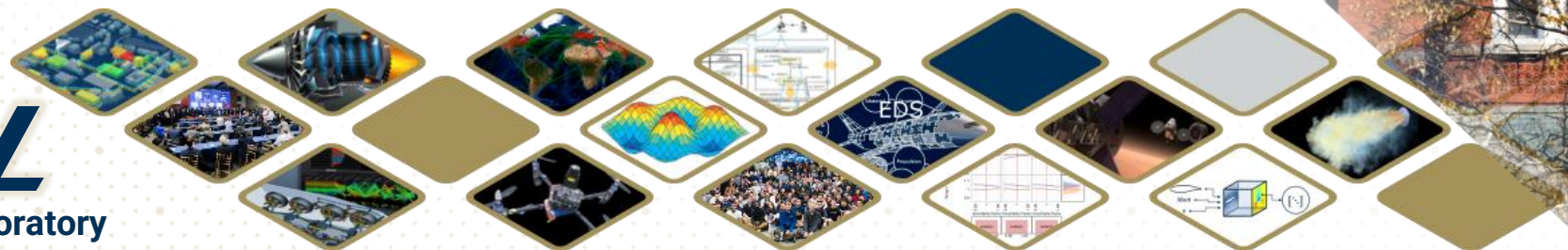
Safety Assessment of Canadarm3

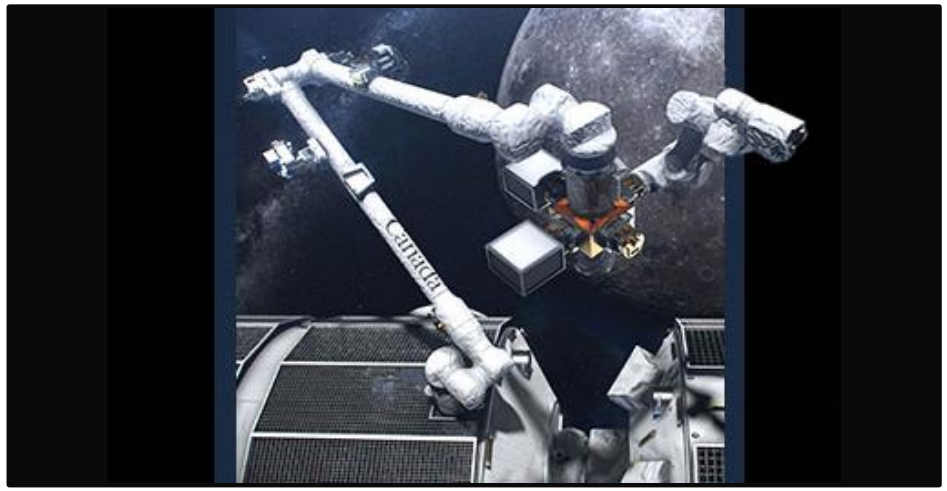
Midterm Review



Aerospace Systems Design Laboratory

Vehicle Overview: Canadarm3

- Robotic arm supporting NASA's Gateway lunar outpost
- Next generation CSA's Canadarm
- Mission:
  - Maintain, repair and inspect the Gateway
  - Catch visiting spacecraft
  - Assist with spacewalks
  - Enable science in lunar orbit



	Canadarm2	Canadarm3
Application	ISS	Lunar Gateway
Range of Motion	No fixed joint, length of ISS	No fixed joint, length of Gateway
Senses	Force-moment sensors; collision avoidance	Force-moment sensors; collision avoidance; 3D vision s ensor tool
Speed	Unloaded: 37cm/s Loaded: 15cm/s	Unloaded: 10cm/s Loaded: TBD
Repairs in Space	Detachable sections for repair	Self-detach sections to be repaired
Control	Controlled by astronaut or ground control	Primarily autonomous with alternative control mode by astronaut or ground control

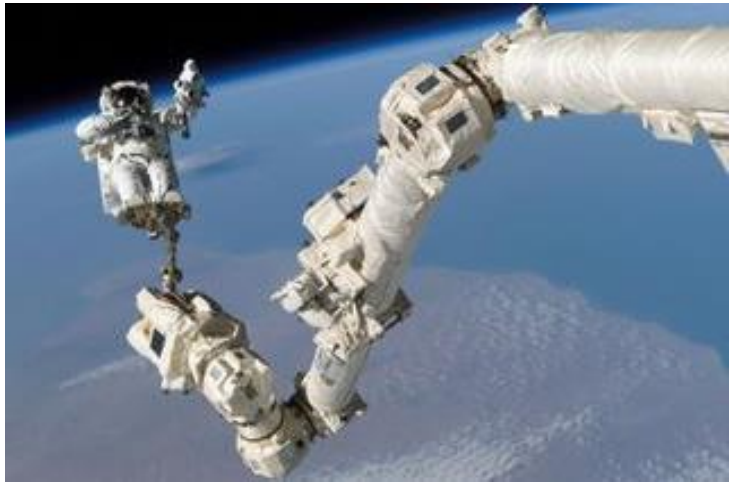
1. Canadarm, Canadarm2, and Canadarm3 – A comparative table | Canadian Space Agency (asc-csa.gc.ca)

Vehicle Mission(s)

Dock Approaching Spacecraft

Undock departing spacecraft

Enable Experiments and Spacewalks

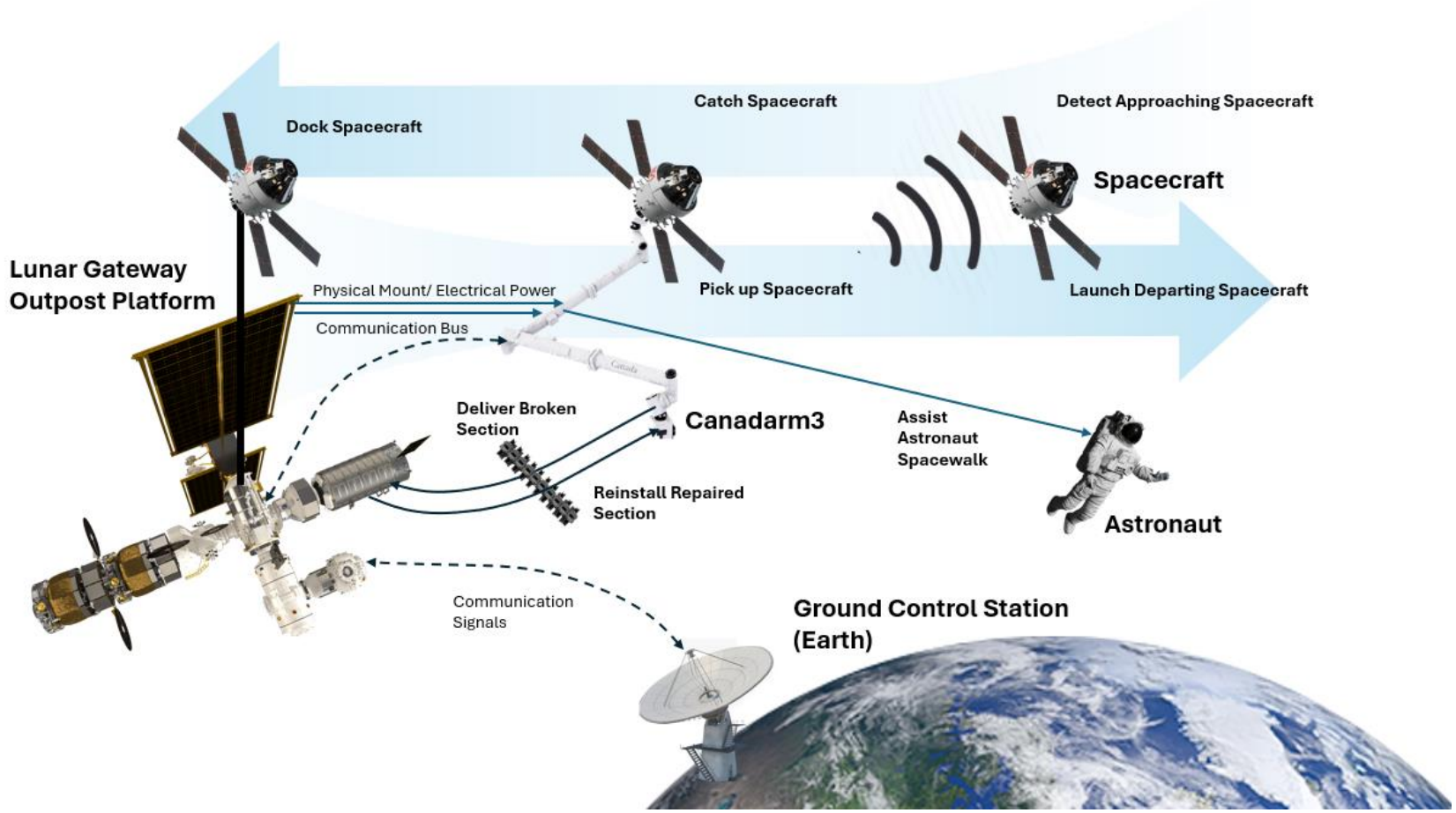


Assist Self-Maintenance

Georgia Tech
Aerospace Systems Design Laboratory

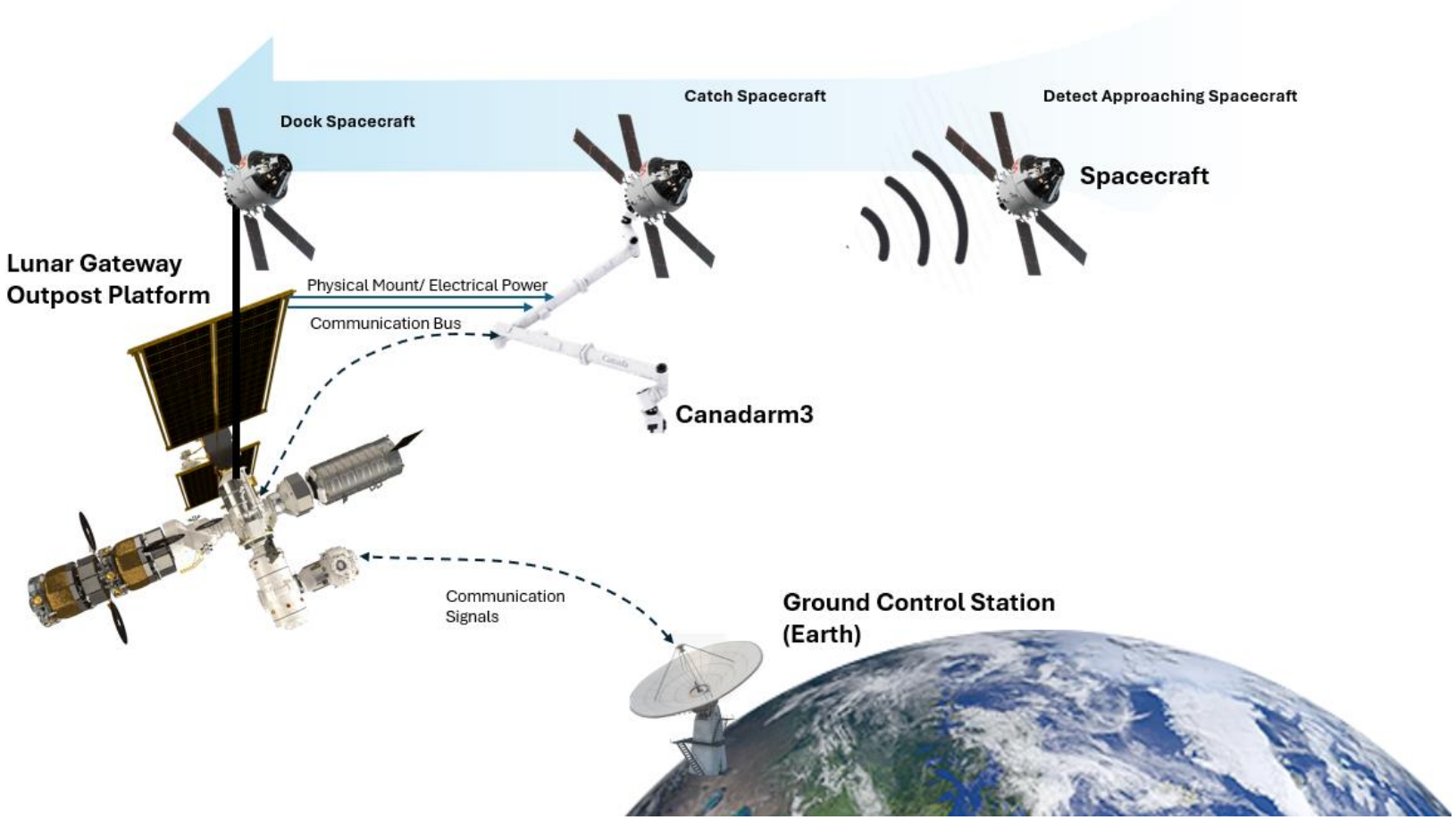
1. https://www.ctvnews.ca/sci-tech/canadian-space-agency-awards-mda-269m-contract-for-next-phase-of-canadarm-3-project-1.5813810
2. https://www.space.com/41776-capturing-a-spacecraft-with-robotic-arm-canadarm2.html
3. https://www.nasa.gov/podcasts/houston-we-have-a-podcast/robotic-arms-in-space/
4. https://www.nasa.gov/international-space-station/mobile-servicing-system/

Concept of Operations – Overall Mission(s)



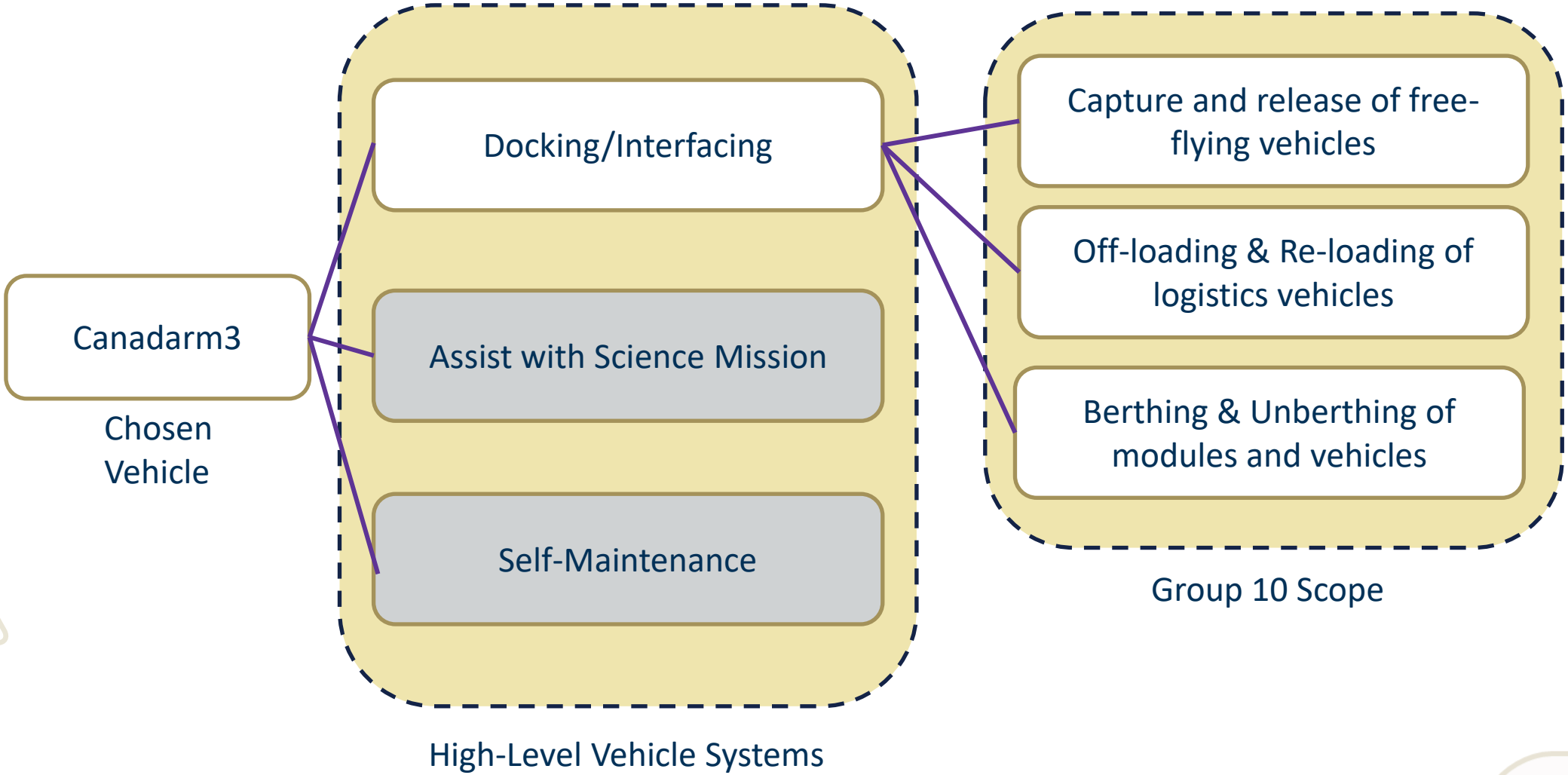
Canadarm3 has several missions including docking and launching spacecraft, assisting in self-maintenance and assisting with science activities (ie. Spacewalks, experiments, etc.)

Concept of Operations – Docking Spacecraft Mission



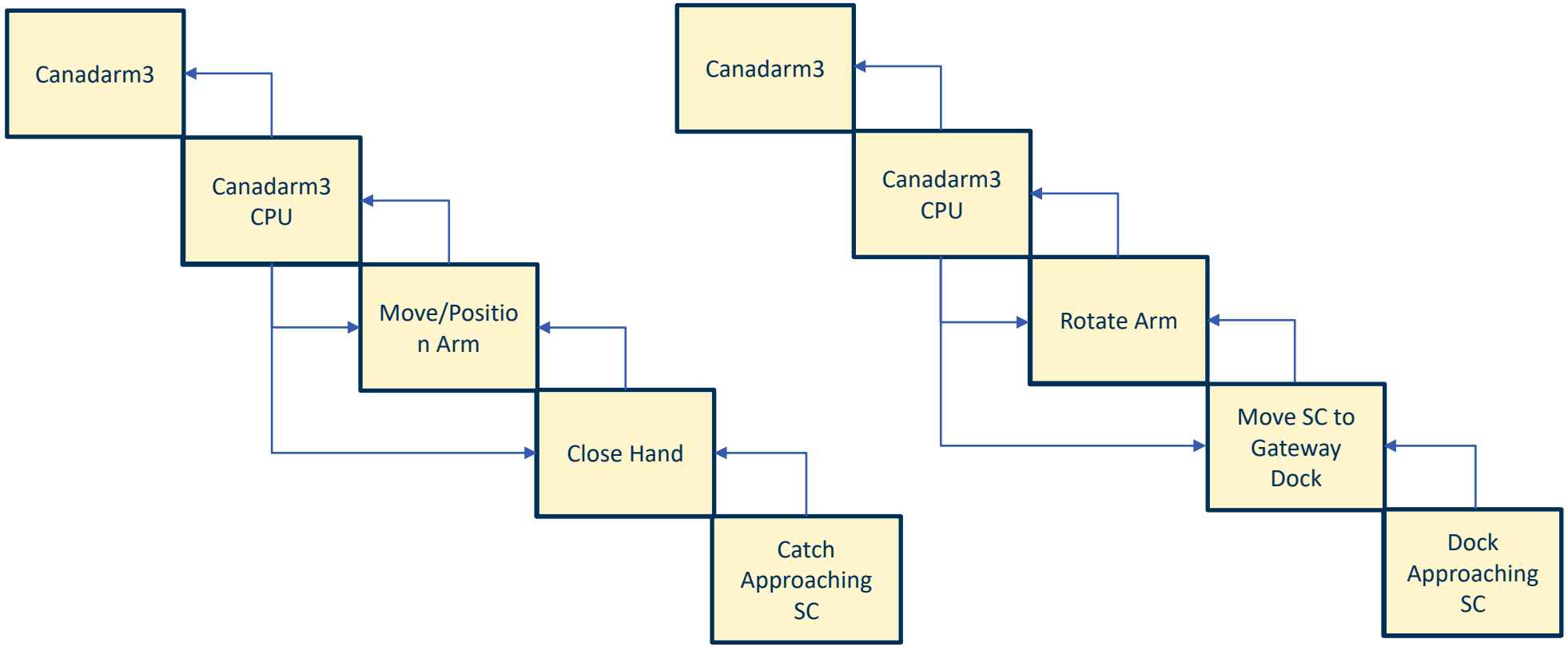
The scope of this project focuses on a functional risk and safety analysis for the Docking Approaching Spacecraft Mission.

Overall Problem Scope

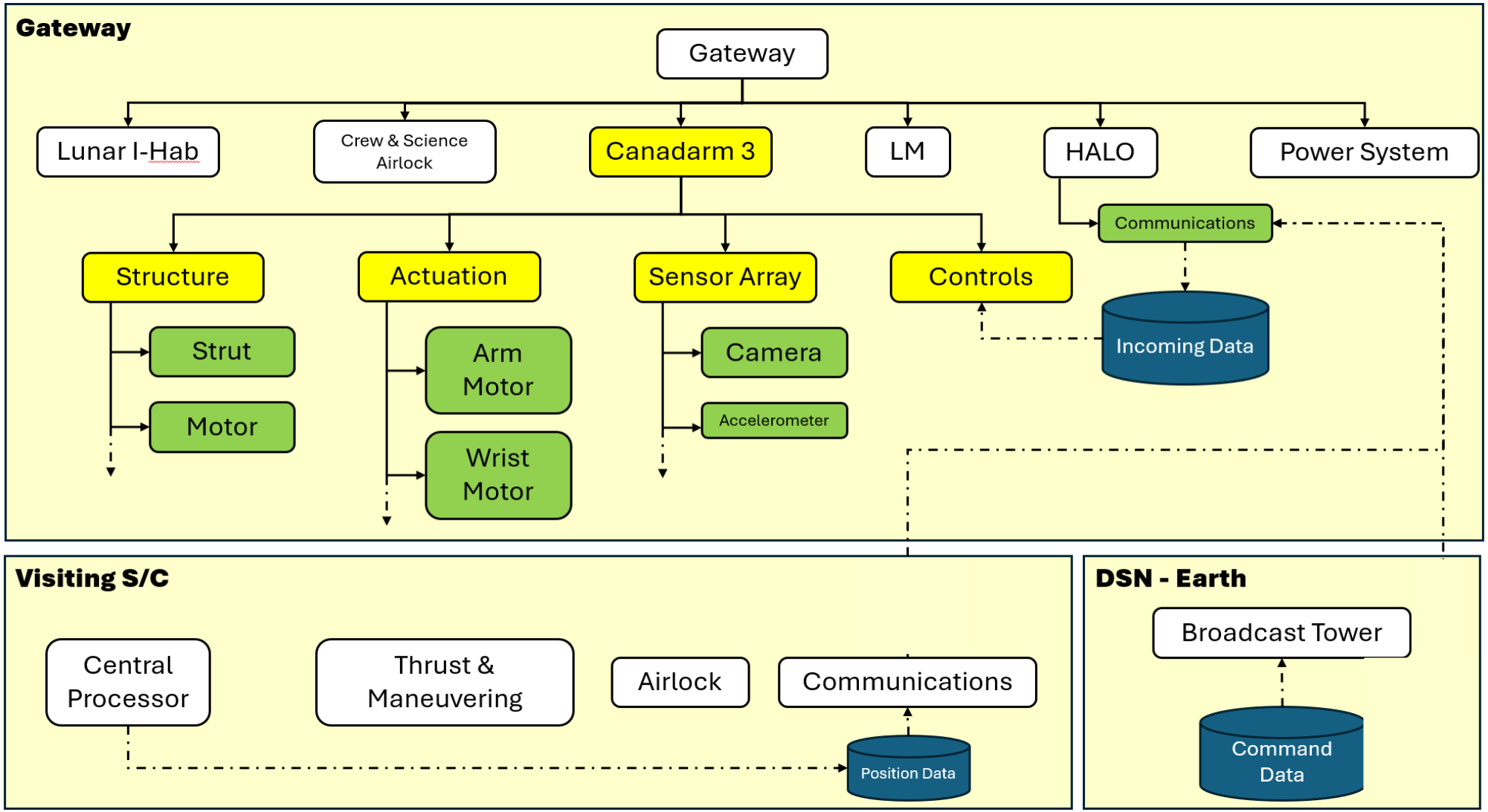


1. https://sqreports.s3.ca-central-1.amazonaws.com/2019/csa_canadarm3_industry_day_presentation.pdf

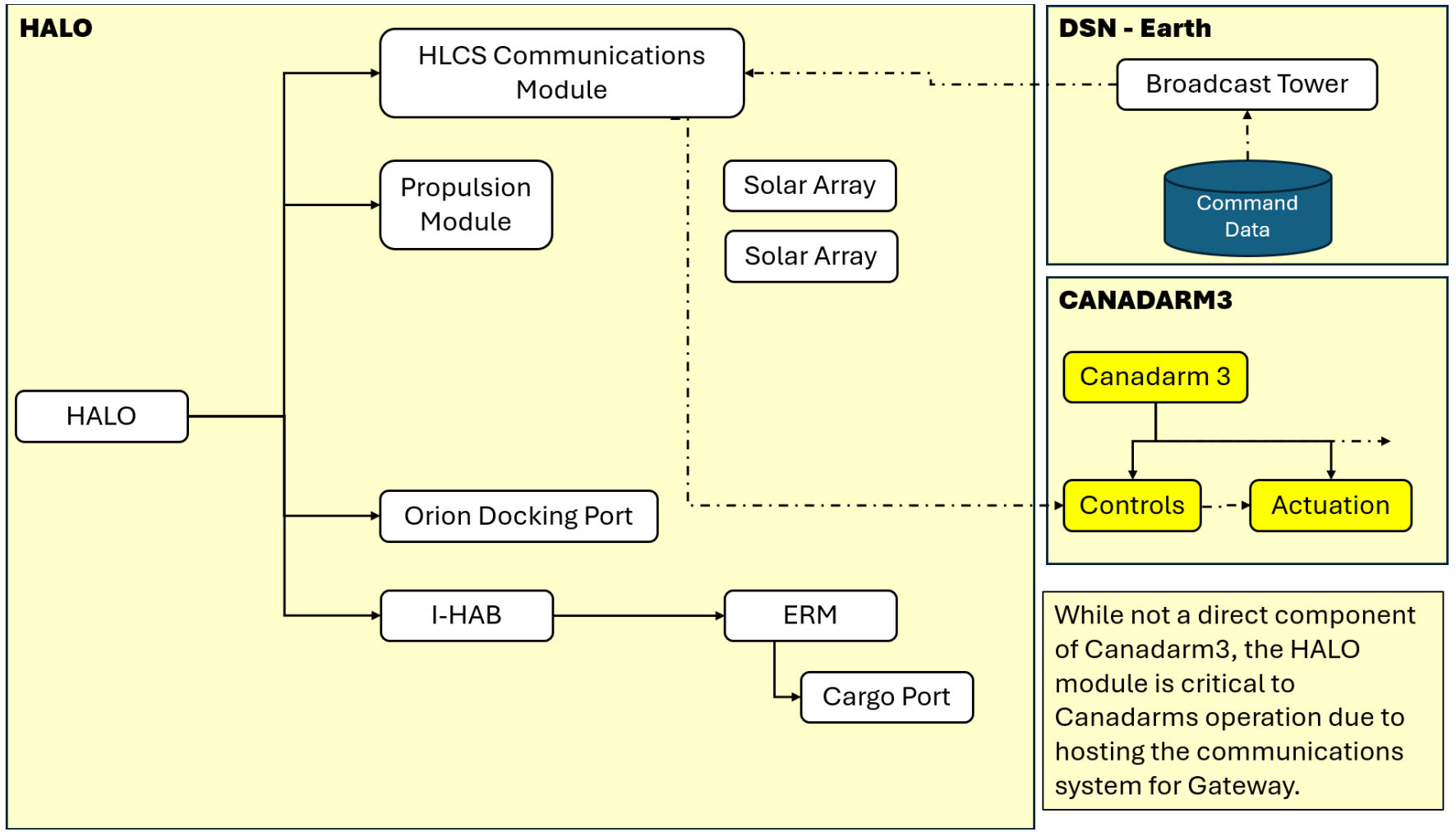
Functional Architecture Diagram - Catch & Dock Spacecraft



Gateway Physical Architecture



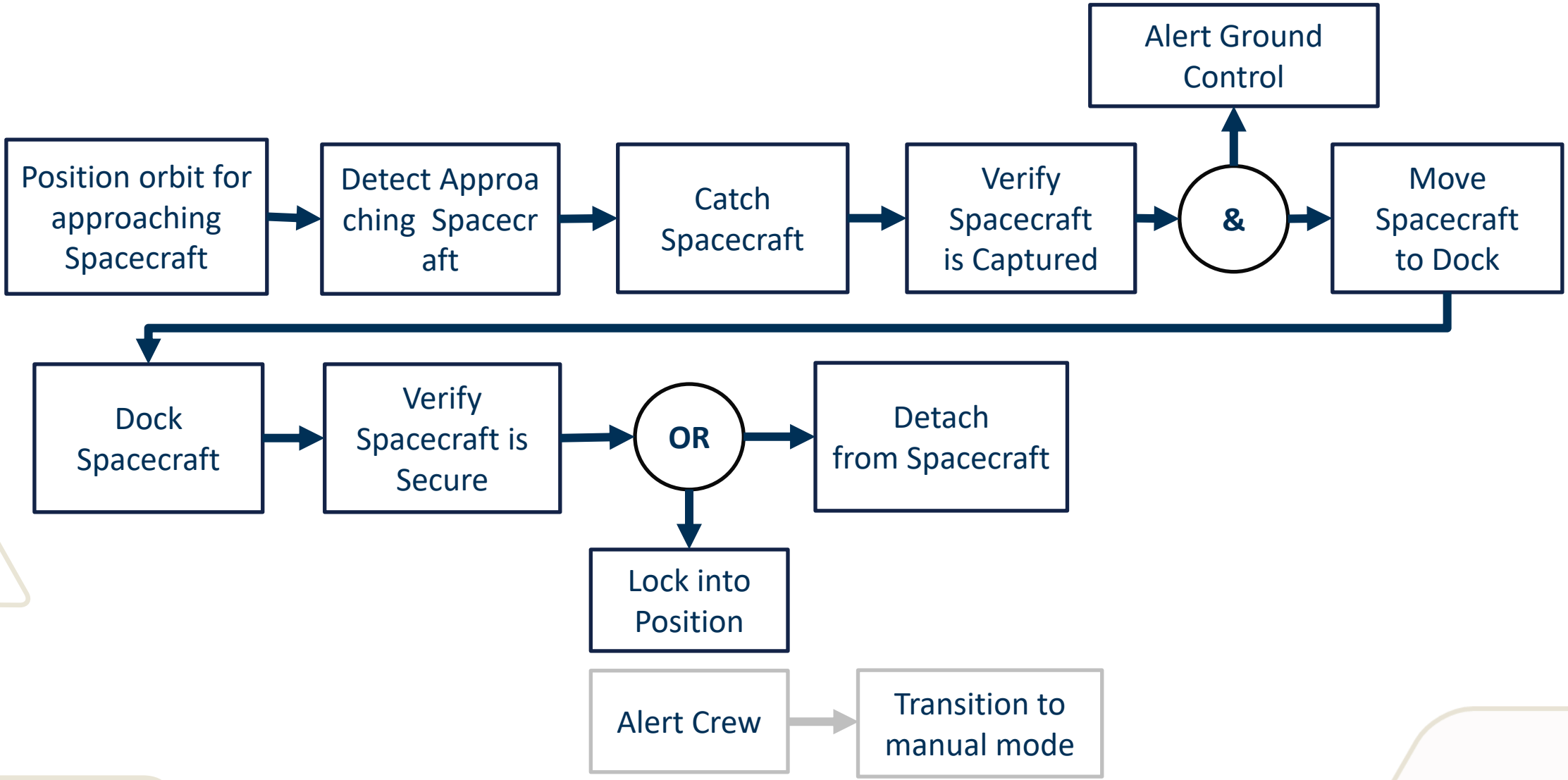
HALO Physical Architecture



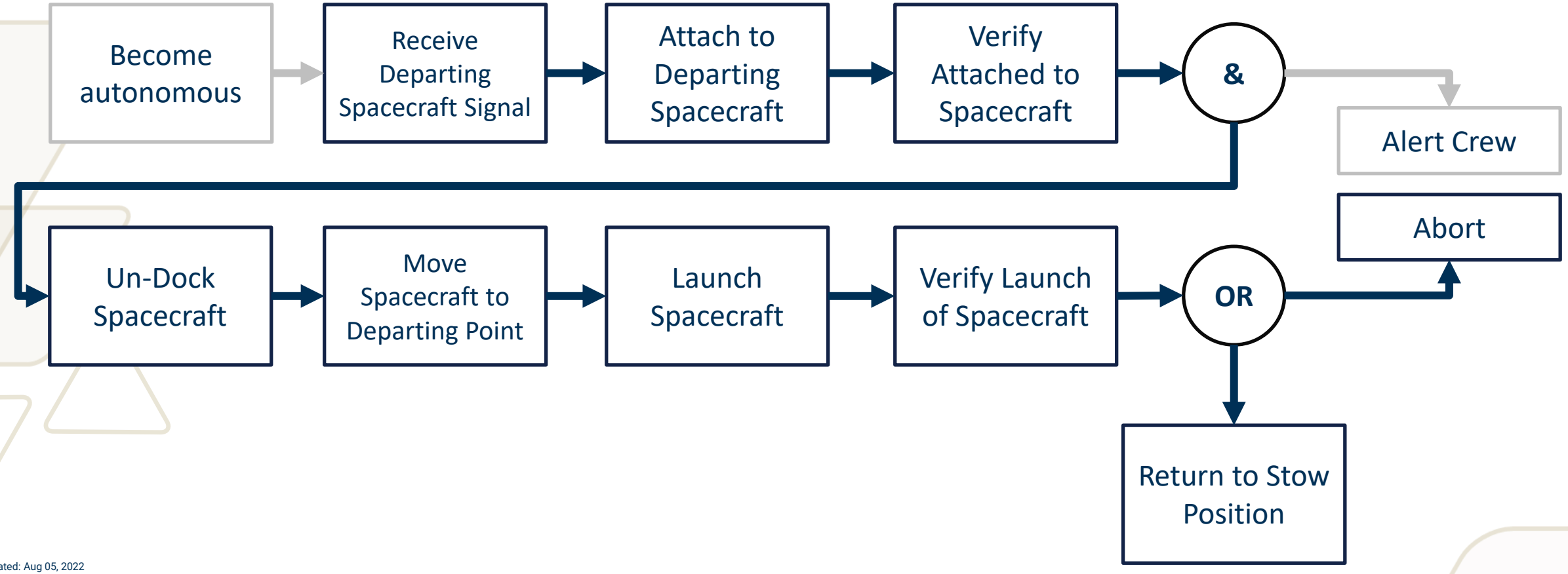
Tier 1 Functional Decomposition - Operations

Dock Approaching Aircraft	Detect Approaching Spacecraft	Catch Approaching Spacecraft	Dock Approaching Spacecraft
Launch Departing Aircraft	Pick up Departing Spacecraft	Launch Departing Spacecraft	
Assist Self-Maintenance	Detect Maintenance Issue	Deliver Broken Section	Replace Repaired Section
Manual Control (Space Walks, Experiments, etc.)		Actuate Control System	Register User Input

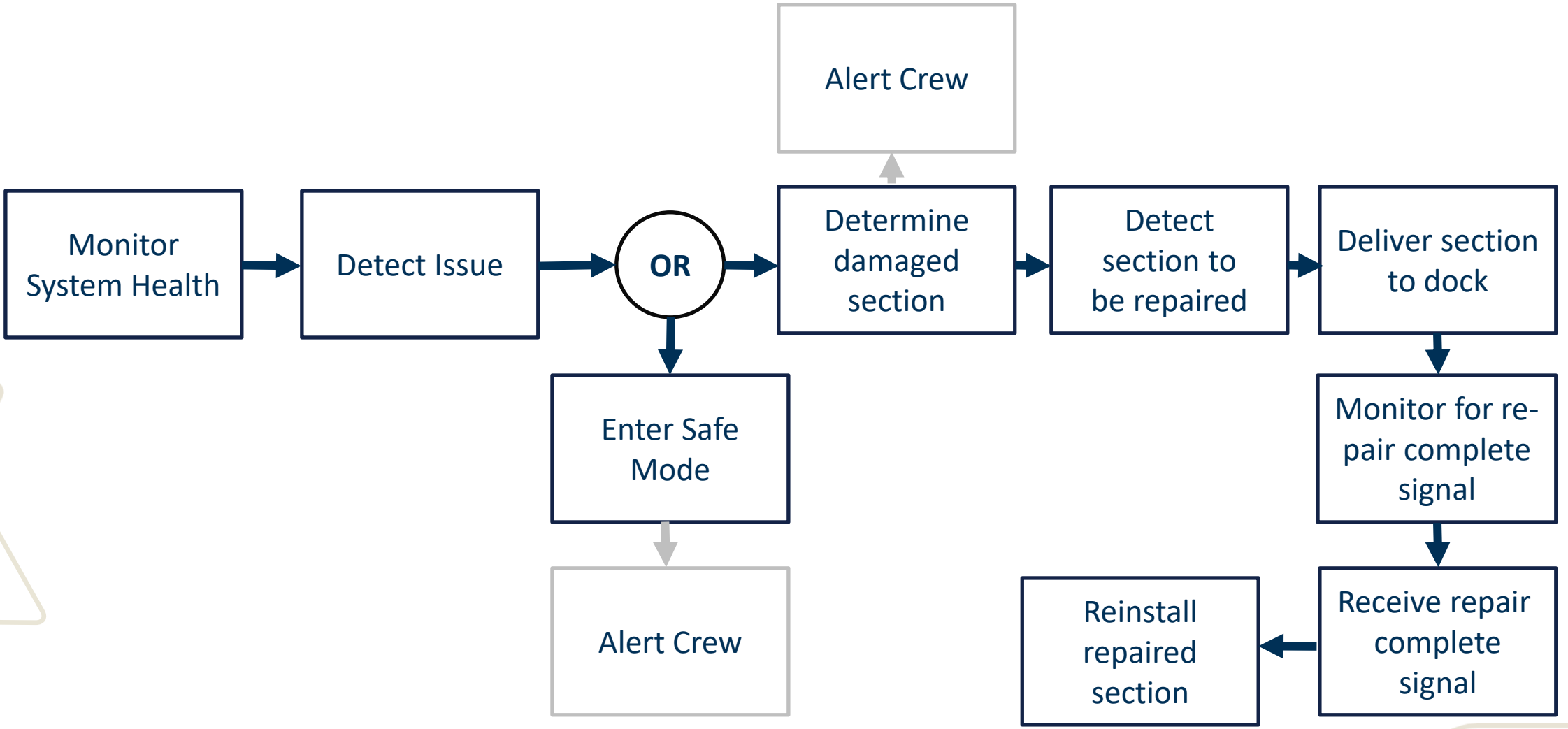
Tier 1 Functional Decomposition - Dock Approaching Spacecraft



Tier 1 Functional Decomposition - Launch Departing Spacecraft

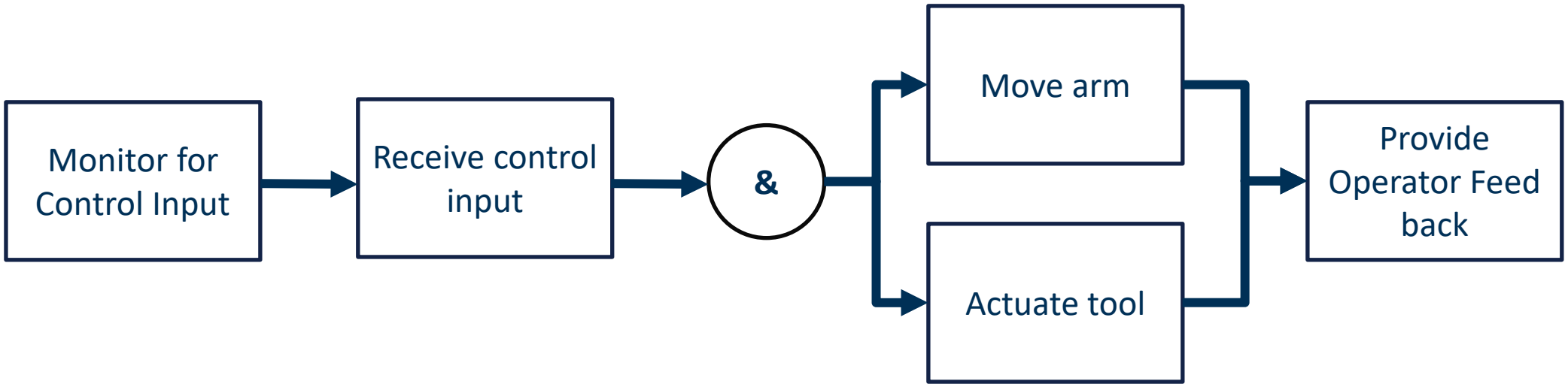


Tier 1 Functional Decomposition - Assist in Self Maintenance

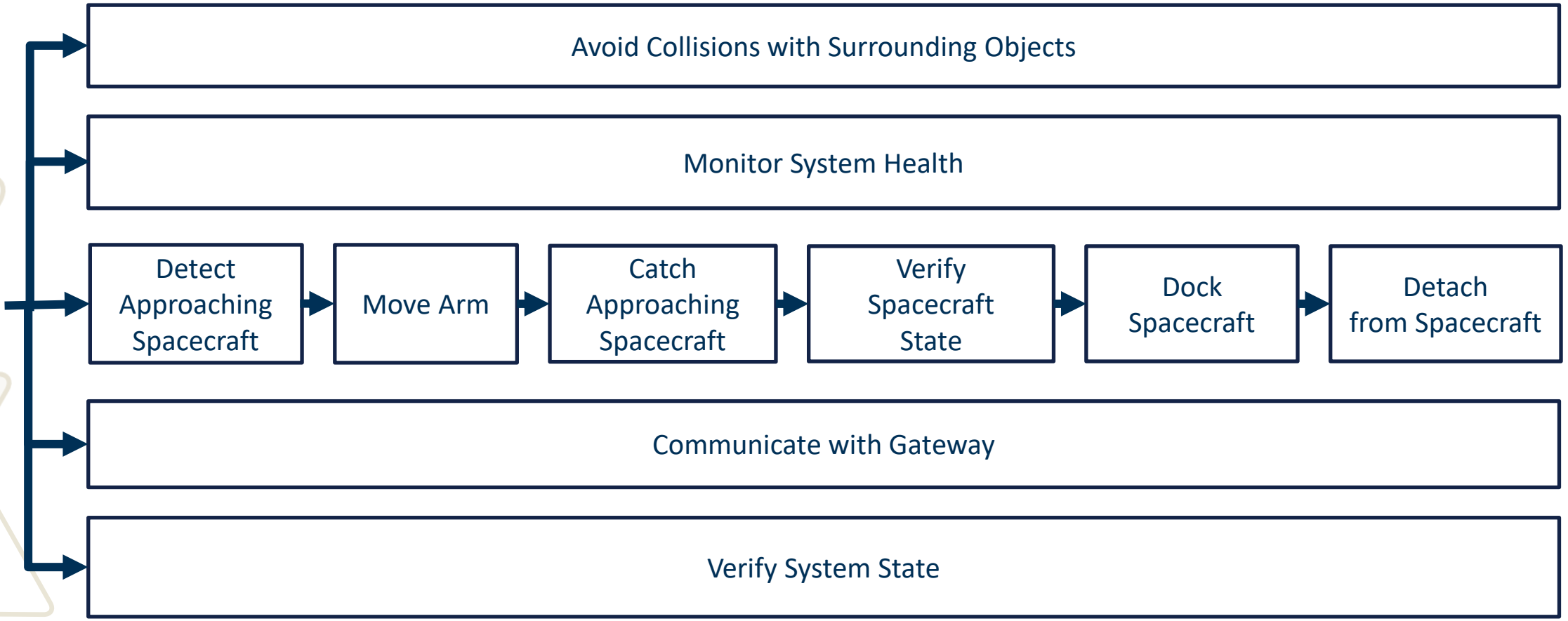


Tier 1 Functional Decomposition - Manual Control Mode

***Manual Control Model enables Space walks, experiments, Gateway repair, etc.*



Tier 1 Functions of Dock Approaching Spacecraft



The above diagram shows that several Tier 1 functions happen simultaneously

Tier 2 Functions of Dock Approaching Spacecraft

Detect Approaching Spacecraft
- Send radar signal
- Monitor radar signal
- Detect spacecraft on signal
- Communicate spacecraft detection to main control

Catch Approaching Spacecraft
- Predict spacecraft trajectory
- Calculate required arm trajectory for intercepting
- Move spacecraft arm
- Detect interception
- Attach to spacecraft

Verify Spacecraft State
- Read arm locking mechanism feedback signals
- Report spacecraft locked state to main controller
- Verify Spacecraft Trajectory

Move Arm
- Calculate trajectory to dock
- Decompose trajectory into effector demand signals
- Actuate effectors
- Verify tracking using feedback signals

Dock Spacecraft
- Set spacecraft on the dock aligned with locking mechanism
- Lock spacecraft into place
- Verify spacecraft docked
- Communicate spacecraft docked

Detach from Spacecraft
- Disengage locking mechanism
- Move arm away from spacecraft

Tier 2 Functions of Dock Approaching Spacecraft

Avoid Collisions with surrounding objects

- Monitor proximity sensors for surrounding objects
- Detect position of surrounding objects
- Adjust control system arm trajectory and/or speed
- Verify new adjusted trajectory avoids obstacles

Communicate with Gateway

- Send system state and health signals on communication bus to Gateway
- Monitor for demand signals
- Receive demand signals
- Process demand signals
- Deliver demand signals to controller

Verify System State

- Sense locking mechanism status
- Monitor lock sensor status
- Determine spacecraft position from lock configuration
- Compare spacecraft position to expected position
- Report system state to controller

Monitor System Health

- Monitor accelerometers for acceptable vibration levels and collision detection
- Monitor sensors against critical limits (speed, te mperature, load, etc.)
- Compare redundant sensors for agreement
- Determine system health from monitored sensors
- Report System health to controller

FHA Overview

The FHA lays out system level functions and potential failure modes; by assigning each of these modes a severity score, the FHA can facilitate vehicle-level safety analysis

The risk values listed in our FHA are representative of mitigation actions taken for the final vehicle, including operating procedures and system redundancy

Probability Criteria

1	2	3	4	5
Near Impossible	Remote	Uncommon	Probable	Frequent

Severity Criteria

==========	1	2	3	4	5
Mission Impact	No impact	Mission delays	Mission options limited	Mission success at risk	Mission failure
Vehicle Impact	No impact	Minor damage	Significant damage	Major damage	Loss of vehicle
Human Impact	No impact	No impact	Mitigation required	Minor injury	Major injury or fatality

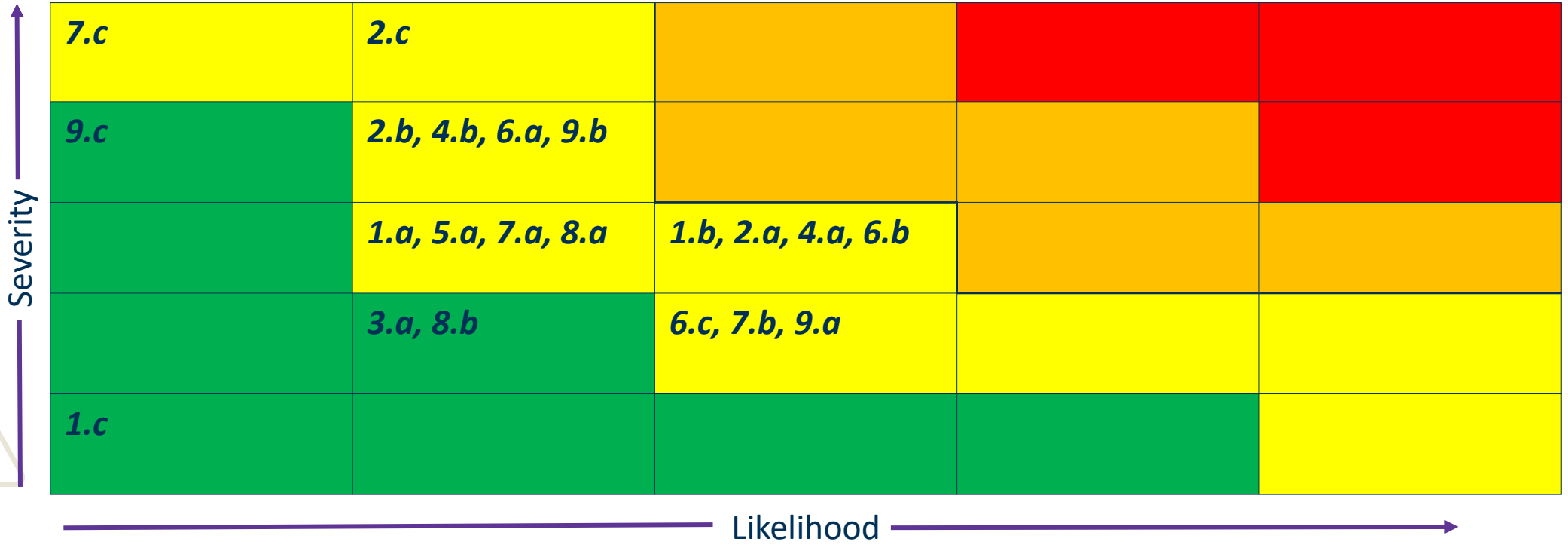
FHA of Dock Approaching Spacecraft

Subfunction	Failure Mode	Likelihood	Severity	Risk Score
1) Detect approaching spacecraft	a) Unable to detect existing spacecraft	2	3	6
	b) Spacecraft detected in the wrong location	3	3	9
	c) Nonexistent spacecraft detected	1	1	1
2) Catch approaching spacecraft	a) Spacecraft missed entirely	3	3	9
	b) Spacecraft collides with Canadarm3	2	4	8
	c) Spacecraft collides with Gateway	2	5	10
3) Verify spacecraft state	a) Unable to verify spacecraft state	2	2	4
4) Avoid collisions with surrounding objects	a) Unable to detect surrounding objects	3	3	9
	b) Able to detect but not able to maneuver away	2	4	8
5) Communicate with Gateway	a) Unable to communicate with Gateway	2	3	6
6) Move arm	a) Unable to move arm at all	2	4	8
	b) Partial mobility of arm	3	3	9
	c) Arm movement fails to meet requirements	3	2	6

FHA of Dock Approaching Spacecraft

Subfunction	Failure Mode	Likelihood	Severity	Risk Score
7) Dock Spacecraft	a) Docking hatch does not engage	2	3	6
	b) Hatch misaligned	3	2	6
	c) Docking state misidentified	1	5	5
8) Detach from Spacecraft	a) Arm does not disengage properly	2	3	6
	b) Arm cannot maneuver away from craft	2	2	4
9) Monitor system health	a) Monitor makes false red reading	3	2	6
	b) Monitor makes false green reading	2	4	8
	c) Monitoring routines crash	1	4	4

Operational Risk Assessment – Risk Matrix



Operational Risk Assessment – Key Risks

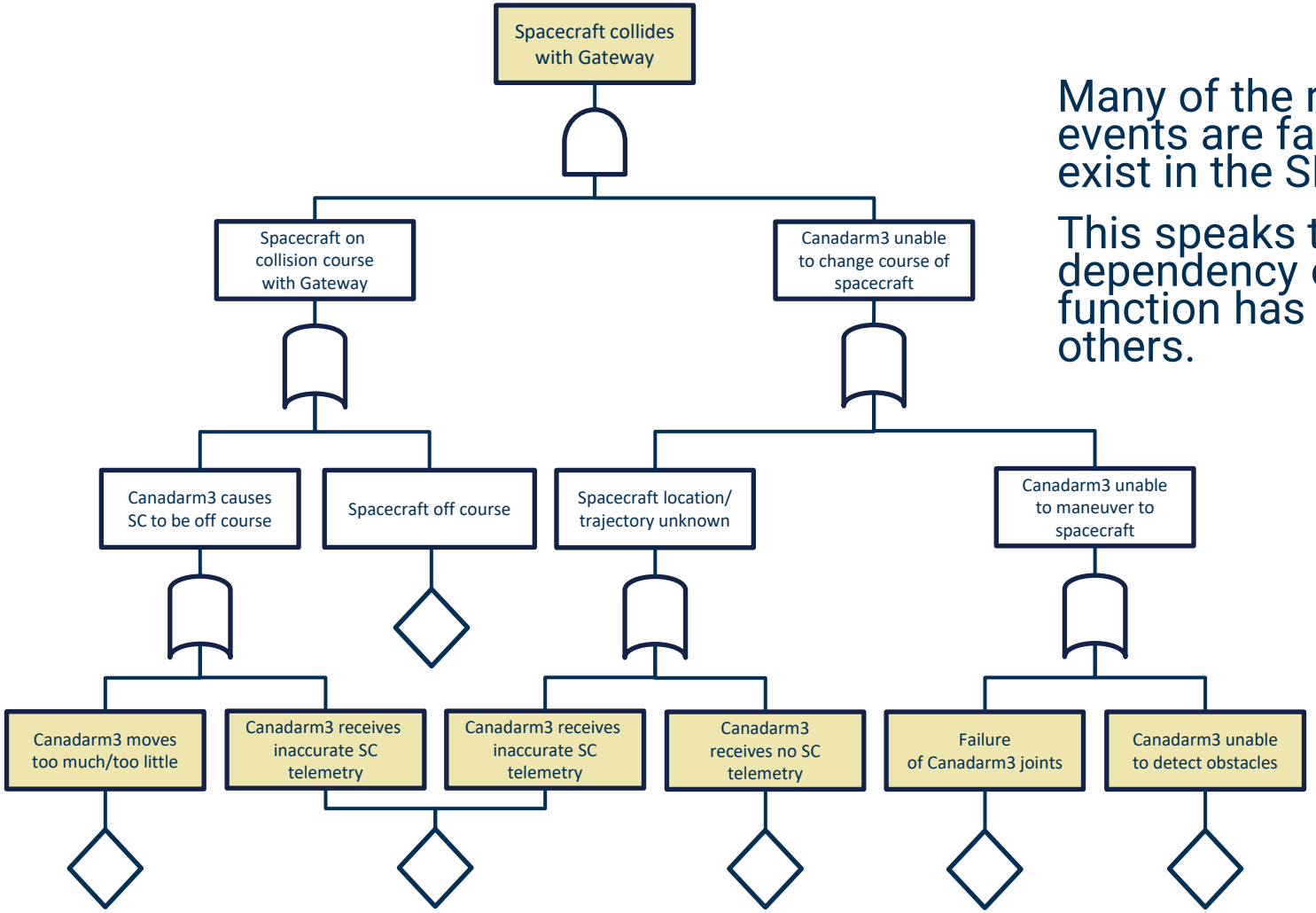
- 2.c - Spacecraft collides with Gateway
  - Even at low speeds, the station is not designed to take impacts.
  - Likelihood is low, as both Canadarm and the spacecraft would have to have major failures
  - Docking patterns and controlled approaches can mitigate
- 9.b - Monitor gives false green
  - The most dangerous risk is the one that is not noticeable. If a software error obscures an issue in Canadarm, all other operations could be disrupted.
  - Redundancy on monitors can help mitigate
- 7.c - Docking state misidentified
  - While seemingly not as bad as an impact, if the station misjudges the state of a docked vessel, the fallout effects could be severe
  - Communications between Gateway, Canadarm, and the visiting craft can mitigate
- 2.a - Spacecraft missed entirely
  - Severity is lower, as there is less danger of physical contact, but mission success could be put in jeopardy if Canadarm misses a spacecraft
  - Similar to 2.c and 7.c, robust communication and docking patterns can increase the reliability of Canadarm

Vehicle Target Level of Safety

- The Vehicle TLS will be conducted as a functional-level analysis. For each functional step, a probability of failure will be determined.
- Probability of failure will be judged on a per-cycle basis, rather than per-hour, as Canadarm3 will experience long periods of inactivity.
- Canadarm1 and Canadarm2 completed their missions with few incidents, and will be used a benchmark to judge the safety of Canadarm3
- Across the vehicle there shall be no single points of failure that do not have a redundancy
- Requirements for Probability of Occurrence of failure modes will be based on the severity assessed in the risk analysis
- Any risks with a severity level of 4 or 5 will have less than a 10E-9 probability of occurrence per cycle

Failure Condition Severity	Probability of Occurrence Requirement
5 - Catastrophic	10E-9
4 - Hazardous	10E-9
3 - Major	10E-6
2 - Minor	10E-4
1 - No Safety Effect	10E-3

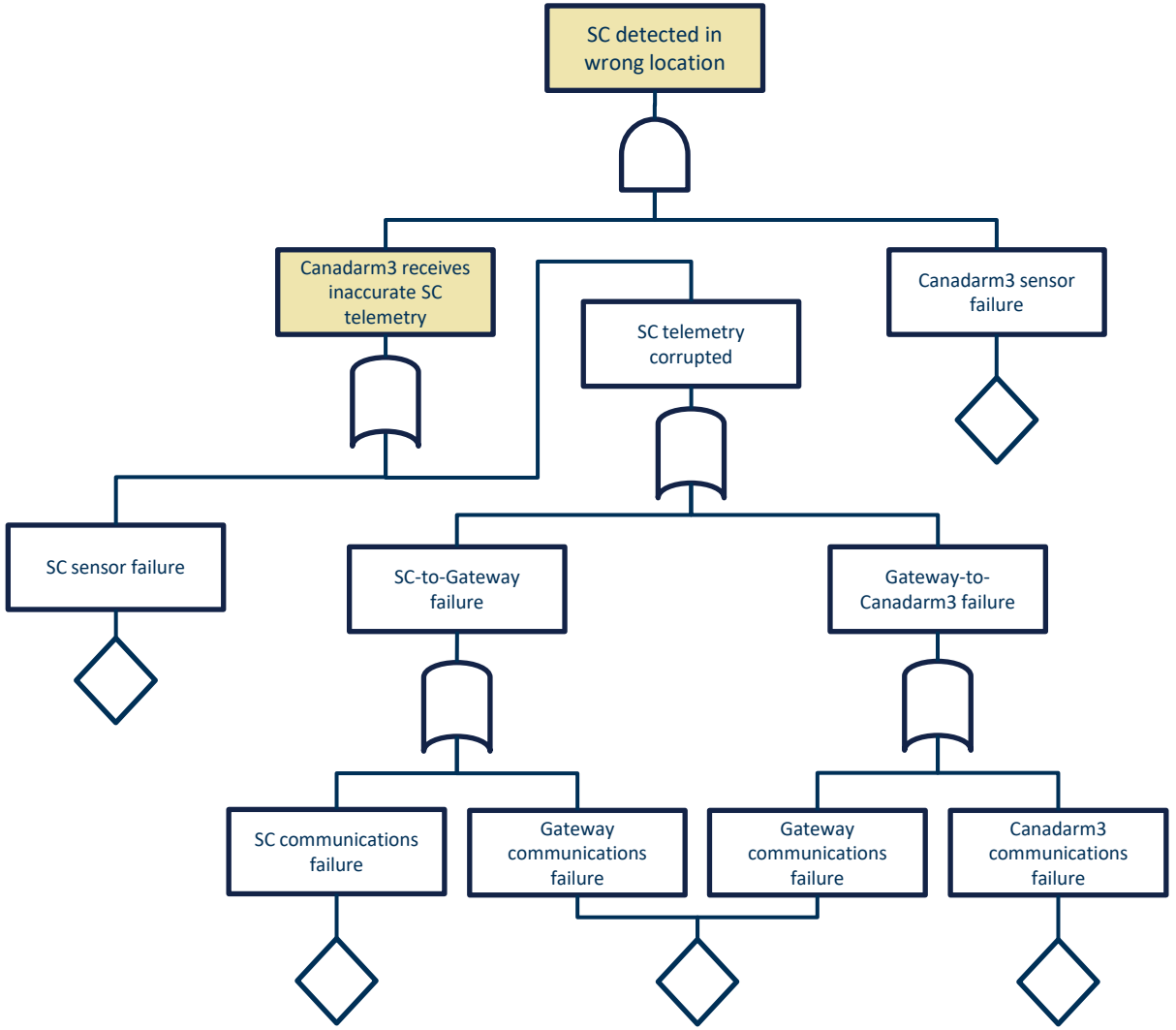
Preliminary System Safety Analysis – Fault Tree Analysis



Many of the random events are failures that exist in the SFHA.

This speaks to the high dependency each function has on the others.

Preliminary System Safety Analysis – Fault Tree Analysis



Conclusions/Takeaways

- Safety assessments are iterative (i.e. Unacceptable risks lead to mitigation strategies and architecture changes, which lower risks to an acceptable level)
- At this high level, the risk assessment has some subjectivity in it. Creating clear definitions associated to the risk levels helped keep rankings consistent across the risks so that the assessment results were useful. More detailed assessments at lower levels would increasingly remove subjectivity as the design matures.
- Many causes of failure root from the communication and control system. Similar to many aircraft and aircraft engines, this may drive an architecture requirement to have two fully redundant control systems

Conclusions/Takeaways

- FTA's may loop in on themselves
  - An item in an FTA may have its own FTA that has another item in the original FTA, etc.
- Quantifying risks as probabilities is difficult as a result, because they just may come from the Risk Matrix itself
- Gateway and other spacecraft missions have less available system monitoring that may lead to additional risks than in on-the-ground systems

Future Recommendations

- In-depth FTA to the component level for communications failures
- Bow tie chart for identifying mitigating event chains and/or redundancies
- Write a detailed Safety Plan
- Identify stakeholders to determine both additional system priorities and available support

References

[1]https://ntrs.nasa.gov/api/citations/20220013534/downloads/Gateway%20Program%20Status%20and%20Overview_22corrected.pdf

[2]https://explorers.larc.nasa.gov/HPMIDEX/pdf_files/17C_Robotics-020918_R1.pdf

[3]https://www.independent.co.uk/space/nasa-orion-apollo-moon-comparison-b2153832.html

[4]https://www.alamy.com/astronaut-performing-a-space-walk-isolated-on-white-background-image261658016.html

[5]https://assetstore.unity.com/packages/3d/environments/industrial/satellite-dish-antenna-156628

[6]https://arc.aiaa.org/doi/pdf/10.2514/6.2018-2464

This page intentionally left blank