Software Safety
Determining Software Criticality Levels

Hosted by Software Policy Research Institute, Seoul, South Korea

Presented by:

Nazan GOZAY GURBUZ

BSME, MSME, MBA

Nov 23, 2017

TAOS
CERTIFICATION & ENGINEERING

About Instructor

Nazan Gozay Gurbuz serves as System Safety and Developement Assurance Specialist, Consultant and Instructor. She is founder of TAOS Certification and Engineering. She has worked in both international and domestic aircraft design, development and production projects for more than 20 years.

She is an active member of SAE S-18 Aircraft & Systems Development and Safety Assessment committee since Jan, 2008, and has provided key contributions to development of SAE-ARP-4754A Aircraft Development Process and SAE-ARP-4761A Safety Assessment Process.

Agenda

- Software safety – an accident and incident
- Key definitions
- Criticality levels in guidelines and standards
- Development assurance concept
- Determining criticality levels by example

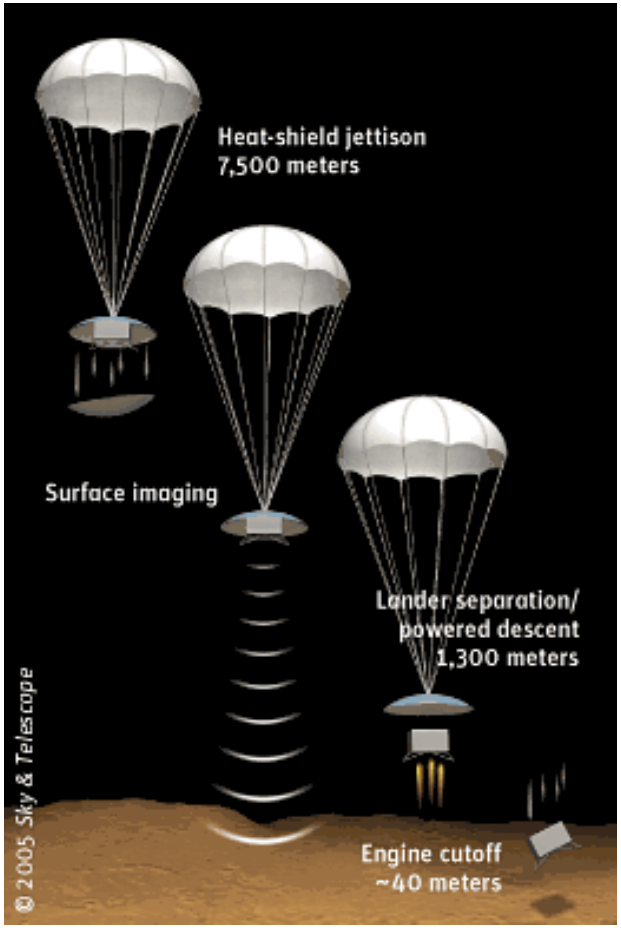
Can **Software** cause;

- death, injury, occupational illness?
- loss of equipment or property?
- damage to the environment?

Accident - Loss of Mars Polar Lander

- Dec 3, 1999
- Onboard **software** mistook the jolt of landing-leg deployment as ground contact and shut down the engines causing Polar Lander to fall and crash.
- Rockets were supposed to continue firing until one of the landing legs touched the surface

http://www.spaceref.com/news/viewnews.html?id=105



Incident - Aircraft In-flight Upset Event

- August 1, 2005
- Boeing 777-200 aircraft, registered 9M-MRG
- During climb, a low airspeed advisory on the aircraft's Engine Indication and Crew Alerting System observed
- Aircraft was approaching the stall speed limit. The stall warning and stick shaker devices also activated.
- The aircraft returned to Perth where an uneventful landing was completed.

AIR DATA INERTIAL REFERENCE UNIT (ADIRU)

https://www.atsb.gov.au/publications/investigation_reports/2005/AAIR/aair200503722.aspx

Incident - Aircraft In-flight Upset

June 2001
Accelerometer **#5** fails, ADIRU disregards accelerometer erroneous output value

Latent software error in the ADIRU algorithm to manage the sensor set

August 2005
Accelerometer **#6** fails, ADIRU latent software anomaly allows uses of previously failed accelerometer **#5** erroneous output value

The conditions involved in this event were not identified in the testing requirements, so were not tested.

What is Safety?

Freedom from those conditions that can cause death, injury, illness, damage to or loss of equipment or property or environmental harm

The state in which risk is acceptable

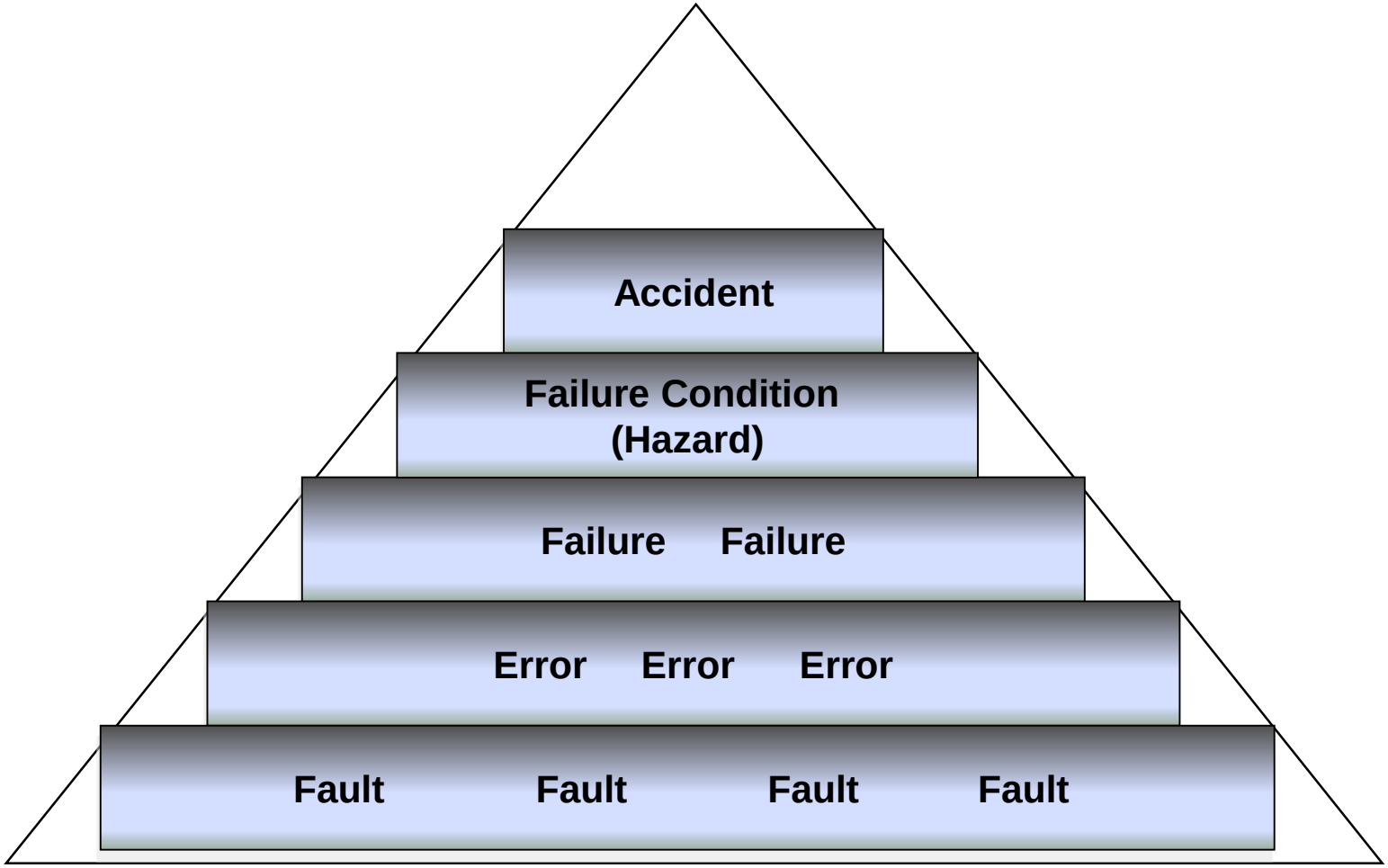
What is Risk?

The combination of the **probability** of an occurrence and its associated level of **severity**.

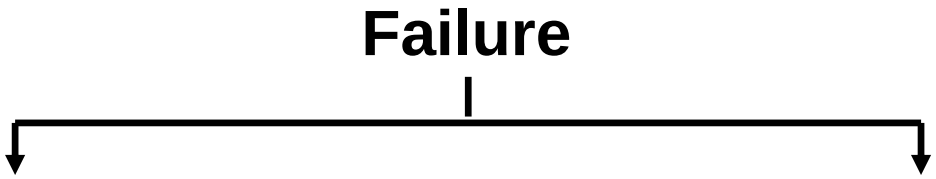
RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Note: Risk Matrix is from MIL-STD-882E

Progression to Accident



Progression to Accident



Systematic Failure

An undesired state of a system, that **is not** associated with physical degradation of a component, that results from a given set of conditions being satisfied.

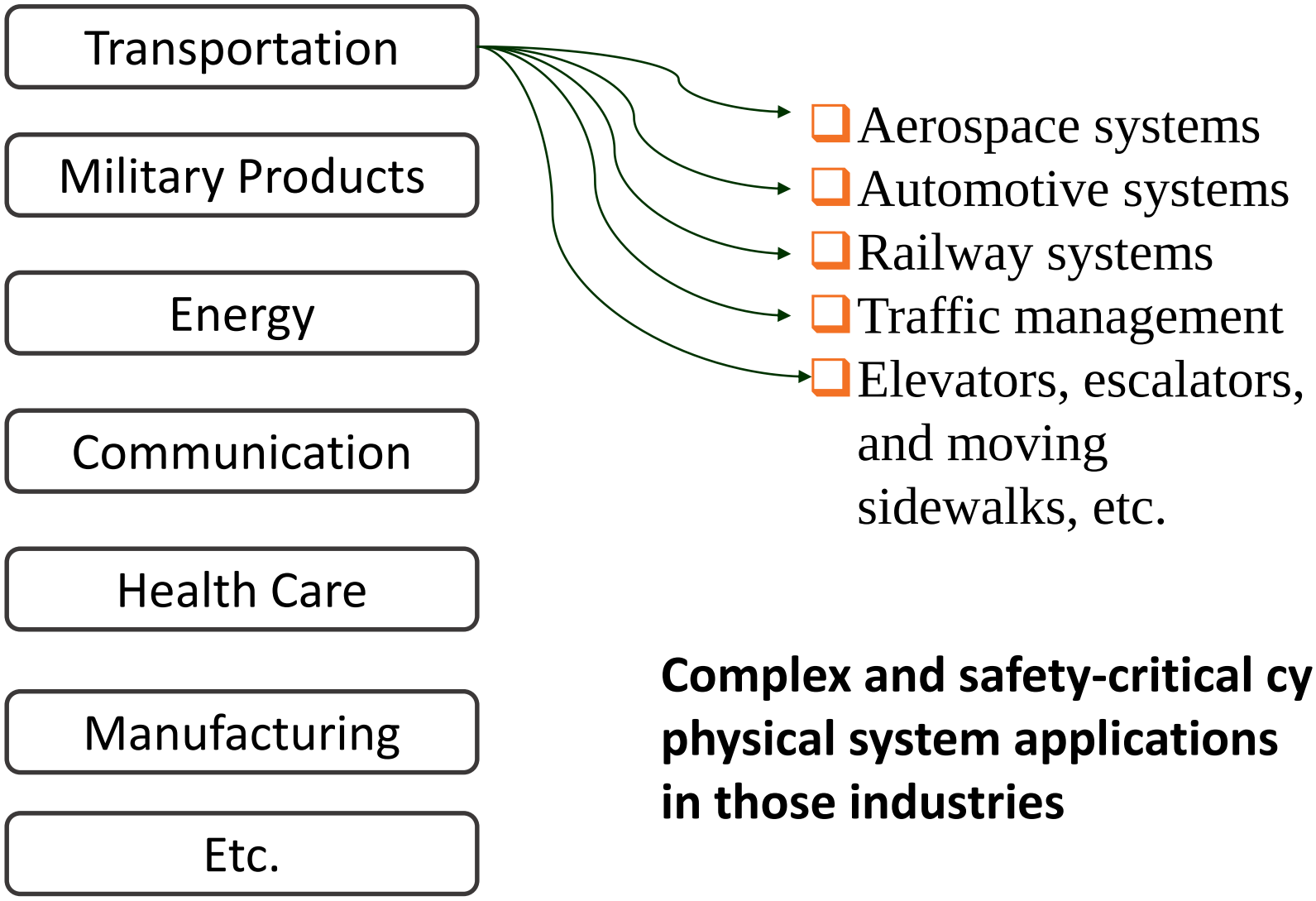
Software failures are always systematic.

Non-Systematic Failure

Non-systematic failures are those that are associated with some physical change and they may occur as a result of random occurrences or intrinsic defects in a component.

* Infant Mortality
* Random Failures
* Wear-out

Cyber Physical Systems



Complex and safety-critical cyber-physical system applications in those industries

Cyber Physical Systems

- Interacting networks of physical and computational components
- Safety assessments of those interactions (between hardware, software with human) are becoming more critical
- Software is generally application specific and its reliability parameters cannot be estimated in the same manner as hardware
- Therefore, another approach called **Development Assurance** is used to mitigate **error** in requirements, design and implementation
- Software criticality levels should be determined to apply sufficient development assurance rigor

Criticality Levels in Standards

Automotive Safety Integrity Level (ASIL)

ISO 26262
Road Vehicles – Functional Safety

Safety Integrity Level (SIL)

IEC 61508 - Functional safety of electrical/ electronic/programmable electronic safety

Software Control Category (SCC)

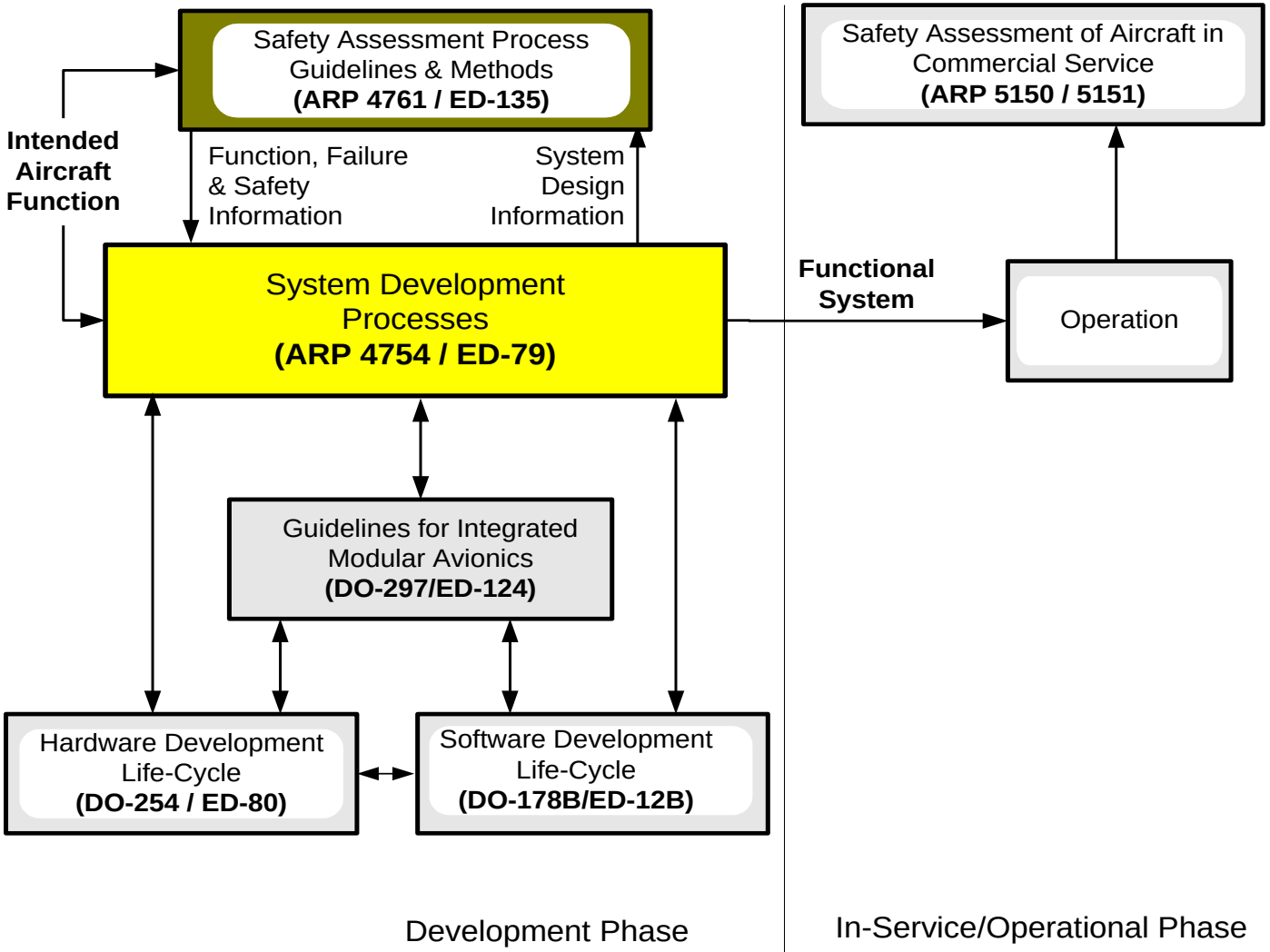
MIL-STD-882
Practice for System Safety

Development Assurance Level (DAL)

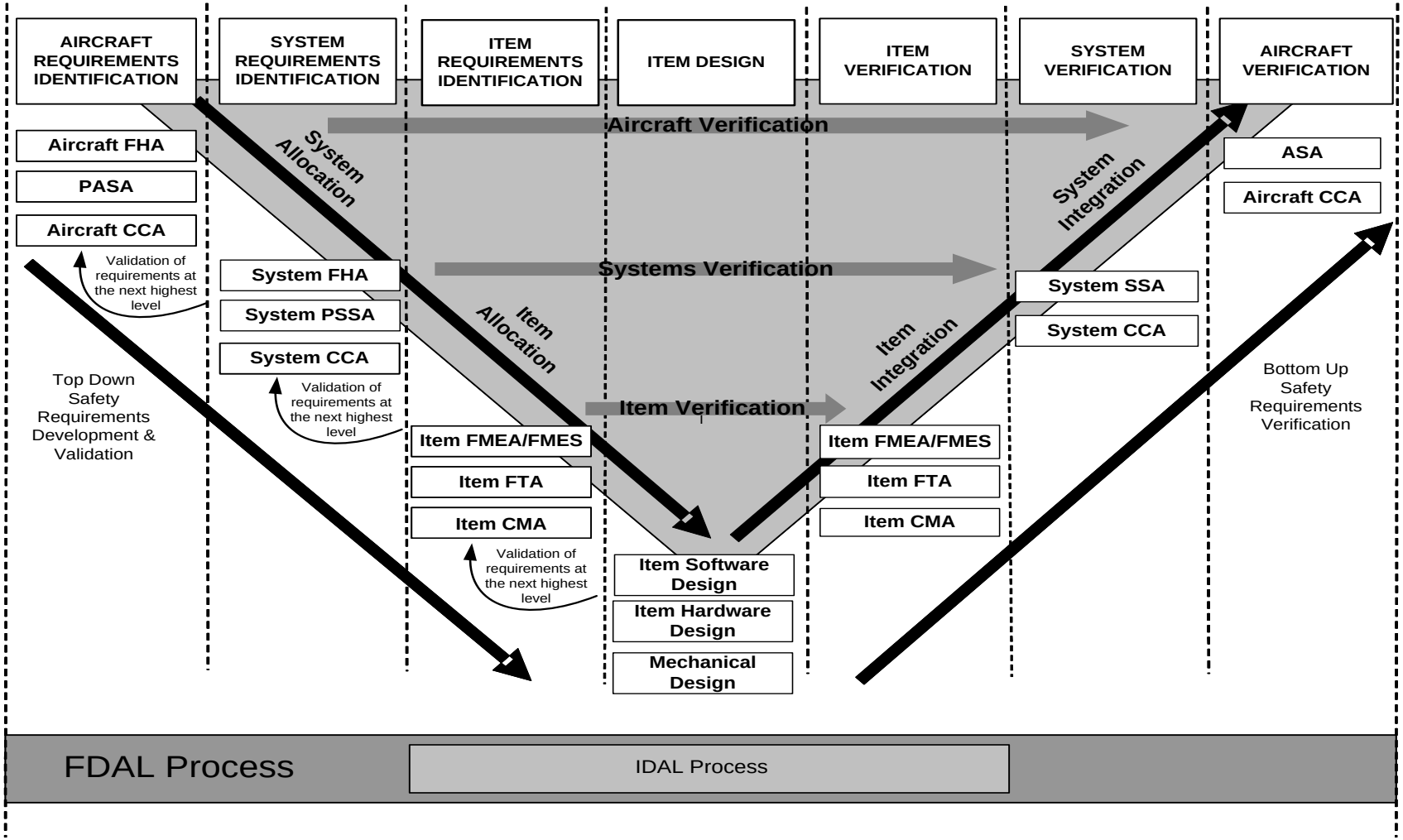
SAE-ARP-4754A
Guidelines for Development of Civil Aircraft and Systems

SAE-ARP-4761
Guidelines and Methods for Conducting the Safety Assessment Process

Development & Safety Processes in Aviation



Safety Assessment Overview



SAE-ARP-4754A- Guidelines for Development of Civil Aircraft and Systems

Development Assurance

Development Assurance is that all of those planned and systematic actions used to substantiate, at an adequate level of confidence, that **errors** in requirements, design and implementation have been identified and corrected such that the system satisfies the applicable certification requirements.

SAE-ARP-4754A

Development Assurance Level

There are two type of Development Assurance Level (DAL);

Function Development Assurance Level (FDAL)

The level of rigor of development assurance tasks performed to **Functions.**

Item Development Assurance Level (IDAL)

The level of rigor of development assurance tasks performed on Item (**Hardware and Software**).

SAE-ARP-4754A

Development Assurance Level

SAE-ARP-4754A Table 5-1

Top-Level Failure Condition Severity Classification Identified in FHA	Associated Top-Level Function FDAL Assignment
Catastrophic	A
Hazardous/Severe Major	B
Major	C
Minor	D
No Safety Effect	E

DALs assigned based on most direct relationship to worst-case failure condition.

Development Assurance Level

SAE-ARP-4754A Table 5-2

TOP-LEVEL FAILURE CONDITION CLASSIFICATION	DEVELOPMENT ASSURANCE LEVEL (NOTES 2 & 4)		
	FUNCTIONAL FAILURE SETS WITH A SINGLE MEMBER	FUNCTIONAL FAILURE SETS WITH MULTIPLE MEMBERS	
		OPTION 1 (NOTE 3)	**OPTION 2**
Column 1	Column 2	Column 3	Column 4
Catastrophic	**FDAL A** (NOTE 1)	**FDAL A** for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than **level C** for the additional Members).	**FDAL B** for two of the Members leading to top-level Failure Condition. The other Member(s) at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level C for the additional Member(s)).
Hazardous/ Severe Major	FDAL B	FDAL B for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level D for the additional Members).	FDAL C for two of the Members leading to top-level Failure Condition. The other Members at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level D for the additional Members).
Major	FDAL C	FDAL C for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.	FDAL D for two of the Members leading to top-level Failure Condition. The other Members at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.
Minor	FDAL D	FDAL D for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.	
No Safety Effect	FDAL E	FDAL E	

Safety Assessment Key Questions

1. What does it do?
2. What can go wrong?
3. What happens if it goes wrong?
4. What can cause it to go wrong?
5. What is the risk?
6. Can we accept the risk?

Safety Assessment Key Questions

What does it do Function	What can go wrong Failure Conditions	What happens if it goes wrong Failure Condition Effects	Failure Condition Classification Failure Condition Severity
Provide pitch control	**Loss of pitch control**	**Loss of aircraft control**	**Catastrophic**

Functional Hazard Assessment

Functional Hazard Assessment (FHA) identify and classify the failure conditions associated with the functions and combinations of functions. Typical failure conditions;

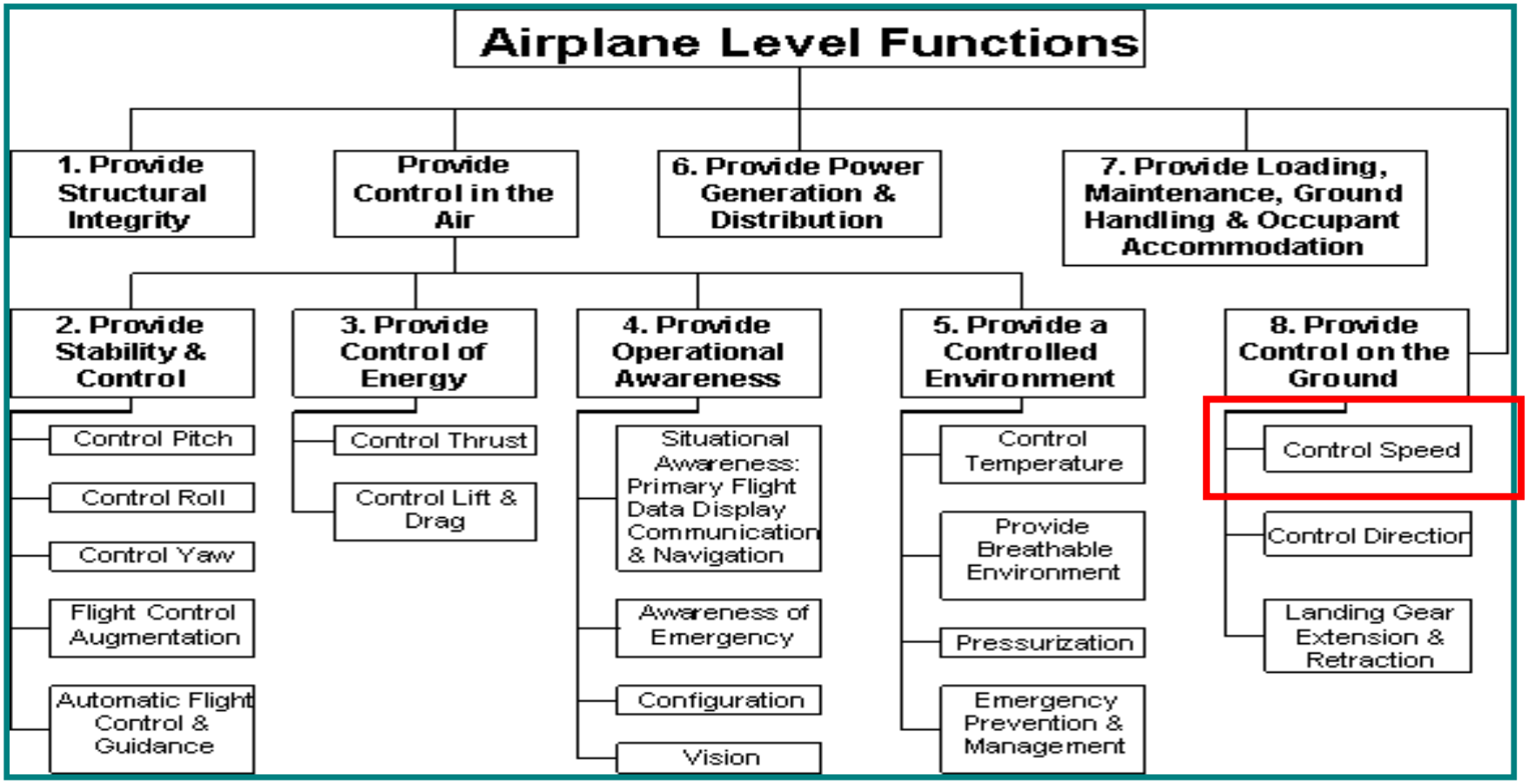
- Loss of a function,
- Inadvertent Operation of a function,
- Erroneous operation of a function

Functional Hazard Assessment

Effects of Failure Condition

Effect on Aircraft	Effect on Crew	Effect on Occupants	Classification	DAL
Complete loss of aircraft Prevents continued safe flight and landing	Crew unable to accomplish required tasks, or Required crew strength or skill in excess of crew capability, or Crew incapacitation	Multiple occupant fatalities	Catastrophic	A
Large reduction in aircraft functional capability or safety margin	Excessive crew workload increase, crew unable to fully accomplish required tasks, or Crew physical distress	Small number of occupant fatalities or severe injuries not including flight crew	Hazardous	B
Significantly reduced aircraft functional capability or safety margin	Significant crew workload increase, or Conditions impairing crew efficiency	Occupant physical distress or non-fatal injuries	Major	C
Slightly reduced aircraft functional capability or safety margin	Slight crew workload increase	Occupant physical discomfort	Minor	D
No effect or aircraft functional capability or safety margin	No effect on crew workload or physiology	No effect on occupant physiology	No Safety Effect	E

Functional Hazard Assessment



Aircraft Functional Hazard Assessment

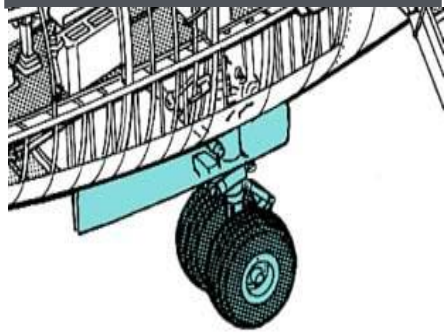
Function	Failure Condition	Phase of Flight	Effects of Failure Condition	Classification	DAL	Verification
Decelerate Aircraft on the ground	**Total loss of deceleration capability**	Landing	Crew is unable to decelerate aircraft resulting in a high speed overrun	**Catastrophic**	**A**	Fault Tree Analysis
	Inadvertent deceleration	Take off after V1	Crew cannot take of resulting in a high speed overrun	**Catastrophic**	**A**	Fault Tree Analysis

High Level Architecture

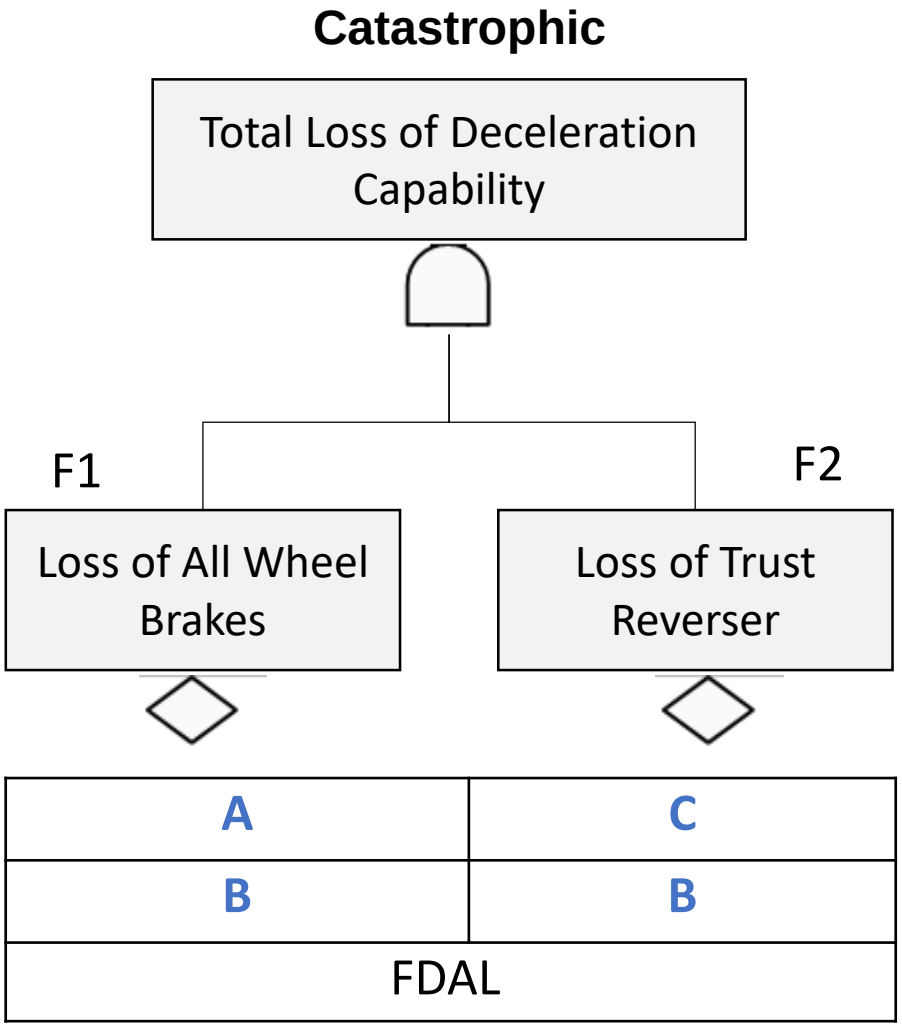
Decelerate Aircraft on the ground

Engine (Reverse Thrust)

Wheel Brakes



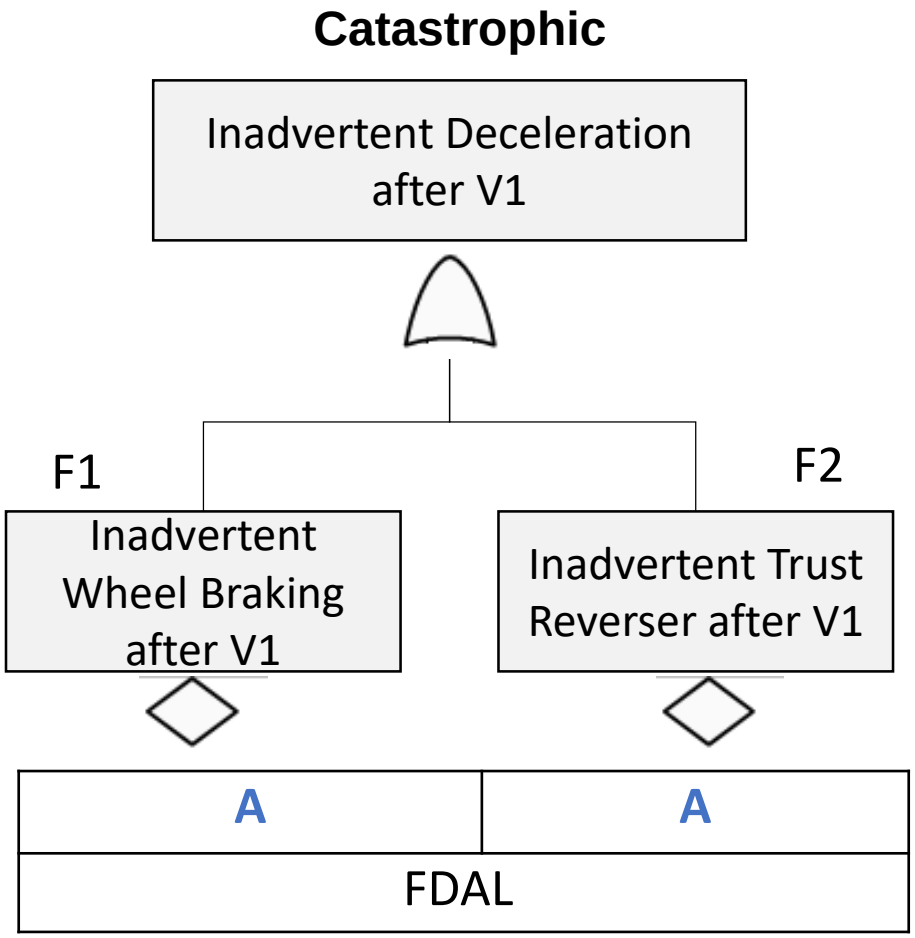
Development Assurance Level



Fault Tree Minimal Cut Sets;

[F1 AND **F2]**

Development Assurance Level

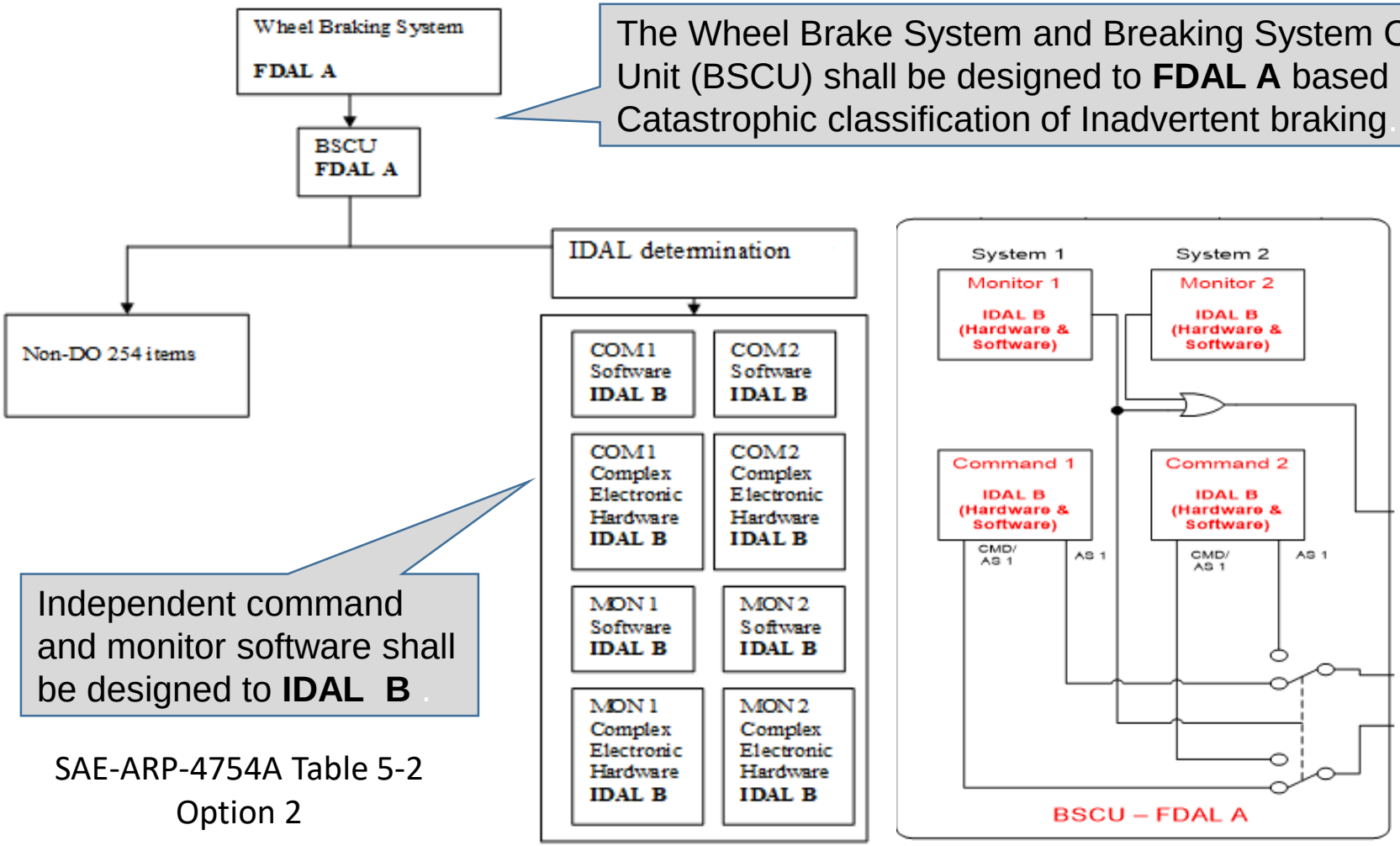


Fault Tree Minimal Cut Sets:

[F1]
OR
[F2]

Note: Evaluate each Failure Condition before assigning criticality levels

Development Assurance Level



The Wheel Brake System and Breaking System Control Unit (BSCU) shall be designed to **FDAL A** based on the Catastrophic classification of Inadvertent braking.

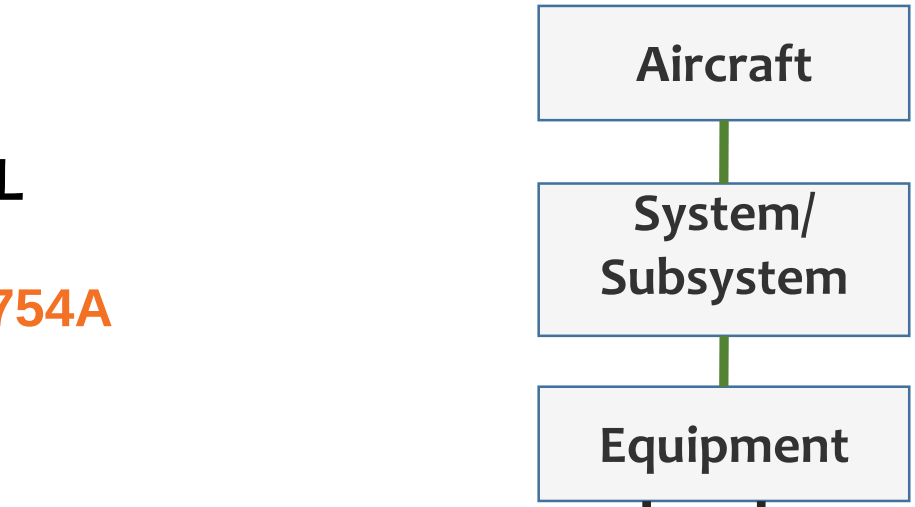
Independent command and monitor software shall be designed to **IDAL B** .

SAE-ARP-4754A Table 5-2
Option 2

Summary

For FDAL

SAE- ARP-4754A



For IDAL

RTCA-DO-254

RTCA-DO-178C

Summary

Murphy's Laws

If anything can go wrong then it will be

Aviation Version

If something can be fitted incorrectly then someone someday will fit it this way

고맙습니다

For more information about TAOS services please visit:

www.taoscertification.com

nazan.gurbuz@taoscertification.com