Aircraft System Safety Assessment

One in a Billion

John Vincent

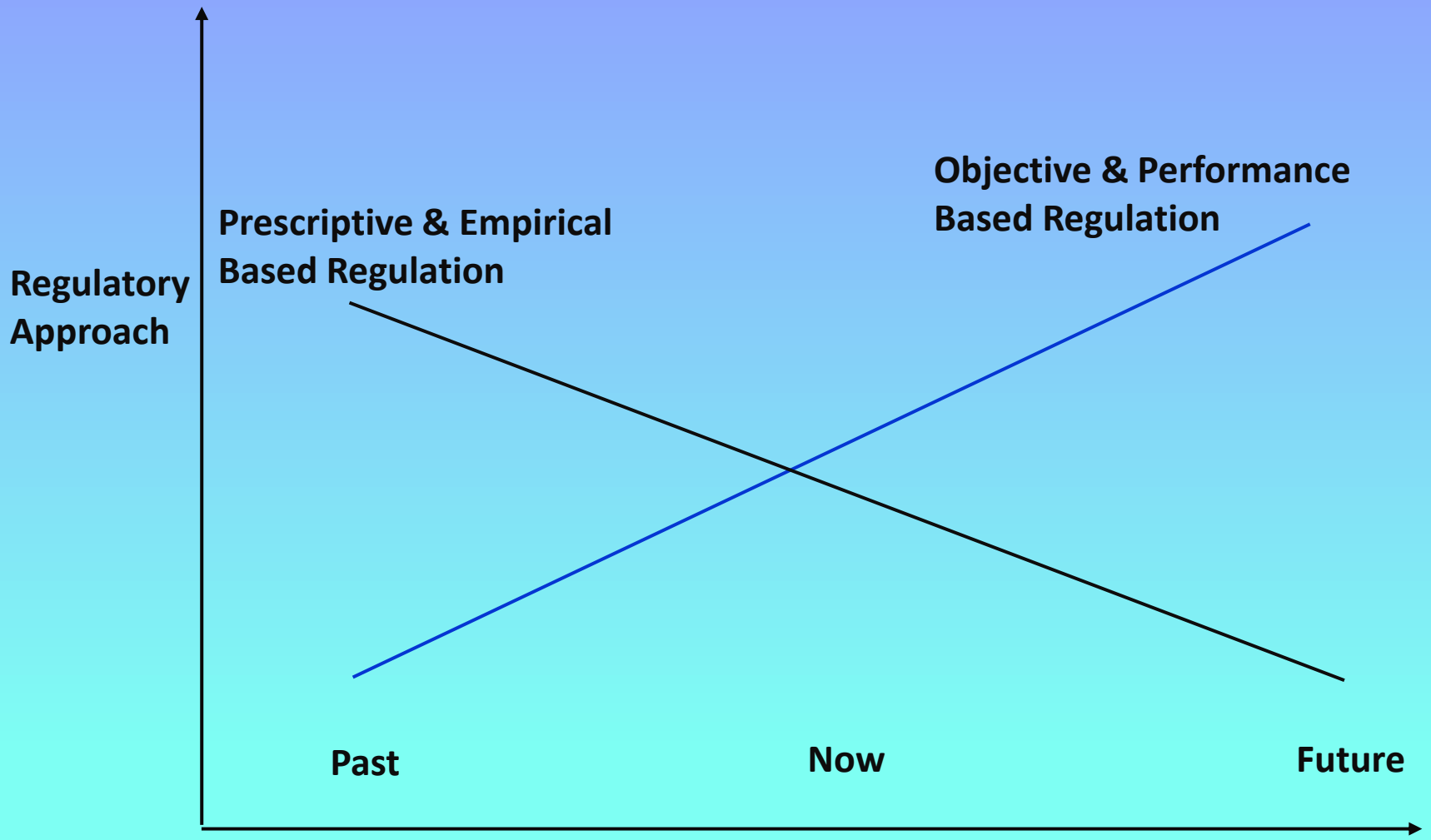
Cologne, November 2021

International Federation of Airworthiness

Who is IFA?

- Non-Governmental Organisation (NGO);
- Independent: non profit / non political;
- Global Membership: a passion for airworthiness;
- Funded by subscriptions, sponsorship and a Trust Fund;
- Run by volunteers
- Charity

- revisit the history of the probabilistic approach,
- talk of the successes and failures in setting safety objectives,
- and put a case for the continued use of a performance-based approach


Regulatory Approach
Prescriptive & Empirical Based Regulation
Objective & Performance Based Regulation
Past
Now
Future

1956

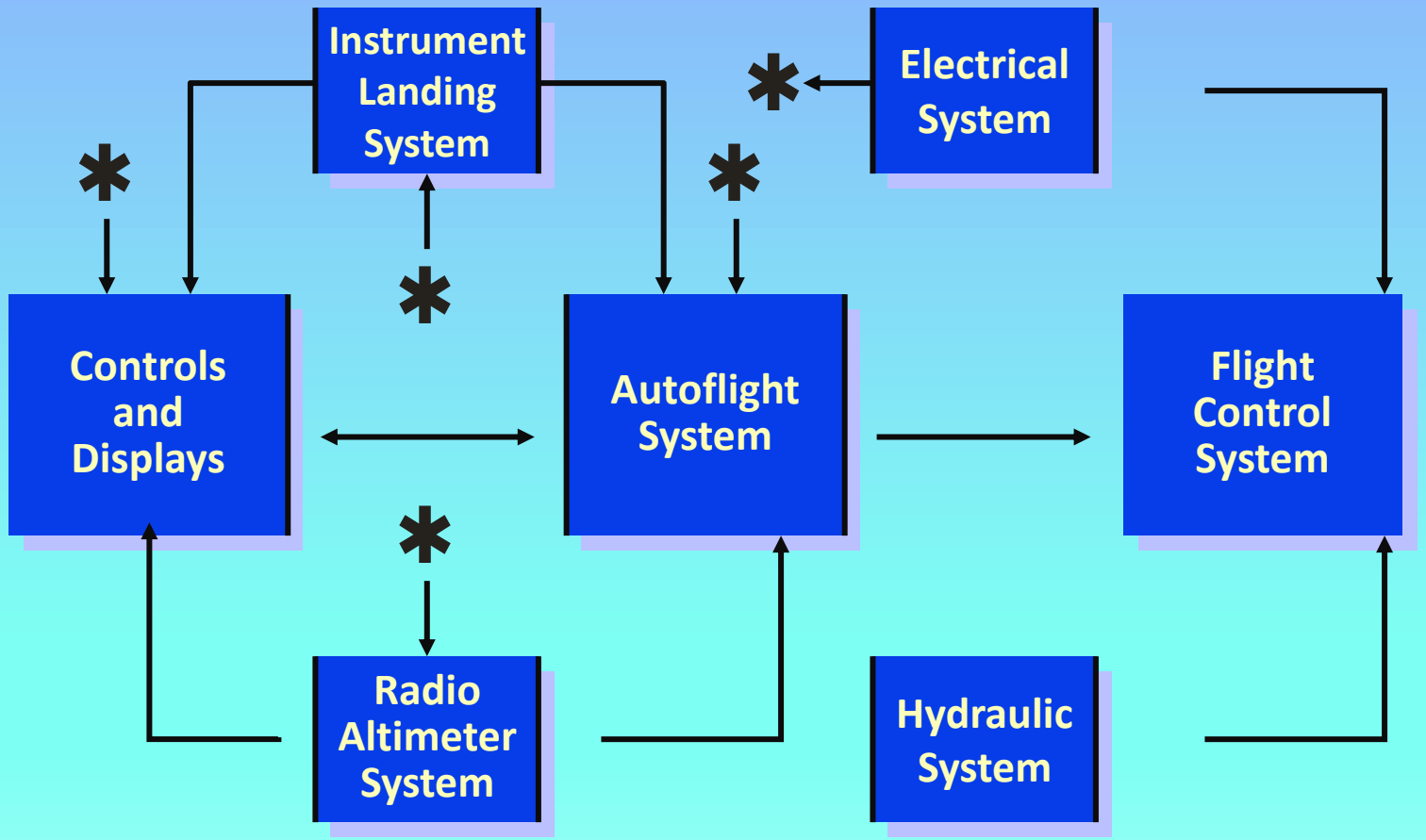
- § 4b.606-1
- Safety criteria 1 for electric utilization system; (FAA policies which apply to § 4b.606 (a) and (b)).
- Electric utilization systems [2] should be analyzed, inspected or tested to assure conformance to the following safety criteria.
  - Loss of system function. The system should not be rendered inoperative by any probable malfunction, [3] if operation of this system is necessary to maintain controlled flight or effect a safe landing for any authorized flight operation.

Automatic (Blind) Landing Systems

1964

- **Not simple,**
- **Not straightforward**
- **&**
- **Not obviously safe**

Automatic Landing System



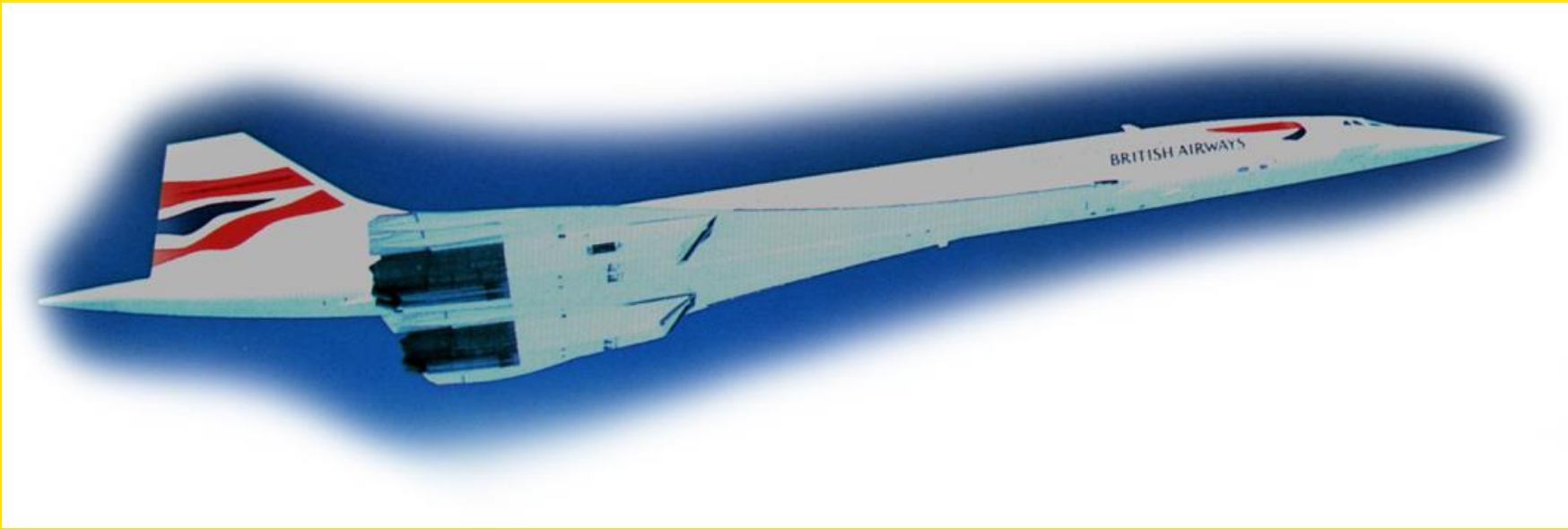
Automatic Landing Systems Safety Objectives

Automatic Landing Systems Safety Objectives

Objective:-	**No increase in risk of accident on landing**
Accident statistics showed:-	**1 fatal accident per million landings (all causes)**
System safety objective:-	**<1 accident in 10 million landings**

Objective: Safe Flight and Landing

- **Concorde**
- **with its advanced technology and complex systems, accelerated the need for generic safety objectives.**
- **Anglo/French Supersonic Transport TSS Standards were created**



Generic System Safety Objectives

Objective:-

No increase in risk of accidents caused by system failures

Jet accident statistics showed (c.1970):

- **Approx. 4 accident per million hours, all causes**
- **0.4 accidents per million hours, systems**

Systems safety objective:

<1 accident per 10 million hours, systems

Generic System Safety Objectives

System Safety Objective for all systems:

<1 accident per 10 million hours

or 1 x 10^{-7} per hour

Assume aircraft contains 10 safety critical systems, each having 10 potential failure conditions which could cause a fatal accident

Safety objective for each of these failure conditions:

<1 accident per billion hours or 1 x 10^{-9} per hour

Working with Probabilities

- **Boeing 737 family has flown >264 million flight hours (April 2014)**
- **Rotorcraft hours flown in Oil and Gas in 2018 - 1 million flight hours**

Binary vs. decimal data measurements

BINARY SYSTEM			DECIMAL SYSTEM		
NAME	FACTOR	VALUE IN BYTES	NAME	FACTOR	VALUE IN BYTES
kibibyte (KiB)	2^{10}	1,024	kilobyte (KB)	10^{3}	1,000
mebibyte (MiB)	2^{20}	1,048,576	megabyte (MB)	10^{6}	1,000,000
gibibyte (GiB)	2^{30}	1,073,741,824	gigabyte (GB)	10^{9}	1,000,000,000
tebibyte (TiB)	2^{40}	1,099,511,627,776	terabyte (TB)	10^{12}	1,000,000,000,000
pebibyte (PiB)	2^{50}	1,125,899,906,842,624	petabyte (PB)	10^{15}	1,000,000,000,000,000
exbibyte (EiB)	2^{60}	1,152,921,504,606,846,976	exabyte (EB)	10^{18}	1,000,000,000,000,000,000
zebibyte (ZiB)	2^{70}	1,180,591,620,717,411,303,424	zettabyte (ZB)	10^{21}	1,000,000,000,000,000,000,000
yobibyte (YiB)	2^{80}	1,208,925,819,614,629,174,706,176	yottabyte (YB)	10^{24}	1,000,000,000,000,000,000,000,000

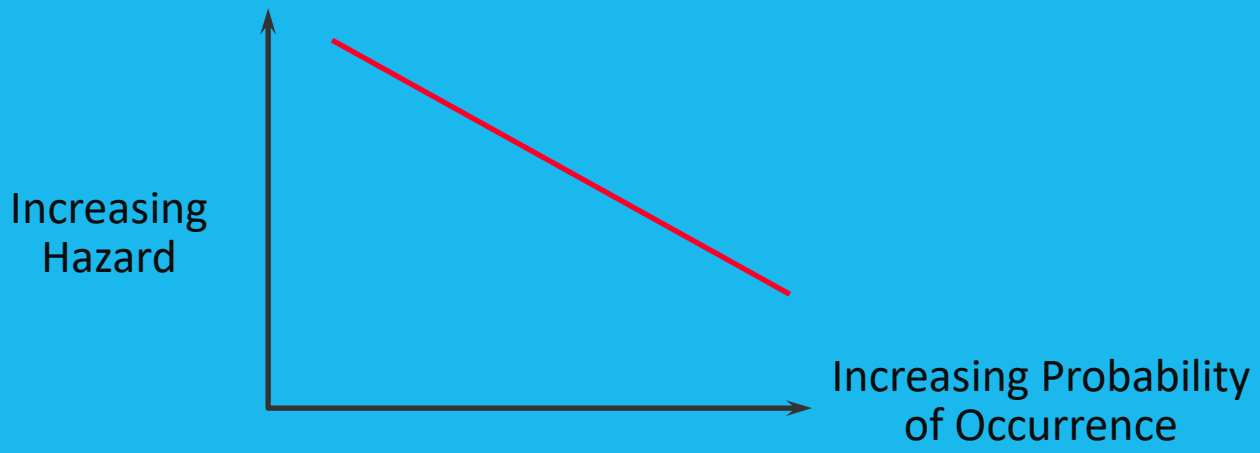
Two principles

Safety Objectives should ensure that:

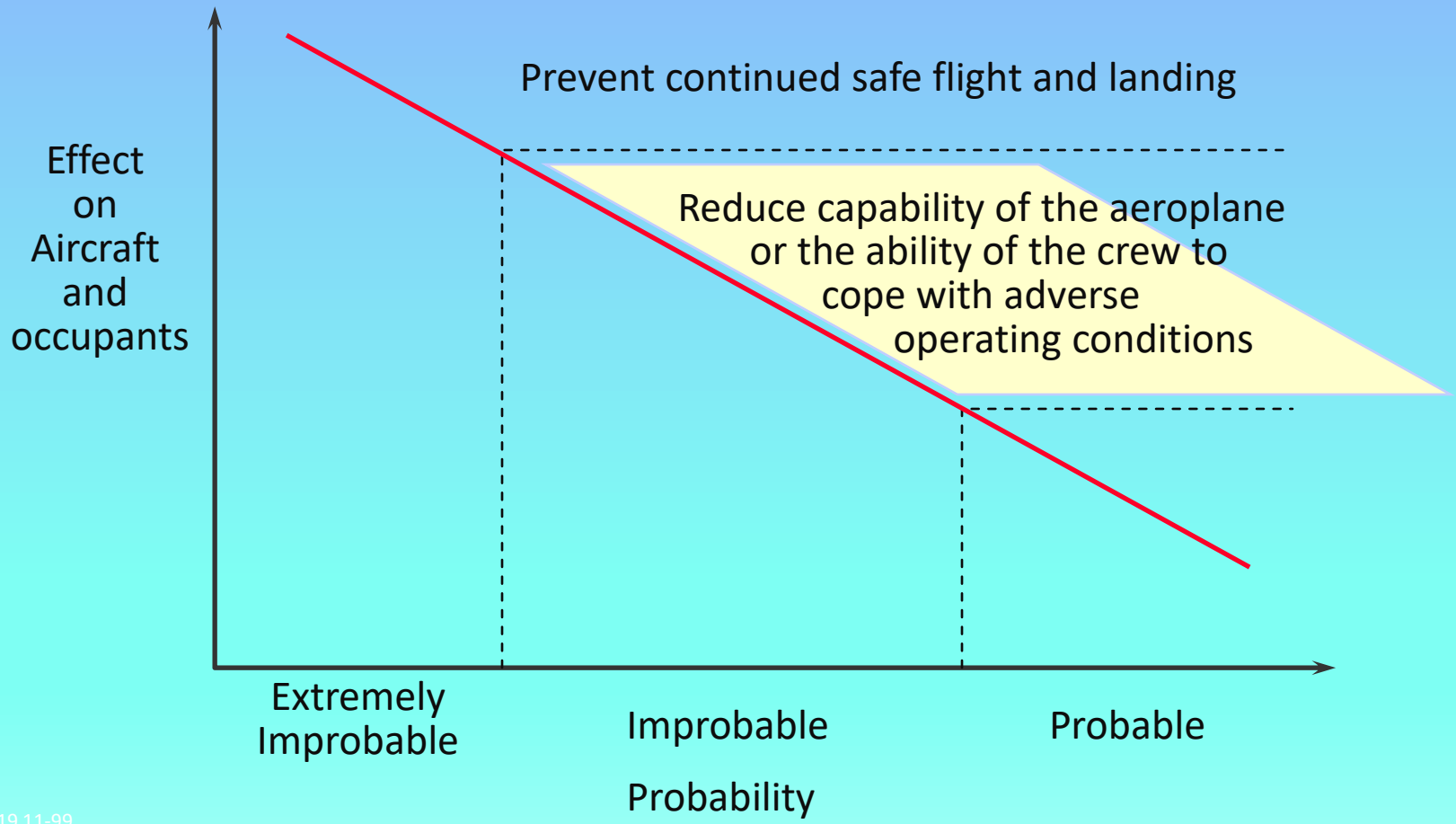
1. **There is no increase in risk of accident, and where possible an improvement in safety**

and

2. **An inverse relationship exists between the probability of an occurrence and the severity of hazard inherent in its effect**

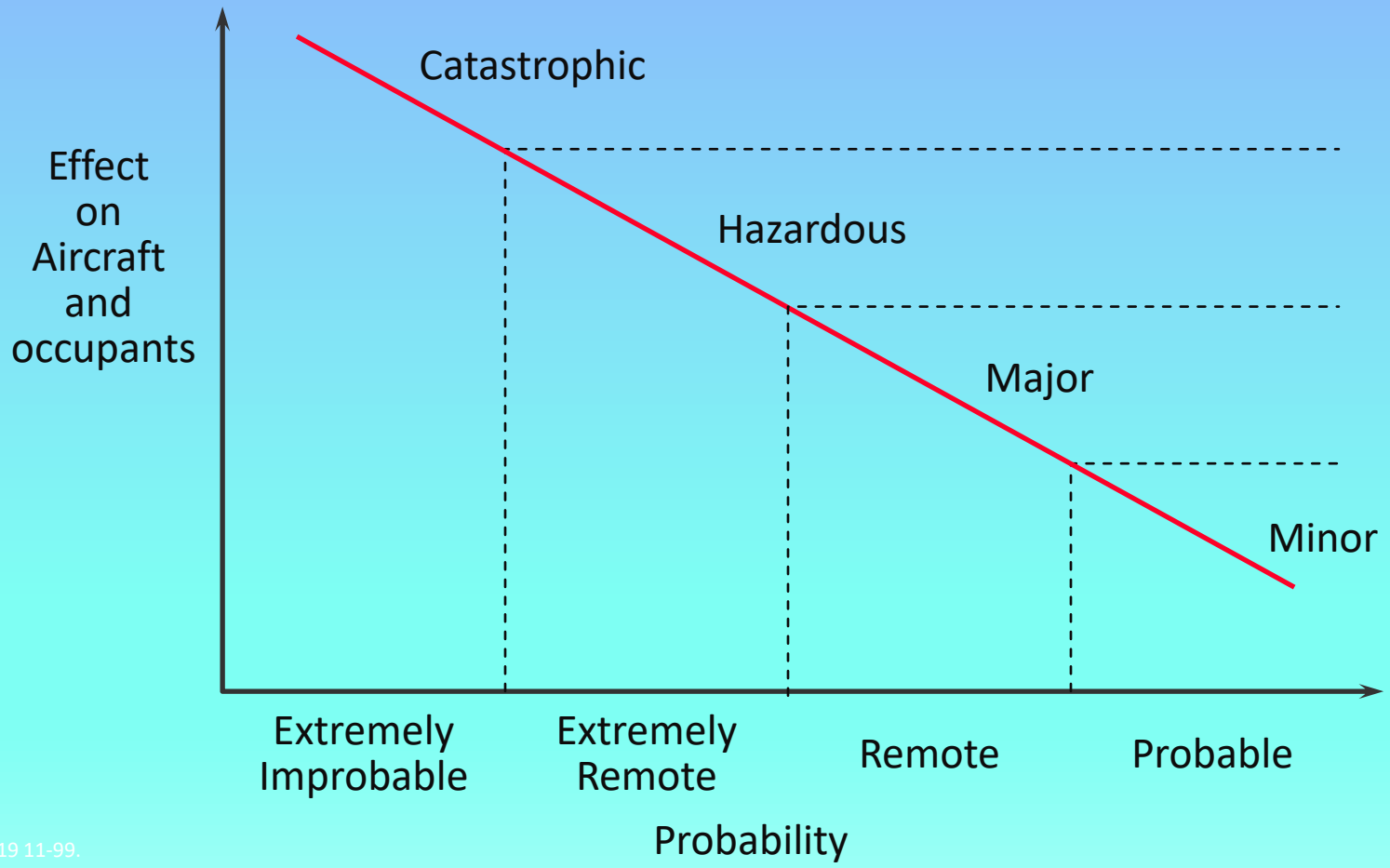


Failure Conditions Probability and Effect: The Inverse Relationship

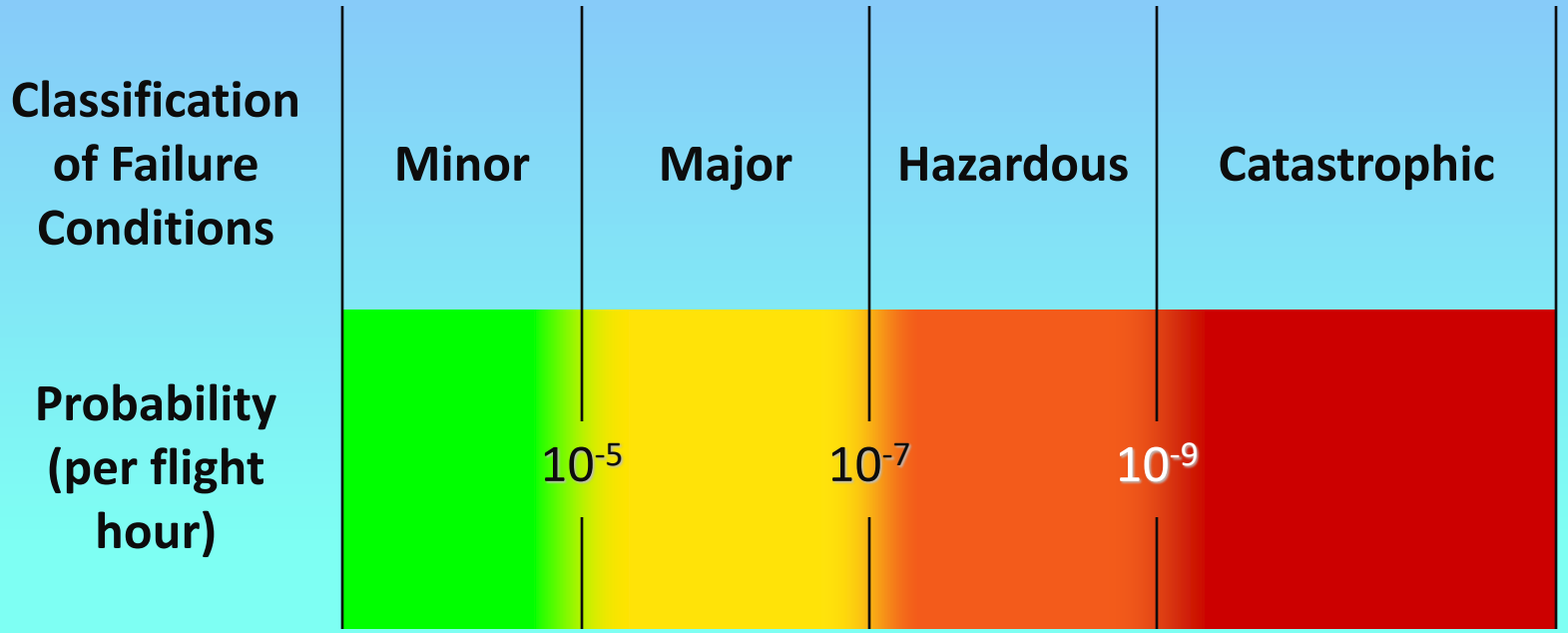


Probability and Effect: The Inverse Relationship

(Advisory Material 25.1309)



Classifications and Probability



Failure Condition Effects and Classifications

Effect on Aircraft and Occupants	Nuisance; Operating limitations, emergency procedures	Significant reduction in safety margins; difficult for crew to cope with adverse conditions, passenger injuries	Large reductions in safety margins; crew extended because of workload or environmental conditions; serious or fatal injury to a small number of occupants	Multiple deaths, usually with loss of aircraft
Classification of Failure Conditions	Minor	Major	Hazardous	Catastrophic

Risk Reduction by Multiplexing

No. of Channels	Single Failure	All Channels Failures
1	$P = 1 \times 10^{-3}$	$P = 10^{-3}$
2	$2P = 2 \times 10^{-3}$	$P^2 = 10^{-6}$
3*	$3P = 3 \times 10^{-3}$	$P^3 = 10^{-9}$
4	$4P = 4 \times 10^{-3}$	$P^4 = 10^{-12}$

- ***Remember a Common Mode failure can totally dominate. A Common Mode failure with a probability of 10^{-7} that affects all 3 Channels would result in a failure risk of $10^{-7} + 10^{-9} = 1.01 \times 10^{-7}$**

System Safety Assessment Key Questions

What is the system?

What does it do?

What can go wrong?

What happens if it goes wrong?

What can cause it to go wrong?

What is the risk?

Can we accept the risk?

What is the System?

Flight Controls

What does it do? ***Function***	What can go wrong? ***Failure Conditions***	What happens if it goes wrong? ***Failure Condition Effects***	 ***Failure Condition Classification***
Pitch control	**Loss of pitch control** **Oscillatory pitch control (high speed)**	**Loss of aircraft control** **Structure damage**	**Catastrophic** **Catastrophic**

System Safety Assessment

Step 1

Functional Hazard Assessment (FHA) establishes Safety Objectives for System Functions

Step 2

Systematic Safety Analysis is undertaken to determine if the system meets the Safety Objectives

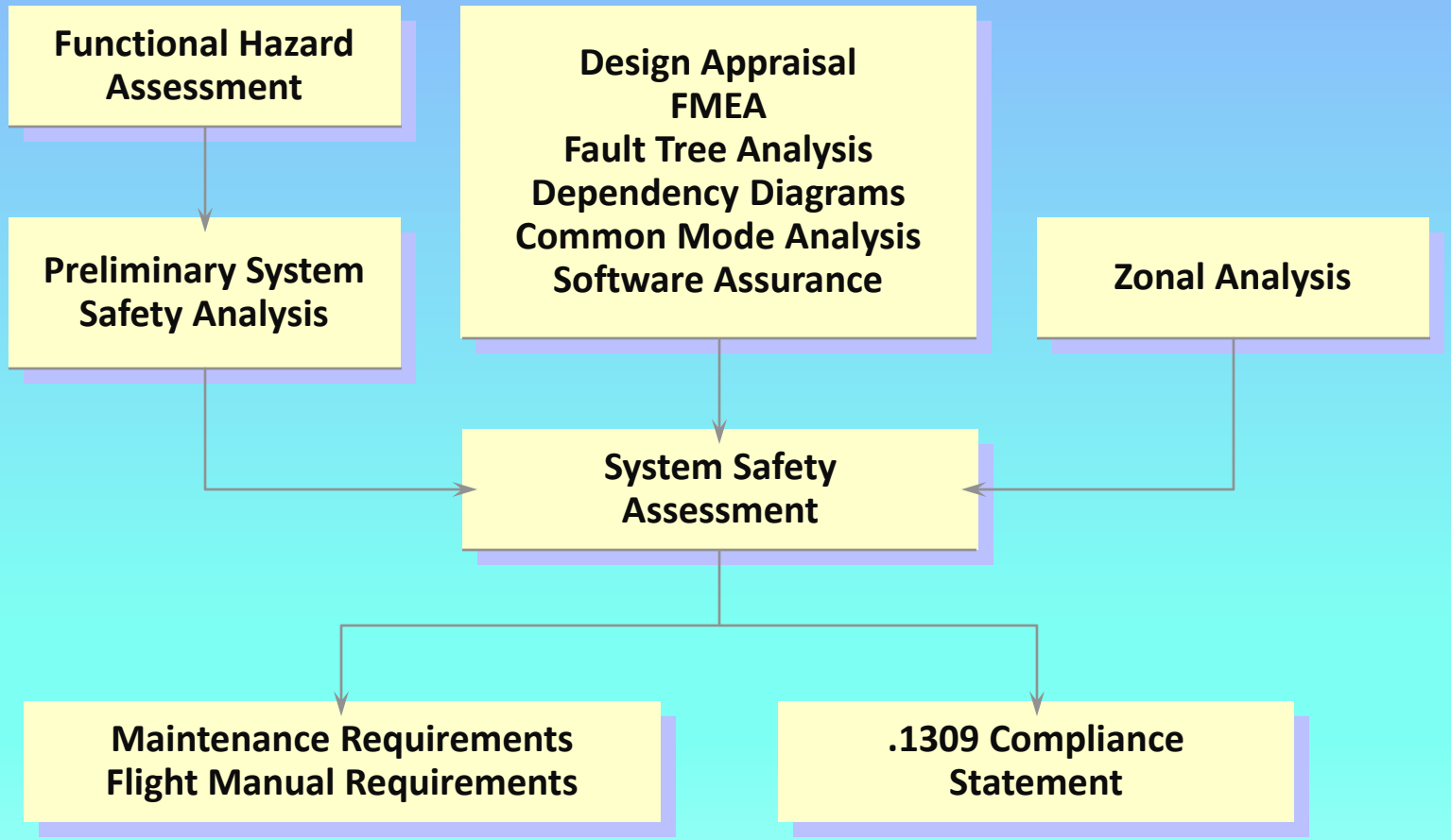
Step 3

Evidence is provided to demonstrate compliance, provide limitations and candidate maintenance requirements

Types of Analysis

Design Appraisal	Failure Mode and Effects Analysis	Fault Tree
Dependency Diagram	Common Cause Analysis	Zonal Analysis
Particular Risk Analysis	Performance Analysis	Development & Software Assurance

System Safety Assessment Process Overview



Safety Advancement

- **The Potential of Technologies to Mitigate Helicopter Accident Factors – An EHEST Study (NLR 2014)**
  - **There are 15 ‘highly promising’ technologies, and 50 are ‘moderately promising’.**
- **European Plan for Aviation Safety (EPAS) 2021-2025**
  - **RMT.0712 Enhancement of the safety assessment processes for rotorcraft designs**

Certification Specification CS 27.1309

NPA 2021-11

….. equipment and systems ….. considered separately and in relation to other systems, must be designed and installed such that so that:

1. Each catastrophic failure condition is extremely improbable; and does not result from a single failure,
2. Each hazardous failure condition is extremely remote; and
3. Each major failure condition is remote, …..

Guidance to .1309

1. **Recognition of**
   - SAE ARP 4754/EUROCAE ED 79 Certification Considerations for Highly-Integrated or Complex Aircraft Systems
   - SAE ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

Safety Performance

- **“There is no reliable process to ensure that assumptions made in safety assessments are valid with respect to operation and maintenance activities”.**
- **Digital Transformation**
  - **Unlocks the opportunity to use data to validate certification assumptions by using operational experience**

Sum up

- It’s not just about numbers. It’s about a clear systematic methodology
- Systems Safety Assessment is a proven method
- Not just on the “to do” list to satisfy the Certification Authorities
- Qualitive processes supported by quantitive methods
- Methods continue to develop apace as technology challenges
- Cloud connected avionics, autonomy and all electric aircraft