Airbus Product Safety
Xavier Jolivet
Safety Enhancement

Basic concepts & Safety Risk Management

Scope & System considered

The very first question in any safety assessment is about defining the system that is considered:

System:

A set of elements (technical, organizational, human, etc.), interacting with one another, in an organized way to achieve common objectives, in given conditions.

Any activity is a "system".

- Most hazards are generated by operational interactions among different system elements.
- It is therefore essential to describe & know the system in terms of its elements.

“Hazard”: what does it mean ?

- **Hazards** are conditions or objects with the potential of […] causing or contributing to unsafe operation of the aircraft…

- **Hazards** are an inevitable part of aviation activities…

- **Common tendency to confuse hazards with their consequences** or outcomes.

  A consequence is an outcome that can be triggered by a hazard (ICAO SMM)

ICAO defines safety [Document No. 9859 (Safety Management Manual)] as follow:

“Hazard identification is a prerequisite to the safety risk management process. Any incorrect differentiation between hazards and safety risks can be a source of confusion. A clear understanding of hazards and their related consequences is essential to the implementation of sound safety risk management.

A hazard is generically defined by safety practitioners as a condition or an object with the potential to cause death, injuries to personnel, damage to equipment or structures, loss of material, or reduction of the ability to perform a prescribed function. For the purpose of aviation safety risk management, the term hazard should be focused on those conditions which could cause or contribute to unsafe operation of aircraft or aviation safety-related equipment, products and services. ”

AIRBUS

Hazards Classification (1/2)

A hazard depends on the scope and boundaries of the system and on the ultimate objectives

Hazards Classification (2/2)

External vs. Internal

- External Hazard (external to the system)
  - Ex: environmental hazards (meteorological, natural), laser beams...

- Internal Hazard (internal to the system)
  - Failure
  - Violations
  - Intrinsic Hazard (system with risk potentiality even without failure)

“Consequence”

- **Consequence** – Potential outcome(s) of the unwanted event

The **effects of an unwanted event** depend on the **properties of the system** and of **the context** in which the error occurs

AIRBUS

“Risk”: what could it mean ?

Many definitions!

- Uncertainty on objectives achievement
- Possibility of a bad result
- Possibility of suffering harm or loss

To be understood, “Risk” needs to be precised:

- What is the context?

  → Often implicit (ex Civil Aviation, Nuclear Industry)

- What is the system and its operations

  → Am I considering risk for a person, an Organisation or a Company , a Product ?...
  What are the normal operations ?

- What would be the ultimate objectives and/or outcomes to be avoided?

  → Finance: no loss of money
  Health: no fatality, no injury….

Risk is often qualified with regards to objectives and/or outcomes:
Risk **of** fatality, of injury, of damage to property, of intrusion ….

AIRBUS

Risk

- **Risk** is the result of an **assessment**
  - Expressed in terms of **predicted probability** and **severity** of the consequence(s) of an unwanted event resulting from hazard, taking as reference the worst foreseeable situation.
- **Risk** exists because of the **exposure** of a system **to hazards**

  - ***Flight ops***
    - *A wind of 15 knots blowing directly across the runway is a hazard*
    - *A pilot may not be able to control the aircraft during landing is one of the consequences of the hazard*
    - *The assessment of the consequences of the potential loss of control of the aircraft by the pilot expressed in terms of probability and severity is the risk*

  - ***Maintenance***
    - *Inappropriate tooling is an hazard*
    - *The technician may not be able to do the required task is the consequence of the hazard*
    - *The assessment of the consequences of delivering an unworthy aircraft is expressed in term of probability and severity is the risk*

Safety Risk Management (SRM)

Example of Risk Scenario

System
Walker

CAUSE

Hazard: Ice on Pavement → **Hazardous Situation**: Walking on Ice

→ **Unwanted Event**: Falling Down

→ **EFFECT**

Consequences: Fracture Leg

Risk Factor: Going Outside

Risk Factor: Sliding

Risk Factor: Fragile Bones

AIRBUS

Safety Risk Management (SRM) - Exercise

Comprehending Risk / Level of Risk

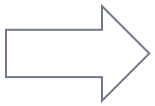
To comprehend risks, they are generally expressed in terms of:

predicted probability and severity,

of the outcomes of an unwanted event,

resulting from hazards,

taking as reference the worst foreseeable situation



Level of Risk

"ICAO Annex 19 Definition of Safety Risk:

"The predicted probability and severity of the consequences or outcomes of a hazard"

AIRBUS

Safety : what does it mean ?

- **Safety** is the state of being "safe“, the condition of being protected against the consequences/outcomes of hazards or of any other event which could be considered non-desirable.

- **Safety** is generally interpreted as implying a risk of fatality, injury or damage to property.
- **Safety** can also be defined to be the control of identified hazards to achieve an acceptable level of risk.

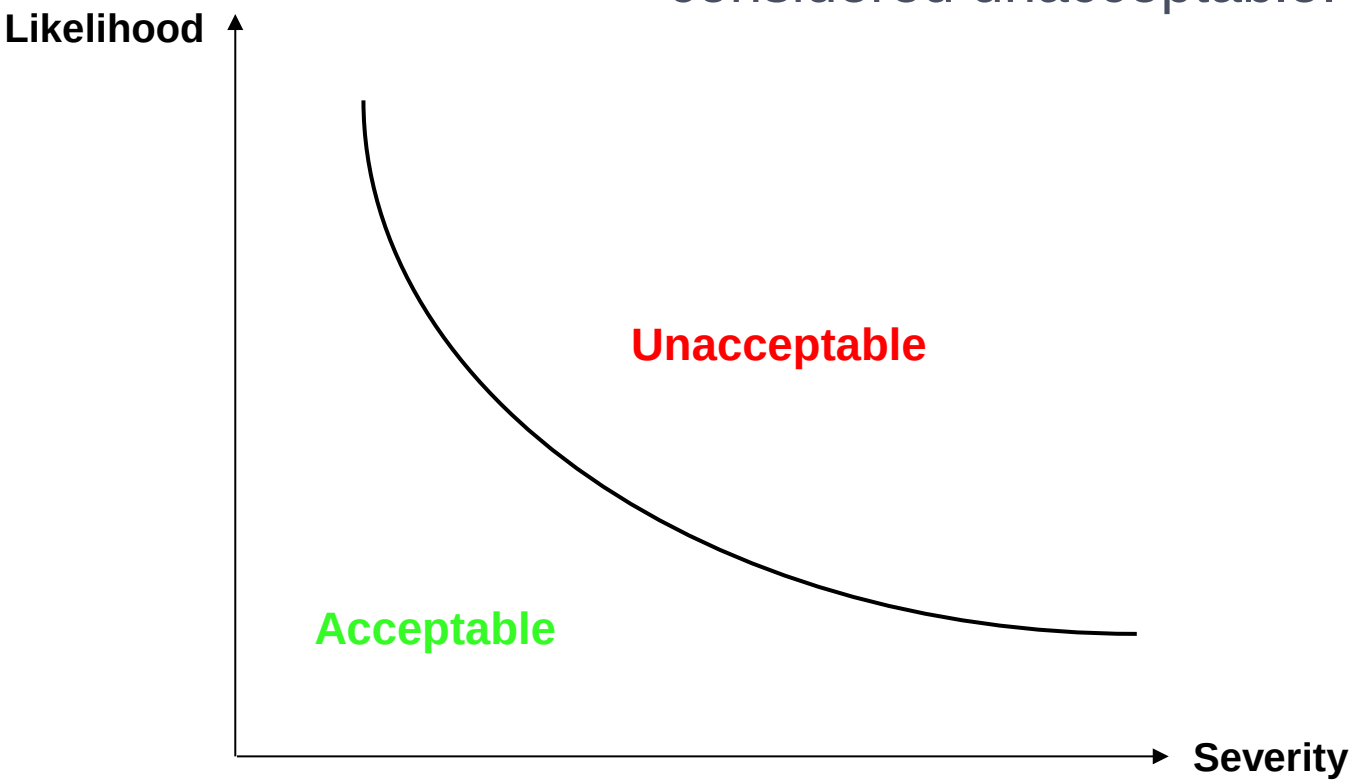
ICAO defines safety [Document No. 9859 (Safety Management Manual)] as:
“The state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management”

AIRBUS

Safety Risk Management (SRM)

Acceptability Threshold

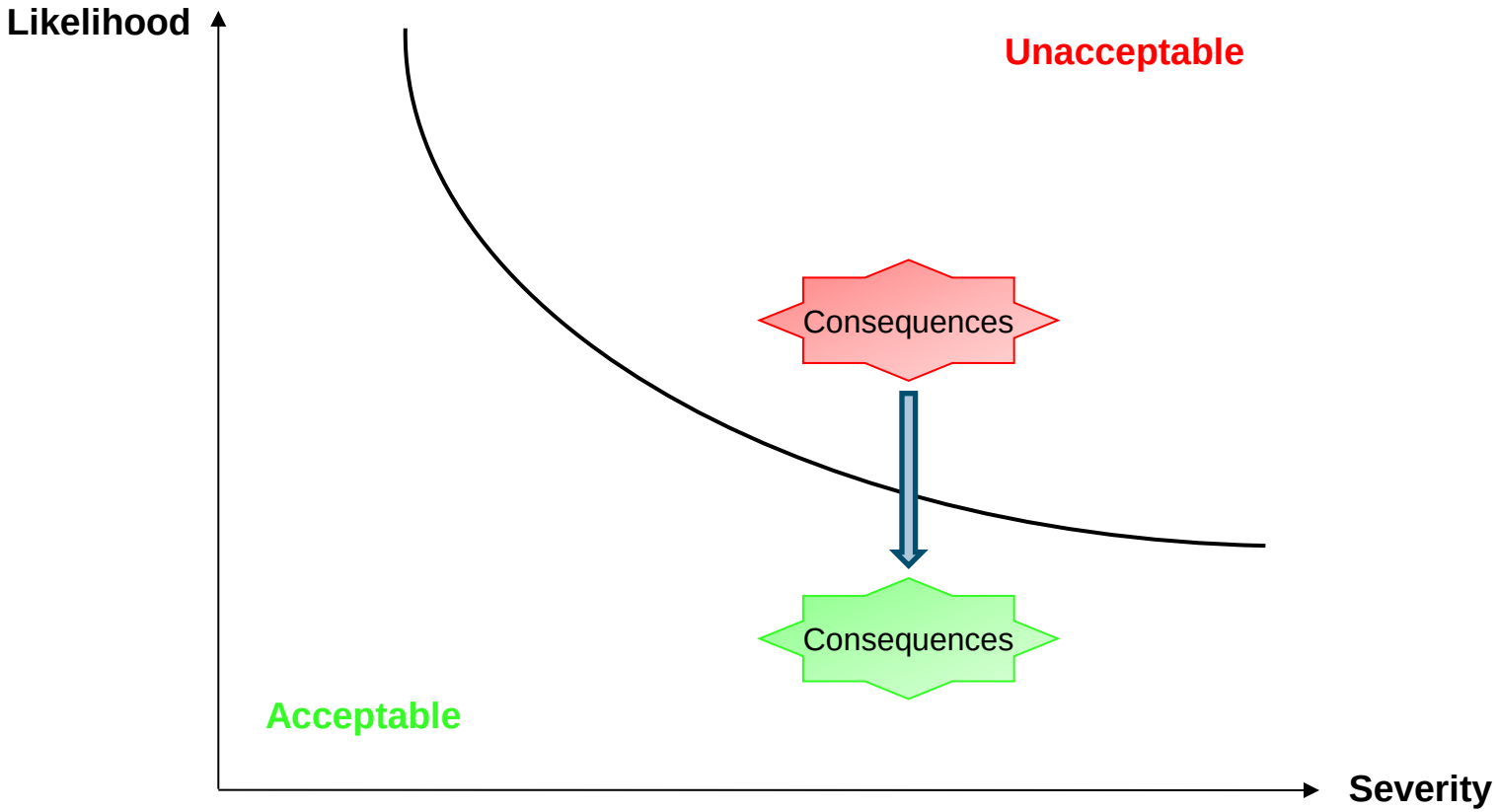
Threshold (defined by the combination of the likelihood and the severity of the consequences) above which a risk is considered unacceptable.



Safety Risk Management (SRM)

Prevention

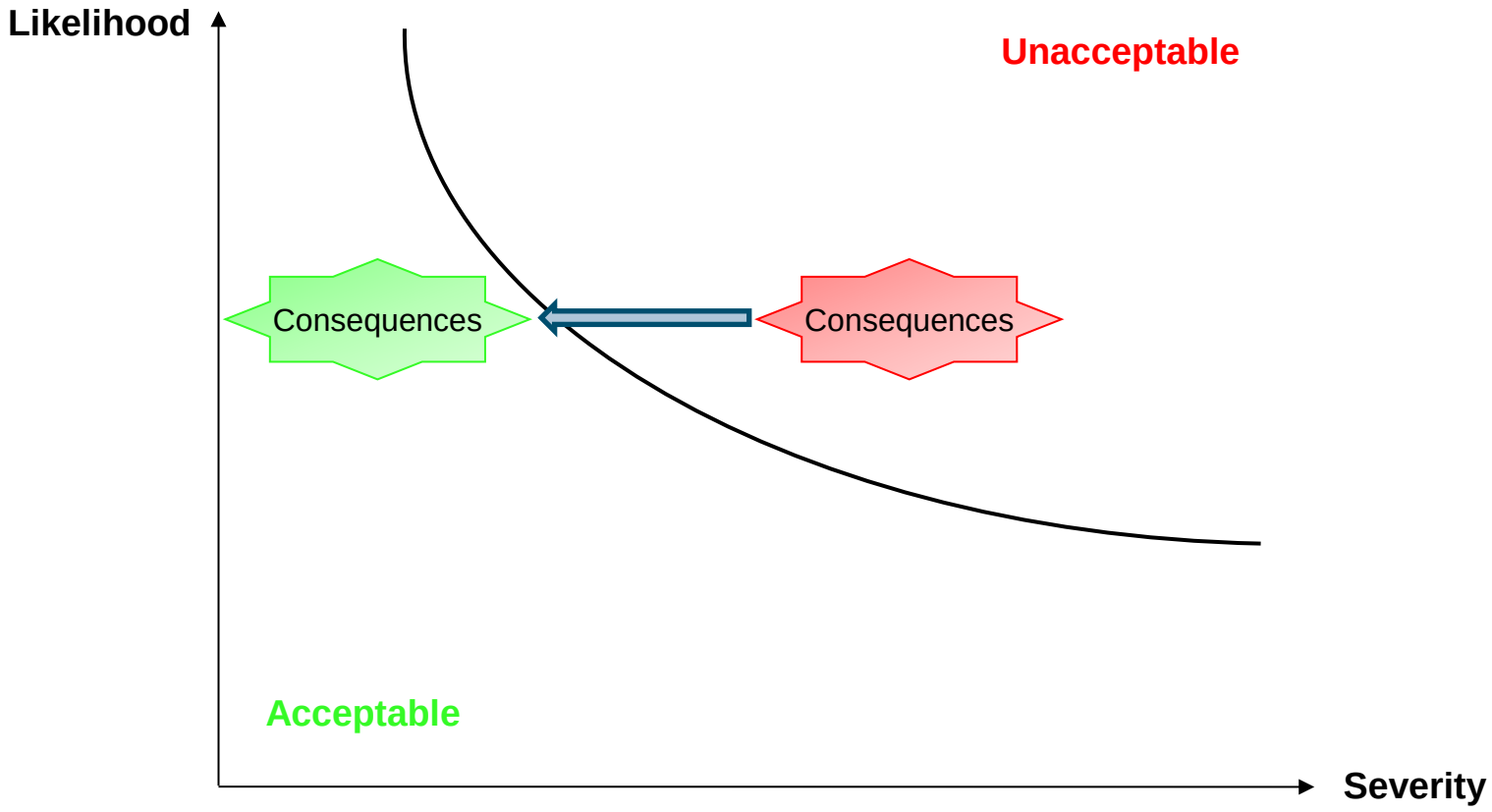
Risk reduction strategy that aims to reduce the likelihood of the unwanted event consequences.



Safety Risk Management (SRM)

Protection

Risk reduction strategy that aims to reduce the severity of the consequences of the unwanted event.



Safety Risk Management (SRM) - Mitigation

- *Hazards are an inevitable part of aviation activities…*

- *…. However, their manifestation and possible consequences can be addressed through various mitigation strategies to contain the potential for a hazard …*

- *Safety risk management encompasses the assessment and mitigation of safety risks. The objective of safety risk management is to assess the risks associated with identified hazards and develop and implement effective and appropriate mitigations.*

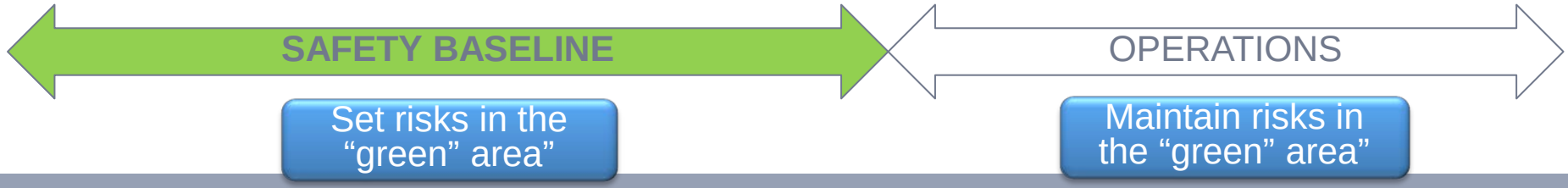
(source ICAO SMM)

Safety Risk Management (SRM)

1 Define system and acceptable risks

2 Identify hazards, assess and control risks

3 Maintain risks at an acceptable level



AIRBUS

Safety Risk Management (SRM)

Examples of Risk Reduction

System
Walker

CAUSE

Hazard: Ice on Pavement

Salt

Hazardous Situation: Walking on Ice

Unwanted Event: Falling Down

Reinforced Personal Equipment

EFFECT

Consequences: Fracture Leg

Staying Home

Crampons

Risk Factor
Going Outside

Risk Factor
Sliding

Risk Factor
Fragile Bones

Adapted from: Airbus Enterprise Risk Management (ERM), Alain Desroches

Ex: ICAO Risk assessment matrix (1/3)

1 Define system and acceptable risks

System = A/C operations

Severity classification

Severity	*Meaning*	*Value*
Catastrophic	— Equipment destroyed — Multiple deaths	A
Hazardous	— A large reduction in safety margins, physical distress or a workload such that the operators cannot be relied upon to perform their tasks accurately or completely — Serious injury — Major equipment damage	B
Major	— A significant reduction in safety margins, a reduction in the ability of the operators to cope with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their efficiency — Serious incident — Injury to persons	C
Minor	— Nuisance — Operating limitations — Use of emergency procedures — Minor incident	D
Negligible	— Few consequences	E

AIRBUS

Ex: ICAO Risk assessment matrix (2/3)

1 Define system and acceptable risks

Likelihood classification

Likelihood	*Meaning*	*Value*
Frequent	Likely to occur many times (has occurred frequently)	5
Occasional	Likely to occur sometimes (has occurred infrequently)	4
Remote	Unlikely to occur, but possible (has occurred rarely)	3
Improbable	Very unlikely to occur (not known to have occurred)	2
Extremely improbable	Almost inconceivable that the event will occur	1

AIRBUS

Ex: ICAO Risk assessment matrix (3/3)

1 Define system and acceptable risks

Risk probability		Risk severity				
		Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely improbable	1	1A	1B	1C	1D	1E

Tolerability description	Assessed risk index
Intolerable region	5A, 5B, 5C, 4A, 4B, 3A
Tolerable region	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A
Acceptable region	3E, 2D, 2E, 1B, 1C, 1D, 1E

AIRBUS

Ex 2: CS 25.1309 Matrix

1 Define system and acceptable risks

System = Aircraft Product

Effect on Aeroplane	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	<-----Minor------>	<-----Major------>	<--Hazardous-->	Catastrophic

Note 1: A numerical probability range is provided here as a 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 aeroplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.

AIRBUS

Steps & activities

2 Identify hazards, assess and control risks

- Identify hazards (internal & external) and possible consequences
- Identify unwanted events / situations
- Assess associated risks
- Decide on the risk acceptability

Building scenarios (chain of events, combination of hazards, triggering events,..)

Rating in terms of severity and likelihood to define the risk level

Risk level versus acceptability criteria

NOT ACCEPTABLE

- Define defences to reduce risk to an acceptable level
- Validate and implement the defences

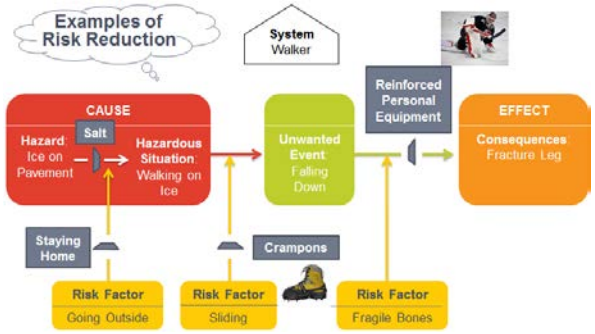
AIRBUS

Risks reduction

2 Identify hazards, assess and control risks

Relevant questions to validate a safety defence:

- Does it address the risk?
- Is it effective?
- Is it appropriate?
- Is it efficient?
- Is additional or different mitigation warranted?
- Does the safety defence strategy generate additional hazards?



AIRBUS

Steps / Activities

3 Maintain risks at an acceptable level

To keep risks under an acceptable level by continuously and actively:

- Monitor the evolution of the system environment
- Seek and analyze system & environment data

DATA

Identify new or detect evolving:
- Hazards
- Scenarios
- Consequences

- Perform new risk assessments or, revaluate existing ones by revisiting initial hypotheses
- Add new defences or reinforce existing ones
- Monitor the effectiveness/efficiency of the safety defences put in place, in particular of mitigation means, and adjust as needed.

AIRBUS