



| ICAO

UNITING AVIATION

SAFETY MANAGEMENT SYSTEM



Mohamed Chakib

Regional Officer, Safety Implementation,
International Civil Aviation Organization (ICAO), MID Office

SMS Aerodrome
Nov 2018, Cairo



ICAO

UNITING AVIATION

Safety Management-Aerodrome



Module 1: Hazard Identification



Introduction

Risk Management Principles

HAZARDS

Concept

Definitions

Coding

DETECTION

Types

Sources

Analysis

DOCUMENTATION

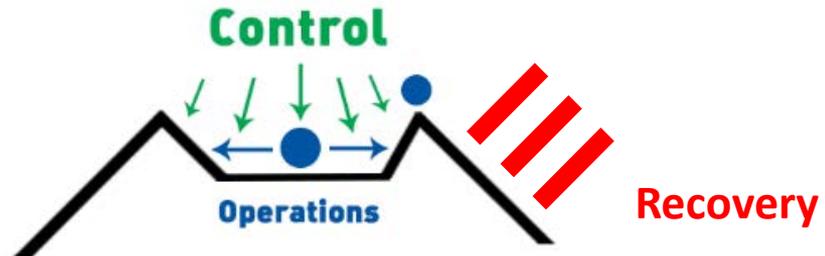
Hazard Register

CONCLUSIONS

How will stay in control with (nearly) no accident ?

Safety Barriers: We have to know them, to understand their role, to monitor Them, “to maintain them”

The questions are: How far they protect us?
How do we know? Can we improve?





What is Risk Management?



What is Risk Management?

- ❑ Safety Risk Management (SRM) is a key component of safety management and includes **hazard identification, safety risk assessment, safety risk mitigation and risk acceptance**.
- ❑ SRM is a **continuous activity** because the aviation system is constantly changing, new hazards can be introduced and some hazards and associated safety risks may change over time.
- ❑ In addition, the effectiveness of implemented safety risk mitigation strategies must be **monitored** to determine if further action is required



Safety Risk Management. What Is It? (Continued)

- ❑ A fundamental component of the Safety Management System (SMS). Risk Management serves to focus safety efforts on those hazards posing the greatest risks.
- ❑ Weighs the probability and severity implied by the risk against the expected gain of taking the risk.
- ❑ Facilitates the balancing act between assessed risks and viable risk mitigation.



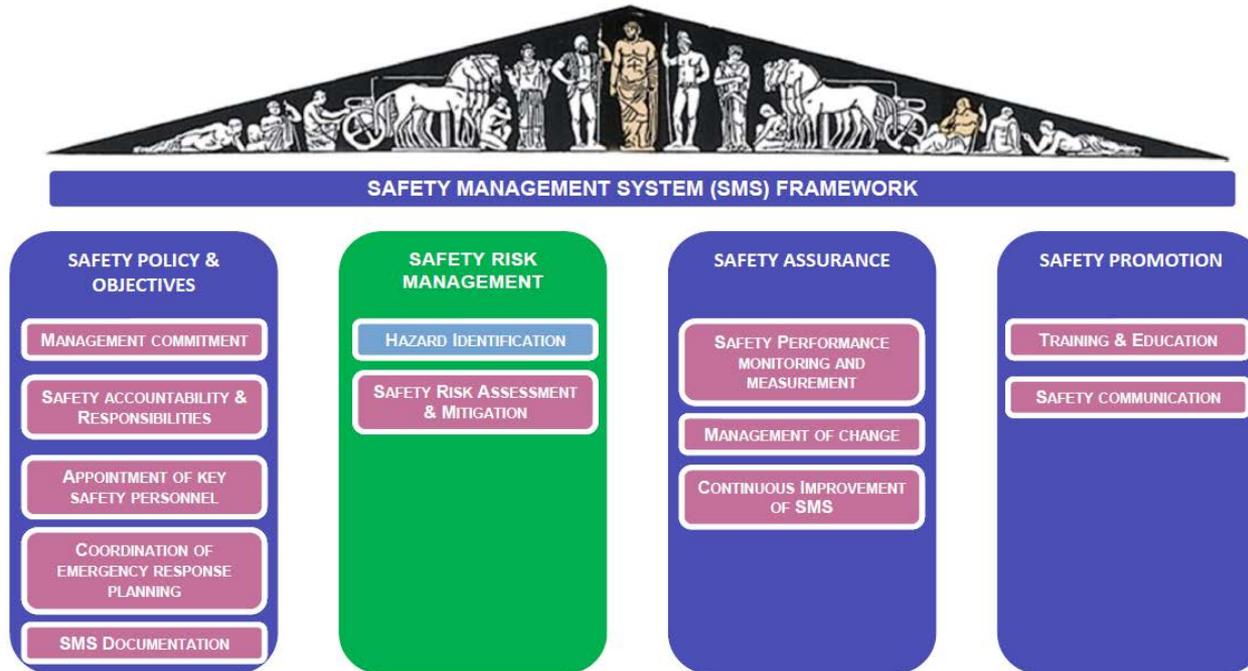
When to Use SRM

1. During initial system and task analysis.
2. For all proposed changes, like new or modified:
 - Systems
 - Procedures
 - Equipment
 - Environment
3. When new hazards are discovered during daily operations or Safety Assurance activities.

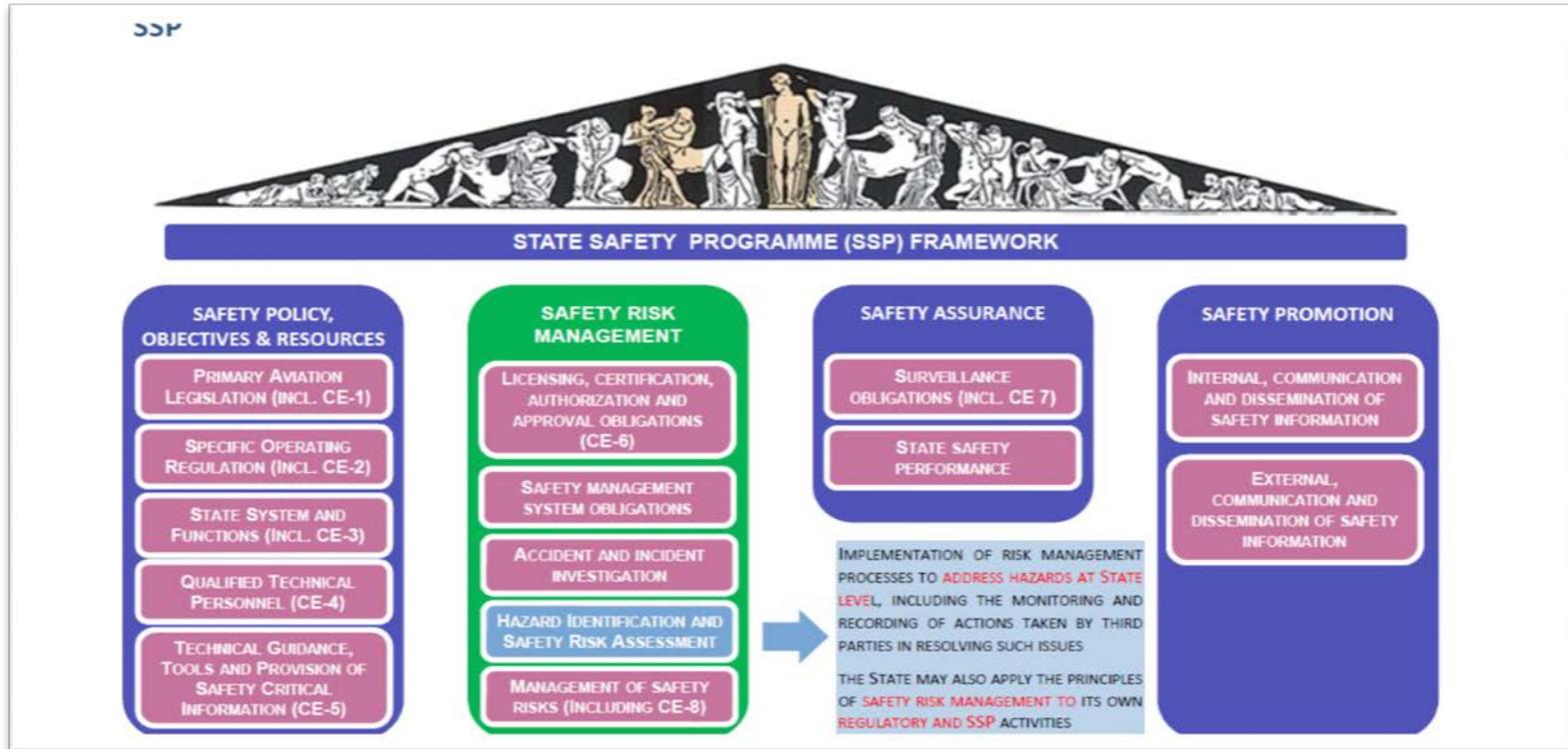


SMS Framework

SMS



SSP Framework



Risk Management Principles

- ❑ Every system is inherently safety **vulnerable**
- ❑ System vulnerabilities are described in terms of:
 - Hazards
 - Consequences
 - Risks
- ❑ Hazards are system components that can **lead to adverse consequences**
- ❑ **Safety risks** are **control** measurements



Risk Management Process



Probabilidad de eventos

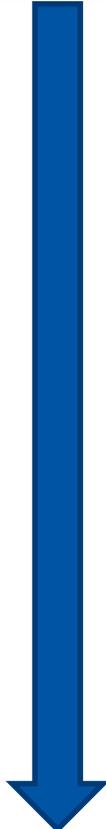
Definición	Ejemplo	Nivel
Preocupante	Reducción de la capacidad de respuesta de los recursos de mantenimiento	5
Grave	Ataque que causa algunas lesiones de carácter intermitente	4
Medio	Ataque que causa lesiones de carácter leve	3
Pequeño	Ataque que causa lesiones de carácter leve	2
Indefinido	Ataque que causa lesiones de carácter leve	1

Severidad del evento

Definición	Ejemplo	Nivel
Preocupante	Ataque que causa lesiones de carácter intermitente	4
Grave	Ataque que causa lesiones de carácter leve	3
Medio	Ataque que causa lesiones de carácter leve	2
Pequeño	Ataque que causa lesiones de carácter leve	1

Probabilidad de riesgo de seguridad operacional

	Preocupante	Grave	Medio	Pequeño	Indefinido
Preocupante	5A	5B	5C	5D	5E
Grave	4A	4B	4C	4D	4E
Medio	3A	3B	3C	3D	3E
Pequeño	2A	2B	2C	2D	2E
Indefinido	1A	1B	1C	1D	1E



Definitions

**System
Vulnerability**

Susceptibility of system to hazards as regards to its exposure, diminish capacity to resist and/or Recover from the effect of hazard

Consequence

Possible result derived from a hazard.
The hazard capability to produce damage
Is materliazed in one or various consequences

What is a Hazard?

- ❑ A **condition** or **an object** with the potential to cause or contribute to an aircraft incident or accident.
- ❑ In aviation, a hazard can be considered as **a dormant potential for harm** which is present in one form or another within the system or its environment. This potential for harm may appear in different forms, for example: as a natural condition (e.g. terrain) or technical status (e.g. runway markings)



Hazard Identification

- ❑ Hazard identification focuses on conditions or objects that could cause or contribute to the unsafe operation of aircraft or aviation safety-related equipment, products and services.
- ❑ A hazard may involve any situation or condition that has the potential to cause adverse consequences. The scope for hazards in aviation is wide.

Source: ICAO SMM Doc. 9859, 4th ED



Hazard identification and prioritization

- ❑ Hazards **exist at all levels in the organization** and are detectable through many sources including reporting systems, inspections, audits, brainstorming sessions and expert judgement.
- ❑ **The goal is to proactively identify hazards** before they lead to accidents, incidents or other safety-related occurrences.





Hazard identification and prioritization

The following should be considered when identifying hazards:

- **system description**;
- **design factors**, including equipment and task design;
- **human performance** limitations (e.g. physiological, psychological, physical and cognitive);
- **procedures and operating practices**, including documentation and checklists, and their validation under actual operating conditions;
- **communication factors**, including media, terminology and language;



Hazard identification and prioritization

The following should be considered when identifying hazards:

- **organizational factors**, such as those related to the recruitment, training and retention of personnel, compatibility of production and safety goals, allocation of resources, operating pressures and corporate safety culture;
- factors related to the **operational environment** (e.g. weather, ambient noise and vibration, temperature and lighting);



Hazard identification and prioritization

The following should be considered when identifying hazards:

- **regulatory oversight factors**, including the applicability and enforceability of regulations, and the certification of equipment, personnel and procedures;
- **performance monitoring systems** that can detect practical drift, operational deviations or a deterioration of product reliability;
- **human-machine** interface factors; and
- factors related to the **SSP/SMS interfaces** with other organizations.



Methods of Hazard Identification- Reactive

Mandatory Reporting Programs

1. This methodology involves analysis of **past outcomes or events**. Hazards are identified through investigation of safety occurrences. Incidents and accidents are an indication of system deficiencies and therefore can be used to determine which hazard(s) contributed to the event.
2. These reports and notifications must be reported to the Safety Manager as well for incorporation into the safety risk management process



Methods of Hazard Identification- Reactive

Voluntary Reporting Programs

1. Employees who work daily in the operational areas of the company are in the best position to be aware of hazards and incidents.
2. The Voluntary Reporting Program is a confidential program that protects the identity of the reporter.
3. The Voluntary Reporting Program is a non-punitive program that does not use the reported information to punish employees, but is instead focused upon developing process improvements to eliminate the identified hazards or control the risks associated with the report.



Methods of Hazard Identification- Proactive

Operational Data Analysis

1. This methodology involves collecting safety data of **lower consequence events or process** performance and analyzing the safety information or frequency of occurrence to determine if a hazard could lead to an accident or incident.
2. The safety information for proactive hazard identification primarily comes from flight data analysis (FDA) programmes, safety reporting systems and the safety assurance function.
3. These sources of operational data help to identify hazards.
4. Do trend analysis: data is monitored and analyzed for *trends* and other indications of inherent hazards.

Hazard Propagation

Hazard



A CONDITION OR OBJECT THAT COULD CAUSE OR CONTRIBUTE TO AN AIRCRAFT INCIDENT OR ACCIDENT

Unsafe Event



THE UNSAFE EVENT IS USUALLY NOT YET A CATASTROPHE, DISASTER OR ACTUAL DAMAGE

IT IS STILL POSSIBLE TO RECOVER FROM IT, AT LEAST TO SOME EXTENT

**Potential outcome/
ultimate
consequence(s)**



THE ULTIMATE CONSEQUENCE IS THE MOST CREDIBLE OUTCOME, ULTIMATE EVENT OR ACCIDENT (SMM)

IT IS USUALLY STATED IN TERMS OF "WORST CREDIBLE SCENARIO"

Hazard Propagation: Unsafe Event

The stage in the escalation of an accident scenario where the accident will occur, unless an active recovery measure is available and is successfully used.

(ref: ECAST guidance on hazard identification)



Hazard Propagation: Potential Outcome/Ultimate Consequences

Definitions:

- The most credible outcome, ultimate event or accident
- The degree of injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function arising from an Outcome. Consequence has a magnitude (ECAST guidance on hazard identification)



Hazard Propagation: Potential Outcome/Ultimate Consequences

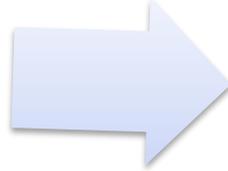
Recommendations:

- **Consequences** are what we ultimately want to prevent. They can be expressed generically as **losses, damages and/or injuries/fatalities** directly. although those descriptions are valid, their added value is limited.
- Instead we want to know how we got to that generic loss or damage. try to describe events based in type of accidents or serious incidents including scenario related details



Hazard Propagation- Example

Hazard



**Unsafe
Event**

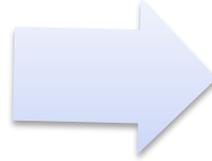


**Potential
outcome**



Hazard Propagation-Example

Hazard



**Unsafe
Event**



**Potential
outcome**





Definitions

- Commercial Aviation Safety Team (CAST)/International Civil Aviation Organization (ICAO) Common Taxonomy Team (CICTT): tasked with developing common taxonomies and definitions for aircraft accident and incident reporting systems.
- **ADREP**: an occurrence category taxonomy that is part of ICAO's accident and incident reporting system. It is a compilation of attributes and the related values that allow safety trend analysis on these categories.

Hazard Coding:

The generic component allows users to capture the nature of a hazard with a view to aid in identification, analysis, and coding.

GENERIC TERM

+

SPECIFIC TERM

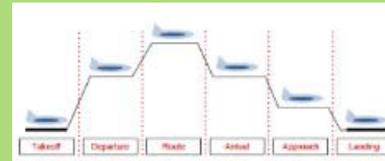
HAZARD TAXONOMY



PRECISE DEFINITION



CONTEXT





GENERIC TERM: HAZARD TAXONOMY (CICCT)

ENVIRONMENTAL (ENV)	SEVERE WEATHER OR CLIMATIC EVENTS (HURRICANES, TYPHOONS, ETC.) ADVERSE WEATHER (FOG, ICE, LOW VISIBILITY, ETC.) GEOGRAPHICAL EVENTS (VOLCANOS, EARTHQUAKES, ETC.) GEOGRAPHY (TERRAIN, ALTITUDES, ETC.) NATURAL EVENTS (WILDLIFE, FIRES, ETC.) PUBLIC HEALTH (EPIDEMICS, ETC.)
TECHNICAL (TECH)	AIRCRAFT (EJ: SYSTEMS, SUBSYSTEMS, COMPONENTS & ASSOCIATED EQUIPMENT) ORGANIZATIONAL FACILITIES (EJ: TOOLS, HANGARS, WORKSHOPS, ETC.) EXTERNAL FACILITIES (FACILITIES AND SYSTEMS EXTERNAL TO THE OPERATION) PHYSICAL ERGONOMICS (HUMAN CHARACTERISTICS ASSOCIATED TO THE PHYSICAL ACTIVITIES OF THE OPERATION)
ORGANIZATIONAL (ORG)	ECONOMICS (GROWTH/RECESSION) OPERATIONAL POLICIES & PROCEDURES MATERIALS/EQUIPMENT ACQUISITION ORGANIZATIONAL CULTURE
HUMAN (HUM)	MEDICAL PSYCHOLOGICAL COGNITIVE PHYSICAL LIMITATION

GENERIC TERM: HAZARD TAXONOMY (CICTT)

ENVIRONMENTAL (ENV)

Hazards existing as a consequence of the habitat or environment within which operations related to the provision of services take place.

The environmental hazards category includes the following subcategories:

- Severe weather or climatic events: Factors related to hurricanes, winter storms, droughts, tornadoes, thunderstorms, lightning, and wind shear.
- Adverse weather conditions: Factors related to icing, freezing precipitation, heavy rain, snow, winds, extreme temperatures, and restrictions to visibility.
- Geographical events: Factors relating to earthquakes, volcanoes, tsunamis, floods, and landslides.
- Geography: Factors relating to mountainous terrain, aerodrome altitude, aerodrome terrain, and large bodies of water such as oceans.
- Natural events: Factors related to wildfires, wildlife activity, and insect or pest infestations.
- Public health events: Factors related to epidemics of influenza or other diseases.

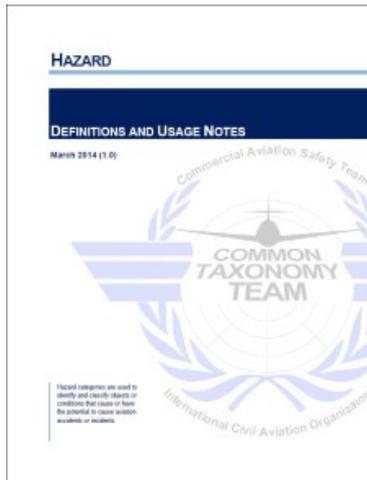
Usage note:

- This category is used to describe factors of the environment that will have an effect on aviation operations. It needs to be described within an aviation context. For example, snow might not be a hazard on its own, but it becomes a hazard with potential consequences in an aerodrome operational context.
- The quantity is an important consideration for environmental events or conditions to become a hazard. A light wind could be advantageous to the operation; however a strong crosswind is a hazard for a landing aircraft.
- In order to add detail to the hazard description, a hazard within a subcategory may be further described in a third level code as a specific component of the hazard.

Definition

Categories

Usage note



SPECIFIC TERM: PRECISE DEFINITION

A WELL DEFINED HAZARD:

- NEEDS TO BE **CLEARLY IDENTIFIABLE**
- SHOULD BE DESCRIBED IN THE DESIRED **(CONTROLLED) STATE**
- **COMMONLY** ACCEPTED **TERMINOLOGY** SHOULD BE USED
- **NO JUDGMENTAL** ADJECTIVES (E.G., POOR, DEFICIENT) SHOULD BE USED **NOR NEGATIVE** MEANINGS OR DESCRIPTIONS OF ABSENCE (E.G., POOR...)

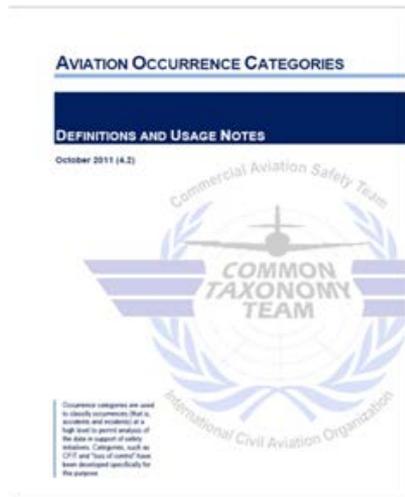


Hazard to be linked to a context to enable further processes and better understanding

Ultimate consequences/potential outcome: ADREP occurrence categories

Recommendation:

To classify operational consequences in terms of ADREP Aviation occurrence category



CONTROLLED FLIGHT INTO OR TOWARD TERRAIN (CFIT)

Inflight collision or near collision with terrain, water, or obstacle without indication of loss of control.

Usage Notes:

- CFIT is used only for occurrences during airborne phases of flight.
- CFIT includes collisions with those objects extending above the surface (for example, towers, trees, power lines, cable car support, transport wires, power cables, telephone lines and aerial masts).
- CFIT can occur during either Instrument Meteorological Conditions (IMC) or Visual Meteorological Conditions (VMC).
- Includes instances when the cockpit crew is affected by visual illusions or degraded visual environment (e.g., black hole approaches and helicopter operations in brownout or whiteout conditions) that result in the aircraft being flown under control into terrain, water, or obstacles.
- If control of the aircraft is lost (induced by crew, weather or equipment failure), do not use this category; use Loss of Control – Inflight (LOC-I) instead.
- For an occurrence involving intentional low altitude operations (e.g., crop dusting, aerial work operations close to obstacles, and Search and Rescue (SAR) operations close to water or ground surface) use the Low Altitude Operations (LALT) code instead of CFIT.
- Do not use this category for occurrences involving intentional flight into/toward terrain. Code all collisions with obstacles during take-off and landing under TOL. Code all suicides under Security Related (SEC) events.
- Do not use this category for occurrences involving runway undershoot/overshoot, which are classified as Undershoot/Overshoot (USOS).
- Includes flying into terrain during transition into forward flight.
- For helicopter operations, not to be used for take-off and landing phases, except when the occurrence involves flying into terrain without indication of loss of control during transition into forward flight.



CFIT



LOC-I



MAC RI

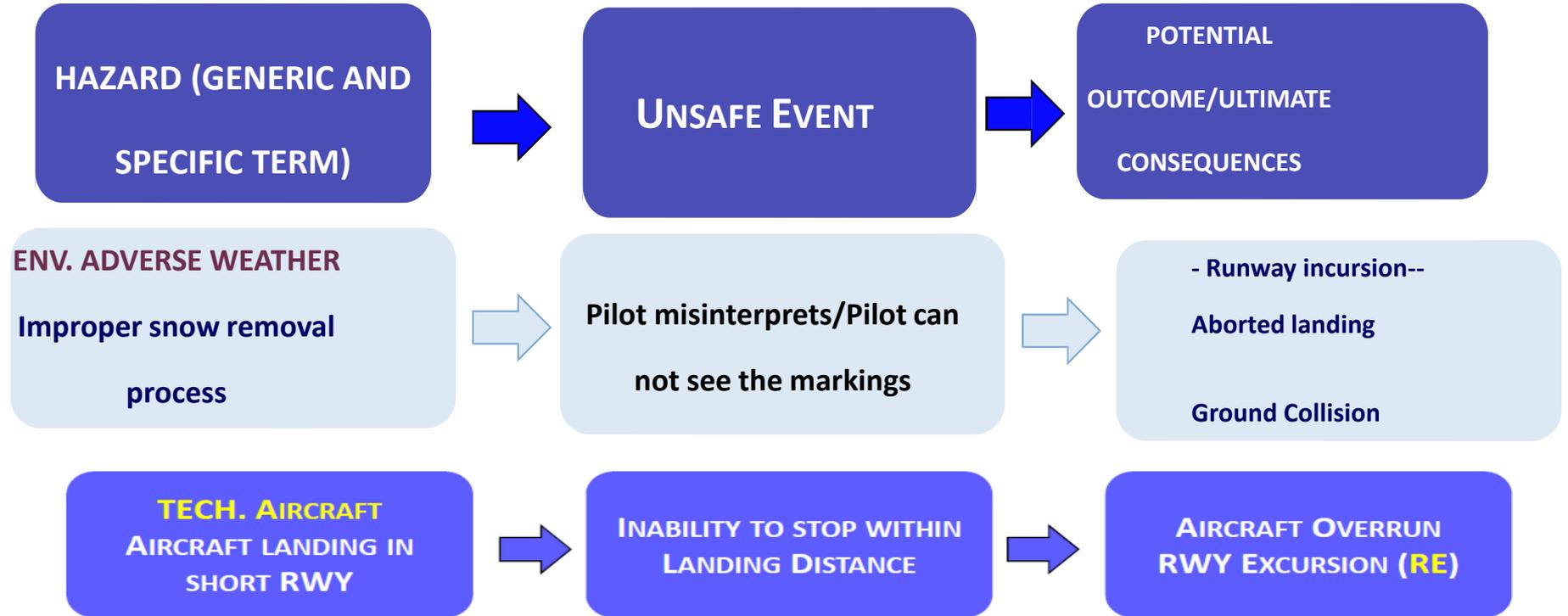


RE



RAMP

Hazard propagation: Aviation examples



Hazard Capture

WHERE FROM?



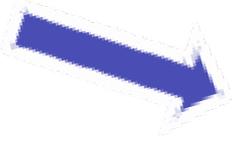
INTERNAL

- PROCEDURES
- REPORTING SYSTEMS
 - FDM
 - AUDITS
- SAFETY STUDIES
- SURVEYS



EXTERNAL

- ACCIDENT REPORTS
- EXTERNAL REPORTING SYSTEMS
- OTHER



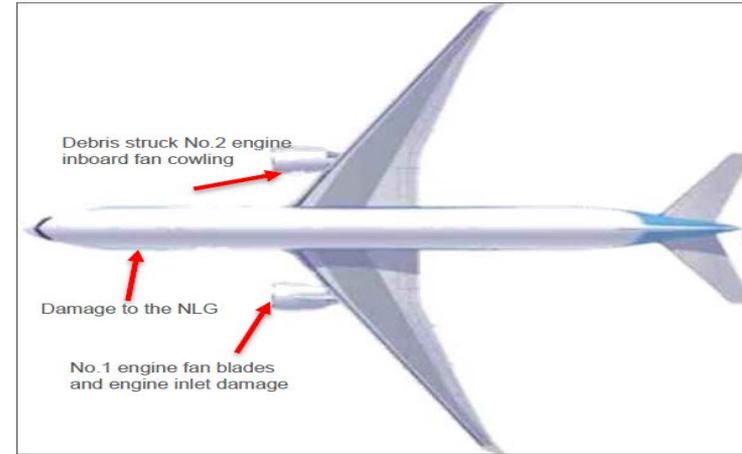
WHEN?

- ROUTINE DATA CAPTURE
- SYSTEM CHANGE PLANS
- **REVIEW OF CURRENT OPERATIONS AND PROCESSES**



Accident Case

- ❑ During take-off, shortly after rotation, crew heard a loud bang with associated #1 Engine EGT, followed by left engine failure. The #1 engine auto shut down and continued take-off.
- ❑ The flight crew then declared an emergency and cleared for landing. As the aircraft was over weighted, the rollout after landing was prolonged causing high brakes temperature.
- ❑ Consequently resulted in the aircraft MLG thermal fuses melted due to the high brakes temperature, and all of the MLG tires deflated.



It was concluded that:

The shedding of the No.1 nose wheel tire tread occurred as a result of **tire contacting FOD**. Subsequently the damaged tire debris was **ingested by the #1 engine causing engine failure**





Some Hazard Identification and Analysis Tools used by airports

Observation and reporting

Anyone working at the airport or using airport facilities should be able to report hazards that they see. The process can be more effective when airport staff has received training on how to identify and report hazards, and a system or tool is available for reporting, like a hotline or intranet based reporting system.

Daily Inspection

Daily inspections are effective in identifying airside hazards. The procedure can be more effective if inspectors have received training to identify types of hazards.

Functional brainstorming

It consists of gathering a group of people to discuss the issue and identify hazards. A facilitator will make the process more effective.

Trend Analysis

Monitoring of safety performance indicators and statistics improves SRM by identifying undesirable trends associated with certain hazards like birdstrikes, runway incursions, and injuries to personnel.



Some Hazard Identification and Analysis Tools used by airports

❑ SRM triggers

Some common safety issues and hazardous situations can signal the need to put the SRM process in action, or the need to convene a formal SRA.

❑ Accident and incident investigation

A thorough investigation can discover the causes and contributing factors, particularly those hazards that are not obvious (for example deficient training), and investigation reports can communicate the identified hazards to airport decision makers for SRM action.

❑ Audits

Safety and SMS audits are effective tools to identify hazards that are not obvious. Hidden hazards can include outdated training, organizational issues, deficient operational processes and procedures.



Some Hazard Identification and Analysis Tools

❑ **Comparative Safety Assessment (CSA)**

- Systematic assessment technique used to support decision-making by assessing and comparing the safety risk of selected alternatives

❑ **Preliminary Hazard List (PHL)**

- Hazard identification tool that provides an initial overview of the potential hazards in the overall flow of the operation

❑ **Preliminary Hazard Analysis (PHA)**

- Initial effort in risk assessment of the selected system

❑ **Operations Analysis Tool**

- Provides an itemized sequence of events or a flow diagram depicting the major events of an operation

❑ **“What If” Process Tool**

- Identifies hazards by visualizing them
- Asks “what if various failures occurred or problems arose?”
- Designed to capture the expertise of personnel involved in planning or executing an operation in a structured manner

Hazards identification methodology

STRUCTURED WHAT-IF TECHNIQUE (SWIFT)

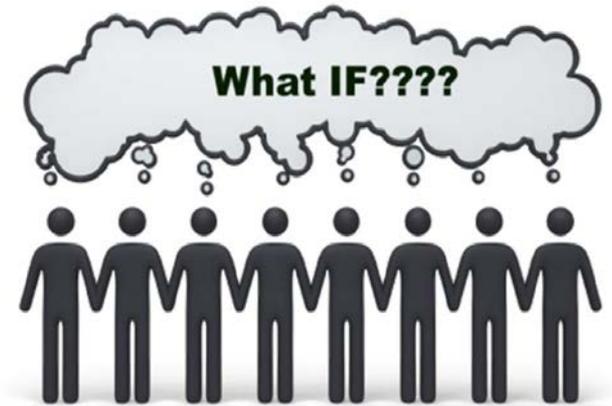


- SWIFT is a facilitated brainstorming group activity It involves a team of experts guided by a facilitator
- Typically carried out on a higher level system description
- A reduced set of prompts is used to initiate discussion

Hazards are recorded for further treatment

LIST OF PROMPTS (EXAMPLE)

- WHAT IF...?
- COULD SOMEONE...?
- HAS ANYONE EVER...?



Template for What-If hazard analysis-Example

System Failure	What if? (1)	Answer (2)	Likelihood (3)	Severity (4)	Control Actions (5)
Fueling equip.	Mechanical failure adrift nozzle during fueling	Fuel may spray out between mating faces	Improbable	Minor	Use of locking mechanism Inspection and maintenance Fueling adapter on aircraft designed to prevent back flow
Human error	Faulty gauge system or human error leads to overfill of aircraft tanks	Fuel spills from surge tank vent on the aircraft wing onto the ramp	Remote	Major (large quantity of fuel spill)	Auto shutoff fueling valves Overfill protection with fuel sensors in surge tank
Aircraft equipment failure	Aircraft brakes are not applied nor chocks are used and aircraft moves	Hose may get ruptured	Improbable	Major	Operator should detect aircraft movement Release dead man's control to stop fuel transfer Chock aircraft

Hazard Log/Register

Documentation

- ✓ A centralized hazard register may be a useful tool that ensures harmonization and avoids duplication.
- ✓ the format may vary from a simple hazard list to a database relating hazards and mitigations and responsibilities

As a minimum, a hazard register should contain:

- Hazard identification and description
- Risk assessment
- Potential consequences
- Risk controls description (mitigations)
- Allocation of responsibilities for mitigations and Associated deadlines
- Other





HAZARD LOG/Register (#1)

IDENTIFIED HAZARD	CONSEQUENCE	EXISTING MITIGATION	RISK	FURTHER MITIGATION MEASURES	REVISED RISK	ACTIONS (BY AND WHEN)
			<i>SEVERITY</i> <i>LIKELIHOOD</i> <i>TOLERABILITY</i>		<i>SEVERITY</i> <i>LIKELIHOOD</i> <i>TOLERABILITY</i>	

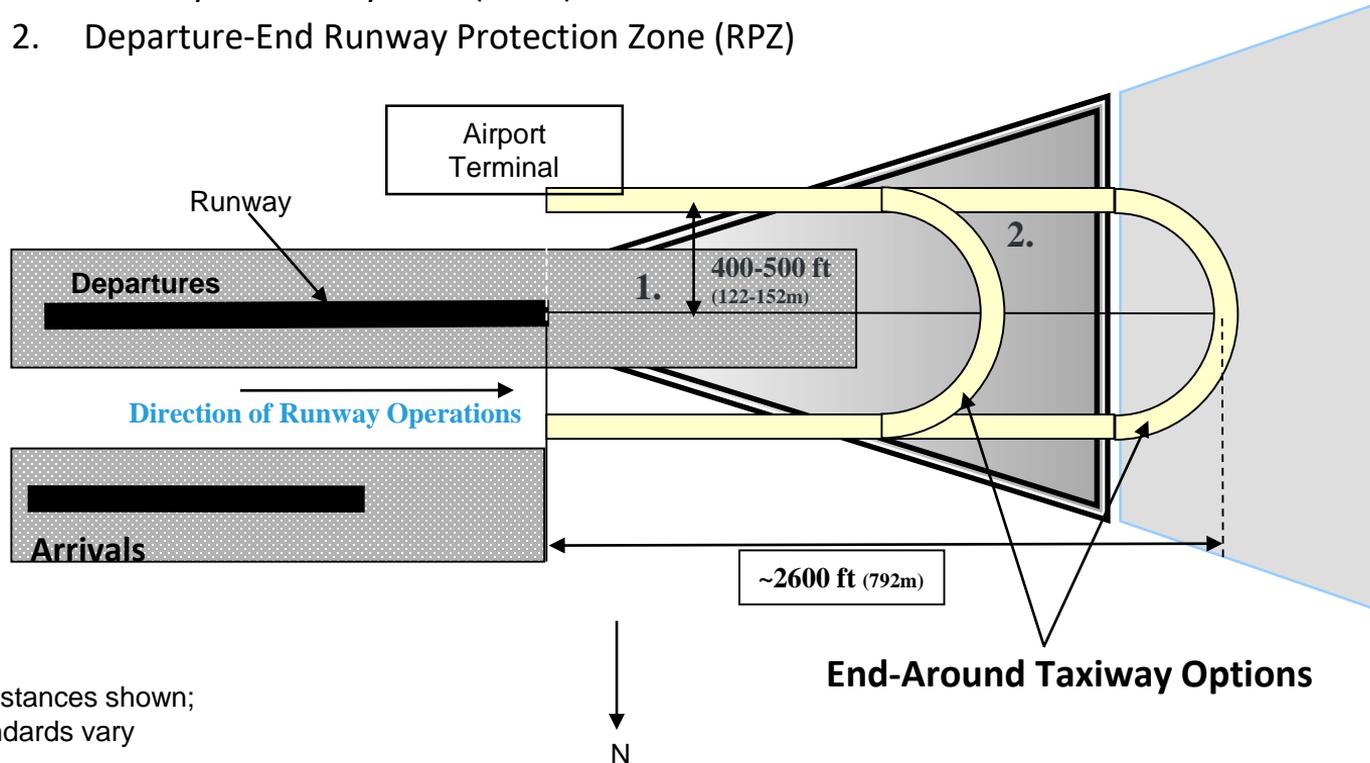


HAZARD LOG/Register (#2)

OPERATION/SYSTEM	HAZARD Nº	HAZARD TAXONOMY		UNSAFE EVENT	POTENTIAL OUTCOME / ULTIMATE CONSEQUENCE	
		GENERIC COMPONENT	SPECIFIC COMPONENT			

Example

-  1. Runway End Safety Area (RESA)
-  2. Departure-End Runway Protection Zone (RPZ)



Nominal distances shown;
actual standards vary

Example: Hazards identification in current operations

GENERIC TERM



ENV: weather conditions exist that can affect braking system during take-off

Tech: aircraft equipment failure during take-off

Hum: Human Error

SPECIFIC TERM



DESCRIPTION
+ CONTEXT

Departure aircraft aborts take-off resulting in rwy overrun going beyond the RESA,

Unsafe Event



Conflict between aircraft taking off and aircraft taxiing on the EAT

Potential outcome



- High severity of RI on the EAT
- Collision with other aircraft on the EAT



Example: Hazards identification in current operations

OPERATION/SYSTEM	HAZARD N°	HAZARD TAXONOMY		UNSAFE EVENT	POTENTIAL OUTCOME / ULTIMATE CONSEQUENCE	
		GENERIC COMPONENT	SPECIFIC COMPONENT			
Take-off	1	Environment Technical Human error	Departure aircraft aborts take-off resulting in rwy overrun beyond the RESA,	Conflict between aircraft taking off and aircraft taxiing on the EAT	<ul style="list-style-type: none">High severity of RI on the EATCollision with other aircraft on the EAT	Aircraft / equipment heavy damages and fatalities



Key Points to Remember

- Hazards are normal system components, and their consequences are usually manageable
- When the hazard is released, control is lost and the system may propagate into an adverse outcome
- Hazards should be categorized into a generic component (in accordance with a standard taxonomy) and a specific component (description)
- Hazards can be captured from data sources including current processes and future changes



ICAO | UNITING AVIATION

