Fault Tolerant Architectures For Space and Avionics

BALLISTA

Dan Siewiorek

Priya Narasimhan

Electrical & Computer
ENGINEERIN

Comparison of Commercial, Space, Avionics

Operational Environment	Commercial	Space	Avionics
Mission duration	Years	Years	Hours
Maintenance Intervention	Manual	Remote	After mission
Outage response time	Hours	Days	Milliseconds
Resources			
1. Power	Unlimited	Minimal	Medium
2. Spare parts	Unlimited	None	After mission

Comparison of Commercial, Space, Avionics

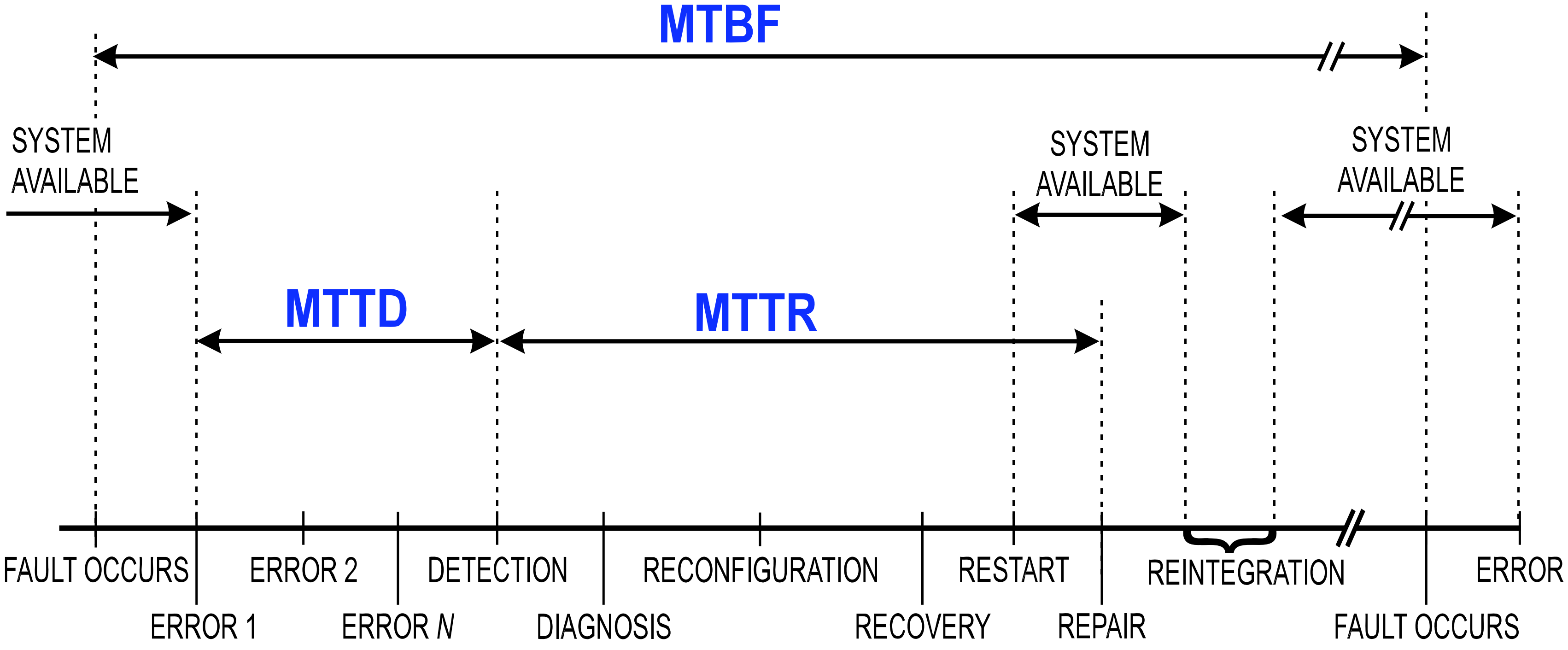
Operational Environment	Commercial	Space	Avionics
Fault-Tolerant Approach			
Fault intolerance	Burn-in	Radiation-hardened components	Shake, rattle, roll
		Design diversity	Design diversity
		Safe system	
Fault tolerance		Component-level redundancy	
		Subsystem-level redundancy	Subsystem-level redundancy
	Multi-computer	Multi-computer	Multi-computer
	Retry	Retry	
	Firewalls		Firewalls
	Software patches	Software reload	

Basic Steps in Fault Handling

- **Fault Confinement -** limits spread of faults
- **Fault Detection -** recognizes something unexpected happened
- **Diagnosis -** identify location of fault
- **Reconfiguration -** replace or isolate faulty component
- **Recovery -** eliminate effect of fault
  - Fault Masking - redundant information
  - Retry - second attempt at operation
- **Restart -** resume after correcting state (hot, warm, cold
- **Repair -** replace component (on-line, off-line)
- **Reintegration -** repaired module returned to operation

MTBF -- MTTD -- MTTR

$$\text{Availability} = \frac{\text{MTBF}}{\text{MTBF + MTTR}}$$



A Scenario for on-line detection and off-line repair. The measures -- MTBF, MTTD, and MTTR are the average times to failure, to detection, and to repair.

Components of a Generic Spacecraft

- **Propulsion -** controls stability and orientation of spacecraft. Passive spin control or active thruster control
- **Power -** generation and storage of electrical power, typically solar cells for generation and batteries for storage
- **Data Communications -** uplink for commands from the ground, downlinks for data and telemetry (temperature, power supply, thruster events)
- **Attitude Control -** dedicated computer to sensing and controlling orientation and stability of spacecraft
- **Command/Control/Payload -** spacecraft control and error recovery

BALLISTA

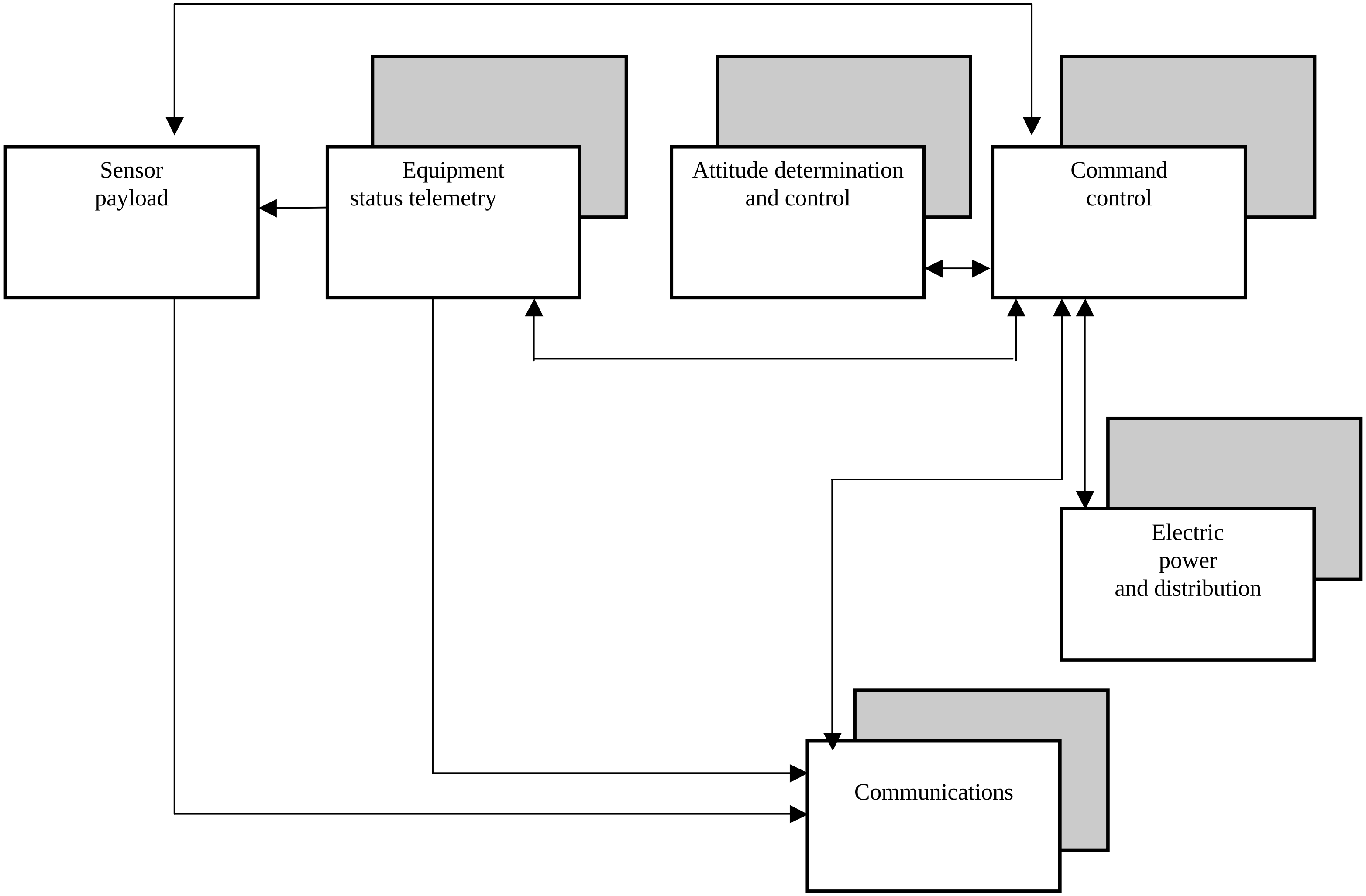
Generic Fault Detection Techniques

- **Self-Tests -** Subsystems perform self-tests, such as checksums on computer memories
- **Cross-Checking Between Units -** Either physical or functional redundancy may be used. When a unit is physically duplicated, one is designated as an on-line unit and the other as a monitor. The monitor checks all the outputs of the on-line unit. Alternatively, there may be disjoint units capable of performing the same function. The less precise calculation can be used as a sanity check on the more precise units.
- **Ground-Initiated Special Tests -** These tests are used to diagnose and isolate failures
- **Ground-Trend Analysis -**Routine processing and analysis or telemetry detect long-term trends in units that degrade or wear out.

Defense Meteorological Satellite Program

- **Propulsion** - Redundant thrusters, including multiple valves for propellant flow control, automatic switchover based on excessive attitude-change rates, and multiple commands required to initiate any firing sequence
- **Power** - Redundant solar cell strings, batteries, power buses; automatic load shedding
- **Data Communication** - Redundant transponders, digital error-detection and correction techniques, switch from directional to omni-directional antennae for backup
- **Attitude Control** - Redundant sensors, gyros, and momentum wheels, along with automatic star reacquisition modes
- **Command/Control** - Hardware testing of parity, illegal instruction, memory addresses; sanity check; memory checksums; task completion timed; watch-dog timers; memory write protection; reassemble and reload memory to map around memory failures.

Defense Meteorological Satellite Program



DMSP Error Recovery Procedure

- Standby block redundancy with cross strapping (e.g. either unit can be switched in) provided at subsystem level, blocks are cross strapped
- Upon error detection, enter “safe” mode shedding all nonessential electrical loads, stop mission sequencing, orient solar panels to obtain maximum solar power, await commands from the ground
- Ground personnel infer source of failure, generate work-around, and upload command sequence to spacecraft
- Ground based diagnosis and work around could take days

Voyager

- **Deep space probe for Jupiter and Saturn fly-bys launched 1977**
- **Planetary encounter**
  - 30 day observatory
  - 30 day far-encounter (observe planet satellites and calibrate sensors)
  - 10 day near-encounter (high resolution observations, Sun/Earth occultation)
  - 30 day post-encounter (observe planet satellites)
- **Block redundancy with Attitude Control Subsystem standby unpowered, Command and Control Subsystem (CCS) standby powered and monitoring**
  - CCS executes self test prior to issuing commands to other subsystems

Voyager Fault Detection

Attitude Control Subsystem (ACS) -

- Failure of CCS to receive “I’m-Healthy” report every 2 seconds
- Loss of celestial (Sun and Canopus) reference
- Failure of power supply, Gyro
- Failure to rewrite memory every 10 hours
- Thruster failure (spacecraft takes longer to turn than expected)
- Parity error on commands from CCS, incorrect command sequence, failure to respond to command from CCS

Command and Control Subsystem (CCS) -

- Low-voltage
- Primary command received before previous one processed
- Attempt to write into protected memory without override
- Processor sequencer reached an illegal state
- Primary output unit unavailable for more than 14 seconds
- Self-test routine not successfully completed
- Output buffer overflow.

Galileo

- Jupiter Orbiter and Probe launched 1990
- Dual architecture with Spun (for field and particle measurements) and Despun (remote sensing) sections communicate through rotary transformers
- Block redundancy for all ten subsystems, all active/unpowered standby spare
- Command and Data Subsystem (CDS) uses active redundancy where both issuing independent commands or operating in parallel on same critical activity
- Over two dozen microprocessors communicating over a message passing bus
- Keep-alive power converts for CDS and Attitude and Articulation Control Subsystem (AACS) random access memories

Galileo Fault Detection

- Test of event durations including transfers between subsystems and transition between all spin and spun/despun modes
- Parity or checksum errors on messages
- Nonimaging science experiments encoded using a Golay (24, 12) error-correcting code.
- Unexpected command codes
- Loss of “Heartbeat” between the AACS and the CDS
- Spin rates above or below set values
- Loss of sun or star identification detected by no valid pulse from acquisition sensor for a given period of time
- Too great an error between control variable setting and measured response

Cassini-Huygens

- **Saturn Orbiter and Probe launched 1997**
- **Huygens probe philosophy is autonomy– since the probe cannot be commanded after separation from the orbiter**
    - Completely redundant power
    - Block redundancy with dual identical Command and Data Management Units (CDMUs), a triply redundant Mission Timer Unit (MTU), two mechanical g-switches (backing up the MTU), a triply redundant Central Acceleration Sensor Unit (CASU) include dual-redundant accelerometers and proximity sensors
    - CDMU executes its own software simultaneously in a hot-backup configuration. One replica's telemetry delayed 6 seconds in case connectivity of the telemetry link temporarily lost. Either replica considers itself invalid if it detects a two-bit error in the same memory word, an Ada exception, or an under-voltage on the CDMU power-line
    - Data from probe redundantly mirrored within the orbiter for later downlinking and transfer to Earth

Huygens ErrorHandling

- **Completely redundant power**
- **Block redundancy with dual identical Command and Data Management Units (CDMUs), a triply redundant Mission Timer Unit (MTU), two mechanical g-switches (backing up the MTU), a triply redundant Central Acceleration Sensor Unit (CASU) include dual-redundant accelerometers and proximity sensors**
- **CDMU executes its own software simultaneously in a hot-backup configuration. One replica's telemetry delayed 6 seconds in case connectivity of the telemetry link temporarily lost. Either replica considers itself invalid if it detects a two-bit error in the same memory word, an Ada exception, or an under-voltage on the CDMU power-line**
- **Data from probe redundantly mirrored within the orbiter for later downlinking and transfer to Earth**

Cassini ErrorHandling

- No single point of failure
- Handle multiple faults with a priority-driven one-fault-at-at-a-time fault-recovery
    - The fault-recovery action depends on mission mode (mission phase, in-flight history, etc.) and the environment (runtime performance of spacecraft hardware)
- Fault-recovery divided between the spacecraft and ground operations
    - Autonomous time-constrained fault-recovery provided onboard spacecraft
    - Each subsystem designed to be self-recovering
    - Command and Data Subsystem (CDS) replica powered off and activated in case the primary CDS replica failed to reset the watchdog timer every 32 seconds
- Cancellation/interruption of a fault-recovery action triggered a "safing response" by entering the system into a low-power state

Mars Pathfinder

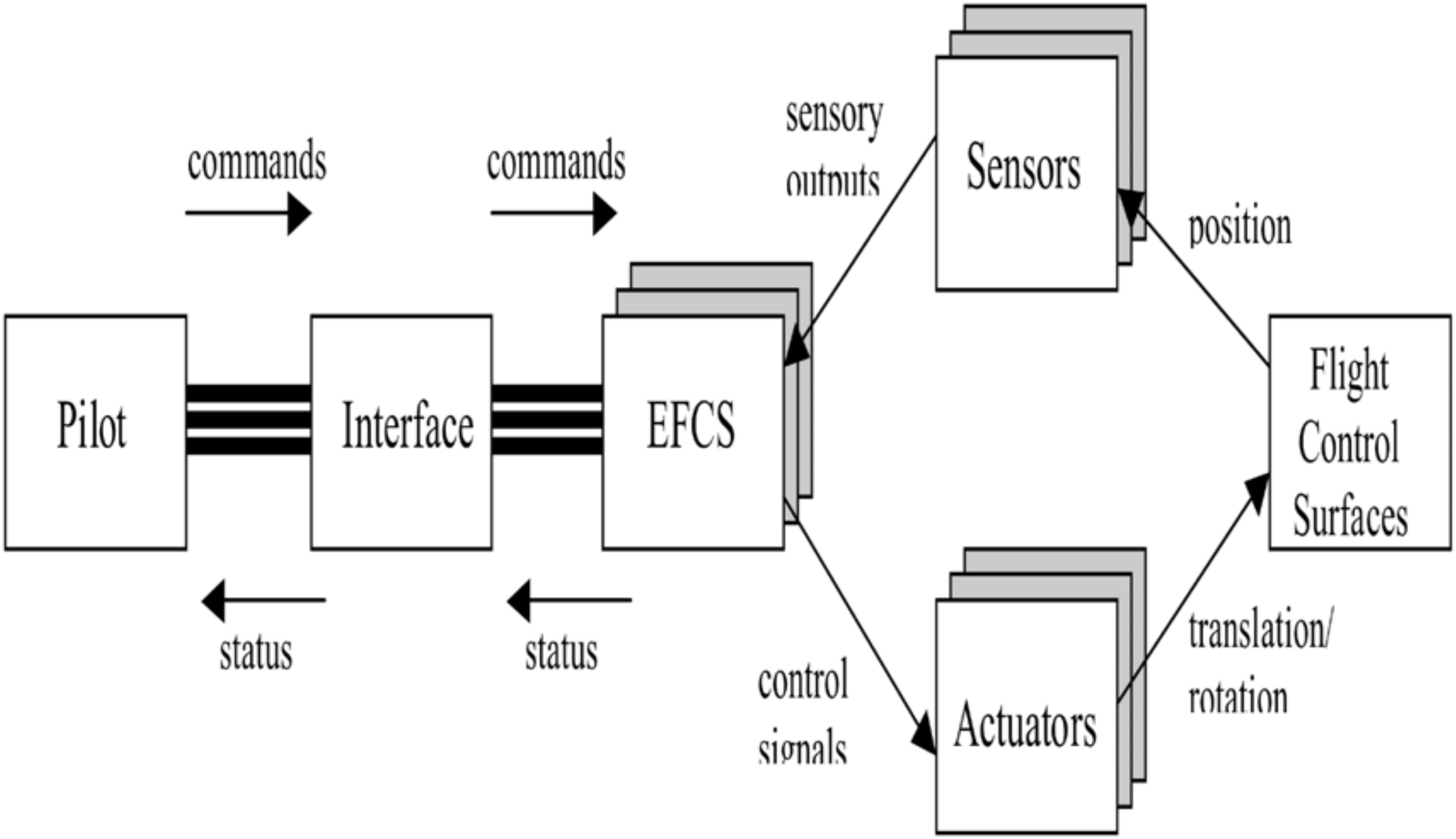
- Mars Planetary Lander with an autonomous mobel rover launched 1996
- Faster (half the time), Better, Cheaper (one tenth the cost)
- Direct, non-orbiting planetary approach using airbag for landing
- Tele-commanded Rover to chart composition of martian rocks and dust
- During development, periodic system failure-mode and fault-tree analyses
- Flight software written in C using object-oriented design principles
- *Short mission duration* allowed use of Grade 2 part quality, use selective, rather than complete, block redundancy
- Failure Mode Effect Criticality Analysis (FMECA) only at the interface subsystem level
- Problem and Failure Reporting (P/FR) invoked only on pre-mission critical problems lead to less than one-tenth the number of reports of traditional missions

BALLISTA

Generic Aircraft Approaches

- **Redundant Paths -** for example, different jet engines drive redundant electrical generators which power two independent computers that in turn drive different hydraulic systems for controlling different flight surfaces
- **Functional Redundancy –** if both generators fail, batteries provide power until a ram air turbine can be deployed
- **Architectural Migration –** from mechanical flight control to parallel mechanical/electronic to all electronic “fly by wire”
- **Tolerate New Fault Classes –** design errors

Generic Avionics Architecture and Electronic Flight Contr System (EFCS)



BALLISTA

Airbus A330/A340/A380

- A310 circa 1983 had ten separate digital flight control computers
- A320 circa 1988 fly by wire, four computers teamed in command/monitor pairs which became standard approach for subsequent Airbus flight control computers
- A340 circa 1992 had one command/monitor pair forming a “fail fast” module failing over to another command/monitor “hot spare” pair. Error detection through mismatched command, sequence checking, self-test when aircraft energized
  - A second command/monitor pair using a different microprocessor and different software provide Design Diversity to tolerate common mode design and manufacturing faults
- A380 employs dual-redundant Ethernet for non-critical functions, electrical and hydraulic flight control diversity
- Design Diversity – dissimilar computers, physical separation, multiple software bases, different software development tools, and data diversity

BALLISTA

Boeing 777

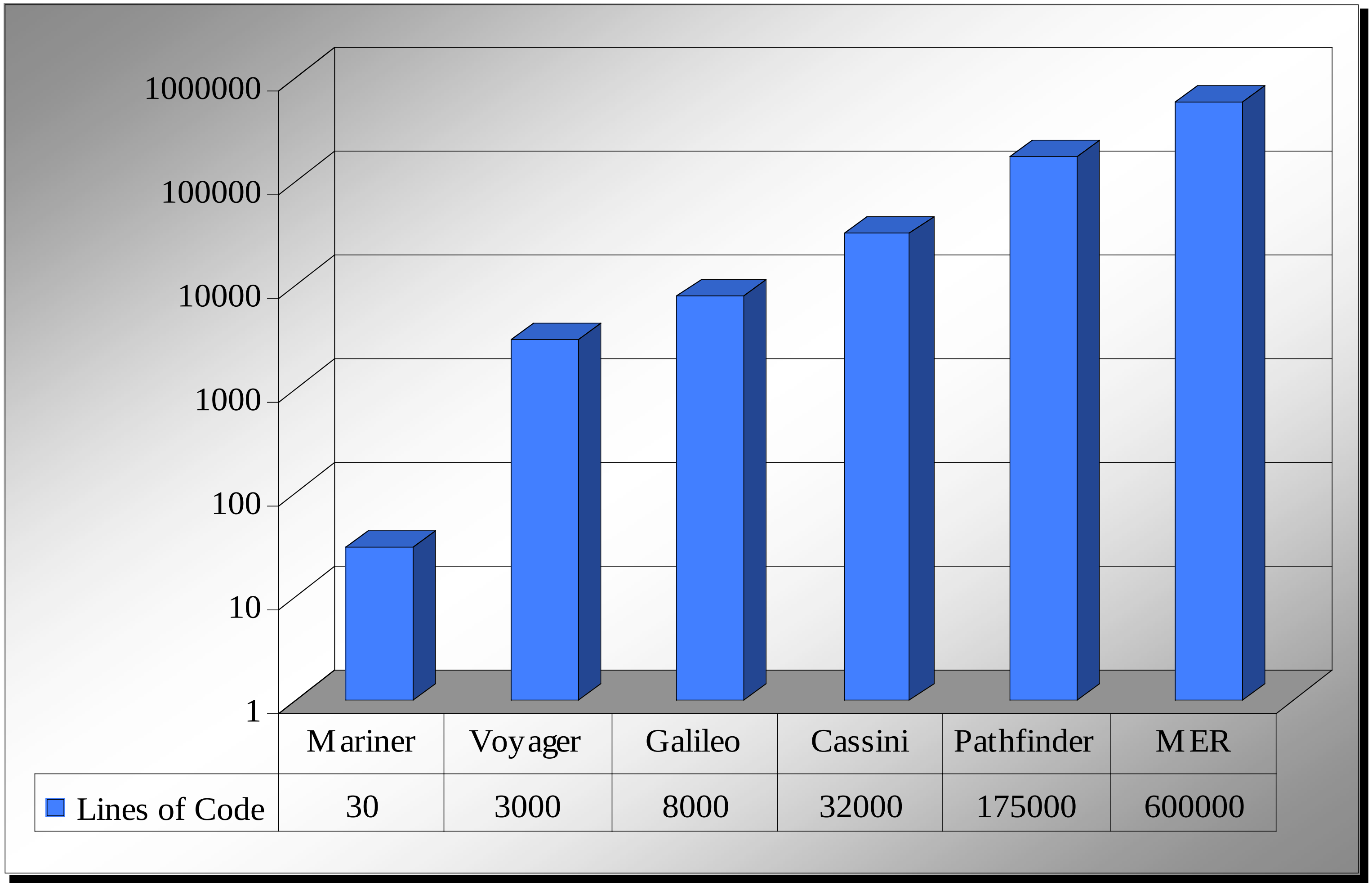
- Goal of Mean Time Between Actions to 25,000 operating hours, reduce probability of degrading below minimum capability to less than 10^{-10}
- Designed to tolerate Byzantine faults, object impact, component failure, power failure, electromagnetic interference, cloud environment
- Byzantine fault tolerance with data synchronization and median voting
- Architecture of flight control computer has three independent channels each composed of three redundant computing lanes (command, monitor, standby). Standby allows dispatch of aircraft even with a lane or data channel failure
- Design diversity in different microprocessor hardware and different software compilers for a fault-intolerant single source code

Fault Tolerant Mechanism for Space/Aircraft

Mission/System	Inception	Configuration (Lines of Code, Memory, Hardware, OS, Middleware, Language)	Fault-tolerance mechanisms
Voyager – outer planet flyby	1977-1989	3000 lines of code	Active/standby block redundancy as command/monitor pair
Galileo – Jupiter orbiter and probe	1989	8000 lines of code	Active/standby block redundancy , microprocessor multicomputer
Cassini-Huygens - Saturn orbiter and probe	1997-2005	32,000 lines of code Code written in Ada	No single point of failure Priority-based one-at-a-time handling of multiple simultaneous faults $3.26 B
Mars Pathfinder - Mars lander and rover	1996-1997	175,000 lines of code 32-bit RSC-6000 processor 128MB DRAM VME backplane VxWorks real-time OS Object-oriented design (in C)	Selective (not full) redundancy Complete environmental testing Adoption of vendor's QA practices Based on short mission duration, budget cap and extreme thermal/landing conditions $280 M
Airbus A340 – flight control computer	1993	Two different processors (PRIM and SEC)	Design diversity emphasized to handle common-mode and common-area failures
Boeing 777 - flight control computer		Code written in Ada ARINC 629 bus Dissimilar multiprocessors	Triple-triple modular redundancy for the primary flight computers Goal to handle Byzantine failures, common-mode and common-area failures Physical and electrical isolation of replicas

BALLISTA

Size of Software in Spacecraft Missions



	Mariner	Voyager	Galileo	Cassini	Pathfinder	MER
🟦 Lines of Code	30	3000	8000	32000	175000	600000

Observations and Trends

- **Commercial off-the-shelf components –** increasing use of commercial standards and components to decrease design time and cost. Accommodations for unique environment and safety issues. Other issues include obsolescence, updates, integration, validation, and adequate technical support**.**
- **Autonomy and fly-by-wire software –** digital control of aircraft and increasing autonomy of spacecraft under software control
- **Escalating fault sources and evolving redundancy –** evolved from basic command/monitor pair to triplication/median pick voting to command/monitor redundancy. Design diversity to tolerate design flaws. Spacecraft focus on availability and longevity while aircraft focus on safety and dependability
- **Safing –** historically spacecraft incorporates safing which may no longer be effective for critical flight phases and autonomous operation
- **Deadlines –** both spacecraft and aircraft systems have “shipping date” deadlines dictated by planetary physics and financial consequences