

NASA

HEAVY LIFT VEHICLE (HLV) FLIGHT COMPUTING ARCHITECTURE STUDY

Study Team Members

NASA

■ CORE TEAM

- Bob Hodson – LaRC – Study Lead
- Dwayne Morgan – WFF
- Yuan Chen – LaRC – Reliability Lead
- Marc Butler – KSC – Mass Lead
- Dave Gwaltney – MSFC
- Joe Schuh – KSC
- Lisa Coe – MSFC
- Jen Petelle – KSC – Software Lead
- Hai Nguyen – JSC
- Robert Decoursey – LaRC
- Terry Koelbl - MSFC (ex officio)

■ ADDITIONAL SUPPORT TEAM

- Philip Youmans – KSC
- Mark Monaghan - KSC
- Amanda Gillespie – KSC
- Duane Pettit – LaRC
- Spence Hatfield - MSFC



Participation from
5 NASA Centers

Overview

NASA

- Study Scope
- Approach
- DRMs & Requirements
- Architectures
- Results
 - Reliability Analysis
 - Power Analysis
 - Mass/Harnessing Analysis
 - HW/SW Redundancy Management Approaches
- Findings
- Feedback Q&A

Study Scope & Goals

NASA

- The SLS Flight Computing Architecture Trade will examine multiple launch vehicle avionics architectures and assess the trade space considering reliability, fault-tolerance, mass, and other factors. Self-checking, voting and other architectural variants will be traded.
- The study team will examine the current DRMs and requirements to best determine key driving requirements for the flight computing architecture. In the absence of information, assumptions will be explicitly stated.
- A goal of the study is develop tools and skills to rapidly assess additional architectures should requirements or assumptions change.
- The study team will report on the architectures assessed and associated data/findings for review and comment by the broader avionics community. Feedback will be incorporated and management will be briefed.
- Out of the initial scope
 - Non-flight computing systems (DFI, FTS, Comm, Power systems, etc)
 - Backup-Flight Systems

Technical Approach

NASA

- ✓ ■ Review of DRMs
- ✓ ■ High Level Requirements Review
 - Identify avionics drivers
- ✓ ■ Review Ares V “strawman” architecture
- ✓ ■ Simplify Ares V architecture and use as a basis for instrumentation and a baseline architecture for comparison
- ✓ ■ Develop candidate set of computing architecture
 - Various Voting & Self-checking Configurations

Technical Approach

NASA

- Assess/Analyze Architectures
 - ➡ ■ Reliability (5 of 6 complete)
 - ✓ ■ Fault tolerant characteristics
 - ✓ ■ Mass (harness complexity)
 - ✓ ■ Power
 - ✓ ■ Hardware/Software Approaches
- ➡ ■ Document and report out to the avionics community and management
 - Incorporate feedback
 - Iterate as needed

A cosmic background featuring a large, dark, cratered planet on the left, a smaller planet in the upper right, and a vibrant nebula with pink and purple hues on the right side.

DRMS & REQUIREMENTS

DRMs & Requirements

NASA

- Reference Missions & Requirement Guidance
 - Proposed HEFT Crewed NEO Missions
 - MARS Reference Missions
 - Space Launch Systems (SLS) Requirements Analysis Cycle guidance
 - Constellation Avionics Driving Requirements
 - Commercial Crew Transportation Systems Certification Requirements
 - NASA Human-Rating Requirements for Space Systems
- Key Driving Requirements
 - The avionics architecture must be human-rateable
 - The avionics architecture must, at a minimum, be fail-operational after one arbitrary fault.
 - The avionics architecture must, at a minimum, fail-safe (for abort initiation) after a second arbitrary fault.
 - The avionics architecture must be highly reliable to meet Loss of Crew (LOC) and Loss of Mission (LOM) for various NASA missions.

ARCHITECTURES



Architecture Studied

NASA

■ Initial Architecture Candidates

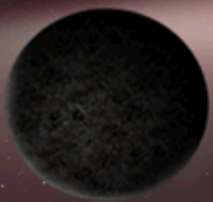
1. Fully Cross-Strapped Switched Triplex Voter
2. Partially Cross-Strapped Switched Triplex Voter
3. Triplex Voter with Self-Checking Switches
4. Channelized Bussed Triplex Voter
5. Bussed Triplex Voter w/o Cross-strap
6. Channelized Bussed Triplex Voter
7. Fully Cross-Strapped Switched Self-Checking
8. Fully Cross-Strapped Bussed Self-Checking
9. Channelized Bussed Self-Checking
10. Self-checking processors, separate busses
11. Self-check pairs (high level)
12. Bussed Triplex Voter

■ Selected Architectures

1. Fully Cross-Strapped Switched Triplex Voter (FCSSTV)
2. Partially Cross-Strapped Switched Triplex Voter (PCSSTV)
3. Channelized Bussed Triplex Voter (CBTV)
4. Fully Cross-Strapped Switched Self-Checking (FCSSC)
5. Fully Cross-Strapped Bussed Self-Checking (FCSBSC)
6. Channelized Bussed Self-Checking (CBSC)

3 Voter, 3 Self-Checking
3 Switched, 3 Bussed
Highly Channelized, Partially & Fully
Cross-Strapped Architectures

"Generic" Stage Elements

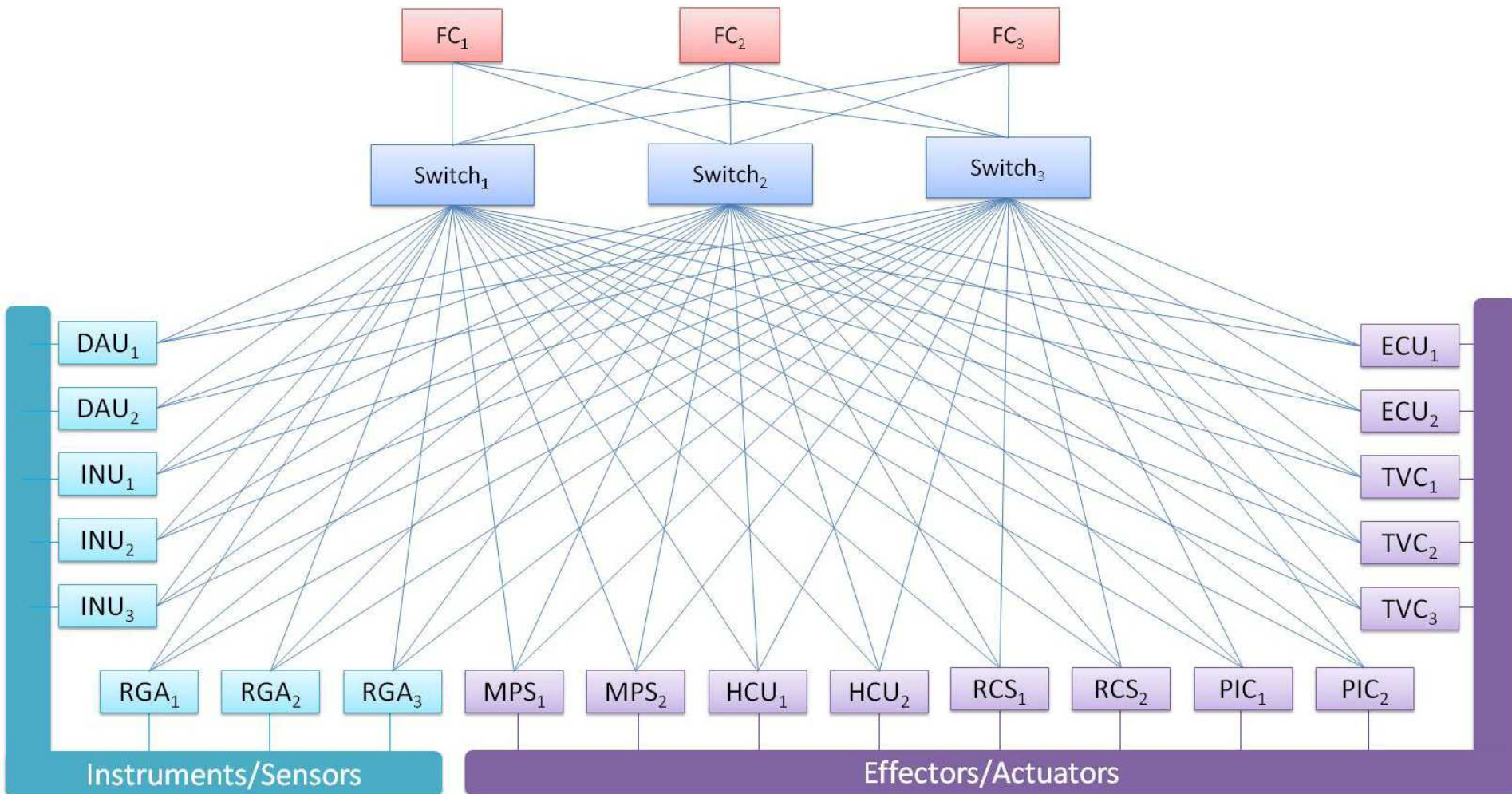


NASA

Unit Acronym	Unit Name	Qty	Min Req.	Function
RGA	Rate Gyro Assembly	3	2	Provides pitch and yaw rate measurements
INU	Inertial Navigation Unit	3	2	Provides acceleration in three axes and angular rates for roll pitch and yaw
DAU	Data Acquisition Unit	2	1	Provides excitation/measurement for sensors for critical system control and monitoring. Since there are only 2 DAUs, for sensor measurements, lower level redundancy is assume to ensure sufficient data integrity.
ECU	Engine Control Unit	2	1	Receives Commands from the FC for engine control and provides the FC with pertinent data for engine control and monitoring
TVC	Thrust Vector Controller	3	2	Receives commands from the FC to command the thrust vector control actuators to the proper position. Provides the FC with pertinent data for TVC actuator control and monitoring
MPS	Main Propulsion System	2	1	Receives commands from FC to control flow of fuel and oxidizer. Provides the FC with pertinent data for MPS control and monitoring (CLSS is part of this).
RCSC	Reaction Control System Controller	2	1	Receives commands from FC to control reaction control jets. Provides the FC with pertinent data for RCS control and monitoring
PIC	Pyro Initiation Controller	2	1	Receives commands from the FC to initiate pyro events. Provides the FC with pertinent data for Pyro circuit monitoring
HCU	Hydraulic Control Unit	2	1	Receives commands from the FC to control hydraulic power generation for the TVC actuator. Provides the FC with pertinent data for Hydraulic Power system control and monitoring

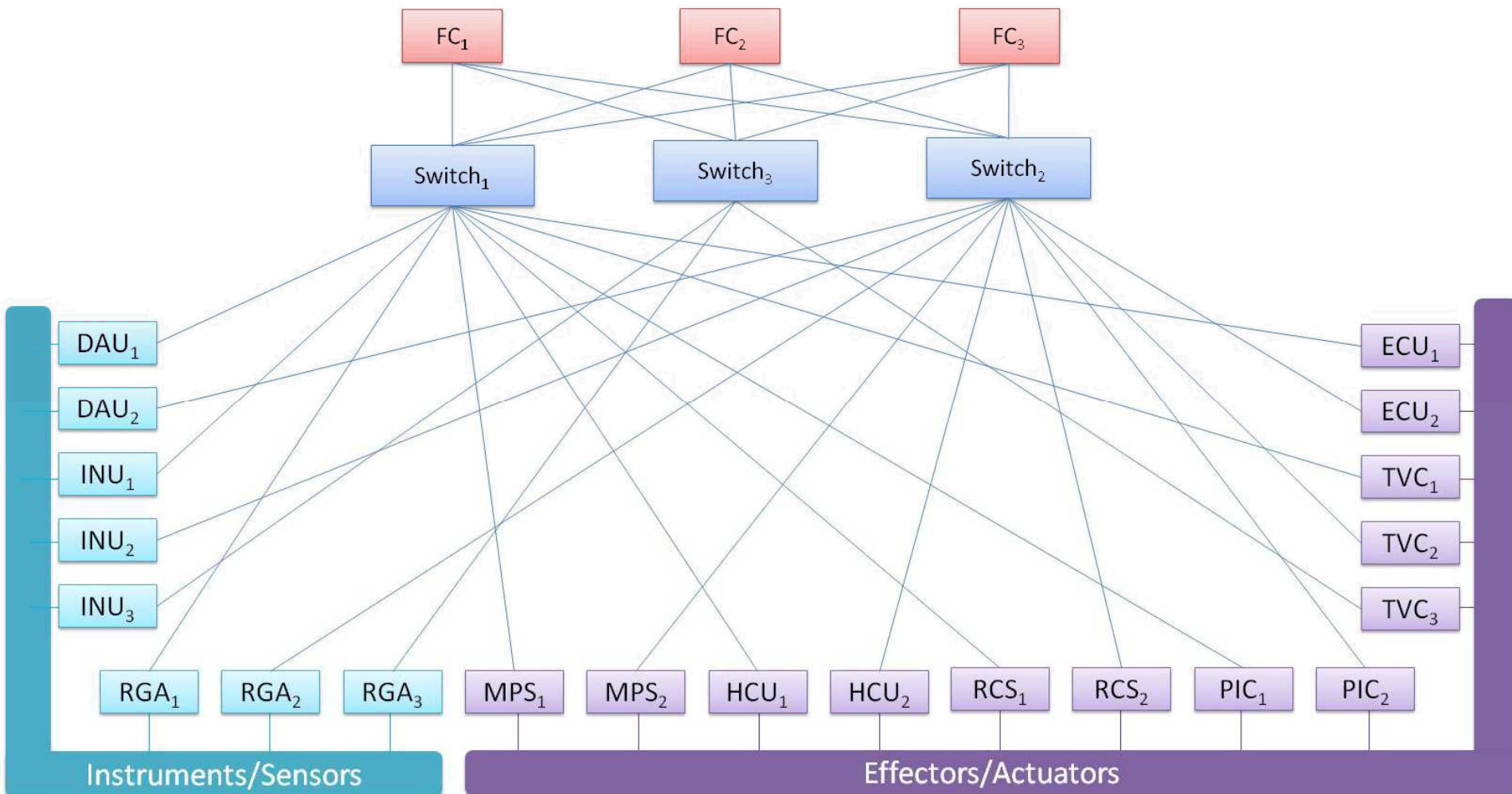
FCSSTV: Fully Cross-Strapped Switched Triplex Voter

NASA



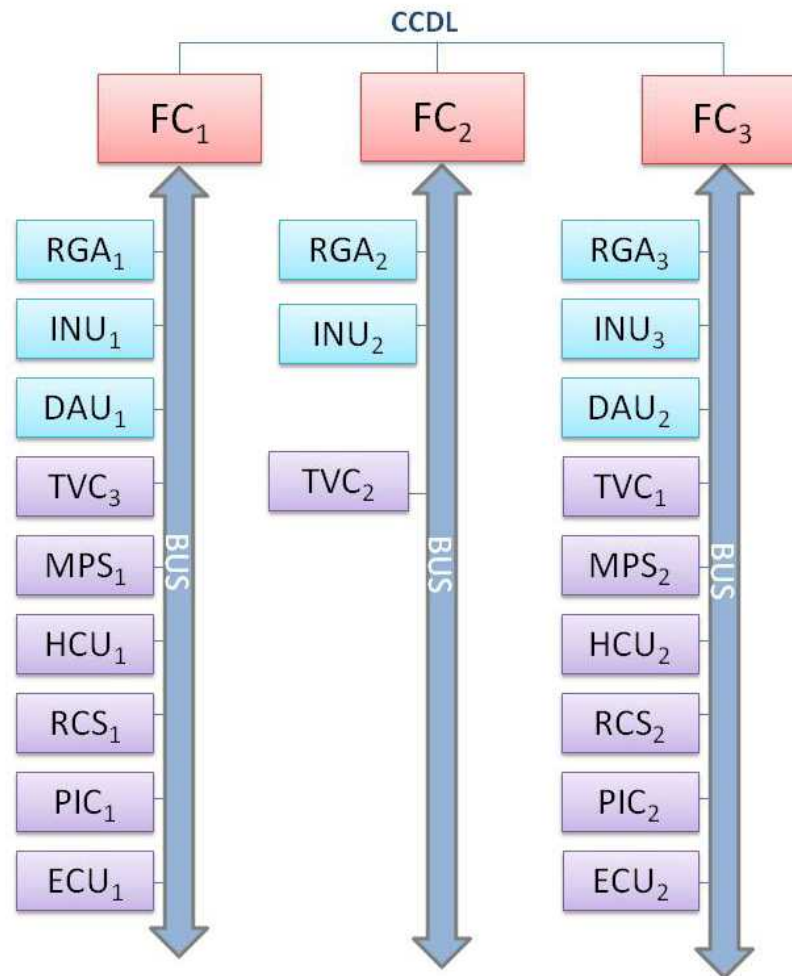
PCSSTV: Partially Cross-Strapped Switched Triplex Voter

NASA



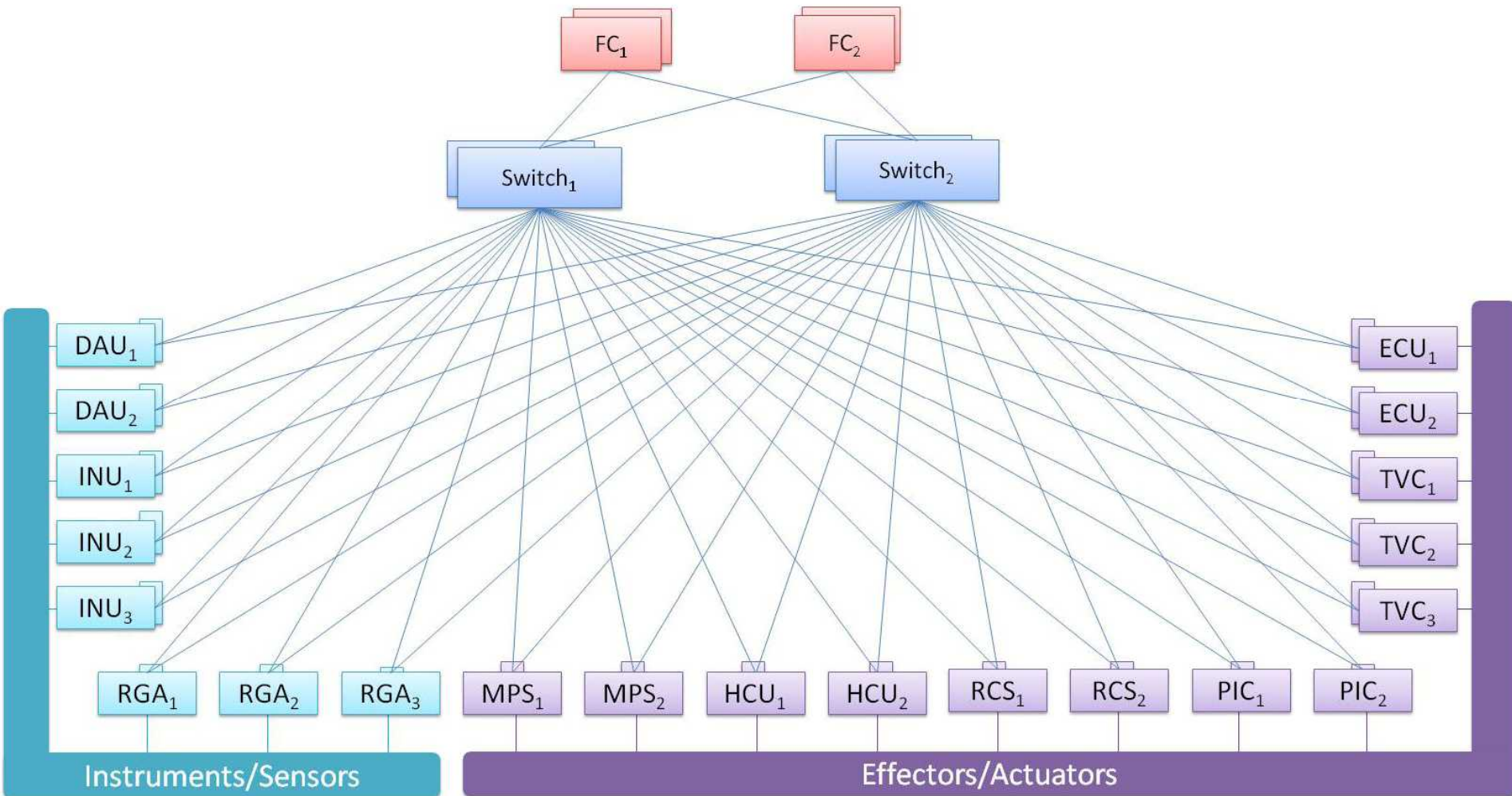
CBTV: Channelized Bussed Triplex Voter

NASA



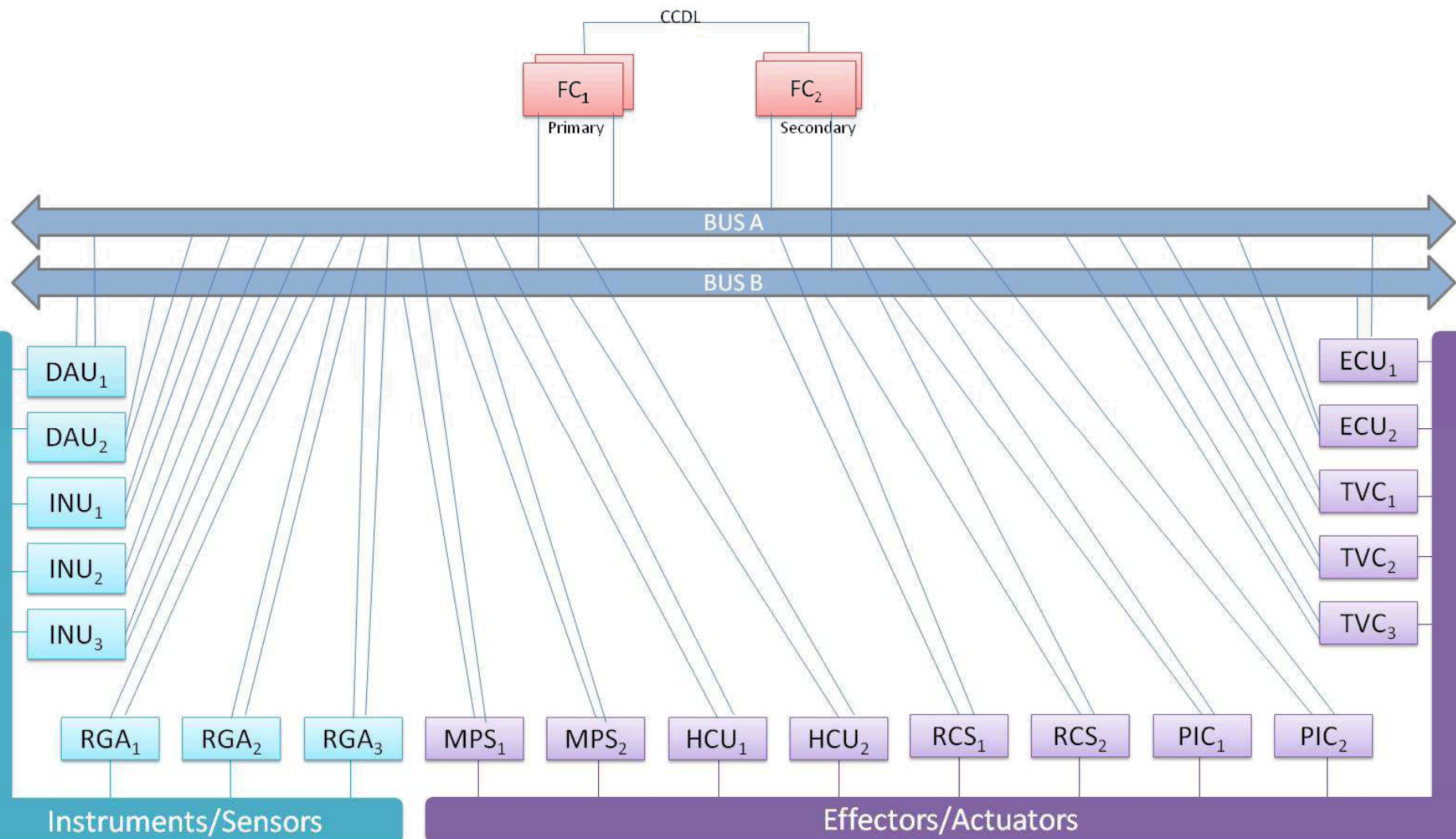
FCSSC: Fully Cross-Strapped Self-Checking

NASA



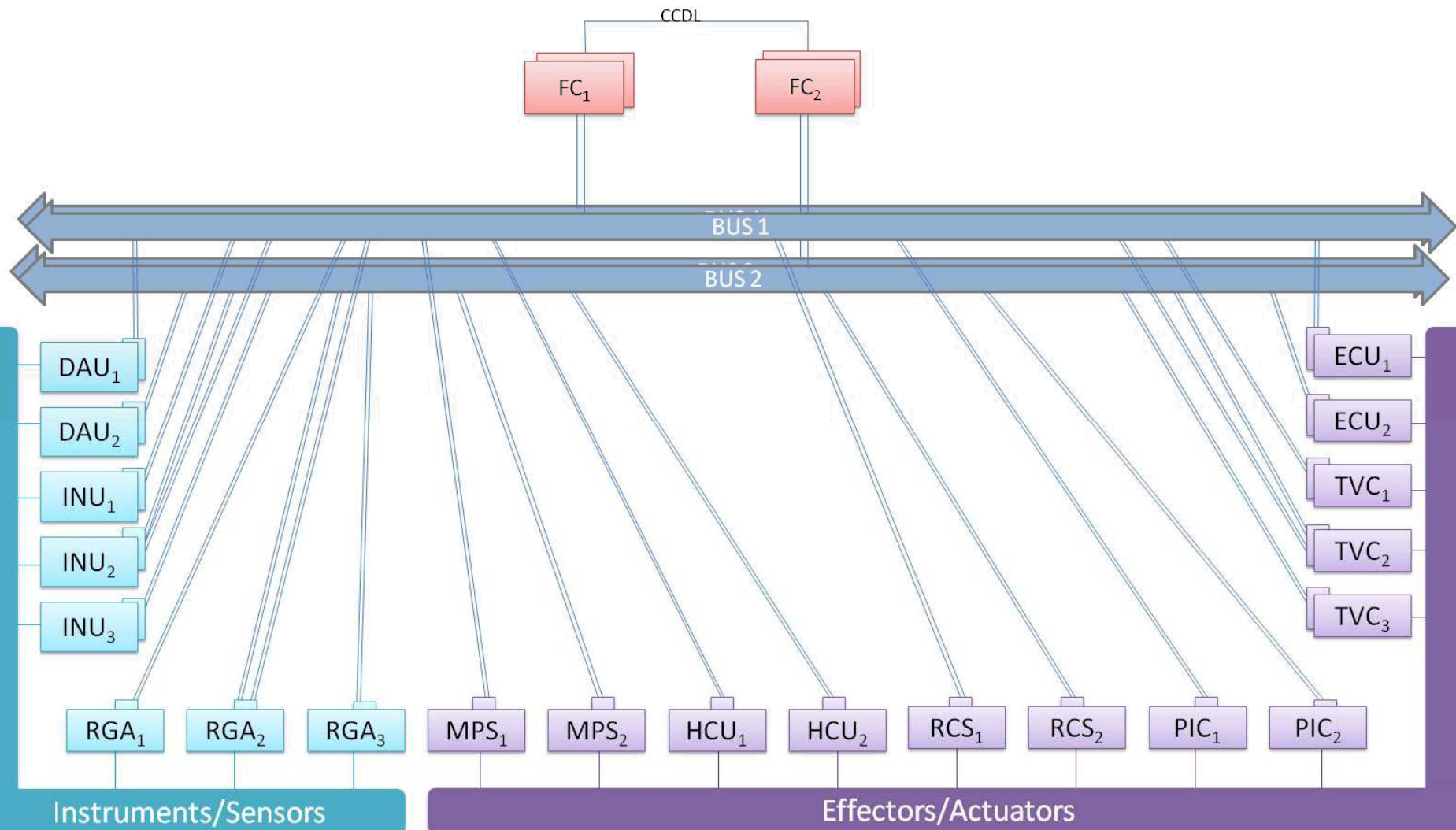
FCSBSC: Fully Cross-Strapped Bussed Self-Checking

NASA



CBSC: Channelized Bussed Self-Checking

NASA



Architecture Assumptions/Comments



NASA

- All architectures are capable of having Byzantine resilient implementations with the given connectivity and redundancy
- Integrity mechanisms vary (self-checking, voting, CRCs, sequence numbers, guardian functionality, etc), assumptions are not presented here but critical for robust implementation – more detail will be provided in the report
- Data flow diagrams for all architectures is not presented here – more detail will be provided in the report

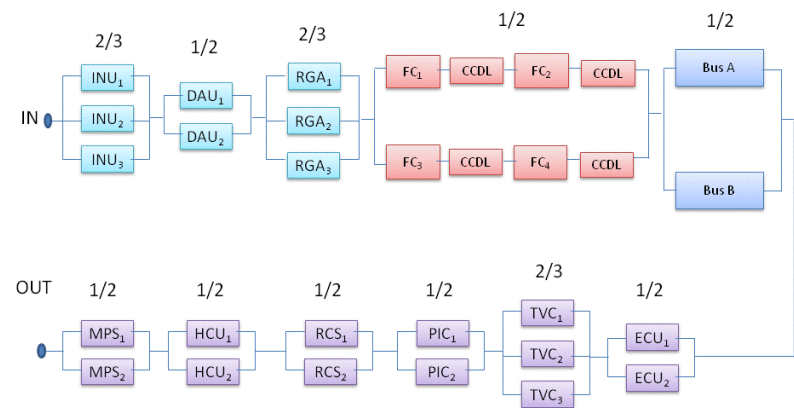


RELIABILITY

Architecture Reliability Analysis

■ Approach

- Develop multiple reliability models and compare results to validate approach
 - Monte Carlo simulation by Relex: 1 million Relex simulation runs.
 - Analytical calculation by Excel: Reliability diagram approach.
- Model architectures with and without cabling
- Perform cut set analysis
- Perform failure probability distribution analysis

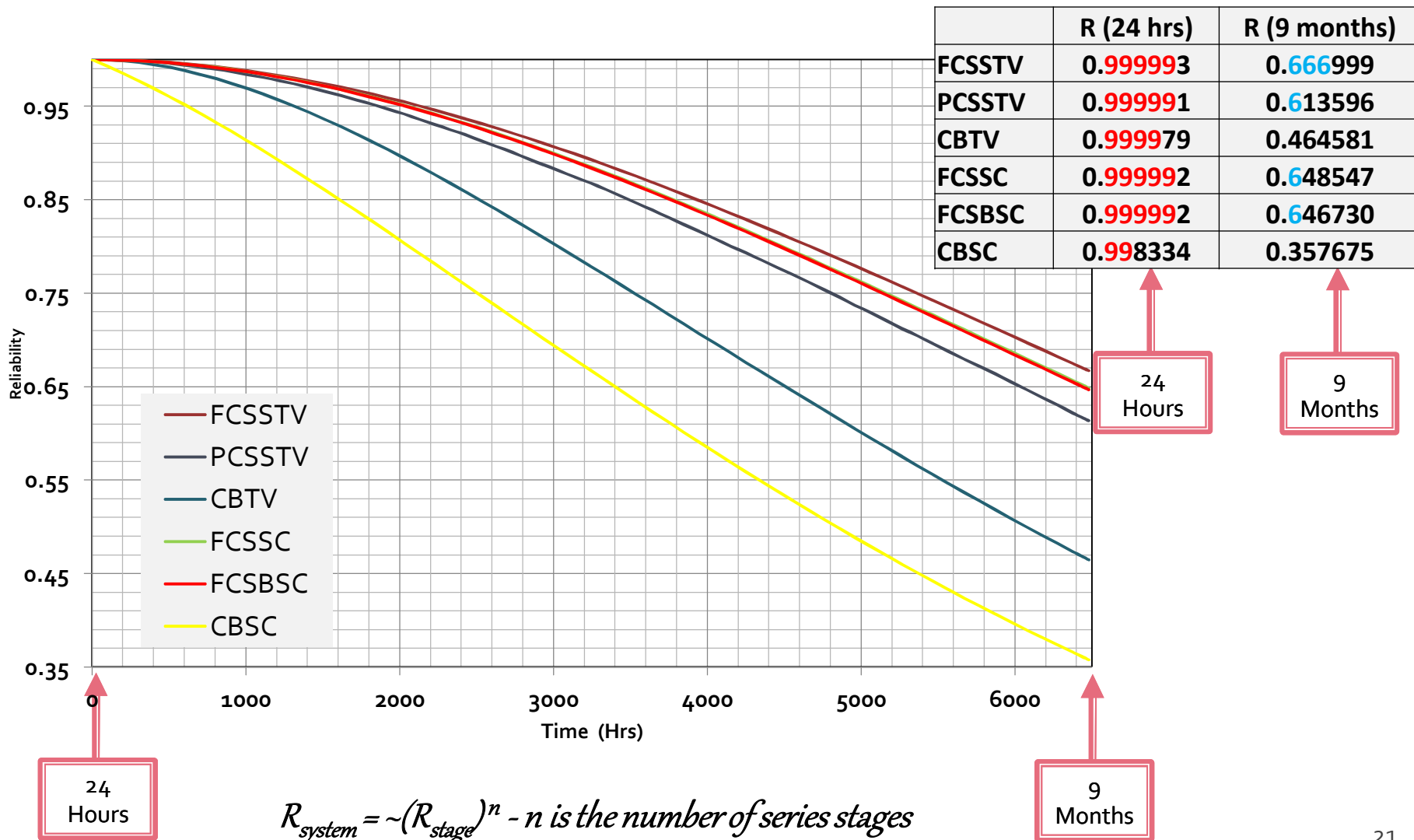


■ Assumptions

- Used MTTF from exiting data sets of comparable hardware items
- Time duration: up to 9-month. 24hours point assessed for “short duration” mission
- Only hard or non-recoverable failures are considered for this analysis.
- For Flight Computers (FCs) and Switches, self-checking pair consists of two FCs or two switches. For other functional units, self-checking pair consists one functional unit plus a self-checking logic.
- Assume one fault tolerance for all functional unit groups.

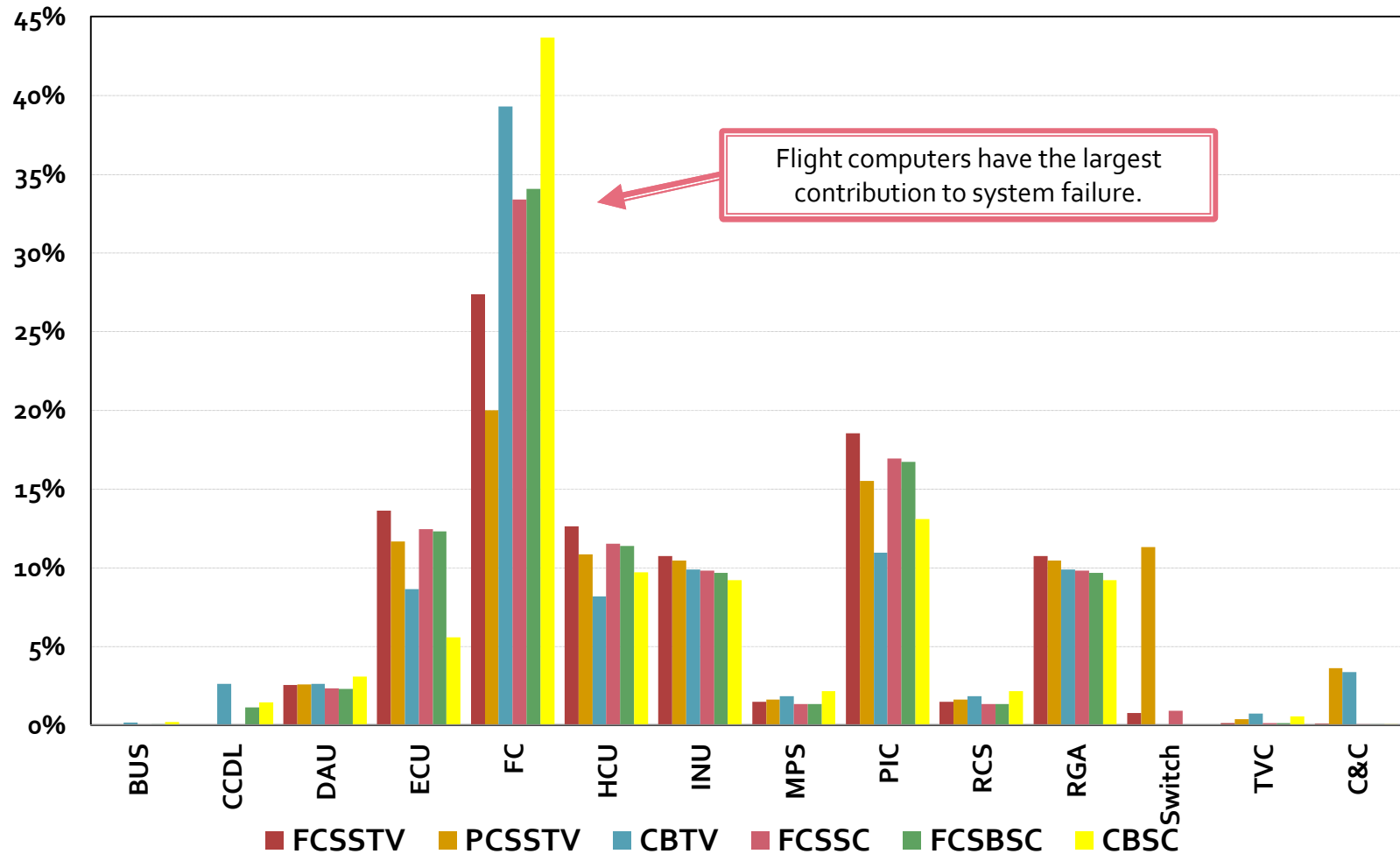
Avionics Reliability Plot for a HLV Single Stage

NASA



Functional Unit Failure Probability Contributions

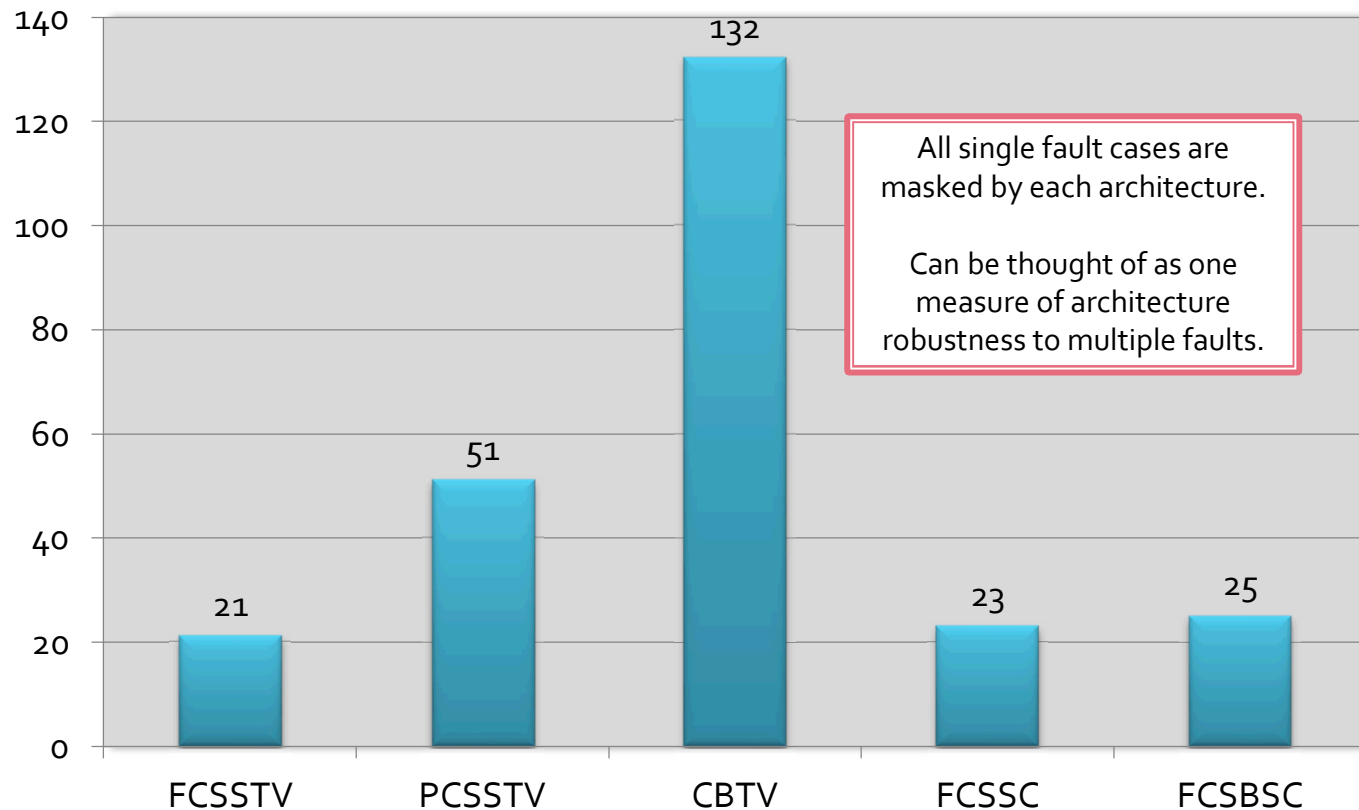
NASA



Cut Set Analysis – 1 & 2 fault failures

NASA

Number of 2-Fault Failure Combinations



POWER



Power Analysis

NASA

■ Approach

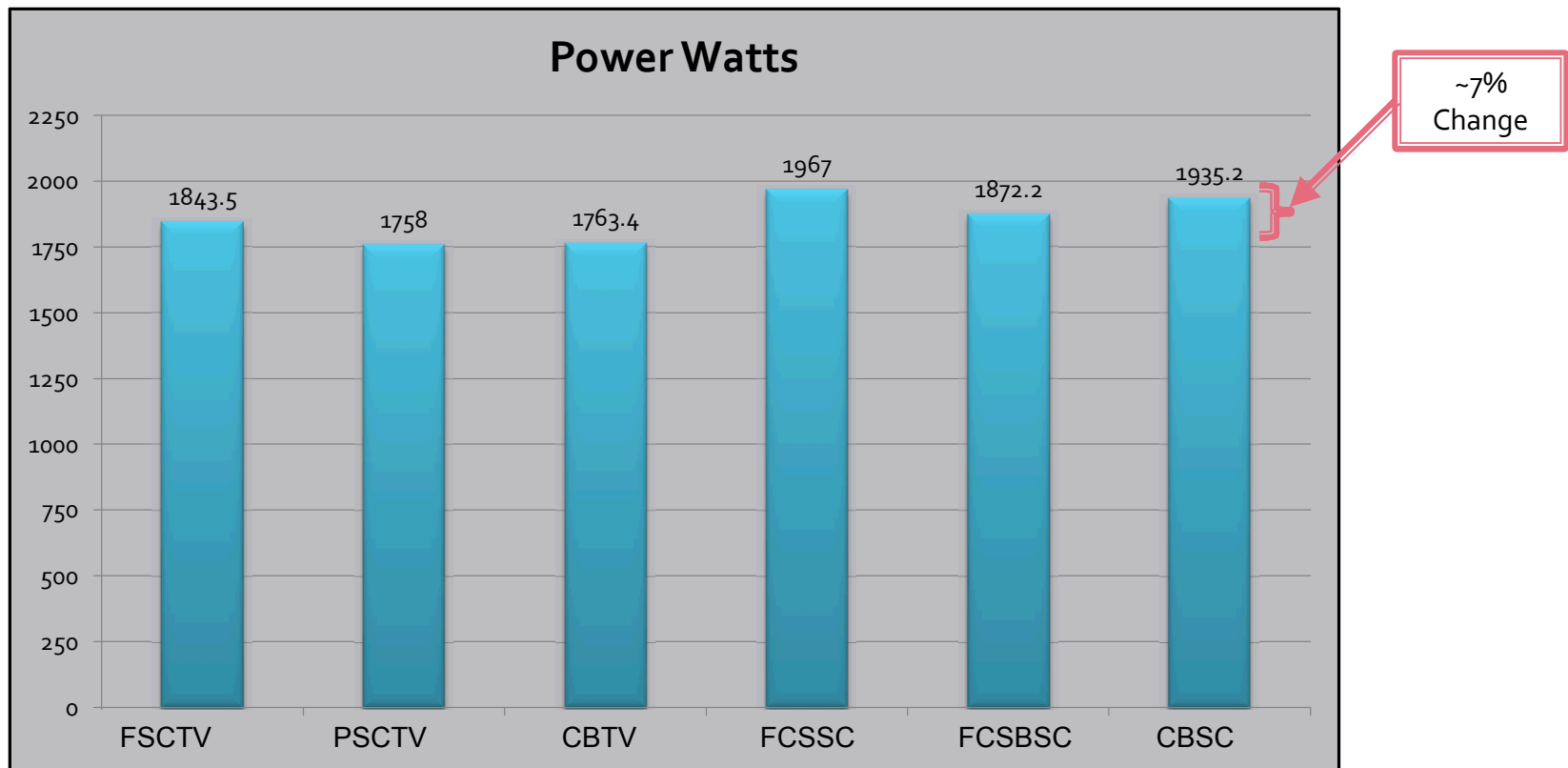
- Determine individual component power specifications (LRUs, 1553 Busses, Switches)
- Determine number of components and calculate total Integrated architecture power.
- Analytical calculation by Excel: Graph Results.

■ Assumptions

- Functional LRU Power (WATTS) based on prior power consumption for ARES I LRUs.
- Switch Power based on size or number of ports served.
- Calculations done for a single stage

Power Analysis for HLV Single Stage

NASA





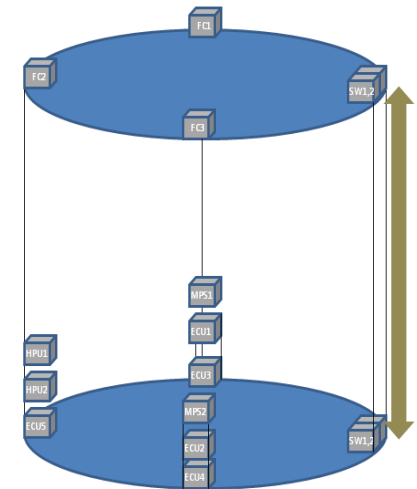
HARNESS MASS

Harness Mass Analysis

NASA

■ Approach

- Model a generic core stage inline heavy lift design with cores stage circular dimensions; (Vertical Length of 215.3' and a Diameter 27.5')
- Incorporates an upper stage avionics ring; lower stage/aft skirt avionics ring; and a specific number of functional avionic units necessary for ascent to LEO.
- Position fundamental avionic units for the upper and lower avionic rings and calculate the cable lengths based on the 6 fundamental architecture layouts, Cross Strapped, Partially Cross Strapped, and Single String.
- Analytical calculation within Excel to determine mass: Graph Results.

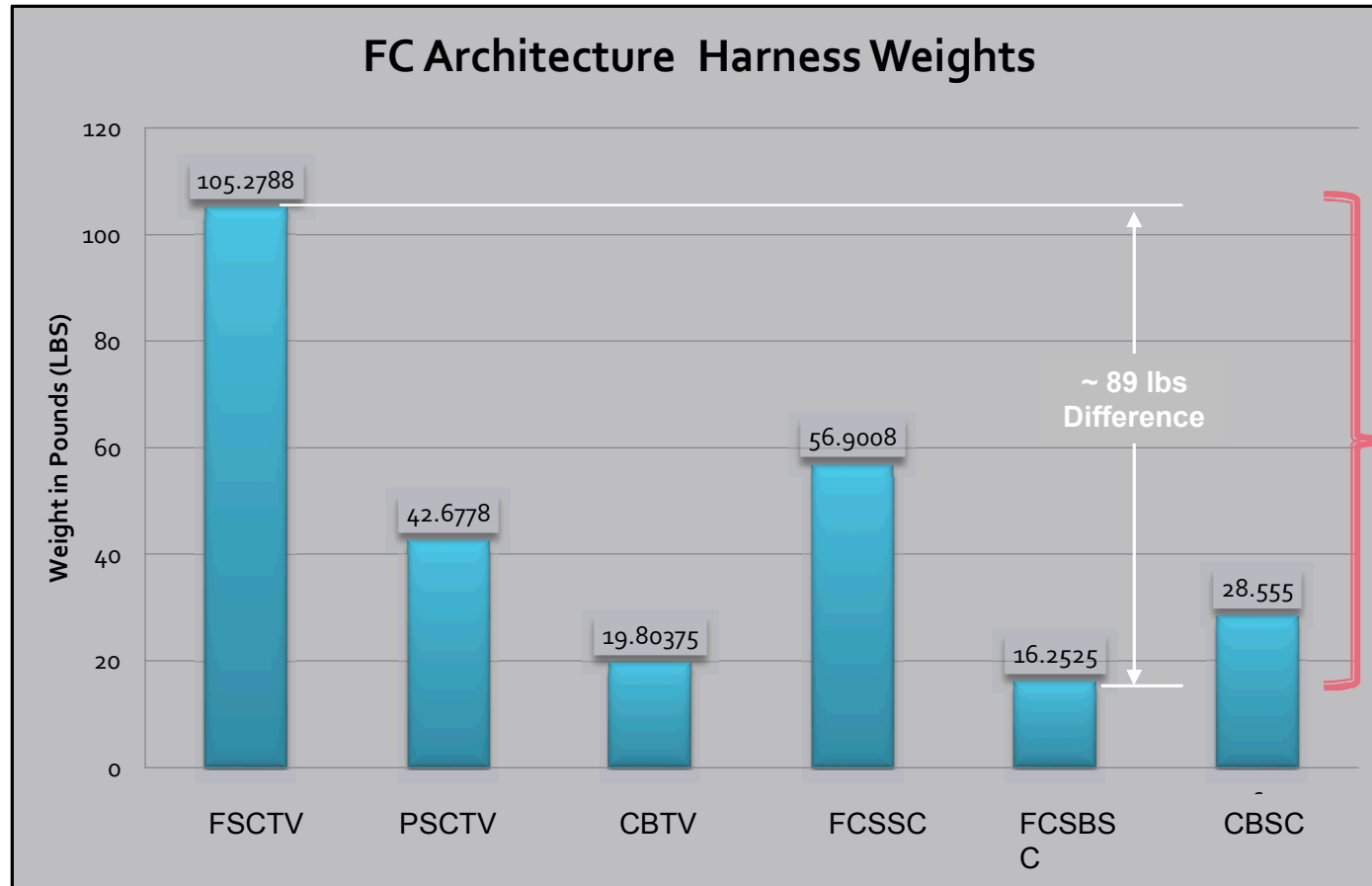


■ Assumptions

- No additional avionics or functional units for boosters or 2nd stage/payloads were considered for the analysis.
- Used 1000BASE-T Twisted-pair cabling (Cat-5, Cat-5e, Cat-6, or Cat-7) at a 100 meter max drive length for the architectures that utilized a switched network.
- Use 1553 cabling as the bus for the bussed architectures

Harness Mass Analysis Results for a Single Stage

NASA



Architectures selection contributes approximately 2% to 9% of avionics harness mass.

HW/SW REDUNDANCY

The background of the slide is a deep space scene. On the left, a large, dark, cratered planet or moon is partially visible. In the upper right, a smaller, dark sphere is seen against a bright light source, creating a lens flare. The background is filled with a colorful nebula in shades of purple, pink, and blue, with numerous small white stars scattered throughout.

HW/SW Redundancy Management Approach

NASA

- Reviewed existing architecture implementation details
 - Shuttle
 - Delta IV
 - Atlas
 - LaRC SPIDER
 - X-38
 - Orion
- Examined the redundancy management and synchronization schemes
 - Systems include both voters and self-checking
 - 4 voters, 2 self-checking
- Examined the implementation approach (HW vs SW) for each case

HW/SW Redundancy Management Observations



NASA

- Implementations varied widely
 - From all in HW to mostly SW
- Understanding implementation details are critical
 - Hardware support can simplify SW (i.e. Self-checking fault detection, hardware-level consistency exchanges for voters) but at the expense of HW complexity
 - Software synch can potentially be affected by other SW design changes
 - Byzantine resilient synch and interactive consistency exchanges can be complicated and challenging to implement in HW or SW
- A balance between HW and SW seems reasonable
 - SW adds flexibility but allows for requirements/schedule creep
 - Makes sense to put mechanisms in HW and policies in SW
 - i.e. detect failure in HW but put what to do in SW

Summary of Preliminary Findings

NASA

■ Reliability

- Multiple architectures (both self-checking and voting) are highly reliable for short duration a short duration HLV mission
- For long duration mission (9 month), channelized architectures have significantly lower reliability
- Cut set analysis shows some architectures as being more robust to 2nd faults
- Flight computer reliability is the biggest contributor to system reliability calculations

■ Power

- Architectural differences result can result in up to 7% difference in power
- No significant power difference between self-checking and voting systems

■ Flight Data Network Harness Mass

- Mass ranges determined were between 16 lbs to 105lbs, which is 2% to 9% percent of the total estimated cable/harness weight for a heavy lift vehicle (assuming ~1200lbs – single stage)
- Cable weight was a function of cross strapping and not a function of the Flight Computer (Self-checking vs Voter)

■ HW/SW Redundancy Management

- Approaches studied varied widely in SW/HW implementation
- Synchronization and interactive consistency exchanges can be complicated and challenging to implement in HW or SW



BACKUP

Potential Future Work



- Effect of scaling for long duration missions
- Consideration of additional architectures
- Further analysis of cut-set results
- Effect of adding additional Flight Computers
- Model intermediate states to include the impact of reconfiguration and data integrity on the reliability
- Analyze differences between Relex and SAPHIRE for reliability analysis
- Power analysis could have a higher fidelity once an architecture is selected and all avionic components have been identified.

Failure Rate (FR) Sensitivity

NASA

