1309 Hazard Assessment Fundamentals

Jim Marko

Manager, Aircraft Integration & Safety Assessment

14 November 2018

Presentation Overview

- Fail-safe design concept
- Safety Assessment principles for hazard classification
- Considerations for assessing safety hazards
- Open Discussion

52X.1309

- The ultimate risk based regulation
  - No single failures leading to a catastrophic failure condition objective
  - Qualitative and quantitative assessments (75/25)
  - Probabilistic safety objectives using “on the order of” terminology

Fail-Safe design concepts

- The airworthiness standards are based on, and incorporate, the objectives, principles and/or techniques of the fail-safe design concept, which considers the effects of failures and combinations of failures in defining a safe design.

- In any system or subsystem, the failure of any single element, component, or connection during any one flight should be assumed, regardless of its probability. Such single failures should not be catastrophic.

- Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless their joint probability with the first failure is shown to be extremely improbable.

Fail-Safe design concepts

- The fail-safe design concept uses a combination of two or more of the following design principles or techniques in order to ensure a safe design;
  - Designed Integrity and Quality, including Life Limits, to ensure intended function and prevent failures,
  - Redundancy or Backup Systems to enable continued function after any single or other defined number of failure(s),
  - Isolation and/or Segregation of Systems, Components, and Elements so that the failure of one does not cause the failure of another,
  - Failure Warning or Indication to provide detection
  - + …….

Safety Assessment Principles for hazard classification

A Systematic and Structured approach for all assessments is the prudent approach

- Assume the aircraft/systems functions under consideration are complex
- Systematically assess the effects on the safety of the aircraft and its occupants resulting from possible failures, considering both individually and in combination with other failures or events.
    - Identify the relevant aircraft functions and failure conditions then start to assess how criticality (hazards) and complexity impacts systems.
    - Identify the relevant system functions, dependencies (resources), interfaces and failure conditions involved.

Safety Assessment Principles for hazard classification

A Systematic and Structured approach for all assessments is the prudent approach

- The safety assessment process methods to be utilized could be the whole or part depending on the criticality and/or complexity of the system, or whether there are reused systems under consideration.

- The rigor of assessment and analysis performed is also dependent on the system criticality or complexity where some systems may be simple enough such that the entire safety assessment can be performed by observation and compliance shown by a simple statement.

- More complex and higher criticality systems may require application of all the safety assessment elements in order to show compliance. Many states in between.

Safety Assessment Principles for hazard classification

Elements of the safety assessment process that may be deployed include:

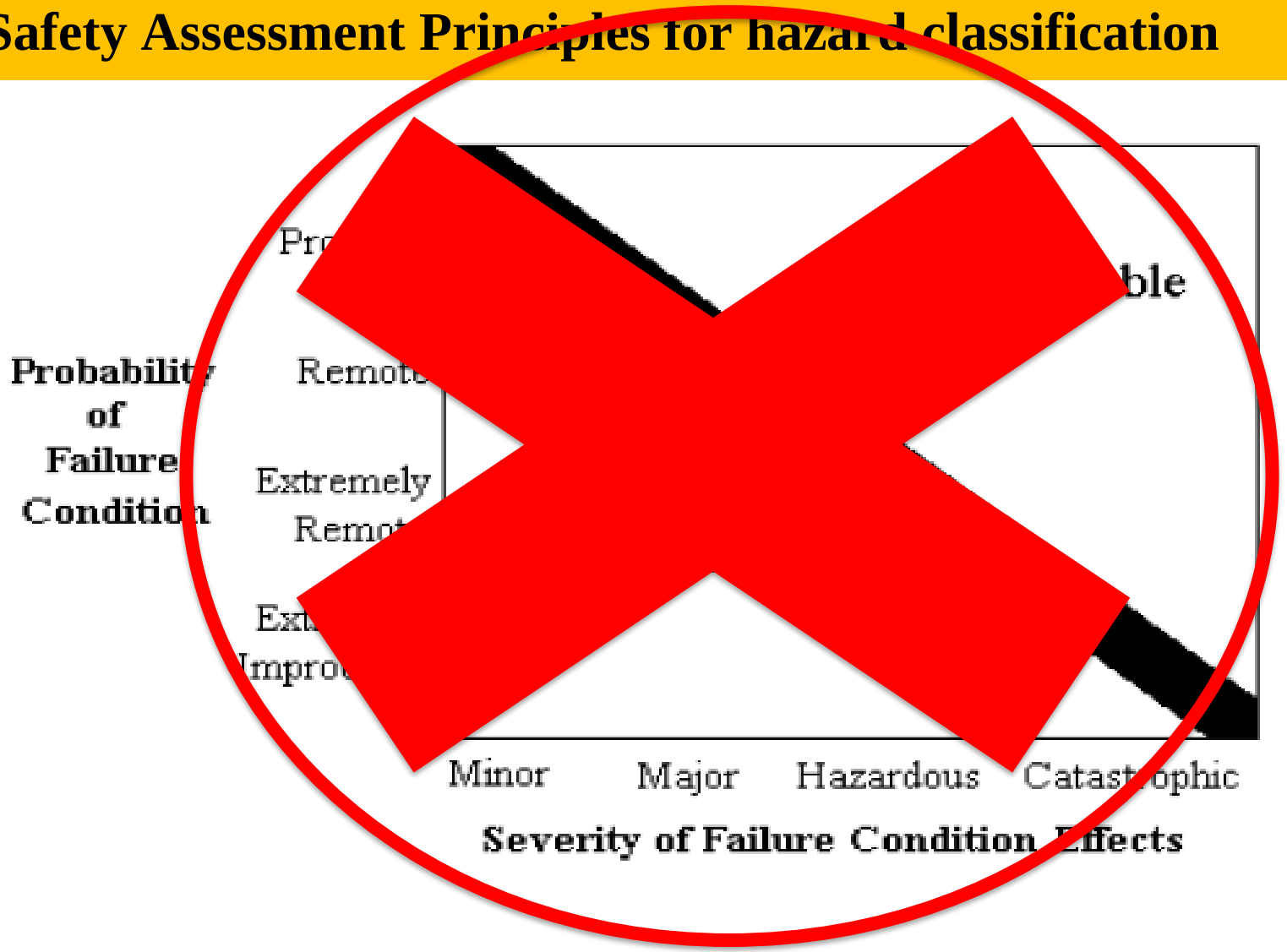
- **Aircraft Functional Hazard Assessment (FHA)**
- **Preliminary Aircraft Safety Assessment (PASA)**
- **System Functional Hazard Assessment (FHA)**
- **Preliminary System Safety Assessment (PSSA)**
  - Fault Tree Analysis (FTA)
  - Failure Mode and Effect Analysis (FMEA)
- Common Cause Considerations (Aircraft and/or System)
  - Zonal Safety Analysis (ZSA)
  - Particular Risk Assessment (PRA)
  - Common Mode Analysis (CMA
- **System Safety Assessment (SSA)**
- **Aircraft Safety Assessment (ASA)**

Safety Assessment Principles for hazard classification

Identify and classify Failure Conditions.

- All relevant engineering organizations specialists, such as systems, structures, propulsion, and flight test should be involved in this process.
- Classic approach is that identification and classification is done by conducting a Functional Hazard Assessment (AFHA/SFHA).
- When classifying a function, consider the loss of function, degradation of the function but also the malfunction as possible hazards (important to be complete and correct).
- Utilize the latest guidance references to the five failure condition classifications.
- Validation evidence is important.

Safety Assessment Principles for hazard classification



Aircraft Functional Hazard Assessment (AFHA)

Example of a High-Level Starting Point

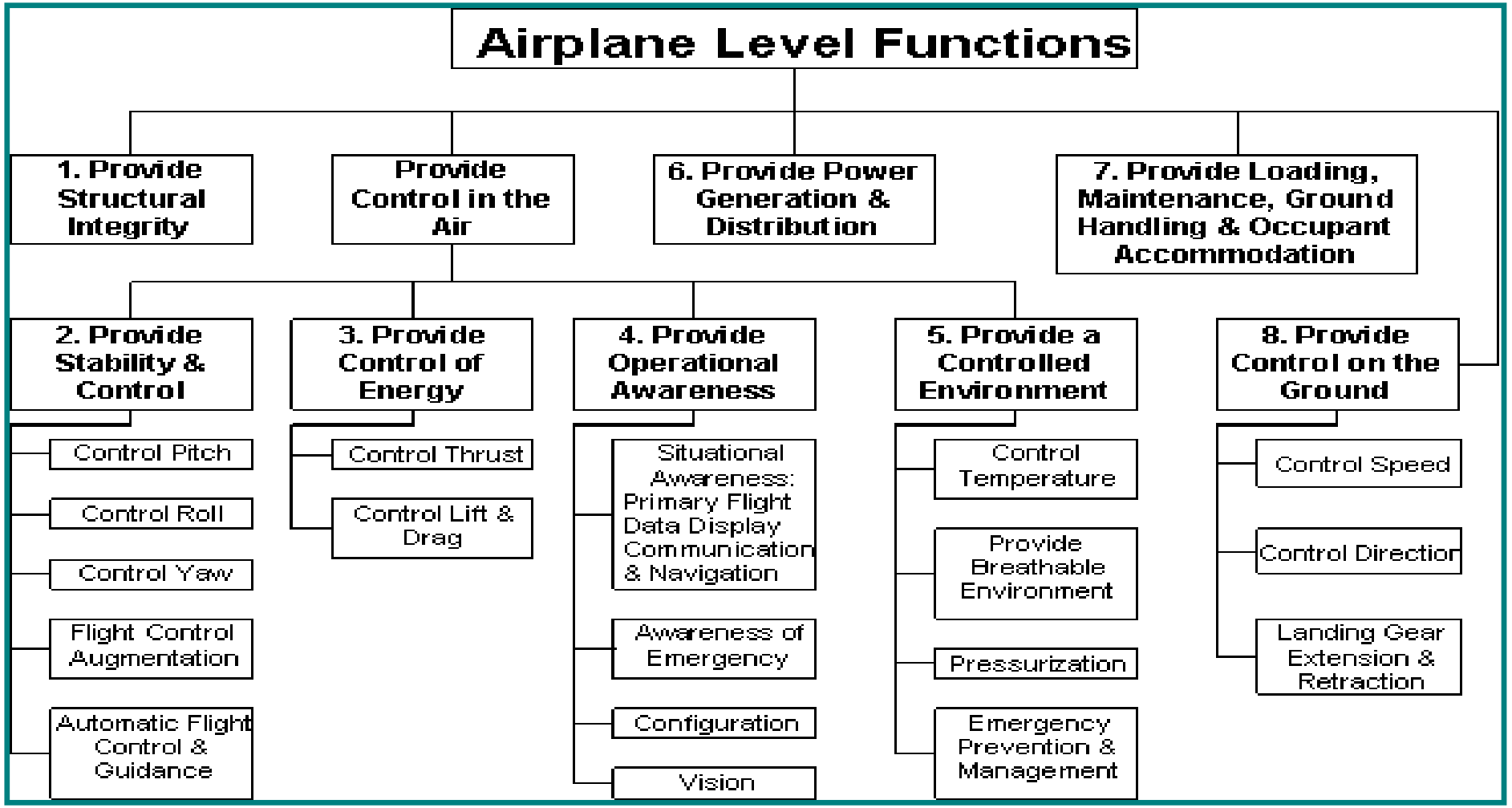
- The process begins with the top-level (aircraft level) definition of functions.
- An assessment of the impact of new or modified function on other aircraft-level functions and their supporting requirements is necessary.
- This is the first and most important step towards constructing a complete and correct AFHA

Aircraft Functional Hazard Assessment (AFHA)

Typical aircraft functions may include:

- Provide structural integrity,
- Provide stability and control in air,
- Provide control of energy in air,
- Provide operational awareness in air,
- Provide a controlled environment in air ,
- Provide power generation and distribution,
- Provide loading, maintenance, ground handling & occupant accommodation,
- Provide control on ground

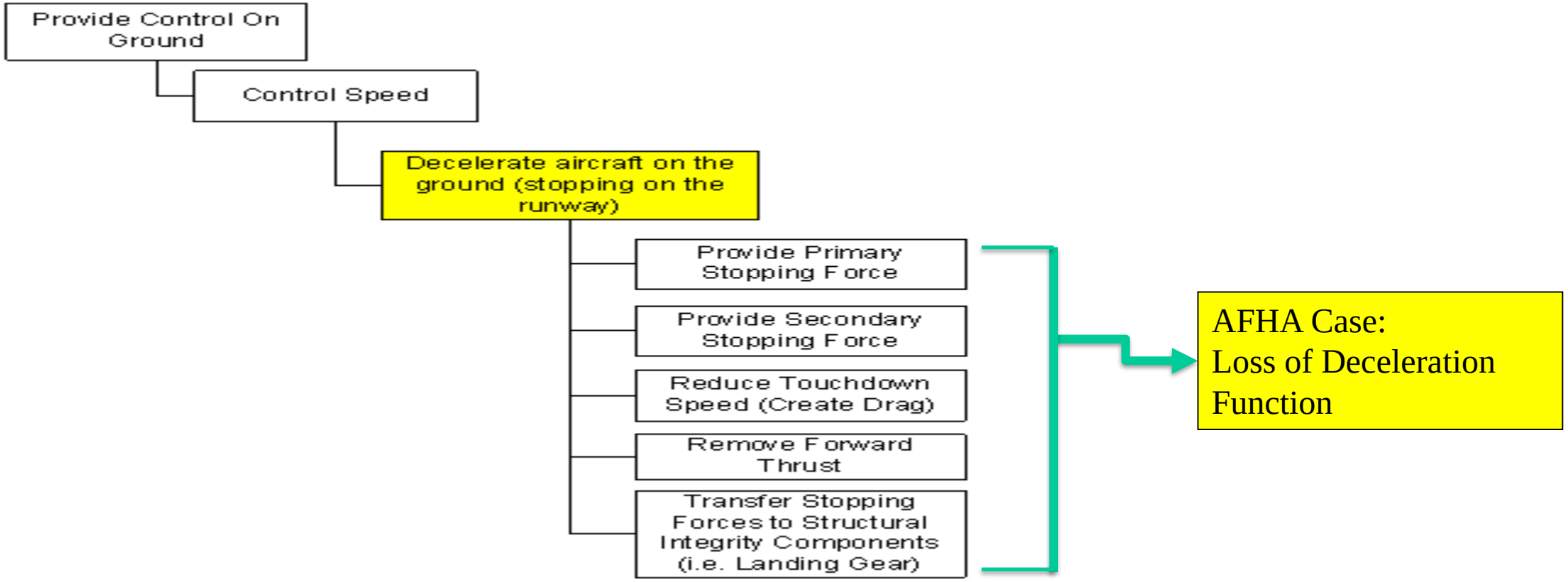
Aircraft Functional Hazard Assessment (AFHA)



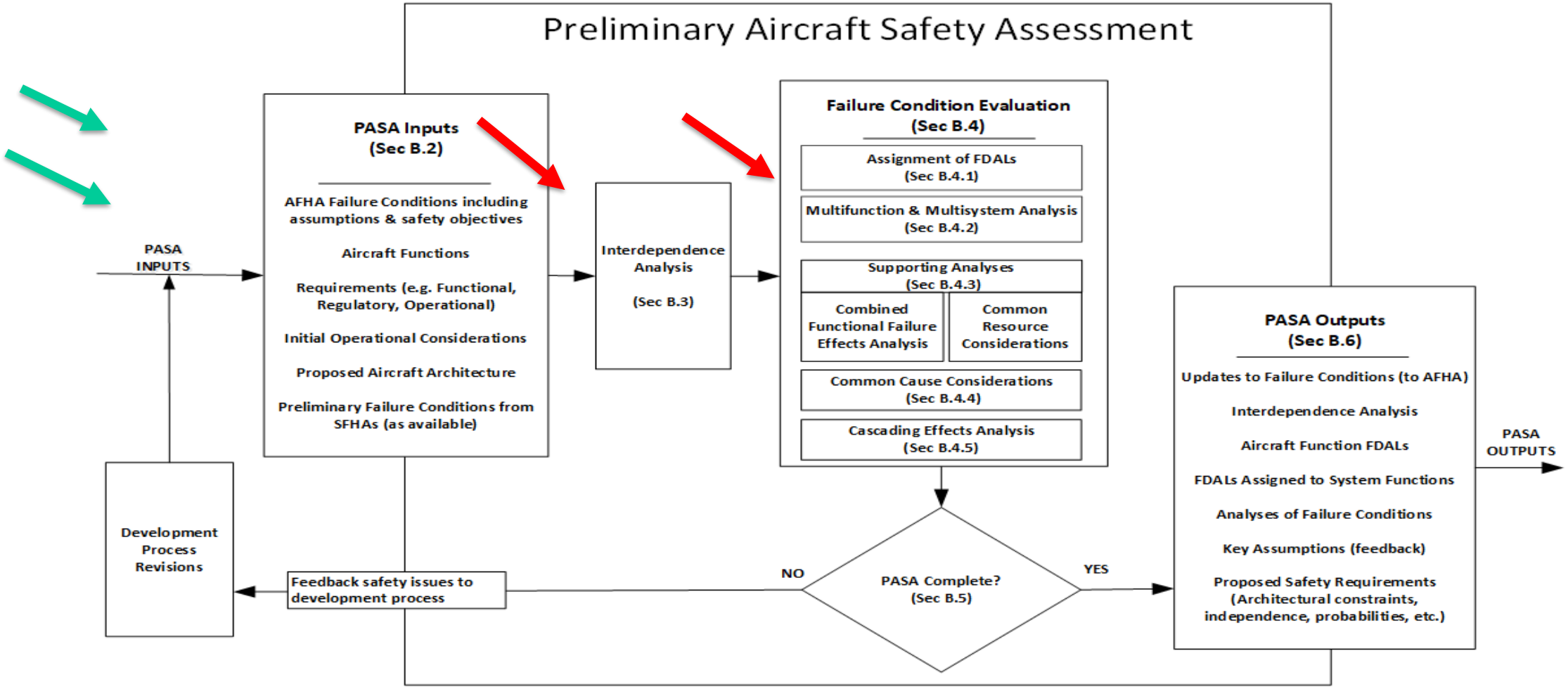
Aircraft Functional Hazard Assessment (AFHA)

Aircraft Functional Decomposition:

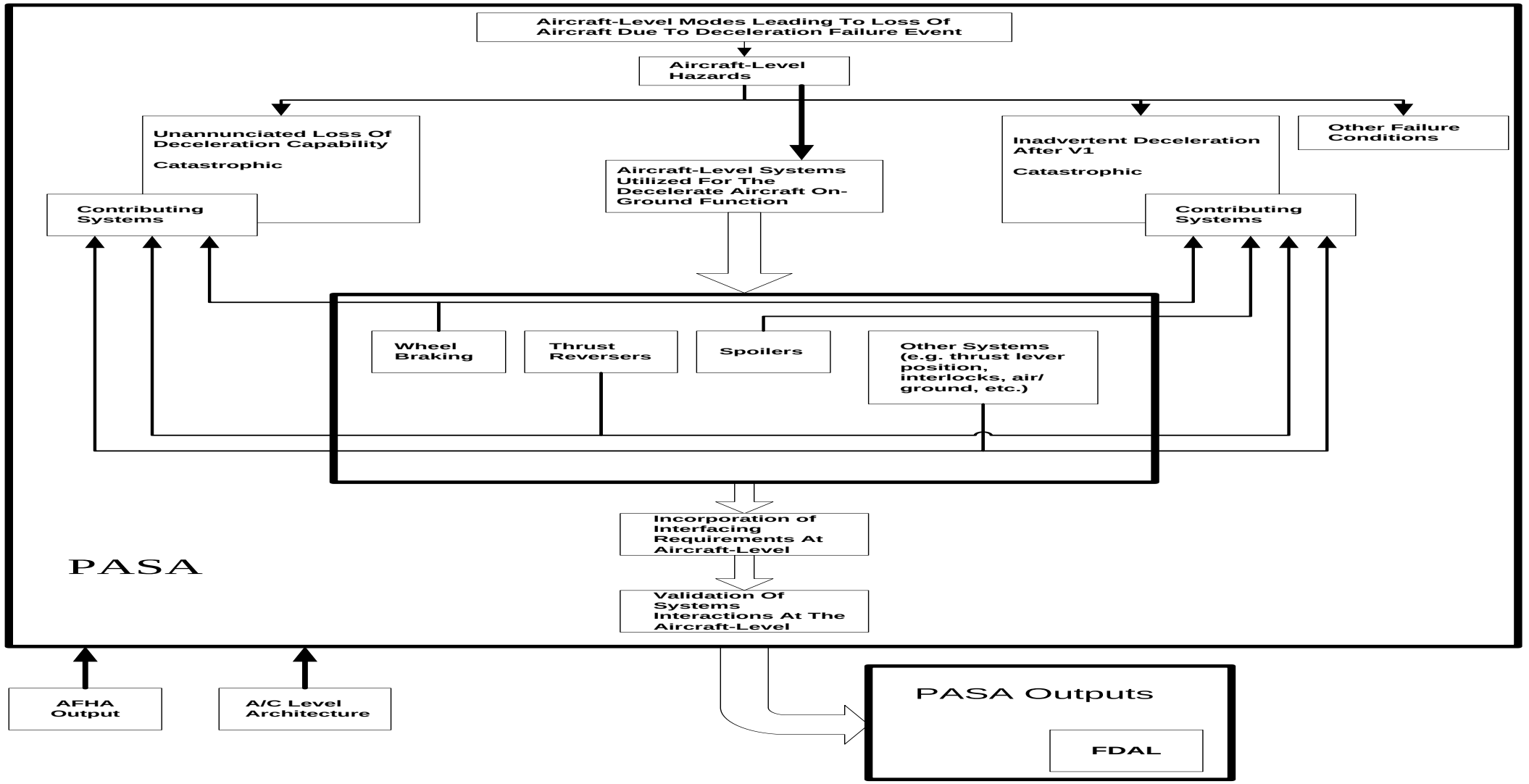
Functional decomposition for “Control Speed”, which is a second level function of the first level aircraft function “Provide Control on the Ground”



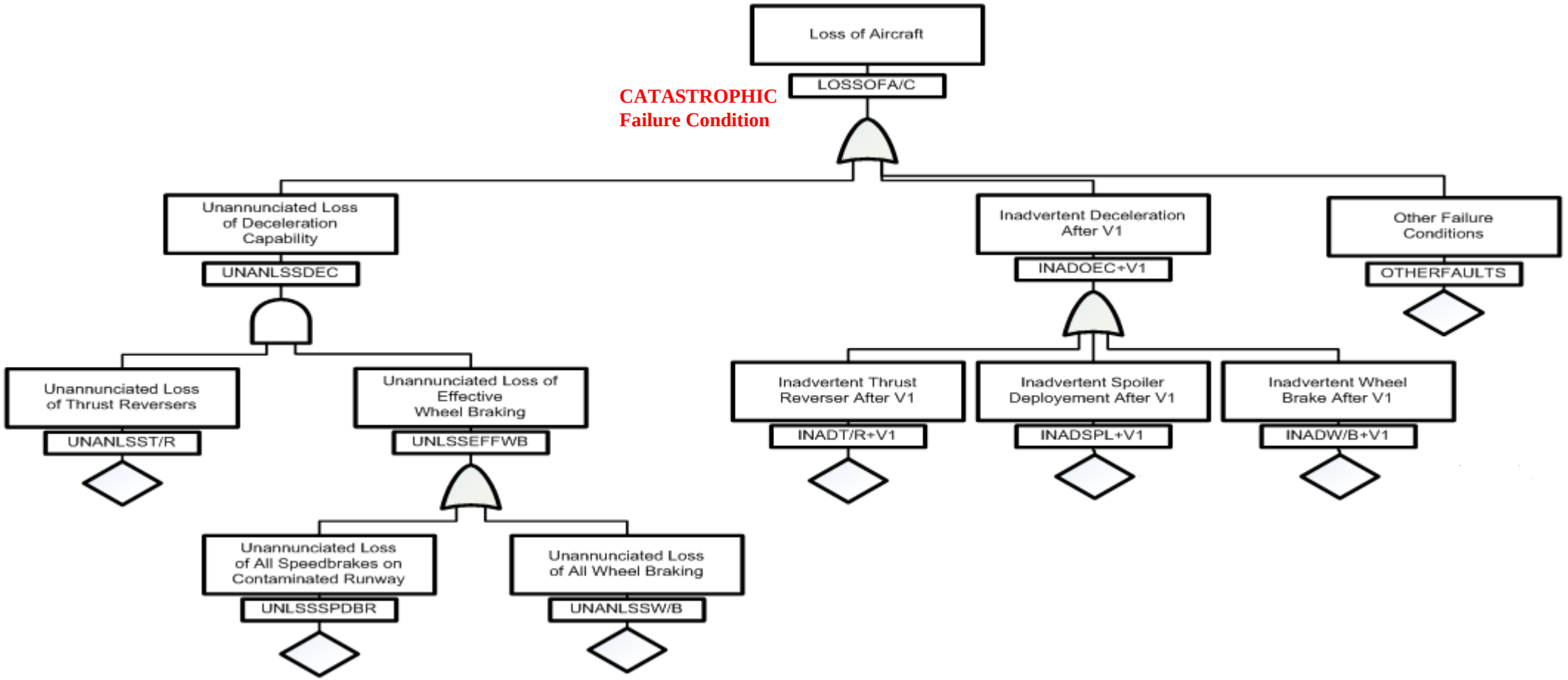
Preliminary Aircraft Safety Assessment (PASA)



Preliminary Aircraft Safety Assessment (PASA)

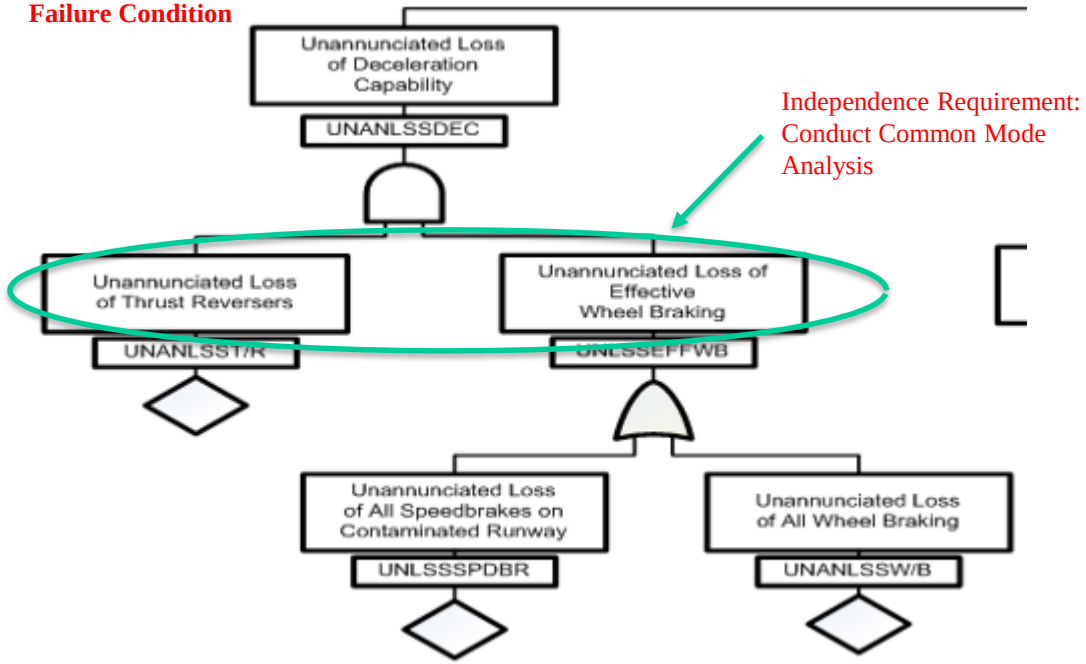


Preliminary Aircraft Safety Assessment (PASA)



Preliminary Aircraft Safety Assessment (PASA)

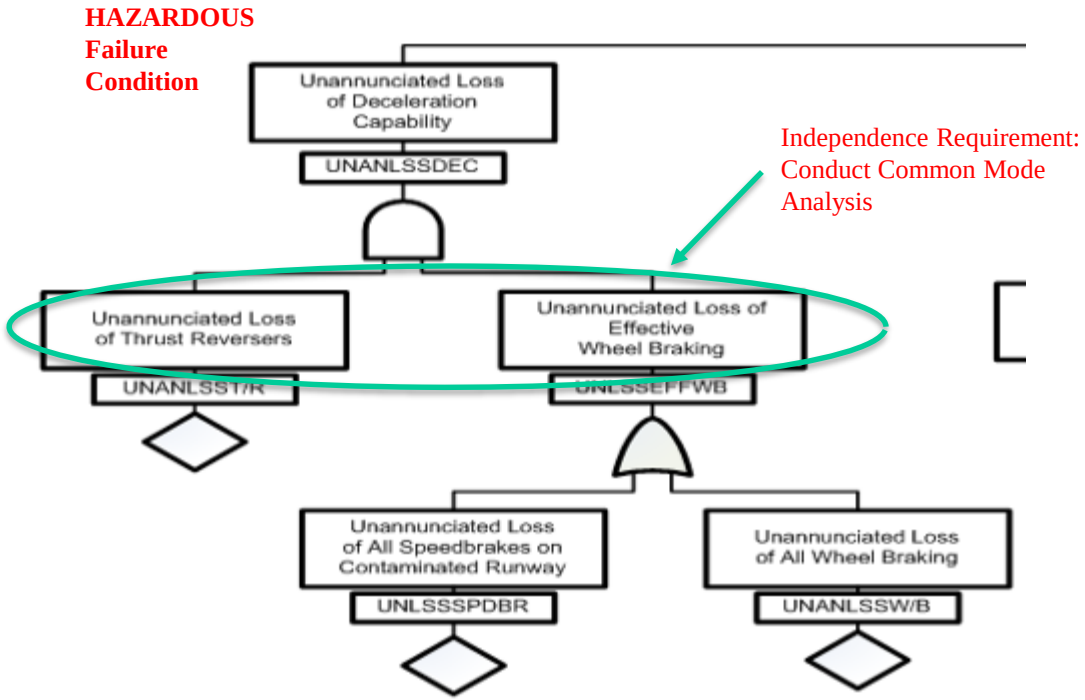
CATASTROPHIC
Failure Condition



What can we learn from this relationship?

- Ensure no single failures
- Ensure failures of all common resources (e.g. electrical, hydraulic, etc.) are considered and cannot lead to simultaneous loss of both functions
- Budget required probability according to desired outcome (e.g. reliability or integrity of one function versus the other)
- Determine if there are zonal/installation needs (separation, segregation of functional components/LRUs)
- Identification of interface requirements
- What assumptions were made (e.g. flight crew reaction times, crew procedures, architectural unknowns, etc.)
- Architectural design constraints (e.g. need for backup function)
- Allocation of Functional Development Assurance Levels (FDALs) to systems
- Identification of safety requirements to be transferred to Requirements Management processes (e.g. Validation)

Preliminary Aircraft Safety Assessment (PASA)



What difference would there be if the same relationship was only a hazardous failure condition?

- Ensure no single failures ??
- Budget required probability according to desired outcome (e.g. reliability or integrity of one function versus the other)
  - Ensure failures of all common resources (e.g. electrical, hydraulic, etc.) are considered and cannot lead to simultaneous loss of both functions
- Determine if there are zonal/installation needs (separation, segregation of functional components/LRUs)
- Identification of interface requirements
- What assumptions were made (e.g. flight crew reaction times, crew procedures, architectural unknowns, etc.)
- Architectural design constraints (e.g. need for backup function)
- Allocation of Functional Development Assurance Levels (FDALs) to systems
- Identification of safety requirements to be transferred to Requirements Management processes (e.g. Validation)

Considerations for assessing hazards: The Nuances of getting Hazard Assessments right

- Hazards are not necessarily treated consistently in regulation and/or guidance materials
- “Things aren’t always as they seem”
- Interpretations will differ for different categories of aircraft
  - General aviation versus transport aircraft, as an example
- Interpretations will differ within the same category
  - System-to-system safety objectives
- Examples to illustrate

Considerations for assessing hazards: Essential Versus Non-Essential Equipment

AC 23.1309-1E

- Determine that operation of installed equipment has no unacceptable adverse effects on any systems or equipment.
- Determine that failures or malfunction (also a failure) of the installed equipment could not result in unacceptable hazards.
- Installation hazards compromising aircraft safety such as fire, smoke, explosion, toxic gases, depressurization, etc. to be explored and justified
- No difference for essential or non-essential equipment

Considerations for assessing hazards: Essential Versus Non-Essential Equipment

AC 29-2C

- Section 29.1309 does not apply to certain required equipment such as life rafts, life preservers, and emergency floatation equipment safety belts, seats, and hand held fire extinguishers.1309 also does not apply to the functional aspects of aircraft non-safety related equipment such as entertainment systems, hoists, Forward Looking Infrared systems (FLIR), or emergency medical equipment such as defibrillators, etc.

- However, it does apply to hazards to the rotorcraft, its occupants, and flight crew introduced by the installation or presence of this type of equipment or system (e.g., Electromagnetic-Interference considerations, fire hazards, and failure of the electrical system fault protection scheme, inadvertent deployment) approved as part of the type design.

Considerations for assessing hazards: Structures Involvement in hazard classification

FAR 29.547(b)– Main and tail rotor structure

- Each rotor assembly must be designed as prescribed in this section and must function safely for the critical flight load and operating conditions. A design assessment must be performed, including a detailed failure analysis to identify all failures that will prevent continued safe flight or safe landing, and must identify the means to minimize the likelihood of their occurrence.

- The intent is to identify the critical components and/or clarify their design integrity to show that the basic airworthiness requirements which are applicable to the rotors will be met.

- A design assessment of the rotors should be carried out in order to substantiate that they are of a safe design and that compensating provisions are made available to prevent failures classified as hazardous and catastrophic.

Considerations for assessing hazards: Structures Involvement in hazard classification

- For the purposes of the assessment required by FAR 29.547(b) , failure conditions are classified according to the severity of their effects using the AC 29-2C criteria for 29.1309 compliance to identify Minor, Major, Hazardous and Catastrophic failure conditions.

- The first stage of the design assessment is identification of all hazardous and catastrophic failure modes.

- The failure analysis to perform is an FMEA structured bottom-up analysis, which is used to evaluate the effects of failures on the system and on the aircraft for each possible item or component failure.

- Consider effects failure modes on the item/component under analysis, the secondary effects on the rotors and on the rotor drive system, on other systems, and at the rotorcraft level.

Considerations for assessing hazards: Minor versus major classification

- Failure Condition: Wing A/Ice Overheating, Annunciated
- AFM procedures to close system shutoff valve and exit icing conditions
- Do crew procedures meet MINOR classification criteria?
  - Involve crew actions that are well within their capabilities. YES
  - A slight increase in crew workload, such as routine flight plan changes. MAYBE
  - Slight reduction in safety margins. MAYBE/MAYBE NOT
- But what happens if the failure is left unchecked
  - The failure will no longer be MINOR
- Result is a <u>MAJOR</u> classification

Considerations for assessing hazards: Hazardous does not always mean the same thing

<u>One Interpretation: The 1309 classic definition</u>

- Failure conditions which would reduce the capability of the aircraft/rotorcraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be –

  (i) A large reduction in safety margins or functional capabilities.
  (ii) Physical distress or higher workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely.
  (iii) Serious or fatal injury to a relatively small number of the occupants (or a passenger or cabin crew member).

Considerations for assessing hazards: Hazardous does not always mean the same thing

A different interpretation

- The engine firewall must be fireproof, support appropriate flight and landing condition loads, and prevent flame penetration when subjected to a flame of 2000F for 15 minutes.

- Essential structure and controls must be protected for the duration of time appropriate to the rotorcraft operation and be able to carry loads and resist any failure that could cause hazardous loss of control when subjected to the temperature resulting from any foreseeable powerplant fire. Insufficient protection to provide enough time for a controlled landing would represent an unsafe feature or characteristic for the rotorcraft design.

- Insufficient protection = Catastrophic failure condition

Considerations for assessing hazards: Hazardous does not always mean the same thing

A different Twist

- 25.1103(d) Induction system ducts and air duct systems
  - For turbine engine and auxiliary power unit bleed air duct systems, no hazard may result if a duct failure occurs at any point between the air duct source and the airplane unit served by the air.
- Safety impact by 1309 = anything greater than NSE (does it mean the same as hazard here?)

Considerations for assessing hazards: Use of Guidance materials

- Conversion between the current application of the five failure condition categories as defined AC 29-2C and the three failure condition categories contained in the present FAR 29.1309 rule.

Present Rule Qualitative Probability Classification	-------- Probable --------		----------Improbable---------		Extremely Improbable
Quantitative Probability Classification	$>10^{-5}$		$\leq 10^{-5}$		$\leq 10^{-9}$
Present Rule Failure Condition Category – AC 29-2C & DO-178A	Non-essential		Essential		Critical
Current Application of Failure Condition Category	No Effect	Minor	Major	Hazardous or Severe - Major	Catastrophic

Considerations for assessing hazards: Use of Guidance materials

Classification of Failure Conditions:	No Safety Effect	<—Minor—>	<—Major—>	<—Hazardous—>	<Catastrophic>
Allowable Qualitative Probability	No Probability Requirement	Probable	Remote	Extremely Remote	Extremely Improbable
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	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal Injury or incapacitation
Classes of Airplanes:	Allowable Quantitative Probabilities and Software (SW) and Complex Hardware (HW) Development Assurance Levels (Note 2)				
Class I (Typically SRE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-4}$ Notes 1 and 4 P=C, S=D	$<10^{-5}$ Note 4 P=C, S=D	$<10^{-6}$ Note 3 P=C, S=C
Class II (Typically MRE, STE, or MTE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-6}$ Note 4 P=C, S=C	$<10^{-7}$ Note 3 P=C, S=C
Class III (Typically SRE, STE, MRE, and MTE greater than 6,000 pounds)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-7}$ Note 4 P=C, S=C	$<10^{-8}$ Note 3 P=B, S=C
Class IV (Typically Commuter Category)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-7}$ Note 4 P=B, S=C	$<10^{-9}$ Note 3 P=A, S=B

Considerations for assessing hazards: Use of Guidance materials

Table for Failure Condition Categories and Probability Definitions					
Effect on rotorcraft	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margin	Large reduction in functional capabilities or safety margins (Note 4)	Loss of rotorcraft
Effect on occupants excluding flight crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a passenger or a cabin crew member (NOTE 2)	Multiple Fatalities
Effect on flight crew	No effect on flight crew	Slight increase in work load which involve crew actions well within crew capabilities such as routine flight plan changes	Physical discomfort or a significant increase in workload or in conditions impairing crew efficiency	Physical distress or excessive workload impairs ability to perform tasks accurately or completely	Fatalities or incapacitation
DO-178C Software Level (Note 3)	E	D	C	B	A
Failure Condition Category	No Effect	Minor	Major	Hazardous or Severe-Major	Catastrophic
Qualitative Probability	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
Quantitative Probability :	No probability requirement	$\leq 10^{-3}$ (Note 1)	$\leq 10^{-5}$	$\leq 10^{-7}$	$\leq 10^{-9}$
Note 1: A numerical probability range is provided here as reference. The applicant is not required to perform a quantitative analysis, or substantiate by such an analysis, that this numerical criterion has been met for Minor Failure Conditions.					
Note 2: This is true if it can be shown that the given failure condition can be contained to a fatal injury of one occupant only.					
Note 3: This is not intended to imply that the identified software levels are assigned a probability value, but instead, shows a correlation to the Failure Condition Category.					
Note 4: Hazardous or Severe-Major failure conditions can include events that are manageable by the crew by use of proper procedures which, if not implemented correctly or in a timely manner, may result in a Catastrophic event.					

Considerations for assessing hazards: "Other" Requirements Relationship with 52X.1309

Aircraft level threat assessments

- More commonly know as Particular Risk Assessments (PRA)
- Assessment objectives are a combination of prevention and/or minimization of the hazards depending on the type of PRA undertaken;

    1. True Survivability only (preventing Catastrophic failures), or
    2. Survivability that looks to prevent Catastrophic failures while also minimizing Hazardous failure conditions to the maximum extent practicable.

Considerations for assessing hazards: "Other" Requirements Relationship with 52X.1309

- .631 Bird Strike – Continued safe flight and landing is the regulation objective
  - Through 1309 PRA, TCCA insists that Hazards be minimized to the maximum extent practicable (Hazards = hazardous & catastrophic failure conditions criteria of 1309)
  - Don't install essential equipment immediately behind areas liable to be struck by birds.
- .731 Wheels & .733 Tire Burst – no direct aircraft hazard objective stated
  - Through 1309 PRA TCCA insists that Hazards be minimized to the maximum extent practicable (Hazards = hazardous & catastrophic failure conditions criteria of 1309)

Considerations for assessing hazards: "Other" Requirements Relationship with 52X.1309

- .863 Flammable Fluids - minimize the probability of ignition of the fluids and vapors, and the resultant hazards if ignition does occur is the objective
  - Through 1309 PRA, TCCA insists that Hazards be minimized to the maximum extent practicable (Hazards = hazardous & catastrophic failure conditions criteria of 1309)

Considerations for assessing hazards: "Other" Requirements Relationship with 52X.1309

- .901 Sustained Engine Imbalance – 1309 PRA
- .903 Uncontained Engine Rotor Failure – 1309 PRA
- .1461 Equipment Containing High Energy Rotors – 1309 PRA
- High Stored Energy devices – 1309 PRA
- Flailing Shafts – 1309 PRA
- + …

1309 Hazards Assessment Fundamentals

- Stay structured and systematic throughout your safety assessment
- Conducting all installations/projects from the aircraft level is the prudent approach to avoid an incomplete assessment

1309 hazards assessment Fundamentals

QUESTIONS ??

Jim.marko@tc.gc.ca

613-773-8295