

**Committee for a Study of Electronic Vehicle Controls
and Unintended Acceleration
National Research Council**

SPECIAL TOPIC

Aircraft Electronics:

**Safety Assurance in Product Design/Development/Certification
and**

**Methods for Monitoring and Evaluating Safety Performance
Engine Control System Perspective**

**Mike James
Honeywell Aerospace**

November 16, 2010

Honeywell

- **Brief Biography**
- **Honeywell Company Overview**
- **FAA Regulations – 14 CFR Part 33**
 - **Airworthiness Standards – Aircraft Engines**
 - **Engine Control System Specific Regulations**
- **Engine Design and Development Integration Process**
 - **Planning through Certification**
- **Electromagnetic Interference and High Intensity Radiated Fields (EMI/HIRF) testing/susceptibility**
- **Other critical topics**
 - **LOTG, UHT, TLD, ECTM, SEU**
 - **SW Assurance levels**
- **Material references**

Biography

Mike James

Michael James Biography

- **Education – The Catholic University of America, BSME**
 - Focus on turbomachinery and thermodynamics
 - Design for Six Sigma Green Belt certification
 - Facilitation Training
- **Honeywell Aerospace (AiResearch, Garrett, Allied Signal . . .)**
 - 30 years of aerospace engineering experience
 - Currently FAA Designated Engineering Representative (DER) (15 years)
 - Delegated for propulsion/APU turbo-machinery with special delegations
 - EMI/HIRF and Lightning
 - DO178B Software and DO-254 Airborne Electronic Hardware (Level A)
 - Analog/digital/fuel engine control systems and accessories
 - Developed Engine Condition Trend Monitoring for propulsion engines
 - Member of SAE E-32 committee developing SW assurance levels for engine health monitoring software (ARP 5987)

Control System Engineering Directly Transportable

Brief Honeywell Overview

- **Leadership:**
 - David M. Cote, Chairman and CEO
- **Headquarters:**
 - Morristown, New Jersey (USA)
- **Number of Employees:**
 - Approximately 122,000 in more than 100 countries
- **Key Business Areas**
 - Automation and Control Solutions (control/thermostats/security)
 - Transportation Systems (Turbochargers/sensors/FRAM)
 - Specialty Materials (Refrigerant replacements/Bio Fuels)
 - Aerospace (Propulsion/Avionics/APU/Brakes/Lighting)

***Honeywell Invents and Manufactures
Breakthrough Technologies***

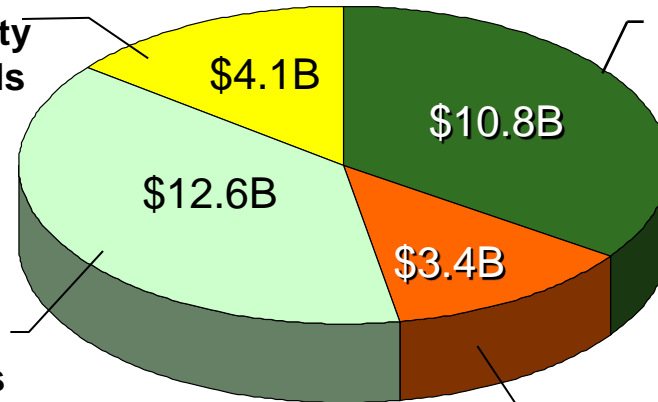
Honeywell's Businesses



2009 Sales **Aerospace**



Specialty Materials



Automation and Control Solutions

Total = \$30.9B

Transportation Systems



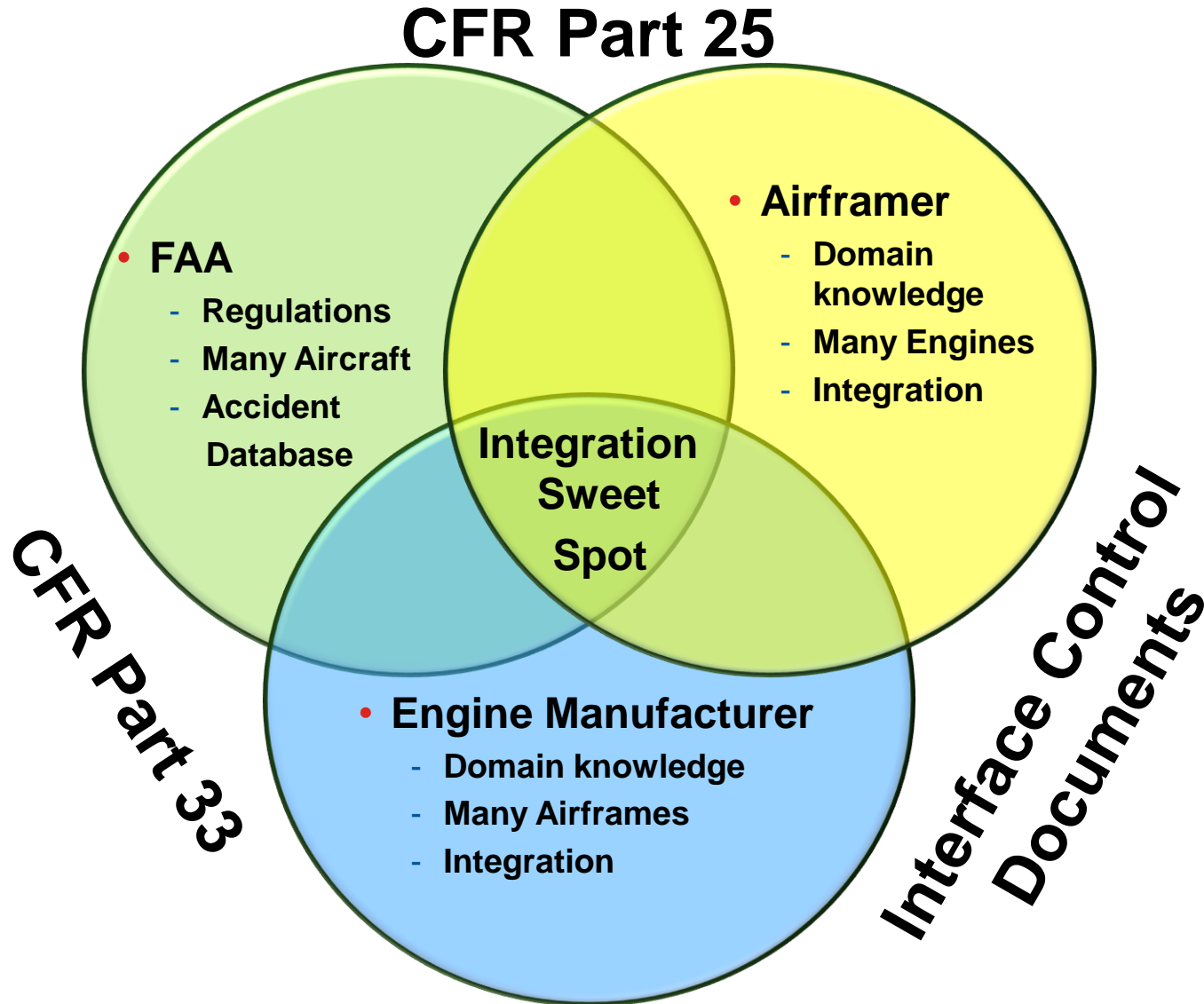
Diverse Businesses, Technologies and Products

FAA Regulations

14 CFR Part 33

Aircraft Engines

FAA Regulations and Supplier Teamwork Needed



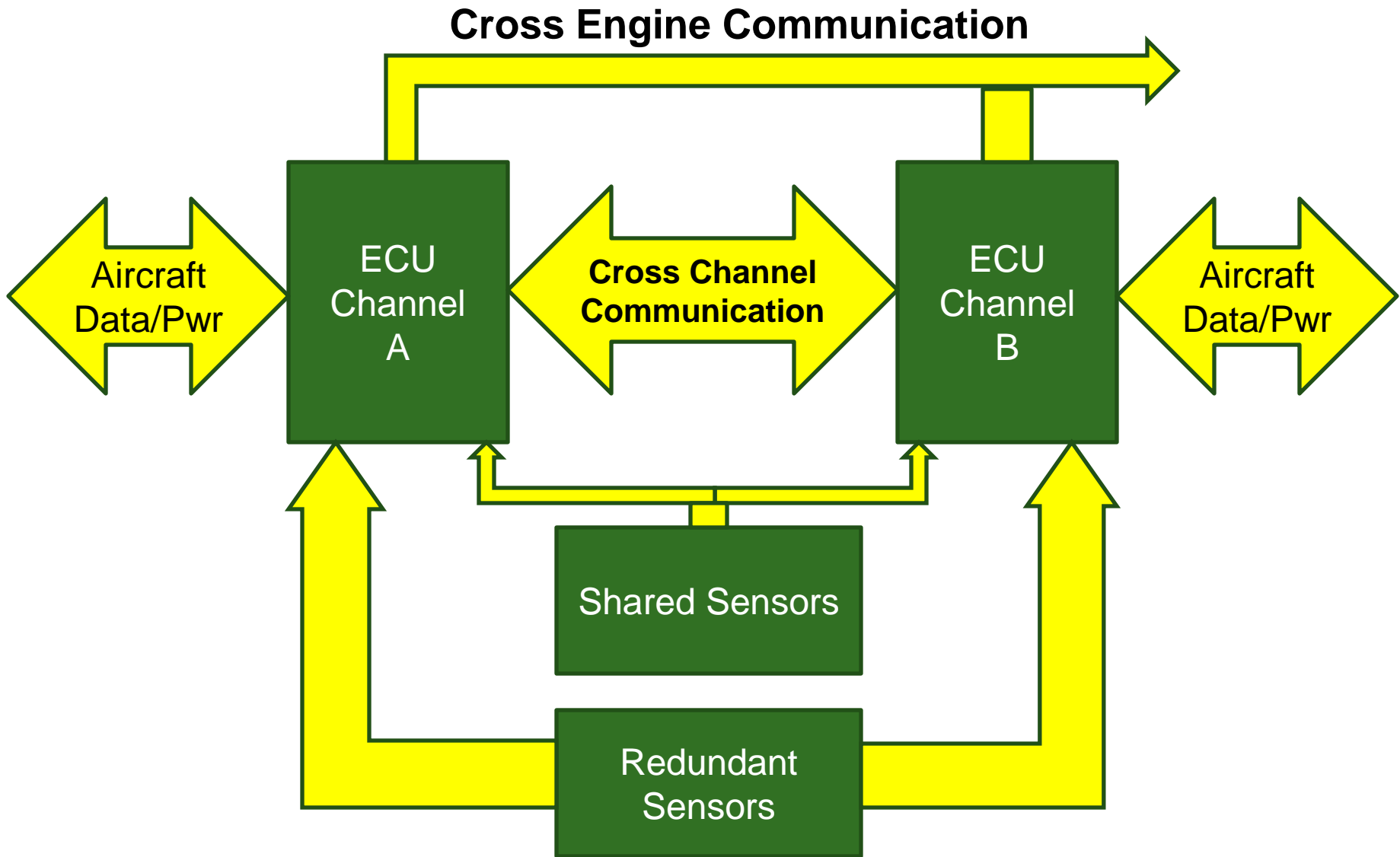
Integration Required for Certification Excellence

Engine Related CFR Part 33 Regulations

- Key Part 33 regulations for Engine Operability and Safety
 - 33.66 Bleed Air System
 - 33.68 Induction Icing
 - 33.70 Life Limited Parts
 - 33.71 Lubrication System
 - 33.73 Power or Thrust response
 - 33.75 Safety Analysis (more later)
 - 33.76 Bird Ingestion
 - 33.77 Foreign Object Ingestion
 - 33.78 Rain and Hail Ingestion
 - 33.87 Endurance Testing
 - 33.88 Engine Over-temperature Testing
 - 33.89 Operation Test
 - 33.90 Initial Maintenance Inspection Test
 - 33.97 Thrust Reversers

Many Specific Regulations for Operation and Safety

Simple Engine FADEC Architecture



Safety Related CFR Part 33 Regulations

- Engine Control System is also germane in many of the Engine Tests and Safety Objectives on the previous page
- Key CFR Part 33 regulations for Engine Control System
 - 33.4 Instructions for Continued Airworthiness
 - 33.5 Instruction Manual for Installing and Operating the engine
 - 33.17 Fire protection (Fuel/oil carrying parts and Engine Control)
 - 33.28 Engine Control Systems (13 items - More later)
 - 33.67 Fuel Systems (Contamination, screens, filters, hot/cold)
 - 33.69 Ignition Systems (Ability to start engines)
 - 33.73 Power and Thrust Response (Accel time and surge free)
 - 33.75 Safety Analysis (More later)
 - 33.91 Engine Components Test (other than engine control)

Many Specific Engine Control System Regulations

33.75 – Critical CFR for Safety

- **CFR 33.75 – Safety Analysis**
 - The applicant must analyze the engine for all likely failures
 - Include secondary and latent failures
 - Multiple failures resulting in Hazardous conditions ($<1.0E-7$ /hour) (1 in 10,000,000 hours)
 - Hazardous engine effects include
 - Non-containment of High Energy debris
 - Bleed air contamination
 - Significant thrust in opposite direction of pilot command
 - Uncontrolled fire
 - Failure of engine mount system
 - Inability to shut the engine down.
 - Identify Major engine failures ($<1.0E-5$ /hour)(1 in 100,000 Hours)
 - Minor engine effects such as In Flight Shutdown

Safety Analysis Identifies Critical Failure Rates

System Safety Assessment Process

- **Preliminary System Safety Assessment (PSSA)**
 - Used as design tool to identify architecture and assign hardware and SW assurance level allocations (Hazardous/Major/Minor)
 - Socialized with airframe manufacturer to begin interface definition for aircraft SSA
- **System Safety Assessment (SSA)**
 - Uses 33.75 criteria
 - Allocate failure rates to system components
- **Fault tree analysis (FTA)**
 - Based on field data, similar parts or predicted for new parts
 - Requires FMEA mapping 33.75 criteria (system integration)
- **Failure Mode and Effects Analysis (FMEA)**
 - Detailed component sub assembly failure modes
 - Failure rates for each mode

The System is Designed to Meet Safety Objectives

CFR 33.28 Critical for Control Systems

- **CFR 33.28 – Engine Controls Systems [Summary]**
 - Validation of design and functional operation verification
 - Environmental Limits (RTCA/DO-160F)
 - Control Transitions
 - **Control Systems failures**
 - Loss of Thrust Control (LOTC)(More later)
 - Single failures can not cause Hazardous Conditions
 - Local events (overheat, leaks etc)
 - Uncontrollable High Thrust (UHT)(More Later)
 - **System Safety Assessment**
 - **Protection Systems (shaft break/overspeed)**
 - **SW and Airborne Electronic hardware (AEH) Integrity assurance levels (Use RTCA /DO-178B and DO-254 methods)**
 - **Aircraft supplied power and data (Integration)**
 - **Engine shutdown means**

Many Aspects to Engine Control System Certification

Engine Design/Development Integration Process

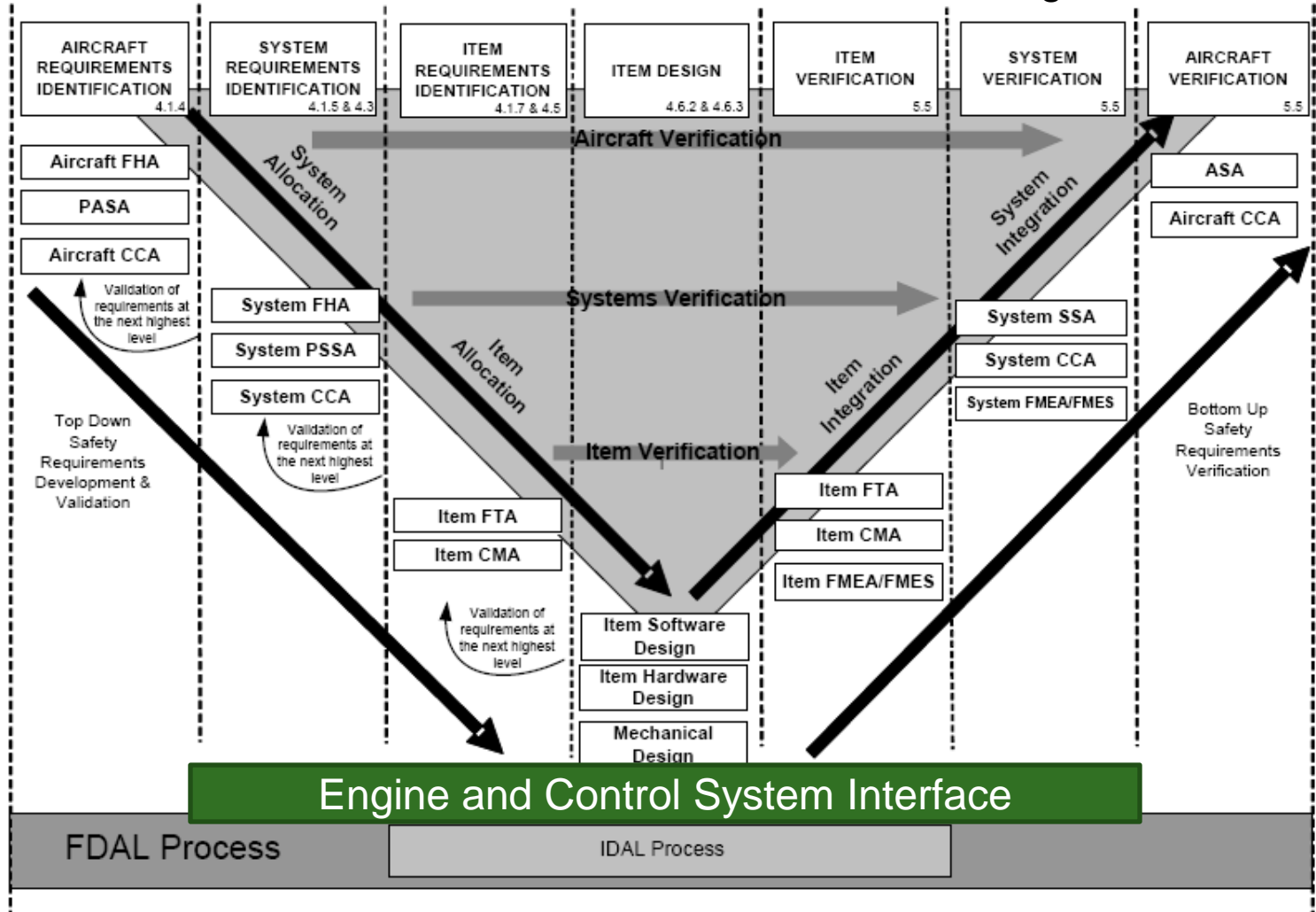
Aircraft Safety Design an Integrated “V” Process

SAE

ARP4754a

- 26 -

Credit to ARP4754 Rev a Committee for this DRAFT Figure



Traceability for Requirements, Design and Test

Control System is Planned, Designed and Verified

Honeywell

Planning => Designing =>

- **Project Specific Certification Plan**
- **Conformity Inspection Plan**
- **Design Change Proposal**
- **Control System Certification Plan**
 - RTCA/DO-160/-178/B/-254 standards
- **Plan for SW Aspects of Certification**
- **Plan for HW Aspects of Certification**

- **Control System Requirements Document (functional)**
- **Hardware procurement specifications and drawings**
- **Software detailed requirements and design documents**
- **PSSA, SSA, FTA, FMEA**
- **Various systems simulation, bench and engine testing for requirements validation**

Verification =>

- **Controls Certification Tests**
 - RTCA/DO-178B/DO-254
 - ECU SW host tests
 - ECU Target Tests
 - RTCA/DO-160F
 - ECU environmental test
 - EMI/HIRF/Lightning tests
 - **System Bench Tests**
 - Single engine/Dual FADEC
 - Dual Engine
 - **Engine ground/flight tests**
 - **SSA**
- **Hardware/Software Reconciliation**
- **Control System Accomplishment Summary**
- **Aircraft Simulated Integration Tests**
- **Aircraft Flight Tests**

RED TEXT = FAA review and approval. BLACK TEXT = Typically FAA DER review and approval.

FAA Oversight and Problem Tracking for Process

Electromagnetic Interference and High Intensity Radiated Fields (EMI/HIRF) Testing and Susceptibility

- **Performed per RTCA/DO160 specification**
 - Section 15 Power Input
 - Section 16 Voltage Spike
 - Section 17 AF Conducted Susceptibility – Power Inputs
 - Section 18 Induced Signal Susceptibility
 - Section 19 RF Susceptibility (Conducted and radiated)
 - Section 20 Emission of RF Energy
- **Testing performed as a system**
 - Includes Engine controls
 - All interface components
 - Some simulated interfaces (ARINC/ Com Bus, switches)
 - Open and/or closed loop
- **Advisory Circular AC 33.28-1 provides guidance for pass/fail criteria**

RTCA DO-160 is Industry/FAA Accepted Standard

EMI/HIRF Testing Pass/Fail Criteria

Pass/Fail criteria based on AC 33.28-1, Chapter 7

- (a) No more than 2 percent power change for less in 3 seconds.
- (b) No transfers to alternate channel or backup modes.
- (c) No fault codes that would lead to misleading hazardous or catastrophic faults recorded in memory.
- (d) No false or misleading annunciation that might lead to inappropriate or unnecessary crew action.
- (e) No hazardous operation, including actuation or disabling of the overspeed circuits.
- (f) No component damage that would prevent the test unit from meeting in-service performance-specified requirements. This includes posttest verification of the lightning protection devices.
- (g) No effect on the ability to shut the engine down.

Monitored Data Must Support Pass/Fail Criteria

- **Assure the environment does not affect the recordings**
 - EMI/HIRF/Power tests cover 400 Hz – 18 GHz
 - DO160E, Section 20, Category L for Conducted/Radiated susceptibility
 - Full threat, no nacelle attenuation – Facilitates installability
 - Field strengths 200-500 V/M average, Pulse Modulated to 7200 v/m
- **Identify the functions and collect data to prove the pass/fail criteria are met**
- **Log all observations – Problem reporting system**
- **Be wary of tests that have no failures**
 - Monitoring is ineffective

Excellence in Test Monitoring is Critical to Success

Special Topics

Honeywell

Loss Of Thrust Control (LOTC)
Time Limited Dispatch (TLD)
Uncontrollable High Thrust (UHT)
Engine Monitoring
Single Event Upset(SEU)
Software Assurance Level

- **LOTC: Definition**

- For Transport Aircraft: Loss of ability to modulate power or thrust from idle to 90% maximum rated power or thrust at given flight condition
- Engine thrust oscillates in an unacceptable manor
 - ◆ Typically defines as +/- 5% of takeoff power

- **Certification Approach**

- Use FHA to identify the system requirements
- Use FTA and FMEA to determine predicted failure rates
- Roll up and determine LOTC probability
- Must meet $< 1 \times 10^{-5}$ /hour criteria
- SSA documents all information

LOTC Defines Acceptable Risk of Power Changes

Time Limited Dispatch

Honeywell

- A method of allowing operation in the presence of faults, **for a limited time**, that assures average system reliability as good as, or better than, a specified level
- TLD takes advantage of available redundancy to permit scheduling of maintenance at convenient intervals
 - No system effect with 1 failure
- Based on maintaining System integrity and reliability level equal to or better than historical Hydromechanical systems
 - Average control system integrity (MTBF for LOTC events per engines in this application) is 100,000 hours part 25, 27, 29 aircraft
 - Markoff Model methodology used to predict reliability
- **Fault Categories/Dispatch Definitions**
 - No Dispatch (ND) Faults
 - Short-Time (ST) Dispatch Faults (i.e. 125 hours)
 - Long-Time (LT) Dispatch Faults (i.e. 500 hours)

TLD Takes Advantage of System Redundancy

- **A result of the September 6, 1997, Saudi Arabian Airlines Boeing 737-200 accident**
 - Un-commanded high thrust failure condition resulted in flight crew unable to reduce engine thrust/power through normal means
 - Takeoff was aborted, the speed brakes were deployed and brakes applied. The thrust reversers did not deploy.
 - The 737 aircraft overran the runway into the sand. Both main gear legs collapsed during a ground-loop and the # 2 engine separated.
 - The fuselage was last seen in use as a snack bar at the King Khalid Air Base, Saudi Arabia in 2003.
- **UHT defined in 3 critical flight regimes**
 - Takeoff,
 - Approach
 - Landing ground roll

UHT Similar to Unintended Acceleration Issue

Uncontrollable High Thrust

- **Can be caused by fuel system contamination**
 - Metering valve stuck at high flow rate
- **Failure criticality dependent on airframe**
 - Wing mounted engine results in more asymmetric thrust.
- **Two major certification approaches**
 - Analyze the aircraft controllability
 - ◆ Can be difficult to convince FAA of validity
 - Design control system to shut the engine down in UHT condition
- **Design requires an Assurance Level A system**
 - Requesting the control system to be Sentient
 - Must predict all possible conditions and failure modes
 - Limited number of sensors (Weight/cost/reliability)
 - ◆ (i.e. Don't have G force, sound, sight etc)

UHT Solutions Require Rigorous Design Process

Honeywell Integrated Condition Based Monitoring

Flight Control Maintenance Diagnostics System



Platform Soldier Mission Readiness System



Primus Epic® Central Maintenance & Aircraft Condition Monitoring



Health & Usage Monitoring (HUMS)



Zing™ Vehicle Diagnostics



CEV Orion Systems Management & Abort Determination



Aircraft Information Management



777 Central Maintenance & Aircraft Condition Monitoring



787 Crew Information & Maintenance System

Automotive - Integrated Vehicle Health Management (IVHM)



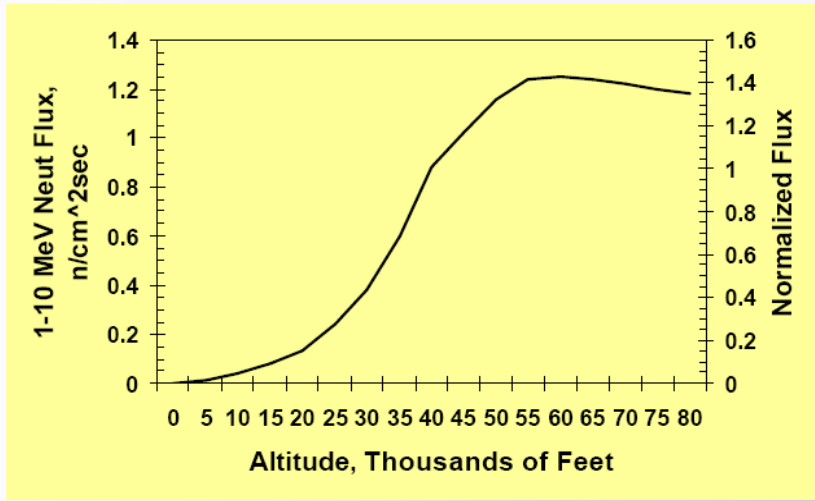
Monitoring Occurs in ALL Platforms

Engine Condition Trend Monitoring

- Field monitoring required for Catastrophic and Hazardous events
- Most modern controllers have monitoring data
- The data can include
 - Performance data
 - Life Cycle counting
 - Event recorders (can be programmed)
 - Engine utilizations data
 - Engine exceedance data
 - Fault recording
 - Continuous “crash” recorder
- Data can be managed on or off aircraft
- Maintenance computer stores faults and exceedances.

Monitoring Provides Data for Incident Investigations

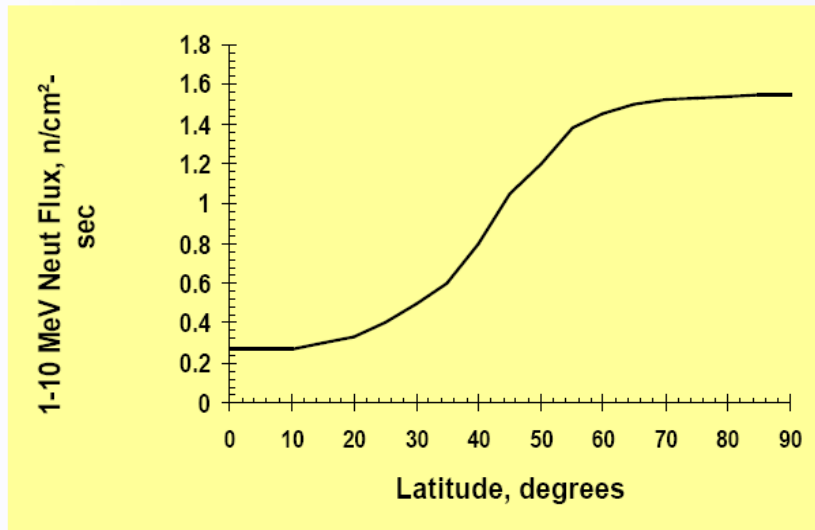
Single Event Upset (SEU) (non-destructive)



- SEU must be part of the design strategy
- Part of SSA effort (1E-8 to 5xE-10 per flight hour)

Implementation Strategies

- Memory redundancy
- Memory verifications (CRC)
- ECU redundancy
- Fault accommodation
- Critical data stored is strategically (devices less susceptible)



High Altitude and Over the Poles is Most Severe

General Protection Fault:31102

MICROSOFT POWER POINT has caused a general protection fault in module KRNL386.exe at 0001:0000751
It has performed an illegal operation. You can push escape to return to windows and save any unsaved information or you can restart your computer.

- * Press any key to return to windows
- * Press CTRL+ALT+DEL again to restart your computer
You will lose unsaved information in programs that are running

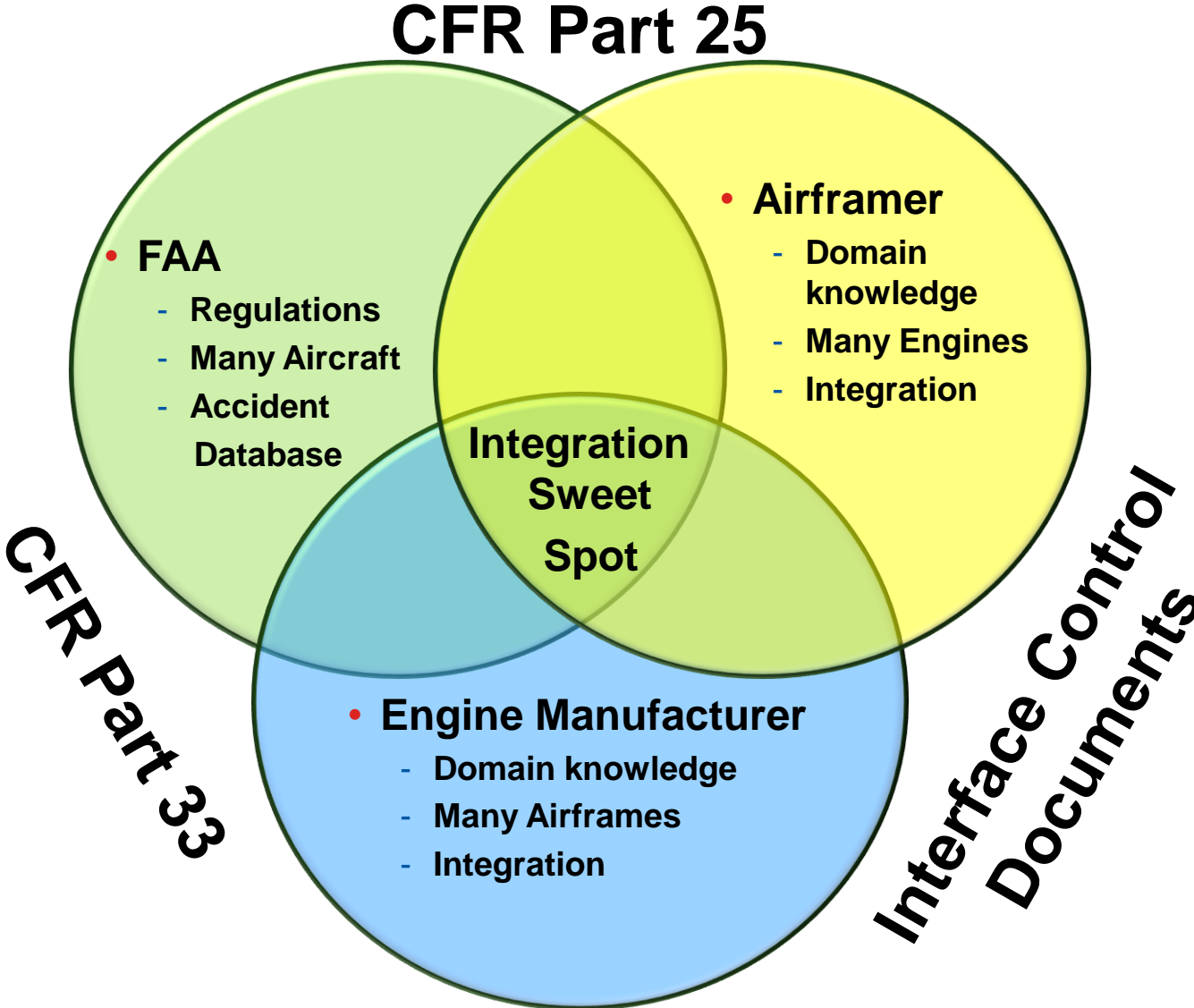
SEU Does Occur on the Ground Too !

Software Assurance Level

- SW is not certified, SW is designed to an assurance level
- RTCA/DO-178B current standard (C is on it's way)
- Rigorous process focused development
 - Very specific SW objectives
 - Objectives vary based on assurance level
 - QA and Configuration management overarching processes
- FAA approval of cert plans and supporting documents
- FAA oversight based on assurance level and experience
- Level A SW will not eliminate Level A events (catastrophic)
- Level A SW does not eliminate SW bugs
- Level A mitigates the probability and criticality of significant SW bugs in the control system

Monitoring Provides Data for Incident Investigations

Certification Environment Very Regulated



Integration Required for Certification Excellence

QUESTIONS?

NOTE:

References at End of Material

REFERENCES

FAA Advisory Circulars

FAA Orders/Notices

RTCA Standards

SAE International Papers

- **AC 20-136A**
 - **Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning**
- **AC 25-1309**
 - **System Design and Analysis**
- **AC 33.4-1**
 - **Instructions for Continued Airworthiness**
- **AC 33.28-1**
 - **Compliance Criteria for 14 CFR Section 33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems**
- **AC 33.87-1**
 - **Calibration Test, Endurance Test and Teardown Inspection for Turbine Engine Certification (33.85, 33.87, 33.99)**

- **Order 8110.49 dated June 3, 2003**
 - Software Approval Guidelines
- **Notice N8110.71 dated April 2, 1998**
 - Guidance for the Certification of Aircraft Operating in High Intensity Radiated Field (HIRF) Environments
- **Order 8110.105 dated July 16, 2008**
 - Simple And Complex Electronic Hardware Approval Guidance
- **PS-ANE100-2001-1993-33.28TLD-R1, June 29, 2001**
 - Policy for Time Limited Dispatch (TLD) of Engines Fitted with Full Authority Digital Engine Controls
- **Notice 8300.117 Dated December 20, 2004**
 - Uncontrolled High Thrust

- **RTCA/DO-160F**
 - **Environmental Conditions and Test Procedures for Airborne Equipment**
- **RTCA/DO-178B**
 - **Software Considerations in Airborne Systems and Equipment Certification**
- **RTCA/DO-254**
 - **Design Assurance Guidance for Airborne Electronic Hardware**

- **ARP5107B**
 - **Guidelines for Time Limited Dispatch (TLD) Analysis for Electronic Engine Control Systems; November 2006**
- **ARP5583**
 - **Guide to Certification of Aircraft in a High Intensity Radiated Field (HIRF) Environment; January 2003**
- **ARP 4754 (Rev A in process)**
 - **Certification Considerations For Highly-integrated Or Complex Aircraft Systems; November 1996**
- **ARP 4761**
 - **Guidelines And Methods For Conducting The Safety Assessment Process On Civil Airborne Systems And Equipment; December 1996**
- **ARP 5757**
 - **Guidelines for Engine Component Tests; March 2008**

Reference Page (Major Links)

- All CFR, AC, Order, Notice references can be found at:
 - [http://www.airweb.faa.gov/Regulatory and Guidance Library/rgWebcomponents.nsf/Frameset?OpenPage](http://www.airweb.faa.gov/Regulatory_and_Guidance_Library/rgWebcomponents.nsf/Frameset?OpenPage)
- RTCA references can be found at:
 - <http://www.rtca.org/>
- SAE International references can be found at:
 - <http://www.sae.org/pubs/>
- Michael James
 - Michael.james@honeywell.com
 - (602) 231-7068