General Certification Assumptions and Possible Pitfalls

Jeffery Schroeder

ICAO Regional Workshop on LOC-I
Lagos, Nigeria
November 19, 2019

Main points

- It’s all about assumptions…too often, we quickly agree on those, and then spend time on the subsequent process

- Since regulations and standards do not consider every scenario, compliance does not necessarily ensure safety

- Even in hindsight, many of the original B737MAX decisions were grey

Outline

- General assumptions (FAA presentation)
  - Definitions
  - Process
  - FHA, FMEA, Fault Tree
- Design grey areas
  - Using single AoA sensor
  - Not putting MCAS in FCOM
  - AOA Disagree alert
  - ODA
- Possible pitfalls (JOEB, NTSB)
  - Pilot – training, identification, response (3 sec)
  - Cannot test all failure paths
  - Multiple failures

General Assumptions

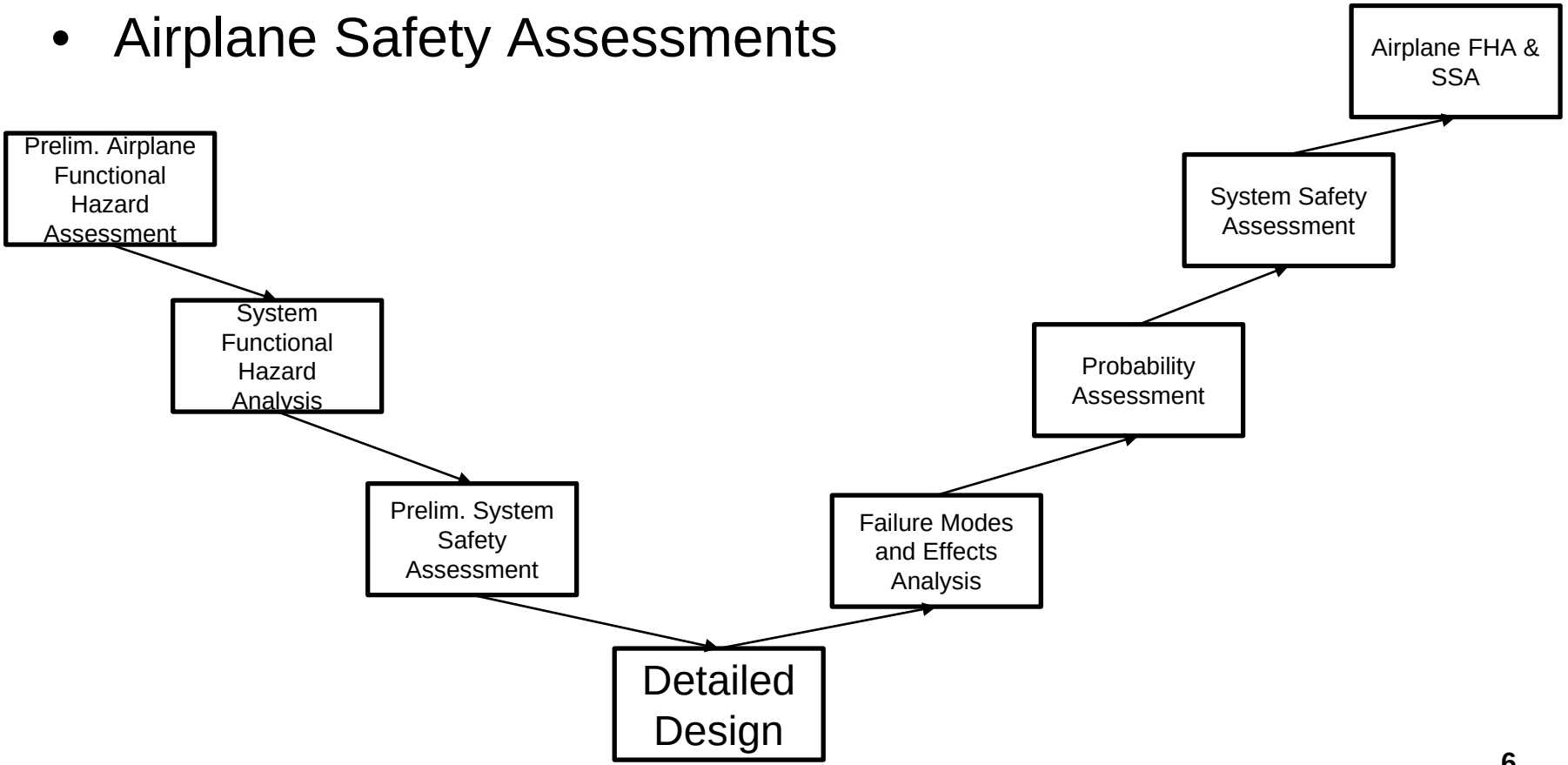
- Definitions
  - Design: Type Certificate
    - Includes airworthiness and operating limitations
    - Manufacturer must show design meets FAA regulations
    - Testing is a key component, like aircraft must take ultimate load (3.75g) for 3 secs without breaking
    - New aircraft must meet the improved requirements (e.g., noise)
    - Certification basis documented on Type Certificate Data Sheet
  - Production: Production Certificate
    - Shows company can consistently reproduce the design
    - Continuing audits check production quality is maintained
    - Parts manufacturer approval - includes modified and replacement parts
  - Airworthiness: Airworthiness Certificate
    - Conforms to its Type Certificate
    - In a condition for safe operation

General Assumptions

- Process

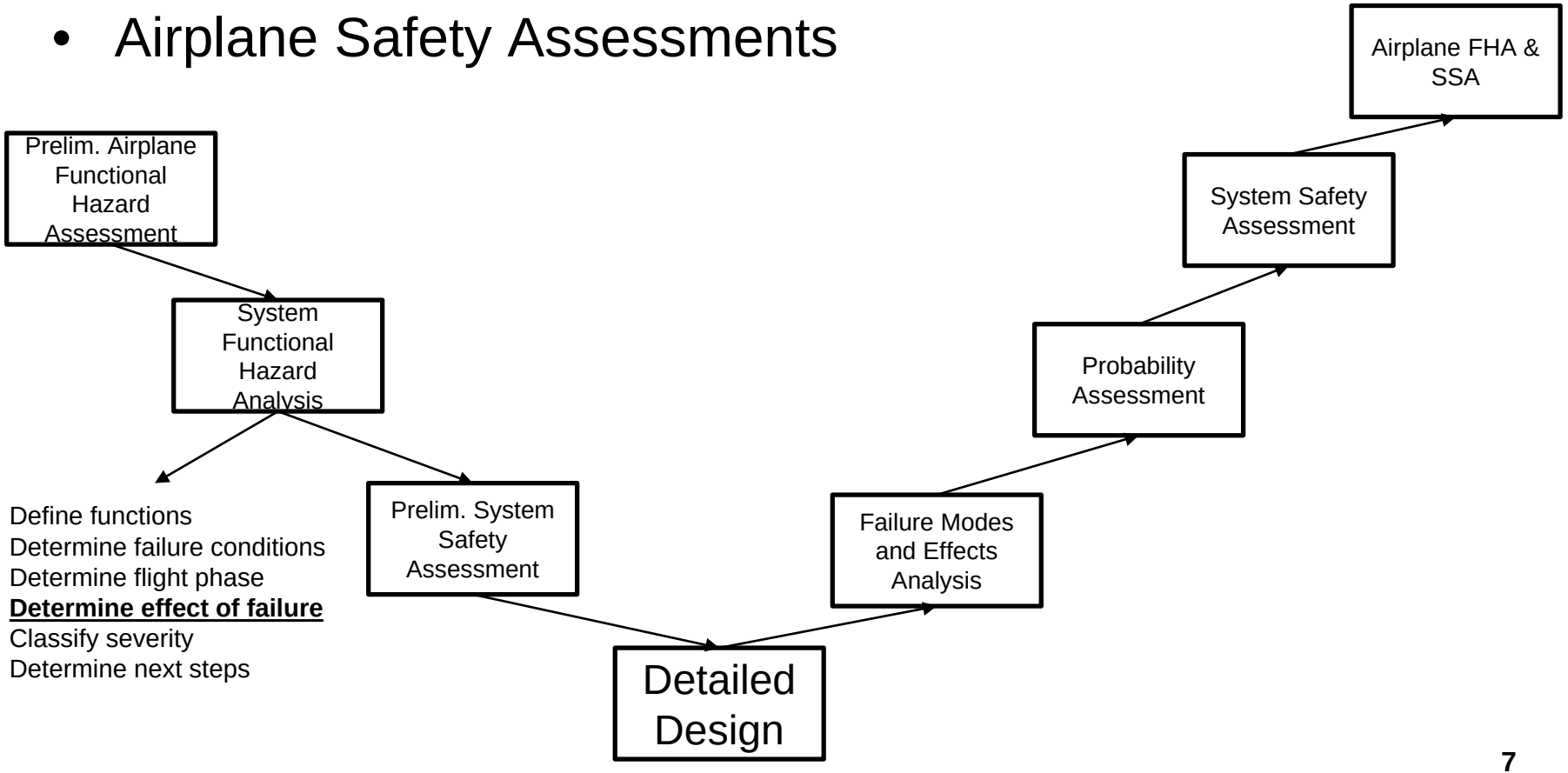
General Assumptions

- Airplane Safety Assessments



General Assumptions

- Airplane Safety Assessments



- Define functions
- Determine failure conditions
- Determine flight phase
- **Determine effect of failure**
- Classify severity
- Determine next steps

General Assumptions

- Assumptions in determining effect of a failure
  - Pilot procedure: Pilot follows appropriate actions and procedures
  - Pilot workload: Pilot workload increase can reduce safety margins
  - Flight phase: List includes typical phases from taxi to landing roll

General Assumptions

- Determine effect of failure

Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Allowable Qualitative Probability	No Probability Requirement	<--Probable--->	<---Remote--->	Extremely <----------> Remote	Extremely Improbable
Allowable Quantitative Probability: Average Probability per Flight hour on the Order of:	No Probability Requirement	<----------> $<10^{-3}$ Note 1	<----------> $<10^{-5}$	<----------> $<10^{-7}$	$<10^{-9}$
Classification of Failure Conditions	No Safety Effect (V)	<-----Minor----> (IV)	<----Major----> (III)	<-Hazardous--> (II)	Catastrophic (I)
DO-178B Software Levels	Level E	Level D	Level C	Level B	Level A
Note 1: A numerical probability range is provided here as reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category airplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.					

Source is Advisory Circular 25.1309A “System Design and Analysis”

General Assumptions

Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Allowable Qualitative Probability	No Probability Requirement	<--Probable--->	<---Remote--->	Extremely <----------> Remote	Extremely Improbable
Allowable Quantitative Probability: Average Probability per Flight hour on the Order of:	No Probability Requirement	<----------> $<10^{-3}$ Note 1	<----------> $<10^{-5}$	<----------> $<10^{-7}$	$<10^{-9}$
Classification of Failure Conditions	No Safety Effect (V)	<-----Minor----> (IV)	<----Major----> (III)	<-Hazardous--> (II)	Catastrophic (I)
DO-178B Software Levels	Level E	Level D	Level C	Level B	Level A
Note 1: A numerical probability range is provided here as reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category airplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.					

Increasing analysis requirements requirements

- Design appraisal
- Failure modes and effects analysis
- Fault trees

Design grey areas

- **“How could you use a single AOA sensor in B737MAX?”**
  - Myth exists that airplane systems do not use single sensors
    - It all depends on the safety effect of the failure of a single sensor
  - Erroneous AOA can cause MCAS to activate, which can result in up to 15% stabilizer movement in 10 secs, causing a pitch down
    - Expected pilot actions include countering pitch down with column inputs and trimming out column forces (AC 25-7C: “The pilot will take immediate action to reduce or eliminate high control forces by re-trimming or changing configuration or flight conditions.”)
  - Large AOA errors cause disagree messages (airspeed and altitude), stall warning activation, and possible airspeed alerts that have memory items and QRH procedures
    - Expected pilot actions include executing memory items of stall recovery, appropriate pitch and thrust memory items, stabilizer cut-out switches for stabilizer trim runaway
  - Both B737MAX accidents had unexpected pilot actions
  - The grey area is “should these unexpected actions have been expected?”

Design grey areas

- **“MCAS description should have been in FCOM”**
  - Part 25.1585 Operating procedures
    - “(b) Information or procedures not directly related to airworthiness or not under the control of the crew, must not be included, nor must any procedure that is accepted as basic airmanship”
  - Discussed extensively, and Boeing proposed removing description of MCAS from FCOM and the training differences tables. The FAA accepted proposal. Supporting rationale not documented in meeting minutes
  - Boeing seemed to conclude that MCAS was automatic, would operate in the background, crews would not likely encounter in normal operation, and failures would appear and be appropriately handled like other existing failures
  - Frankly, many crews do not understand how speed trim works in the earlier B737NGs…and stabilizer trim runaways are typically not a part of recurrent training
  - Expecting crews to diagnose detailed stabilizer trim failure effects is challenging (there are 4 different trim rates)
  - Yet, the possible entirety of the full effects and possible confusion of these AOA failures were not fully considered.

Design grey areas

- **“The airplane should have had an AOA Disagree Alert”**
  - Requirements had inclusion of AOA Disagree Alert. Implementation mistake resulted in the alert being included only if AOA Gauge option was added
    - A root cause analysis of this error has resulted in a process change at the manufacturer
  - Some have concluded that having this alert would have caused proper maintenance actions after the first Lion Air incident (as other alerts were noted previously, although stick shaker activation was not, and that is a mandatory reporting item)
  - Admittedly, the memory items associated with the other alerts were not executed, so it is questionable whether it would have affected crew actions

Design grey areas

- **“The Organization Designation Authorization is flawed” or “Can you believe a manufacturer can certify their own designs?”**
  - This process delegates certain certification functions to Boeing with FAA oversight
  - It is not unique to the FAA nor to Boeing
  - Contrast this, in principle, with how other industries operate (automobile, medical)
  - It allows for appropriate expertise to evaluate system safety
  - Obviously, as the present situation shows, it is in the OEM’s best interest to competently evaluate system safety
  - It is arguable that perhaps Low Mach changes to MCAS should have received more FAA oversight
  - The grey area is the balance between OEM and regulator oversight
  - Joint Authorities Technical Review recommending reviewing “whether ODA process can be made less cumbersome and bureaucratic to avoid stifling needed communications”

Possible pitfalls

- “As aircraft systems become more complex, ensuring that the certification process adequately addresses potential operational and safety ramifications for the entire aircraft that may be caused by the failure or inappropriate operation of any system on the aircraft becomes not only far more important, but also far more difficult” - Joint Authorities Technical Review, 2019

Possible pitfalls

- “As aircraft systems become more complex, ensuring that the certification process adequately addresses potential operational and safety ramifications for the entire aircraft that may be caused by the failure or inappropriate operation of any system on the aircraft becomes not only far more important, but also far more difficult” - Joint Authorities Technical Review, 2019
- “To the extent [regulations and standards] do not address every scenario [as systems become more complex], compliance with every applicable regulation and standard does not necessarily ensure safety” – Joint Authorities Technical Review, 2019

Possible pitfalls

- “As aircraft systems become more complex, ensuring that the certification process adequately addresses potential operational and safety ramifications for the entire aircraft that may be caused by the failure or inappropriate operation of any system on the aircraft becomes not only far more important, but also far more difficult” - Joint Authorities Technical Review, 2019
- “To the extent [regulations and standards] do not address every scenario [as systems become more complex], compliance with every applicable regulation and standard does not necessarily ensure safety” – Joint Authorities Technical Review, 2019
- Revisit “the FAA’s standards regarding the time needed by pilots to identify and respond to problems that arise.” – Joint Authorities Technical Review, 2019

Possible pitfalls

- “Thus, the NTSB concludes that the assumptions that Boeing used in its functional hazard assessment of uncommanded MCAS function for the 737 MAX did not adequately consider and account for the impact that multiple flight deck alerts and indications could have on pilots’ responses to the hazard” - NTSB, 2019

Possible pitfalls

- “Thus, the NTSB concludes that the assumptions that Boeing used in its functional hazard assessment of uncommanded MCAS function for the 737 MAX did not adequately consider and account for the impact that multiple flight deck alerts and indications could have on pilots’ responses to the hazard” - NTSB, 2019
- “Develop design standards, with the input of industry and human factors experts, for aircraft system diagnostic tools that improve the prioritization and clarity of failure indications (direct and indirect) presented to pilots to improve the timeliness and effectiveness of their response.” – NTSB, 2019

Conclusions

- It’s all about assumptions…too often, we quickly agree on those, and then spend time on the subsequent process

- Since regulations and standards do not consider every scenario, compliance does not necessarily ensure safety

- Even in hindsight, many of the original B737MAX decisions were grey