Crane Aerospace & Electronics

Design Considerations for
Flight Critical Power Systems
APEC 2015

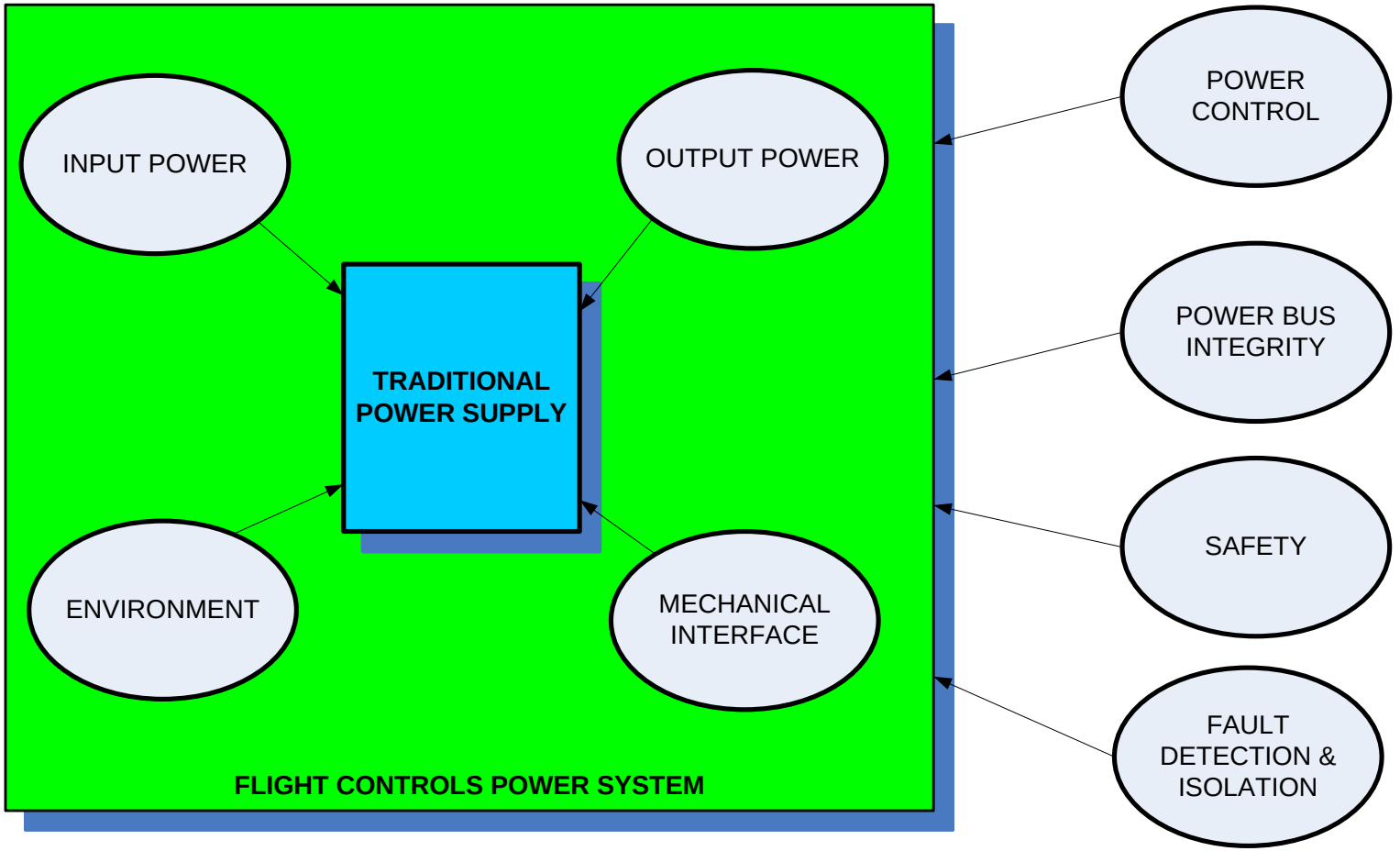
CRANE®
AEROSPACE &
ELECTRONICS

Abstract

- Flight Control Power Systems represent a unique challenge for commercial power supply applications.
- This presentation will discuss the major design considerations that need to be addressed for powering flight control electronics equipment on commercial aircraft.
- Topics will include Power Bus Integrity, Power Control, Safety Related Functions, Fault Protection, Monitors and Reporting.

Traditional vs. Flight Control Power Systems

- Flight control considerations adds complexity to traditional power supply design



Drives the need to use a systems level development approach

Systems Approach to Design

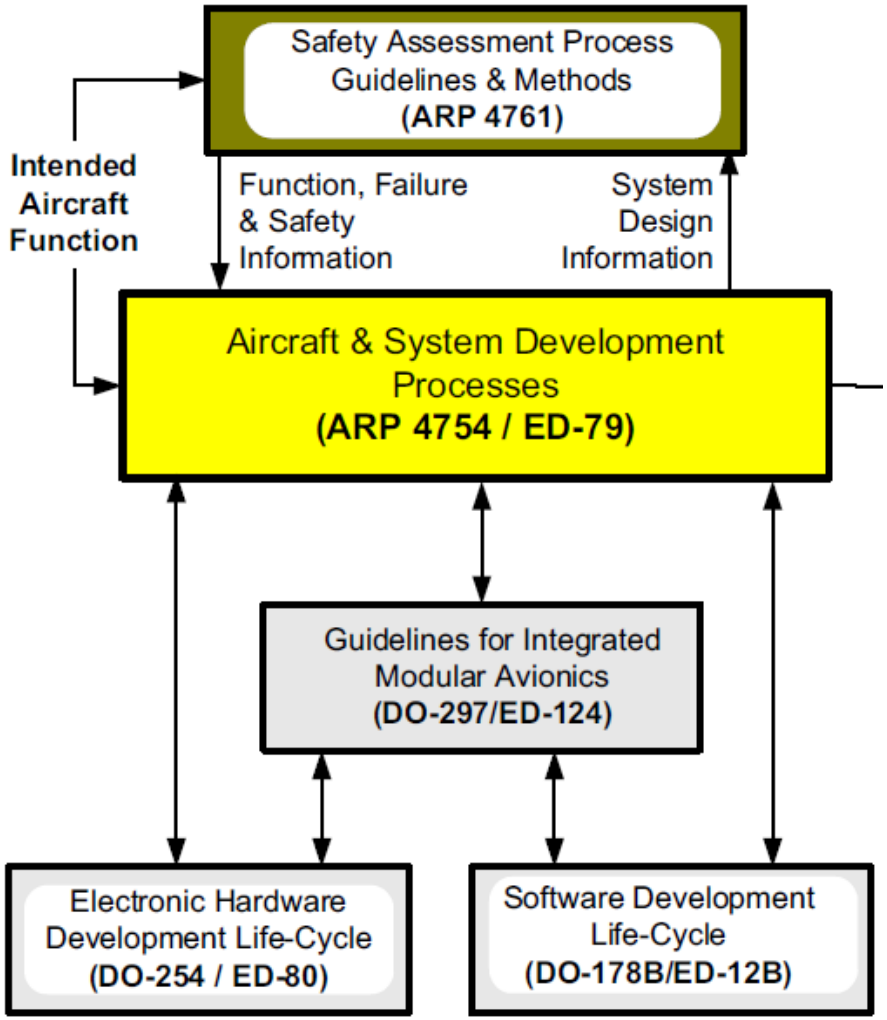
- Air Worthiness Authorities and their regulations are the driving force for equipment used on aircraft.

- FAA Advisory Circular Examples
  - AC 20-174 Development of Civil Aircraft and Systems
  - AC 20-170 Integrated Modular Avionics Development, Verification, Integration and Approval using RTCA/DO-298 and Technical Standard Order C153
  - AC 20-152 Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware
  - AC 20-115 C Airborne Software Assurance

- FAA Order Example
  - Order 8110.105, Change 1, Simple and Complex Electronic Hardware Approval Guidance

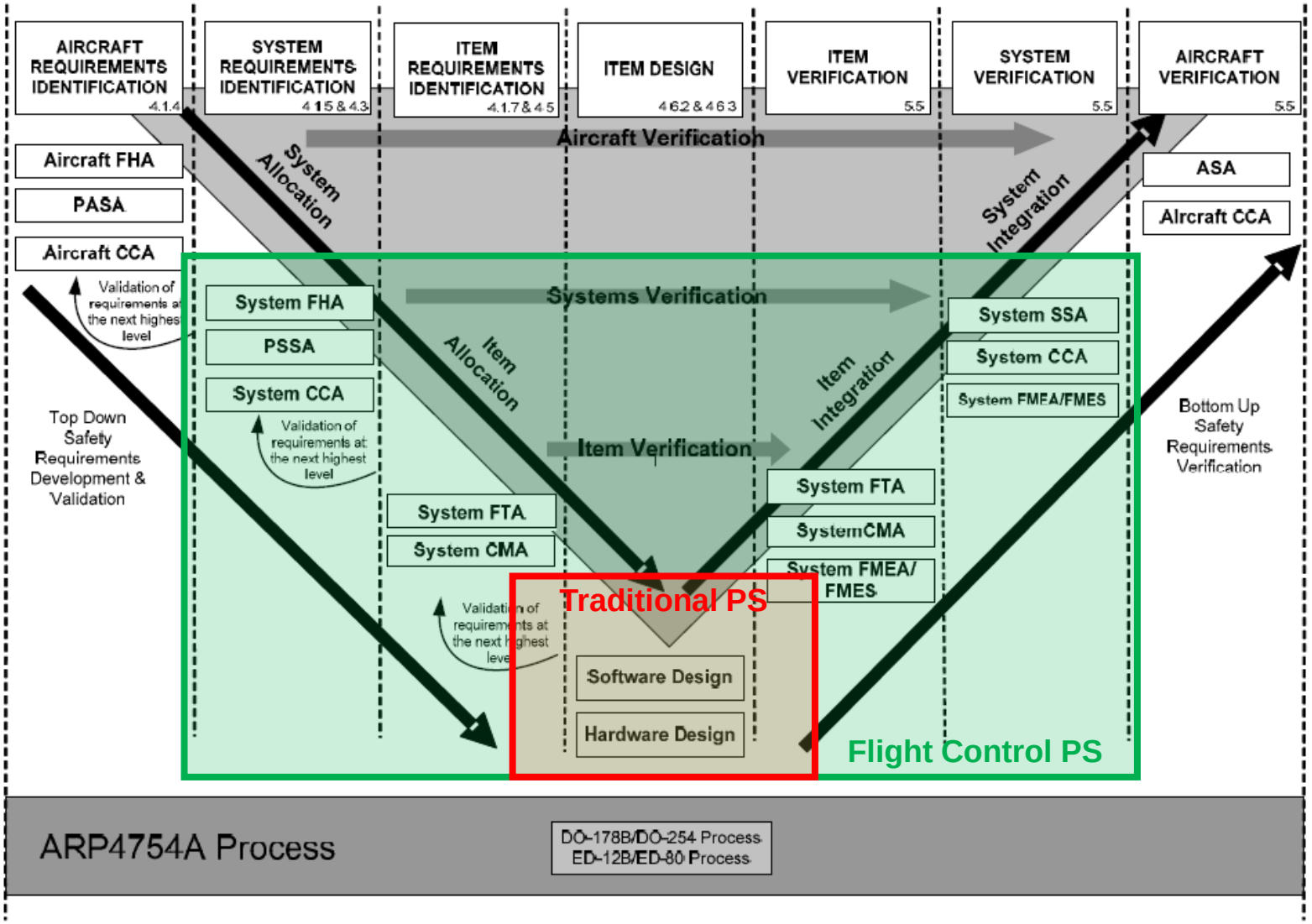
Systems Approach to Design

- Industry Standards and Guidelines for Product Development



Systems Approach to Design

- Flight Control Power System Responsibilities are expanded



Systems Approach to Design

- Requirements generation and management are key to a successful development program
  - Driven by Safety
  - Level of scrutiny driven by criticality of functions
  - Goal is to minimize design errors
  - Implemented using an organized development process
  - Provide evidence of work products for certification support

- Requirements at the proper levels are needed to create the Architecture and Design

- Verification must be against the requirement sets

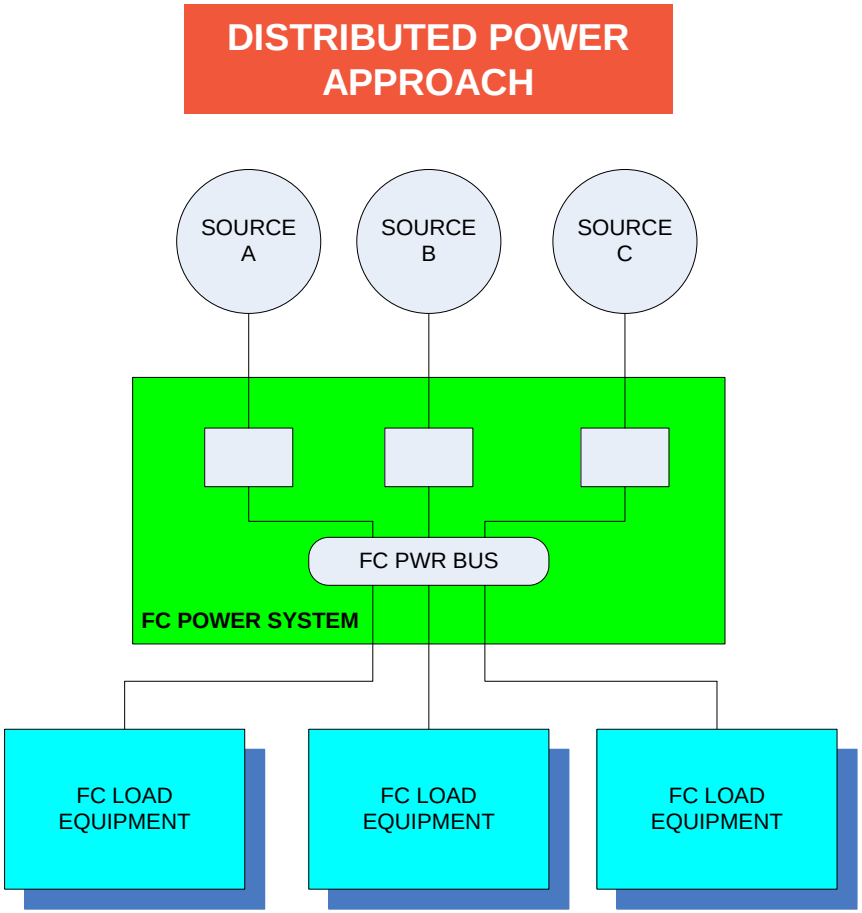
Systems Approach to Design

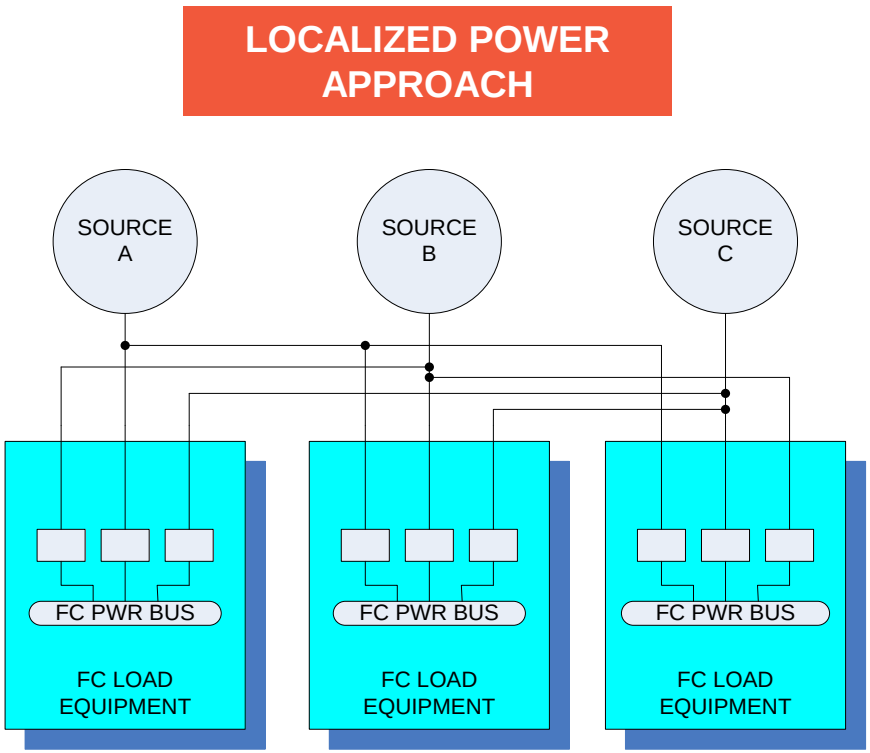
Failure Condition Classification	Impact on Passengers& Cabin Crew	Impact on Aircraft (Safety Margin)	Flight Crew (Pilots)	Allowable Quantitative Probability (per Flt Hr)	Design Assurance Level
Catastrophic	Multiple Fatalities	Loss of aircraft; Unable to continue safe flight and landing	Unable to respond or compensate for the failure condition	< 1E-9	A
Hazardous	Serious or fatal injury to small number of occupants.	Large reduction in safety margins or functional capability of aircraft.	Physical distress or excessive workload; such that crew cannot perform tasks accurately or completely.	< 1E-7	B
Major	Physical distress or injuries to passengers or cabin crew	Significant reduction in safety margins or functional capability of aircraft.	Significant increase in workload or in conditions impairing crew efficiency; possible discomfort to the flight crew.	< 1E-5	C
Minor	Physical discomfort to passengers or cabin crew	Slight reduction in safety margins or functional capability of aircraft.	Slight increase in workload; implementation of countermeasures (e.g. revised flight plan)	< 1E-3	D
No Safety Effect	Not defined.	No effect on safety or operational capability of the aircraft.	No effect on crew workload.	No requirement	E

This summary table is derived from FAA AC25.1309-1B and EASA AMC 25.1309

Power Bus Integrity

- High level of integrity
- Forces architectures with redundancy
- Redundancy approach can be implementation specific





Power Control

- Power typically needs controls on input and/or output
  - Controls must be compatible with power bus integrity requirements

- Considerations for systems with multiple inputs
  - On/Off control
  - Priorities of input source
  - Automatic switching of sources to achieve uninterruptable power
  - Protection between power sources

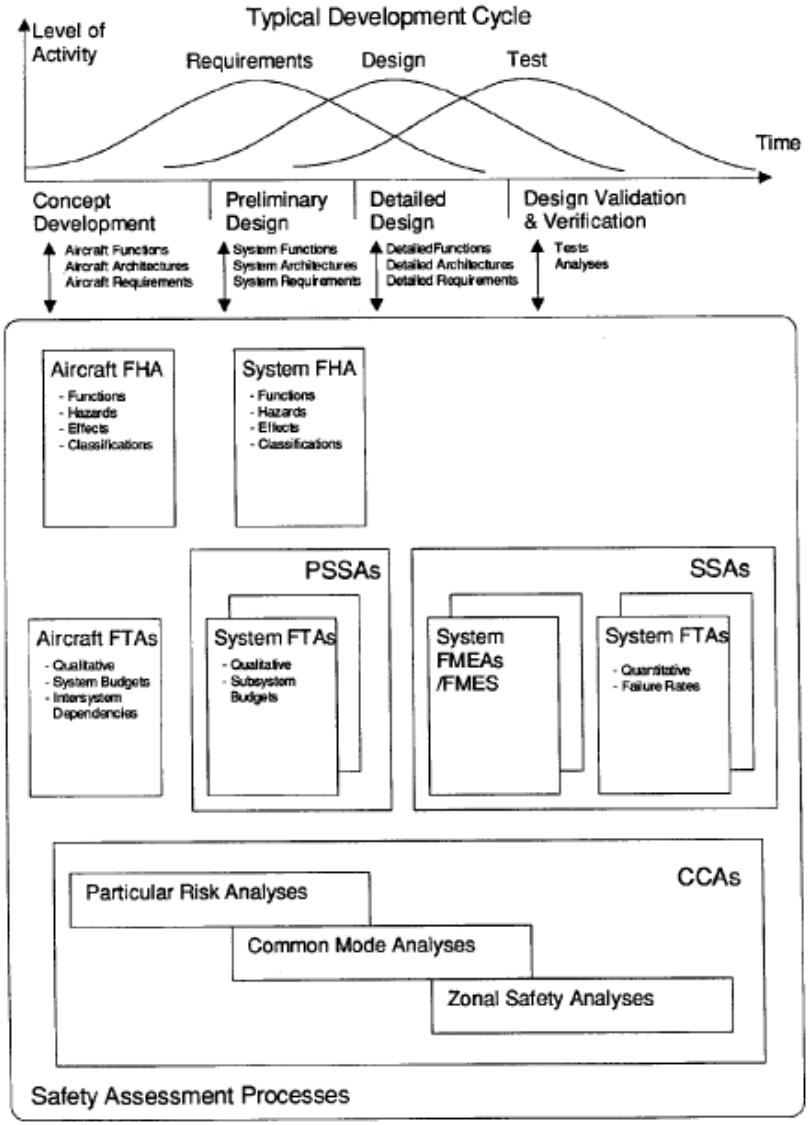
- Considerations for systems with multiple outputs
  - On/Off control
  - Protection means
    - Internal Hazards
    - External Hazards
    - Protection between outputs

Safety Related Functions

- ARP4761 Process Overview
  - FHA – Functional Hazard Assessment
  - PSSA – Preliminary System Safety Assessment
    - FTA – Fault Tree Analysis (Preliminary)
  - SSA – System Safety Assessment
    - FMEA – Failure Modes & Effects Analysis
    - FTA – Fault Tree Analysis (Update & Quantification)
  - CCA – Common Cause Analysis
    - ZSA – Zonal Safety Analysis
    - PRA – Particular Risks Analysis
    - CMA – Common Mode Analysis

Safety Related Functions

- Safety Assessment Process is integrated into the development cycle
- Both Qualitative and Quantitative Requirements must be considered
- Common Cause Analysis are also required



Safety Related Functions

- Often drives levels of redundancy into the design
  - May also require dissimilar implementation
- Typically requires independent control and monitor functions
- May require physical separation of functions
- May require isolation between functions

Fault Protection

- Required to prevent hazards from propagation
  - From loads or sources to power system
  - From power system to loads and sources
- Often requires a level of integrity
  - Drives power system architecture
  - Requires fault tree analysis to verify

Monitor and Reporting

- Required to minimize exposure times for power system safety requirements
- Often required to support flight control level safety requirements
- Required to support on aircraft maintenance objectives
  - Fault Detection
  - Fault Storage
  - Fault Isolation
- Typically reported using combination of discrete and data bus interfaces

Concluding Remarks

- Flight Control Power System considerations add complexity
- Systems approach to development is necessary to ensure a safe design
- Working hand in hand with your customer is key to the success of the program

The Crane Advantage!

for more information please visit CraneAE.com