Unique Dependability Issues for Commercial Airplane Fly-By-Wire Systems

Y. C. (Bob) Yeh, Ph. D.
Associate Technical Fellow
Boeing Commercial Airplanes
Flight Controls Systems

18th IFIP World Computer Congress
Toulouse, France, August 22-27, 2004

Topical Days #3 Fault Tolerance for
Trustworthy and Dependable
Information Infrastructures, August 23-24, 2004

Unique Dependability Issues for Commercial Airplane Fly-By-Wire Systems

- Introduction
  - Fundamental Concepts of Dependability
  - Flight Controls Industry Experiences on Design Faults
- Generic Error and Dissimilarity Considerations
- Common Mode Failure and Single Point Failure
- Simplicity

Fundamental Concepts of Dependability (Avizienis & Laprie & Randell)

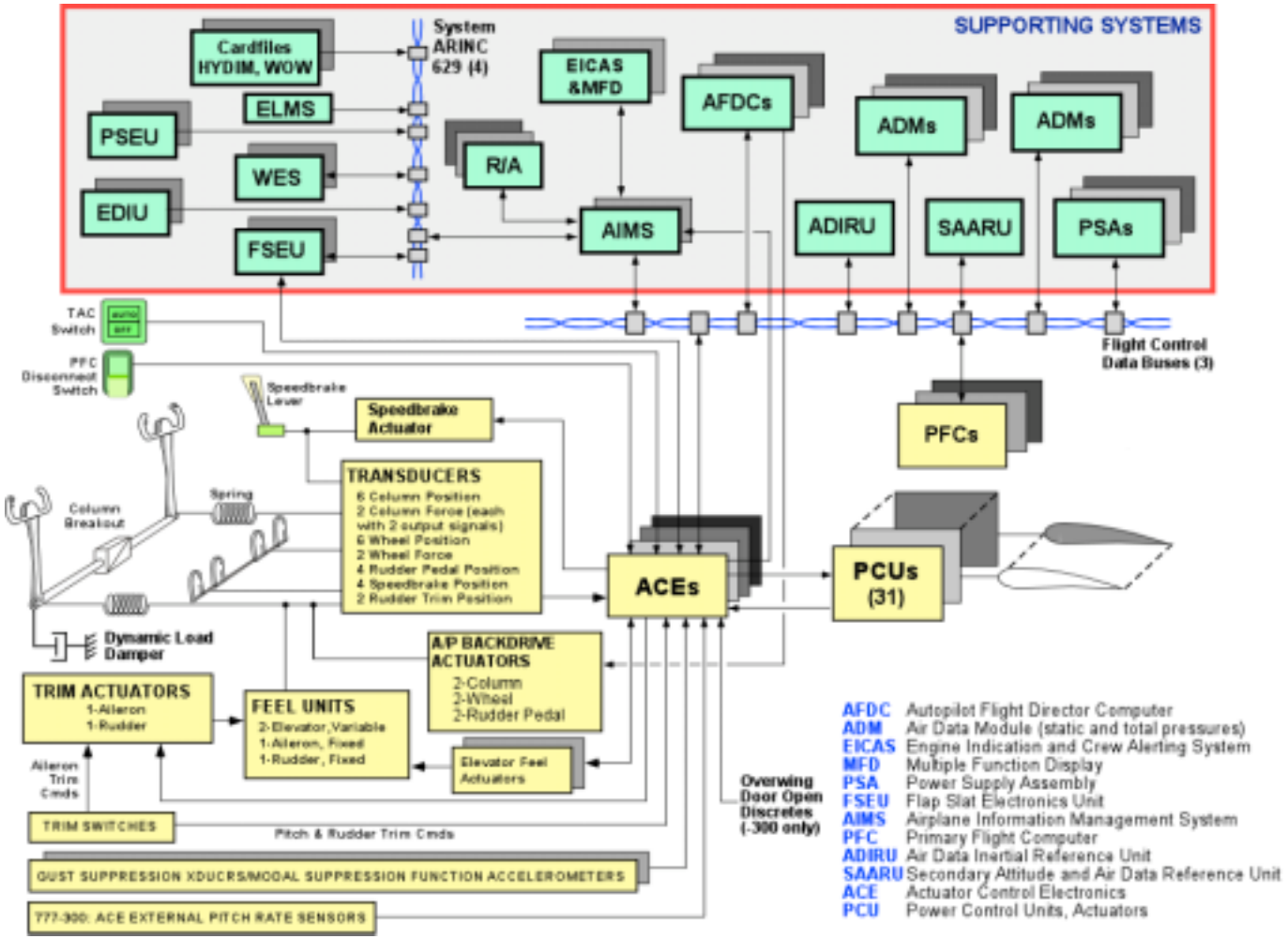
- Among 4 classes of accidental or non-malicious faults,
  - Human-made interaction faults
  - Design faults
  - Physical internal faults
  - Physical external faults
- Human-made interaction and design faults dominate as sources of failure/error for larger, controlled systems

Flight Controls Industry Experiences on Error Types of Complex Flight Controls Systems

- Requirement Error*
- Implementation Misunderstanding*
- Software Design or Coding Error*
- Future Process Errors in Previously Qualified Electronics Parts
- Relatively new programmable VLSI circuits whose number of states approach infinity and therefore non-deterministic

**Can be attributed to Interaction Fault, Software/Hardware Interface Incompatibility*

777 Primary Flight Control System

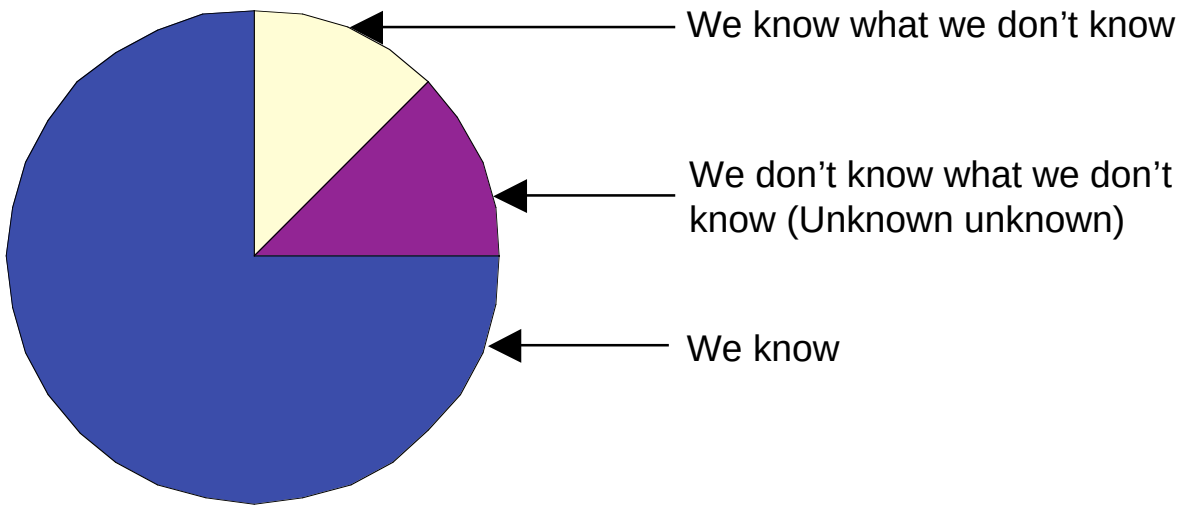


Generic Error and Dissimilarity Considerations of FBW Systems

- *Airbus FBW is designed to cover software design faults via design diversity*
- *Boeing FBW is designed to cover (very complex) hardware design faults and compiler faults*

Common Mode Failure and Single Point Failure

- *To meet extremely high functional integrity and functional availability requirements (of 1.0E-10 per hour), multiple redundant hardware resources are required for FBW systems.*
- *The fault tolerance for trustworthy FBW system design should consider all known and unknown causes of problem/failure/error, known as common mode failure and single point failure.*



Common Mode Failure and Single Point Failure

- *Airplane susceptibility to common mode and common area damage is addressed by designing the systems to both component and functional separation requirements. This includes criteria for providing installations resistant to maintenance crew error or mishandling, such as:*
  - *impact of objects*
  - *electrical faults*
  - *electrical power failure*
  - *electromagnetic environment*
  - *lightning strike*
  - *hydraulic failure*
  - *structural damage*
  - *radiation environment in the atmosphere*
  - *ash cloud environment in the atmosphere*
  - *fire*
  - *rough or unsafe installation and maintenance*

Simplicity of Direct Mode and its Transition

- *The virtue of simplicity is preserved in otherwise complex FBW systems via:*
  - *Simplicity of Transition to Direct Mode*
  - *Simplicity of Direct Mode hardware implementation*

Primary Flight Control Modes

	PITCH	ROLL	YAW
NORMAL Control	CONTROL C* Maneuver Cmd with Speed Feedback **Manual Trim for Speed Variable Feel** ENVELOPE PROTECTION Stall Overspeed AUTOPILOT Backdrive	CONTROL Surface Cmds Manual Trim Fixed Feel ENVELOPE PROTECTION Bank Angle AUTOPILOT Backdrive	CONTROL Surface Cmd Ratio Changer Wheel/Rudder Cross Tie Manual Trim Yaw Damping Fixed Feel Gust Suppression ENVELOPE PROTECTION Thrust Asymmetry AUTOPILOT Backdrive
SECONDARY Control	CONTROL **Surface Cmd (Augmented)** **Flaps Up/Down Gain** **Direct Stabilizer Trim** **Flaps Up/Down Feel**	CONTROL Surface Cmd Manual Trim Fixed Feel	CONTROL Surface Cmds, Flaps Up/Down Gain PCU Pressure Reducer Manual Trim Yaw Rate Damper (If available)
DIRECT Control	CONTROL **Surface Cmd (Augmented)** **Flaps Up/Down Gain** **Direct Stabilizer Trim** **Flaps Up/Down Feel**	CONTROL Surface Cmd Manual Trim Fixed Feel	CONTROL Surface Cmds, Flaps Up/Down Gain PCU Pressure Reducer Manual Trim

Actuator Control Electronics Architecture