian satellite collision with debris Sep 2023	An inactive Russian satellite reportedly crashed into orbital debris, causing fragmentation.	Illustrates that even non-operational satellites can suffer catastrophic collisions with debris, contributing to congestion.	Aging inoperative spacecraft left in orbit; no protection against hypervelocity debris impacts.	Orbital Today "NASA Satellite Has Near Miss With Space Debris"
RESURS-P1 breakup (Russia) 27 Jun 2024	Non-operational Russian Earth-observation satellite RESURS-P1 fragmented in orbit, creating hundreds of debris pieces; ISS crew sheltered in Soyuz/Dragon.	Modern example of a large fragmentation event directly impacting human spaceflight operations.	Structural failure of aging satellite (exact cause under investigation).	Reuters "Russian satellite breaks up in space, forces ISS astronauts to shelter" Al Jazeera "ISS astronauts take cover as defunct Russian satellite shatters"

Recommendations for ACAS - Propulsion and Energy Management

Recommendations for ACAS Operation	Associated Controllers	STPA Correlation
R.18: Conduct routine diagnostics and maintenance of propulsion systems to prevent performance degradation or fuel inefficiencies.	- SC Operators (CT-04) - SC Developers (CT-05)	[LS-H.CP.05] [CR-06.B.04]
R.20: Develop and implement fault prediction models for propulsion systems to preemptively address potential failures.	- SC Developers (CT-05) - ACAS (CT-06.A)	[CR-06.B.02] [SC-1.10.3]
R.22: Maintain propulsion emergency reserves for availability during unexpected collision avoidance scenarios.	- SC Developers (CT-05) - ACAS (CT-06.A)	[CR-06.B.02]

Recommendations for ACAS – SSA/STC

Recommendations for ACAS Operation	Associated Controllers	STPA Correlation
R.31: Extend separation thresholds for operations involving crewed spacecraft or human-habited systems to increase safety margins.	- Space ADM (CT-02) - STCP (CT-03) - SC Operators (CT-04)	[LS-H.05.03] [H-4.9]
R.43: Use predictive analytics to model the impact of planned maneuvers on adjacent orbital zones and notify affected operators.	- STCP (CT-03) - ACAS (CT-06.A)	[SC-3.11.1] [SC-4.10.2] [H-2.13]
R.50: Conduct joint exercises with operators to improve response times during high-risk scenarios.	- STCP (CT-03) - SC Operators (CT-04) - Space ADM (CT-02)	[CR-04.01] [LS-H.08.05]
R.51: Develop and implement systems that integrate real-time environmental factors, such as solar activity or atmospheric drag, into conjunction risk assessments.	- STCP (CT-03) - SC Operators (CT-04) - SC Developers (CT-05) - ACAS (CT-06.A)	[SC-4.7.1] [H-2.13]
R.54: The spacecraft should inform the Ground Control Center of the generated maneuver plans and the schedule for execution of the autonomous collision avoidance maneuvers.	- Spacecraft (CT-06) - ACAS (CT-06.A) - GCC (CT-04)	[SC-4.4.3] [CR-06.C.03] [UCA-H.08] [LS-H.08.03]

Applicability of the results – Accident analysis

Overview / Summary	Causal Factors and Research Correlations	Preventive and Mitigation Measures
Iridium-33 and Cosmos-2251 (2009) On 10 Feb 2009, operational **Iridium-33** collided with defunct **Cosmos-2251** at ~11.7 km/s, producing >2,000 fragments. First-ever satellite–satellite collision.	• CDMs available but not trusted due to uncertainty (**SC-2.0.2, SC-2.1.1**) • Divergent probability thresholds prevented timely maneuver (**SC-4.3.1, UCA-H.05, UCA-H.10**). • Unclear responsibility to act, Cosmos inoperative; only Iridium could maneuver (**SC-1.9.1, SC-1.9.2**), Operator duties (**CR-04.04, CR-04.05**). • No standardized coordination workflow (who maneuvers, when) (**SC-4.4.1, SC-4.4.3**).	• A multi-layered validation process for NDM/CDM inputs (**R.01**) could have increased Iridium's confidence in the warnings, prompting a preventive CAM. • Real-time cross-checking of multiple SSA data feeds (**R.02**) could have exposed inconsistencies and supported a maneuver decision. • Automating threshold updates for collision probability (**R.03**) would have avoided mismatched Pc interpretations across operators. • A standardized communication framework for conjunction handling (**R.08, R.42**) could have supported the clarity of maneuver responsibility. • Automated notifications with fallback escalation (**R.10**) could have required Iridium to act as Cosmos was non-operational. • Regular testing of collision-risk models (**R.29**) could have tuned Pc assessments to the dense LEO environment, lowering the decision latency. • Shared platforms (**R.49**) for real-time conjunction analysis • Onboard autonomy for time-critical maneuvers when comms are delayed (**R.97**).