National Aeronautics and Space Administration

Christopher Marchant

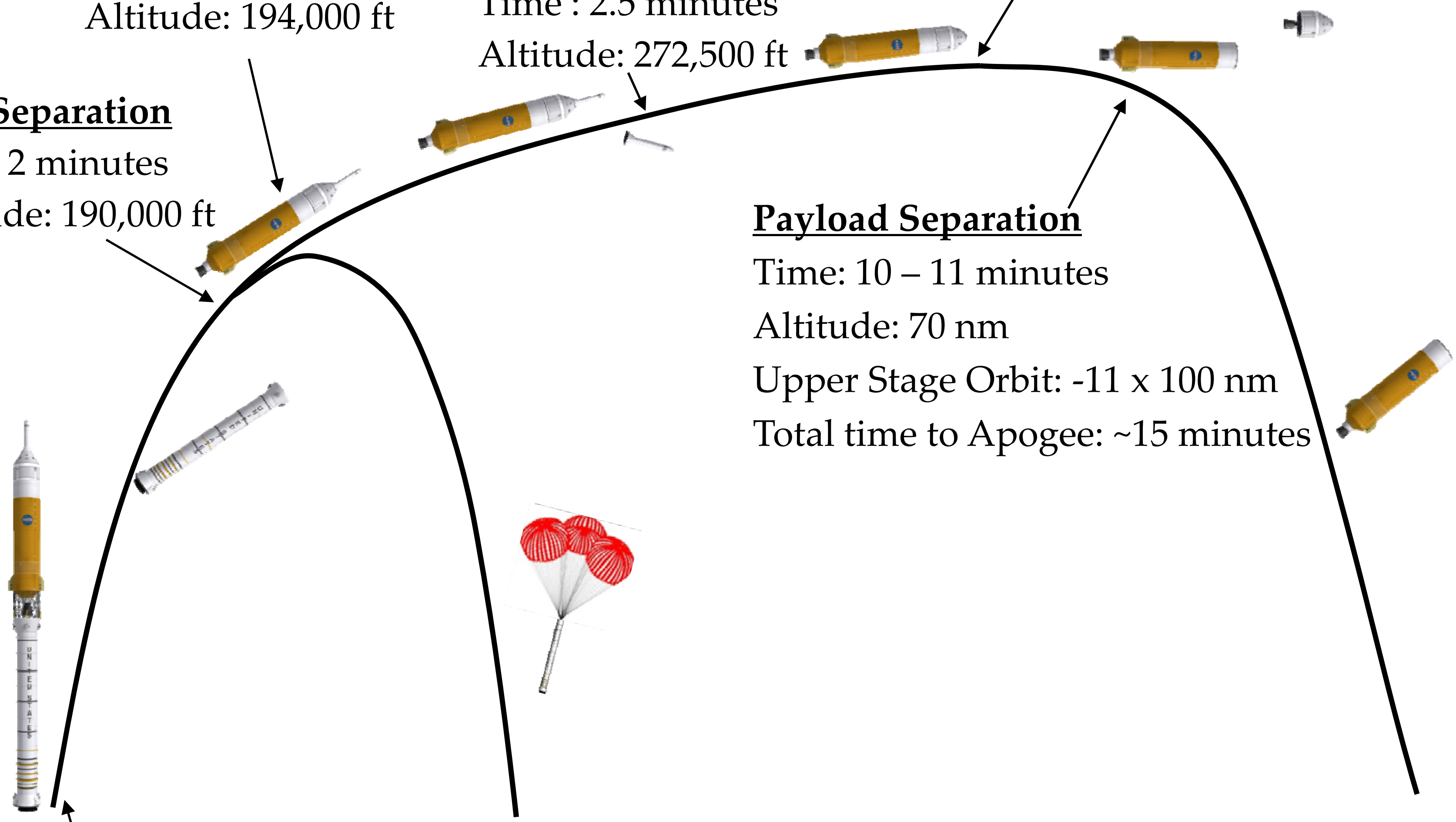
Ares I Avionics Introduction

www.nasa.gov

Presentation Outline

- ♦ Ares I Architecture Overview
- ♦ Human Rating Requirements
- ♦ Ares I *Avionics* Architecture Overview
- ♦ Maintaining Critical Functionalities through Redundancy

Reference Mission Timeline



Upper Stage (J-2X) Engine Start

Altitude: 194,000 ft

SM Panel and LAS Jettison

Time : 2.5 minutes

Altitude: 272,500 ft

Main (Upper Stage) Engine Cutoff (MECO)

SRB Separation

Time: 2 minutes

Altitude: 190,000 ft

Payload Separation

Time: 10 – 11 minutes

Altitude: 70 nm

Upper Stage Orbit: -11 x 100 nm

Total time to Apogee: ~15 minutes

Ignition

Time: 0.0 sec

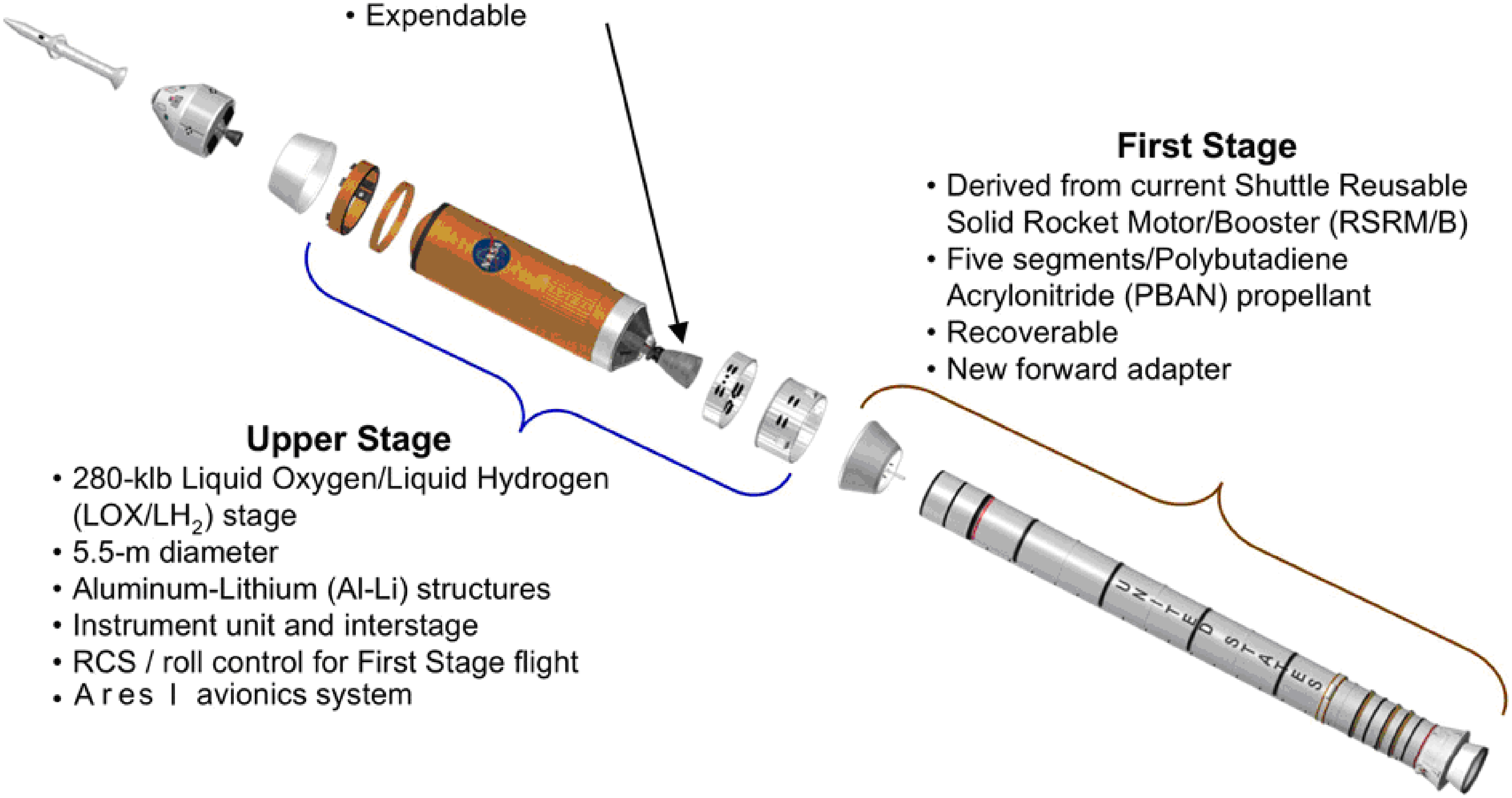
Weight: 2,000,000 lb

1st Stage Splashdown

Upper Stage Impact

(Not To Scale)

Ares I Architecture Overview



Upper Stage Engine

- Saturn J–2 derived engine (J–2X)
- Expendable

First Stage

- Derived from current Shuttle Reusable Solid Rocket Motor/Booster (RSRM/B)
- Five segments/Polybutadiene Acrylonitride (PBAN) propellant
- Recoverable
- New forward adapter

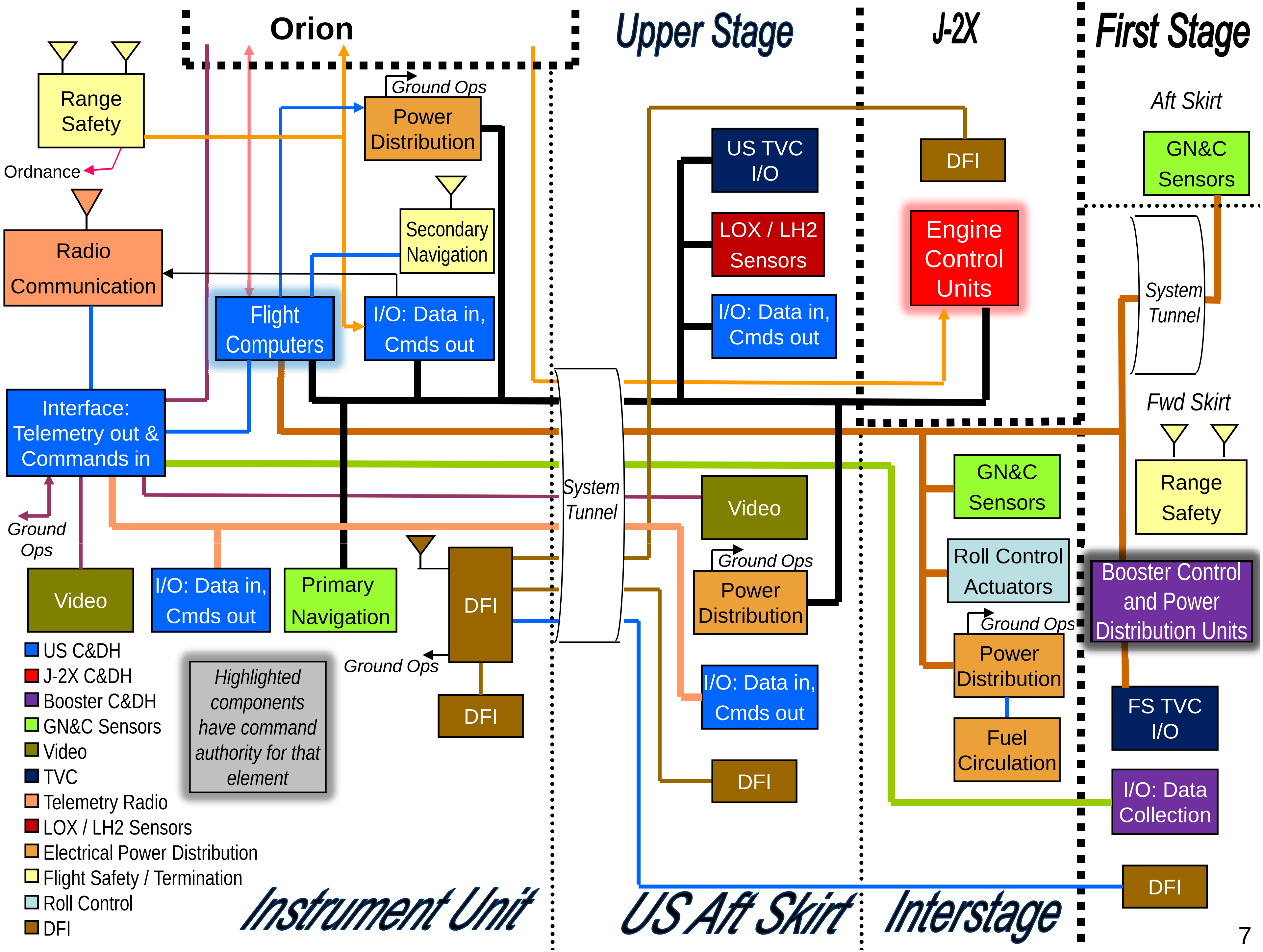
Upper Stage

- 280-klb Liquid Oxygen/Liquid Hydrogen (LOX/LH_2) stage
- 5.5-m diameter
- Aluminum-Lithium (Al-Li) structures
- Instrument unit and interstage
- RCS / roll control for First Stage flight
- Ares I avionics system

Human Rating Requirements

- **As of 2008, the NASA requirements for certain critical systems in new human-rated vehicles have changed to rebalance reducing failure occurrence with maximizing failure containment**
- **From NPR 8705.2B, Human-Rating Requirements for Space Systems:**
  - 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 … . Failure of primary structure, structural failure of pressure vessel walls, and failure of pressurized lines are excepted from the failure tolerance requirement …
- **Based on maximum Ares I flight time, modifying avionics design to single fault tolerance reduced cost and weight without significantly reducing reliability**
- **Shuttle, in contrast, was developed with dual fault tolerance for critical electronics**
  - Shuttle was the first NASA human-rated spacecraft built to those standards
  - Shuttle intended for ~2 week missions; cannot provide crew escape (i.e. land) without working avionics

Major Avionics Functions and Locations



Orion

Upper Stage

J-2X

First Stage

Range Safety

Ordnance

Radio Communication

Ground Ops

Power Distribution

Secondary Navigation

Flight Computers

I/O: Data in, Cmds out

Interface: Telemetry out & Commands in

Ground Ops

Video

I/O: Data in, Cmds out

Primary Navigation

DFI

Ground Ops

DFI

System Tunnel

US TVC I/O

LOX / LH2 Sensors

I/O: Data in, Cmds out

Video

Ground Ops

Power Distribution

I/O: Data in, Cmds out

DFI

DFI

Engine Control Units

GN&C Sensors

Roll Control Actuators

Ground Ops

Power Distribution

Fuel Circulation

Aft Skirt

GN&C Sensors

System Tunnel

Fwd Skirt

Range Safety

Booster Control and Power Distribution Units

FS TVC I/O

I/O: Data Collection

DFI

- 🟦 US C&DH
- 🟥 J-2X C&DH
- 🟪 Booster C&DH
- 🟩 GN&C Sensors
- 🟫 Video
- ■ TVC
- 🟧 Telemetry Radio
- 🟥 LOX / LH2 Sensors
- 🟧 Electrical Power Distribution
- 🟨 Flight Safety / Termination
- □ Roll Control
- 🟫 DFI

Highlighted components have command authority for that element

Instrument Unit

US Aft Skirt

Interstage

Architectural Drivers

- **Use technologies with existing suppliers of space rated parts**
  - MIL-STD-1553B data bus technology used for most critical functions
  - RS-422 used for other high criticality functions
  - Computers contain commercial CPUs and open-standard backplanes
  - Ethernet supplier base being developed for space rated components used in non-critical applications and interfaces external to the Ares I
- **Centralize overall Ares I command & control within the Upper Stage**
  - First Stage and J-2X engine avionics perform data collection, actuator oversight, and local command routing, while the Upper Stage computers maintain system control from terminal launch countdown to Orion separation
- **Minimize mutual connections that might lead to a common-mode hardware failure of the redundant avionics strings**
  - No cross-strapping of data buses
  - No cross-strapping of power
  - Cross-Channel Data Links are independent, point-to-point transmission lines
- **Ease the software development effort by using a commercial off-the-shelf (COTS) operating system for C&DH computers**
  - DO-178B certifiable software that has passed rigorous verification
  - ARINC 653 (time and space partitioning) to separate software modules

Ares I Avionics Architecture Heritage

- **An evolved version of existing/previous systems**
  - Shuttle Data Processing System (DPS)
    - Fly-by-wire control system
    - Four string system
      - All strings share all critical tasks (all strings perform identical/redundant work to produce identical/redundant outputs)
    - Link to Main Engine controllers that each use a pair of self-checking pairs for error detection, error masking, and recovery of function after an error
      - Ares I Upper Stage Engine (J-2X) also expected to use an engine controller based on a pair of self-checking pairs for the same reasons
    - Thrust Vector Control (TVC) actuators vote incoming commands from all strings for fault-tolerance of the steering function
    - Independent strings of attitude control hardware linked to a single avionics bus (each bus is linked to any single flight control computer at a given time)
  - Seawolf submarine Ship Control System
    - Four string, voting system
    - Controlled functions include steering, diving, and depth control
  - X-38
    - Prototype Crew Return Vehicle (ISS lifeboat)
    - Flight control computers form a voting system; one processor per string
    - Maximum automation, minimal reliance on the crew

Systems Timeline

- ♦ **Shuttle – NASA, first flight in 1981**

- ♦ **Seawolf – US Navy, first ship of class commissioned 1997**

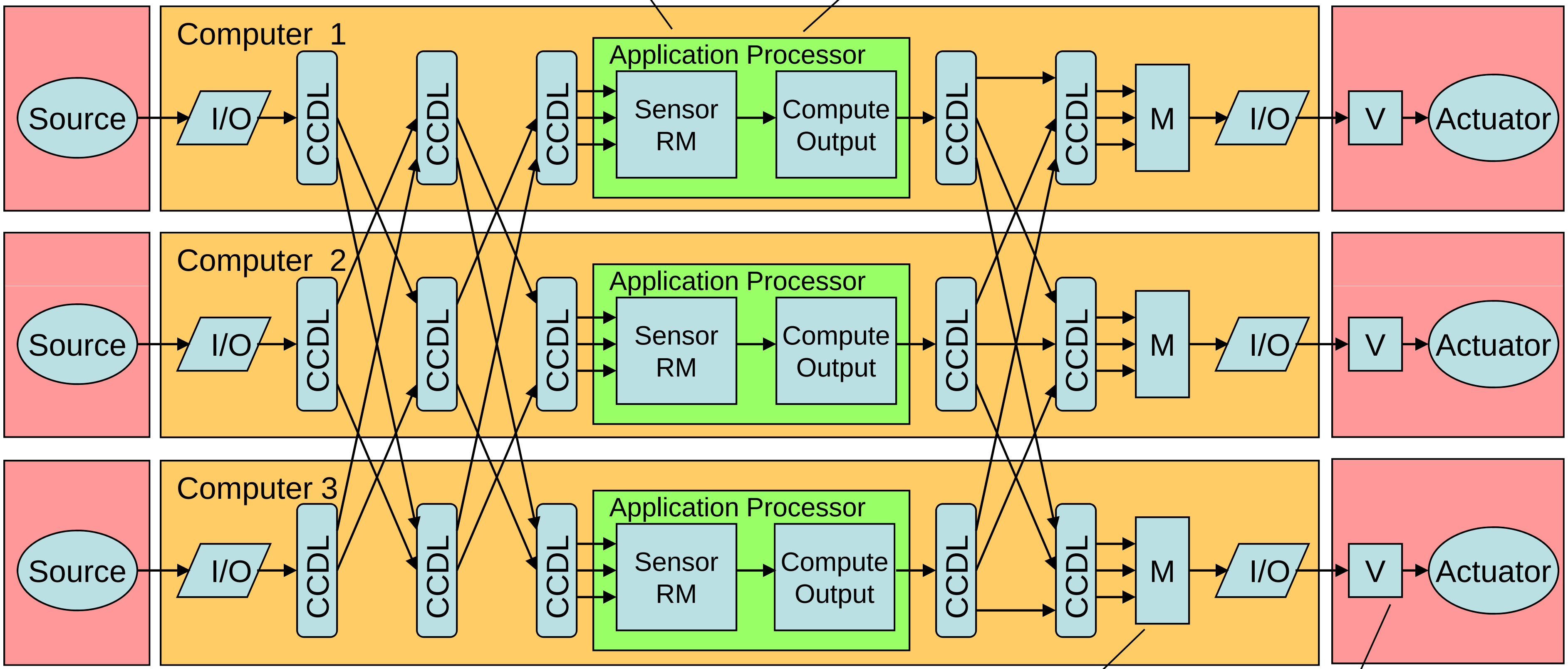
- ♦ **X-38 – NASA, cancelled (after several atmospheric test flights but prior to first space flight) in 2002**

Control System: Redundant Data Sources Feed Cross-Strapped Computers and Detached Actuators

Identical sets of inputs, fed to identical processors performing identical software synchronously, produce identical outputs, as verified by voting. RM filters out input values not universally available, i.e. the Byzantine General's problem

Select input copy to use in computations

Adds checksum, destination, & sequence count to commands for validation



CCDL = Cross-Channel Data Link, **RM** = Redundancy Management, **I/O** = input/output task

M = Majority function (bit-for-bit voting)

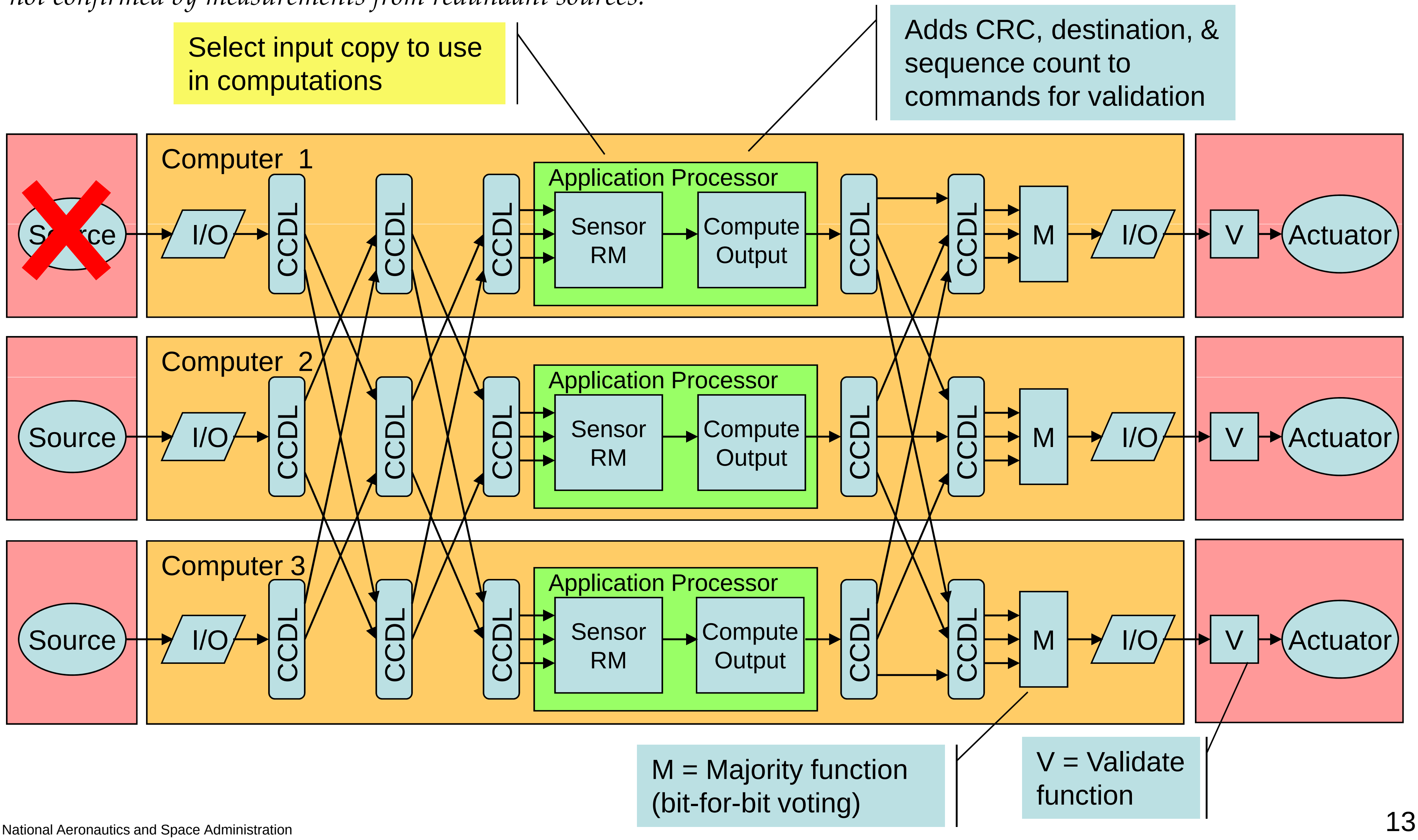
V = Validate function

System Availability through Redundancy

- **Initially, all redundant hardware (strings of hardware):**
  - Is running
  - Shares equal command authority
  - Shares equal actuation authority
  - Shares equal sensing responsibility
  - Receives all redundant copies of all inputs from all redundant strings
- **If a Fault occurs:**
  - Faults are masked or corrected
  - Faults are tracked
- **Fault vs. Failure:**
  - Repeating (contained) faults by the same component show an increased risk for future uncontained failure
  - Faults relating to critical functions or faults not easily masked can be treated as a failure immediately
- **Failure Recovery:**
  - Force the failed component into a benign (often inactive state)
  - Graceful Degradation: Redundant components already in operation continue to provide needed functionality without the need for a formal transfer of control or the delay associated with enabling replacement components

Fault Management: Sensor / Data Source Failure or I/O Collection Failure

Sensor RM function in each computer filters out a data source that sends divergent information via comparison with redundant values and/or application of sensor heuristics. This can detect sensor outputs that at first seem plausible, but are not confirmed by measurements from redundant sources.



Select input copy to use in computations

Adds CRC, destination, & sequence count to commands for validation

M = Majority function (bit-for-bit voting)

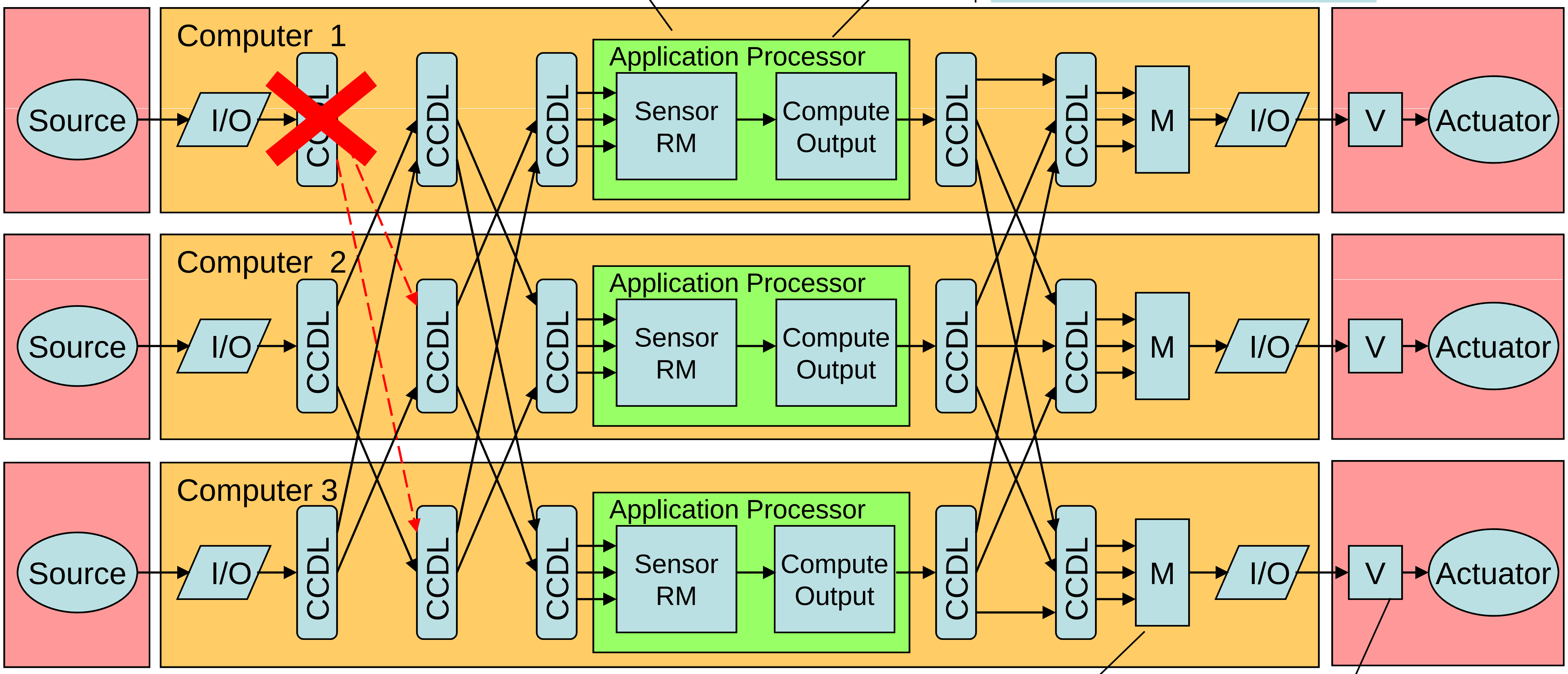
V = Validate function

Fault Management: Error in Data Sharing

The data distributing method based on two-rounds of exchange attempts to deliver copies of data from all redundant sources to each computer. Values not universally available are not used by any computer (e.g. all computers filter out source 1 to avoid the "Byzantine General" problem). Filtering must be done before updating local data stores to maintain uniformity.

Select input copy to use in computations

Adds CRC, destination, & sequence count to commands for validation

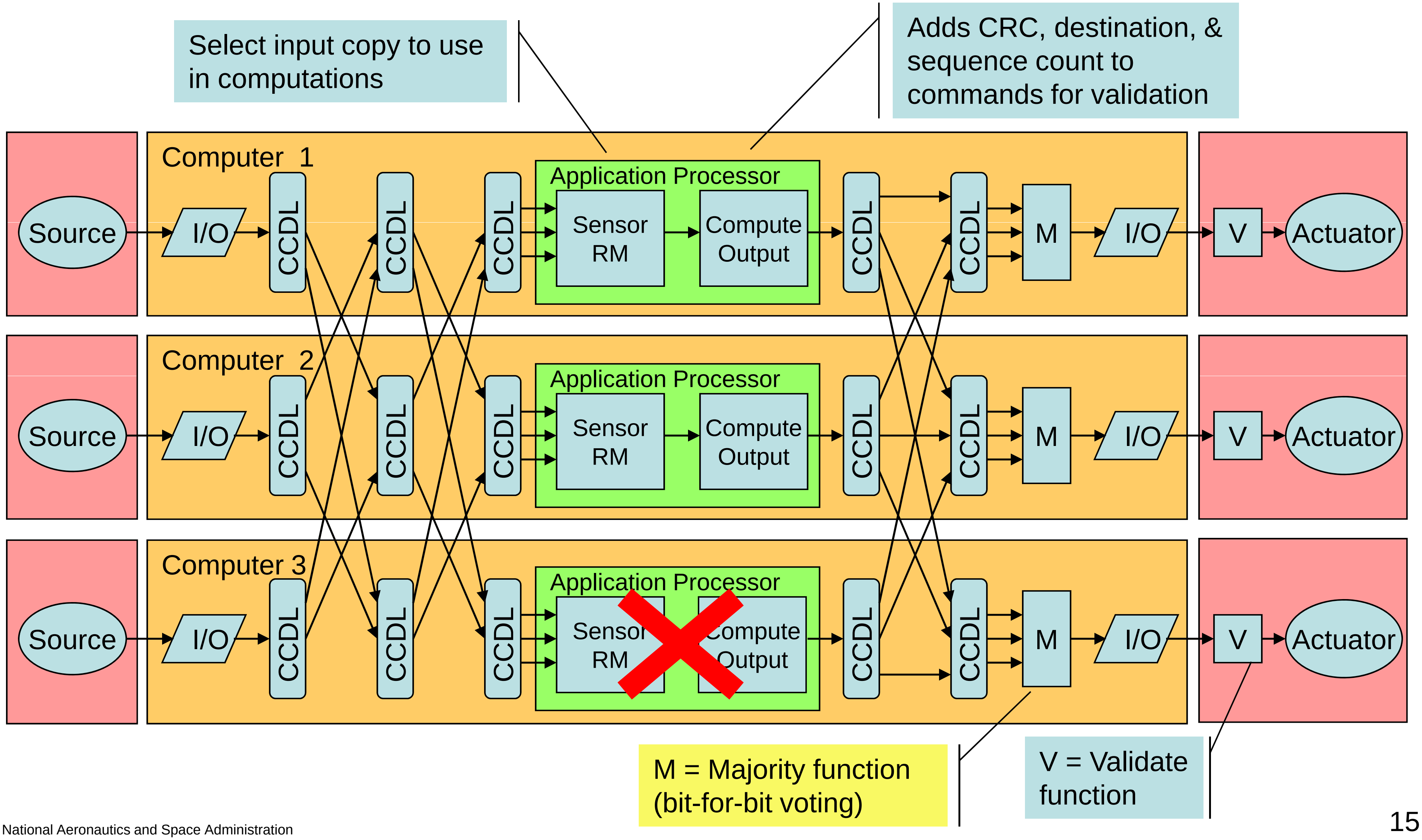


M = Majority function (bit-for-bit voting)

V = Validate function

Fault Management: Failed Application Processor (corrupted memory location, timing sliver, etc.)

Majority voting function only transmits an output if identical copies are generated by 2+ processors. Externally generated outputs replace locally produced versions as necessary.



Select input copy to use in computations

Adds CRC, destination, & sequence count to commands for validation

M = Majority function (bit-for-bit voting)

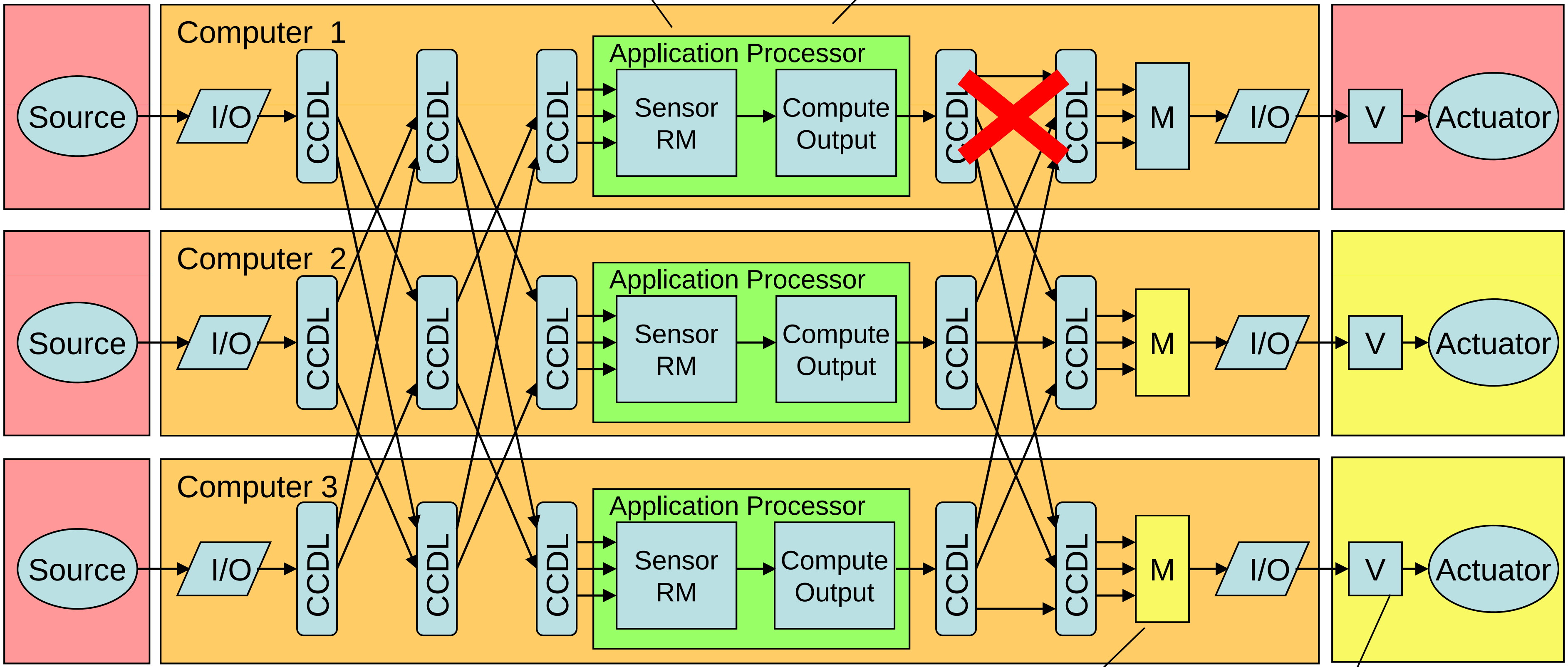
V = Validate function

Fault Management: Recovery from Output Distribution Failure

Should a computer fail to properly distribute an output, redundant outputs from the other computers replace what is missing and/or redundant actuators, with different commanding paths, provide the needed function.

Select input copy to use in computations

Adds CRC, destination, & sequence count to commands for validation



M = Majority function (bit-for-bit voting)

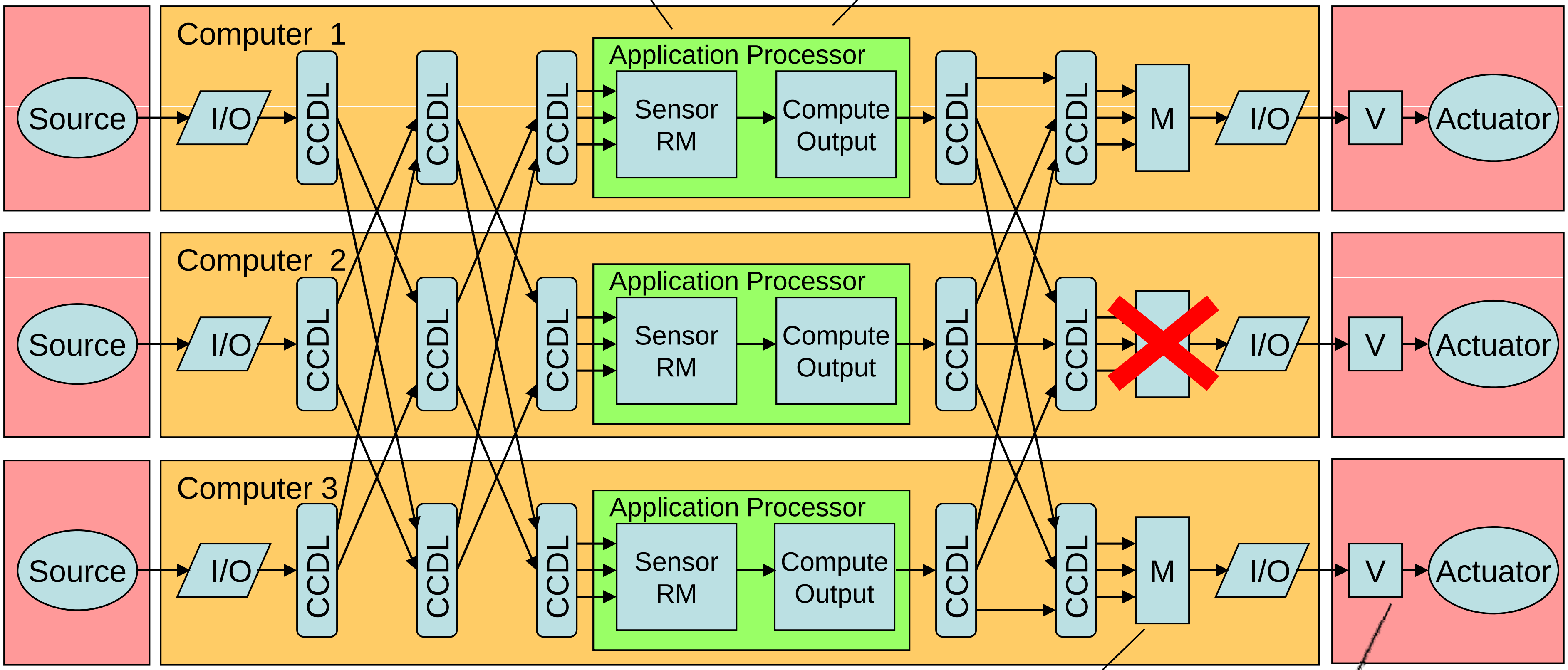
V = Validate function

Fault Management: Output Selection Function Fails

Validate Function rejects any command the Majority voting function has altered, has repeated (a stale output from a previous command cycle), or has misdirected (to the wrong actuator).

Select input copy to use in computations

Adds CRC, destination, & sequence count to commands for validation



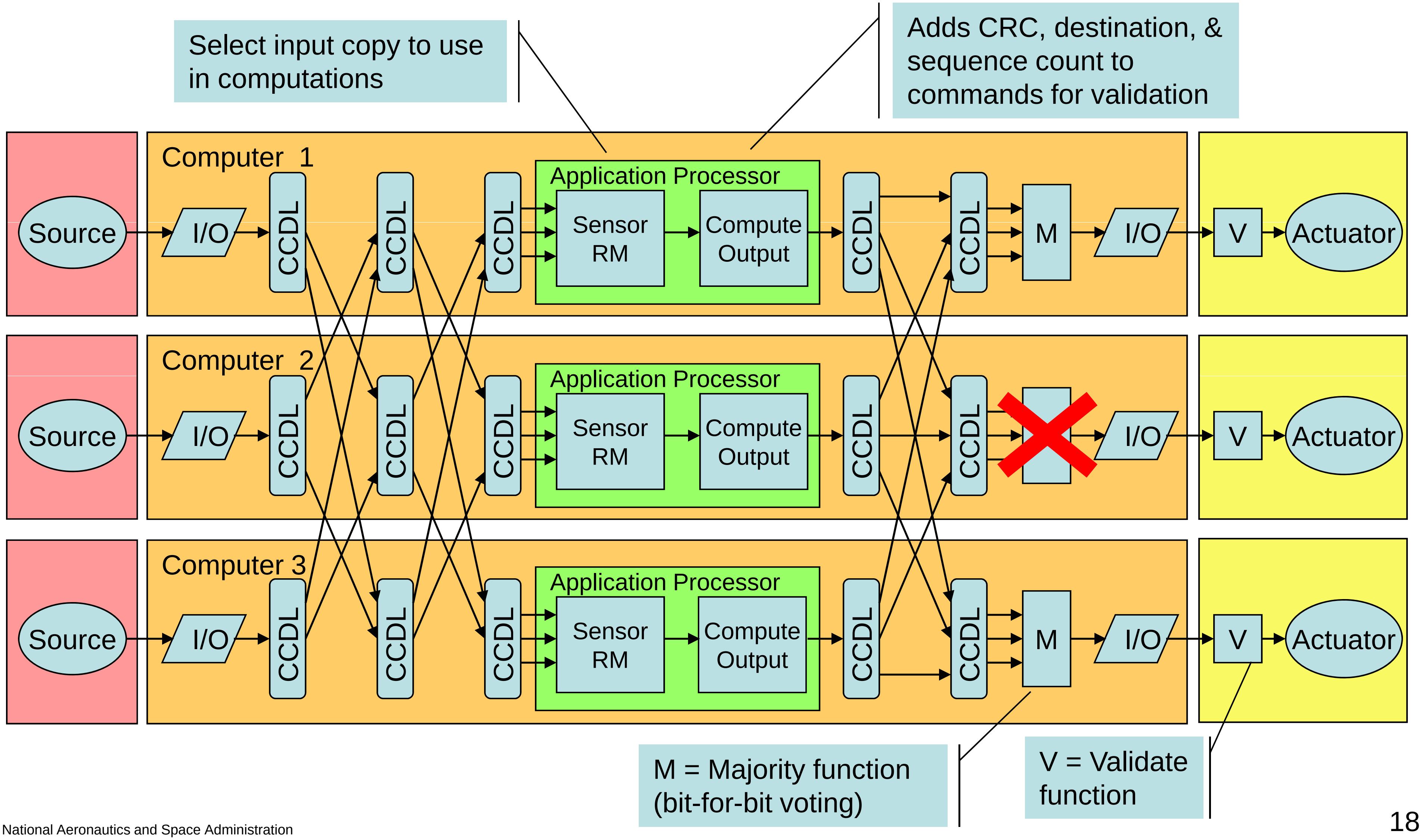
M = Majority function (bit-for-bit voting)

V = Validate function

National Aeronautics and Space Administration

Fault Management: Errant Transmission of a Minority Value

Actuators must filter out minority values OR tolerate a single cycle in an unintended state OR require two-stage commanding (allows replacement of errant commands).



Select input copy to use in computations

Adds CRC, destination, & sequence count to commands for validation

M = Majority function (bit-for-bit voting)

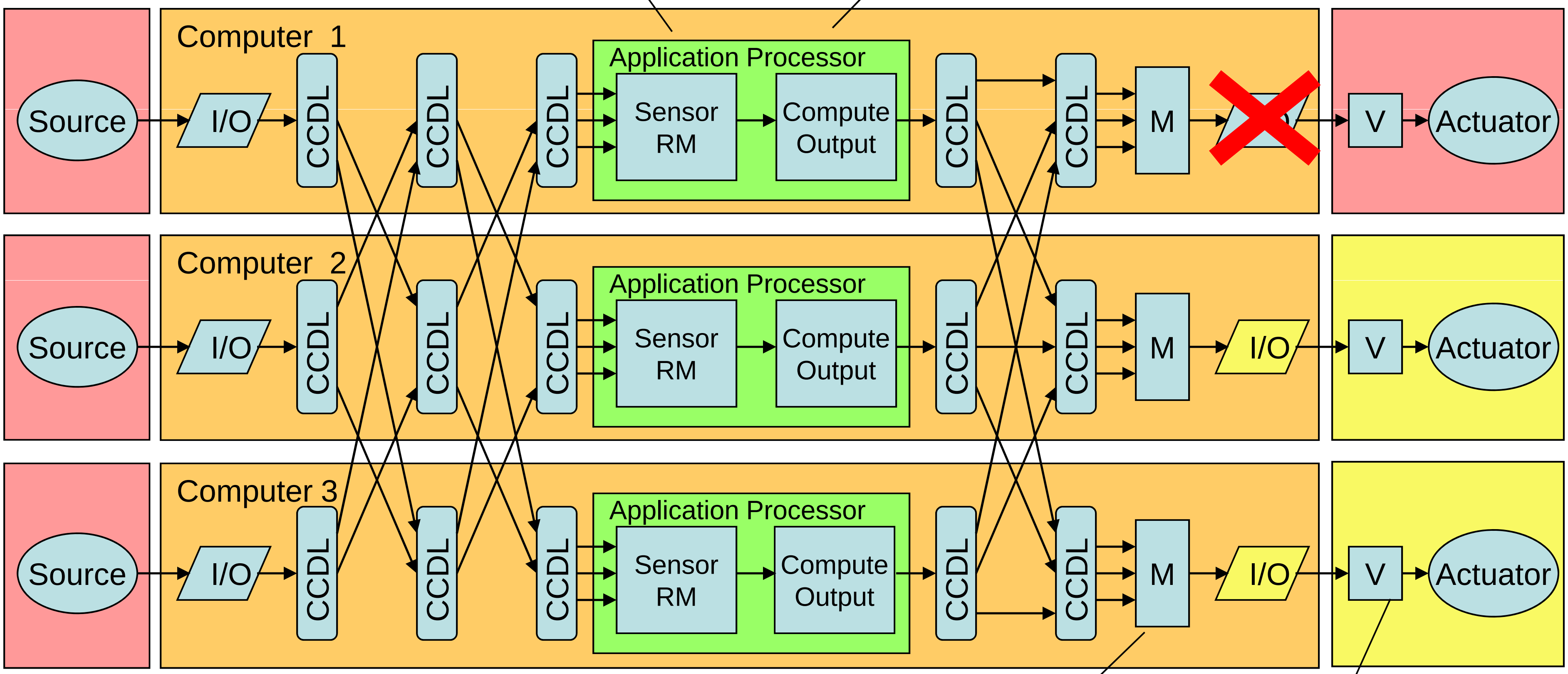
V = Validate function

Fault Management: Failed Output Transmission

The architecture allows for full flight functionality with any one string missing, thus a lost output does not cause loss of function (redundant, operational strings fill in without delay).

Select input copy to use in computations

Adds CRC, destination, & sequence count to commands for validation



M = Majority function (bit-for-bit voting)

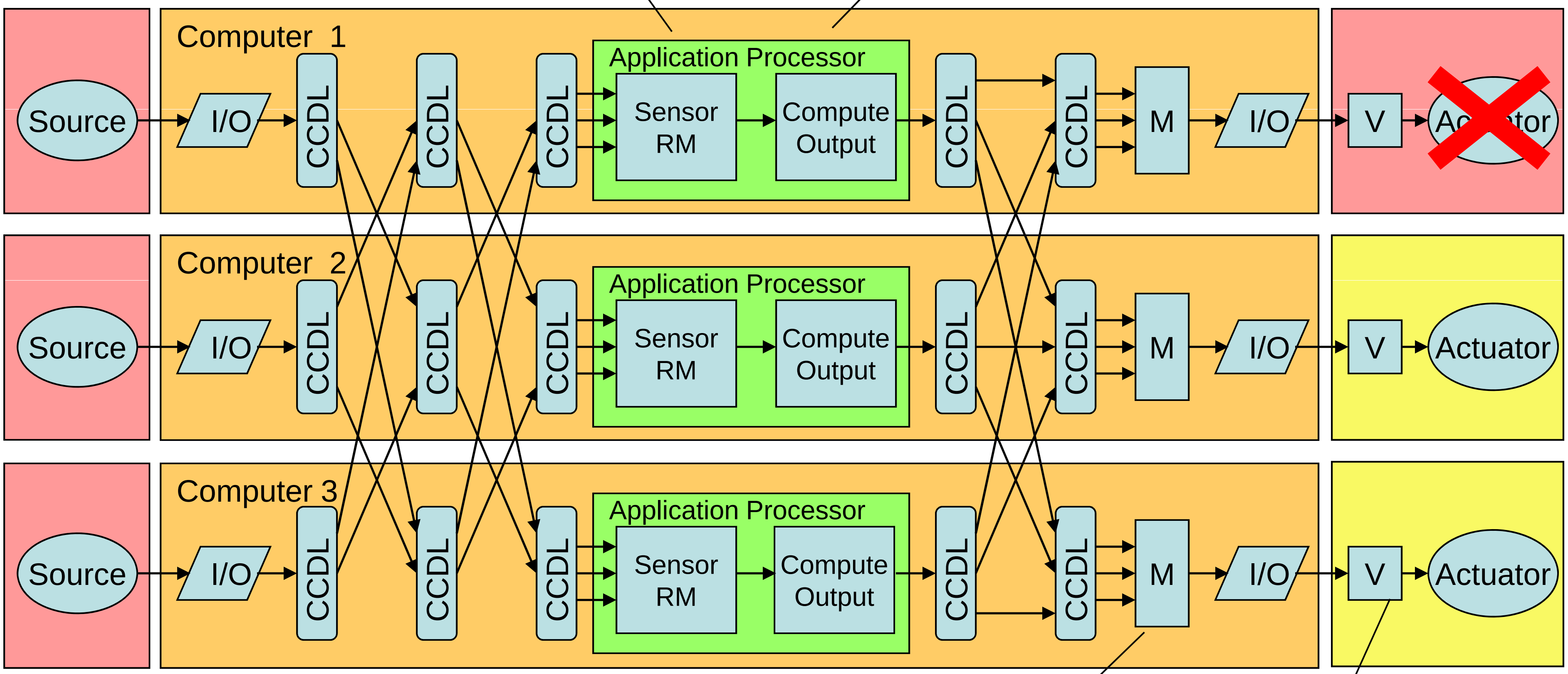
V = Validate function

Fault Management: Actuator Error

Failed actuators are externally forced into a safe state (generally by removing all external power sources) while allowing system functionality to be maintained using redundant actuator copies.

Select input copy to use in computations

Adds CRC, destination, & sequence count to commands for validation



M = Majority function (bit-for-bit voting)

V = Validate function

Summary

- The Ares I avionics uses a multi-string, voting architecture to provide single fault tolerance and enhanced crew safety
- The system draws upon experience gained from building earlier systems such as Shuttle, X-38, and Seawolf submarines
- The system uses existing technologies for critical systems, as much as possible, to reduce development risk

BACKUP MATERIAL

Acronym / Abbreviation List

- 1° – Primary
- 2° – Secondary
- Al – Aluminum
- C&DH – Command and Data Handling
- CCDL – Cross-Channel Data Link
- Cmds – Commands
- COTS – Commercial Off The Shelf
- CPU – Central Processing Unit
- CRC – Cyclical Redundancy Checking
- Cryo – Cryogenics
- DFI – Development Flight Instrumentation
- DPS – Data Processing System
- FS – First Stage
- FWD - Forward
- GN&C – Guidance, Navigation, and Control
- GPS – Global Positioning System
- I/O – Input / Output
- ISS – International Space Station
- klb – kilo (1000) pounds (force)
- LAS – Launch Abort System
- lb – pounds (force)
- LH_2 – Liquid Hydrogen
- Li – Lithium
- LOX – Liquid Oxygen
- m – Meter
- M – Majority voting/selection function
- MECO – Main Engine Cut-Off
- NASA – National Aeronautics and Space Administration
- nm – Nautical Mile
- NPR – NASA Procedural Requirements
- Ops – Operations
- PBAN – Polybutadiene Acrylonitride
- RCS – Reaction Control System
- RM – Redundancy Management
- RSRB – Reusable Solid Rocket Booster
- RSRM – Reusable Solid Rocket Motor
- SM – Service Module
- SRB – Solid Rocket Booster
- TVC – Thrust Vector Control
- US – Upper Stage
- V – Validate

Abstract

- The Ares I is the next generation human-rated launcher for the United States' Constellation program. This system is required to provide single fault tolerance within defined crew safety and mission reliability limits. As part of the effort to achieve those safety goals, Ares I includes an avionics subsystem built as a multi-string, voting architecture. The avionics design draws upon experience gained from building fly-by-wire systems for Shuttle, X-38, and Seawolf. Architectural drivers for the avionics design include using proven technologies with existing suppliers of space rated parts for critical functions (to reduce overall development risk), easing the software development effort by using an off-the-shelf, DO-178B certifiable, ARINC-653 operating system in the main flight computers, minimizing mutual data and power connections that might lead to a common-mode hardware failure of the redundant avionics strings, and centralizing overall Ares I command & control within the Upper Stage.