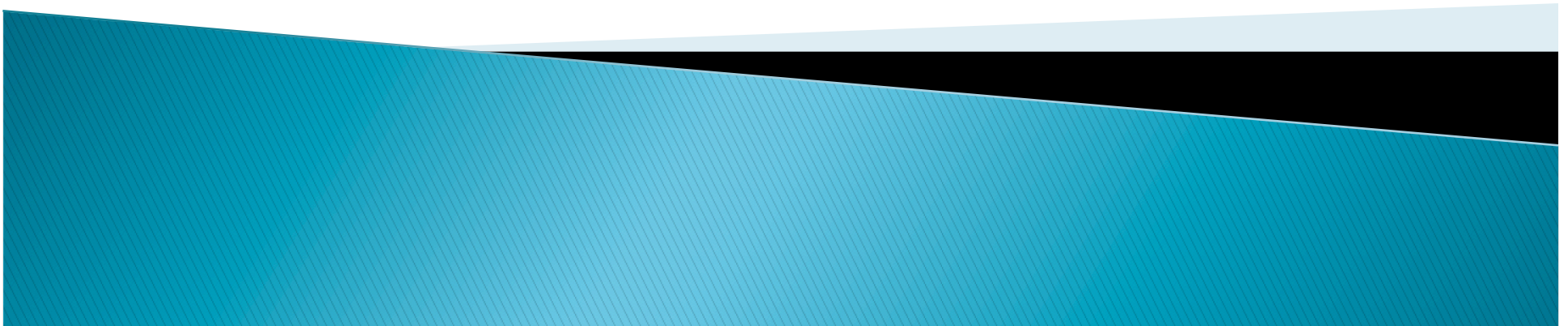


Airbus Software Failures and the Lufthansa A320 Crash

CS777– Software Reliability and Quality
Assurance

By: Anthony Sinatra



Airbus and Fly-By-Wire Technology

- ▶ One of the first manufacturers to develop 'fly-by-wire' technology
- ▶ Introduces a computer system between pilot and control surfaces
- ▶ Computer is actually flying the plane with pilot as a guide
- ▶ Prevent the aircraft from being handled dangerously by preventing pilots from exceeding preset limits, such as stall, spin or limiting

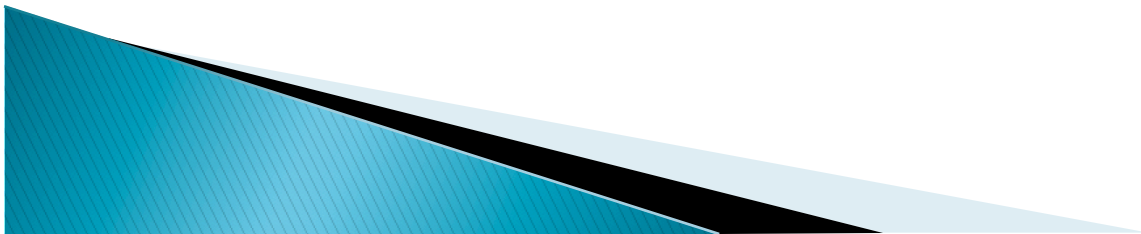


Fly-By -Wire Technology (mishap)



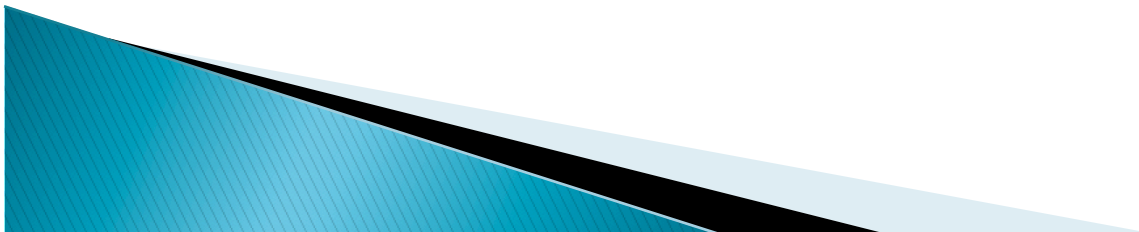
Lufthansa Flight # 2904 and the Airbus A320

- ▶ September 14, 1993, Lufthansa flight 2904, an Airbus 320, landing in Warsaw in crosswinds, wind-shear, and rain.
- ▶ High winds and water fooled the computer to think the aircraft had not yet landed.
- ▶ Computer disabled the braking system.
- ▶ Skidded off the runway and killed first officer, one passenger and injured 45 others.
- ▶ Aircraft completely destroyed



Lufthansa Flight # 2904 and the Airbus A320 software

- ▶ In order for thrust–reverse and brake flaps to be activated, one of two conditions must be met:
 - Aircraft must be lower than 3 meters and there is a weight of over 12 tons on each landing gear
 - Wheels of plane are turning with more than 72 knots
- ▶ Neither condition was met upon landing so the braking system was not activated
 - Plane landed inclined to balance wind shear so 12 tons on each landing gear was not reached
 - Plane hydroplaned so the 72 knots speed was not met



Lufthansa Flight # 2904

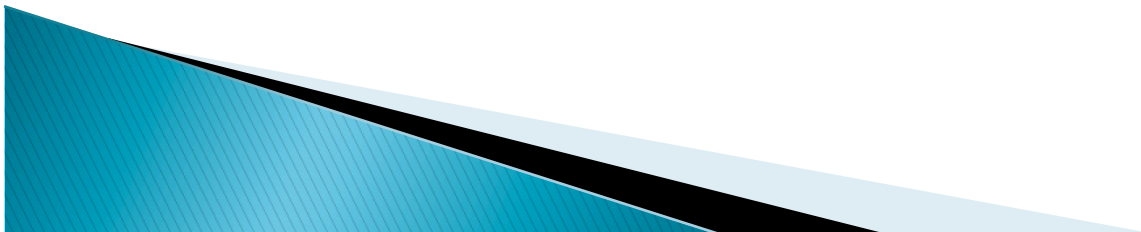


Photo Copyright Mariusz Słecinski

AIRLINERS.NET

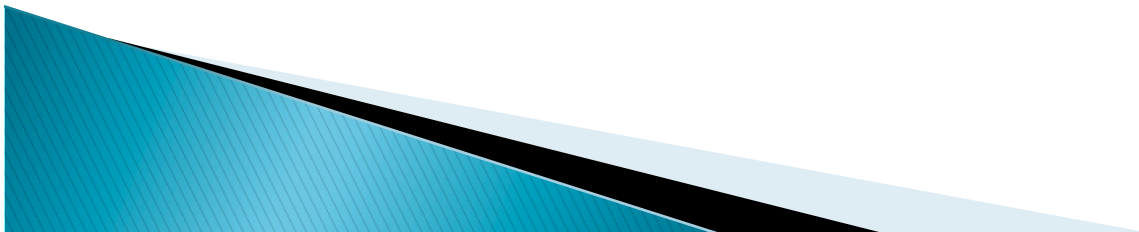
Airbus and Reliability

- ▶ Catastrophe could have been prevented if landing logic was re-worked.
- ▶ Not necessarily a bug, but a design flaw
- ▶ Airbus never accounted for these landing conditions
- ▶ Airbus changed the sensors to trigger brakes at 2 tons, not 12.
- ▶ Lufthansa changed the operating procedures



Airbus and Reliability

- ▶ System unreliable for pilots because plane landed although not 'technically'
- ▶ Software conditions for landing not met so no braking applied
- ▶ If pilots were informed about the braking system, incident may have been avoided.
- ▶ Combination of software and human causes is ultimately responsible



Airbus Reliability Levels

- ▶ Realistic level of reliability of 99.99996% or more
- ▶ 1960 A320s X 4 flights per day (average) X 365 days a year = 2,822,400
- ▶ $2,822,399 / 2,822,400 = .9999996$ or 99.99996% reliability (one incident per year)
- ▶ If system was tested under many different scenarios, design flaw could have been capture prior to release

