Imperial College London

T29 Transport, Environmental Impacts and Safety: Week 1

February 12 2019

Dr. Arnab Majumdar
Centre for Transport Studies
Imperial College London
a.majumdar@imperial.ac.uk

Plan

Topic Objectives

- Plan of lectures
- What is safety?
- Introduction to SMS - hazards
- Approaches to safety
- Definitions

Lecture objectives

To teach the fundamental tenets of transport safety based upon elements of safety management systems (SMS)

Fundamentals of safety including:

- the evolution of its management into a structured and systematic process;

- necessary to ensure the overall integrity of an organisation in its aim to ensure safety and prevent accidents.

Intended Learning Objectives

By the end of today's lecture you will be able to:

- Understand the importance of hazards and their link to safety risk;
- Summarise the different approaches to safety;
- Evaluate the importance of definitions when considering accident statistics.

What is safety?

Safety is a commonly used word **but** can have different meanings

Dictionary:

1. the quality or condition of being safe; freedom from danger, injury, or damage; security.
2. (technical) the stability of a building, machine or other construction, the tranquillity of its operation and the fact that it does not endanger its environment.

Relative - only defined if the condition of its surrounding is defined as well.

Basic idea of transport safety

We want to reach our destination without getting hurt.

Occasionally we do get hurt, therefore we are willing to accept some risk in travelling:

- acknowledge there is a chance we could get killed travelling, and
- we travel with this risk in mind.

Aviation safety

In ATM and aviation in general, safety is defined as (ICAO, 2009, 2013):

"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".

'acceptable' or 'tolerable' level of risk:

- A very generic and relative societal expectations in terms of commercial aviation safety (or ATM).

Imperial College London

The two paradigms

Safety- I

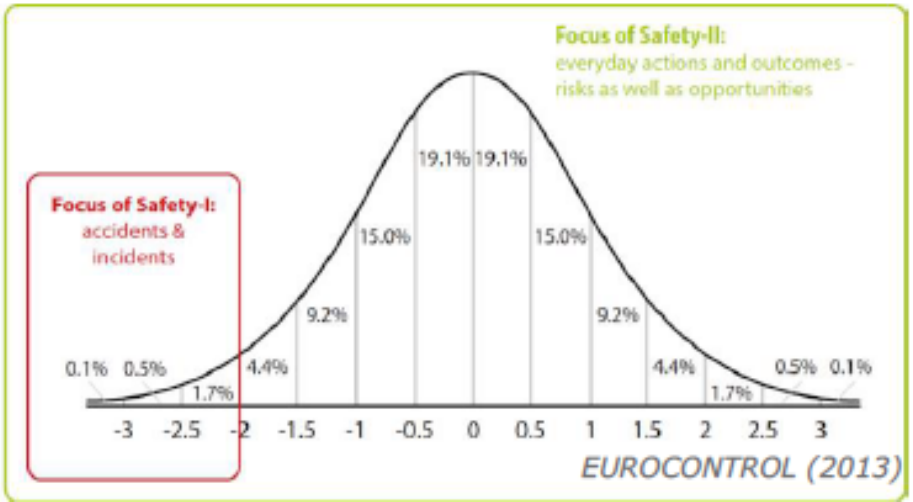
"the state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management"

ICAO

Safety- II

"the system's ability to succeed under varying conditions, so that the number of intended and acceptable outcomes (in other words, everyday activities) is as high as possible"

Hollnagel (2013)



Imperial College London

The two paradigms – their difference

	Safety-I	Safety-II
Definition of safety	That as few things as possible go wrong.	That as many things as possible go right.
Safety management principle	Reactive, respond when something happens or is categorised as an unacceptable risk.	Proactive, continuously trying to anticipate occurrence developments and control/enhance its variability.
View of the human factor in safety management	Humans are predominantly seen as a liability or hazard.	Humans are seen as a resource necessary for system flexibility and resilience.
Role of performance variability	Harmful, should be prevented as far as possible.	Inevitable but also useful. Should be monitored and managed.
Accident investigation	Accidents are caused by failures and malfunctions. The purpose of an investigation is to identify the causes.	Things basically happen in the same way, regardless of the outcome. The purpose of an investigation is to understand how things usually go right as a basis for explaining how things occasionally go wrong.
Risk assessment	Accidents are caused by failures and malfunctions. The purpose of an investigation is to identify causes and contributory factors.	To understand the conditions where performance variability can become difficult or impossible to monitor and control.

Aviation accidents

- First fatal crash soon after Wright Brothers flight
- First mid-air collision in 1910 though no fatalities
- Uberlingen:

http://www.youtube.com/watch?v=9kJ7aTOo_Yc

Safety Management System

A SMS is:

- An enhanced and rigorous framework to deal with safety issues at all levels of an organisation.

Various functions in SMS rely on similar concepts:

- understand these interactions to ensure that proper methodologies are derived to complement each other.

Stakeholders

Consider an airport:

- major areas of operations are the runways and taxiways.
- stakeholders at an airport, e.g. airlines, air traffic control, airport authorities and regulators, interact.
- operations can be thought of as a **socio-technical system**
- people actively interact with technology in order to achieve production goals (i.e. aircraft departing and arriving) through the delivery of services.

Hazards

A major characteristic of socio-technical systems is the presence of **hazards**:

"condition(s) or object(s) with the potential to cause injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function"

Hazards (1)

Hazards are not necessarily damaging, but:

- have the potential to be safety critical.

Potential effects should be assessed and controlled, for instance, by:

- preventing them to occur in the first place, or

- mitigating their consequences.

Hazards (2)

Keep safety risks under a reasonable degree of control: system is considered to be safe

Safety must encompass relatives rather than absolutes,

- hazards are an integral part of inherently safe systems, and
- safety risks are acceptable as long as they are controlled.

Where can we find hazards?

In any part of a system and include those associated with:

- design factors (e.g. physical airport surface infrastructure, aircraft, ATC equipment),
- procedures and operational practices (e.g. inadequacy of procedures for the actual operating conditions),
- human performance and work environment (e.g. physical ability to carry out the work, noise, temperature, lighting), and
- organisational factors (e.g. compatibility of production and safety goals).

Imperial College London

What are the consequences of a hazard?

Every hazard has a **consequence**, "the potential outcome (or outcomes) of a hazard."

Can be damaging and present a risk to safety.

To prioritise hazard mitigation efforts:

- quantify consequences of hazards.

What is safety risk? (1)

The assessment, expressed in terms of:

- Predicted probability i.e. “the likelihood that an unsafe event or condition might occur”, and
- Severity i.e. “the possible consequences of an unsafe event or condition, taking as a reference the worst foreseeable situation”,

of the consequences of a hazard.

What is safety risk? (2)

After the safety risk of the consequence of a hazard has been determined:

- assess tolerability of safety risks (i.e. “the tolerability of the consequences of hazards”).

Use a safety risk assessment matrix and subsequently evaluated by means of a safety risk tolerability matrix.

If safety risks are considered to be intolerable, they must be mitigated.

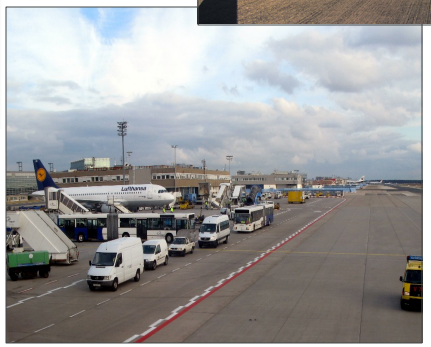
Imperial College London

Airport surface

Incursions / Collisions

Aircraft - Aircraft

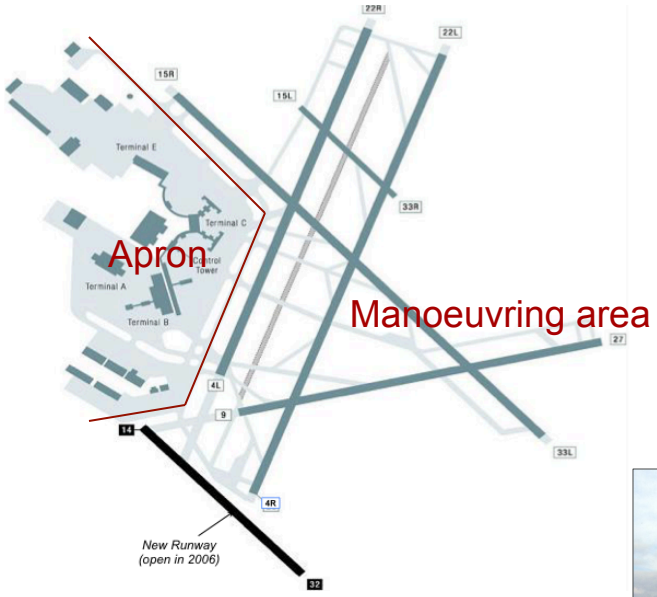
Aircraft – Pedestrian



Aircraft - Vehicle

Excursions

Animals, Foreign Objects, etc.



Hazard -> catastrope (1)

Hazard: Wind blowing at 15 knots across a runway.

Consequences of this hazard: a runway excursion, an occurrence whereby an aircraft leaves the paved runway surface, because the pilot is not able to control the aircraft in crosswinds.

Imperial College London

Probability & Severity

Frequency	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

Severity of occurrence	Meaning	Value
Catastrophic	- Equipment destroyed - Multiple deaths	A
Hazardous	- A large reduction in safety margins, physical distress or a workload such that the operator 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 increase in workload, or as a result of conditions impairing their efficiency - Serious incident - Injury to person	C
Minor	- Nuisance - Operating limitations - Use of emergency procedures - Minor incident	D
Negligible	- Little consequences	E

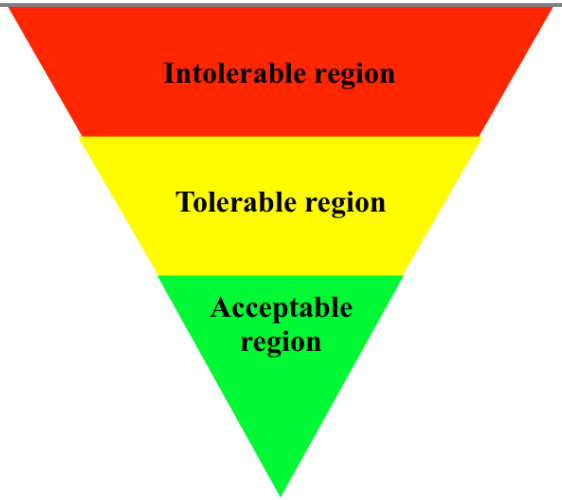
Imperial College London

Safety Risk Assessment Matrix

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

Imperial College London

Safety Risk Tolerability Matrix

Suggested criteria	Assessment risk index	Suggested criteria
	5A, 5B, 5C, 4A, 4B, 3A	Unacceptable under the existing circumstances.
	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C	Acceptable based on risk mitigation. It may require management decision.
	3E, 2D, 2E, 1A 1B, 1C, 1D, 1E	Acceptable.

Imperial College London

Hazard -> catastrope (2)

Safety risk is intolerable (ICAO safety risk index category 4A);

Runway excursions are unacceptable under the existing circumstances.

Mitigate

Task for next week!

What are the possible mitigations for runway excursions?

- Search possible solutions
- Coherent argument for these recognise pros and cons.
- Will discuss beginning of the lesson.

Does it ever get that bad?

The Mangalore air crash 22 May 2010

https://www.youtube.com/watch?v=LkjWm3AIC3A

Summary

1. Identification of hazards,

2. Identification of the consequences of hazards

3. Assessment of the consequences of hazards in terms of probability and severity (the product of probability and severity is the safety risk), and

4. Mitigation of safety risks through the development and implementation of safety risk mitigation strategies.

Imperial College
London

How do accidents occur?

- Understand the accident prevention process
- Built on various methodologies and theories from basic correction of problems identified after the occurrence of an accident to the sophisticated modelling of accidents and incidents.
- Incidents focus - considered as precursors to accidents
- Incident data - key operational aspect to the prevention of accidents and more generally to a Safety Management System (SMS)

Why are accidents important? (1)

Two factors:

Chicago Convention on Civil Aviation:

- International Civil Aviation (ICAO) member states are required to provide air traffic services to ensure the safety of aircraft, passengers and others directly affected by the operations of the aircraft

- Legal duty

Importance of public perception of aviation safety

Why are accidents important? (2)

Detailed understanding of the factors that cause accidents:

- Prevent them
- Ensure maximum safety.

Needs two items:

- consensus on the definition of an accident
- realise how safety management has progressed from reactive towards preventive measures.

Reactive approach I

Initial approach to safety based on the forensic analysis of aircraft accidents:

- first fatal accident during a test flight in the US in 1908
- detailed investigation produced the first accident report

See: https://www.thoughtco.com/the-first-fatal-airplane-crash-1779178

Reactive approach II

Accident cause:

- accidental breaking of a propeller blade and
- consequential unavoidable loss of control resulting in a crash

Findings used to improve aircraft design through structural changes to the propellers.

Reactive approach III

Beginning of the application of a *reactive approach to safety*, i.e. identifying and fixing problems after they occur.

All safety critical industries such as aviation, chemical, oil or energy production take accidents very seriously and rapidly started to apply a reactive approach to safety.

Why reactive is not good enough

Whilst fulfilling legal responsibilities to investigate accidents:

- assumes their inevitability;
- need to improve safety through reliable solutions.

BUT

Waiting for an accident to happen!

Need to be proactive.

The proactive approach (1)

Assumes that interventions made at the level of incidents may prevent accidents:

- occurrences whose outcome is less severe than with accidents
- **safety triangle principle** which identifies a relationship between accident and incident and states that a larger of number of incidents occur before an accident happen,
- measures to reduce the number of incidents are considered as a safeguard against accidents.

The proactive approach (2)

Approach advocates:

- means for the reporting of incidents, and
- the collection and analysis of related information.
- reliant on an efficient incident reporting system that allows all occurrences perceived as “less safe” to be taken into consideration for the identification of safety problems.

What is needed to be proactive?

- Just culture in the organisation and
- Real desire to learn from identified mistakes without the fear of being systematically blamed for unintentional errors.

Reliability of reported information depends on how organisations:

- handle blame and punishment, and
- encourage –and even reward individuals– to provide essential safety-related information in an atmosphere of trust with no fear of punishment.

What is needed to be proactive? (1)

Analysis of the information contained in incident reports (i.e. “safety data”) usefully serves for identification of:

- hazards,
- variations,
- disruptions and
- degradations

of certain situations otherwise undetected because they do not lead systematically to consequences as obvious as with accidents.

Defences against potential safety problems and build resilience in the overall system.

The predictive approach (2)

Can we predict when and where the next safety problem in the system will arise?

- Correct all deficiencies in the system before they lead to any occurrences, including incidents

- Observe daily normal operations and efficiency of the existing safety barriers in the system and monitor

The predictive approach (3)

What type of safety data is needed for this?

- Not just accident and incident related
- Need to identify anything with the potential to impact safety, e.g. hazards, not seen before

The predictive approach (4)

When designing a new system:

- estimate the prediction of certain risks
- what can possibly go wrong,
- to which extent it can go wrong and
- likelihood of going wrong.

Predictive: hazards 1

- Hazard to a system (or system hazard) is an uncommon and/or unwanted state of the system during which the normal operative conditions of this system are affected.

- System hazard has the potential to:

  - jeopardise the safety of the system and

  - contribute to the development of an incident or in the worst case of an accident.

Predictive: hazards 2

- Hazard may be identified as precursor to an incident but may not always cause alone a safety occurrence.

- A power outage is a hazard to the Air Traffic Control (ATC) system, however if the affected ATC centre is equipped with an emergency power generator and applies appropriate recovery procedures, the ATC functions will be preserved together with the level of service, thus preventing safety occurrences.

Imperial College London

Belgian airspace outage 27 May 2015

http://uk.reuters.com/article/uk-belgium-traffic-airspace-idUKKBN0OC0S420150527

https://www.yahoo.com/news/belgian-airports-standstill-air-traffic-failure-092103852.html?ref=gs

Power failure

Euros 50 million

Aviation accidents

Hazard identification is part of the risk management process:

- proactive methods rely on a significant amount of incident data that are not easily handled and whose potential are not always fully exploited,

- predictive measures rely on an even larger amount of data, which makes it more advanced and also more difficult to achieved.

Accidents status

Currently:

- state-of-the-art safety methodologies are well-developed and implemented at the level of proactive approaches; but

- fewer provide risk prediction capabilities.

- reactive to proactive => accident to incident

Imperial College London

Accident approaches summary – Task

Approach	Safety Data	Attributes/ features
Reactive		
Proactive		
Predictive		

Hazard Probability

While the concepts of a hazard and its severity are straightforward in estimation of risk:

- Not true for **estimation of probability of a hazard**.
- Four major difficulties

Hazard Probability difficulties (1)

1. Tendency to assume the "*symmetry between the past and the future*", implies factors that:

   - existed at the time of an accident can always be found in retrospective analysis,

   - were present in an accident in the past will be present in the future as well, the mechanisms of accident propagation do not change over time;

2. Limited scientific validity of methods used for probability calculations;

Imperial College London

Hazard Probability difficulties (2)

3. Inability of calculations to account for "as done" operations of the system as opposed to "as imagined"; and

4. A number of biases including:

a) confirmatory bias (tendency to confirm the pre-conceived hypotheses on occurrence causation),

b) bias in predicting cumulative causes (tendency to assume the proportionality between the contributing factors but that seemingly small (irrelevant) factors can bring about severe consequences (i.e. the Butterfly effect)).

Imperial College London

What are the consequences?

Chernobyl, Challenger and Überlingen:

- probability of an accident was estimated to be **1E-09 or less**,

….BUT….. They happened!!!

What is an accident and an incident?

Confusion:

- Consensus about accident meaning within the safety community.
- Various industries use the same criteria that emphasise the damaging and observable outcome aspect.
- Ignores occurrences related to security aspects.

Imperial College London

Why do definitions matter?

- Critical to the establishment of official statistics to avoid potential misinterpretations.

- Benchmarking purposes - statistics about the number of accidents in the world.

- Definitions of the type of occurrences accounted for and the type of normalisation can lead to many different interpretations:

  - absolute number increasing while the rate decreasing considering the augmentation of operations.

ICAO Accident Definition

"an occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which a person is fatally or seriously injured; the aircraft sustains substantial damage or structural failure; or the aircraft is missing or is completely inaccessible"

Accident, the outcome translates into evident physical damage (or disappearance) to person(s) or infrastructure.

Imperial College London

What does the maritime industry say?

The UK's 2012 Merchant Shipping (Accident Reporting and Investigation) Regulations provides specific accident classifications.

Used by Maritime Accident Investigation Board.

Classifications resemble those established by:

- European Union – European Maritime Safety Agency
- International Maritime organisation – equivalent to ICAO

MAIB Definition of an accident

An event or sequence of events which has resulted in:

- the death or serious injury of an individual;
- loss of individual from a ship;
- loss or presumed loss of a vessel;
- material damage to a vessel;
- the stranding or disabling of the vessel,
- involvement of vessel in collision (with another vessel or external object);
- damage by a vessel to external marine infrastructure endangering safety of vessel or external individuals/vessels;
- pollution or potential of pollution caused by damage to vessel.

ICAO incident definition

- Criteria more vague

- Assumes that incidents are less severe than accidents.

Definition

"an occurrence, other than an accident, associated with the operation of an aircraft which affects or could affect the safety of operation".

ICAO incident defintion

Features:

- relatively ambiguous compare to the one of an accident,
- both unexpected and unforeseen; and result in unwanted outcome.
- characterisation of the outcome different.
- incident, the safety of the operations has been affected and jeopardised but no physical damages observed.

FRA accident/incident definition –US –(1)

"Accident/Incident" describe the entire list of reportable events. These include:

- collisions, derailments,
- and other events involving the operation of on-track equipment and causing reportable damage above an established threshold;
- impacts between railroad on-track equipment and highway users at crossings; and
- all other incidents or exposures that cause a fatality or injury to any person, or an occupational illness to a railroad employee.

FRA accident/incident definition –US – (2)

- **Train accidents**. A safety-related event involving on-track rail equipment (both standing and moving), causing monetary damage to the rail equipment and track above a prescribed amount. Reported on form FRA F 6180.54, (The threshold for 2008 is $8,500)
- **Highway-rail grade crossing incidents**. Any impact between a rail and highway user (both motor vehicles and other users of the crossing as a designated crossing site, including walkways, sidewalks, etc., associated with the crossing. Reported on form FRA F 6180.57
- **Other incidents**. any death, injury, or occupational illness of a railroad employee that is not the result of a "train accident' or "highway-rail incident." Reported on form FRA F 6180.55a

ERA accident/incident definition –Europe – (1)

Train accidents - an unwanted or unintended sudden event or a specific chain of such events which have harmful consequences divided into the following categories:

- collisions;
- derailments;
- level crossing accidents;
- accidents to persons involving rolling stock in motion;
- fires and others;

ERA accident/incident definition –Europe – (1)

'**serious accident**':

- any train collision or derailment of trains resulting in the death of at least one person or serious injuries to five or more persons or extensive damage to rolling stock, the infrastructure or the environment, and any other accident with the same consequences which has an obvious impact on railway safety regulation or the management of safety;

'extensive damage' means damage that can be immediately assessed by the investigating body to cost at least **EUR 2 million in total**;

ERA accident/incident definition –Europe – (2)

'**significant accident**':

- any accident involving at least one rail vehicle in motion, resulting in at least one killed or seriously injured person, or in significant damage to stock, track, other installations or environment, or extensive disruptions to traffic, excluding accidents in workshops, warehouses and depots;

'Significant damage' to stock, track, other installations or environment' means damage that is equivalent **to EUR 150 000 or more**;

ERA accident/incident definition –Europe – (3)

'**non-significant accident**': any accident involving at least one rail vehicle in motion, resulting in at least one minor injured person, or in any damage (**less than 150 000 EUR**) to stock, track, other installations or environment, or

- any disruptions to traffic (less than 6 hours), excluding accidents in workshops, warehouses and depots;

'Extensive disruptions to traffic' means that train services on a main railway line are suspended for six hours or more;

Question

Can we compare the railway accident rates in the USA and Europe?

Imperial College London

Contact details

Lloyd's Register Foundation
Transport Risk Management Centre

Imperial College
Centre for Transport Studies
South Kensington Campus
London SW7 2 AZ

Telephone: +44 (0)20 7594 6037
Email: a.majumdar@imperial.ac.uk

www.imperial.ac.uk/lrf-trmc