



The Requirements



- *NPR 705.2B, Human Rating Requirements*
 - *Places the responsibility on the program to determine the appropriate implementation of failure tolerance to catastrophic events.*
 - *The overall objective is to provide the safest design that can accomplish the mission given the constraints imposed on the program.*
 - *Since space system development will always have mass, volume, schedule, and cost constraints, choosing where and how to apply failure tolerance requires integrated analyses at the system level to assess safety and mission risks.*
 - *The use of PRA to justify the level of failure tolerance is approached with caution.*
 - *PRA is a powerful tool when used to compare the relative merits of competing design options and increased failure tolerance.*
 - *However, the use of PRA, in an absolute sense, to claim that the system design is safe because the PRA satisfies a specified loss of crew probabilistic number does not comply with the spirit or the intent of this requirement.*



NPR 8705.2B, Human Rating Requirements



- **2.3.7.1 The Program Manager shall perform an integrated safety and design analysis to determine the following:**
 - **a. The requirements for additional levels of failure tolerance (above the minimum of 1 failure tolerant per 3.2.2) for the space system.**
 - **b. The appropriate implementation of failure tolerance for the space system, to include an evaluation of dissimilar redundancy and backup systems (Requirement).**
- **3.2.2 The space system shall provide failure tolerance to catastrophic events (minimum of one failure tolerant), with the specific level of failure tolerance (one, two or more) and implementation (similar or dissimilar redundancy) derived from an integrated design and safety analysis (per the requirement in paragraph 2.3.7.1) (Requirement).**
 - *Failure of primary structure, structural failure of pressure vessel walls, and failure of pressurized lines are excepted from the failure tolerance requirement provided the potentially catastrophic failures are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance. Other potentially catastrophic hazards that cannot be controlled using failure tolerance are excepted from the failure tolerance requirements with concurrence from the Technical Authorities provided the hazards are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance.*



Orion Philosophy



- Each hazard cause must be addressed individually and controlled.
 - Hazard controls must prevent the hazard from occurring. Thus, emergency systems and crew survival modes, which are responses to hazard occurrence, are not used as hazard control.
- The hazard control strategy for each hazard cause must be justified as adequate based on the associated risk of hazard occurrence with the controls in place.
 - Vulnerability assessments, including PRA results, communicate risk drivers and potential reliability weaknesses which may result in higher risk of hazard occurrence
 - Hazards judged to have an unacceptably high risk are targeted for risk reduction, possibly using additional failure tolerance.
- When all hazard causes have a valid, accepted hazard control strategy and the corresponding risk is accepted by the required stakeholders, then the design is deemed “good enough”.



Orion Vulnerability Assessments



- Vulnerabilities = technical risks affecting safety, mission success, vehicle reliability, vehicle performance, or operability.
- Vulnerabilities are identified through several engineering analyses
 - integrated vehicle performance analyses (power, thermal, operational)
 - Structural analyses (margins of safety)
 - Probabilistic Risk Assessment (PRA) (LOC LOM risk drivers)
 - Fault Tree Analysis (hazards and causes)
 - System reliability analyses (FMEA/CIL, RMS assessments)
 - Operability assessments (crew-vehicle interfaces, operator requirements and constraints)

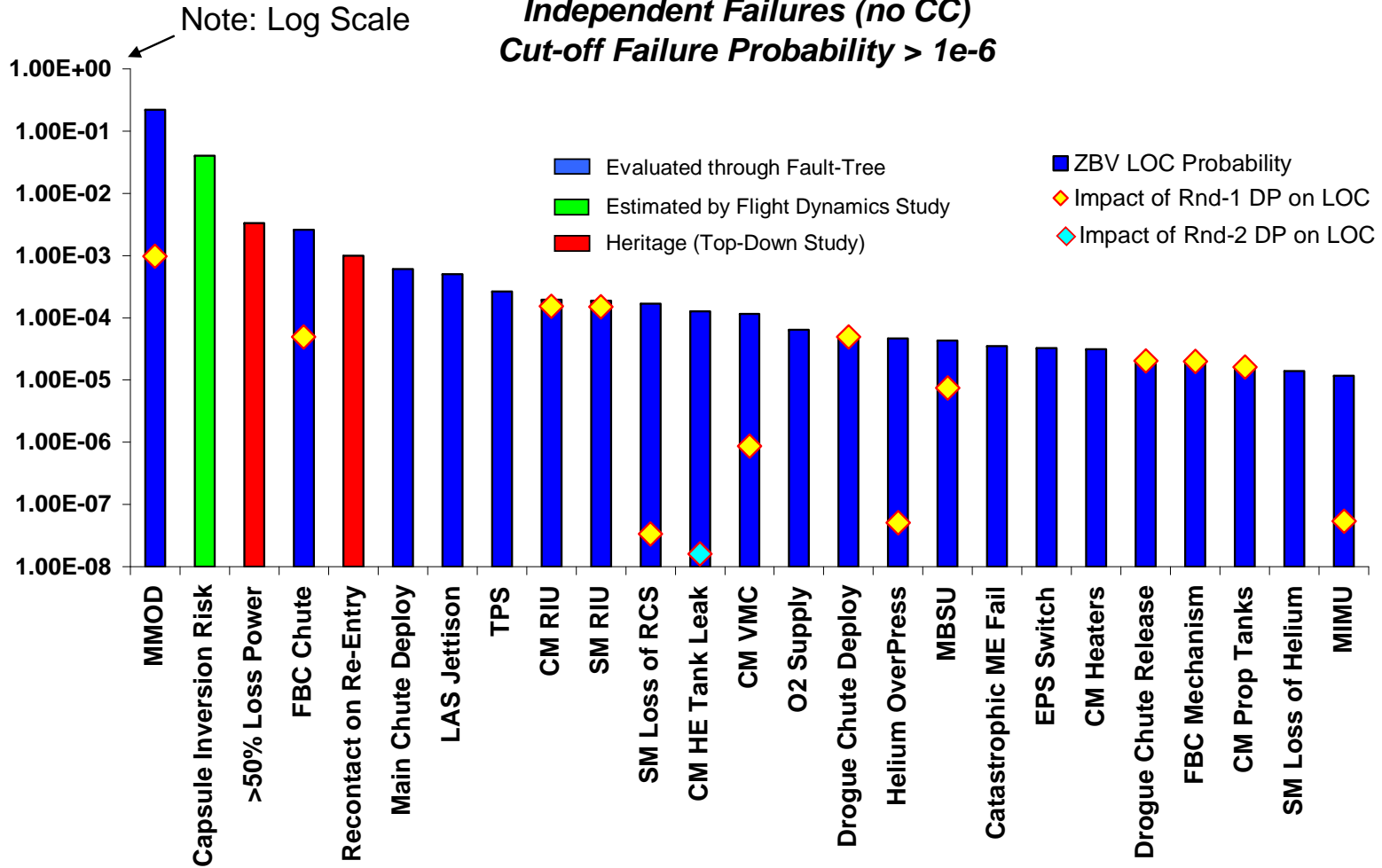


Risk Status

(from Nov. Briefing to Administrator)



Probability of LOC Risk for Top Concerns
Zero-Based Vehicle Point of Departure
Independent Failures (no CC)
Cut-off Failure Probability > 1e-6

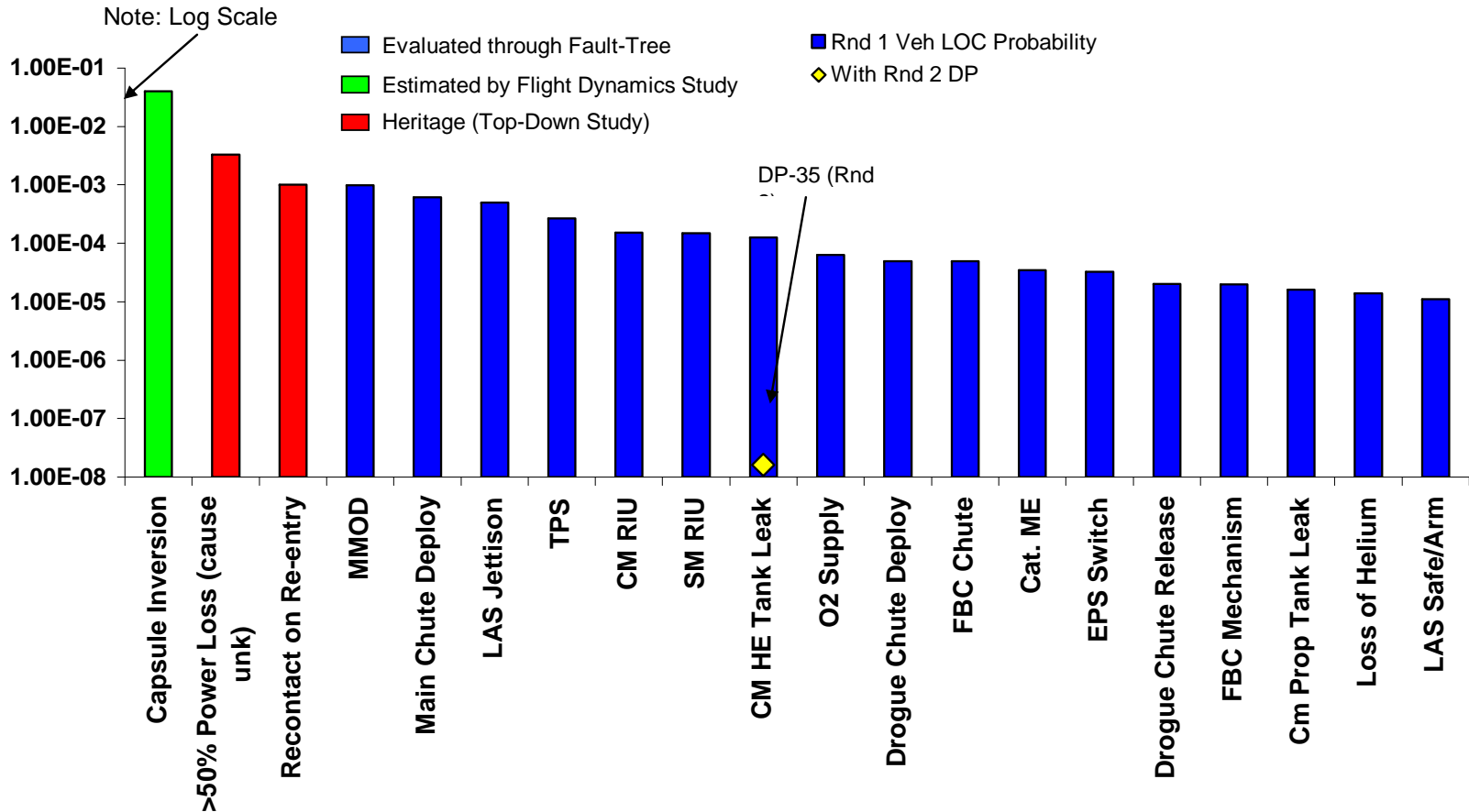




Risk Status (from Nov. Briefing to Administrator)



Probability of LOC Risk for Top Concerns
Round One Point of Departure
Independent Failures (no CC)
Cut-off Failure Probability $\geq 1e-6$

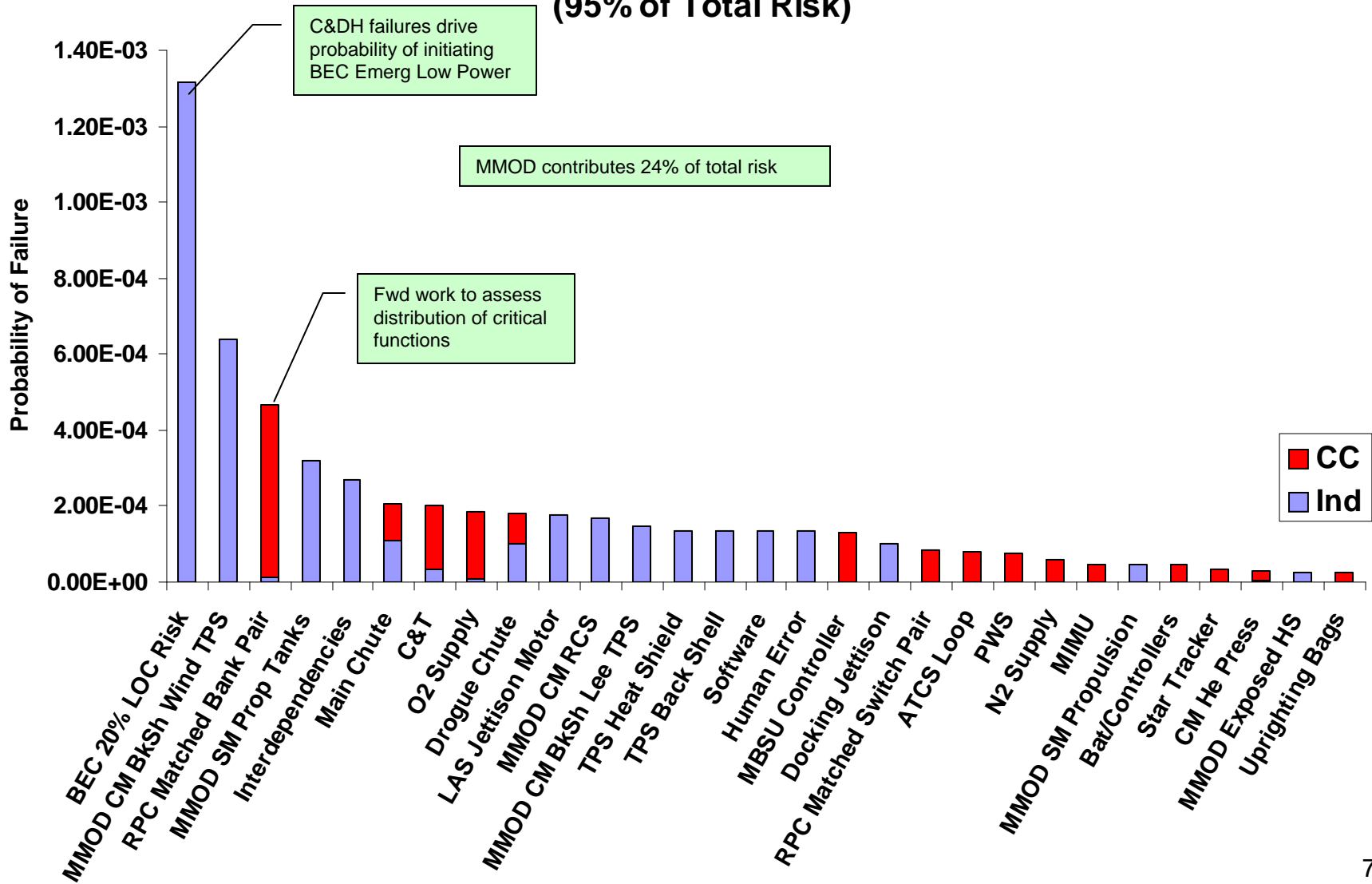




Top Drivers – LS LOC (May/2008)



LS LOC Top Drivers (95% of Total Risk)

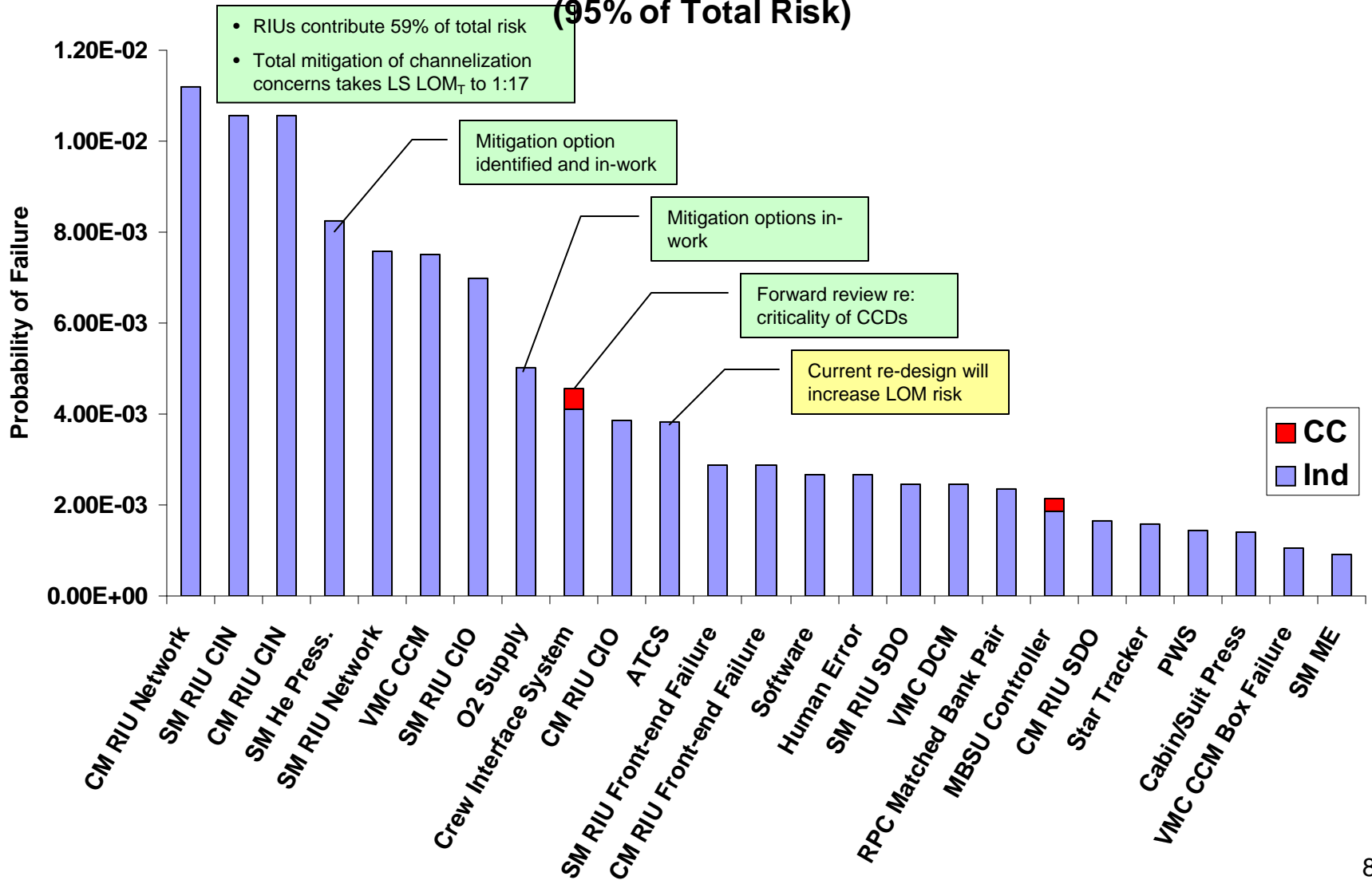




Top Drivers – LS LOM₀ (May/2008)



LS LOM₀ Top Drivers (95% of Total Risk)





Orion Avionics Operational Mode Philosophy



- **Primary**

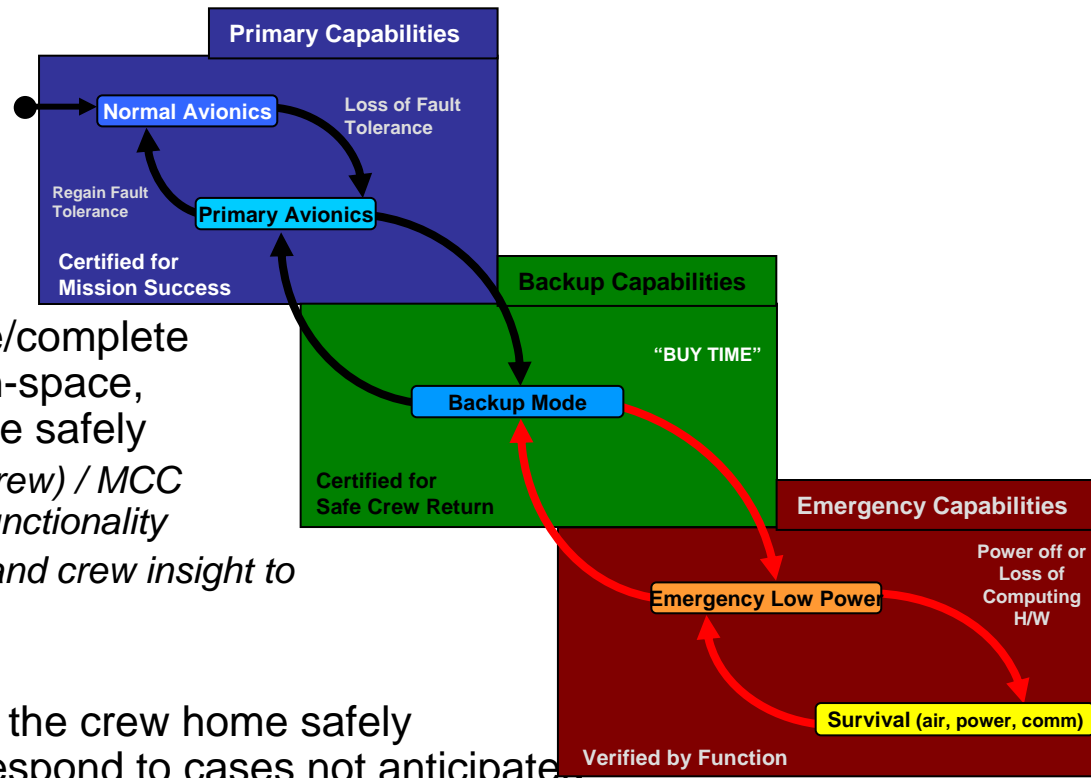
- System functionality to execute the mission within the designed fault tolerance

- **Backup**

- System functionality to execute/complete critical events (ascent, abort, in-space, entry) and return the crew home safely
 - *Requires additional manual (crew) / MCC operations to implement the functionality*
 - *Assumes reasonable ground and crew insight to system operations*

- **Emergency**

- Minimum functionality to return the crew home safely and maximize survivability to respond to cases not anticipated.
 - *Requires extensive manual (crew) / MCC operations to implement the functionality*
 - *Assumes limited ground and crew insight to system operations*





Orion Avionics

Key Architectural Features



- **General**
 - Primary flight control, display & control (D&C), and comm & track (C&T) functions will have no single point failures affecting more than one function
 - Automatic re-initialization of D&C and C&T functions
 - Autonomous heater control with set point override
 - Sun-Safe mode provides optimum power/thermal configuration with power load shed
- **Backup (all mission phases)**
 - Backup to flight control module only
 - Utilize primary displays & controls and comm & track capabilities through network access
 - Common mode failure protection through dissimilar software (selected functions)
 - Certified functionality to return the crew safely in any mission phase
 - Executes operator initiated recovery of primary system
 - Automatic fault detection & annunciation with manual isolation and reconfiguration



Orion Avionics

Key Architectural Features (cont.)



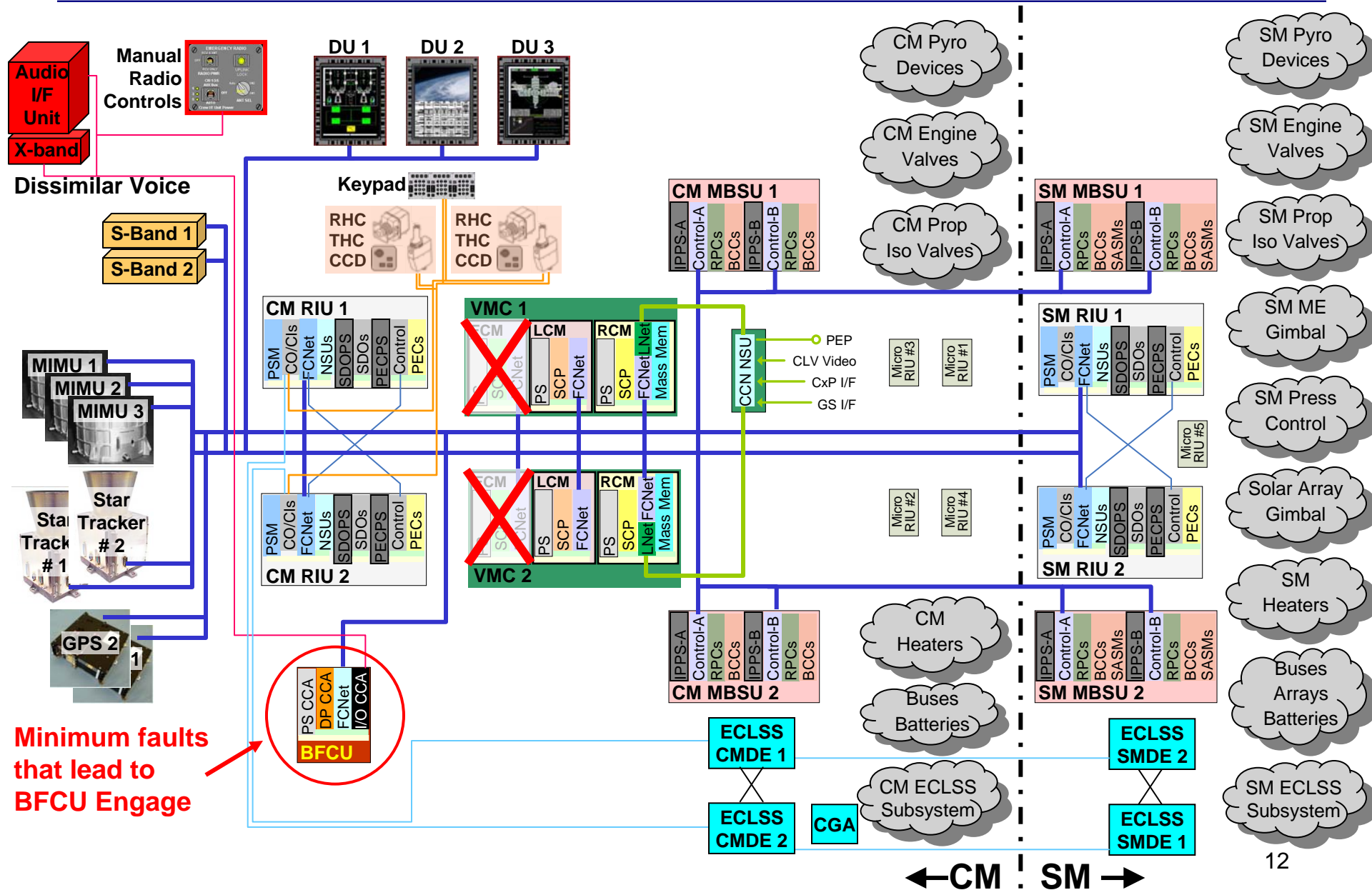
- **Emergency (In-space through landing)**
 - Fault protection for significant radiation or loss of power, active thermal event
 - Low-power BFCS with limited software computing & display capability
 - Verified by subsystem to a narrow range of functionality
 - “Hard-wired” to 1 string of safety critical functions required for safe return
 - Will sustain crew in suit but crew not required to be in suit for survival
 - Software assist is required for most Emergency functions
 - **Emergency Survival Mode (in space only)**
 - Maintain a breathable atmosphere & cabin environment
 - Maintain periodic voice communications with the ground
 - Reconfigure electrical system to power up and down core avionics

Distributing subsystem functionality where it improves P_{LOC} and P_{LOM}



Backup System Diagram (BFCU Engaged Upon 2 FCM Faults)

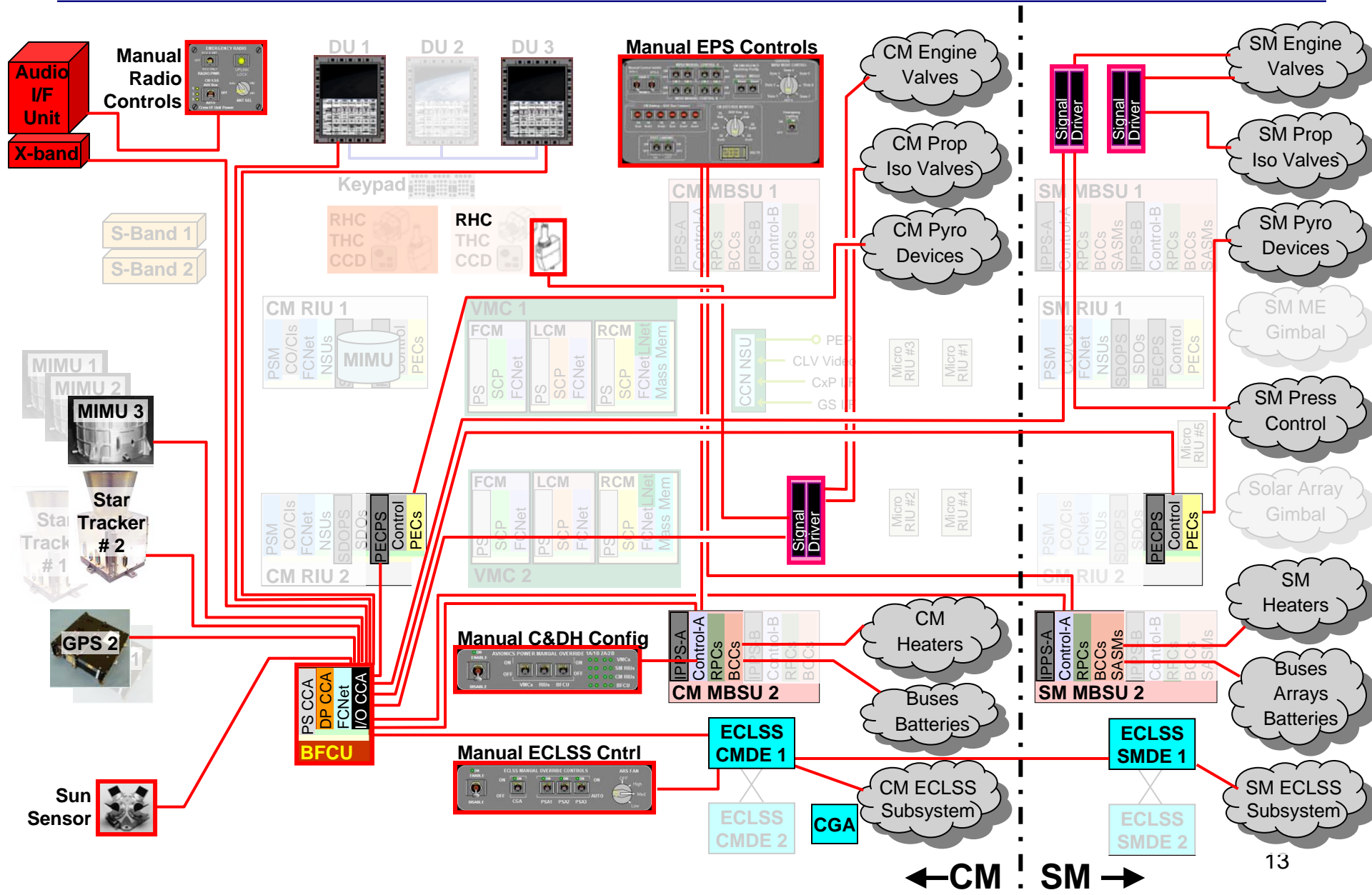
- Nominal
- Primary
- Backup**
- Low Power
- Survival





Emergency Low Power Mode Diagram

- Nominal
- Primary
- Backup
- Low Power**
- Survival





Emergency Survival Mode Diagram

- Nominal
- Primary
- Backup
- Low Power
- Survival**

