

# DO-178C in Multicore Avionics: Avionics: Certification Paths for for Electric Aircraft



# Speaker Introduction



**By : Charles Antony Raj**

**Senior Manager, Systems & Software Engineering, Collins Aerospace**  
**Conf42 Robotics 2025 | November 20**

- Specializing in avionics certification, multicore systems integration, and DO-178C compliance for next-generation aircraft platforms.

# The Multicore Revolution in Aviation

**85%**

## Adoption Rate

Multicore processors deployed in electric and next-generation aircraft

**60%**

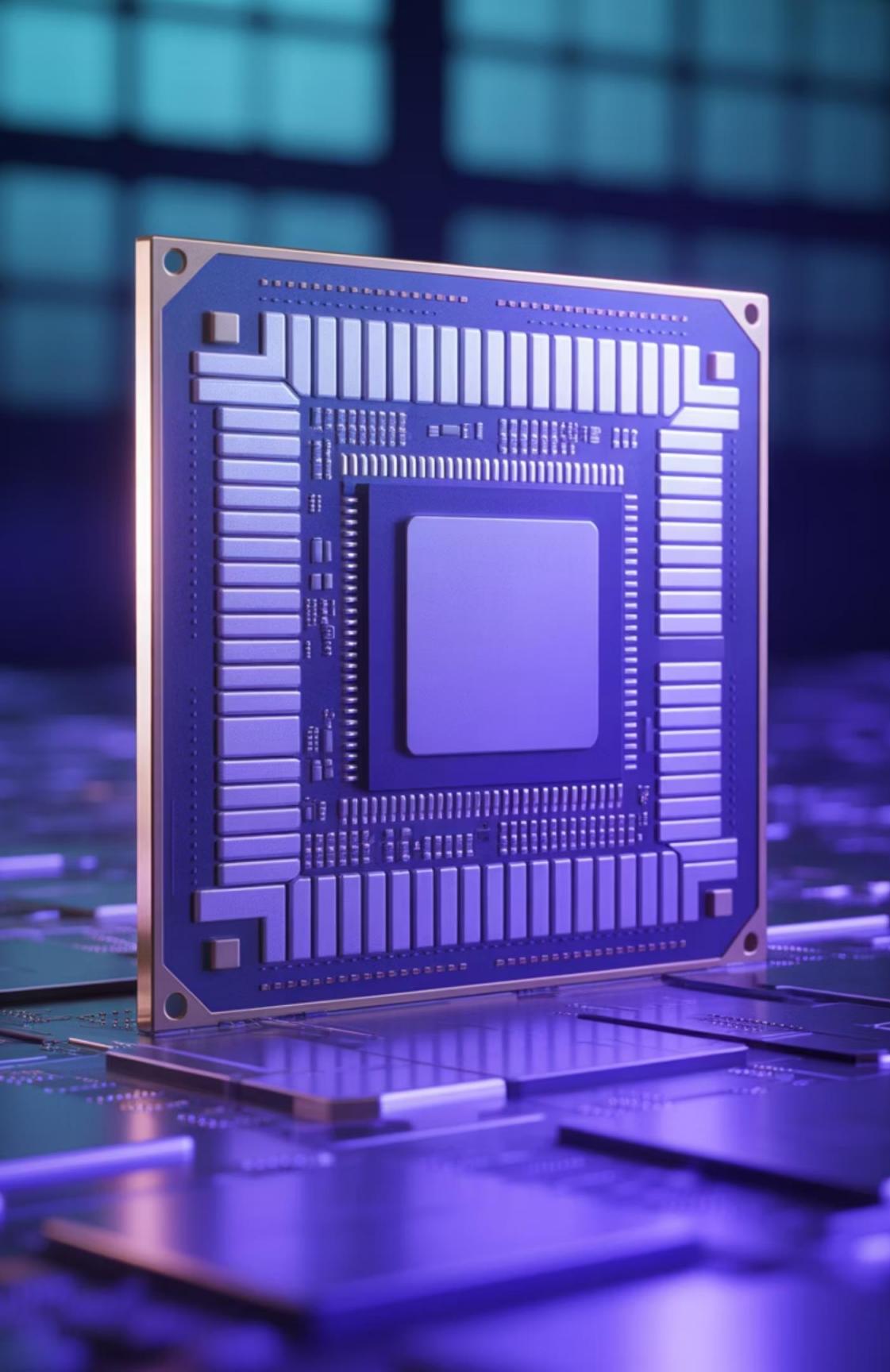
## Certification Delays

Systems facing delays due to multicore challenges

**30%**

## Time Savings

Reduction in compliance cycles with proven practices



# Why Multicore for Electric Aircraft?

## Performance

Enhanced computational power for complex robotic control systems and autonomous functions

## Integration

Consolidation of multiple avionic functions onto fewer platforms reduces weight and complexity

## Efficiency

Optimized power consumption critical for electric propulsion architectures

# The Certification Challenge

Multicore architectures fundamentally alter how we approach safety-critical software certification under DO-178C, particularly for Design Assurance Level A through C systems.

## Shared Resource Contention

Multiple processes competing for cache, memory buses, and I/O channels create unpredictable timing behavior

## Execution Interference

Cross-core interactions can impact deterministic execution required for critical flight control functions

## WCET Validation

Proving worst-case execution time becomes exponentially more complex in parallel processing environments

# DO-178C & CAST-32A Framework

## DO-178C Foundation

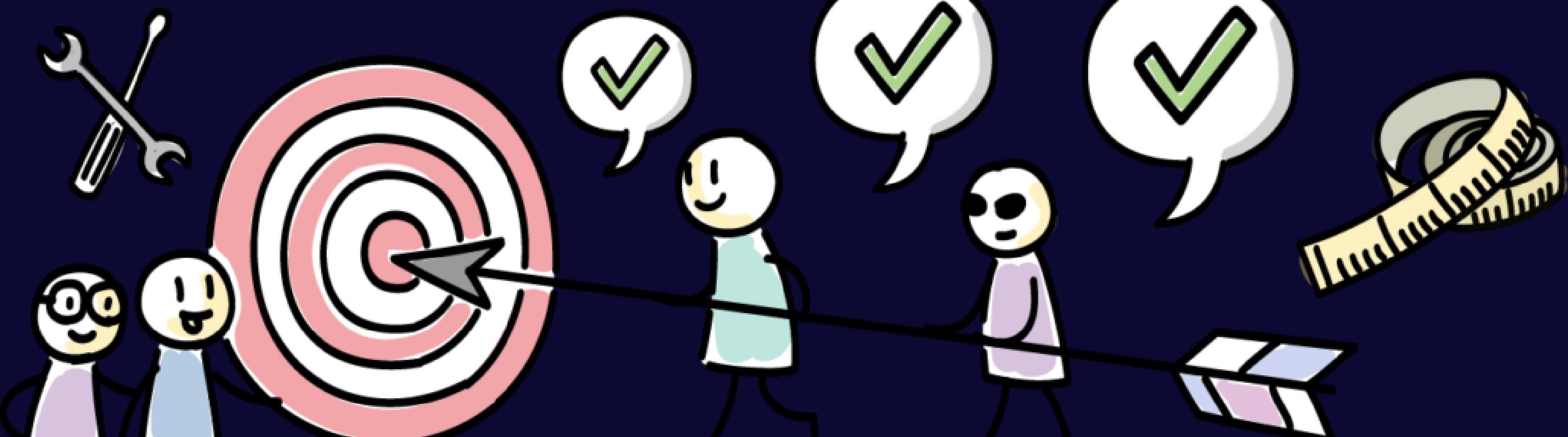
Software Considerations in Airborne Systems and Equipment Certification provides the baseline requirements for airborne software.

- Design Assurance Levels (A-E)
- Verification and validation processes
- Configuration management
- Quality assurance objectives

## CAST-32A Guidance

Multi-core Processors position paper issued by certification authorities addresses specific multicore challenges.

- Interference mitigation strategies
- Timing analysis requirements
- Resource usage validation
- Documentation expectations



## Certification objectives summary

- Early MCP planning & HW characterization (document interference channels).
- Resource usage budgeting & partitioning (time, space, I/O).
- Demonstrate WCET bounds under interference (measurement + analysis).
- Error detection/handling for MCP-specific faults.
- Produce an MCP Accomplishment Summary for the cert authority.

# Partitioning for Safety

Effective partitioning isolates critical robotic control processes from lower-criticality functions, ensuring that failures cannot propagate across DAL boundaries.

01

## Spatial Partitioning

Dedicated memory regions prevent unauthorized access between partitions

02

## Temporal Partitioning

Time-sliced execution guarantees CPU access for critical processes

03

## Resource Isolation

Core assignment and cache allocation minimize interference

04

## Validation Testing

Robustness testing confirms partition integrity under stress

# Measurement-Based Timing Analysis

Traditional static analysis methods struggle with multicore complexity. Measurement-based approaches provide practical paths to WCET determination.



## Instrumentation

Deploy timing monitors and performance counters across execution paths



## Test Campaign

Execute comprehensive scenarios covering operational and stress conditions



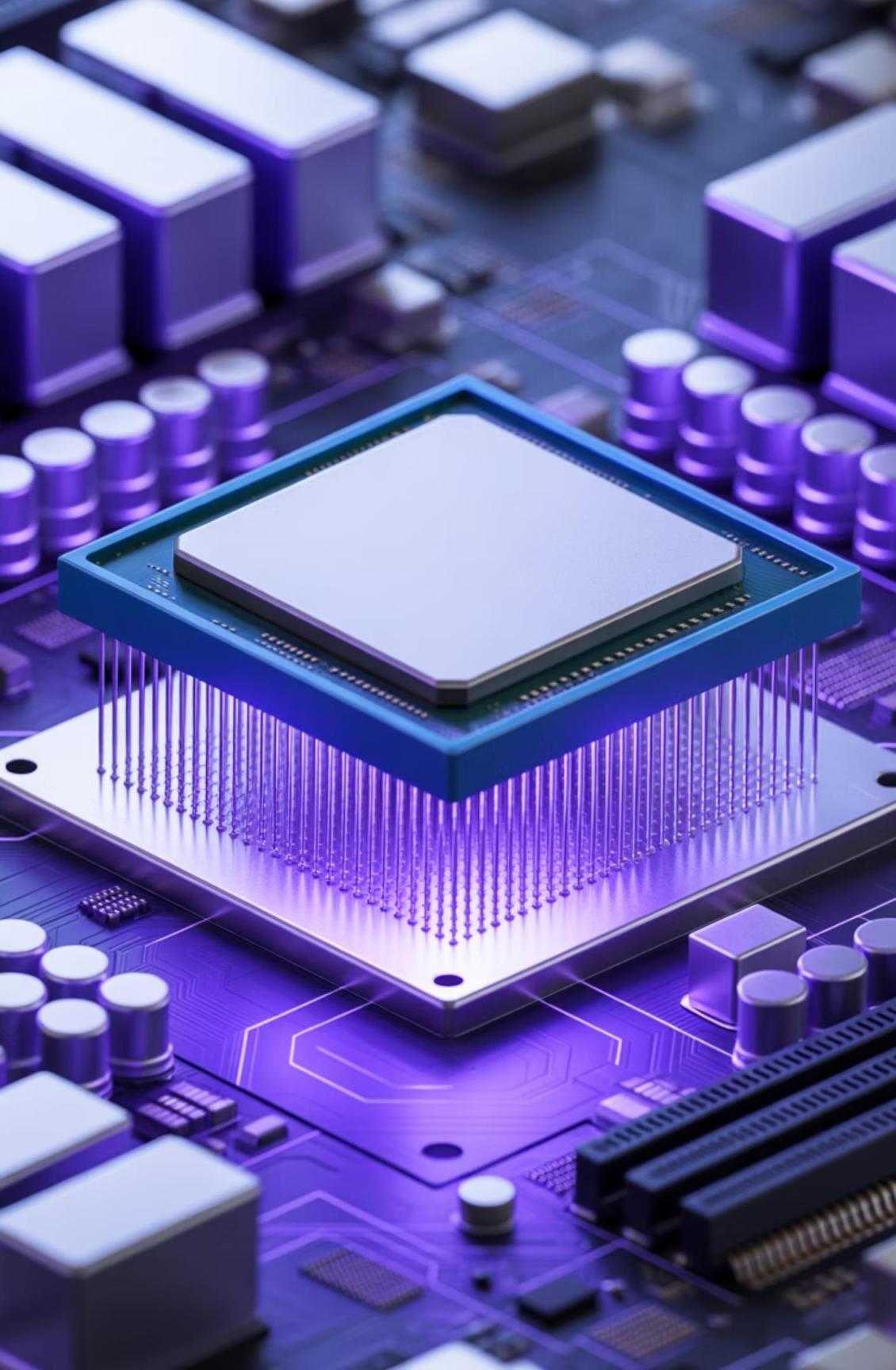
## Data Analysis

Identify bottlenecks, interference patterns, and timing margins



## Validation

Demonstrate compliance with timing budgets and safety margins



# Interference Channels

1

## Cache Interference

Shared L2/L3 caches create eviction patterns that affect execution timing

2

## Memory Bus Contention

Simultaneous memory access from multiple cores introduces wait states

3

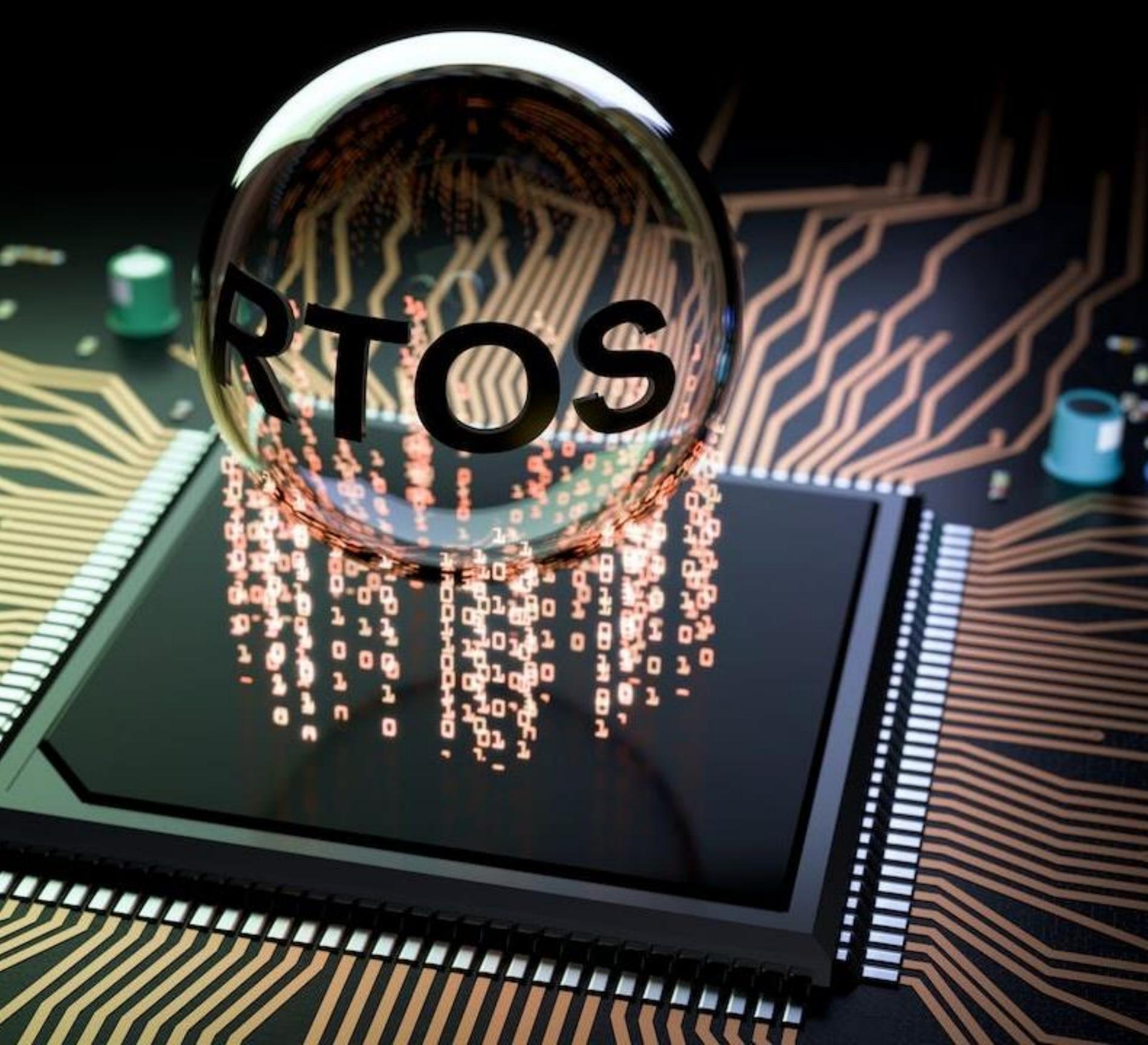
## Peripheral Access

Shared I/O controllers and DMA channels can delay critical operations

4

## Interconnect Delays

Core-to-core communication adds unpredictable latency to distributed functions



---

## Tools, RTOSs, and vendor support

- RTOS with multicore partitioning (e.g., INTEGRITY-178 tuMP — used in early multicore certs).
- Timing analysis & measurement suites (Rapita, LDRA, Wind River toolchains, vendor-specific profiler + TTCN-type test harnesses).
- Hardware-assisted tracing (ETM, PTM), platform configuration managers, and QoS monitors.

# Certification Strategy for Electric Aircraft

Proven approaches that electric aircraft programs are applying to accelerate safe multicore deployment while maintaining regulatory compliance.

## Phase 1: Architecture

Define partitioning strategy and select certified RTOS with multicore support

## Phase 3: Integration

Implement measurement-based validation with comprehensive test coverage



## Phase 2: Analysis

Conduct interference analysis and establish timing budgets per CAST-32A

## Phase 4: Certification

Compile evidence packages and engage with certification authorities early

# Robotic Control System Integration



## Critical Considerations

Robotic control loops demand predictable, deterministic execution. Multicore platforms must preserve real-time guarantees.

- Sensor fusion processing on dedicated cores
- Flight control laws with guaranteed response times
- Autonomous decision-making with temporal isolation
- Fail-safe monitoring without interference

# Documentation & Evidence

Certification authorities require comprehensive evidence demonstrating multicore safety. Key artifacts include:



## Interference Analysis

Detailed examination of all interference channels with mitigation strategies



## Timing Reports

WCET validation data with margins and confidence levels



## Test Results

Robustness testing demonstrating partition effectiveness



## Compliance Matrix

Traceability from CAST-32A objectives to verification activities



## Common pitfalls & how to avoid them

- Pitfall: assuming single-core WCET equals multicore WCET — avoid.
- Pitfall: too-late platform selection → huge rework.
- Pitfall: insufficiently exercised interference tests (use stress matrix covering all resource combos).
- Solution: early HW-in-the-loop, interference generators, and tool-supported trace.



## Case study: PU-3000 / INTEGRITY-178 tuMP

- PU-3000 (CMC Electronics) achieved civil multicore certification using INTEGRITY-178 tuMP; demonstrated practical path to DO-178C DAL A on multicore.



# The Path Forward

Multicore avionics enable the robotics-driven aerospace future. Success requires balancing innovation with rigorous safety practices.

## **Adopt proven partitioning strategies that isolate critical functions**

Leverage spatial and temporal isolation to prevent interference propagation

## **Implement measurement-based timing analysis with comprehensive test coverage**

Build confidence through empirical data rather than theoretical worst-cases

## **Engage certification authorities early and maintain continuous dialogue**

Alignment on approach prevents costly rework during final certification



# Example certification plan

- Select platform & RTOS; multicore risk assessment.**
- Platform characterization & interference map.**
- Partitioning & resource budgets defined (time, memory, IO).  
IO).**
- WCET analysis (static + measured) under interference**
- Integration test matrix, error handling verification.**
- MCP Accomplishment Summary & submission.**

**Thank You!**  
**Questions and Discussion..?**