

# Safety Risk Management Training



# Importante

---

El contenido en este curso es de propiedad de Air Learning Center.

Se prohíbe la reproducción total o parcial de este material sin el consentimiento de sus autores.

Las fuentes de información, imágenes y datos utilizados en el presente documento han sido citados según aplique.

# Acuerdos

---

- Idioma de la presentación: Ingles
- Uso de celular (en silencio)
- Breaks (15 min cada 2 horas)
- Preguntas: Abiertas puede realizar interrupciones levantando la mano o preguntas al final de cada tema.
- Evaluación: El curso va a ser evaluado, 70% es la nota mínima para aprobar el curso.
- Metodología: Presencial

# ¿Para qué vine a este curso?

---

Al finalizar el curso, el participante contara con las habilidades y las herramientas para identificar, evaluar y mitigar los riesgos de manera efectiva, asegurando el bienestar de las personas y el éxito de su organización.



# Conociendo al instructor

---

## Manuel Muñoz

- Ingeniero Aeronáutico con Maestría en Mantenimiento y producción de aeronaves y Maestría en Administración de Empresas (M.B.A.) especialista de más de 10 años trabajando en áreas de seguridad operacional, especialista en confiabilidad técnica y aeronavegabilidad continuada.



# Conozcámonos

---

Breve presentación del instructor y de los participantes.

Uno a uno respondamos estas preguntas que ayudarán a conocernos mejor:

- Nombre Completo
- Profesión y/o ocupación
- ¿Cuáles son sus responsabilidades principales?
- Sus expectativas precisas (¿Que espera del curso?)



# ¿Cuál es el contenido del curso?

---

- Introduction to Safety Risk Management
- Hazard Identification
- Risk Assessment and Analysis
- Risk Control Measures
- Incident Investigation and Analysis
- Safety Performance Monitoring and Improvement
- Case Studies and Best Practices

# ¿Cuál es el contenido del curso?

---

- **Introduction to Safety Risk Management**
- Hazard Identification
- Risk Assessment and Analysis
- Risk Control Measures
- Incident Investigation and Analysis
- Safety Performance Monitoring and Improvement
- Case Studies and Best Practices

# Introduction to Safety Risk Management

---

Risk management is a formalized way of dealing with hazards. It is a logical process of evaluation where you weigh the potential costs of a risk against the potential benefits you might receive, if you allowed that risk to stand uncontrolled.

In order to better understand risk management, the terms “hazard” and “risk” need to be understood

# Definition of Safety Risk Management

---

The definition of safety risk management is the systematic process of identifying, assessing, controlling, and monitoring risks to prevent incidents, accidents, injuries, and damage to people, property, and the environment. It involves the application of policies, procedures, and practices to minimize the potential negative impact of hazards and risks within an organization.

# Definition of Safety Risk Management

---

Here are some key reasons why it is crucial:

1. **Prevention of Incidents and Injuries:** Safety risk management focuses on identifying potential hazards and taking proactive measures to eliminate or control them. By implementing effective risk management practices, organizations can prevent accidents, injuries, and other negative consequences, safeguarding the well-being of employees, contractors, visitors, and the public.
2. **Legal and Regulatory Compliance:** Compliance with safety laws, regulations, and standards is a fundamental requirement for organizations. Safety risk management helps ensure that an organization meets the legal obligations related to safety. Failure to comply can lead to legal consequences, penalties, fines, and damage to the organization's reputation.

# Definition of Safety Risk Management

---

3. **Protection of Assets and Resources:** Implementing robust risk management practices helps protect valuable assets, including infrastructure, equipment, materials, and intellectual property. By identifying and managing risks effectively, organizations can minimize financial losses due to damage, theft, or operational disruptions.
4. **Reputation and Brand Protection:** Organizations that prioritize safety risk management demonstrate their commitment to the well-being of their employees and stakeholders. A strong safety record enhances the organization's reputation and brand image, attracting customers, investors, and business partners. Conversely, incidents or accidents resulting from inadequate risk management can cause reputational damage and lead to loss of trust.



# Definition of Safety Risk Management

---

5. **Cost Reduction:** Effective safety risk management can lead to cost savings in various ways. By preventing accidents and injuries, organizations avoid expenses related to medical treatment, compensation claims, and property damage repairs. Additionally, a proactive approach to risk management can reduce insurance premiums and improve overall operational efficiency.
6. **Increased Employee Morale and Productivity:** When employees feel safe and supported in the workplace, their morale and productivity tend to increase. By implementing safety risk management measures, organizations create a positive work environment that fosters employee well-being, job satisfaction, and engagement.

# Definition of Safety Risk Management

---

7. Compliance with Stakeholder Expectations: Customers, employees, shareholders, and other stakeholders increasingly expect organizations to prioritize safety and responsible risk management. By meeting these expectations, organizations can enhance stakeholder satisfaction and maintain long-term relationships.
8. Continuity of Operations: Managing safety risks ensures the continuity of business operations. By identifying and addressing potential risks, organizations can minimize disruptions caused by incidents, accidents, or other safety-related issues. This leads to uninterrupted production, service delivery, and customer satisfaction.

In summary, safety risk management is essential for organizations to protect their people, assets, and reputation, while ensuring legal compliance and achieving operational excellence. By implementing effective risk management practices, organizations can create a safer work environment, prevent incidents, and ultimately achieve sustainable success.

# Basic Principles and Objectives of Safety Risk Management

---

1. **Prevention:** The primary objective of safety risk management is to prevent incidents, accidents, and harm to people, property, and the environment. The focus is on identifying and addressing potential hazards and risks before they result in negative consequences.
2. **Hazard Recognition and Evaluation:** Safety risk management involves systematically identifying and evaluating hazards in the workplace. This includes assessing the severity and likelihood of each hazard to determine its level of risk.
3. **Risk Assessment and Analysis:** Risk assessment involves analyzing and quantifying risks based on the likelihood and consequences of potential incidents. This process helps prioritize risks, allocate resources effectively, and make informed decisions about risk control measures.

# Basic Principles and Objectives of Safety Risk Management

---

4. Hierarchy of Controls: Safety risk management follows the hierarchy of controls, which prioritizes risk controls in the following order: elimination, substitution, engineering controls, administrative controls, and personal protective equipment. The objective is to implement the most effective control measures that eliminate or minimize risks.
5. Continuous Improvement: Safety risk management aims to foster a culture of continuous improvement. This involves regularly reviewing and updating risk assessments, control measures, and safety processes based on new information, lessons learned from incidents, and evolving best practices.

# Basic Principles and Objectives of Safety Risk Management

---

6. **Employee Involvement:** Engaging employees at all levels is crucial in safety risk management. Encouraging their active participation, involvement in hazard identification, risk assessments, and decision-making helps improve the effectiveness of risk management efforts.
7. **Compliance with Laws and Standards:** Safety risk management ensures compliance with relevant laws, regulations, and industry standards. Adhering to legal requirements and industry guidelines helps establish a minimum level of safety and mitigates the potential for legal and financial repercussions.

# Basic Principles and Objectives of Safety Risk Management

---

8. Communication and Training: Effective communication and training are essential in safety risk management. Clear and timely communication of hazards, risks, control measures, and procedures ensures that everyone involved understands their roles, responsibilities, and the necessary safety protocols.
9. Integration with Business Operations: Safety risk management should be integrated into all aspects of business operations. It should align with the organization's goals, policies, and procedures to ensure that safety is an integral part of decision-making and day-to-day activities.

# Basic Principles and Objectives of Safety Risk Management

---

10. Performance Monitoring and Evaluation: Regular monitoring and evaluation of safety performance help assess the effectiveness of risk management strategies, identify trends, and make data-driven decisions. This includes analyzing incident data, conducting safety audits, and measuring key performance indicators.

# Relevant Laws, regulations and standards

---

- International Civil Aviation Organization (ICAO) Standards and Recommended Practices: ICAO sets global standards and recommended practices for aviation safety through its Annexes to the Convention on International Civil Aviation. Annex 19, titled "Safety Management," provides the framework for safety management systems (SMS) implementation and safety risk management in aviation. **(SMM Doc 9859)**
- Federal Aviation Administration (FAA) Regulations (United States): In the United States, the FAA is the regulatory authority for civil aviation. The FAA regulations, particularly Title 14 of the Code of Federal Regulations (14 CFR), cover various aspects of aviation safety risk management, including safety management systems, risk assessments, safety reporting, and safety oversight. **(Risk Management Handbook (FAA-H-8083-2A))**



# Relevant Laws, regulations and standards

---

- European Union Aviation Safety Agency (EASA) Regulations: EASA is the regulatory agency responsible for aviation safety in the European Union. The agency establishes regulations, such as the European Union Aviation Safety Management System (EU-ASMS) regulation, which outlines the requirements for implementing safety management systems and conducting safety risk assessments.
- Aircraft Accident Investigation Authorities: Each country has its own authority responsible for investigating aircraft accidents and incidents. These authorities, such as the National Transportation Safety Board (NTSB) in the United States or the Air Accidents Investigation Branch (AAIB) in the United Kingdom, play a crucial role in identifying safety risks, conducting investigations, and making recommendations to improve aviation safety.

# Relevant Laws, regulations and standards

---

- International Air Transport Association (IATA) Standards and Guidance: IATA develops standards, recommended practices, and guidance material for the airline industry. These resources address various aspects of safety risk management, including safety management systems, risk assessments, incident reporting, and auditing.
- International Organization for Standardization (ISO): ISO plays an important role in facilitating world trade by providing common standards among different countries. These standards are intended to ensure that products and services are safe, reliable, and of good quality. **ISO 31000** provides direction on how companies can integrate risk-based decision making into an organization's governance, planning, management, reporting, policies, values and culture.

# Relevant Laws, regulations and standards

---

- Airline Operations Manuals: Airlines develop their own operations manuals, including safety management system manuals, which outline their specific safety risk management procedures and processes. These manuals align with regulatory requirements and industry best practices, ensuring a consistent approach to safety risk management within the airline.

# ¿Cuál es el contenido del curso?

---

- Introduction to Safety Risk Management
- **Hazard Identification**
- Risk Assessment and Analysis
- Risk Control Measures
- Incident Investigation and Analysis
- Safety Performance Monitoring and Improvement
- Case Studies and Best Practices

# Hazard Identification

---

Understanding the difference between hazards and risks is crucial in safety risk management. Here's the differentiation between the two concepts:

- Hazard: A hazard refers to any potential source, situation, or act that has the potential to cause harm, damage, or adverse effects to people, property, or the environment. Hazards can be physical, chemical, biological, ergonomic, or psychosocial in nature.
- 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

---

Understanding the difference between hazards and risks is crucial in safety risk management. Here's the differentiation between the two concepts:

- Risk: Risk is the likelihood or probability that a particular hazard will actually cause harm or adverse consequences, taking into account both the severity of the potential harm and the likelihood of its occurrence. It involves the assessment of the potential for loss, injury, or damage resulting from exposure to a hazard. Risk is often expressed as a **combination of the severity of the harm and the probability of its occurrence.**

# Hazard Identification

---

Here are some examples of hazards and associated risks:

1. Hazard: Bird Strikes

Risk: The risk of a bird colliding with an aircraft during takeoff, landing, or in flight, which can damage the aircraft's structure or engines, potentially leading to loss of control or engine failure.

2. Hazard: Runway Incursions

Risk: The risk of an unauthorized aircraft, vehicle, or person entering an active runway without proper clearance, posing a collision risk with landing or departing aircraft.

# Hazard Identification

---

## 3. Hazard: Fire Hazards

Risk: The risk of fires breaking out in the aircraft cabin, cargo compartments, or engine areas, which can jeopardize the safety of passengers, crew, and the aircraft itself.

## 4. Hazard: Pilot Fatigue

Risk: The risk of flight crew members experiencing fatigue due to long duty hours, inadequate rest periods, or circadian rhythm disruptions, which can impair their performance and decision-making abilities, increasing the likelihood of errors or accidents.



# Hazard Identification

---

## 5. Hazard: Weather Conditions

Risk: The risk of adverse weather conditions, such as thunderstorms, icing, or low visibility, which can affect aircraft performance, disrupt communication and navigation systems, and increase the probability of incidents or accidents.

## 6. Hazard: Maintenance Errors

Risk: The risk of errors or oversights during aircraft maintenance and inspections, including failure to identify or repair equipment malfunctions or structural issues, which can compromise the safety and airworthiness of the aircraft.

# Methods for identifying hazards

---

- 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.



# Methods for identifying hazards

---

- 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.



# Methods for identifying hazards

---

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;

# Methods for identifying hazards

---

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);

# Methods for identifying hazards

---

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
- Factors related to the **SSP/SMS interfaces** with other organizations.

# Methods for identifying hazards

---

## 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 for identifying hazards

---

## Methods of Hazard Identification- Proactive / Predictive

- **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. Safety / Quality Audits and Inspections
3. Industry Data and trends



# Methods for identifying hazards

---

## **Methods of Hazard Identification- Proactive / Predictive**

- **Operational Data Analysis**

4. The safety information for predictive hazard identification primarily comes from flight data analysis (FDA) programs.
5. These sources of operational data help to identify hazards.
6. Do trend analysis: data is monitored and analyzed for trends and other indications of inherent hazards.

# Methods for identifying hazards

## WHERE FROM?

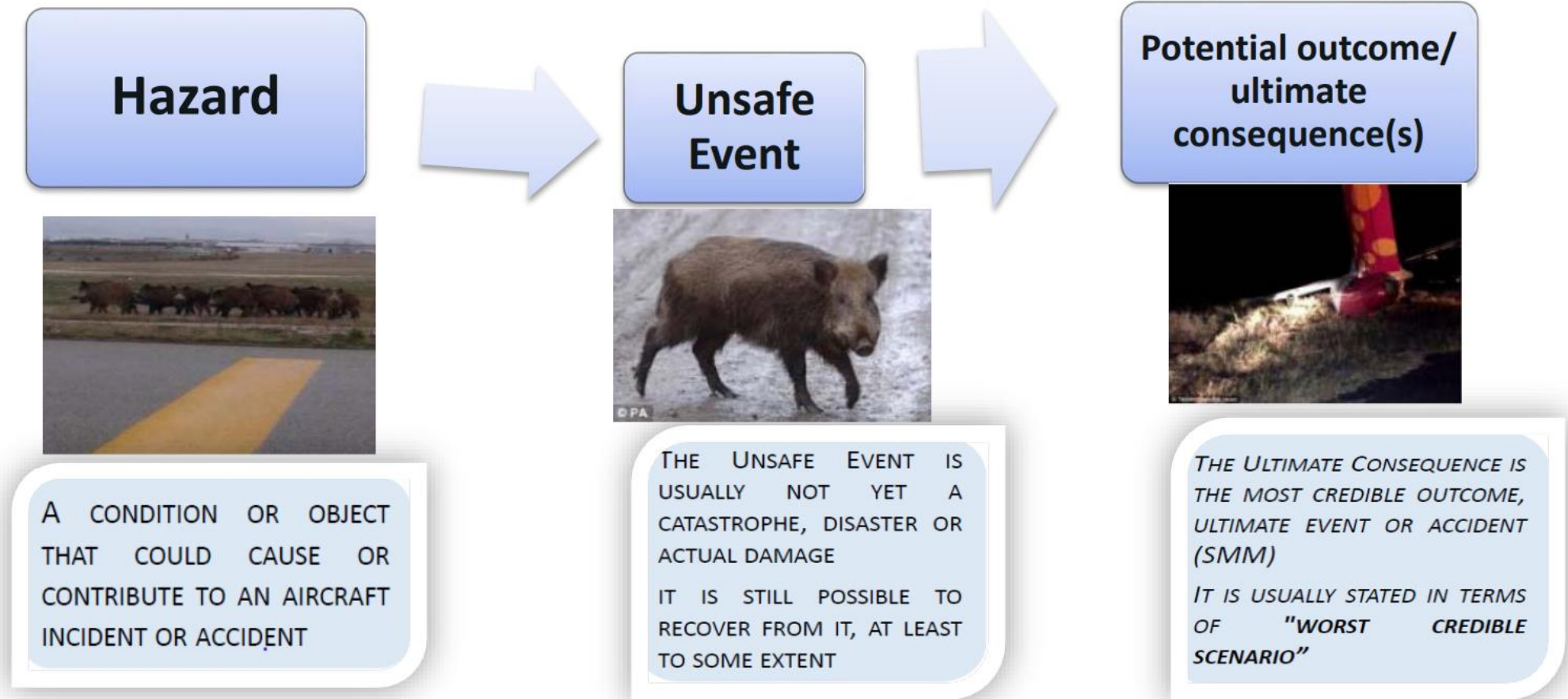


## WHEN?

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



# Hazard Propagation



# Hazard Propagation

---

## 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



# Hazard Propagation





# Hazard Propagation

---



# Hazard Identification and Analysis Tools

---

- Comparative Safety Assessment (CSA)
  - Process used to compare and evaluate the safety performance of different systems, technologies, designs, or operational procedures. It involves a systematic and objective analysis of safety characteristics and risks associated with each option being considered.
- 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)
  - Process used in safety engineering and risk management to identify and assess potential hazards associated with a system, product, or project during the early stages of development. The goal of a PHA is to identify hazards that could lead to accidents, injuries, damage, or other adverse effects and to initiate the risk management process.

# Hazard Identification and Analysis Tools

---

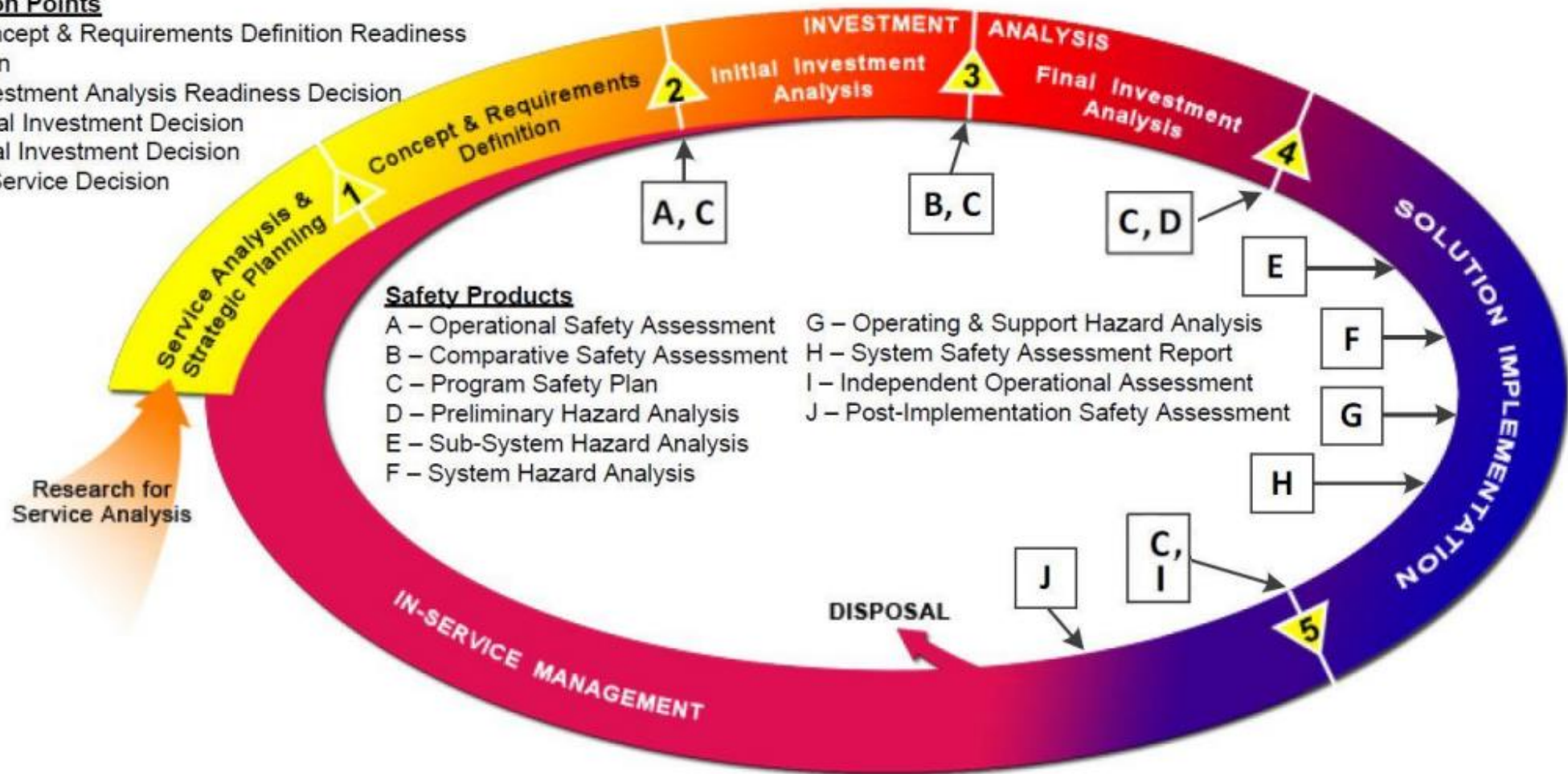
- Operations Analysis Tool
  - Provides an itemized sequence of events or a flow diagram depicting the major events of an operation
- “What If” Process Tool
  - Identifies hazards by visualizing them
  - Asks “what if various failures occurred or problems arose?”
  - Designed to capture the expertise of personnel involved in planning or executing an operation in a structured manner



# Hazard Identification and Analysis Tools

## Decision Points

- 1 – Concept & Requirements Definition Readiness Decision
- 2 – Investment Analysis Readiness Decision
- 3 – Initial Investment Decision
- 4 – Final Investment Decision
- 5 – In-Service Decision



# Assessing the severity and likelihood of identified hazards

---

Assessing the severity and likelihood of identified hazards is an essential step in risk management and helps prioritize the hazards based on their potential impact and likelihood of occurrence.

## 1. Severity Assessment:

- a) Consequences: Evaluate the potential consequences or impacts that could result from the occurrence of the hazard. This may include injuries, fatalities, property damage, environmental damage, financial losses, operational disruptions, or reputational harm.
- b) Magnitude: Assess the magnitude or severity of the consequences on a predefined scale, such as minor, moderate, major, or catastrophic. This scale should align with the specific context and objectives of the risk assessment.

# Assessing the severity and likelihood of identified hazards

---

Assessing the severity and likelihood of identified hazards is an essential step in risk management and helps prioritize the hazards based on their potential impact and likelihood of occurrence.

## 1. Severity Assessment:

- c) Potential Chain of Events: Consider the potential escalation or chain of events that could result from the hazard. Evaluate the potential for cascading effects or the exacerbation of consequences.

## 2. Likelihood Assessment:

- a) Probability: Assess the likelihood or probability of the hazard occurring within a given timeframe. This assessment may be qualitative (low, medium, high) or quantitative (probability values, percentages).

# Assessing the severity and likelihood of identified hazards

---

Assessing the severity and likelihood of identified hazards is an essential step in risk management and helps prioritize the hazards based on their potential impact and likelihood of occurrence.

## 2. Likelihood Assessment:

- b) Frequency: Consider the frequency of exposure to the hazard, such as the number of times or duration that individuals or assets are exposed to the hazard over a specific period.
- c) Historical Data: Draw on historical data, incident records, near-miss reports, or industry statistics to inform the likelihood assessment. Analyzing past occurrences of similar hazards can provide insights into their likelihood of occurrence.

# Assessing the severity and likelihood of identified hazards

---

Assessing the severity and likelihood of identified hazards is an essential step in risk management and helps prioritize the hazards based on their potential impact and likelihood of occurrence.

## 3. Expert Judgment and Stakeholder Inputs:

- a) Engage subject matter experts, stakeholders, and individuals with relevant knowledge to provide their expert judgment and inputs on the severity and likelihood assessments. Their expertise and perspectives can enhance the accuracy and reliability of the assessments.
- b) Consensus Building: Foster a collaborative environment where stakeholders can discuss and share their insights. Seek consensus on the severity and likelihood assessments, considering different viewpoints and experiences.

# Assessing the severity and likelihood of identified hazards

---

Assessing the severity and likelihood of identified hazards is an essential step in risk management and helps prioritize the hazards based on their potential impact and likelihood of occurrence.

## 4. Risk Matrix or Scoring:

- a) Use a risk matrix or scoring system to combine the severity and likelihood assessments and generate an overall risk rating for each hazard. A risk matrix typically categorizes risks into levels, such as low, medium, and high, based on their combination of severity and likelihood.

## 5. Documentation and Communication:

- a) Document the severity and likelihood assessments for each identified hazard, along with the rationale and supporting information. This documentation serves as a reference and supports decision-making processes.

# Assessing the severity and likelihood of identified hazards

---

Assessing the severity and likelihood of identified hazards is an essential step in risk management and helps prioritize the hazards based on their potential impact and likelihood of occurrence.

## 5. Documentation and Communication:

- b) Communicate the results to relevant stakeholders, management, or decision-makers. Clearly convey the significance of each hazard based on its assessed severity and likelihood, helping prioritize risk mitigation efforts.

Remember that severity and likelihood assessments are subjective and depend on available information, expertise, and the specific context of the risk assessment. Regular review and update of assessments are crucial as new information becomes available or as conditions change.

# ¿Cuál es el contenido del curso?

---

- Introduction to Safety Risk Management
- Hazard Identification
- **Risk Assessment and Analysis**
- Risk Control Measures
- Incident Investigation and Analysis
- Safety Performance Monitoring and Improvement
- Case Studies and Best Practices



# Risk Assessment and Analysis

---

Risk assessment techniques can be classified into three broad categories: qualitative, semi-quantitative, and quantitative. These techniques differ in the level of numerical analysis and data utilization involved in the assessment process

- Qualitative Risk Assessment:
- Semi-Quantitative Risk Assessment:
- Quantitative Risk Assessment:

# Risk Assessment and Analysis - Qualitative Risk Assessment

---

**Qualitative risk assessment** is a subjective approach that focuses on understanding and evaluating risks based on their characteristics without assigning specific numerical values. It relies on expert judgment, experience, and qualitative scales or categories to assess and prioritize risks.

# Risk Assessment and Analysis - Semi-Quantitative Risk Assessment:

---

**Semi-quantitative risk assessment** combines qualitative and quantitative elements to assess risks. It assigns numerical values to certain aspects of the risk assessment, such as likelihood and consequences, while still using qualitative scales for other components.

# Risk Assessment and Analysis - Quantitative Risk Assessment

---

**Quantitative risk assessment** involves a rigorous and data-driven analysis of risks using mathematical models, probabilistic techniques, and numerical data. It quantifies risks by assigning specific numerical values to likelihood, consequences, and other relevant factors.

# Risk Assessment and Analysis

TECHNIQUE	KEY FEATURES	ADVANTAGES	LIMITATIONS
QUALITATIVE RISK ASSESSMENT	<ul style="list-style-type: none"><li>• Subjective assessment based on expert opinions and knowledge.</li><li>• Uses qualitative scales or categories to describe and rank risks (e.g., low, medium, high).</li><li>• Relies on qualitative descriptors of likelihood and consequences.</li><li>• Typically involves risk matrices or risk-ranking approaches.</li></ul>	<ul style="list-style-type: none"><li>• Requires minimal data and quantitative analysis.</li><li>• Can be conducted quickly and with limited resources.</li><li>• Allows for a broad understanding of risks and easy communication of results.</li></ul>	<ul style="list-style-type: none"><li>• Subjective nature may introduce bias and inconsistency.<ul style="list-style-type: none"><li>• Lacks precise numerical values for risk comparison and decision-making.</li></ul></li><li>• Limited ability to perform detailed risk comparisons or cost-benefit analyses.</li></ul>

# Risk Assessment and Analysis

TECHNIQUE	KEY FEATURES	ADVANTAGES	LIMITATIONS
SEMI-QUANTITATIVE RISK ASSESSMENT	<ul style="list-style-type: none"><li>• Combines qualitative and quantitative elements.</li><li>• Assigns numerical values to certain risk aspects (e.g., likelihood or consequence scales).</li><li>• Uses qualitative descriptors for other risk aspects.</li><li>• Can incorporate risk matrices or scoring systems.</li></ul>	<ul style="list-style-type: none"><li>• Provides a more structured and consistent assessment compared to qualitative methods.</li><li>• Allows for limited numerical analysis and comparison of risks.</li><li>• Enables a more detailed understanding of risk profiles.</li></ul>	<ul style="list-style-type: none"><li>• Still relies on subjective assessments and qualitative descriptors.</li><li>• Limited precision and accuracy compared to fully quantitative methods.</li><li>• May require more effort and data than qualitative methods</li></ul>

# Risk Assessment and Analysis

TECHNIQUE	KEY FEATURES	ADVANTAGES	LIMITATIONS
QUANTITATIVE RISK ASSESSMENT	<ul style="list-style-type: none"><li>Utilizes mathematical models, data analysis, and statistical techniques.</li><li>Assigns specific numerical values to likelihood, consequences, and other risk factors.</li><li>Uses probabilistic analysis to estimate risks and their uncertainties.</li><li>Allows for detailed scenario analysis and simulations.</li></ul>	<ul style="list-style-type: none"><li>Provides precise and quantitative risk estimates.</li><li>Enables rigorous comparison and analysis of risks.</li><li>Facilitates more informed decision-making and resource allocation.</li></ul>	<ul style="list-style-type: none"><li>Requires extensive data collection and analysis.</li><li>Can be time-consuming and resource-intensive.<ul style="list-style-type: none"><li>Relies on assumptions and models that may introduce uncertainties.</li></ul></li></ul>

# Risk Assessment and Analysis

---

The choice of risk assessment technique depends on various factors, including the complexity of the system, the availability of data, the resources and expertise available, and the specific objectives of the risk assessment. Organizations may use a combination of techniques, starting with qualitative or semi-quantitative assessments and transitioning to quantitative methods as more data and resources become available or as the need for more detailed analysis arises.



# Risk Assessment and Analysis

---

TECHNIQUE	EXAMPLES OF USAGE
QUALITATIVE RISK ASSESSMENT	<ul style="list-style-type: none"><li>• Safety</li><li>• Project Risk Management</li></ul>
SEMI-QUANTITATIVE RISK ASSESSMENT	<ul style="list-style-type: none"><li>• Safety</li><li>• Environmental Risk Analysis</li><li>• IT Security Risk Assessment</li></ul>
QUANTITATIVE RISK ASSESSMENT	<ul style="list-style-type: none"><li>• Safety</li><li>• Financial Risk Management</li><li>• Process Safety Analysis</li></ul>

# Risk Assessment and Analysis - Methodologies

---

## **BOWTIE**

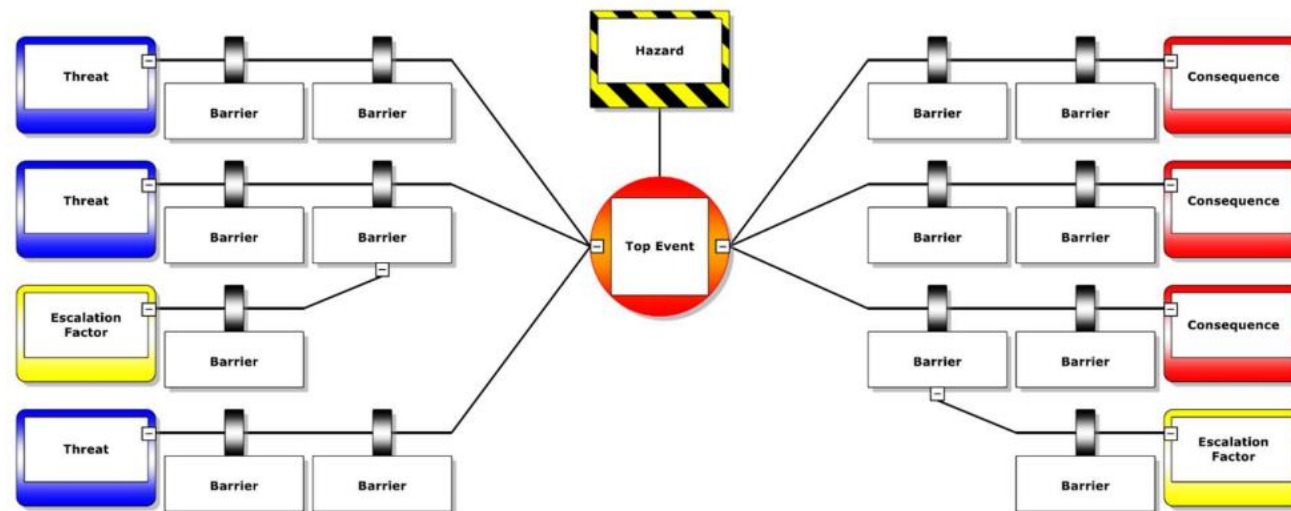
The bowtie methodology is used for risk assessment, risk management and (very important) risk communication. The method is designed to give a better overview of the situation in which certain risks are present; to help people understand the relationship between the risks and organizational events. The strength of the methodology lies in its simplicity

Bowtie analysis is a risk management technique that combines qualitative and semi-quantitative approaches to visualize and analyze risks and their control measures.

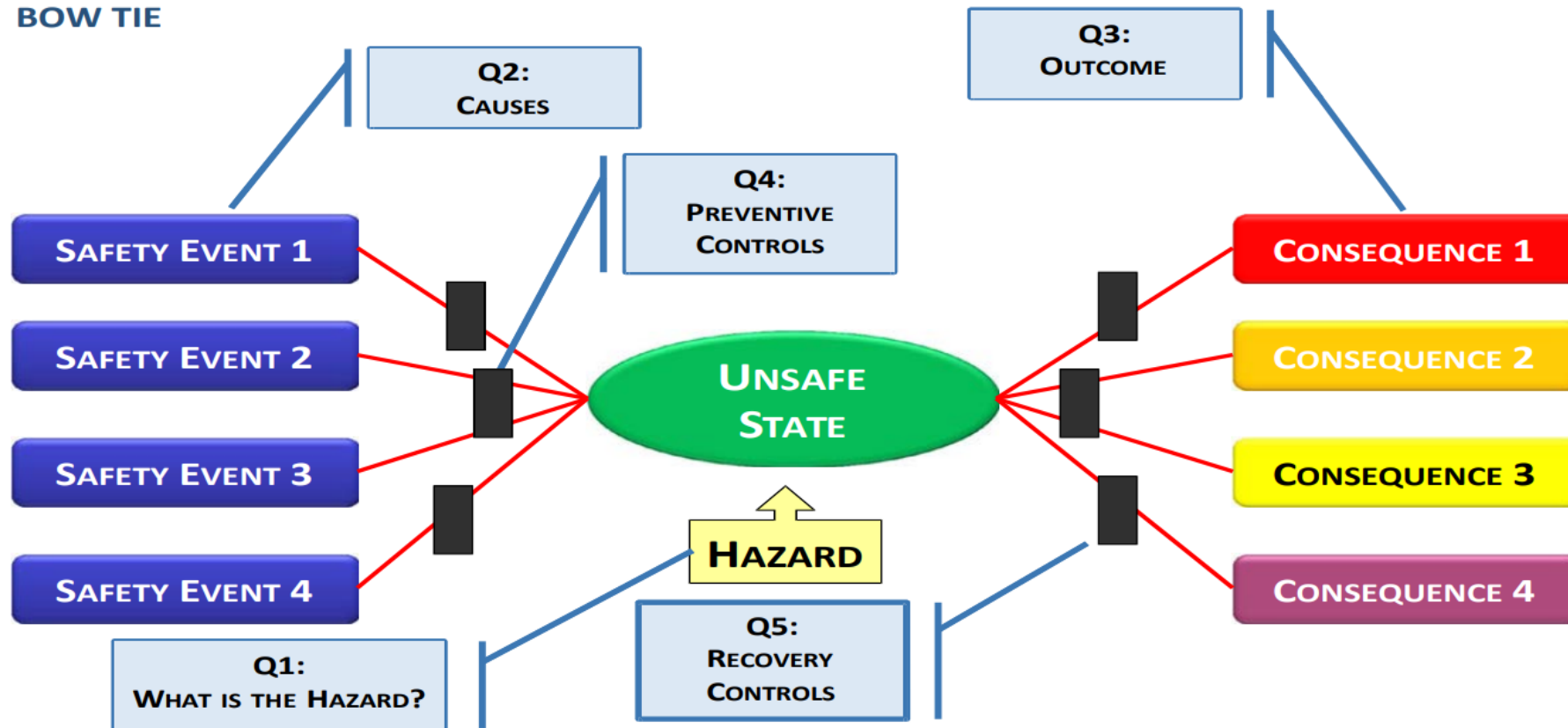
# Risk Assessment and Analysis - Methodologies

## BOWTIE

The Bowtie analysis method involves creating a diagram that resembles a bowtie, hence the name. The diagram visually represents the causal relationships between hazards, potential consequences, and the preventive and mitigative barriers (control measures) in place to manage those risks.



# Risk Assessment and Analysis - Methodologies



# Risk Assessment and Analysis - Methodologies

---

## **BOWTIE**

While Bowtie analysis incorporates qualitative elements such as identifying hazards, consequences, and barriers, it also allows for a semi-quantitative assessment of the effectiveness of barriers and the likelihood of occurrence. This is typically done by assigning qualitative scales or values (such as low, medium, high) to the likelihood and effectiveness of barriers, rather than precise numerical values.

# Risk Assessment and Analysis - Methodologies

---

## **OPERATIONAL RISK ASSESSMENT (ORA / ARMS)**

Operational Risk Management consists of three elements: Hazard Identification, Risk Assessment and Risk mitigation. The main objective of Risk Management is to make sure that all risks remain at an acceptable level.

The objective for Operational Risk Assessment (ORA) is the Assessment of operational risks in a systematic, robust and intellectually cohesive manner. Operational Risk Assessment is needed in three different contexts:

# Risk Assessment and Analysis - Methodologies

## OPERATIONAL RISK ASSESSMENT (ORA)

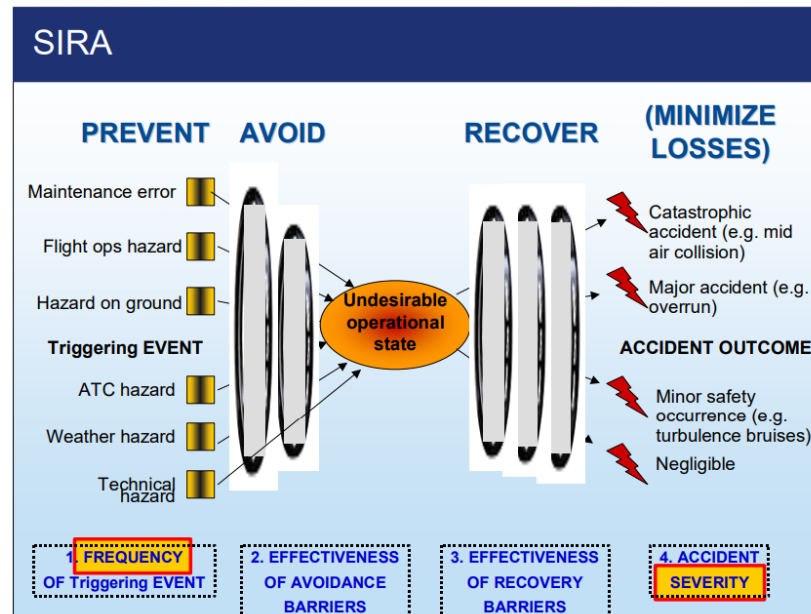
1. Individual safety Events may reflect a high level of risk and consequently require urgent action. Therefore, all incoming events need to be risk assessed. This step is called Event Risk Classification (ERC).

Question 2 What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?				Question 1 If this event had escalated into an accident outcome, what would have been the most credible outcome?		Typical accident scenarios
Effective	Limited	Minimal	Not effective			
50	102	502	2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	
10	21	101	500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	
2	4	20	100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	
1				No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)
						Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
						High speed taxiway collision, major turbulence injuries
						Pushback accident, minor weather damage

# Risk Assessment and Analysis - Methodologies

## OPERATIONAL RISK ASSESSMENT (ORA)

2. The Hazard Identification process may lead to the identification of Safety Issues, which need to be risk assessed to determine what actions, if any are needed. This step is called Safety Issue Risk Assessment (SIRA).





# Risk Assessment and Analysis - Methodologies

---

## **OPERATIONAL RISK ASSESSMENT (ORA)**

3. From time to time there will be a need to carry out Safety Assessments, typically related to a new or revised operational activity (e.g. new destination). The activity needs to be risk assessed at the planning stage, according to the “Management of Change” process of the company.

# Risk Assessment and Analysis - Methodologies

---

## **SYSTEM-THEORETIC ACCIDENT MODEL AND PROCESSES – STAMP**

STAMP focuses particular attention on the role of constraints in safety management. Instead of defining safety in terms of preventing component failure events, it is defined as a continuous control task to impose the constraints necessary to limit system behavior to safe changes and adaptations.

Accidents are seen as resulting from inadequate control or enforcement of constraints on safety-related behavior at each level of the system development and system operations control structures.

# Risk Assessment and Analysis - Methodologies

---

## **SYSTEM-THEORETIC ACCIDENT MODEL AND PROCESSES – STAMP**

Accidents can be understood, therefore, in terms of why the controls that were in place did not prevent or detect maladaptive changes, that is, by identifying the safety constraints that were violated at each level of the control structure as well as why the constraints were inadequate or, if they were potentially adequate, why the system was unable to exert appropriate control over their enforcement.

STAMP also overcomes the other limitations of event chain models. System accidents arising from the interaction among components and not just component failure accidents are easily handled.

# Risk Assessment and Analysis - Methodologies

---

## **System-Theoretic Process Analysis – STPA**

STPA (System-Theoretic Process Analysis) is a relatively new hazard analysis technique based on an extended model of accident causation. In addition to component failures, STPA assumes that accidents can also be caused by unsafe interactions of system components, none of which may have failed.

# Risk Assessment and Analysis - Methodologies

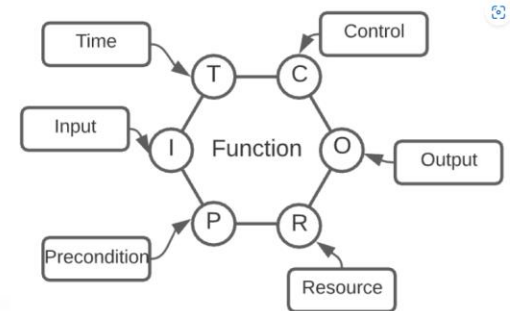
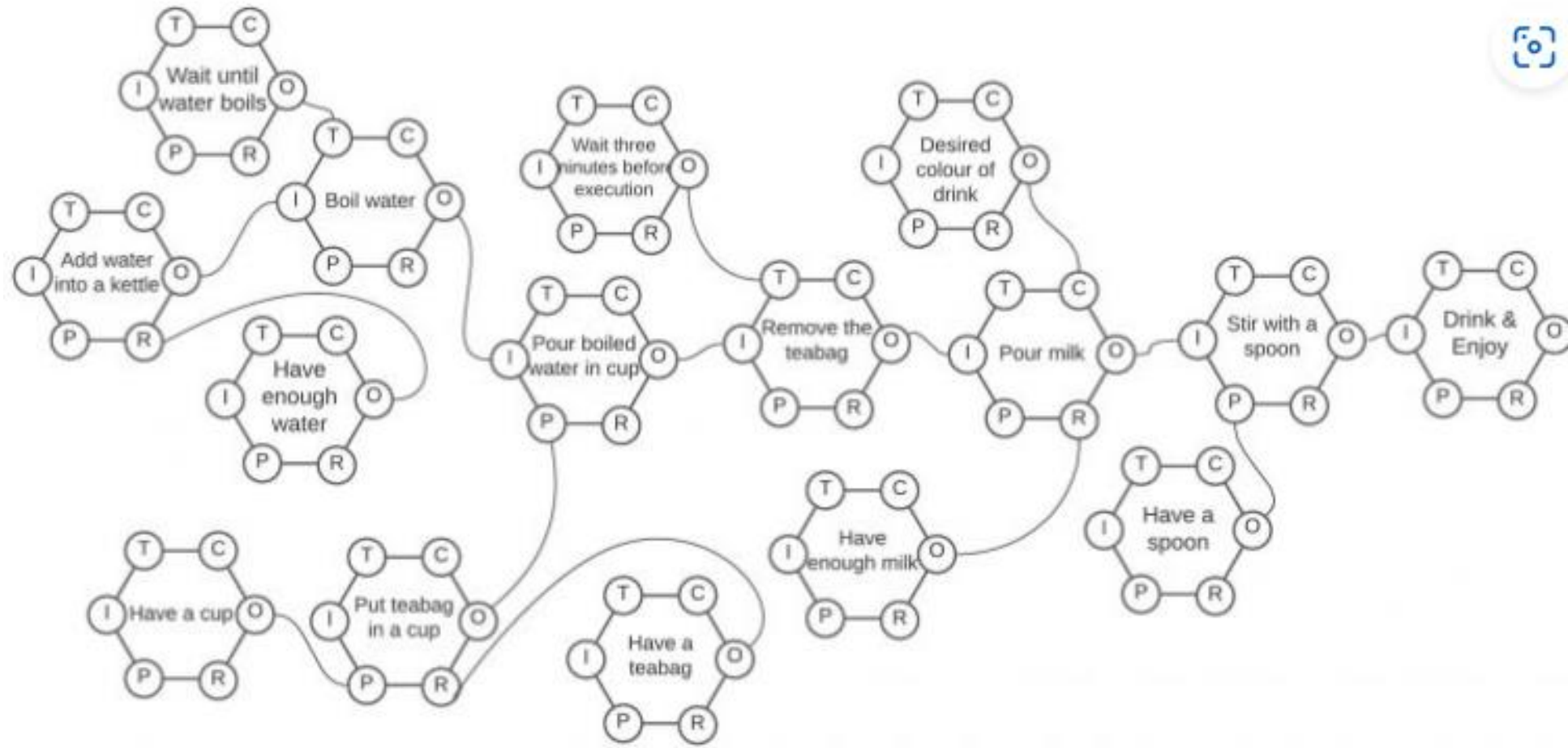
---

## **FRAM – FUNCTIONAL RESONANCE ANALYSIS METHOD**

THE FRAM is a method to analyze how work activities take place either retrospectively or prospectively. This is done by analyzing work activities in order to produce a model or representation of how work is done. This model can then be used for specific types of analysis, whether to determine how something went wrong, to look for possible bottlenecks or hazards, to check the feasibility of proposed solutions or interventions, or simply to understand how an activity (or a service) takes place.

The FRAM is a method for modelling non-trivial socio-technical systems. It is NOT a risk assessment method, and it is not an accident analysis method. Neither is a FRAM model a flow model, a network model, or a graph. But the model produced by a FRAM analysis can serve as the basis for a risk analysis, an event investigation, or for something entirely different.

# Risk Assessment and Analysis - Methodologies



# Risk Assessment and Analysis - Methodologies

---

## **FRAM – FUNCTIONAL RESONANCE ANALYSIS METHOD**

Step 1: Identifying essential system functions and characterizing each function by six basic parameters.

Step 2: Characterizing the (context dependent) potential variability through common performance conditions. Eleven common performance conditions (CPCs) are identified in the FRAM method to be used to elicit the potential variability:

- 1) availability of personnel and equipment
- 2) training, preparation, competence

# Risk Assessment and Analysis - Methodologies

---

## **FRAM – FUNCTIONAL RESONANCE ANALYSIS METHOD**

- 3) communication quality,
- 4) human-machine interaction, operational support
- 5) availability of procedures
- 6) work conditions
- 7) goals, number and conflicts
- 8) available time
- 9) circadian rhythm, Stress
- 10) team collaboration
- 11) Organizational quality



# Risk Assessment and Analysis - Methodologies

---

## **FRAM – FUNCTIONAL RESONANCE ANALYSIS METHOD**

Step 3: Defining the functional resonance based on possible dependencies/couplings among functions and the potential for functional variability.

Step 4: Identifying barriers for variability (damping factors) and specifying required performance monitoring

- (1) Physical barrier systems block the movement or transportation of mass, energy, or information.
- (2) Functional barrier systems set up pre-conditions that need to be met before an action (by human and/or machine) can be undertaken.

# Risk Assessment and Analysis - Methodologies

---

## **FRAM – FUNCTIONAL RESONANCE ANALYSIS METHOD**

Step 4: Identifying barriers for variability (damping factors) and specifying required performance monitoring

(3) Symbolic barrier systems are indications of constraints on action that are physically present. Examples include signs, checklists, alarms, and clearances. Potential functions encompass preventing, regulating, and authorizing actions.

(4) Incorporeal barrier systems are indications of constraints on action that are not physically present. Examples include ethical norms, group pressure, rules, and laws.

# Risk Matrix

---

A risk matrix is a graphical tool used to assess and prioritize risks based on their severity (consequence) and likelihood (probability). It provides a visual representation of the risks, allowing stakeholders to easily understand and compare the relative importance of different risks.

The risk matrix is commonly used in risk management and decision-making processes to determine the level of attention and resources required for each identified risk

# Risk Matrix

The severity axis is divided into categories or levels that describe the potential impact or consequences of the risk. These levels can range from minor to catastrophic, or any other appropriate scale depending on the context.

Severity Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A					
Probable B					
Remote C					
Extremely Remote D					
Extremely Improbable E					*

High Risk
Medium Risk
Low Risk

\* Unacceptable with Single Point and/or Common Cause Failures

The likelihood axis is divided into categories or levels that represent the probability or frequency of the risk occurring. This scale can be qualitative (low, medium, high) or quantitative (assigned numerical values or percentages).

The cells of the matrix represent the combination of consequence and likelihood levels, creating a grid-like structure.

# Risk Matrix - ERC

Question 2

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?			
Effective	Limited	Minimal	Not effective
50	102	502	2500
10	21	101	500
2	4	20	100
1			

Question 1

If this event had escalated into an accident outcome, what would have been the most credible outcome?	
Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)
Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft
Minor Injuries or damage	Minor injuries, minor damage to aircraft
No accident outcome	No potential damage or injury could occur

Typical accident scenarios
Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
High speed taxiway collision, major turbulence injuries
Pushback accident, minor weather damage
Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

The main objective of Event Risk Classification is to act as the first screening of all incoming safety data and to identify when urgent action is necessary

# Risk Matrix - ERC

---

## Question 1

- Take all the contextual factors as they were (the location, airport, crew, aircraft, time of day, weather, etc.)
- In your mind, try to escalate the event into an accident outcome.
  - If it was virtually impossible that the event could have escalated into an accident outcome, then you are at the bottom row, at ERC value 1.
  - If you can imagine credible accident scenarios (even if improbable ones), then consider the most probable scenario and judge its typical consequence (pick the resulting row in the matrix).

# Risk Matrix - ERC

---

## Question 2

- Now think how much “safety margin” existed between the real-life event and the imagined accident scenario. Consider both the number of the remaining barriers and how strong they are. Barriers that already failed are ignored. Only the barrier which worked and any subsequent barriers still in place are considered. You should pick...
  - The extreme right column, if the only thing separating the event from an accident was pure luck or exceptional skill, which is not trained nor required
  - The 3rd column from the left, if some barrier(s) were still in place but their total effectiveness was “minimal” – e.g. this could be a GPWS warning just before an imminent CFIT.

# Risk Matrix - ERC

---

## Question 2

- The 2nd column if the effectiveness of the barrier(s) was “limited”. Typically, this is an abnormal situation, more demanding to manage, but with still a considerable remaining safety margin– e.g. a moderate error in loadsheet or loading vs. slight rotation problems at take-off.
- The extreme left column, if the safety margin was “effective”, typically consisting of several good barriers – e.g. pax smoking in the lavatory v.s. in-flight fire accident.



# Risk Matrix - ERC

Maintenance error, reduced braking capability. A single aisle aircraft with 110 pax almost overran runway end at landing. Blown tires.

Question 2

What was the effectiveness of the remaining barriers between this event and the most probable accident scenario?			
Effective	Limited	Minimal	Not effective
50	102	502	2500
10	21	101	500
2	4	20	100
1			

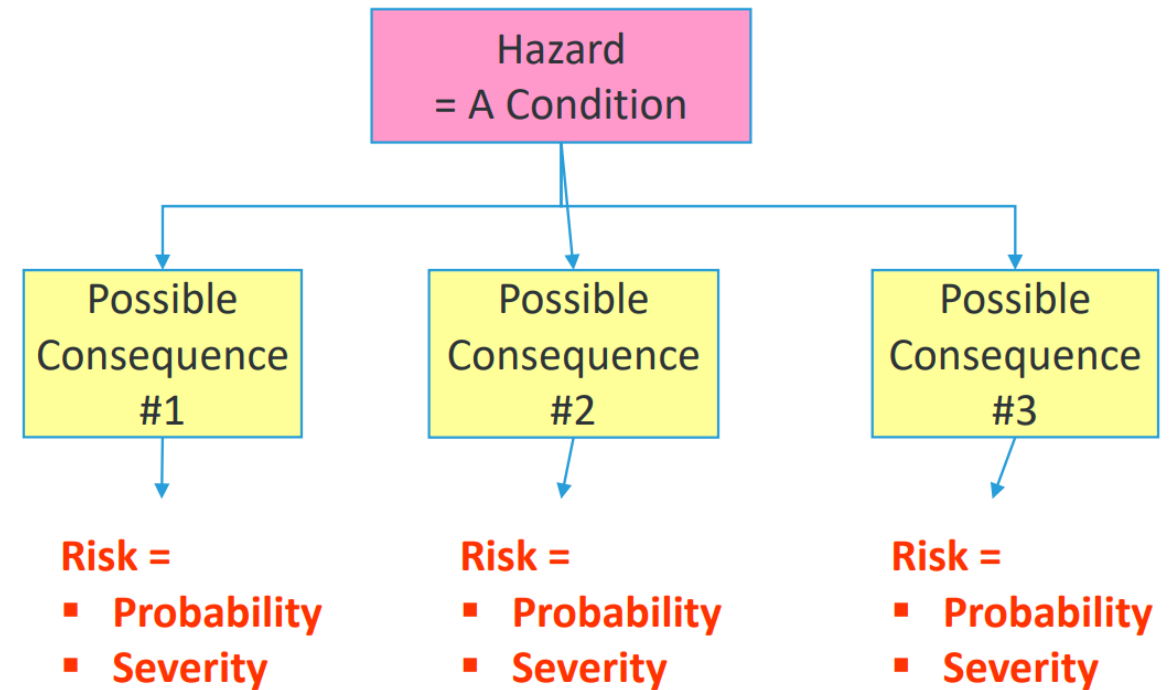
Question 1

If this event had escalated into an accident, what would have been the most probable outcome?	
Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)
Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft
Minor Injuries or damage	Minor injuries, minor damage to aircraft
No accident outcome	No potential damage or injury could occur

# Assessing and prioritizing risks based on their potential impact

Assessing and prioritizing risks based on their potential impact is a crucial aspect of risk management.

By understanding the potential consequences of risks, organizations can allocate resources and implement appropriate mitigation measures to address the most significant risks.



# Assessing and prioritizing risks based on their potential impact

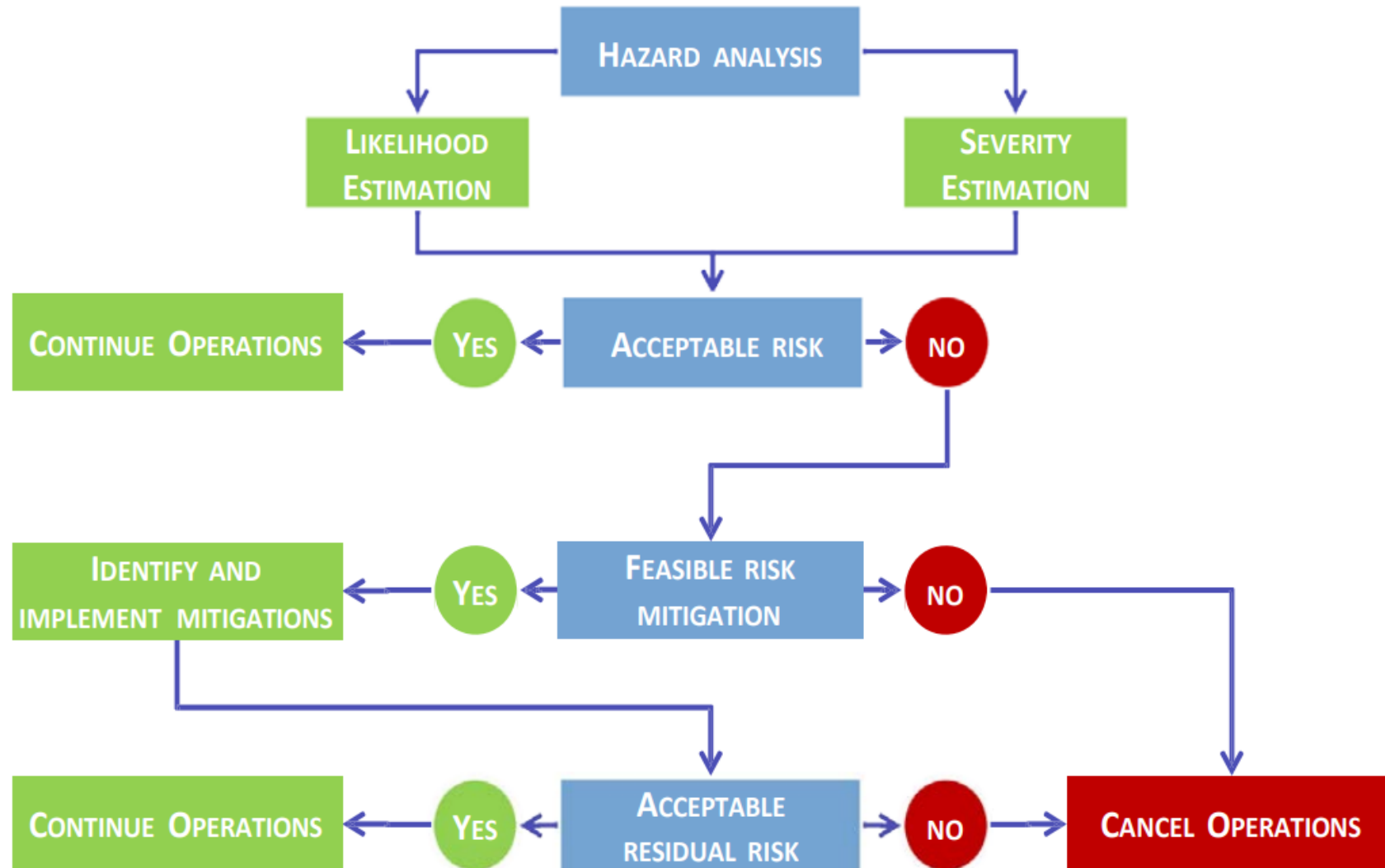
VALUE	SEVERITY	ICAO SMM (Fig 2.12)	FAA ARP Internal Order 5200.11
A	CATASTROPHIC	<ul style="list-style-type: none"> <li>Equipment destroyed</li> <li>Multiple deaths</li> </ul>	<ul style="list-style-type: none"> <li>- Complete loss of aircraft and/or facilities or fatal injury in passenger(s)/worker(s);</li> <li>- or Complete unplanned airport closure and destruction of critical facilities; or</li> <li>- Airport facilities and equipment destroyed</li> </ul>
B	HAZARDOUS	<ul style="list-style-type: none"> <li>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</li> <li>Serious injury</li> <li>Major equipment damage</li> </ul>	<ul style="list-style-type: none"> <li>- Severe damage to aircraft and/or serious injury to passenger(s)/worker(s); or</li> <li>- Complete unplanned airport closure, or</li> <li>- Major unplanned operations limitations (i.e. runway closure), or</li> <li>- Major airport damage to equipment and facilities</li> </ul>
C	MAJOR	<ul style="list-style-type: none"> <li>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</li> <li>Serious incident</li> <li>Injury to persons</li> </ul>	<ul style="list-style-type: none"> <li>- Major damage to aircraft and/or minor injury to passenger(s)/worker(s), or</li> <li>- Major unplanned disruption to airport operations, or</li> <li>- Serious incident, or</li> <li>- Deduction on the airport's ability to deal with adverse conditions</li> </ul>
D	MINOR	<ul style="list-style-type: none"> <li>Nuisance</li> <li>Operating limitations</li> <li>Use of emergency procedures</li> <li>Minor incident</li> </ul>	<ul style="list-style-type: none"> <li>- Minimal damage to aircraft or</li> <li>- Minor injury to passengers, or</li> <li>- Minimal unplanned airport operations limitations (i.e. taxiway closure), or</li> <li>- Minor incident involving the use of airport emergency procedures</li> </ul>
E	NEGLIGIBLE	<ul style="list-style-type: none"> <li>Few consequences</li> </ul>	No damage to aircraft but minimal injury or discomfort of little risk to passenger(s) or workers

# Assessing and prioritizing risks based on their potential impact

---

- Prioritize Risks:
  - Rank or prioritize the risks based on their assessed consequence levels.
  - Consider both the individual consequence levels and the overall potential impact of the risk on the organization.
  - Take into account other factors, such as the likelihood of the risk occurring, the effectiveness of existing controls, and the organization's risk tolerance.

# Assessing and prioritizing risks based on their potential impact



# Assessing and prioritizing risks based on their potential impact

---

- Two possible types of risk can be estimated during the assessment of a particular system:
  - Inherent risk is associated to the worst foreseeable (or credible) situation subject to analysis
  - Residual risk that takes into account the effect of the safety actions that could be implemented to improve system's safety performance by bringing down risk to an acceptable level

## Decision making at management level

Inherent risk

Residual risk



- Barriers have brought the risk down to an acceptable level but
- Additional effort may be required to obtain further risk

# Consideration of human factors in risk assessment

---

Considering human factors in risk assessment is essential for understanding the influence of human behavior, capabilities, and limitations on the likelihood and consequences of risks.

Human factors encompass a wide range of factors, including individual characteristics, organizational factors, and the interaction between humans and the systems they operate in.

# Consideration of human factors in risk assessment

---

1. Human Performance and Error:
  - i. Understand how human performance can contribute to or mitigate risks. Consider factors such as cognitive workload, attention, fatigue, stress, and the potential for human error.
  - ii. Assess the potential consequences of human errors or failures in tasks or processes that could lead to accidents, incidents, or operational disruptions.



# Consideration of human factors in risk assessment

---

2. Training and Competence:
  - i. Assess the adequacy of training programs and ensure that personnel have the necessary knowledge, skills, and competence to perform their tasks safely and effectively.
  - ii. Consider the impact of training on error reduction, situation awareness, decision-making, and response to abnormal or emergency situations.

# Consideration of human factors in risk assessment

---

3. Communication and Teamwork:
  - i. Evaluate the effectiveness of communication channels, information sharing, and coordination among individuals and teams.
  - ii. Assess the potential risks associated with breakdowns in communication, misinterpretation, poor coordination, or inadequate teamwork.

# Consideration of human factors in risk assessment

---

4. Training and Competence:
  - i. Assess the adequacy of training programs and ensure that personnel have the necessary knowledge, skills, and competence to perform their tasks safely and effectively.
  - ii. Consider the impact of training on error reduction, situation awareness, decision-making, and response to abnormal or emergency situations.

# Consideration of human factors in risk assessment

---

5. Organizational Culture and Work Environment:
  - i. Consider the influence of organizational factors, such as leadership, management systems, safety culture, and work environment, on risk perception, reporting, and decision-making.
  - ii. Assess the potential impact of organizational factors on individual and team performance, motivation, job satisfaction, and well-being.

# Consideration of human factors in risk assessment

---

## 5. Human Factors Integration:

- i. Ensure that human factors considerations are integrated into risk assessment methodologies, procedures, and decision-making processes.
- ii. Involve human factors specialists or experts in the risk assessment process to provide insights and expertise on human performance and its interaction with the system.

# Management of Change

---

Management of Change is a formal process for systematic and proactive identification of hazards and of appropriate mitigation strategies and measures, to be applied to all changes concerning the safety of services provided by an aviation organization.

# Management of Change

---

When is MOC Needed?

1. New / Changes in Operating Procedures
2. Facilities Changes
3. New / Changes in regulatory requirements
4. Management Changes

# Management of Change

---

A formal process for change management should take into account the following three considerations:

- Criticality of systems and activities: *“how important is this equipment/activity to safe system operations”?*
- Stability of systems and operational environments: Changes may be the result of programmed change such as growth, operations to new destinations, changes in fleets, changes in contracted services, or other changes directly under the control of the organization.
- Past performance: Past performance of critical systems is a proven indicator of future performance.



# Management of Change - STPA

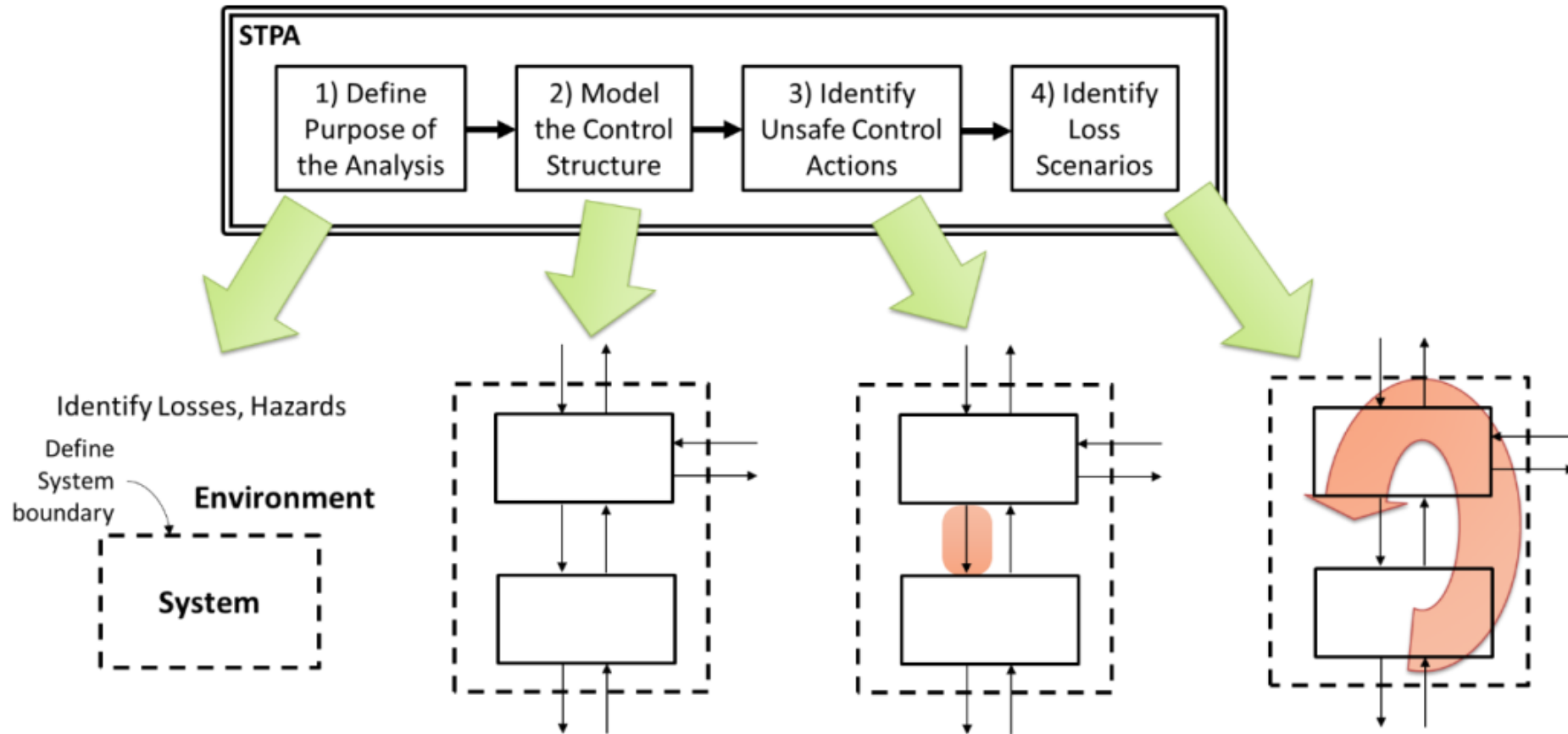
---

## System-Theoretic Process Analysis (STPA)

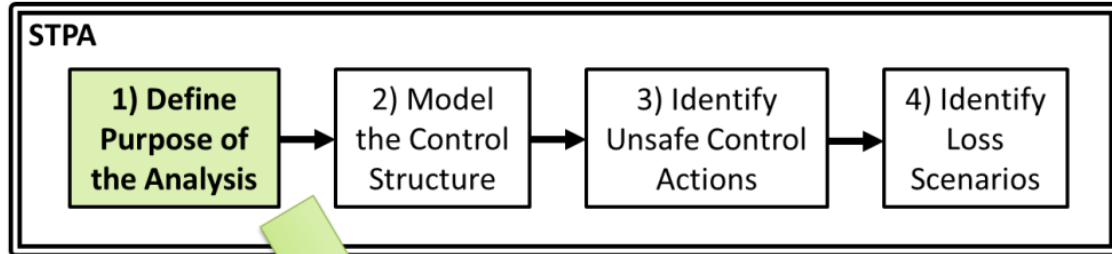
Is a technique for development and safety assessment, STPA can help anticipate hazardous scenarios caused by:

- Software, computers, and automation
- Human error/confusion
- System design errors
- Flawed assumptions
- Missing design requirements
- Interactions between systems

# Management of Change - STPA

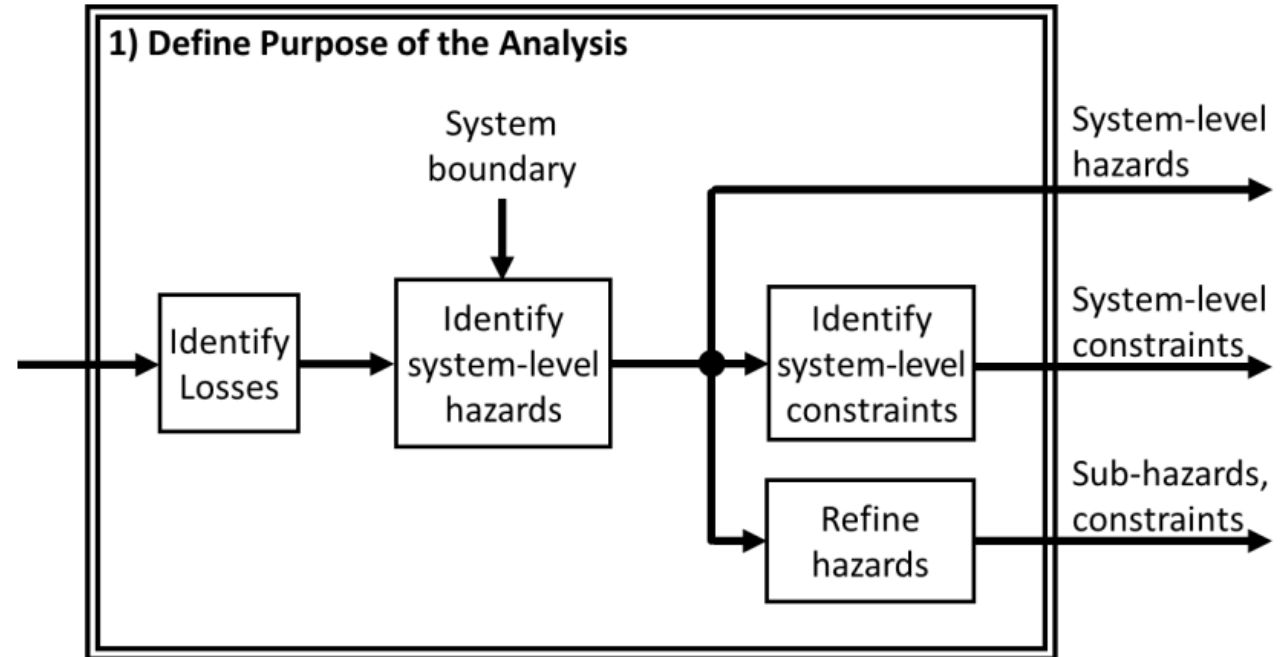
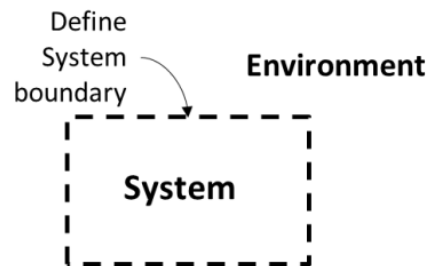


# Management of Change - STPA



## 1) Define Purpose of the Analysis

Identify Losses, Hazards



# Management of Change - STPA

---

Hazards are often very similar within an industry. Once you have identified the hazards appropriate for your industry, product, or services, you are likely to be able to reuse the list with perhaps small changes.

Aircraft

Losses:

L1. Loss of life or serious injury to people

L2. Damage to the aircraft or objects outside the aircraft

# Management of Change - STPA

---

## Hazards

H-1: Aircraft violate minimum separation standards in flight (L1, L2)

H-2: Controlled flight of aircraft into terrain (L1, L2)

H-3: Loss of aircraft control (L1, L2)

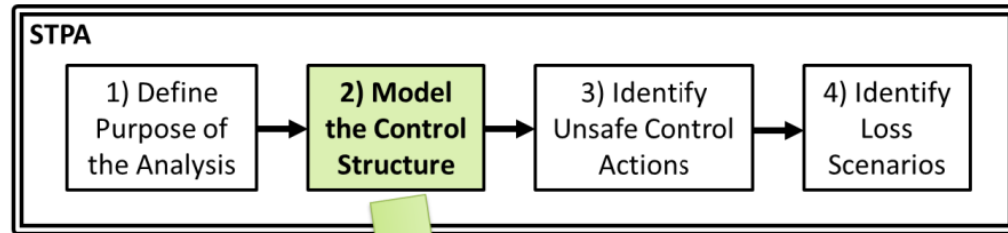
H-4: Aircraft airframe integrity is lost (L1, L2)

H-5: Aircraft environment is harmful to human health (L1, L2)

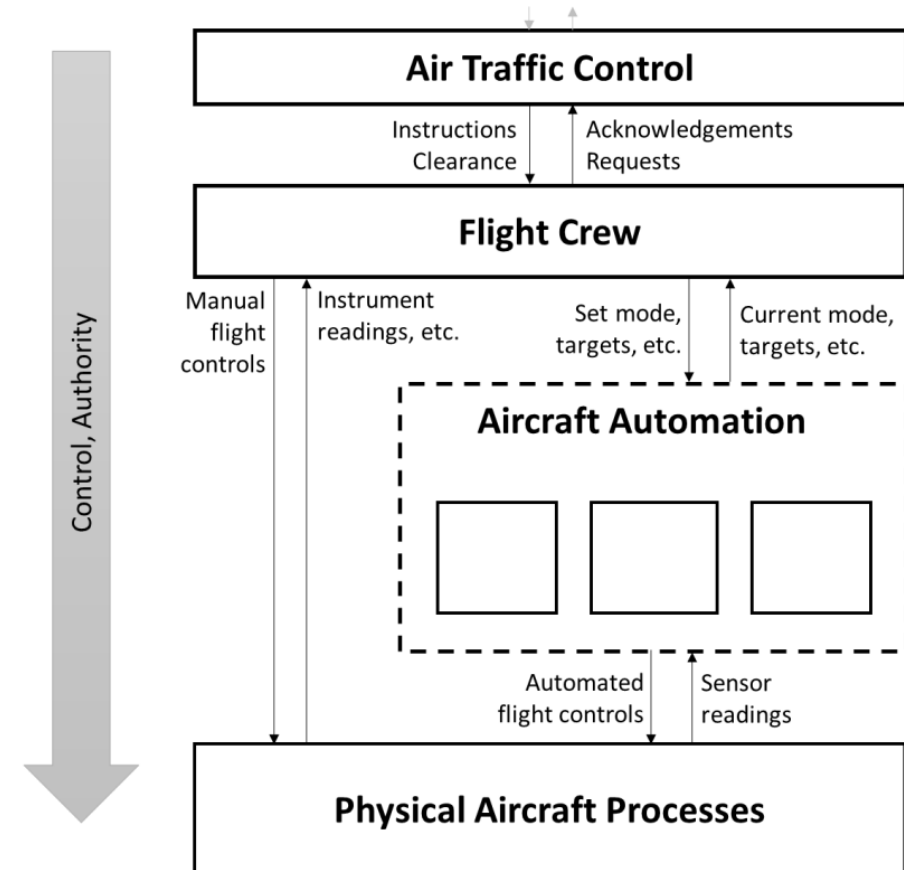
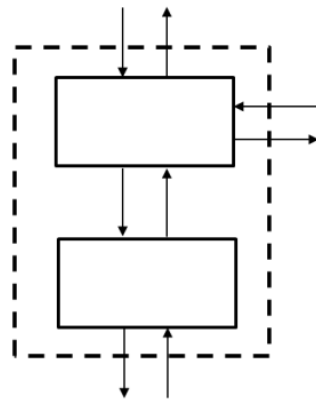
H-6: Aircraft departs designated taxiway, runway, or apron on ground (L1, L2)

H-7: Aircraft comes too close to other objects on the ground (L1, L2)

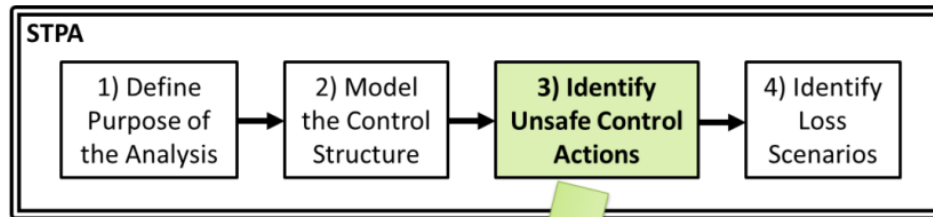
# Management of Change - STPA



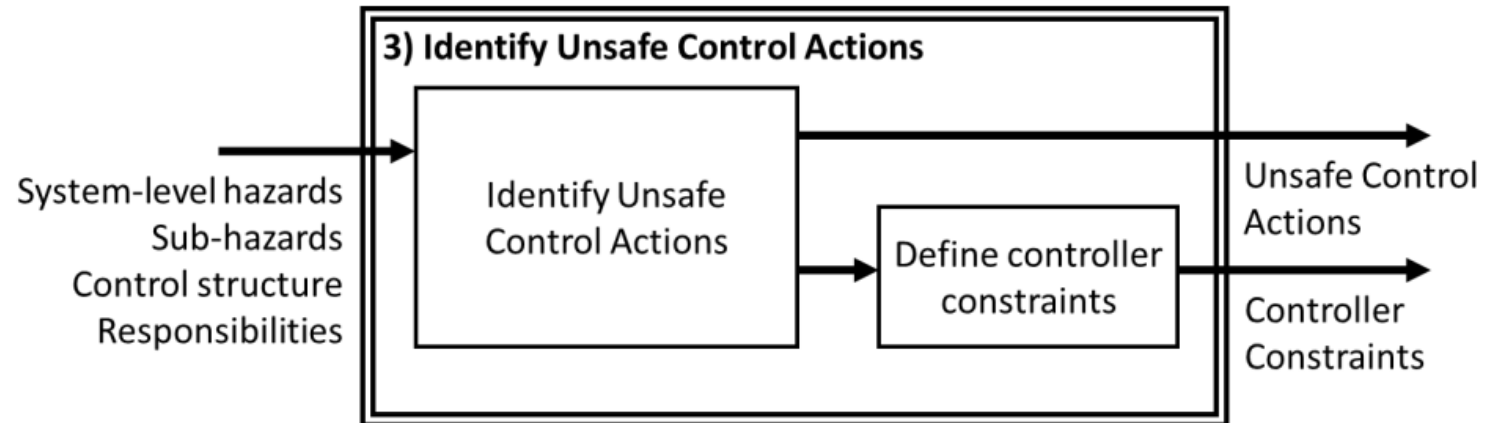
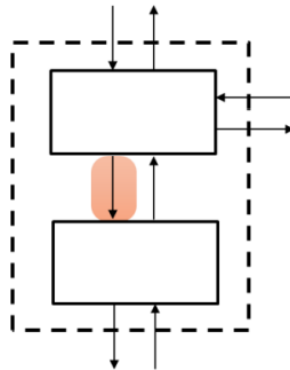
## 2) Model the Control Structure



# Management of Change - STPA



## 3) Identify Unsafe Control Actions

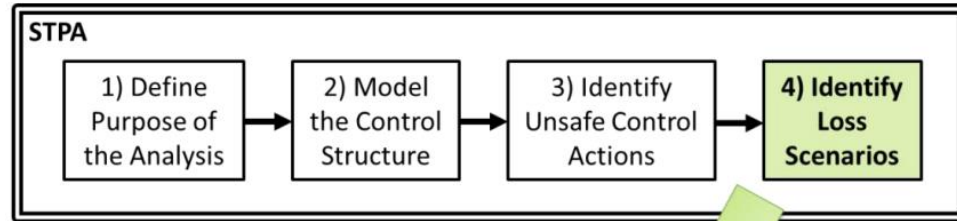


# Management of Change - STPA

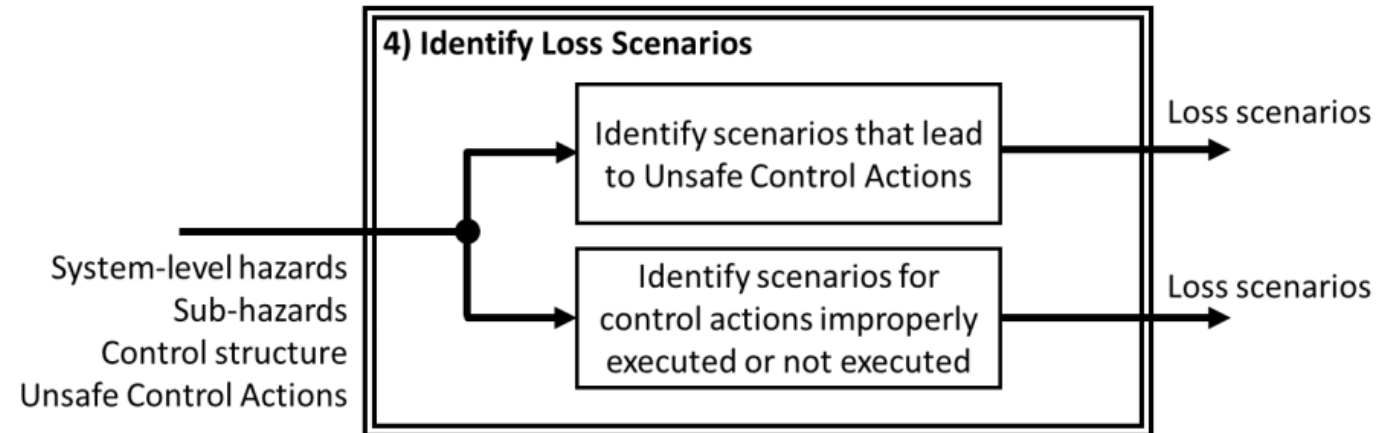
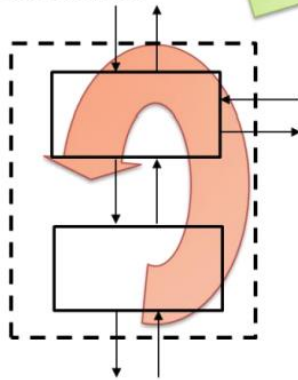
Control action	Not providing causes hazard	Providing causes hazard	Incorrect Timing/Order	Stopped Too Soon / Applied too long
Manual braking via brake pedals	Crew does not provide manual braking during landing, RTO, or taxiing when Autobrake is not providing braking or is providing insufficient braking	<p>Crew provides manual braking with insufficient pedal pressure</p> <p>Crew provides manual braking with excessive pedal pressure (resulting in loss of control, passenger/crew injury, brake overheating, brake fade or tire burst during landing)</p>	<p>Crew provides manual braking before touchdown (causes wheel lockup, loss of control, tire burst)</p> <p>Crew provides manual braking too late (TBD) to avoid collision or conflict with another object (can overload braking capability given aircraft weight, speed, distance to object (conflict), and tarmac conditions)</p>	<p>Crew stops providing manual braking command before safe taxi speed (30 kts) is Reached</p> <p>Crew provides manual braking too long (resulting in stopped aircraft on runway or active taxiway)</p>



# Management of Change - STPA



## 4) Identify Loss Scenarios



# ¿Cuál es el contenido del curso?

---

- Introduction to Safety Risk Management
- Hazard Identification
- Risk Assessment and Analysis
- **Risk Control Measures**
- Incident Investigation and Analysis
- Safety Performance Monitoring and Improvement
- Case Studies and Best Practices

# Hierarchy of controls

---

The hierarchy of risk control measures, also known as the hierarchy of controls, is a systematic approach to managing risks and minimizing hazards in the operation.

It provides a framework for selecting and implementing the most effective control measures to reduce the likelihood and severity of risks.

The hierarchy is typically presented in a descending order of effectiveness, with the most effective measures at the top.

# Hierarchy of controls

---

## 1. Elimination:

- i. The most effective control measure is to eliminate the hazard or risk altogether.
- ii. This can be achieved by redesigning processes, removing hazardous substances, or eliminating the need for a hazardous task or activity.
- iii. If the hazard is completely eliminated, there is no longer a need for further control measures.

# Hierarchy of controls

---

## 2. Substitution:

- i. If elimination is not feasible, the next best option is to substitute the hazardous materials, equipment, or processes with less hazardous alternatives.
- ii. This involves replacing the hazardous substance or equipment with safer alternatives that perform the same function.

# Hierarchy of controls

---

## 3. Engineering Controls:

- i. Engineering controls involve modifying the work environment or equipment to reduce the exposure to hazards.
- ii. Examples include installing physical barriers, ventilation systems, noise enclosures, or safety interlocks.
- iii. These controls are designed to isolate workers from the hazard or remove the hazard from the work environment.

# Hierarchy of controls

---

## 3. Administrative Controls:

- i. Administrative controls focus on changing work practices, procedures, and policies to reduce the risk.
- ii. Examples include implementing safety training programs, work rotation, job planning, signage, and warning systems.
- iii. These controls rely on human behavior and compliance with safety rules and procedures.

# Selecting and implementing appropriate control measures

---

- Safety risk mitigation is often referred to as a **safety risk control**.
- Safety risks should be managed to an acceptable level by mitigating the safety risk through the application of appropriate safety risk controls.
- This should be balanced against the time, cost and difficulty of taking action to reduce or eliminate the safety risk.
- The level of safety risk can be lowered by **reducing the severity** of the potential consequences, **reducing the likelihood** of occurrence or by **reducing exposure** to that safety risk. It is easier and more common to reduce the likelihood than it is to reduce the severity



# Selecting and implementing appropriate control measures

---

A risk mitigation strategy may include multiple approaches and it is important to consider them to find an optimal solution. Each proposed safety risk mitigation alternative should be examined from the following perspectives:

- Effectiveness: the extent to which the alternatives reduce or eliminate the safety risks can be determined in terms of the technical, training and regulatory defenses that can reduce or eliminate safety risks
- Cost-benefit: the extent to which the perceived benefits of the mitigation outweigh the costs

# Selecting and implementing appropriate control measures

---

A risk mitigation strategy may include multiple approaches and it is important to consider them to find an optimal solution. Each proposed safety risk mitigation alternative should be examined from the following perspectives:

- Practicality: the extent to which mitigation can be implemented and how appropriate it is in terms of available technology, financial and administrative resources, legislation and regulations, political will, etc..
- Acceptability: the extent to which the alternative is consistent with stakeholder paradigms

# Selecting and implementing appropriate control measures

---

A risk mitigation strategy may include multiple approaches and it is important to consider them to find an optimal solution. Each proposed safety risk mitigation alternative should be examined from the following perspectives:

- Enforceability: the extent to which compliance with new rules, regulations or operating procedures can be monitored
- Durability: the extent to which the mitigation will be sustainable and effective
- Residual safety risks: The degree of safety risk that remains subsequent to the implementation of the initial mitigation and which may necessitate additional safety risk control measures

# Selecting and implementing appropriate control measures

---

A risk mitigation strategy may include multiple approaches and it is important to consider them to find an optimal solution. Each proposed safety risk mitigation alternative should be examined from the following perspectives:

- Unintended consequences: The introduction of new hazards and related safety risks associated with the implementation of any mitigation alternative.
- Time: Time required for the implementation of the safety risk mitigation alternative

# Integration of risk controls into work processes and procedures

---

Integration of risk controls into work processes and procedures is crucial for ensuring that the identified control measures are effectively implemented and consistently followed in day-to-day operations.

1. Document Standard Operating Procedures (SOPs)
  - Develop clear and detailed SOPs that outline the step-by-step processes and procedures for performing tasks or activities.
  - Incorporate the identified control measures into the SOPs, specifying the required safety protocols, equipment, and actions to mitigate the identified risks.

# Integration of risk controls into work processes and procedures

---

Integration of risk controls into work processes and procedures is crucial for ensuring that the identified control measures are effectively implemented and consistently followed in day-to-day operations.

## 2. Embed Risk Controls in Risk Assessments

- Include the specific control measures and safety considerations associated in the risk assessment documentation.
- Clearly define the roles and responsibilities of individuals involved in executing the tasks and ensuring compliance with the control measures.

# Integration of risk controls into work processes and procedures

---

Integration of risk controls into work processes and procedures is crucial for ensuring that the identified control measures are effectively implemented and consistently followed in day-to-day operations.

## 3. Provide Training and Education

- Conduct training programs to educate employees about the identified control measures and their integration into work processes.
- Ensure that employees understand the purpose, importance, and proper implementation of the controls.

# Integration of risk controls into work processes and procedures

---

Integration of risk controls into work processes and procedures is crucial for ensuring that the identified control measures are effectively implemented and consistently followed in day-to-day operations.

## 4. Conduct Regular Audits and Inspections:

- Schedule routine audits and inspections to verify that the implemented control measures are effectively integrated into work processes and procedures.
- Identify any gaps or deviations from the prescribed controls and take corrective actions promptly.



# Integration of risk controls into work processes and procedures

---

Integration of risk controls into work processes and procedures is crucial for ensuring that the identified control measures are effectively implemented and consistently followed in day-to-day operations.

## 4. Continuous Improvement and Feedback:

- Encourage employees to provide feedback on the effectiveness and practicality of the integrated control measures.
- Regularly review and evaluate the implemented controls, considering any lessons learned, emerging risks, or technological advancements.
- Seek input from employees and safety professionals to identify opportunities for improvement and update work processes and procedures accordingly.

# Integration of risk controls into work processes and procedures

---

By integrating risk controls into work processes and procedures, organizations promote a culture of safety and ensure that control measures become an inherent part of daily operations. Regular reinforcement, training, and monitoring are vital to sustain the effectiveness of the controls and maintain a safe working environment.

# Monitoring and evaluating the effectiveness of control measures

---

Control measures are the heart of your aviation safety management systems (SMS) risk mitigation efforts. You may call your "control measures" either:

- Risk controls; or
- Simply "controls"

***Control measures need to actively exist in the operational environment, and not simply exist "on paper."***

# Monitoring and evaluating the effectiveness of control measures

---

We often see three different types of monitoring activities

- Periodic performance monitoring: evaluating control measures in a formal review process on an annual or semiannual basis, such as with auditing.
- Scheduled monitoring: monitoring control measures on a regular basis, such as reviewing hazard trends and identifying problem control measures once per month; and

# Monitoring and evaluating the effectiveness of control measures

---

We often see three different types of monitoring activities

- Ongoing monitoring: monitoring affected control measures on a daily basis, such as when hazard reports are submitted.

# Monitoring and evaluating the effectiveness of control measures

---

## **Periodically Monitoring the Performance of Control Measures**

Periodically monitoring the effectiveness of control measures involves an infrequent but thorough assessment of control measures. Periodic monitoring activities usually involve:

- Formal review of control measures
- Stress testing the SMS to expose inadequate control measures
- Auditing control measures

# Monitoring and evaluating the effectiveness of control measures

---

## Periodically Monitoring the Performance of Control Measures

Aviation safety programs can have literally hundreds of control measures. It's not feasible to evaluate each one. In a periodic review. Safety management needs to **efficiently** monitor the effectiveness of control measures. To do this, safety management should do the following before they begin their periodic review:

# Monitoring and evaluating the effectiveness of control measures

---

## **Periodically Monitoring the Performance of Control Measures**

- Review safety data charts for trends
- Review hazard register to see which hazards are continually arising in safety issues
- Review classifications during issue management to evaluate which classifications are not being mitigated.



# Monitoring and evaluating the effectiveness of control measures

---

## **Scheduled Monitoring of the Effectiveness of Control Measures**

Scheduled monitoring happens more frequently than periodic monitoring, such as during hazard analysis and review. Not all safety issues require an in-depth hazard analysis. Generally, such operations are reserved for mid to high-risk issues.

# Monitoring and evaluating the effectiveness of control measures

---

## **Scheduled Monitoring of the Effectiveness of Control Measures**

When such issues are reported, management needs to undertake hazard analysis activities, such as:

- Fishbone diagram root cause analysis
- Bowtie analysis
- Decision trees

# Monitoring and evaluating the effectiveness of control measures

---

## **Scheduled Monitoring of the Effectiveness of Control Measures**

These operations naturally incorporate risk control review into the analysis process and should quickly point out inadequacies in the risk control, as well as identify which risk controls are meeting needs.

# Monitoring and evaluating the effectiveness of control measures

---

## **Scheduled Monitoring of the Effectiveness of Control Measures**

Situations for scheduled monitoring are:

- Responsible manager's mandatory review of hazards;
- Safety cases
- Management of change
- Risk analysis and investigations
- Risk scenario analysis.

# Monitoring and evaluating the effectiveness of control measures

---

## **Ongoing Assessment of Control Measure Effectiveness**

Ongoing assessments of control measure effectiveness happen almost on a daily basis. This method is used to monitor the effectiveness of control measures through common interactions with the safety management system

# Monitoring and evaluating the effectiveness of control measures

---

## **Ongoing Assessment of Control Measure Effectiveness**

- When issues are reported
- When corrective preventative actions (CPAs) are created;
- When CPAs are reviewed
- When issues are validated (reviewed)
- Other issue management activities

# Monitoring and evaluating the effectiveness of control measures

---

## **Ongoing Assessment of Control Measure Effectiveness**

Ongoing monitoring should be a natural product of issue management. When issues are reported, safety management is tasked with identifying:

- Why the issue was mitigated
- How the issue could have been further mitigated (if applicable)

# Monitoring and evaluating the effectiveness of control measures

---

## **Ongoing Assessment of Control Measure Effectiveness**

Ongoing monitoring should be a natural product of issue management. When issues are reported, safety management is tasked with identifying:

- What controls worked/did not work
- If further controls are needed



# Monitoring and evaluating the effectiveness of control measures

---

In short, issue management forces safety management to look directly at pertinent safety controls to evaluate whether or not they worked as desired. This is a natural way to monitor control measures whenever safety issues are reported.

# ¿Cuál es el contenido del curso?

---

- Introduction to Safety Risk Management
- Hazard Identification
- Risk Assessment and Analysis
- Risk Control Measures
- **Incident Investigation and Analysis**
- Safety Performance Monitoring and Improvement
- Case Studies and Best Practices

# Importance of incident investigation in safety risk management

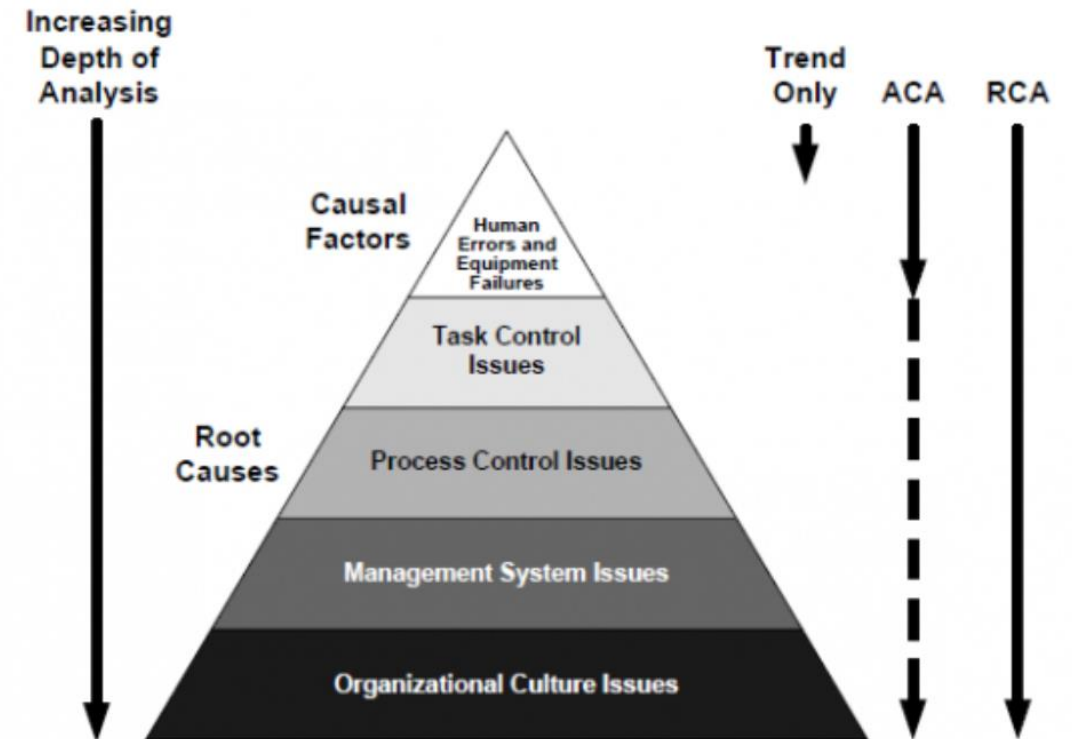
---

Incident investigation plays a critical role in safety risk management by providing valuable insights into the causes and contributing factors of incidents, accidents, and near-misses.



# Importance of incident investigation in safety risk management

1. Identifying Root Causes
2. Learning from Mistakes
3. Enhancing Safety Procedures and Controls
4. Strengthening Safety Culture
5. Compliance and Legal Requirements
6. Benchmarking and Performance Evaluation
7. Stakeholder Communication and Transparency



# Accident, Incident, Near Miss

---

ICAO Annex 13 defines an accident as 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 damage or structural failure
- The aircraft is missing or is completely inaccessible

# Accident, Incident, Near Miss

---

There are several ways to classify an accident. These include classification by the level of damage incurred, by the extent of injuries caused, or by the cost of the damage to the aircraft. The following definitions are used in various classification taxonomies:

## Damage

**Destroyed:** The aircraft is not repairable, or, if repairable, the cost of repairs exceeds 50% of the cost of the aircraft when it was new



# Accident, Incident, Near Miss

---

## Damage

**Substantial:** Damage or failure that adversely affects the structural strength, performance, or flight characteristics of the aircraft, and which would normally require major repair or replacement of the affected component. Not considered in substantial damage are; engine failure or damage limited to an engine only, bent or dented skin, damage to landing gear (to include wheels and tires), flaps, or wingtips





# Accident, Incident, Near Miss

---

## Damage

**Minor :** Damage that neither destroys the aircraft nor causes substantial damage.





# Accident, Incident, Near Miss

---

## Injury

**Fatal:** An injury that results in death in the accident itself, or up to 30 days after the accident

**Serious:** An injury that requires more than 2 days of hospitalization up to 7 days after the accident. Fracture of any bone (except simple fractures of the toes, fingers, or nose). Serious also includes injury to an internal organ, any muscle or tendon damage, any second- or third-degree burn, or any burn covering more than 5 percent of the body.

**Minor:** An injury that requires less than 2 days of hospitalization up to 7 days after the accident.



# Accident, Incident, Near Miss

---

## Accident Classifications

**Hull Loss Accident:** An accident in which the aircraft damage is not repairable or is damaged but not repaired. Hull loss accidents include when the aircraft is missing, or if the wreckage is inaccessible.



# Accident, Incident, Near Miss

---

## Accident Classifications

**Major Accident:** An accident in which any of the following three conditions are met:

- The aircraft is destroyed
- There were multiple fatalities
- There was one fatality and the aircraft sustained substantial damage



# Accident, Incident, Near Miss

---

## Accident Classifications

**Fatal Accident:** An accident causing one or more fatalities to occupants of the aircraft

**Accident:** An accident in which the aircraft sustained substantial damage

**Serious Accident:** An accident in which either of the following two conditions are met:

- A single fatality without substantial damage
- At least one serious injury and aircraft substantially damaged





# Accident, Incident, Near Miss

---

## Accident Classifications

**Minor Accident:** An accident in which the aircraft sustained minor damage



# Accident, Incident, Near Miss

---

## **Incident**

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



# Accident, Incident, Near Miss

---

## Incident

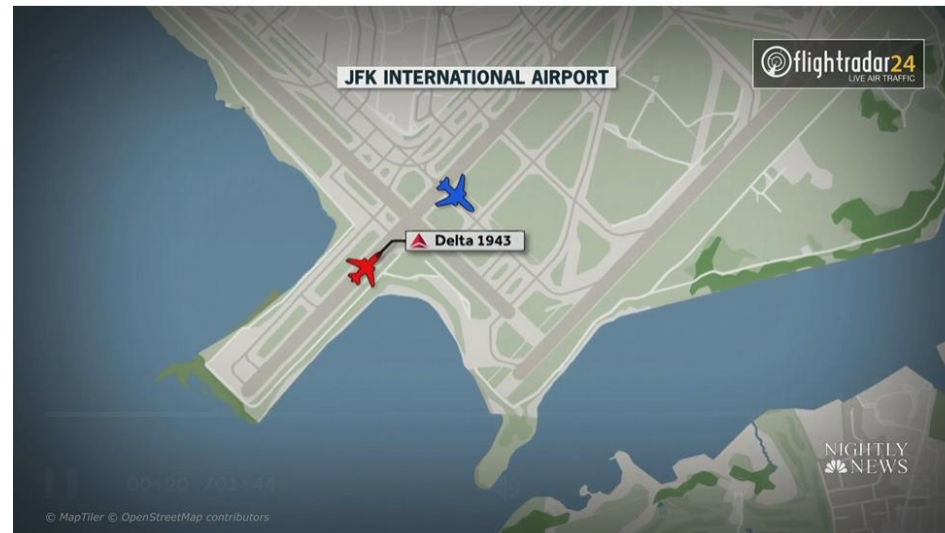
**Serious Incident:** An incident involving circumstances indicating that there was a high probability of an accident and associated with the operation of an aircraft which, in the case of a manned aircraft, takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, or in the case of an unmanned aircraft, takes place between the time the aircraft is ready to move with the purpose of flight until such time as it comes to rest at the end of the flight and the primary propulsion system is shut down.



# Accident, Incident, Near Miss

## Near-Miss

An incident that does not cause harm





# Steps involved in conducting an incident investigation

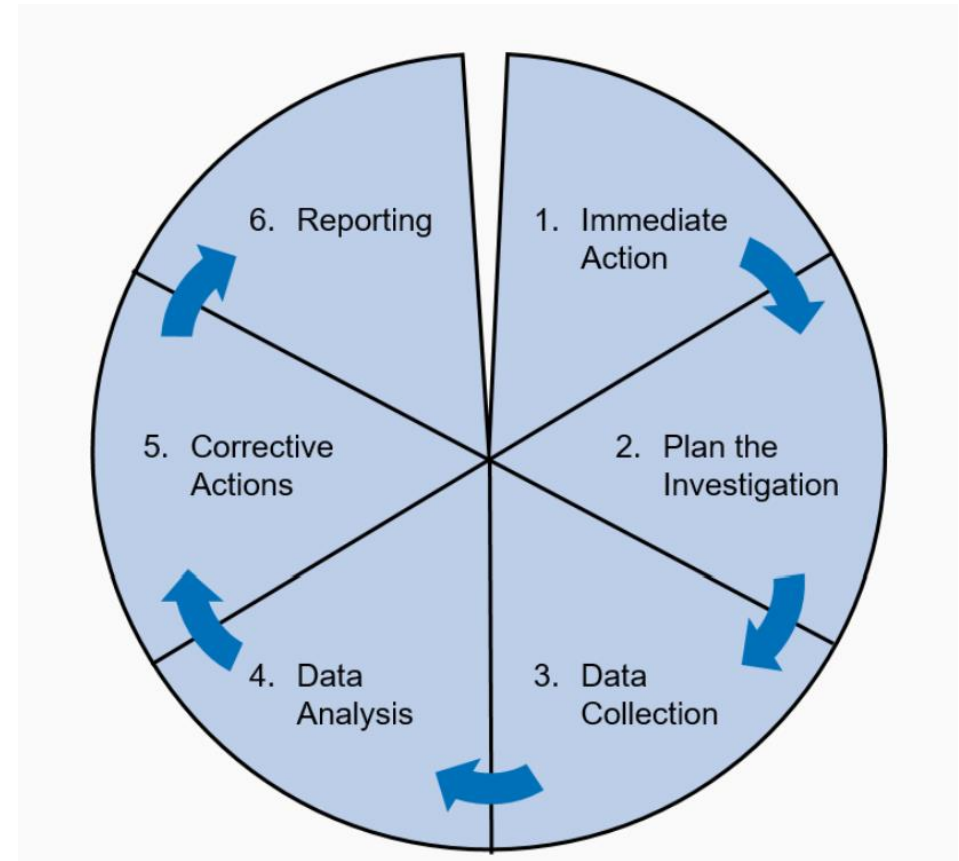
## 1. Immediate Action

In the event of an incident, immediate action to be taken may include making the area safe, preserving the scene and notifying relevant parties, such as:

- Accountable Executives
- Safety Managers
- Relevant Authorities

Preserving the scene include:

- Secure data such as CCTV footage
- Secure aircraft data (FDR, CVR)

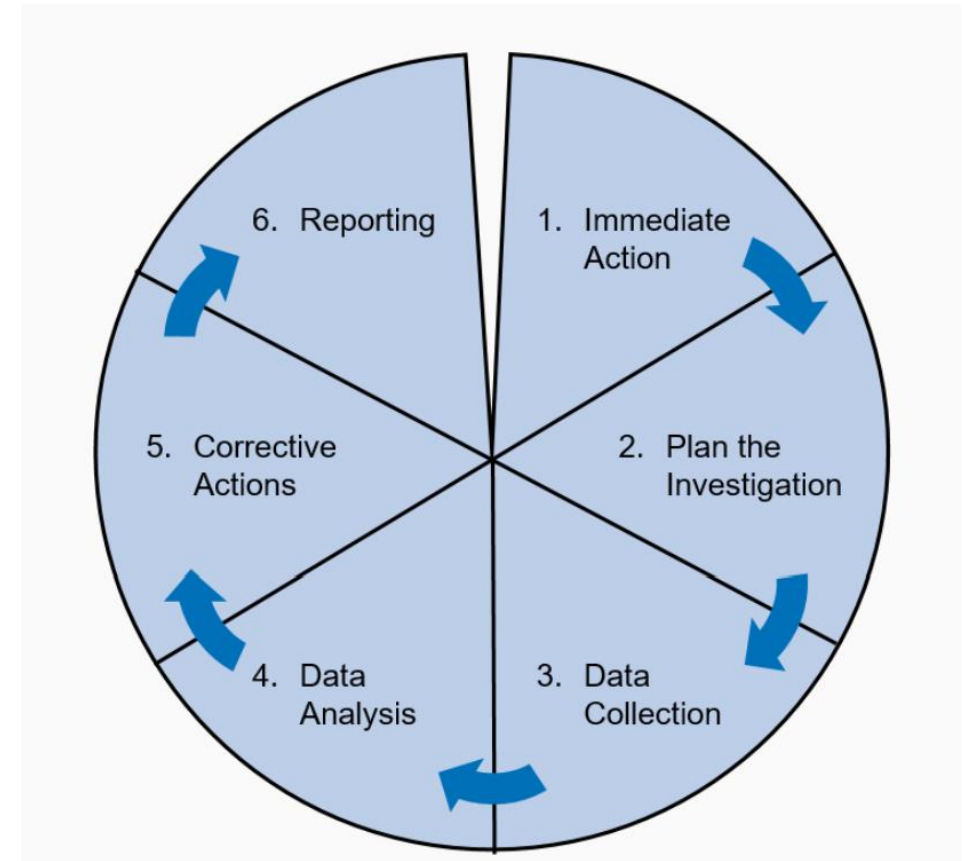


# Steps involved in conducting an incident investigation

## 2. Plan the Investigation

Planning ensures that the investigation is systematic and complete. What resources will be required? Who will be involved? How long will the investigation take?

**Set up of the investigation team** with the required skills and expertise. The size of the team and the expert profile of its members depend on the nature and severity of the occurrence being investigated. The investigating team may require the assistance of other specialists. Often, a single person is assigned to carry out internal (to the concerned organization) investigation of an incident considered to have limited potential to cause harm.

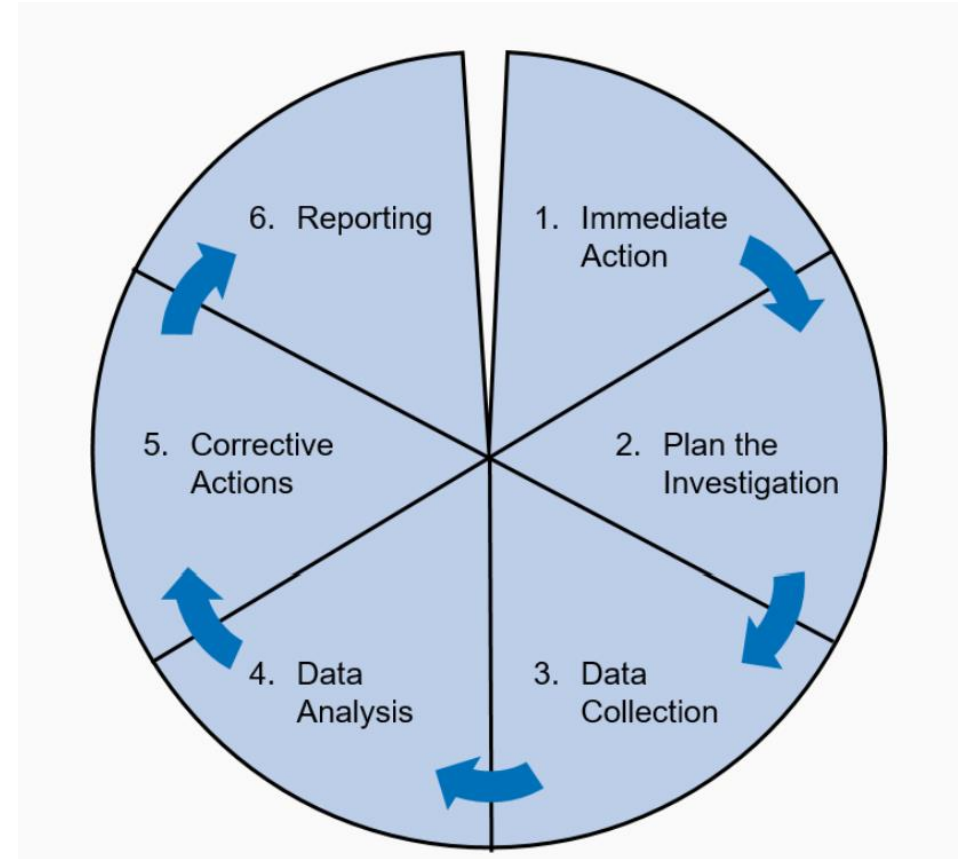


# Steps involved in conducting an incident investigation

---

## 3. Data Collection

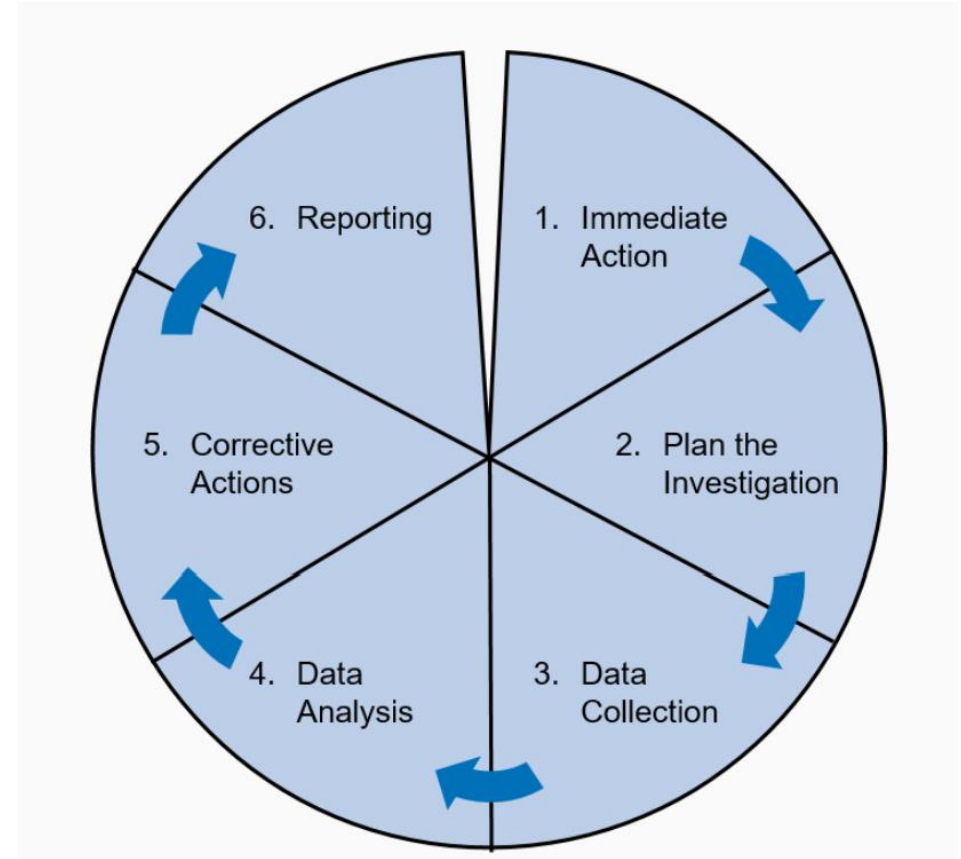
Once the incident site is secure and the immediate response measures are in place, it's crucial to shift the focus toward gathering as much data and information about the incident as possible. Time is of the essence during this phase because vital information can be lost, memories can fade, and physical evidence can be compromised as regular work operations resume.



# Steps involved in conducting an incident investigation

## 3. Data Collection

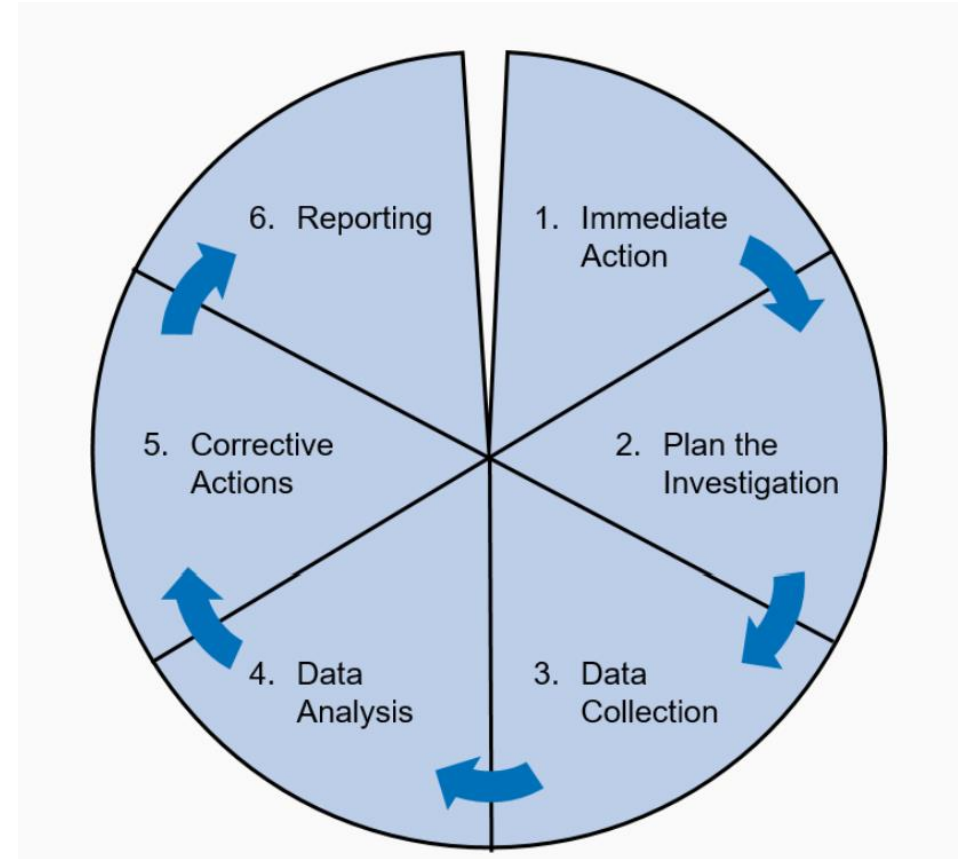
**Interview Witnesses:** Begin by speaking with everyone who witnessed the incident. Ask each witness to provide a comprehensive account of what they saw, experienced, or noticed leading up to, during, and following the incident. Encourage them to share seemingly insignificant details, sometimes providing crucial insights. These interviews should be conducted non-threatening to create an atmosphere of trust. Remember, the goal here is to gather information, not to assign blame.



# Steps involved in conducting an incident investigation

## 3. Data Collection

**Collect Documentation:** Gathering relevant documentation is an important part of the information collection phase. This might include equipment logs, maintenance records, training documents, safety inspection reports, operational guidelines, and other records that might shed light on the incident. Photographs or video footage of the incident site and any equipment can provide valuable visual evidence. At the same time, diagrams or sketches can help visualize the layout and movement during the incident.

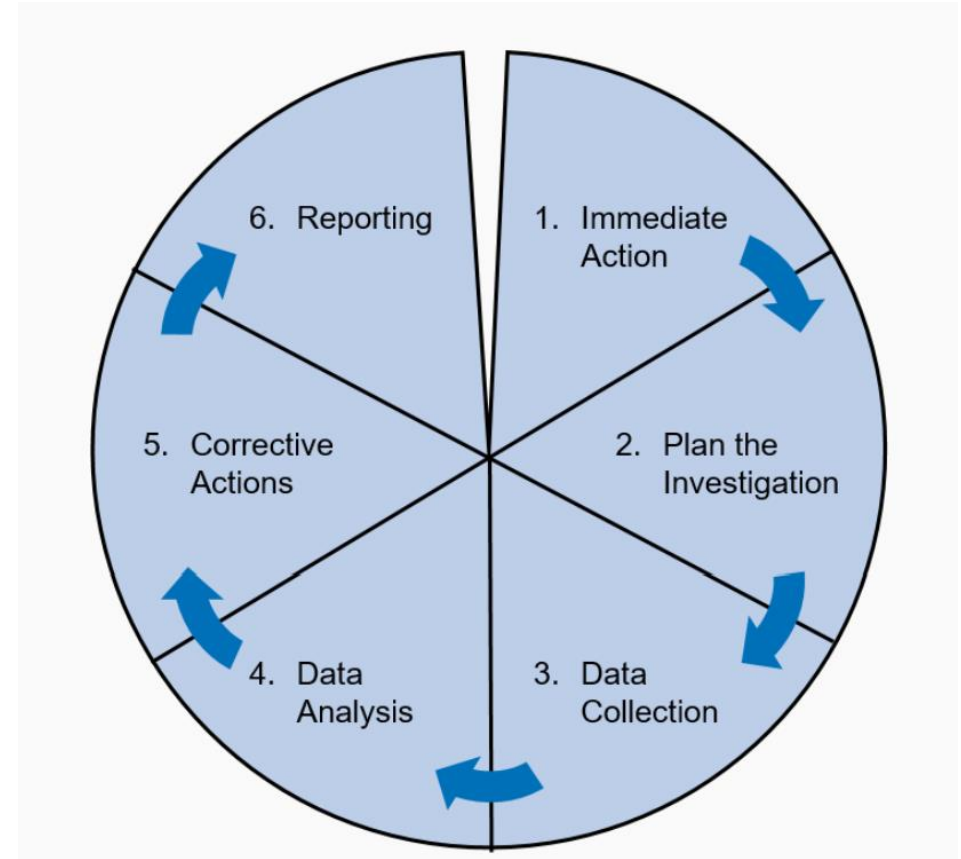




# Steps involved in conducting an incident investigation

## 3. Data Collection

**Identify Information Gaps:** After collecting all available data and information, the investigator should review it thoroughly to identify gaps or inconsistencies. If certain aspects of the incident remain unclear or unexplained, further investigation may be needed to fill these gaps. This could involve additional witness interviews, a more detailed examination of the physical evidence, or consultation with technical experts.

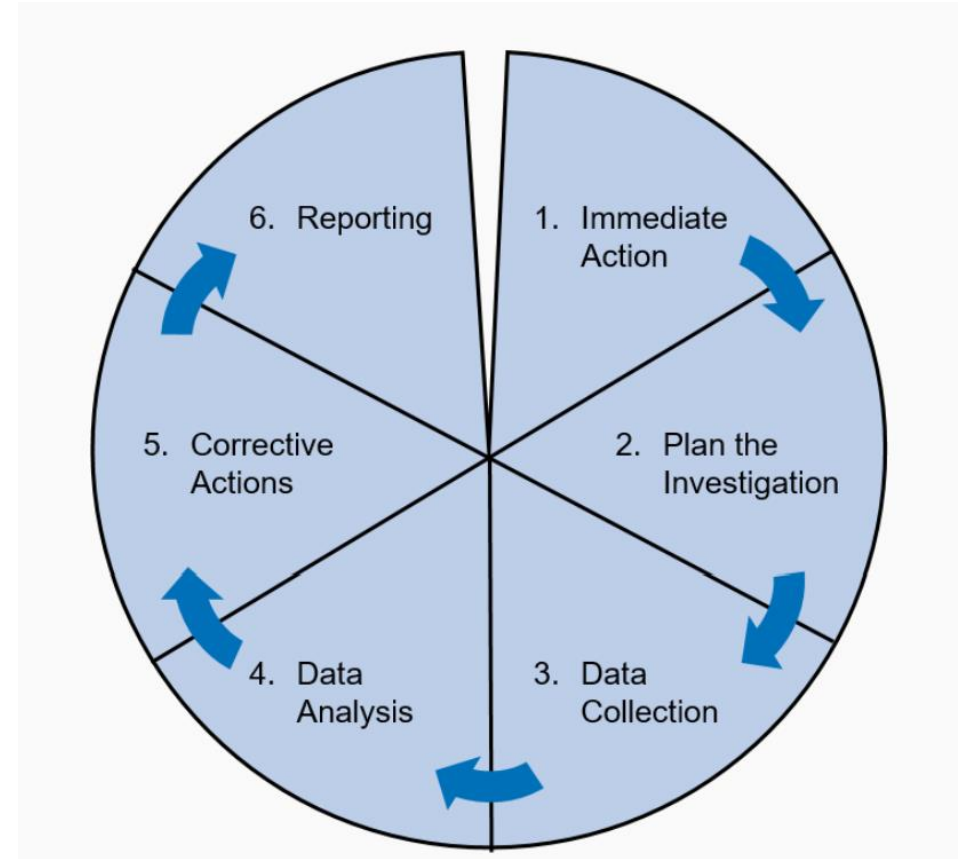


# Steps involved in conducting an incident investigation

## 3. Data Collection

### **Identify Information Gaps:**

Through comprehensive and diligent information gathering, investigators can assemble a detailed and accurate understanding of the incident, providing a solid foundation for the next stages of the investigation. This phase is crucial for revealing the underlying factors and conditions that contributed to the incident, guiding the way toward effective preventative measures.

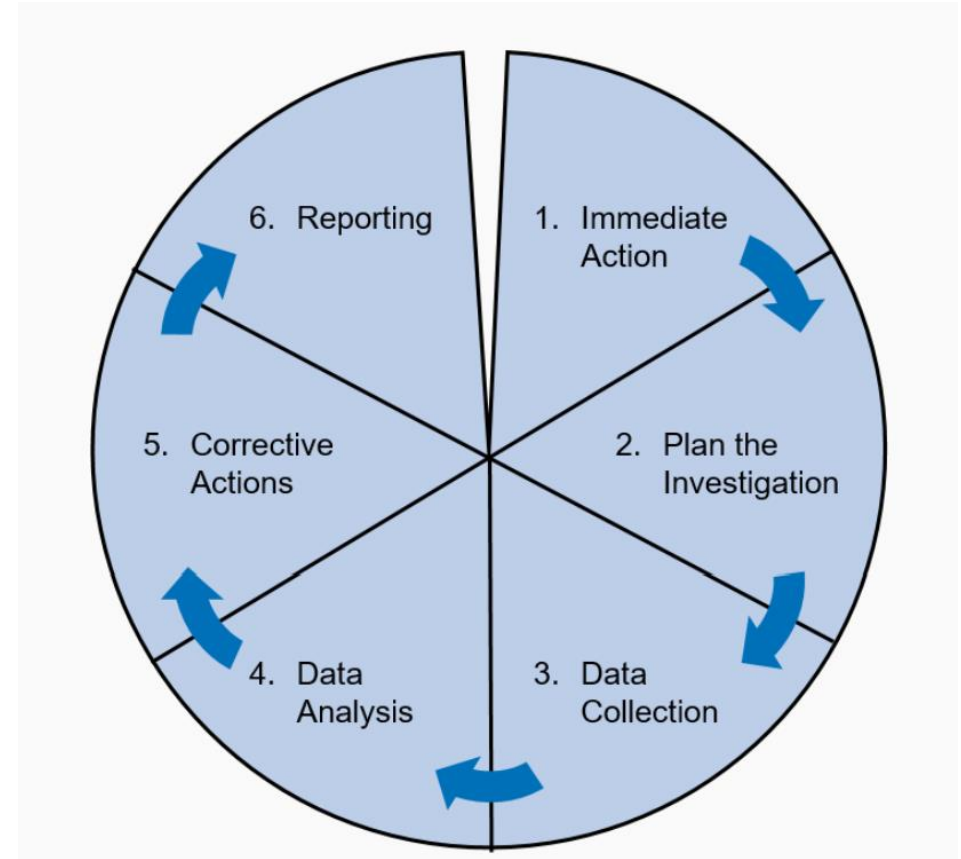


# Steps involved in conducting an incident investigation

## 4. Data Analysis

Typically, an incident is not just a single event, but a chain of events. The sequence of events needs to be understood before identifying why the incident happened

Once all the information has been collected, it's time to transition to the analysis phase of the investigation. This involves synthesizing and examining the gathered data to understand the events and factors contributing to the incident.



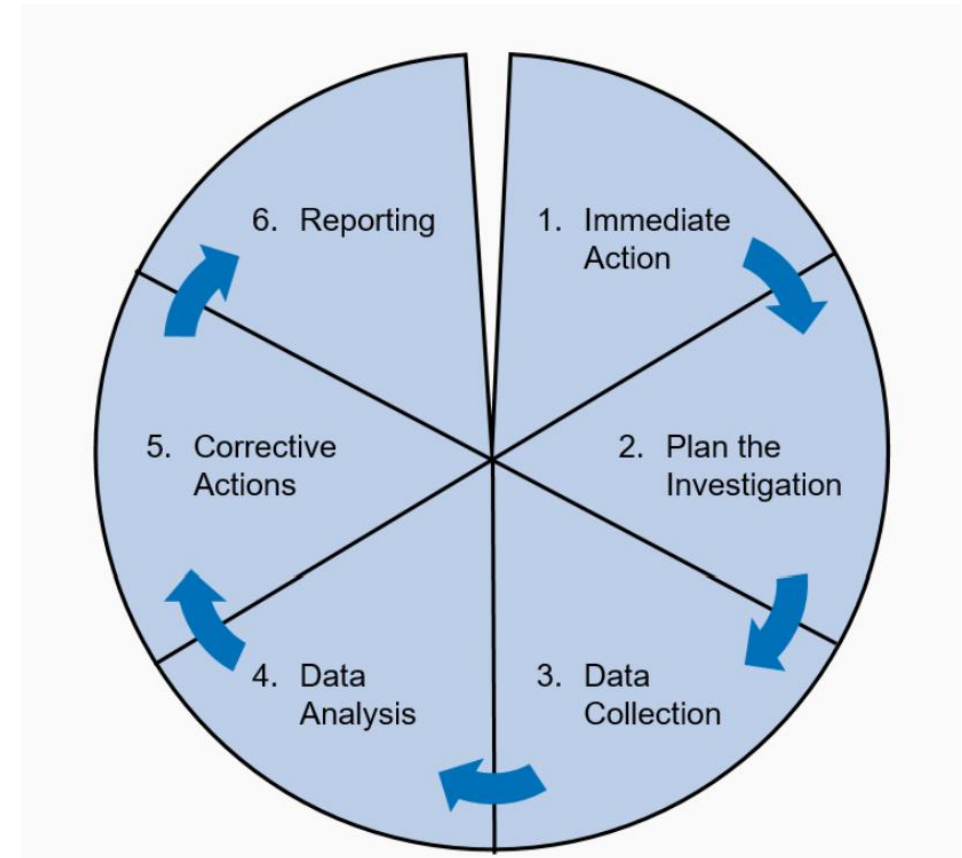


# Steps involved in conducting an incident investigation

## 4. Data Analysis

### Timeline Creation

Creating a detailed incident timeline is one of the most effective ways to begin the analysis. Start from the earliest known relevant event—this could be hours, days, or even weeks before the actual incident, especially if factors like equipment maintenance, operational changes, or environmental conditions played a role. Continue through the incident itself and include any notable post-incident actions. This chronological account provides a clear sequence of events and can help identify cause-and-effect relationships.

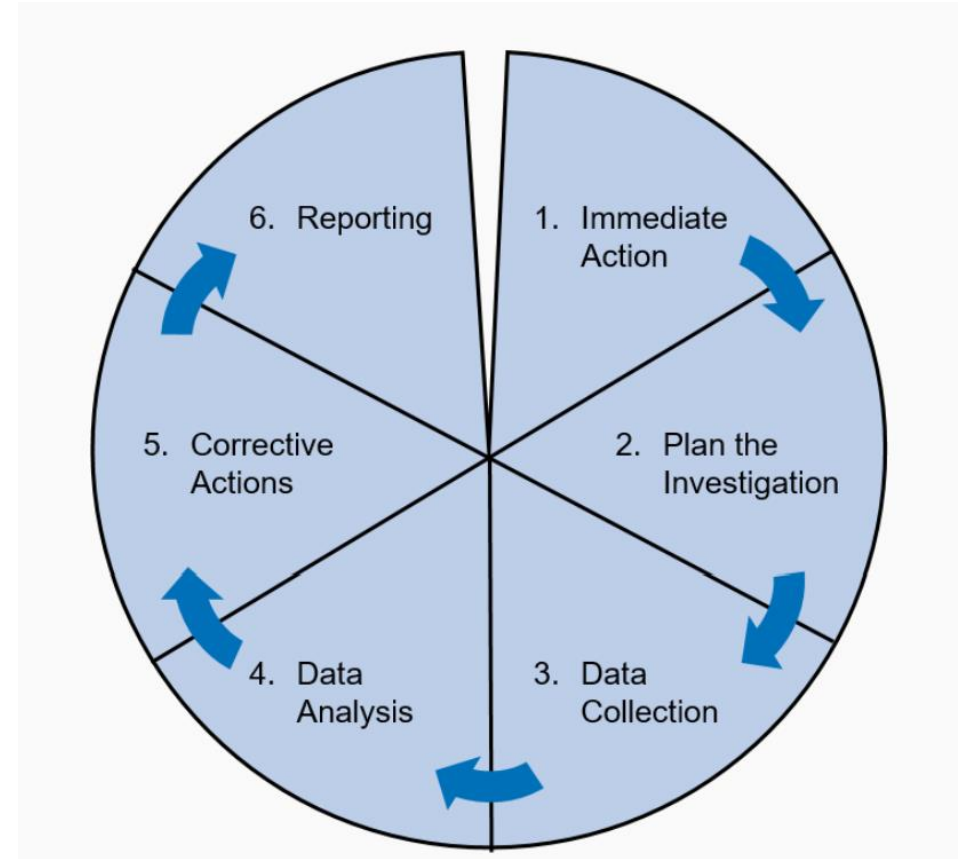


# Steps involved in conducting an incident investigation

## 4. Data Analysis

### Logical Analysis

In addition to a chronological overview, organizing the information logically is helpful. This means categorizing data based on common themes, such as human actions, equipment performance, environmental conditions, and procedural adherence. This approach can help highlight patterns and correlations that might not be immediately apparent in a chronological view, leading to a deeper understanding of contributing factors and underlying root causes

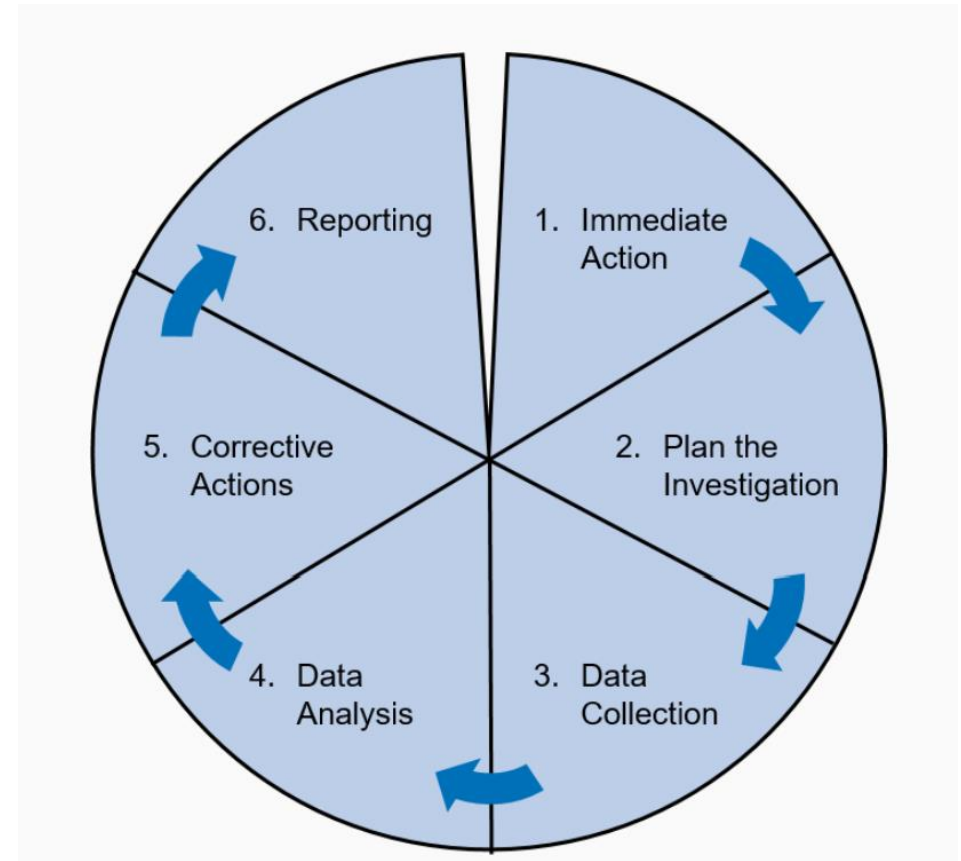


# Steps involved in conducting an incident investigation

## 4. Data Analysis

### Identifying Knowns And Unknowns

As part of the analysis, the investigator should clearly delineate what is known from the gathered data and what remains unknown or unclear. Acknowledging these unknowns can help identify limitations in the current understanding of the incident and indicate areas where further information might be required.

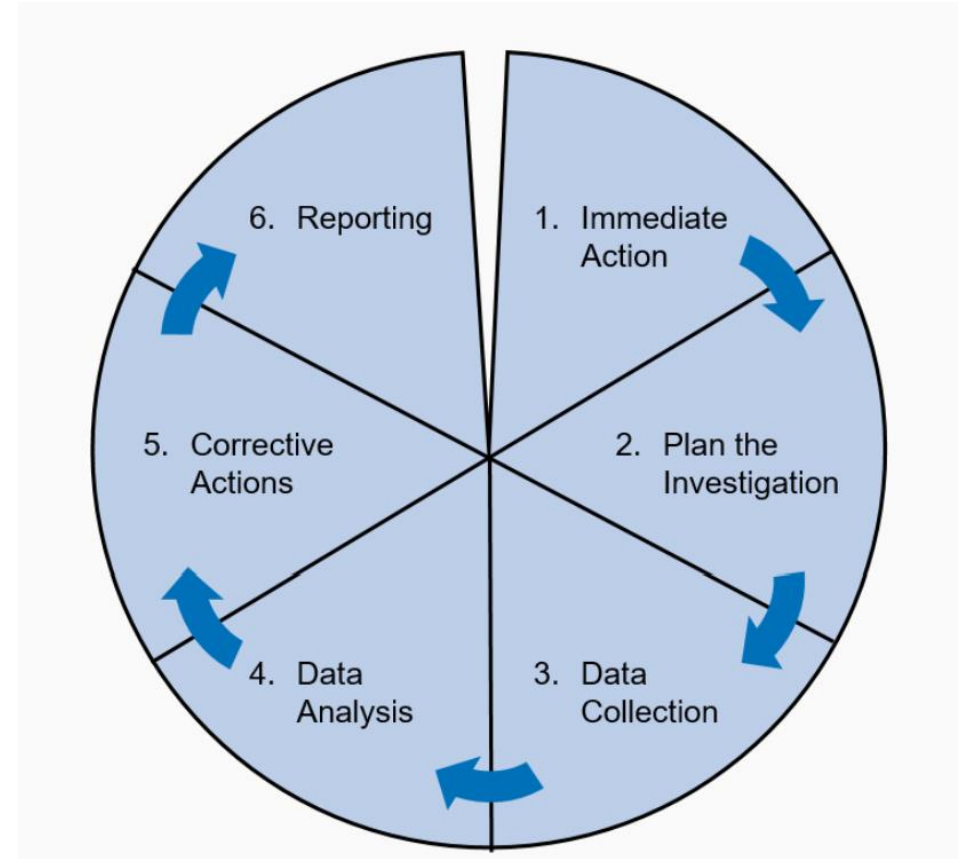


# Steps involved in conducting an incident investigation

## 4. Data Analysis

### **Determining Probable Cause**

With a detailed understanding of the events leading up to, during, and following the incident, the investigator can now work towards identifying the probable cause or causes of the incident. This is often a complex process, as it's rare for incidents to have a single, simple cause. Instead, it's usually a combination of interconnected factors, like human error, equipment failure, procedural deficiencies, or environmental conditions.



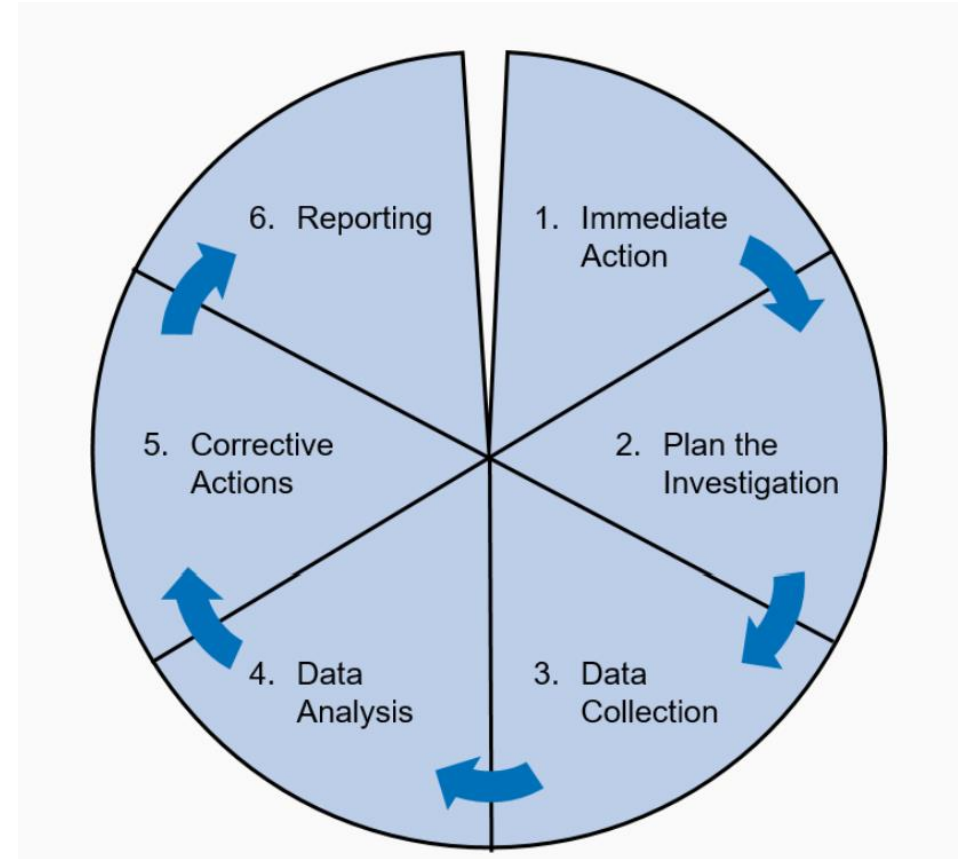
# Steps involved in conducting an incident investigation

## 4. Data Analysis

### **Determining Probable Cause**

Through comprehensive and thoughtful analysis, investigators can move beyond the simple facts of the incident to understand the underlying causes, ultimately providing the insights needed to prevent similar incidents in the future.

RCA tools are useful to determine probable causes, but consider that the use of the incorrect tool could leave underlying causes uncovered

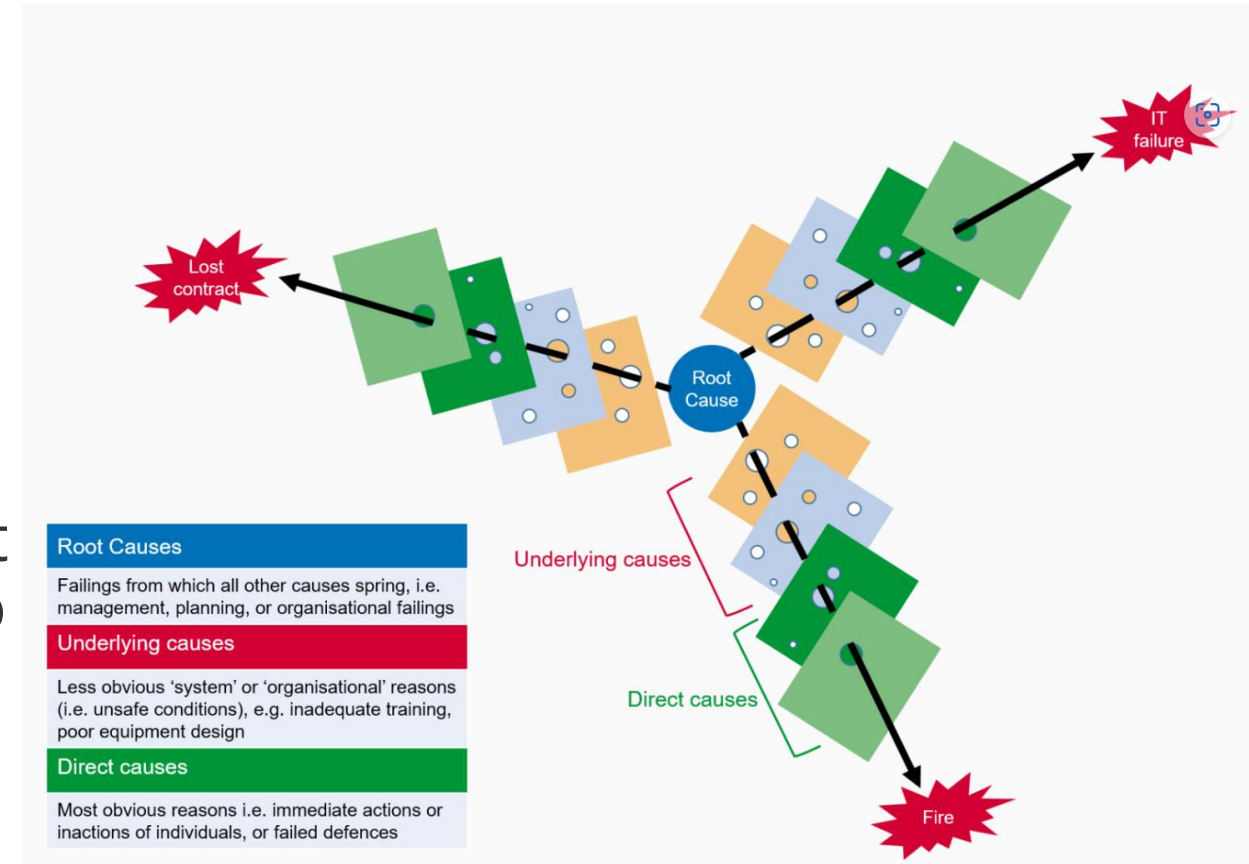




# Steps involved in conducting an incident investigation

## 5. Corrective Actions

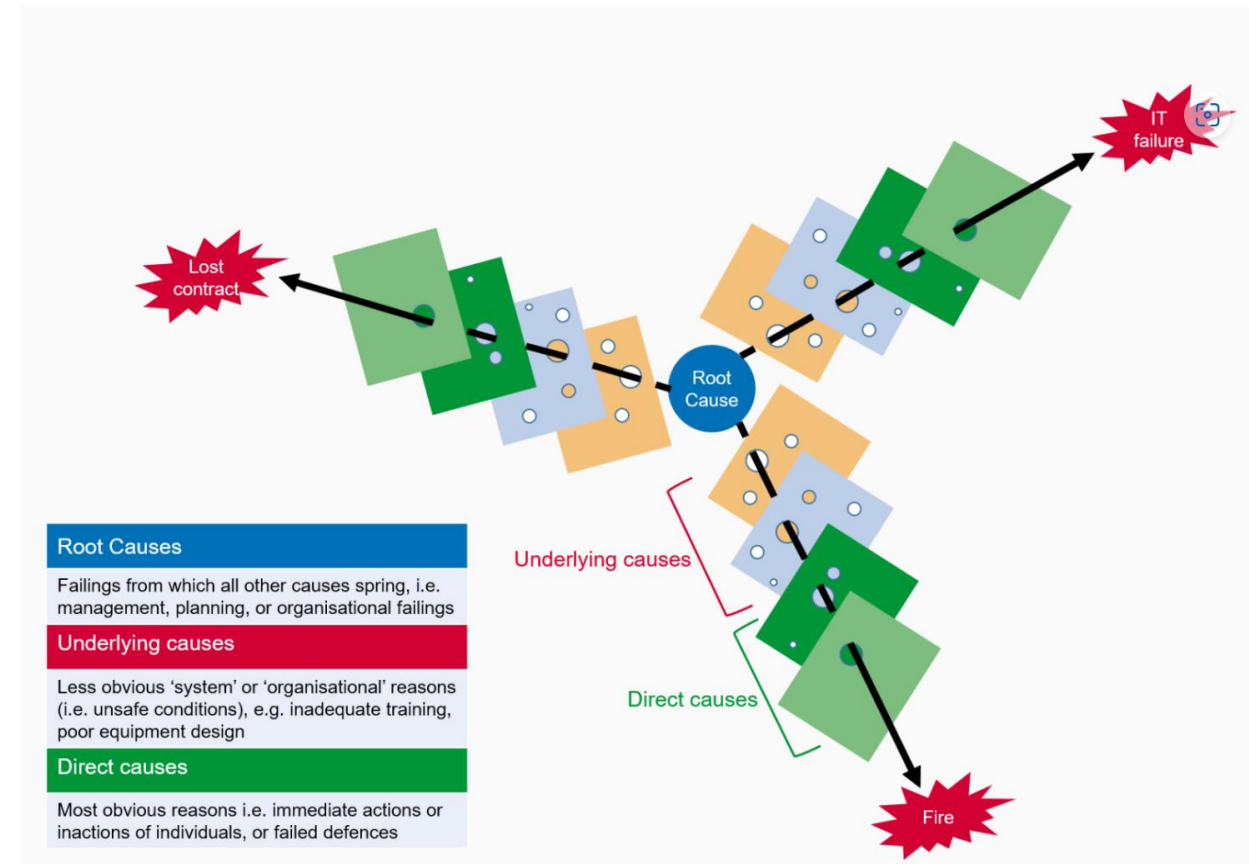
Many investigations make the mistake of raising actions which deal only with the direct causes – a quick fix, putting last-lines-of-defense back in place. By ignoring the root and underlying causes, not only do they miss an opportunity to reduce the risk of recurrence of the incident, but they also leave open the possibility that other, dissimilar incidents may also occur, arising from the same, common root cause



# Steps involved in conducting an incident investigation

## 5. Corrective Actions

Identifying the lessons to be learned from a safety occurrence requires an understanding of not just what happened, but why it happened. Therefore, the investigation should look beyond the obvious causes and aim to identify all the contributory factors, some of which may be related to weaknesses in the system's defenses or other organizational issues.

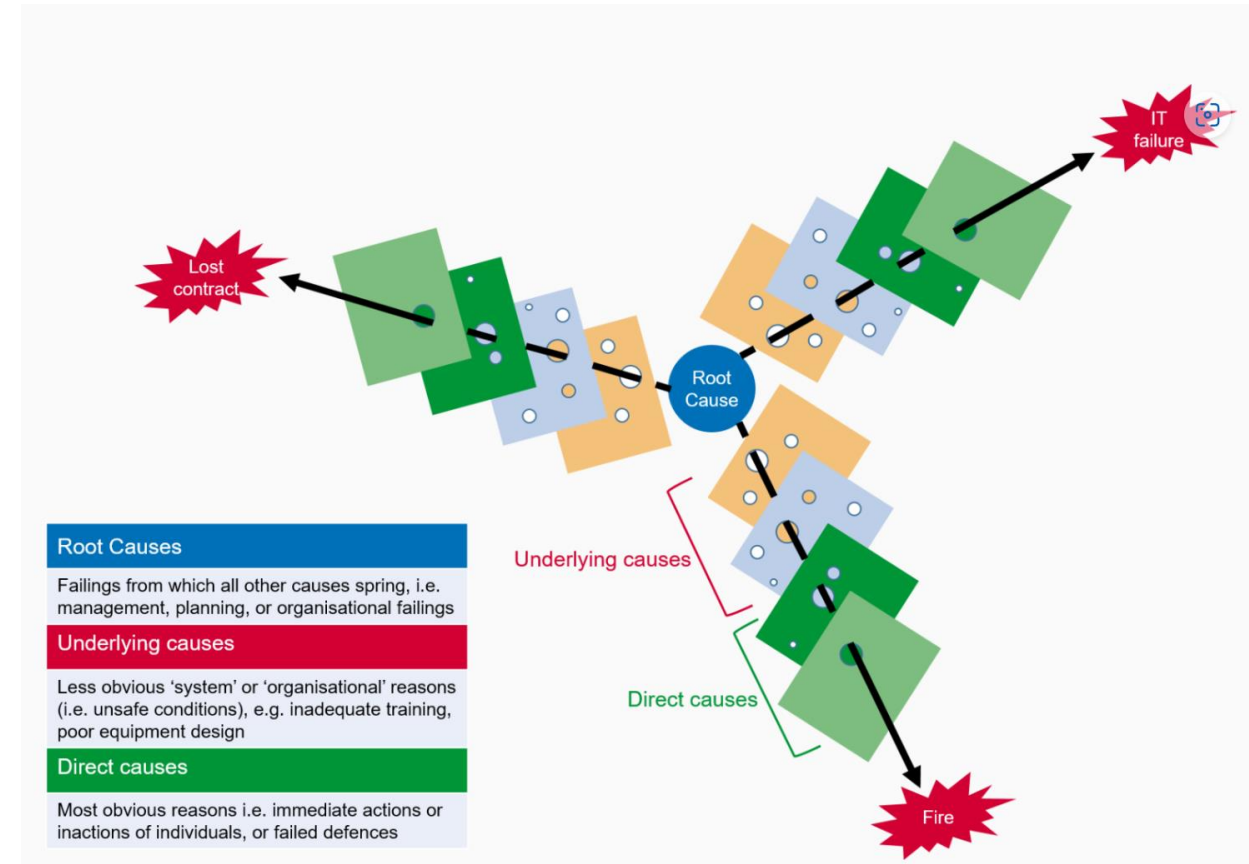


# Steps involved in conducting an incident investigation

## 5. Corrective Actions

**Identification** of safety recommendations and actions to be taken in order to eliminate or mitigate the safety deficiencies identified by the investigation. The safety recommendations are the main product of any occurrence investigation and are made in the final report.

**Communication of safety** messages to those who have the authority to implement the safety recommendations and to the aviation community in general by means of safety information exchange and lesson dissemination.



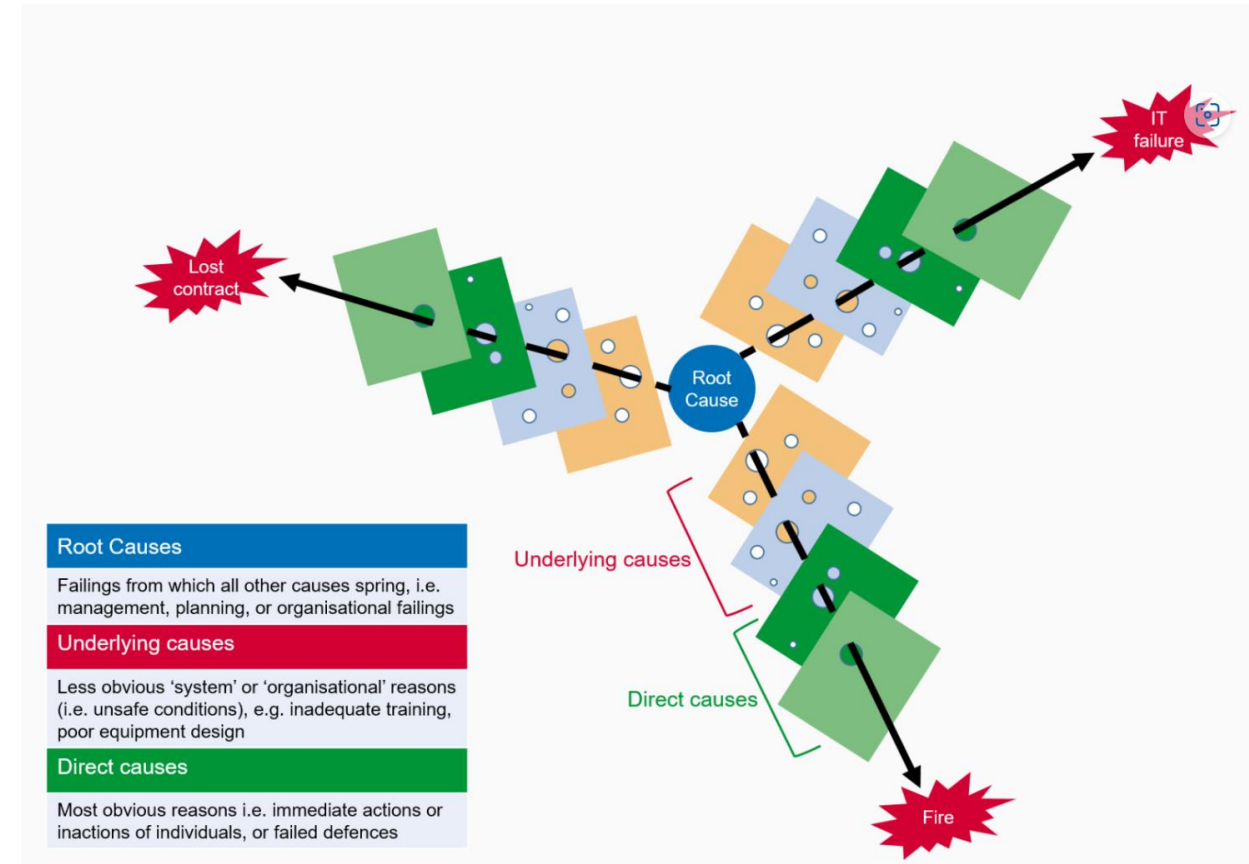


# Steps involved in conducting an incident investigation

## 5. Corrective Actions

For maximum effectiveness, the outcome of the investigation should focus on determining hazards and risks and not on identifying individuals to blame and punish.

The way the investigation is conducted **influences** the overall **safety culture** in the aviation service provider organization.

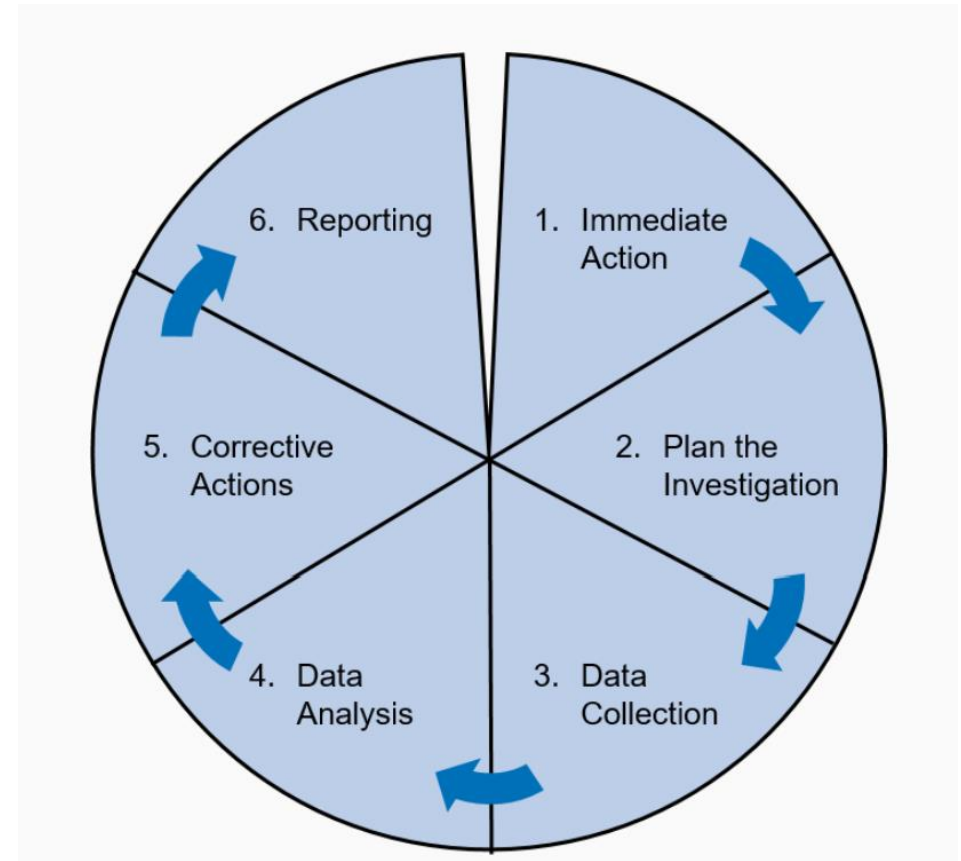


# Steps involved in conducting an incident investigation

---

## 6. Reporting

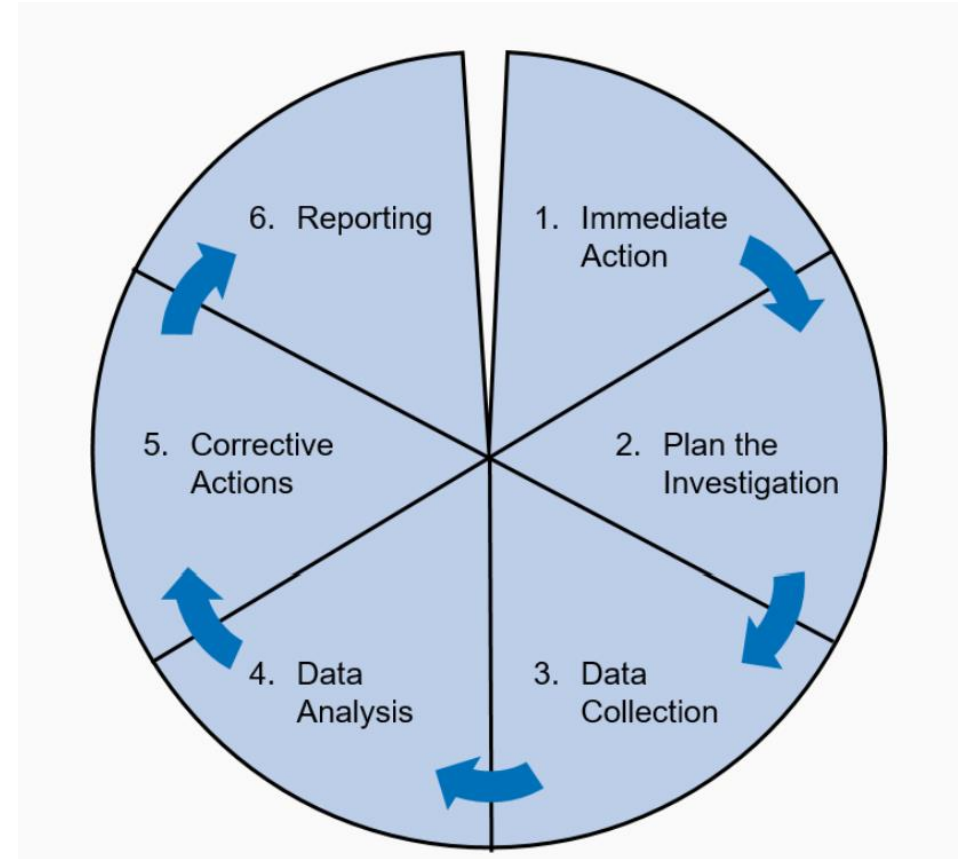
Following the in-depth analysis phase, consolidating all the findings into a comprehensive and coherent report is crucial. This report is the official record of the incident, its investigation, and the derived conclusions. It facilitates communication about the incident and can serve as a valuable tool for future reference and learning.



# Steps involved in conducting an incident investigation

## 6. Reporting

**Compilation of Facts:** The report should start by laying out all the facts about the incident. This includes the date, time, location, personnel involved, description of the incident, and a record of any injuries or damage sustained. In this section, the investigator should stick to the facts, avoiding speculation or subjective interpretation.

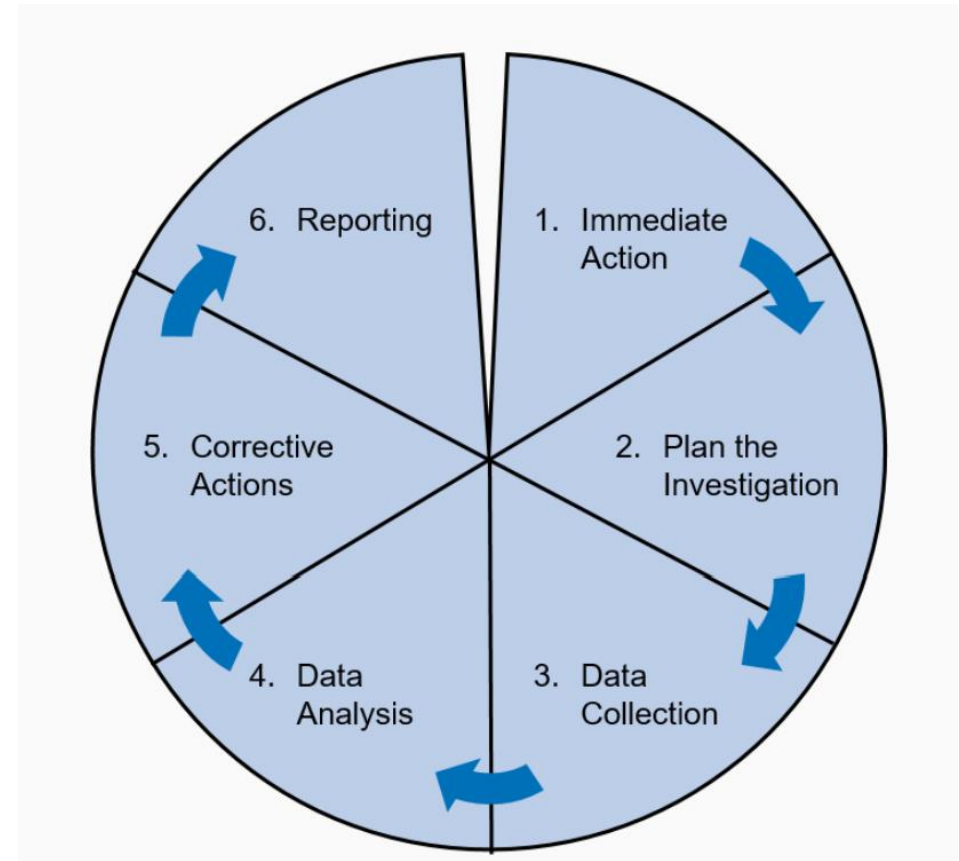


# Steps involved in conducting an incident investigation

---

## 6. Reporting

**Summary of Findings:** This section of the report outlines the key findings from the investigation. It should provide a clear and concise overview of what occurred, drawing on the chronological and logical analyses conducted. This summary should be easy to understand, even for individuals not involved in the investigation, and should avoid technical jargon wherever possible.



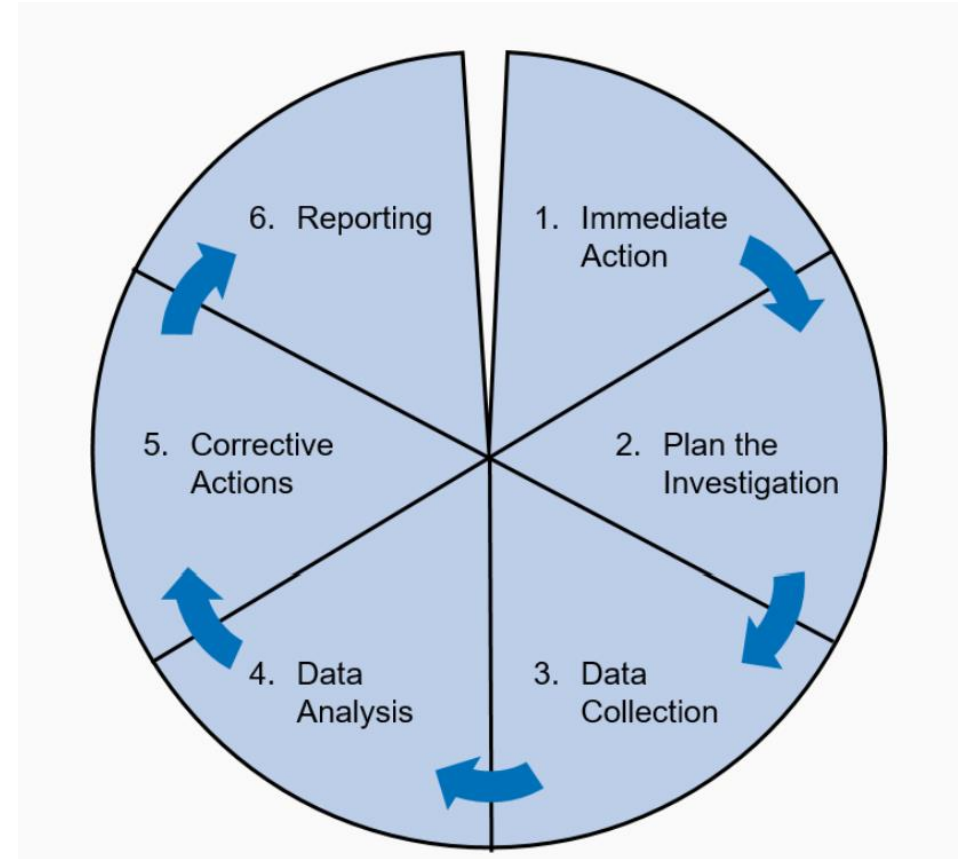
# Steps involved in conducting an incident investigation

---

## 6. Reporting

### **Conclusion and Probable Cause:**

The report should clearly state the investigator's conclusions based on the analyzed data. This includes the identification of the probable cause or causes of the incident. This section must be backed by evidence from the investigation to support its validity.

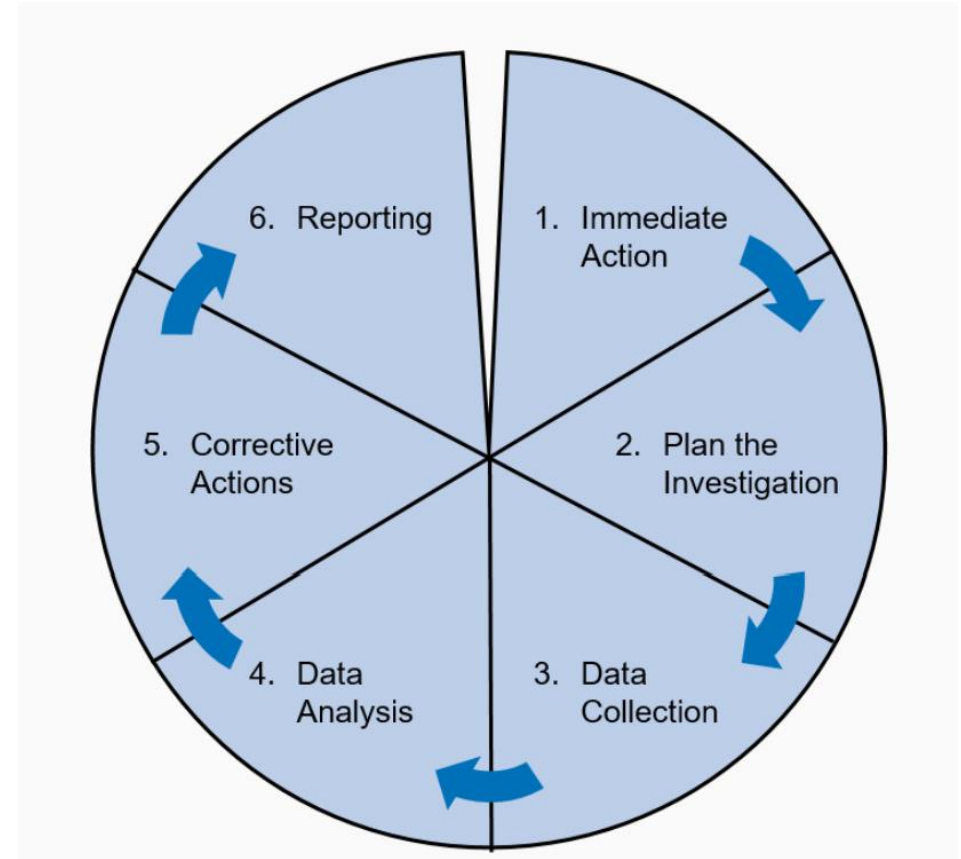


# Steps involved in conducting an incident investigation

---

## 6. Reporting

The investigation process culminates in the sharing of its results and recommendations. The true value of an incident investigation lies not just in identifying what went wrong but in leveraging that knowledge to enhance safety measures and prevent future incidents.



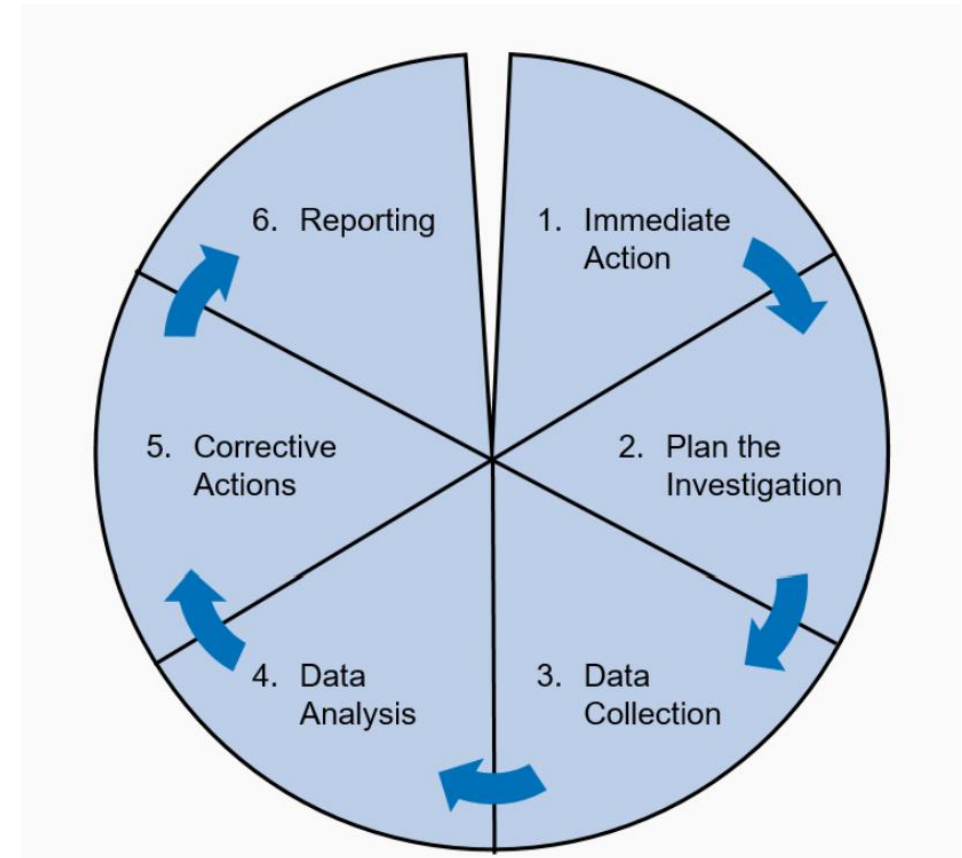


# Steps involved in conducting an incident investigation

## 6. Reporting

### Share The Findings

The first step in sharing the findings is identifying the appropriate audiences. This typically includes all relevant stakeholders, from the management team responsible for implementing changes to the workers who can benefit from a deeper understanding of safe practices

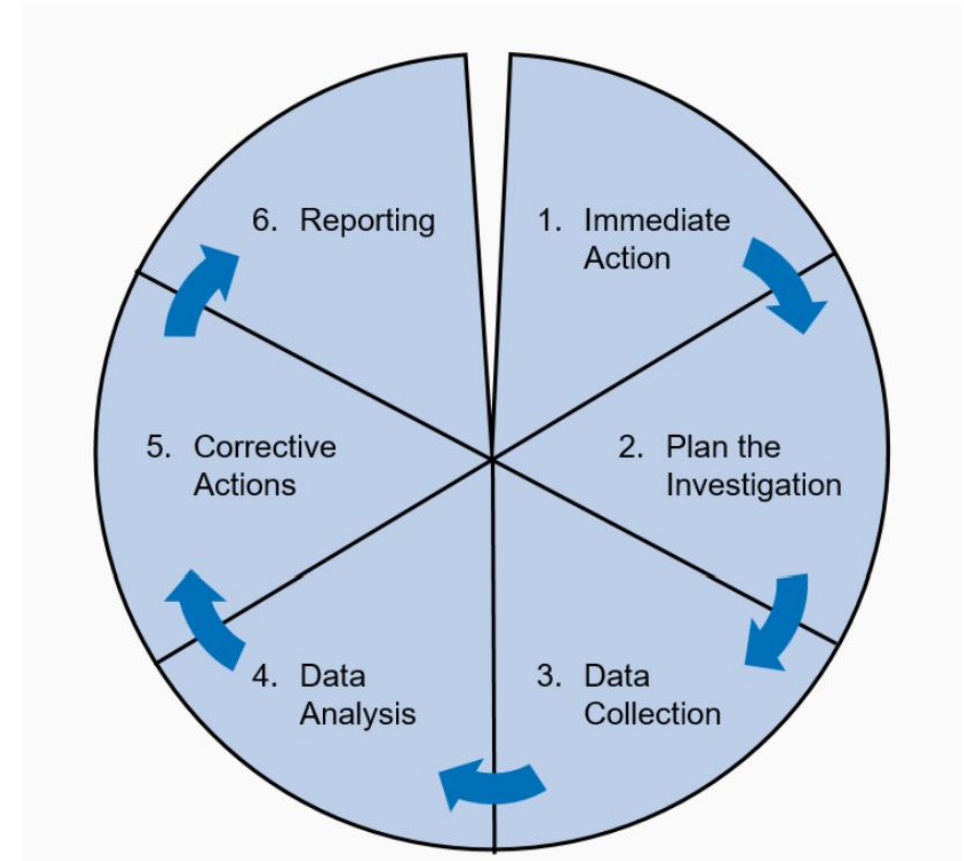


# Steps involved in conducting an incident investigation

## 6. Reporting

### Share The Findings

The next step involves disseminating the investigation results. This could take several forms, such as written summaries, visual presentations, or verbal briefings, and should be tailored to best suit the audience. Regardless of the format, the communication should clearly articulate the conditions and contributing factors that led to the incident and the necessary changes or recommendations to prevent a similar occurrence.



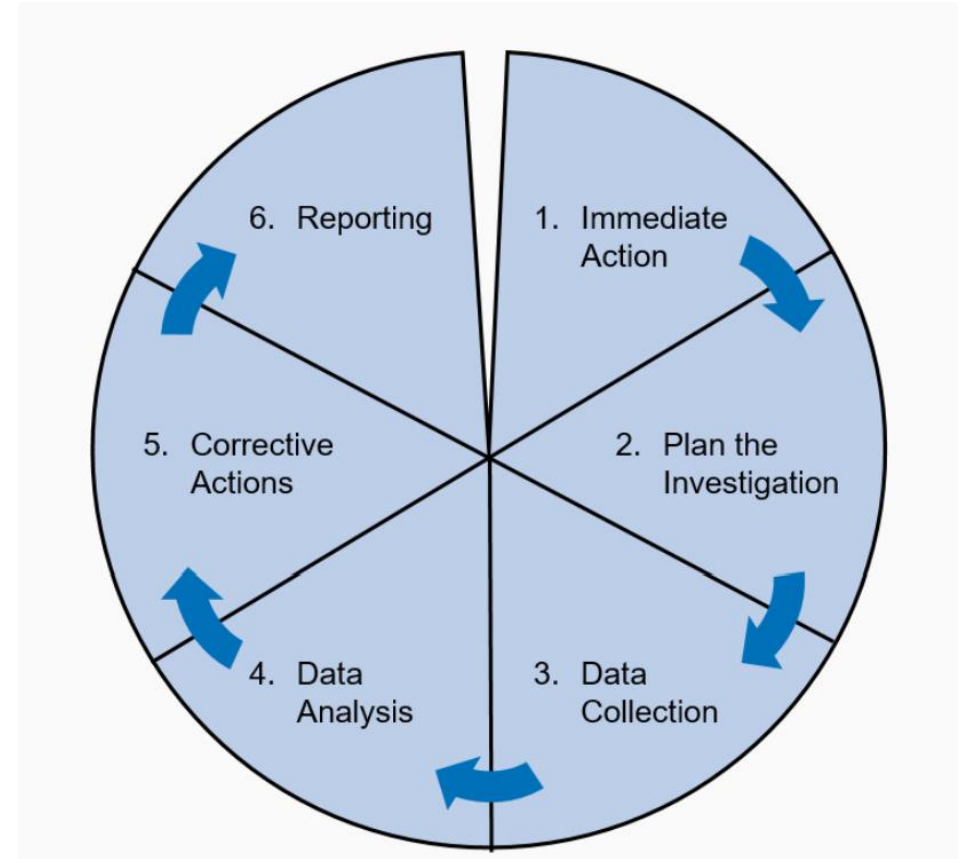


# Steps involved in conducting an incident investigation

## 6. Reporting

### Share The Findings

Sharing the results of an investigation is a powerful tool to enhance safety culture within an organization. It demonstrates the company's commitment to safety and transparency, reinforces the importance of safe practices, and motivates employees to prioritize safety in their daily operations. Additionally, it empowers workers with the knowledge and understanding to make safer choices and take appropriate action in potential risk situations.

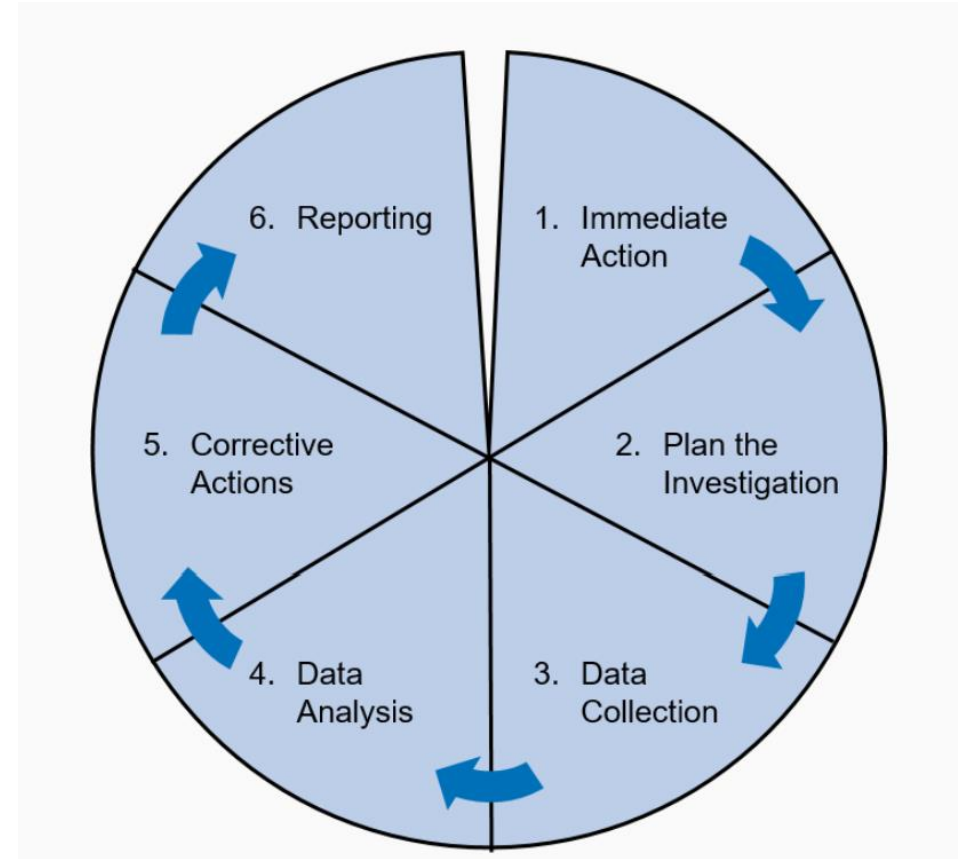


# Steps involved in conducting an incident investigation

## 6. Reporting

### Implementation Of Changes

The final stage in the incident investigation process is the implementation of changes based on the investigation's findings and recommendations. This proactive step is critical in preventing the recurrence of similar incidents and continually improving the overall safety of the workplace.



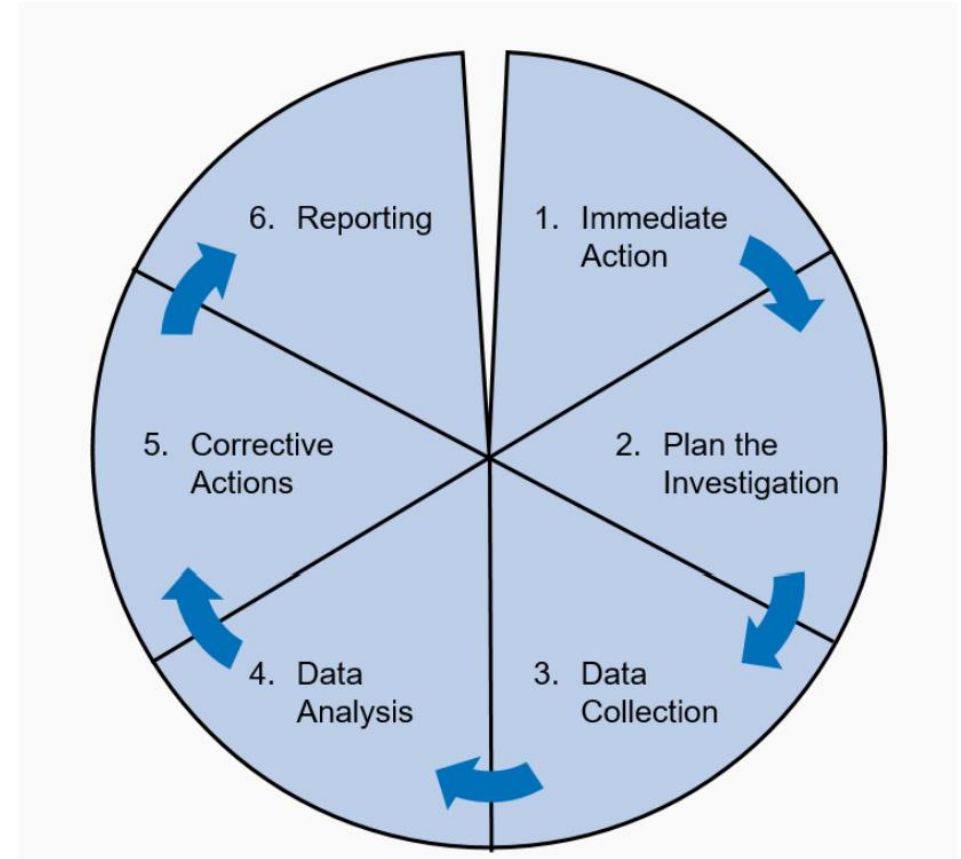
# Steps involved in conducting an incident investigation

## 6. Reporting

### **Action Plan Development:**

The first part of this stage involves developing an action plan based on the investigator's recommendations. The plan should clearly outline the necessary changes to policies, procedures, training, equipment, or any other operational aspect identified as contributing factors to the incident.

This might involve changes to work procedures, improvements in training programs, or even changes in the organizational culture toward safety.

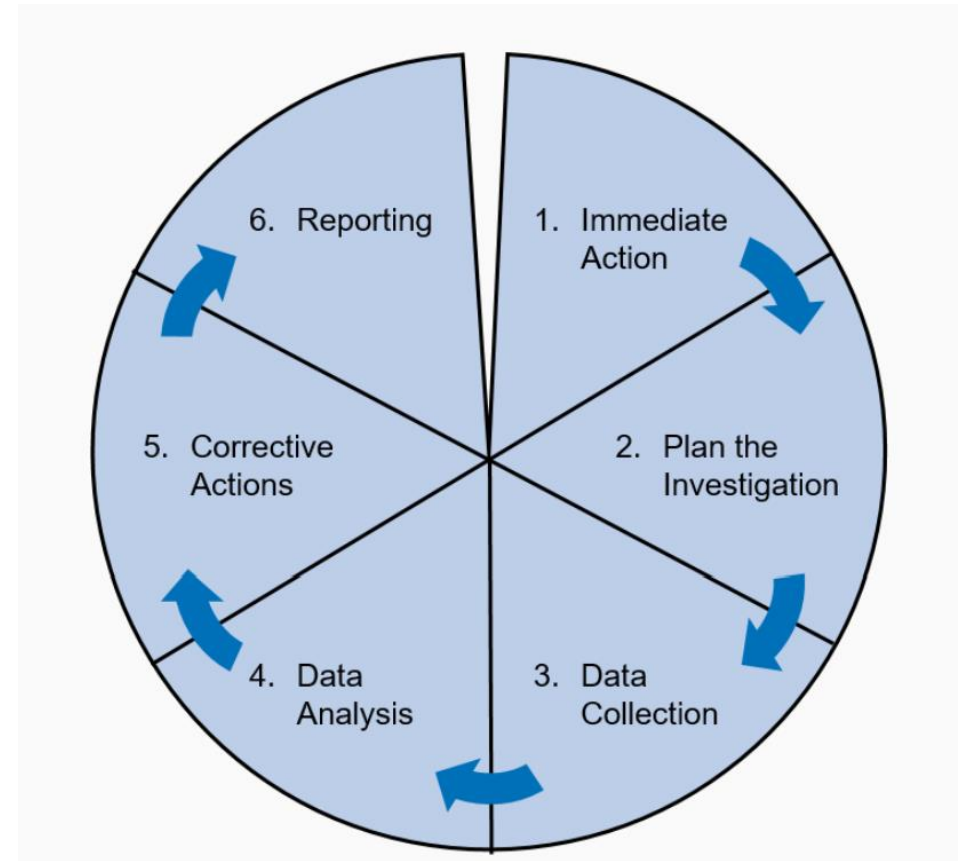


# Steps involved in conducting an incident investigation

## 6. Reporting

### Implementation Of Changes

Once the action plan is ready, the next step is the actual execution of the changes. This may require resources such as time, personnel, and budget, so proper planning and allocation of resources are essential. Management plays a critical role here, as they must oversee the implementation, provide the necessary support, and ensure that everyone understands their role in the new processes.

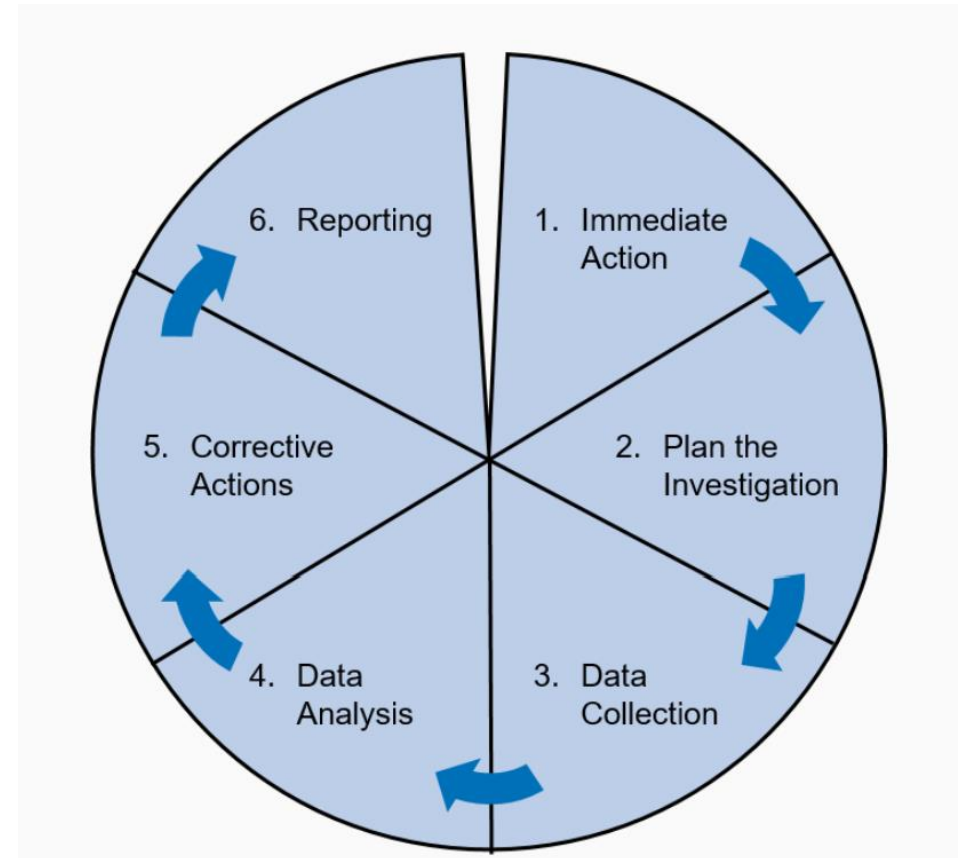


# Steps involved in conducting an incident investigation

## 6. Reporting

### **Follow-Up And Monitoring**

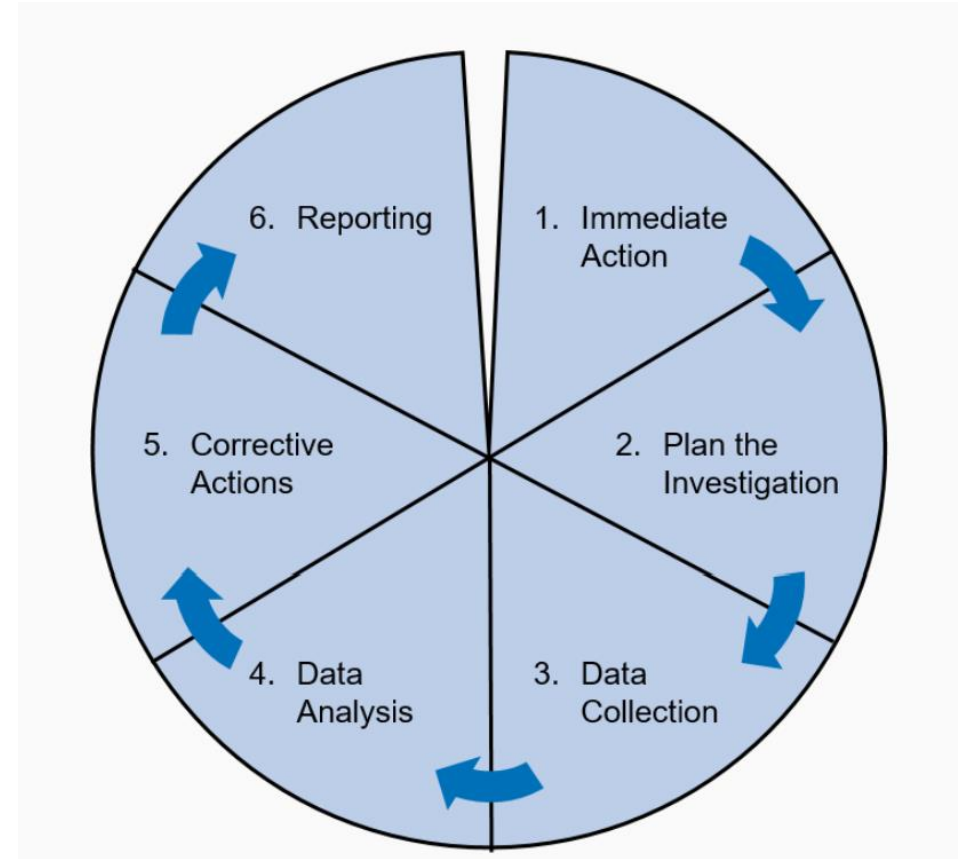
Making changes is not a one-time activity but an ongoing process. Regular monitoring and follow-ups are necessary to ensure that the implemented changes are effective and are being adhered to. This might involve periodic safety audits, continuous training and retraining of staff, and open communication lines for employees to raise safety concerns. It's also essential to review the effectiveness of the changes made periodically and adjust as necessary for continuous improvement.





# Steps involved in conducting an incident investigation

The ultimate aim of all these steps is to **transform** the unfortunate occurrence of an incident into a **learning experience** that strengthens the organization's safety culture. The changes made due to an investigation should **contribute** to a safer, more aware, and more responsible work environment, thus ensuring that the **resources invested** in the incident investigation translate into meaningful, **long-term benefits**.



# Root cause analysis techniques

---

Root cause analysis (RCA) techniques are used to identify the underlying causes of problems or incidents. They help organizations understand the fundamental reasons behind an issue and develop effective corrective actions.

RCA tools can be very simple or very complex depending on the scope of the investigation, there isn't a best or worst tool, their effectiveness mainly depends on the correct or incorrect use of the tool, and understanding of the limitations of each tool

# Root cause analysis techniques

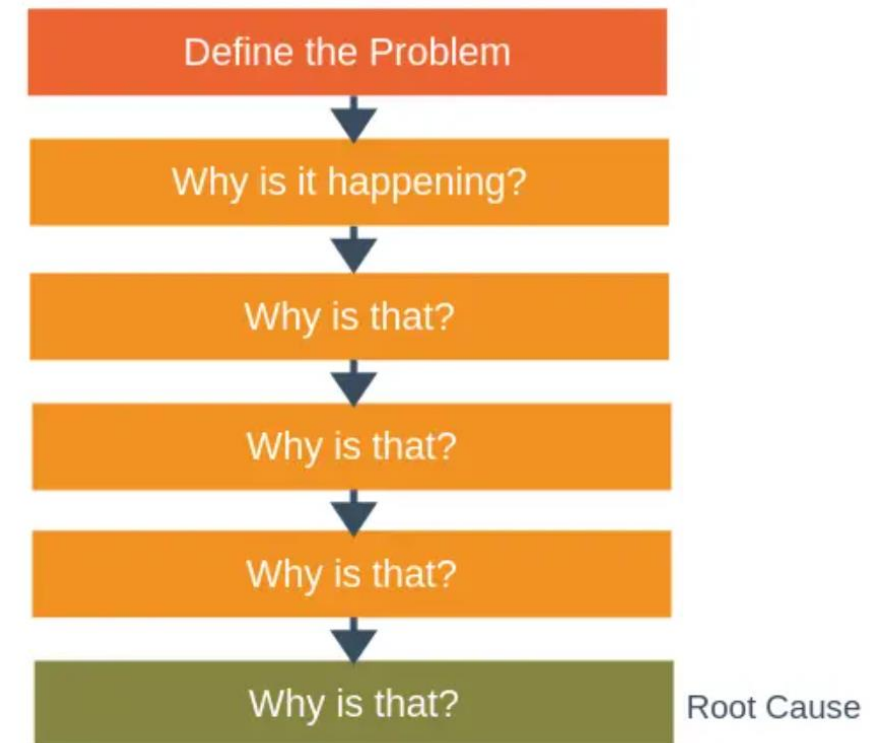
## 5 Whys

This technique involves repeatedly asking "why" to uncover deeper layers of causality. By asking "why" at least five times, you can trace the root cause of the problem. It helps to identify multiple contributing factors and uncover underlying issues that may not be immediately apparent.

You can use 5 Whys for troubleshooting, quality improvement, and problem solving, but it is most effective when used to resolve simple or moderately difficult problems.

Sakichi Toyoda, the Japanese industrialist, inventor, and founder of Toyota Industries, developed the 5 Whys technique in the 1930s. It became popular in the 1970s, and Toyota still uses it to solve problems today.

### The 5 Whys





# Root cause analysis techniques

RCA TOOL	ADVANTAGES	LIMITATIONS
5 Whys	<ul style="list-style-type: none"><li>• Simplicity</li><li>• Cost-Effective</li><li>• Identifying Multiple Causes</li><li>• Focus on Root Causes</li><li>• Engages Cross-functional Teams</li></ul>	<ul style="list-style-type: none"><li>• Subjectivity</li><li>• Incomplete Analysis</li><li>• Lack of Standardization</li><li>• Assumption-based Analysis</li><li>• Limited Scope</li></ul>

# Root cause analysis techniques

---

## **Fishbone Diagram (Ishikawa Diagram)**

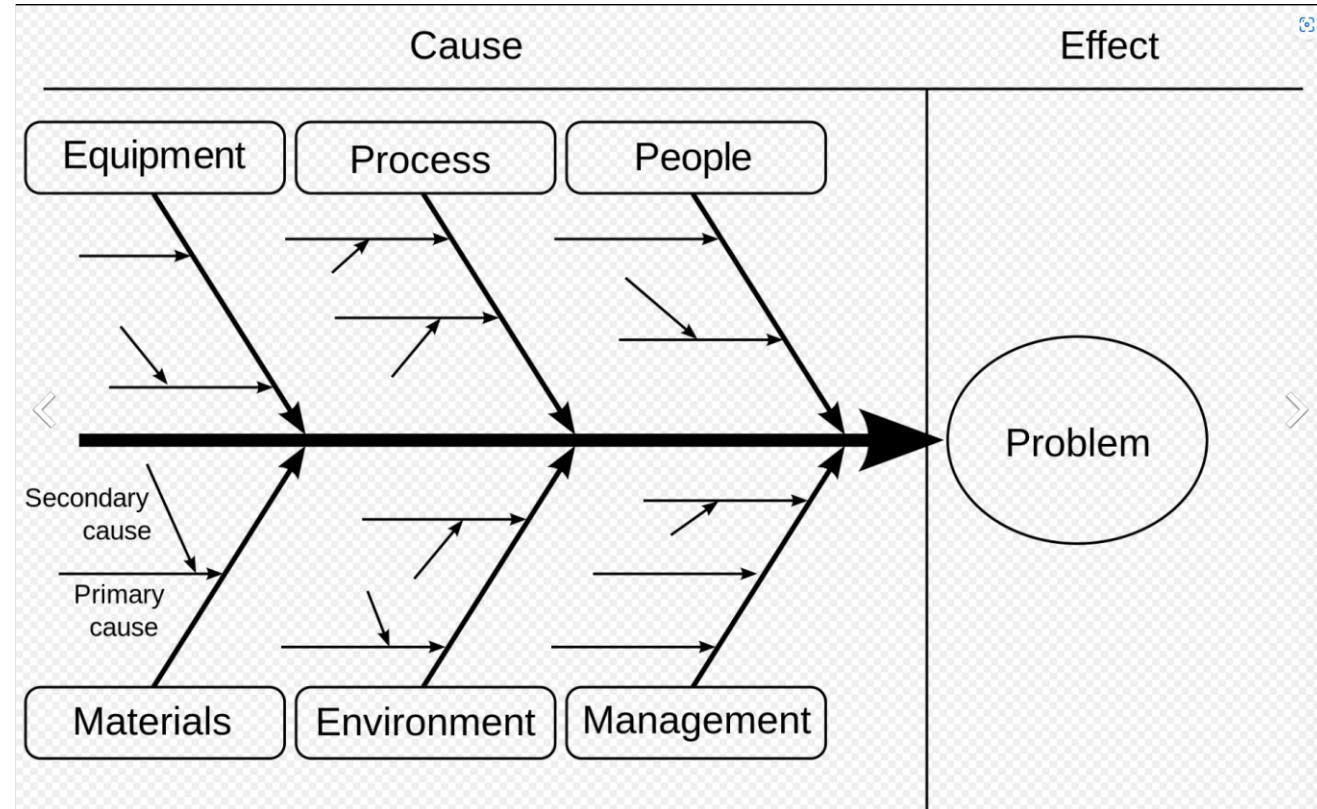
This visual tool helps identify potential causes by categorizing them into different factors or categories, often referred to as the 6 Ms (Manpower, Methods, Machines, Materials, Measurement, and Environment). It provides a structured approach to brainstorming and analyzing the causes of a problem.

Ishikawa diagrams were popularized in the 1960s by Kaoru Ishikawa, who pioneered quality management processes in the Kawasaki shipyards, and in the process became one of the founding fathers of modern management.

# Root cause analysis techniques

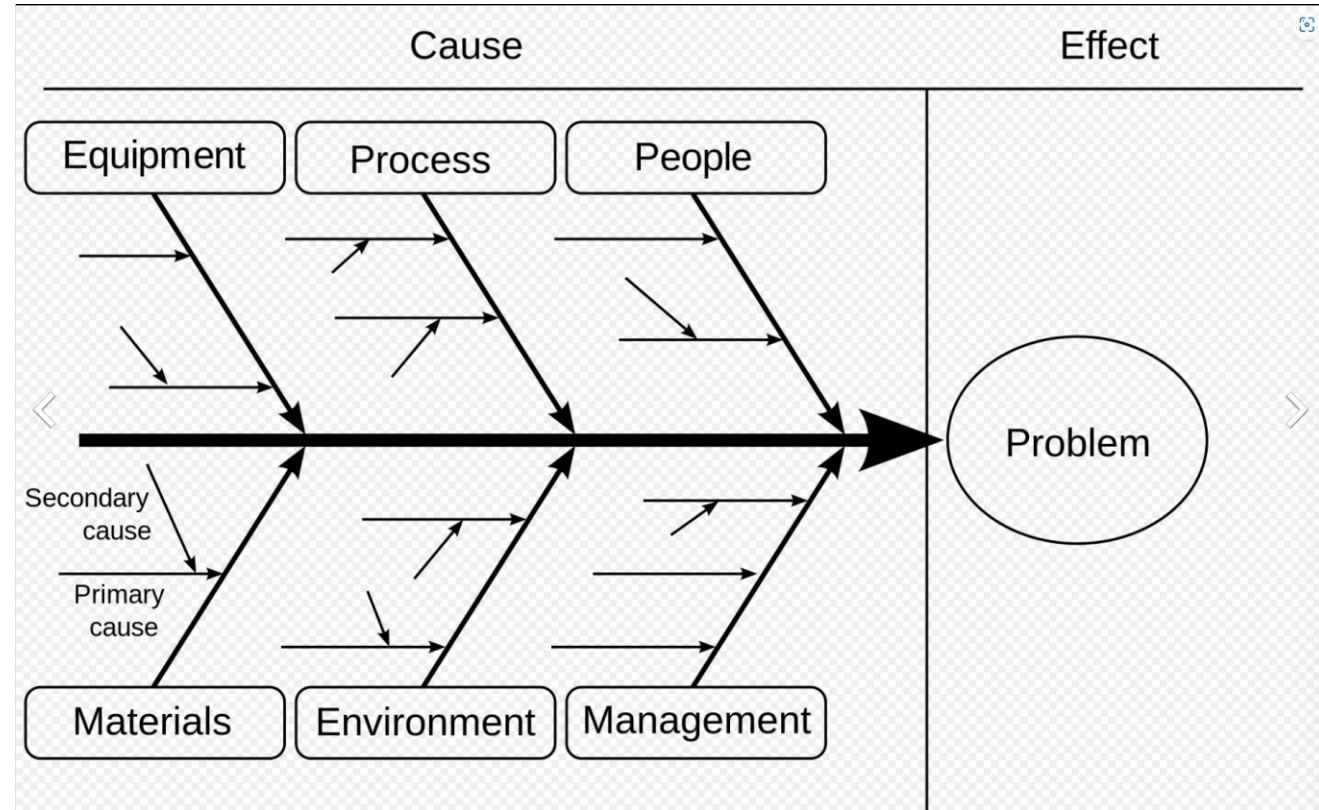
These diagrams have:

- A “head,” which is your hazard/risk event;
- 4-6 “fins” which are the categories that you are using to organize root causes of a safety event (e.g., Man, Machine, Mission, Management, etc.);
- Fins can be a predefined model, such as 5-M or SHELL, or a custom model created by you;
- Each fin will have multiple “branches”; and
- Each branch may or may not have sub-branches.



# Root cause analysis techniques

Filling out these diagrams simply involves looking at the safety issue from the perspective of each fin (category) and establishing the relevant factors (branches). Next, for each branch, establish the reasons (sub-branches) that the branch exists. These sub-branches are usually your root causes.



# Root cause analysis techniques

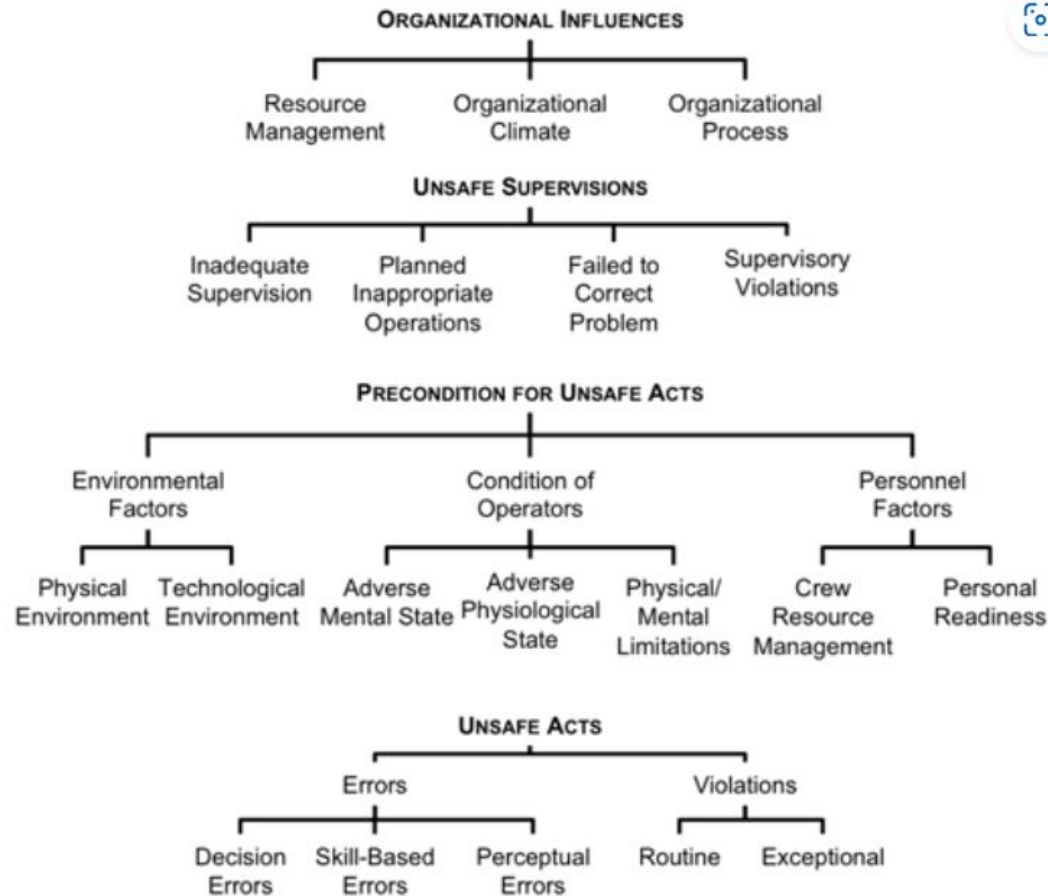
RCA TOOL	ADVANTAGES	LIMITATIONS
Fishbone Diagram	<ul style="list-style-type: none"><li>• Visual Representation</li><li>• Comprehensive Analysis<ul style="list-style-type: none"><li>• Team Collaboration</li></ul></li><li>• Identifying Root Causes<ul style="list-style-type: none"><li>• Documentation and Communication</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Simplified Relationships<ul style="list-style-type: none"><li>• Subjectivity</li></ul></li><li>• Lack of Quantification<ul style="list-style-type: none"><li>• Limited Scope</li><li>• Time and Effort</li></ul></li></ul>

# Root cause analysis techniques

## Human Factors Analysis and Classification System (HFACS)

The Human Factors Analysis and Classification System (HFACS) is a framework used to analyze and understand human factors in accidents and incidents.

It is specifically designed to identify and categorize the underlying human factors that contribute to safety-related events. HFACS provides a systematic approach to examining human performance in complex systems and helps identify areas for improvement in order to prevent future incidents.

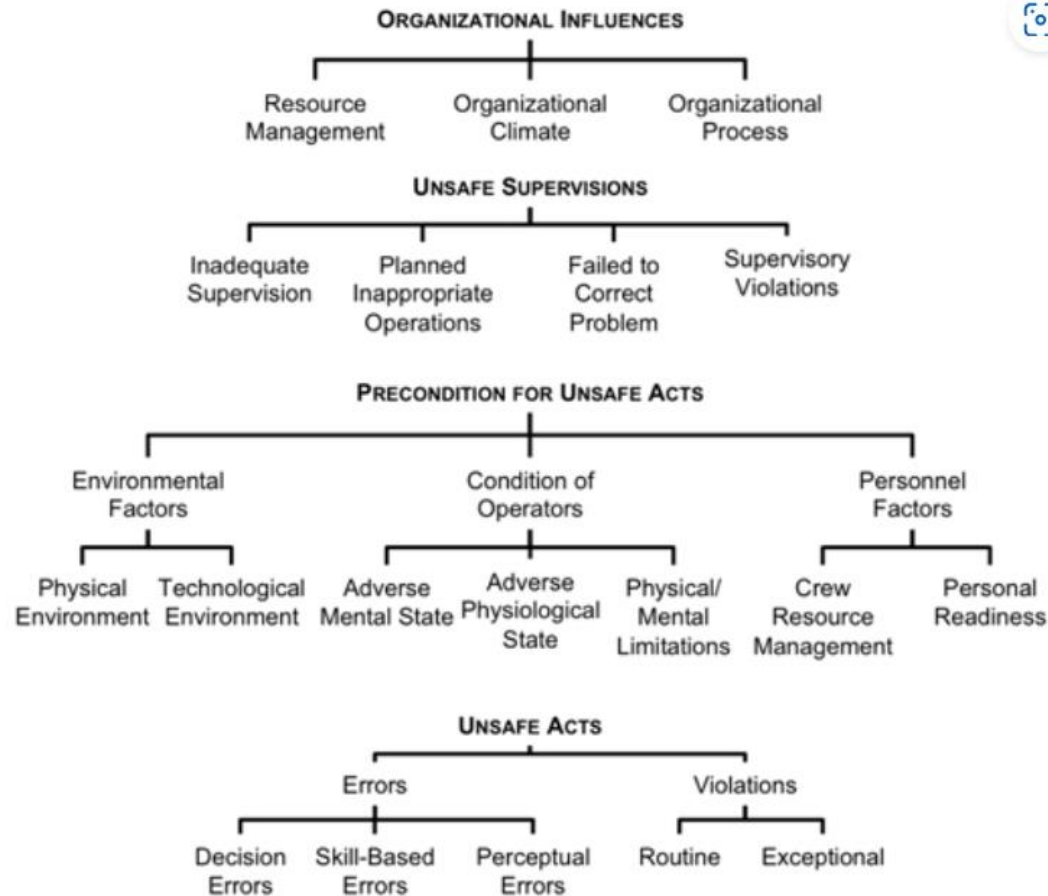


# Root cause analysis techniques

## Human Factors Analysis and Classification System (HFACS)

The key components of the HFACS framework include:

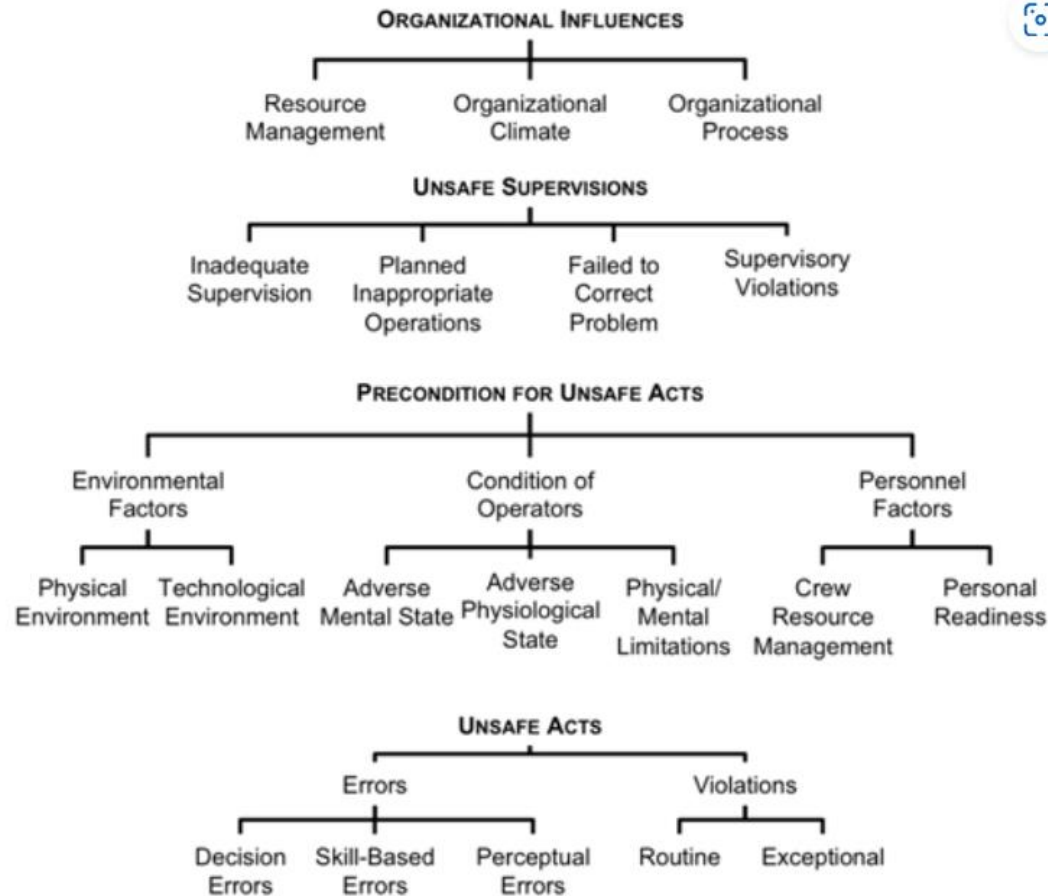
1. Unsafe Acts
2. Preconditions for Unsafe Acts
3. Supervision
4. Organizational Influences



# Root cause analysis techniques

## Human Factors Analysis and Classification System (HFACS)

The HFACS framework helps identify not only the immediate causes or actions leading to accidents but also the deeper underlying factors that contribute to human error or unsafe behavior. By analyzing accidents and incidents through the lens of HFACS, organizations can gain insights into the systemic issues and develop strategies to improve human performance, enhance safety, and prevent future incidents.





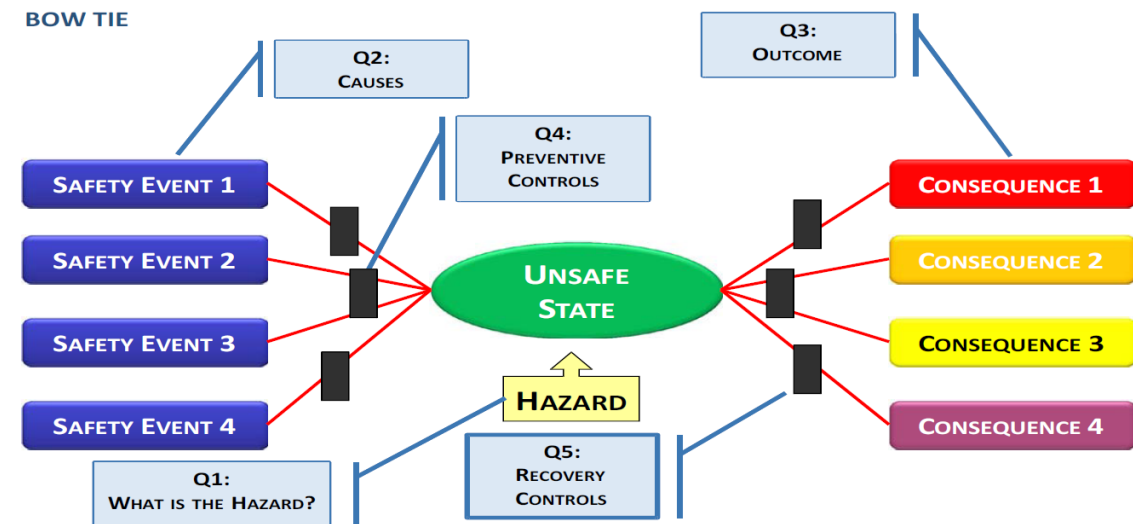
# Root cause analysis techniques

RCA TOOL	ADVANTAGES	LIMITATIONS
HFACS	<ul style="list-style-type: none"><li>• Comprehensive Analysis</li><li>• Focus on Human Factors<ul style="list-style-type: none"><li>• Causal Analysis</li><li>• Actionable Insights</li></ul></li><li>• Application in Multiple Industries</li></ul>	<ul style="list-style-type: none"><li>• Complexity of Analysis<ul style="list-style-type: none"><li>• Subjectivity</li></ul></li><li>• Overemphasis on Individual Factors</li><li>• Limited Predictive Capability</li><li>• Resource and Training Requirements</li></ul>

# Root cause analysis techniques

## Bowtie Analysis

Is traditionally considered a comprehensive analysis solution, as it establishes everything from root causes to final consequences. Because bowtie analysis is so thorough, it can be time-consuming and abstruse. However, there is no reason organizations can't use only the "left side" of the bowtie to establish a timeline of all contributing events from root causes to hazardous conditions.

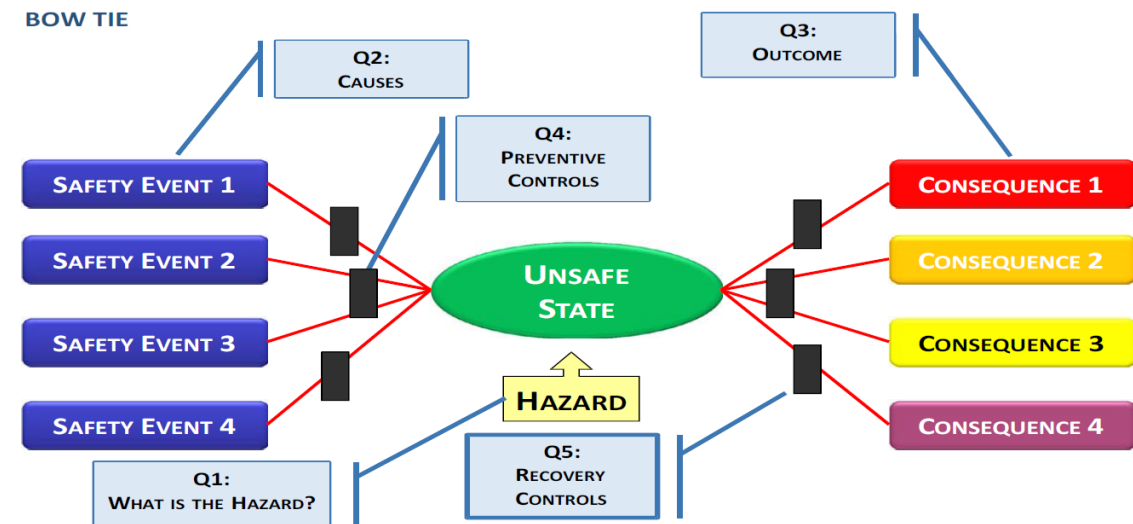


# Root cause analysis techniques

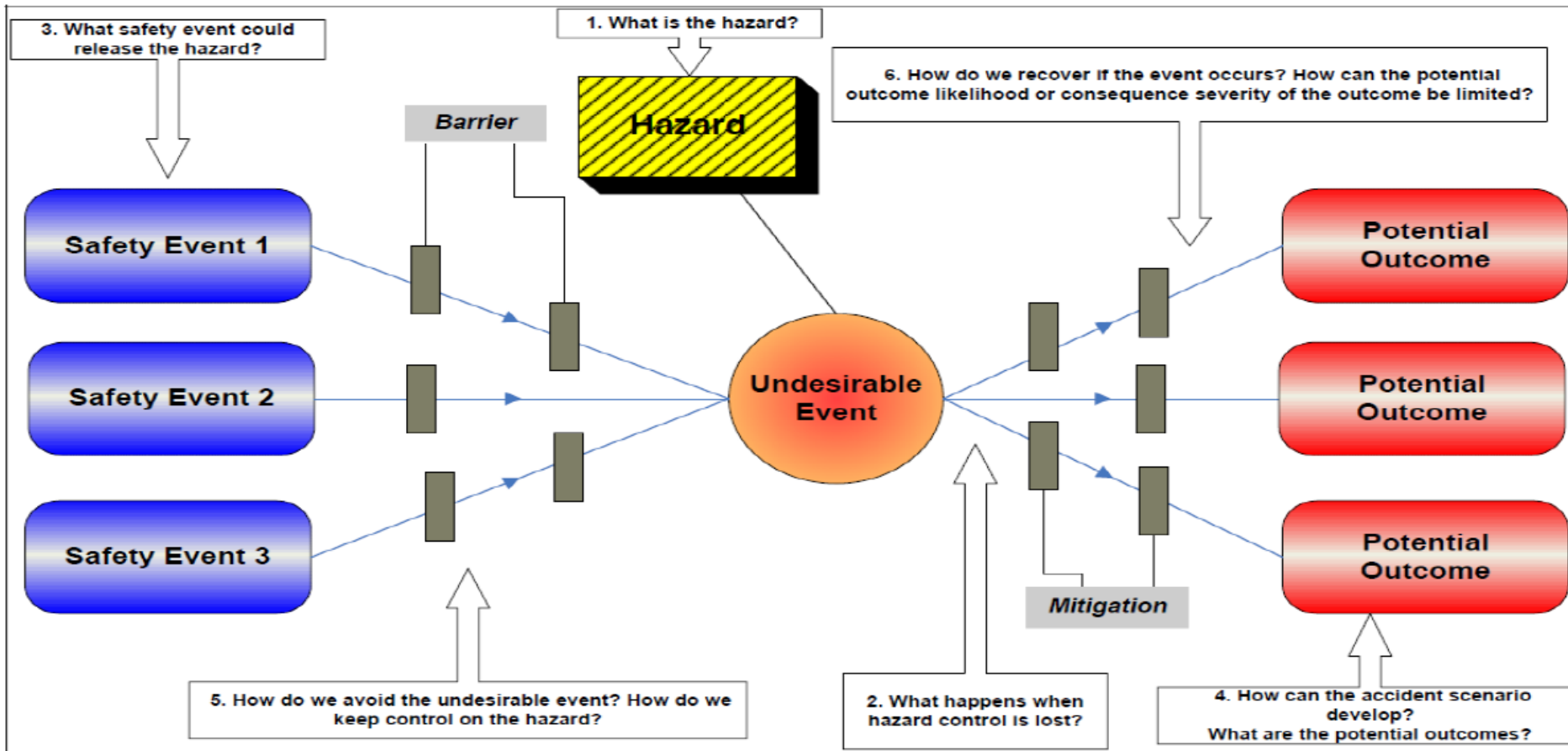
## Bowtie Analysis

Performing bowtie analysis for root causes is somewhat similar to 5 whys analysis:







- Establish hazardous condition;
- Ask “Why did this happen?” and list the preceding event(s);
- For each preceding event ask, “And why did this happen?” – once again, list the preceding events; and
- Like the 5 whys, when your answer is “just because,” you have arrived at a root cause.



# Root cause analysis techniques



# Root cause analysis techniques

TERM		MEANING
	HAZARD	SOMETHING IN, AROUND OR PART OF THE SYSTEM WHICH HAS THE POTENTIAL TO CAUSE DAMAGE
	UNSAFE STATE (TOP EVENT)	STATE WHEN CONTROL IS LOST OVER THE HAZARD
	SAFETY EVENT (TRIGGERING EVENT)	WHATEVER WILL CAUSE THE UNSAFE EVENT
	BARRIER/MITIGATION	ELEMENTS THAT INTERRUPT THE PROPAGATION SO THAT THE TRIGGERING EVENT DOES NOT RESULT IN A LOSS OF CONTROL OF THE HAZARD OR DO NOT ESCALATE INTO A POTENTIAL OUTCOME.
	CONSEQUENCE	RESULTS FROM THE UNSAFE EVENT
	ESCALATION FACTOR	FACTORS OR CONDITIONS WHICH MAKE A BARRIER/MITIGATION TO FAIL

# Root cause analysis techniques



State when control is lost over the hazard



Also known as **undesired state** or **unsafe event**:

- The **first event** in a chain of negative events **leading to unwanted consequences**
- It is not a catastrophe yet, but now there is exposure to the potential harm of the hazard
- However, it should be possible to bring the situation under control again



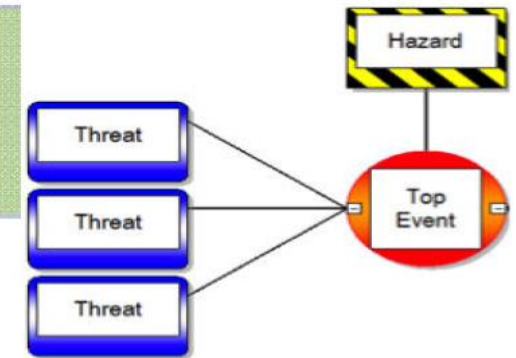
# Root cause analysis techniques

SAFETY  
EVENT

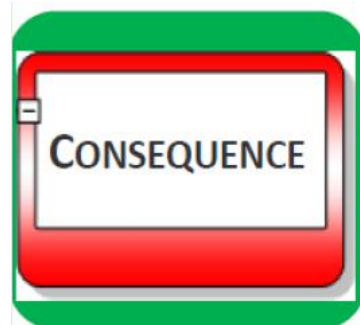
A possible cause that can release the hazard by producing the top event

Also known as threats, causes or triggering events:

- there can be multiple safety events for one top event
- each safety event represents a single scenario that could independently lead to the top event.
- direct means causally direct (not necessarily in terms of time)



# Root cause analysis techniques



An unwanted event resulting from the release of the hazard

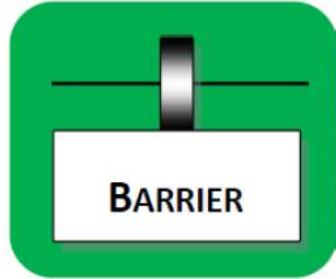


Also known as potential outcomes:

- Consequences are events that are caused by the top event
- What we ultimately want to prevent



# Root cause analysis techniques



Safety barriers are physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents



**Also known as controls or mitigations. There are three different places for barriers :**

- Between a safety event and the top event (**preventive barriers** – also known as **proactive barriers**)
- Between the top event and a consequence (**recovery barriers**, also known as **reactive or defense barriers**)
- Between a barrier and an escalation factor (**escalation factor barriers**)

# Root cause analysis techniques

---

## **Preventive Barriers**

Act against a safety/top event its effect takes place before the top event has happened. It can follow two strategies

- Elimination: Remove the safety event and make sure that there is nothing (or less) to cause the top event
- Prevention: Stop the safety event from becoming a top event, either by blocking the causal effect of the safety event or directly stopping the top event from happening

# Root cause analysis techniques

---

## **Recovery Barriers**

Aimed at regaining control once it is lost (top event has occurred). They act on the likelihood or severity of a potential consequence though:

- Control: Prevents the consequence from happening
- Mitigation: Does not prevent the consequence from happening, but lessens the severity of the consequence

# Root cause analysis techniques



A condition that leads to increased risk by defeating or reducing the effectiveness of a barrier

The following three escalation factor categories can be used :

Human factors: anything a person does to make a barrier less effective

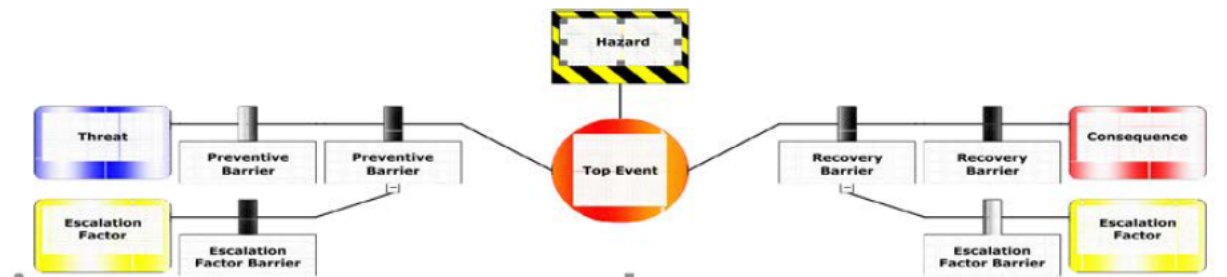
Abnormal conditions: anything in the environment that causes a barrier to be put under strain

Loss of critical services: if a barrier relies on an outside service, losing that service might cause it to lose effectiveness

# Root cause analysis techniques

## ESCALATION FACTORS BARRIERS:

- Barrier that manages the conditions which reduce the effectiveness of other barriers
- Escalation factor barriers are the same concept as all the previously discussed barriers, but now they do not prevent/mitigate a top event or consequence from happening, but they prevent a barrier from failing.
- The same principles that apply to normal barriers also apply to escalation factor barriers



# Root cause analysis techniques

RCA TOOL	ADVANTAGES	LIMITATIONS
Bowtie	<ul style="list-style-type: none"><li>• Visual Representation</li><li>• Comprehensive Risk Assessment</li><li>• Proactive Risk Management<ul style="list-style-type: none"><li>• Communication and Engagement</li></ul></li><li>• Integration with Management Systems</li></ul>	<ul style="list-style-type: none"><li>• Complexity and Expertise</li><li>• Assumptions and Subjectivity</li><li>• Lack of Quantitative Analysis</li><li>• Potential Oversimplification</li><li>• Maintenance and Upkeep</li></ul>



# Root cause analysis techniques

---

## **Causal Analysis using System Theory (CAST)**

The Causal Analysis based on System Theory (CAST) is a method used to conduct a systematic investigation of accidents or incidents. It aims to identify the underlying systemic causes and contributing factors that led to the event.

Because the ultimate goal is to learn how to avoid losses in the future, the causes identified should not be reduced to an arbitrary “root cause.” Instead, the goal is to learn as much from every accident as possible.

Developed by Professor Nancy G. Leveson (MIT), this technique is based on her System Theoretic Accident Model and Processes (STAMP). STAMP is a systems-theory-based model that includes “not only component failure and faults but system design errors and unplanned and unanticipated interactions among components that have not failed.

# Root cause analysis techniques

---

## **Causal Analysis using System Theory (CAST)**

In order to understand CAST and the methodology, some basic terminology is needed

**Accident:** An undesired, unacceptable, and unplanned event that results in a loss. For short, simply a loss.

**System Goals:** The reason the system was created in the first place

**System Constraints:** The ways that the goals can acceptably be achieved

The constraints may conflict with the goals, therefore; system reliability is clearly not synonymous with system safety or security



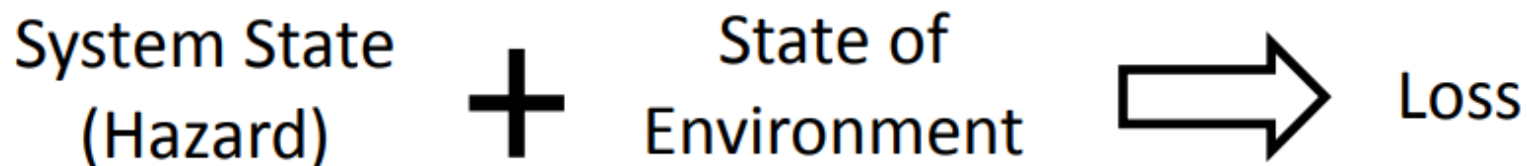
# Root cause analysis techniques

---

## Causal Analysis using System Theory (CAST)

**Incident or Near-Miss:** An undesired, unacceptable, and unplanned event that does not result in a loss, but could have under different conditions or in a different environment

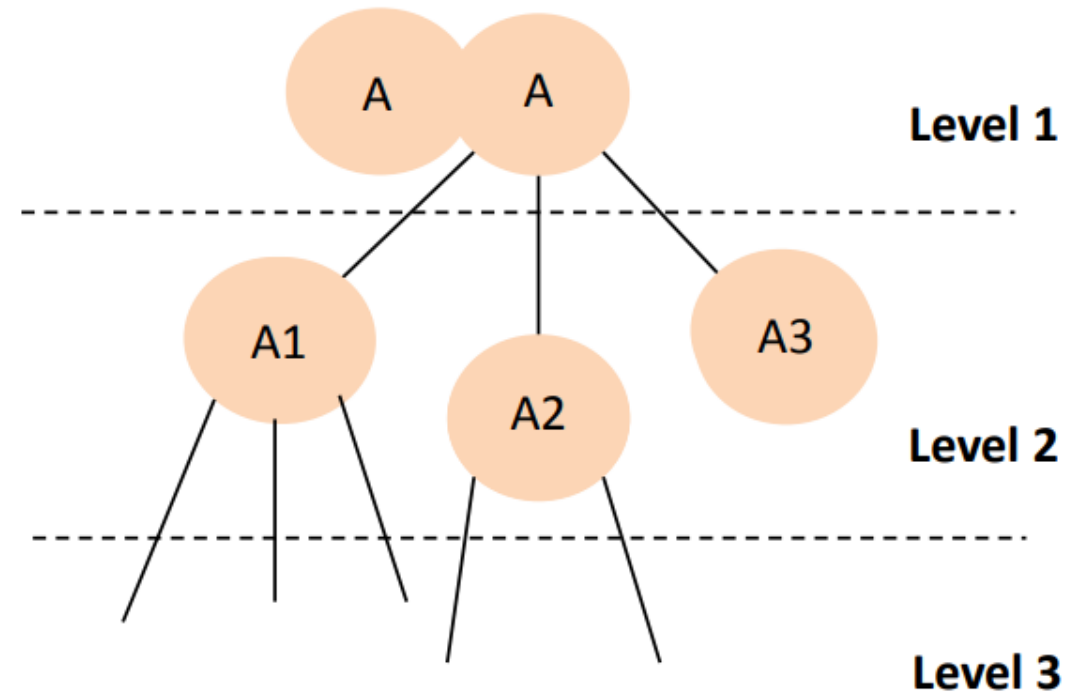
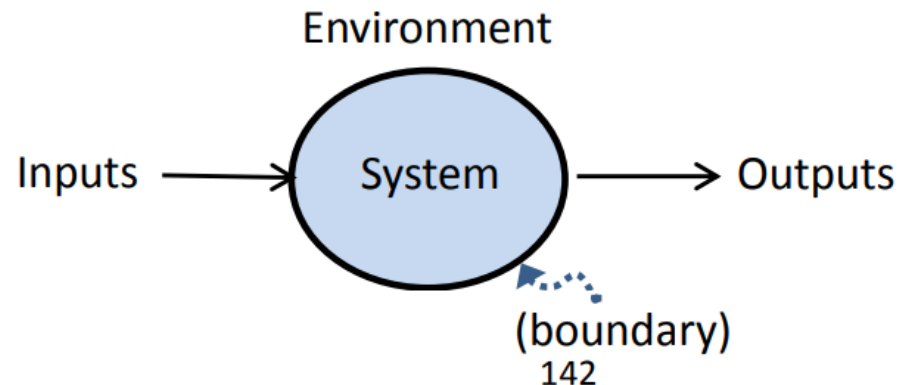
**Hazard or Vulnerability:** A system state or set of conditions that, together with specific environmental conditions, can lead to an accident or loss.



# Root cause analysis techniques

## Causal Analysis using System Theory (CAST)

**System:** A set of things (referred to as system components) that act together as a whole to achieve some common goal, objective, or end.



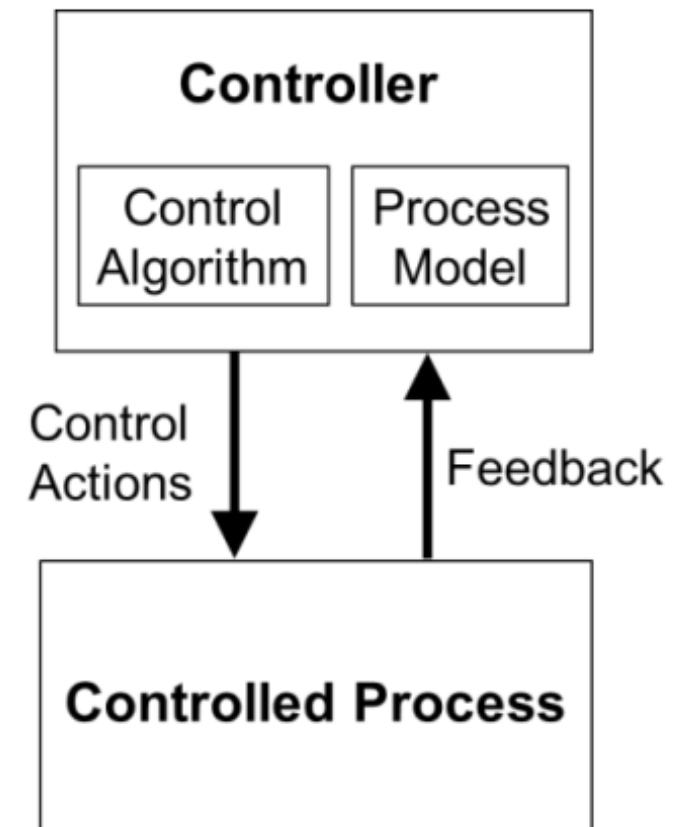
# Root cause analysis techniques

---

## Causal Analysis using System Theory (CAST)

**Control:** A control system is a set of mechanical or electronic devices that regulates other devices or systems by way of control loops.

A control system commands, directs, or regulates the behavior of other devices or processes using control loops. Such control systems may range from a single home heating controller using a thermostat to control a boiler to large industrial control systems used for controlling complex processes and machinery.



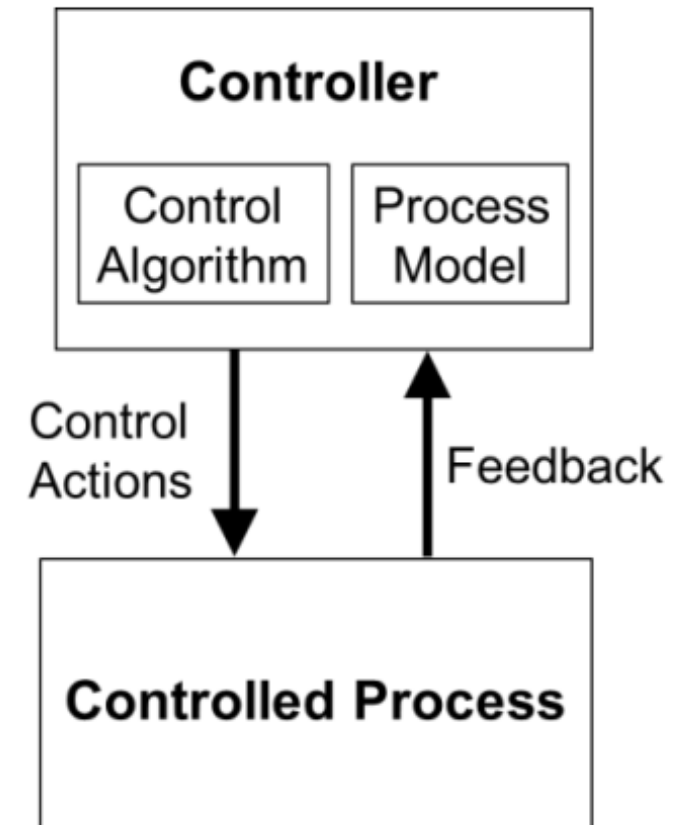
# Root cause analysis techniques

---

## Causal Analysis using System Theory (CAST)

In order to control a process, the controller must have a goal or goals, which can include maintaining constraints on the behavior of the controlled process. In addition, the controller must have some way to affect the behavior of the controlled process.

There are two general operational modes for a control loop: feedback control and feedforward control.



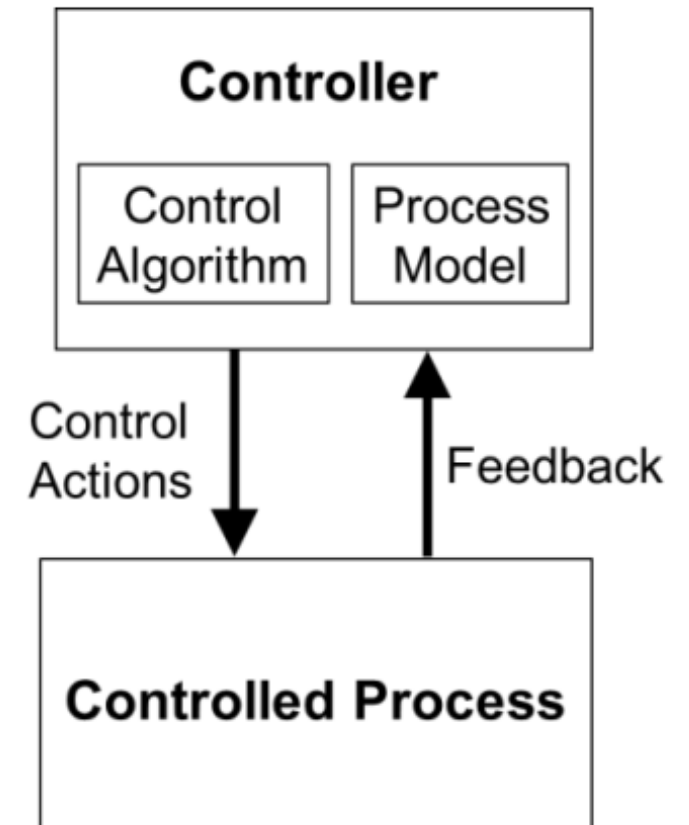
# Root cause analysis techniques

---

## Causal Analysis using System Theory (CAST)

**Feedback control:** The controller uses the process model to decide what control actions to provide, for example, when driving, a driver may read the speedometer (feedback) and decide to brake or step on the accelerator to keep the automobile's speed at a desired level.

**Feedforward control:** The controller uses a model of the current state of the process (in this case the car speed) and the future (operating on an incline) and then provides a control action without specific feedback to identify the need.



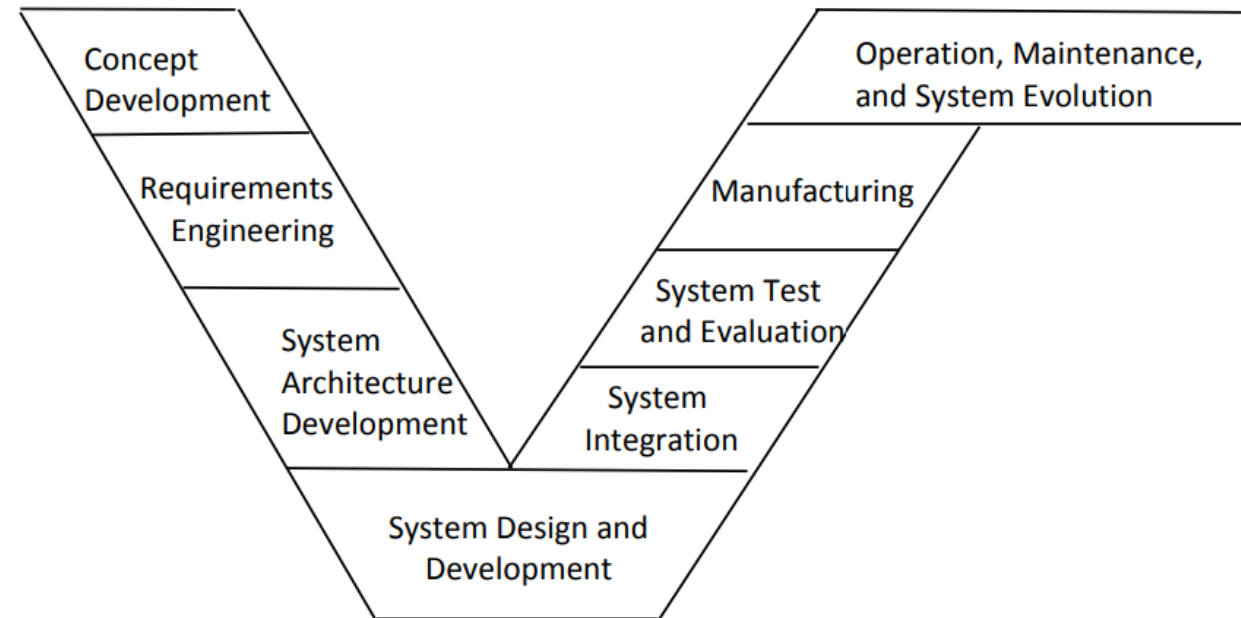
# Root cause analysis techniques

---

## Causal Analysis using System Theory (CAST)

**Systems Engineering:** Is the attempt to put structure into the design and construction of a system in order to improve the results of the engineering effort.

**Systems Theory:** is a set of principles that can be used to understand the behavior of complex systems, whether they be natural or man-made systems



# Learning from incidents and implementing corrective actions

---

**WHY ARE WE NOT  
LEARNING ENOUGH  
FROM INCIDENTS /  
ACCIDENTS?**

# Learning from incidents and implementing corrective actions

---

## Common Problems in Accident Analysis

- Root cause seduction and oversimplification of causes
- Hindsight bias
- Focus on blame
- Narrow view of human error
- Inadequate model of accident causality



# Learning from incidents and implementing corrective actions

---

## Root Cause Seduction

Assuming there is a root cause gives us an illusion of control.

- Usually focus on operator error or technical failures
- Ignore systemic and management factors
- Leads to a sophisticated “whack a mole” game
  - Fix symptoms but not process that led to those symptoms
  - In continual firefighting mode
  - Having the same accident over and over



# Learning from incidents and implementing corrective actions

---

## **Oversimplification of Causes**

Almost always there is:

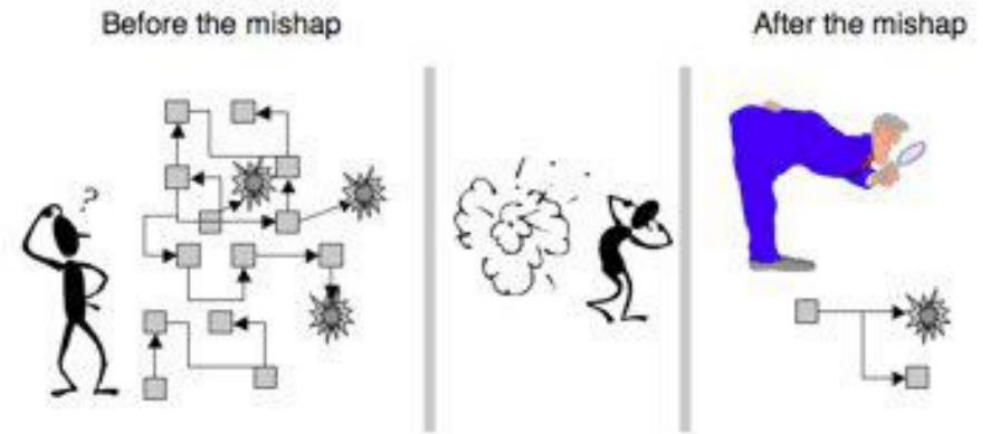
- Operator “error”
- Flawed management decision making
- Flaws in the physical design of equipment
- Safety culture problems
- Regulatory deficiencies

Basically, flaws throughout the safety control structure

# Learning from incidents and implementing corrective actions

## Hindsight Bias

- After an incident
  - Easy to see where people went wrong, what they should have done or avoided
  - Easy to judge about missing a piece of information that turned out to be critical
  - Easy to see what people should have seen or avoided
- Almost impossible to go back and understand how world looked to somebody not having knowledge of outcome
- To learn, need to identify
  - Not what people did “wrong”
  - **But why it made sense for people to do what they did**



Learning from incidents and  
implementing corrective actions

---

**DO OPERATORS  
REALLY CAUSE MOST  
ACCIDENTS?**

# Learning from incidents and implementing corrective actions

---

## Operator Error: Traditional View

- Assumption: Operator error is cause of most incidents and accidents
- So do something about operator involved (fire, retrain, admonish)
- Or do something about operators in general
  - Marginalize them by putting in more automation
  - Rigidify their work by creating more rules and procedures



# Learning from incidents and implementing corrective actions

---

## Operator Error: Systems View

- Human error is a symptom, not a cause
- All behavior affected by context (system) in which occurs
- Role of operators in our systems is changing
  - Supervising rather than directly controlling
  - Systems are stretching limits of comprehensibility
  - Designing systems in which operator error inevitable and then blame accidents on operators rather than designers



# Learning from incidents and implementing corrective actions

---

## Operator Error: Systems View

- To do something about error, must look at system in which people work:
  - Design of equipment
  - Usefulness of procedures
  - Existence of goal conflicts and production pressures
- **Human error is a symptom of a system that needs to be redesigned**



# Learning from incidents and implementing corrective actions

## Blame is the Enemy of Safety

- Goal of the courts is to establish blame
  - People stop reporting errors
  - Information is hidden
  - Learning is inhibited
- Goal of engineering is to understand why accidents occur in order to prevent them





# Learning from incidents and implementing corrective actions

---

[Example from Gerry Bruggink and C.O. Miller]

## WHO

NTSB determined probable cause of this accident was:

1. The flight crew's failure to use engine anti-icing during ground operations and takeoff
2. Their decision to take off with snow/ice on the airfoil surfaces of the aircraft, and
3. The captain's failure to reject the takeoff during the early stage when his attention was called to anomalous engine instrument readings.

## WHY

Contributing Factors:

1. The prolonged ground delay between de-icing and receipt of ATC clearance during which the airplane was exposed to continual precipitation.
2. The known inherent pitch-up characteristics of the B-737 aircraft when the leading edge is contaminated with even small amounts of snow or ice, and
3. The limited experience of the flight crew in jet transport winter operations.

# Learning from incidents and implementing corrective actions

---

- What was the cause of this accident?
- Note the use of the word “failure”
  - A pejorative word: a judgment
  - Assigning blame

The captain's failure to reject the takeoff during the early stage when his attention was called to anomalous engine instrument readings.



# Learning from incidents and implementing corrective actions

---

- What was the cause of this accident?
- Note the use of the word “failure”
  - A pejorative word: a judgment
  - Assigning blame

The captain's failure to reject the takeoff during the early stage when his attention was called to anomalous engine instrument readings.

vs.

The captain did not reject the takeoff during the early stage when his attention was called to anomalous engine instrument readings.

- Accusatory approach to accident analysis (“who”)



# Learning from incidents and implementing corrective actions

---

[Example from Gerry Bruggink and C.O. Miller]

## WHAT

Based on the available evidence, the Accident Board concludes that a thrust deficiency in both engines, in combination with contaminated wings, critically reduced the aircraft's takeoff performance, resulting in a collision with obstacles in the flight path shortly after liftoff.

# Learning from incidents and implementing corrective actions

---

## WHY

### **Reason for the thrust deficiency:**

1. Engine anti-icing was not used during takeoff and was not required to be used based on the criteria for “wet snow” in the aircraft’s operations manual.
2. The engine inlet probes became clogged with ice, resulting in false-high thrust readings.
3. One crew member became aware of anomalies in cockpit indications but did not associate these with engine inlet probe icing.
4. Despite previous incidents involving false thrust readings during winter operations, the regulator and the industry had not effectively addressed the consequences of blocked engine inlet probes.

### **Reason for the wing contamination: ...**

1. Deicing/anti-icing procedures.
2. The crew’s use of techniques that were contrary to flight manual guidance and aggravated the contamination of the wings.
3. ATC procedures that resulted in a 49-minute delay between departure from the gate and takeoff clearance.

# Learning from incidents and implementing corrective actions

---

- Did you get a different view of the cause of this accident?
- Do you now think it was just flight crew “failures”? Are there other factors?

Accusatory:

Who

Why

Explanatory:

What

Why

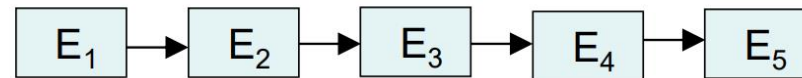


- Do you think the recommendations will be different?

# Learning from incidents and implementing corrective actions

## Use of Inappropriate Accident Models

- Identifies how we learn from and try to prevent accidents
- Linear “chain of failure events” is used today



Each event is the direct result of the preceding event

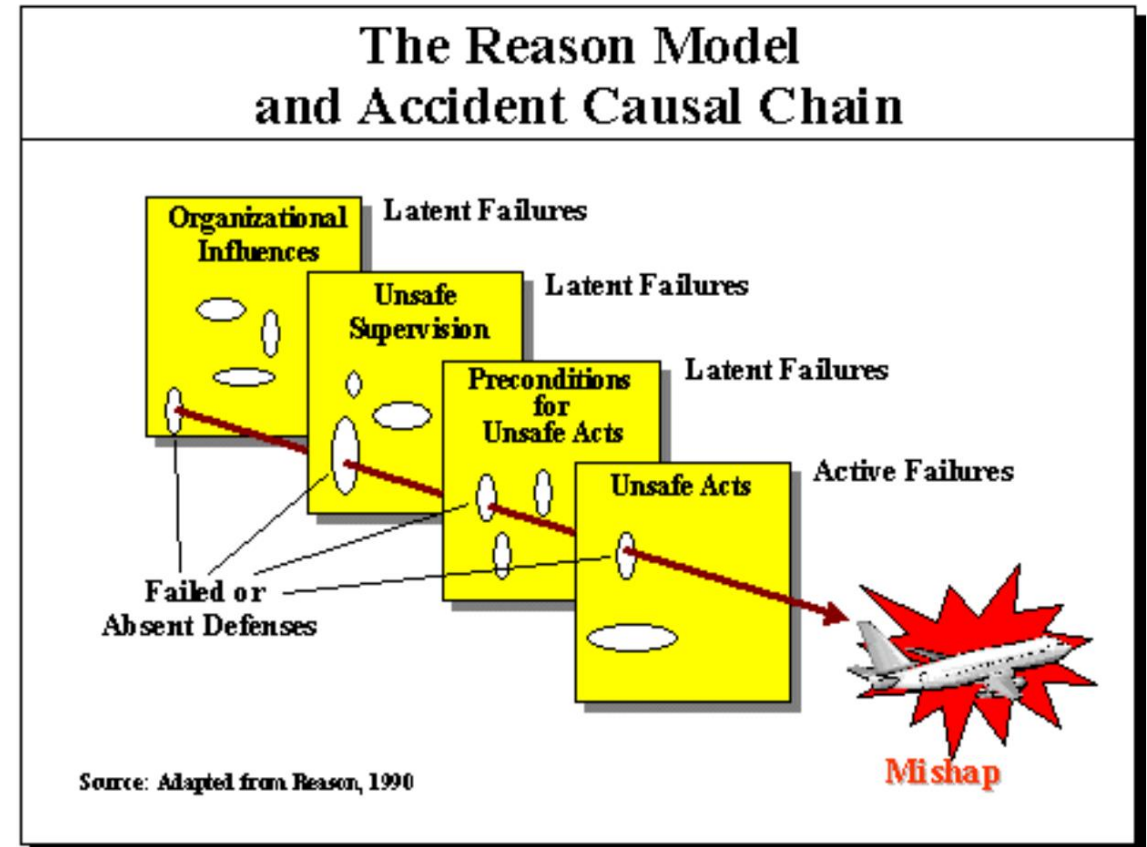


Heinrich, 1932

# Learning from incidents and implementing corrective actions

COE (Chain of Events) models describe simple, direct relationships but omit more complex and indirect relationships. Note that the Domino, Swiss Cheese, and Bow Tie models are the COE events model using different real world analogies, i.e., dominos, Swiss cheese slices, and formal men's apparel. They are not different causal models, but simply different names and graphical representations for the same thing.

***The question is not whether a model is right or wrong. The question is whether it is the most useful explanation for the goals of accident causal analysis and prevention.***



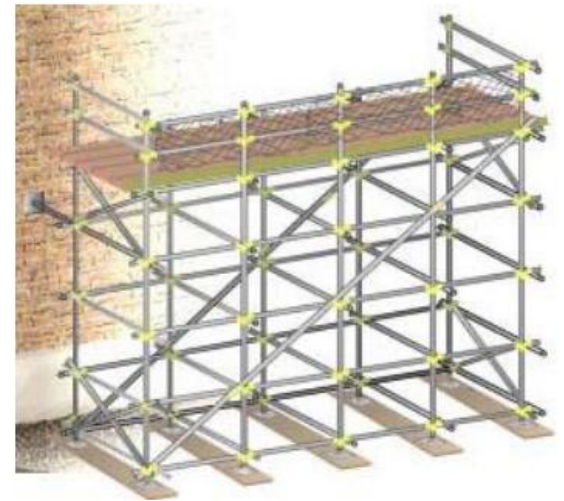


# Learning from incidents and implementing corrective actions

---

## Scaffolding Accident

- Assembling a large, complex product
- Part was not available when needed so decision made to add it later
- When part arrived, had to disassemble a large piece of product to insert missing part
- Scaffolding constructed during previous shift
- When went to remove large piece, the scaffolding kept it from being removed.
- Took floorboards out of scaffolding
- Removed piece and four workers were holding the piece while they moved it to the end of the scaffolding to take it down to the shop floor
- All four turned and one fell through hole in scaffolding

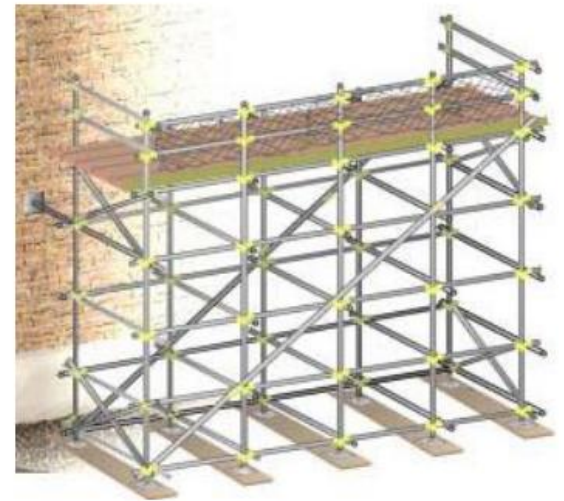


# Learning from incidents and implementing corrective actions

---

## Scaffolding Accident

- Identified “root cause”
  - Lack of experience doing job
  - Did not know there was a shop aid for this job
  - Did not perceive any undue risk and did not ask for help
- Recommendations:
  - Tell workers not to remove floorboards from scaffolding.
  - Add tool information to job instructions
  - During daily kickoff meeting, discuss potential hazards and ensure safe work practices for assigned tasks of the day
- Causal analysis tool:
  - Error: Worker stepped in a hole?
  - Why?
    - “Lack of situational awareness”
    - “Made a mistake”



# Learning from incidents and implementing corrective actions

---

Report did not ask:

- Why were they doing a job for which they had no experience and without oversight from someone who did?
- Why did they not know about proper job aids?
- Whose responsibility was it to ensure right equipment was available and used?
- Why did they not ask for advice when scaffolding prevented them from doing their job? (“Find a way” culture)
- Who provides oversight for “out-of-sequence” work?
- Why was blame for not understanding risks involved placed on them and not their supervisors?
- Why was incorrect scaffolding for job constructed in the first place?

# Learning from incidents and implementing corrective actions

---

- Why were the people constructing it not aware of what scaffolding was required?
- Who evaluates the hazards of out-of-sequence jobs?
- Was there documentation of tools needed for job?
- Why was the job not done when it originally was supposed to be done?
- Why was there no oversight of this out-of-sequence job?
- There was supposed to be a meeting about how to accomplish this work. Why was it never held? Why didn't the work wait until it could be?
- Are workers often expected to jury rig solutions with no oversight or input from others?

# Learning from incidents and implementing corrective actions

---

- Accidents are a dynamic control problem rather than a failure problem.
  - Hazards result from lack of enforcement of safety constraints in system design and operations
  - Losses involve interaction of humans, physical components, software, organizational factors, regulatory factors, culture, etc.
- Controls are created to prevent hazards. Accidents occur when the controls are ineffective.

# Learning from incidents and implementing corrective actions

---

## Goals for Accident/Incident Analysis

- Minimize hindsight bias
- Provide a framework or process to assist in understanding entire accident process and identifying systemic factors
- Get away from blame (“who”) and shift focus to “why” and how to prevent in the future
- Determine:
  1. Why people behaved the way they did
  2. Weaknesses in the safety control structure that allowed the loss to occur

# Root cause analysis techniques

---

## **Causal Analysis using System Theory (CAST)**

- A structured technique to analyze accident causality from a system perspective
  - Helps to generate questions to be asked
  - Paradigm change from what is done by other tools
    - Goal is not to start by looking for failures.
    - Why didn't designed controls prevent the accident?
    - What changes in the controls are needed to prevent future accidents?
- Identify how each of components in control structure contributed to the loss
- “What-Why” (explanatory) not “Who-Why” (accusatory)

# Root cause analysis techniques

---

## Causal Analysis using System Theory (CAST)

~~“Examine failures”~~

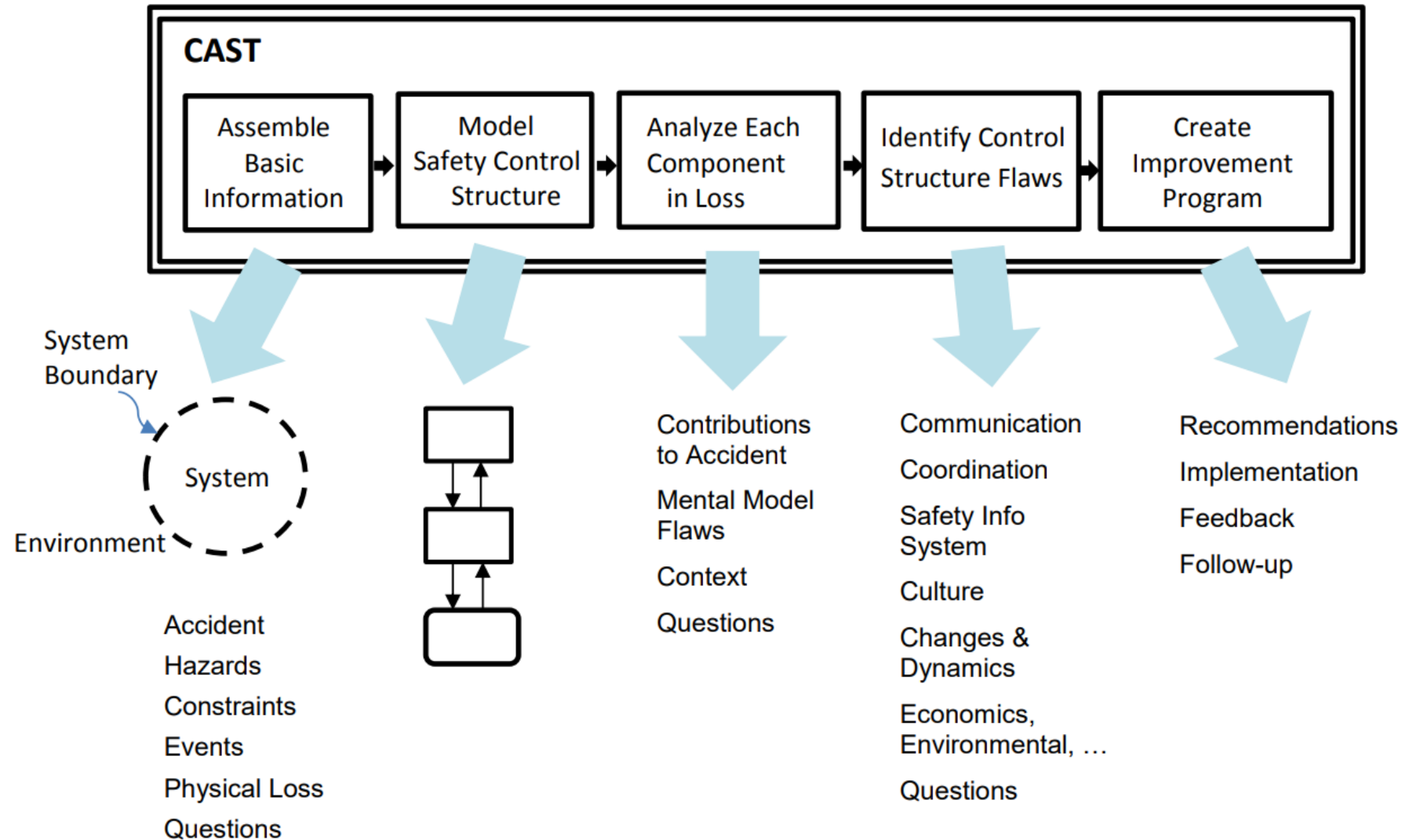


“Determine why designed controls were ineffective”

- Accidents are caused by complex interactions among humans, hardware, software, and social structures (not just chains of failure events)



# Root cause analysis techniques



# Root cause analysis techniques

RCA TOOL	ADVANTAGES	LIMITATIONS
CAST	<ul style="list-style-type: none"><li>• Systematic Perspective</li><li>• Identifying Root Causes</li><li>• Prevention and Improvement</li><li>• Multidisciplinary Approach</li><li>• Integration with Safety Management Systems</li></ul>	<ul style="list-style-type: none"><li>• Resource-Intensive<ul style="list-style-type: none"><li>• Complexity</li><li>• Subjectivity</li><li>• Learning Curve</li></ul></li><li>• Integration Challenges</li></ul>

# ¿Cuál es el contenido del curso?

---

- Introduction to Safety Risk Management
- Hazard Identification
- Risk Assessment and Analysis
- Risk Control Measures
- Incident Investigation and Analysis
- **Safety Performance Monitoring and Improvement**
- Case Studies and Best Practices

# Monitoring and evaluating the effectiveness of control measures

---

Establishing safety performance indicators (SPIs) involves a systematic process to identify and define metrics that can effectively measure and track safety performance within an organization.

In order to establish SPIs, a model must be put in place in the organization to establish objectives and targets.

# Monitoring and evaluating the effectiveness of control measures

---

## **Safety Planning**

Basic element of the safety management system that allows the organization's safety objectives and goals to be established, as well as the identification of the necessary means and resources to achieve them.

1. Set safety goals
2. Define the acceptable level of safety
3. Establish safety goals to ensure compliance with safety objectives
4. Establish management indicators to measure and demonstrate the acceptable level of safety meets the proposed goals

# Monitoring and evaluating the effectiveness of control measures

---

## **Safety Objectives**

- A brief, high-level statement of the desired safety achievement or result to be achieved through the service provider's safety management system
- Safety objectives are developed from the organization's main safety risks and should be taken into account during the subsequent development of safety performance indicators and targets.

# Monitoring and evaluating the effectiveness of control measures

---

## **Safety Targets and Safety Performance Indicators**

- The service provider's projected or planned target for a safety performance indicator, in a specified period of time, that is consistent with the safety objectives.
- Data-based safety metric used to observe and assess safety performance

# Monitoring and evaluating the effectiveness of control measures

---

## **ALoSP Concept**

- Minimum level of safety performance, expressed in terms of safety performance objectives and indicators
- ALoSP is a performance-based approach that defines actual safety performance levels within a prescribed State Safety Program (SSP) framework. The concept is expressed through two specific metrics, safety performance objectives and safety performance indicators.
- A State's core safety indicators generally consist of high-impact safety indicators (for example, accident and serious incident rates). Subsequently (at a mature stage of ALoSP), lower impact safety indicators can be developed.



# Monitoring and evaluating the effectiveness of control measures

---

## **ALoSP Concept**

In order to implement an effective ALoSP model, the Safety Management System must:

a) Identify all safety-critical sectors and safety indicators that define the level of safety

Referring to:

- Exposure of the organization to a particular risk (Probability of occurrence)
- Severity of consequences related to a hazard

# Monitoring and evaluating the effectiveness of control measures

---

## **ALoSP Concept**

- b) identify the goals that define the level to be maintained or the desired improvement to be achieved for the relevant indicators in each sector with a view to achieving Improvement
- c) identify alerts that indicate an actual or developing safety performance problem in a particular indicator or safety sector
- d) review safety performance to determine if modifications or additions to existing indicators, targets or alerts are needed to achieve continual improvement

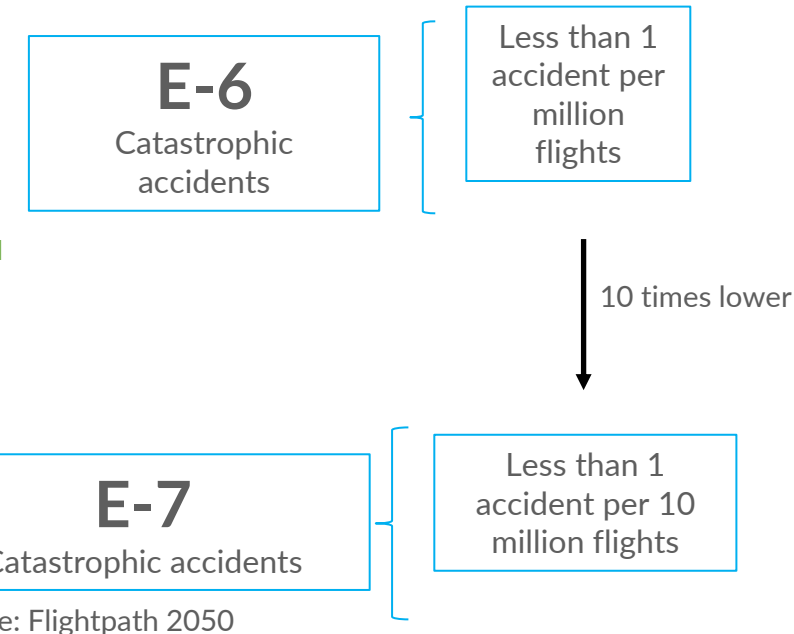
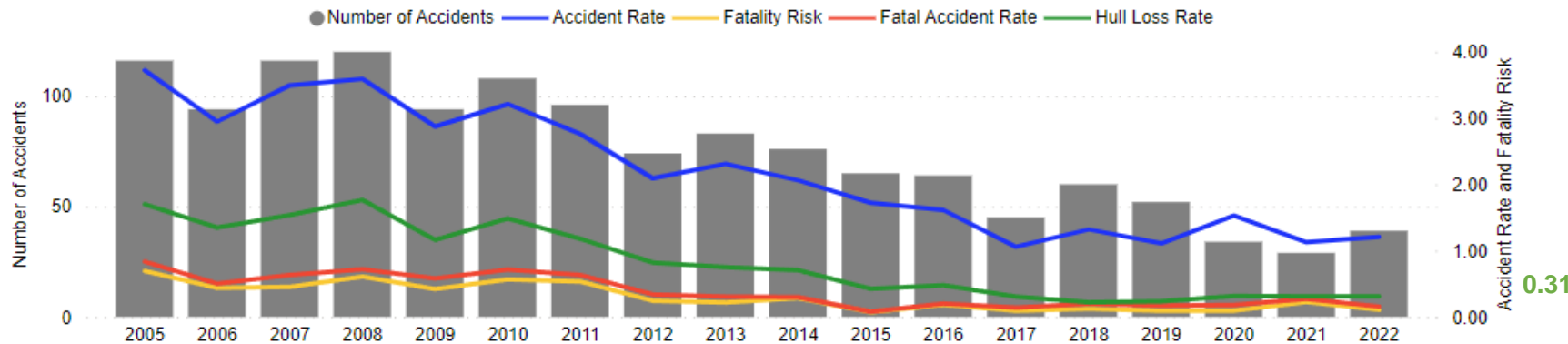
Operators must define the tolerability of risk exposure and its consequences, aligning their objectives and performance indicators **(SPIs)**.

# Monitoring and evaluating the effectiveness of control measures

## How to define an ALoSP

A maximum probability acceptable to the company must be defined for each level of severity (Catastrophic, Major, Medium).

Accident Rate (per Million Sectors) and Fatality Risk (per Million Sectors) by Year \* Data source IATA



Target =

Source: Flightpath 2050

# Monitoring and evaluating the effectiveness of control measures

---

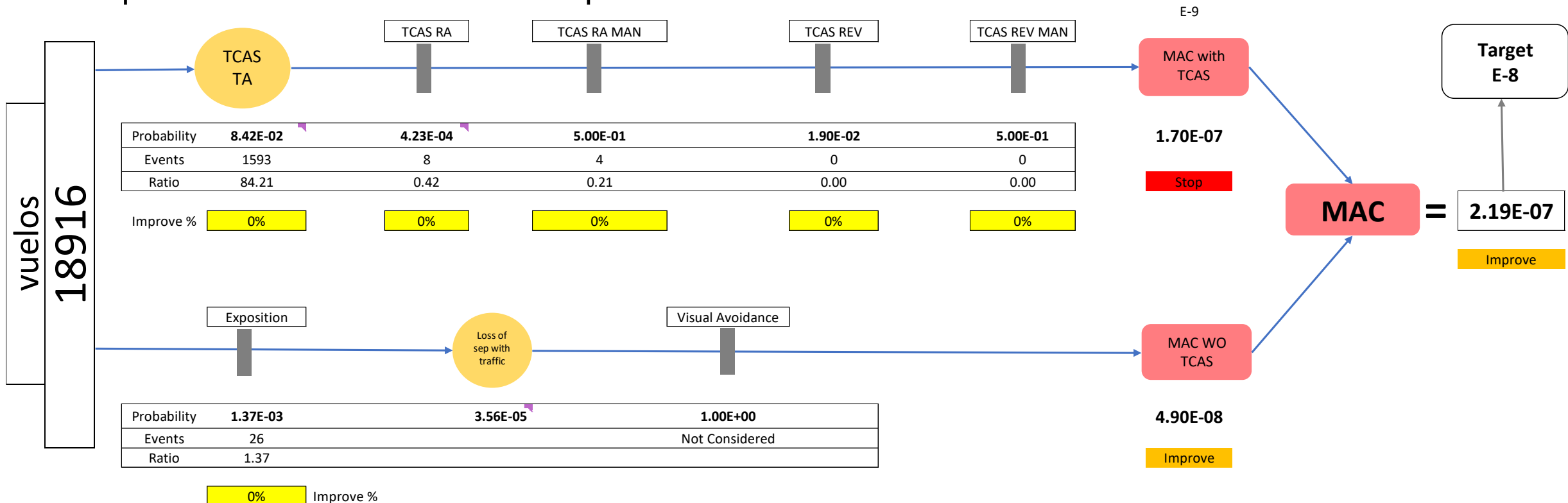
## How to define an ALoSP

- Which ones are identified as the precursors for catastrophic accidents (Hull Loss)
  1. LOC-I: Loss of Control in Flight
  2. MAC: Mid –Air Collision
  3. CFIT: Controlled Flight into terrain
  4. RWY-COL: Runway Collision

# Monitoring and evaluating the effectiveness of control measures

## How to define an ALoSP

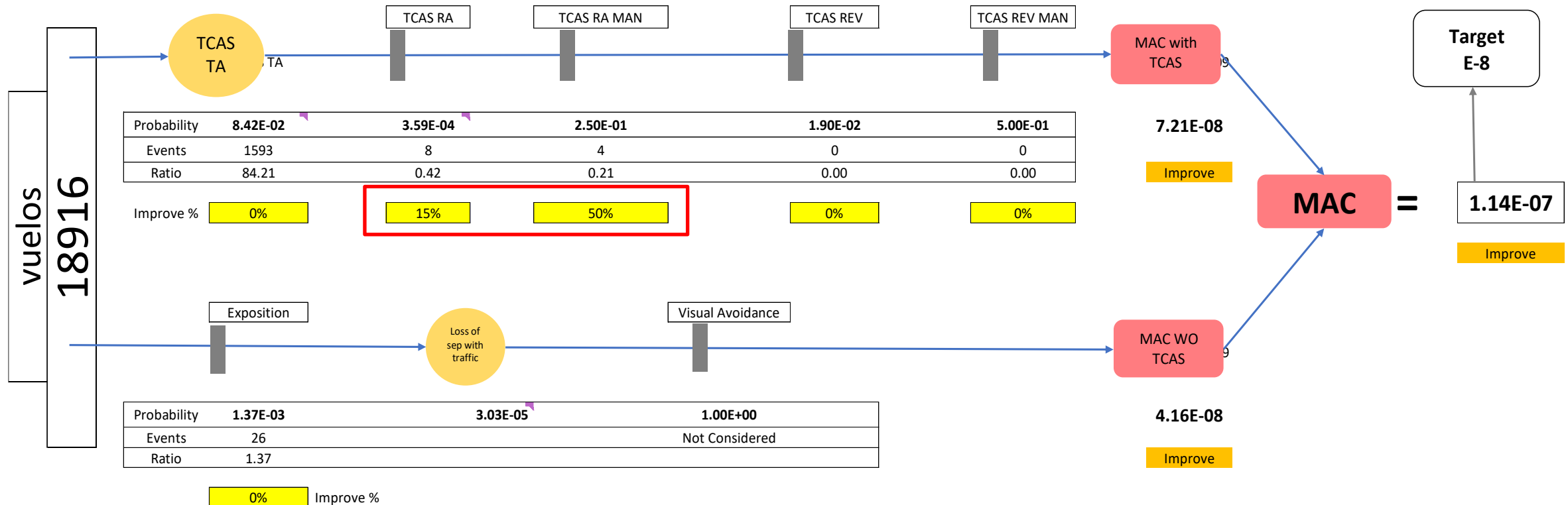
For each precursor, the current risk exposure is assessed within the specific operational context. For example Mid-Air Collision



# Monitoring and evaluating the effectiveness of control measures

## How to define an ALoSP

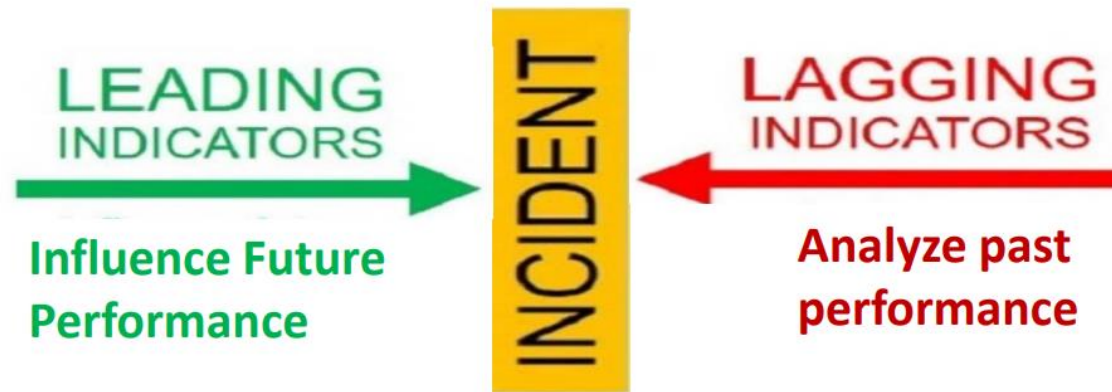
Once the probability of occurrence is established within the ALoSP model, the indicators and improvement goals to be met are identified.



# Monitoring and evaluating the effectiveness of control measures

---

- Once the indicators to be measured and the goals to be met are established, the description of the indicator associated with its respective goal is made.
- Lagging – leading indicators can be used depending on what you want to measure



- **Lagging SPIs:** SPIs based on the result (usually negative results)
- **Leading SPIs:** Process-based SPIs (measure conditions that have the potential to contribute to a result)

# Monitoring and evaluating the effectiveness of control measures

---

## How to describe SPIs and SPTs

- Mid-Air Collision

**Safety Objective:** Reduce aircraft separation reduction events

SPI 1: Number of TCAS RA activations per 1000 FC (Lagging)

SPT: Reduce TCAS RA procedures by 15% per 1000 FC

SPI 2: Number of TCAS maneuvers performed appropriately (Lagging)

SPT 2: Reduce by 50% inappropriately executed TCAS maneuvers

SPI 3: Crews trained in new SOPs associated with the activation of TCAS RA alarms

SPT 3: Train 50% of the crews in the new SOPs in a period of 6 months.



# Monitoring and evaluating the effectiveness of control measures

---

## Conclusions

- Safety planning should be carried out before beginning to establish SPIs
- The organization must establish its acceptable level of security, which shall not be higher than the safety level established by the state (SSP).
- The goals and indicators must be established to achieve that acceptable level of Safety, NEVER based on historical data of the organization's results.
- For each security objective, it is recommended to establish process and result SPIs
- Continuous monitoring of the results must be carried out to evaluate the mitigation actions to be implemented
- The SSP must be proactively involved in establishing the acceptable security levels of its country-region in order to standardize the measurements of each air operator.

# ¿Cuál es el contenido del curso?

---

- Introduction to Safety Risk Management
- Hazard Identification
- Risk Assessment and Analysis
- Risk Control Measures
- Incident Investigation and Analysis
- Safety Performance Monitoring and Improvement
- **Case Studies and Best Practices**

# Case Studies and Best Practices

---

## **KLM – Pan Am Accident (Tenerife 1977)**

For this Case Study, we are going to use three methodologies to investigate the accident and compare the final conclusions and recommendations. The methodologies used are:

1. FTA: Fault Tree Analysis
2. FMEAC: Failure Mode and Effects Analysis
3. CAST: Causal Analysis based on System Theory

# Case Studies and Best Practices

---

## Accident Description

The Tenerife airport disaster occurred on March 27, 1977, when two Boeing 747 passenger jets collided on the runway at Los Rodeos Airport on the Spanish island of Tenerife. The collision occurred when KLM Flight 4805 initiated its takeoff run while Pan Am Flight 1736 was still on the runway. The impact and resulting fire killed everyone on board KLM 4805 and most of the occupants of Pan Am 1736, with only 61 survivors in the front section of the aircraft. With 583 fatalities, the disaster is the deadliest accident in aviation history.

Tenerife was an unscheduled stop for both flights. Their destination was Gran Canaria Airport, serving Las Palmas on the nearby island of Gran Canaria.

Both flights had been routine until they approached the islands. At 13:15, a bomb planted by the separatist Canary Islands Independence Movement exploded in the terminal of Gran Canaria Airport, injuring eight people.



# Case Studies and Best Practices

---

## Accident Description

KLM Flight 4805 was a charter flight for Holland International Travel Group and had arrived from Amsterdam Airport Schiphol, Netherlands.

Pan Am Flight 1736 had originated at Los Angeles International Airport, with an intermediate stop at New York's John F. Kennedy International Airport (JFK).

Los Rodeos was a regional airport that could not easily accommodate all of the traffic diverted from Gran Canaria, which included five large airliners.(17) The airport had only one runway and one major taxiway running parallel to it, with four short taxiways connecting the two. While waiting for Gran Canaria airport to reopen, the diverted airplanes took up so much space that they had to park on the long taxiway, making it unavailable for the purpose of taxiing. Instead, departing aircraft needed to taxi along the runway to position themselves for takeoff, a procedure known as a backtaxi or backtrack.



# Case Studies and Best Practices

---

## Accident Description

The authorities reopened Gran Canaria airport once the bomb threat had been contained. The Pan Am plane was ready to depart from Tenerife, but access to the runway was obstructed by the KLM plane and a refueling vehicle; the KLM captain had decided to fully refuel at Los Rodeos instead of Las Palmas, apparently to save time.

The Pan Am aircraft was unable to maneuver around the refueling KLM in order to reach the runway for takeoff, due to a lack of safe clearance between the two planes, which was just 3.7 meters (12 ft). The refueling took about 35 minutes, after which the passengers were brought back to the aircraft.





# Case Studies and Best Practices

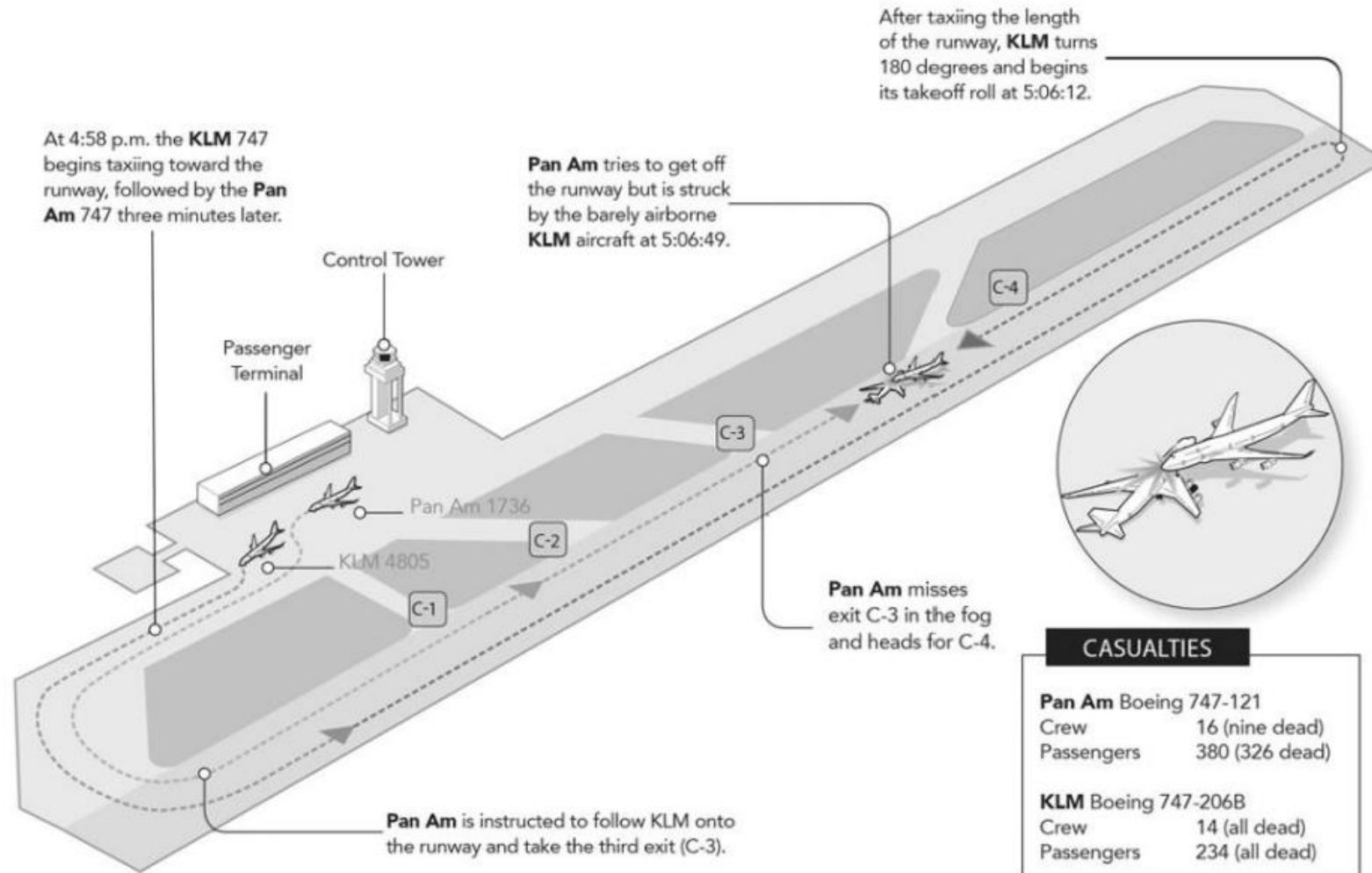


Illustration by Steve Karp

# Case Studies and Best Practices

Time	Event
12:30	KLM flight 4805, a Boeing 747, from Amsterdam to the Canary Islands and Pan Am flight 1736, another Boeing 747 bound for Los Angeles and New York to the Canary Islands, were diverted to Los Rodeos airport in Tenerife due to a bomb threat.
13:38	The KLM aircraft landed at Tenerife airport.
14:15	The Pan Am aircraft landed. Pan Am aircraft had to park behind the KLM flight in such a way that it could not depart until the KLM aircraft left
14:30	Las Palmas airport reopened, Pan Am aircraft was ready to take off for flight as its passengers remained on the aircraft. KLM's passengers had abandoned the aircraft, so there was a delay in their re-boarding and refuelling to shorten the return time to Las Palmas. Meanwhile, the weather conditions started to get worse, and visibility on the runway decreased due to fog.
16:56	The KLM aircraft began taxiing for takeoff and initially headed towards a runway parallel to the take-off runway. This directive was changed shortly after, and KLM was asked to taxi on the take-off runway and eventually make a 180-degree turn and wait for further instructions. Pan Am was asked to follow KLM on the take-off runway and leave the take-off runway via taxiway C3, use the parallel runway for the remainder of the taxi, then pull behind the KLM flight. Pan Am's request to stay away from the take-off runway and remain on the runway until KLM left was denied.

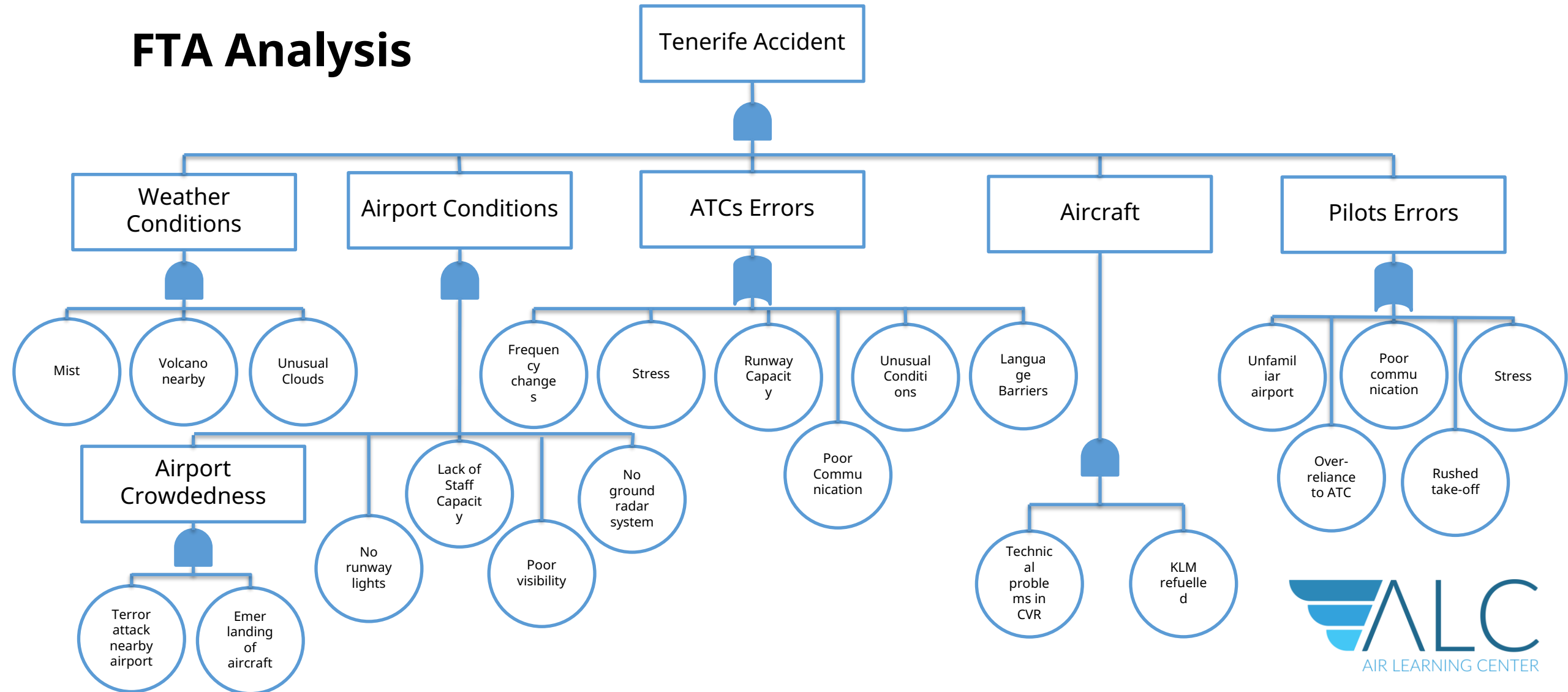


# Case Studies and Best Practices

Time	Event
17:06	Despite being instructed to wait, the KLM plane started to move after making a 180 degree turn at the end of the take-off runway and said "we are now taking off". Neither the air traffic controllers nor the Pan Am crew were sure of what this vague statement meant, but Pan Am reassured the controllers that it would report once it had moved away from the take-off runway when a message was heard in the KLM cockpit. When the engineer asked the pilot of KLM flight, "Is he not clear then, that Pan Am?" the pilot replied "yes", and there was no further conversation. The collision of the two planes occurred 13 seconds later at 17:06. None of the 234 passengers and 14 crew members of the KLM aircraft survived and died. Of the 380 passengers and 16 crew members on board the Pan Am flight, 70 survived, but later 9 died, resulting in a total of 583 fatalities.

# Case Studies and Best Practices

## FTA Analysis



# Case Studies and Best Practices

---

## FTA Analysis

- FTA identified 22 basic events for the cause of the Tenerife accident, as shown in the previous figure. Adverse weather conditions, inadequate airport conditions, Air Traffic Controllers (ATCs) errors, conditions at the aircraft and pilot errors were main factors leading to the accident.
- Adverse weather conditions on the day of the accident reduced visibility. Airport was located in a challenging position for flight safety. The fact that the accident occurred on Sunday and the presence of two personnel at the airport posed a problem in itself.
- The absence of lights in the middle of the runway and the absence of a radar system to show the location of the aircraft on the ground constitute a chain of negligence.

# Case Studies and Best Practices

---

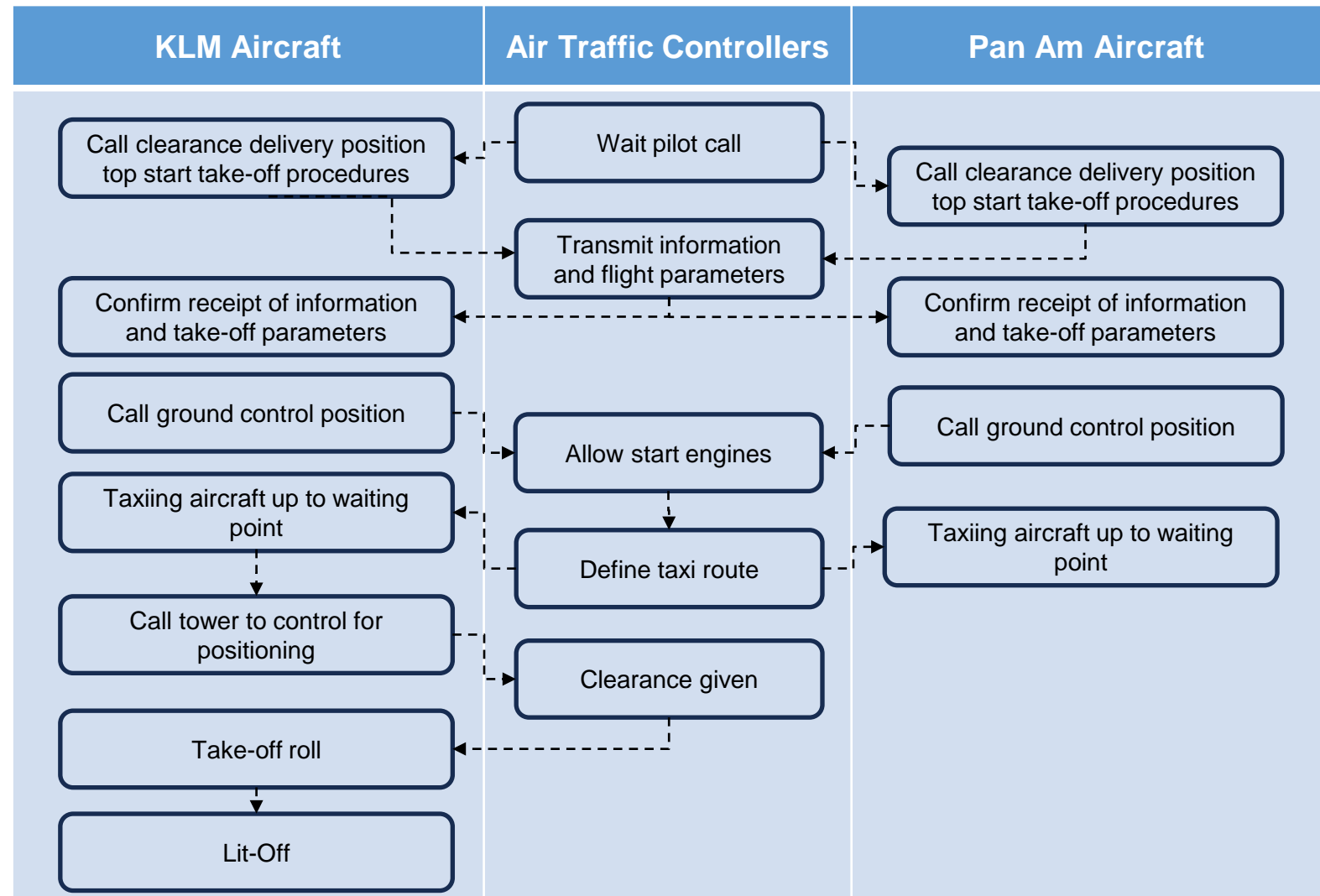
## FTA Analysis

- There were only two ATCs working at the tower. One of them changed the radio frequency, which resulted in poor communication between ATCs and pilots.
- Accident reports highlighted that Pan Am aircraft captain request for waiting for the KLM aircraft take-off was not heard at all. While pilots at both aircraft made errors, KLM aircraft captain was also rushed to take-off, and this decision was the last chain of the event for the Tenerife accident
- FTA revealed that stress and poor communication were of great importance in the causes of the accident.
- With the FTA application, 4 causes were related to organizational factors, 12 to human, 3 to technology and 5 to environmental factors

# Case Studies and Best Practices

## FMEA Analysis

- Tenerife accident occurred while KLM aircraft was taking-off and Pan Am aircraft was taxiing on the runway. Thus, FMEA was applied by considering the take-off process,



# Case Studies and Best Practices

Sub-system	Function	Failure Mode	Effects	Causes
KLM Aircraft	Call clearance delivery position to start take-off procedures	Delays on the call	Putting extra pressure on the KLM and Pan Am crew and passengers Delays on the flight	<ul style="list-style-type: none"><li>• Captain decided to take fuel to fly back to Amsterdam</li></ul>
	Confirm receipt of information and take-off parameters	Delays on receiving the parameters	Putting extra pressure on the KLM and Pan Am crew and passengers Delays on the flight	<ul style="list-style-type: none"><li>• Coordination problems among the various centers</li></ul>
	Call ground control position	Delays on the call ground control position	Extra pressure on the crew	<ul style="list-style-type: none"><li>• The airport is not designed to accommodate such aircrafts</li><li>• A third controller is not in present</li></ul>
	Taxiing aircraft up to the waiting point	Wrong taxiing	Confusion to both approach controller and captain KLM missed turning at Taxiway C3	<ul style="list-style-type: none"><li>• Miscommunication</li><li>• Runway size is small for such a large aircraft</li></ul>

# Case Studies and Best Practices

Sub-system	Function	Failure Mode	Effects	Causes
KLM Aircraft	Take-off roll	Wrong take-off initiated	KLM aircraft started releasing its brake too soon	<ul style="list-style-type: none"><li>• No light available runway centerline</li><li>• No ground radar system</li><li>• Released its break without clearance</li><li>• Captain rushed to take-off</li><li>• Poor visibility at the runway</li><li>• Poor communication among the crew</li><li>• Poor communication between the captain and the controller</li><li>• A high pitched sequal overlays controller's sound and it is distorted.</li></ul>
	Lift-off	Inadequate lift-off	Aircraft collision	<ul style="list-style-type: none"><li>• Initiated the take-off too soon</li></ul>
Air traffic controllers	Wait for the pilot call	Delays on the call	Increased stress	<ul style="list-style-type: none"><li>• KLM captain decided to take fuel to fly back to Amsterdam</li><li>• KLM aircraft blocked the way of Pan Am aircraft</li></ul>
	Transmit information and flight parameters	Delays on transmitting information	Putting extra pressure on the controllers and pilots at two aircrafts	<ul style="list-style-type: none"><li>• Coordination problems among the various centers</li></ul>

# Case Studies and Best Practices

Sub-system	Function	Failure Mode	Effects	Causes
Air traffic controllers	Define the taxi route	The inadequate direction is given	KLM required to make 180 degrees turn at the end of the runway Pan Am missed turning at Taxiway C3	<ul style="list-style-type: none"> <li>Miscommunication between pilots and controllers</li> <li>No ground radar system</li> <li>A third controller is not in present</li> <li>A lack of personnel</li> <li>No runway number signs</li> </ul>
	Clearance given	Confusing clearance is given	KLM released its brake and initiated the take-off before the clearance given	<ul style="list-style-type: none"> <li>Miscommunication between controllers and KLM pilots</li> <li>Stress on both parts</li> <li>Different frequencies gave the clearances to both aircraft</li> </ul>
Pan Am aircraft	Call clearance delivery position to start take-off procedures	Delays on the call	Putting extra pressure on the KLM and Pan Am crew and passengers Delays on the flight	<ul style="list-style-type: none"> <li>KLM aircraft blocked the way of Pan Am aircraft</li> </ul>
	Confirm receipt of information and take-off parameters	Delays on receiving the parameters	Putting extra pressure on the KLM and Pan Am crew and passengers Delays on the flight	<ul style="list-style-type: none"> <li>Coordination problems among the various centers</li> </ul>



# Case Studies and Best Practices

Sub-system	Function	Failure Mode	Effects	Causes
Pan Am aircraft	Call ground control position	Delays on the call ground control position	Extra pressure on the crew	<ul style="list-style-type: none"><li>• The airport is not designed to accommodate such aircrafts</li><li>• A third controller is not in present</li><li>• A lack of personnel</li></ul>
	Taxiing aircraft up to the waiting point	Wrong taxiing	Pan Am missed turning at Taxiway C3 Aircraft remained in the runway while KLM taking-off	<ul style="list-style-type: none"><li>• The controller's transmission blocked pan Am's transmission</li><li>• Poor visibility at the runway</li><li>• No runway number signs</li><li>• Miscommunication between Pan Am crew and the controller</li><li>• Heavy Spanish accent of the controller</li></ul>

# Case Studies and Best Practices

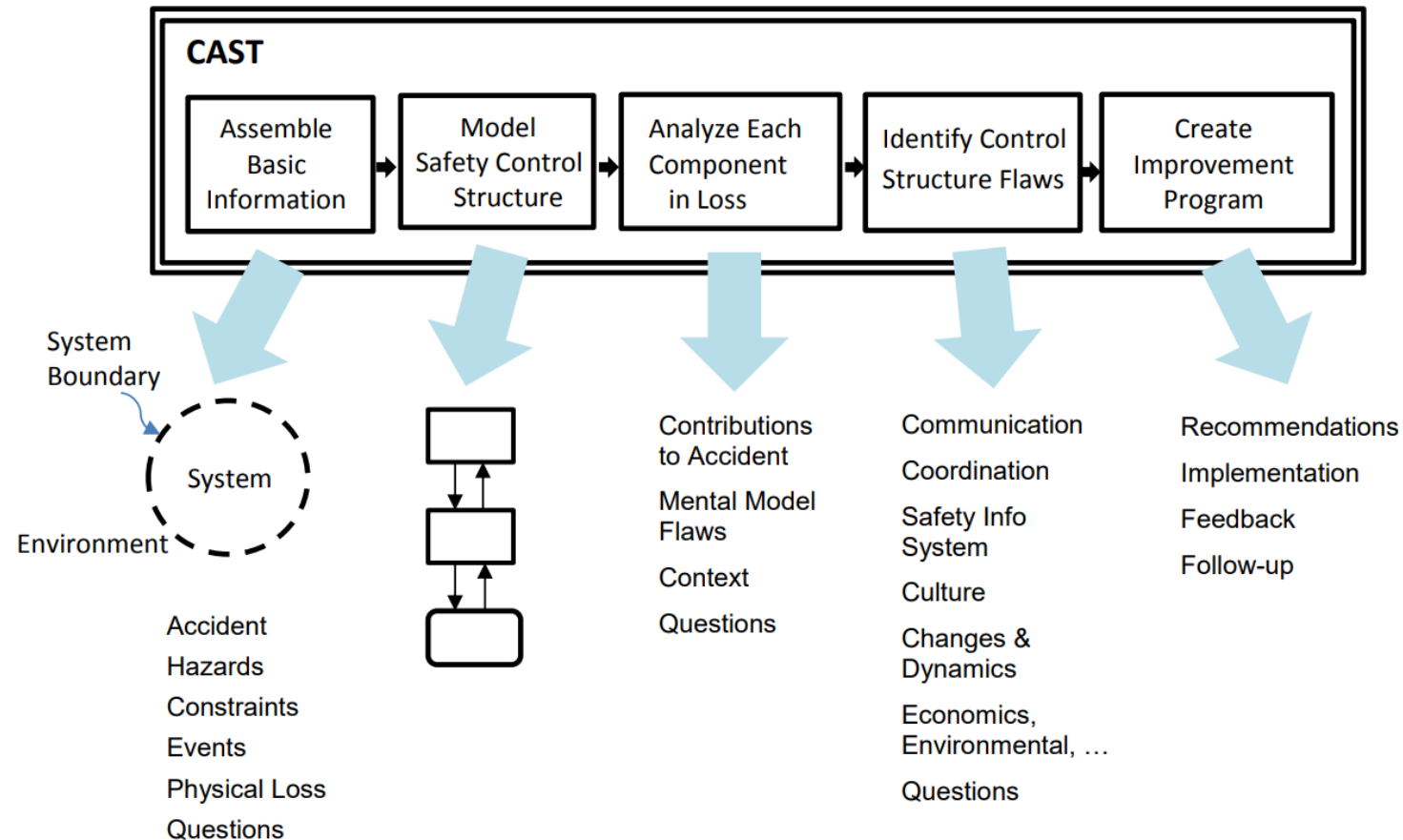
---

## **FMEAC Analysis**

- FMEAC analysis identified communication problems and poor visibility at the runway.
- Additionally, several factors, such as poor airport design for large aircraft, a lack of personnel available at the control tower, and stress were revealed to be the contributory factors of the accident
- In the FMEA application, several causes were repeated in different cases. Among 23 causes, 7 were related to organizational, 13 to human, 6 to technology and 1 to environmental factors.

# Case Studies and Best Practices

## CAST Analysis



# Case Studies and Best Practices

---

## **CAST Analysis**

### Basic Components of a CAST Analysis

1. Collect the basic information to perform the analysis:
  - a) Define the system involved and the boundary of the analysis,
  - b) Describe the loss and hazardous state that led to it
  - c) From the hazard, identify the system-level safety constraints required to prevent the hazard (the system safety requirements and constraints).
  - d) Describe what happened (the events) without conclusions nor blame. Generate questions that need to be answered to explain why the events occurred.

# Case Studies and Best Practices

---

## **CAST Analysis**

### Basic Components of a CAST Analysis

- e) Analyze the physical loss in terms of the physical equipment and controls, the requirements on the physical design to prevent the hazard involved, the physical controls (emergency and safety equipment) included in the design to prevent this type of accident, failures and unsafe interactions leading to the hazard, missing or inadequate physical controls that might have prevented the accident, and any contextual factors that influenced the events.

The goal of rest of analysis is to identify the limitations of the safety control structure that allowed the loss and how to strengthen it in the future.

# Case Studies and Best Practices

---

## **CAST Analysis**

### Basic Components of a CAST Analysis

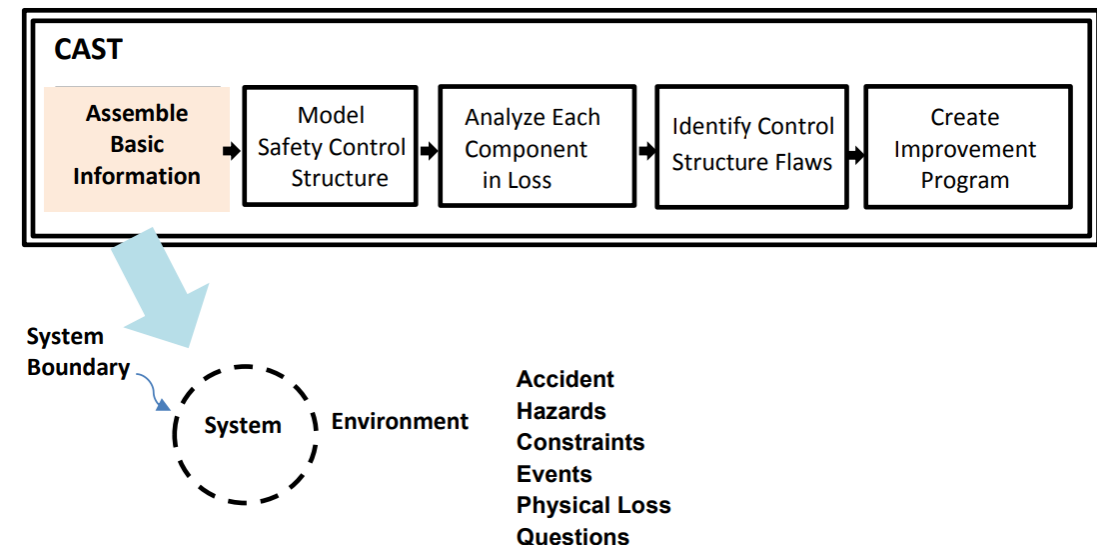
2. Model the existing safety control structure for this type of hazard.
3. Examine the components of the control structure to determine why they were not effective in preventing the loss: Starting at the bottom of the control structure, show the role each component played in the accident and the explanation for their behavior (why they did what they did and why they thought it was the right thing to do at the time).
4. Identify flaws in the control structure as a whole (general systemic factors) that contributed to the loss. The systemic factors span the individual system control structure components.
5. Create recommendations for changes to the control structure to prevent a similar loss in the future. If appropriate, design a continuous improvement program for this hazard as part of your overall risk management program.

# Case Studies and Best Practices

## CAST Analysis

Identify the boundaries of the system of concern:

- In the Tenerife accident, the system analyzed is:
  - The Regulatory Agencies
  - The Airlines
  - Air Traffic Controllers
  - Operations Management
  - Pilots
  - Aircraft



# Case Studies and Best Practices

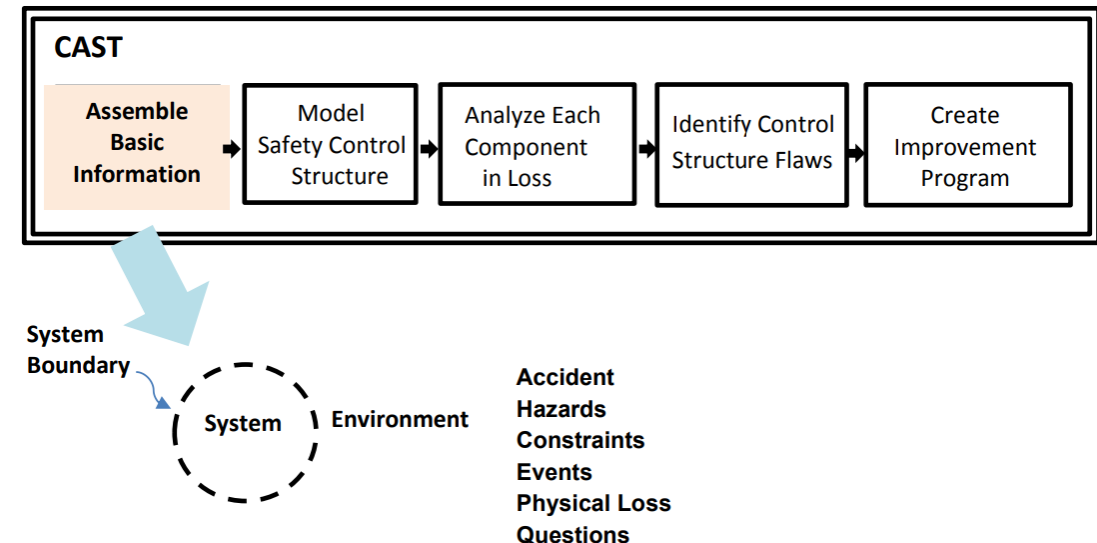
## CAST Analysis

Identify the hazards that led to the loss and the constraints that must be satisfied in the design and operation of the system

**System Hazard 1:** Aircraft enters into a wrong area

Safety Constraints:

1. Aircraft has to enter the correct area





# Case Studies and Best Practices

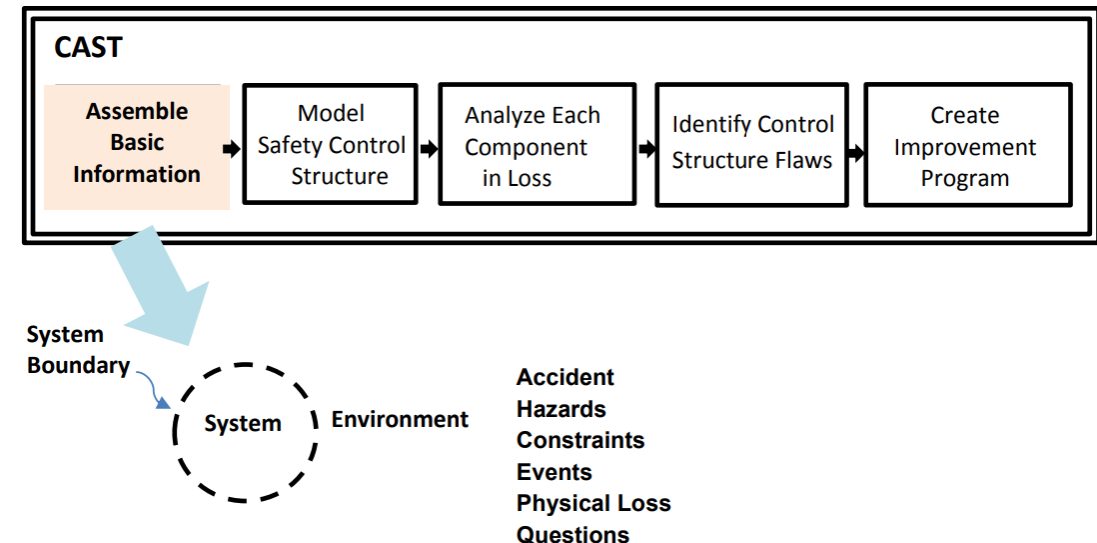
## CAST Analysis

Identify the hazards that led to the loss and the constraints that must be satisfied in the design and operation of the system

**System Hazard 2:** Aircraft prepares to take-off from the wrong taxiway

Safety Constraints:

1. Aircraft has to be in the right taxiway on time



# Case Studies and Best Practices

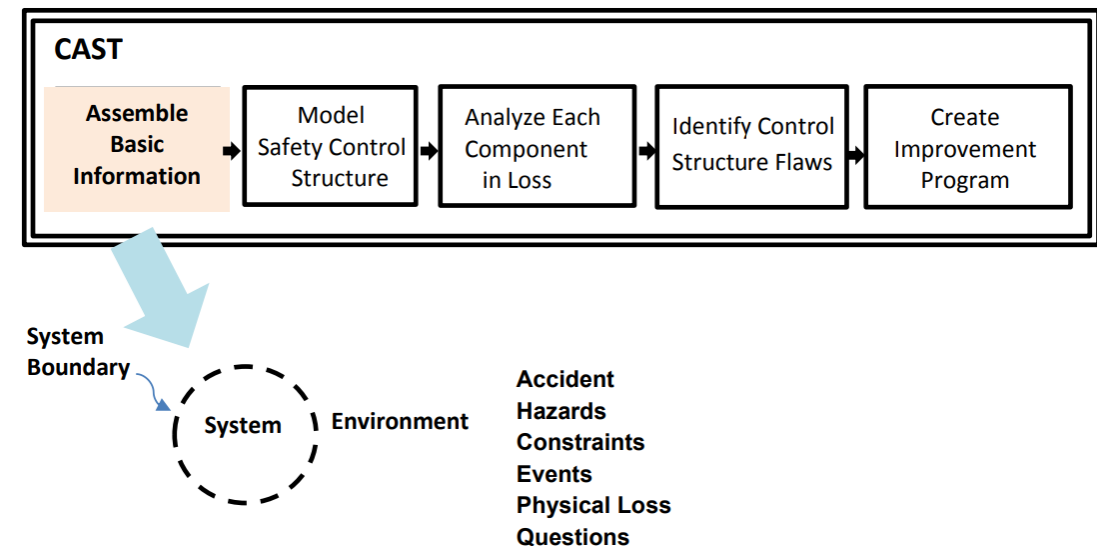
## CAST Analysis

Identify the hazards that led to the loss and the constraints that must be satisfied in the design and operation of the system

**System Hazard 3:** Aircraft violate minimum separation standards

Safety Constraints:

1. Pilots have to obey the minimum flight standards

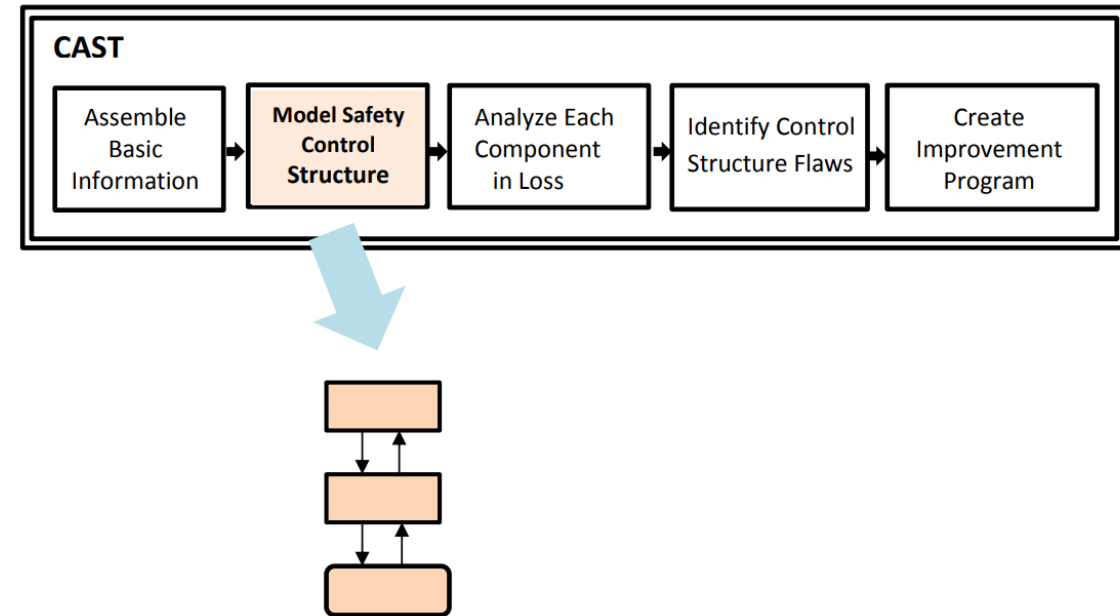


# Case Studies and Best Practices

## CAST Analysis

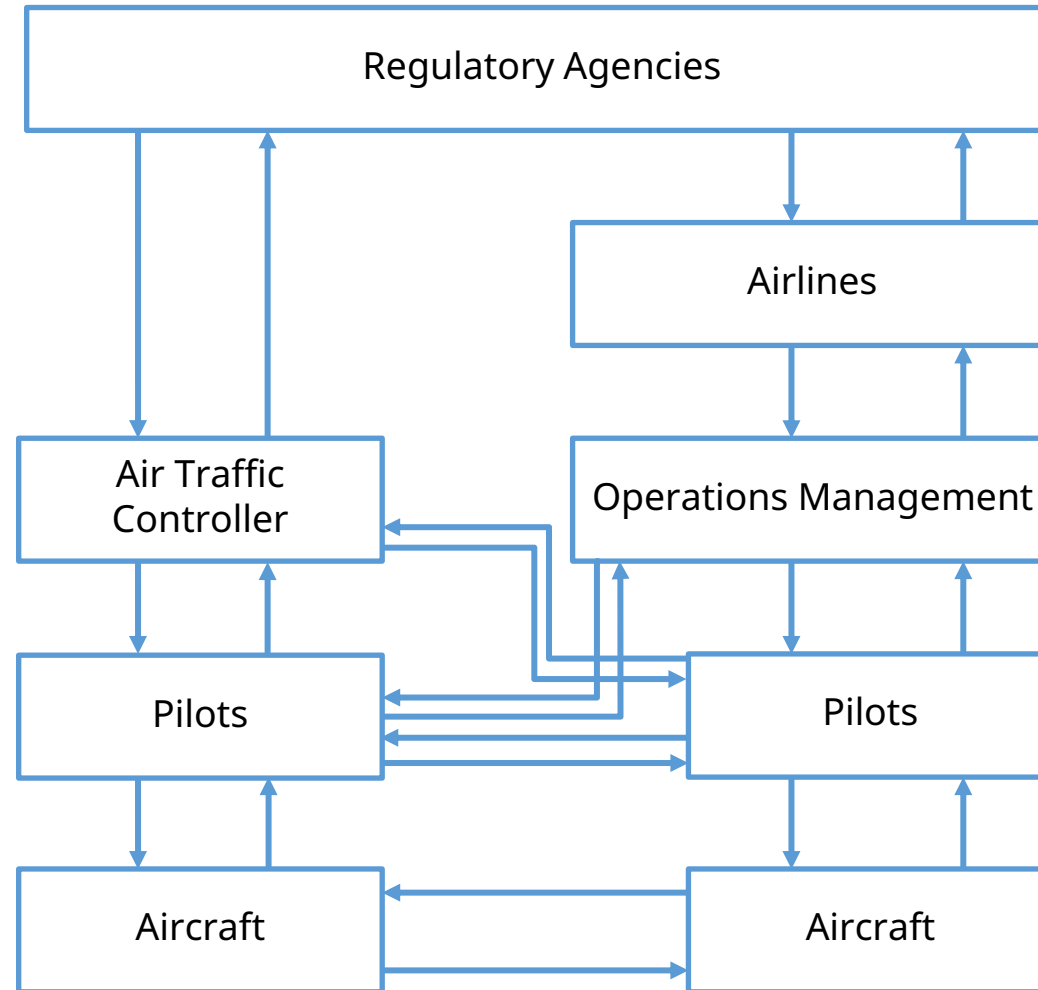
Because CAST focuses on the controls and controllers and their role in the accident, modeling the control structure is necessary to start the analysis.

If a control structure for the system does not already exist, most people find it helpful to start with a very abstract, high-level control structure that involves the general controls for this type of event.



# Case Studies and Best Practices

## CAST Analysis



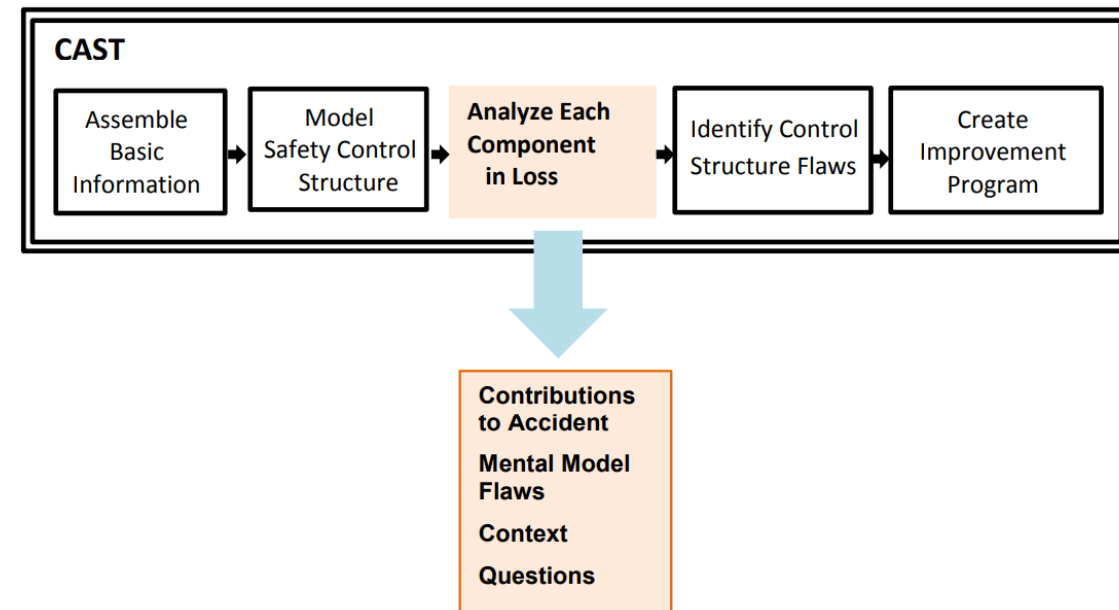
# Case Studies and Best Practices

## CAST Analysis

Once the basic control structure and controls are identified, the next step is to show why the control structure, i.e., the current controls, did not prevent the accident.

There will be two parts to this process, the first looks at the individual controllers (which may be automated or human) and the role they played in the accident.

The second looks at the operation of the control structure as a whole and the interactions among the components



# Case Studies and Best Practices

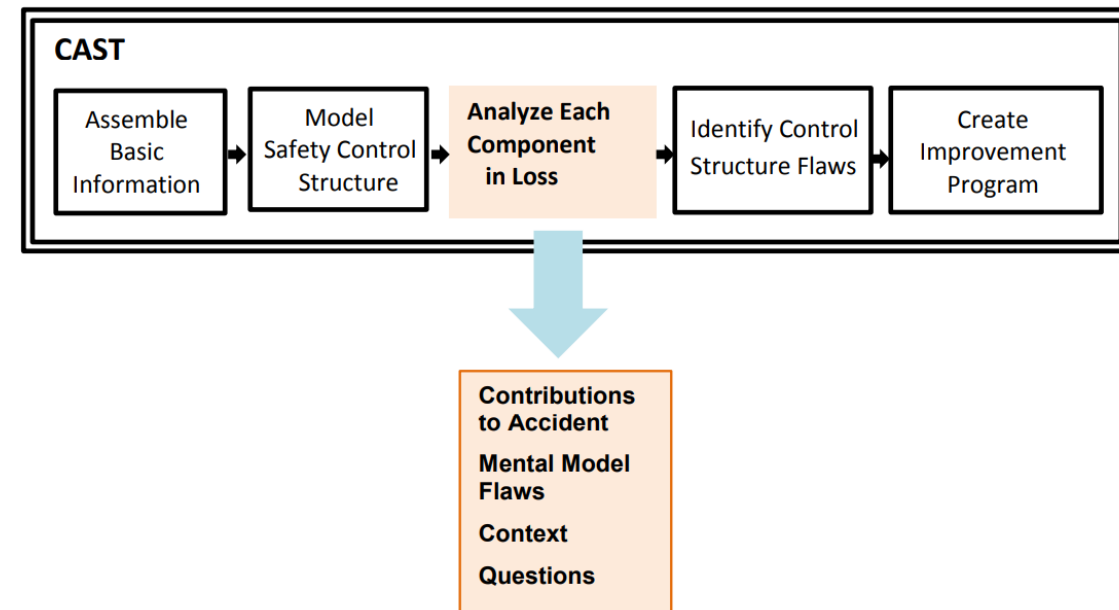
## CAST Analysis

There are several parts in the CAST analysis of each controller:

- Component responsibilities related to the accident
- Contribution (actions, lack of actions, decisions) to the hazardous state:

Why?

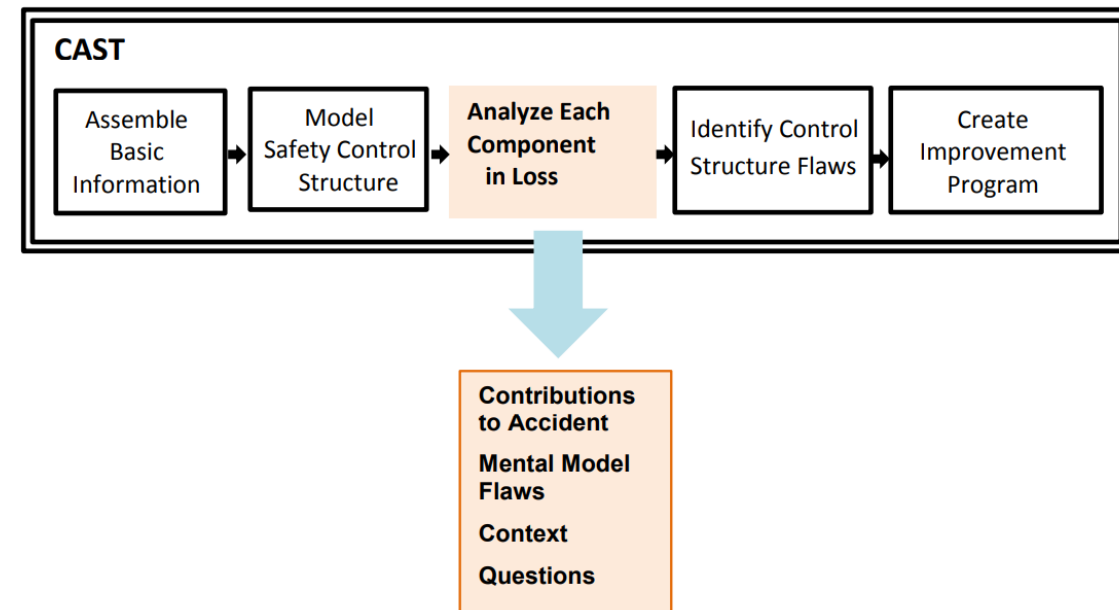
- Flaws in the mental/process model contributing to the actions:
- Contextual factors explaining the actions, decisions, and process model flaws



# Case Studies and Best Practices

## **CAST Analysis Regulatory Agencies Safety Related Responsibilities**

Registration of aircraft, certification of aircraft airworthiness & operating manuals, issuing airworthiness directives, certification of airline operating procedures, certification of aircrew training, certification of ATC training, certification of maintenance, and checking compliance with regulations



# Case Studies and Best Practices

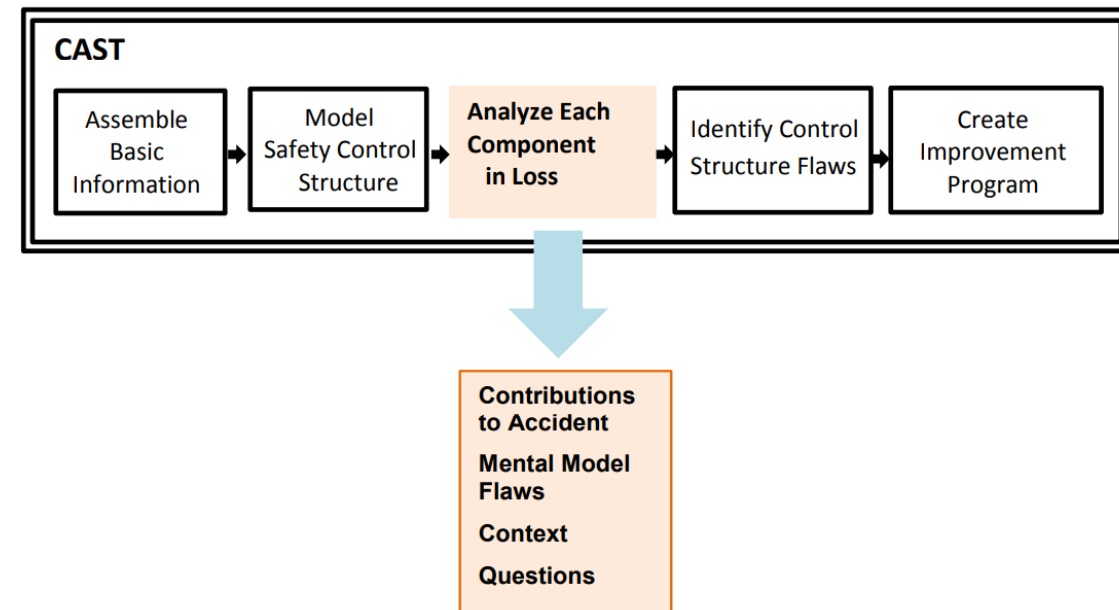
---

## CAST Analysis

### Regulatory Agencies

**Contribution (actions, lack of actions, decisions) to the hazardous state:**

Issued AD that emphasized information already in-flight manuals. Added explanation, but insufficient and incorrect. Initial regulatory requirements insufficient for safe operation





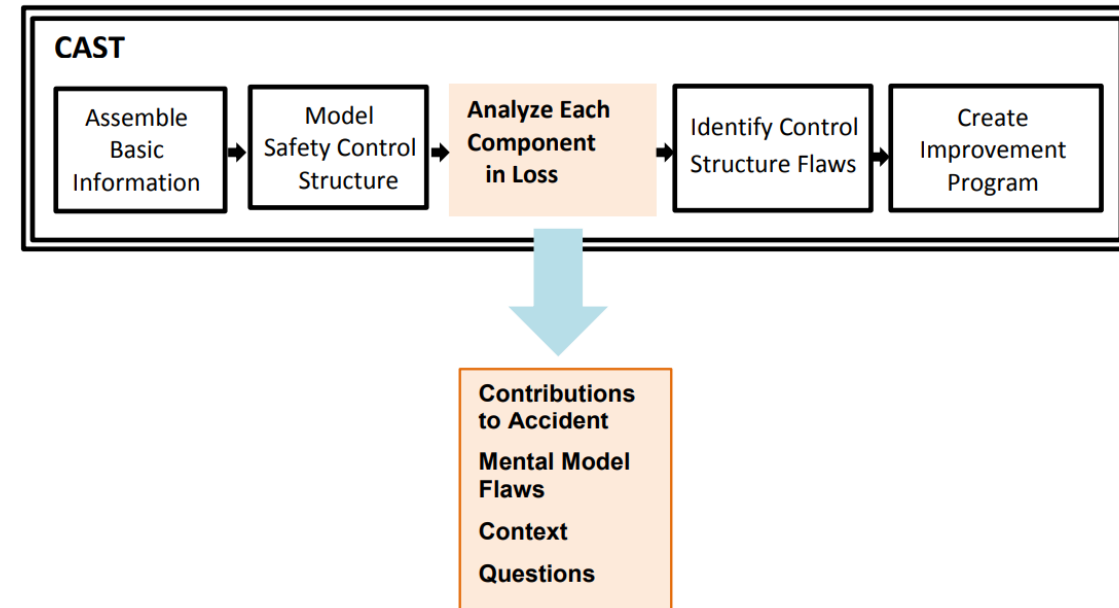
# Case Studies and Best Practices

## CAST Analysis

### Regulatory Agencies

**Flaws in the mental/process model contributing to the actions:**

Act quickly to fix a known problem. Changes to operating procedures are believed to be sufficient and are handled in the same way as necessary action against previous accidents was addressed and closed



# Case Studies and Best Practices

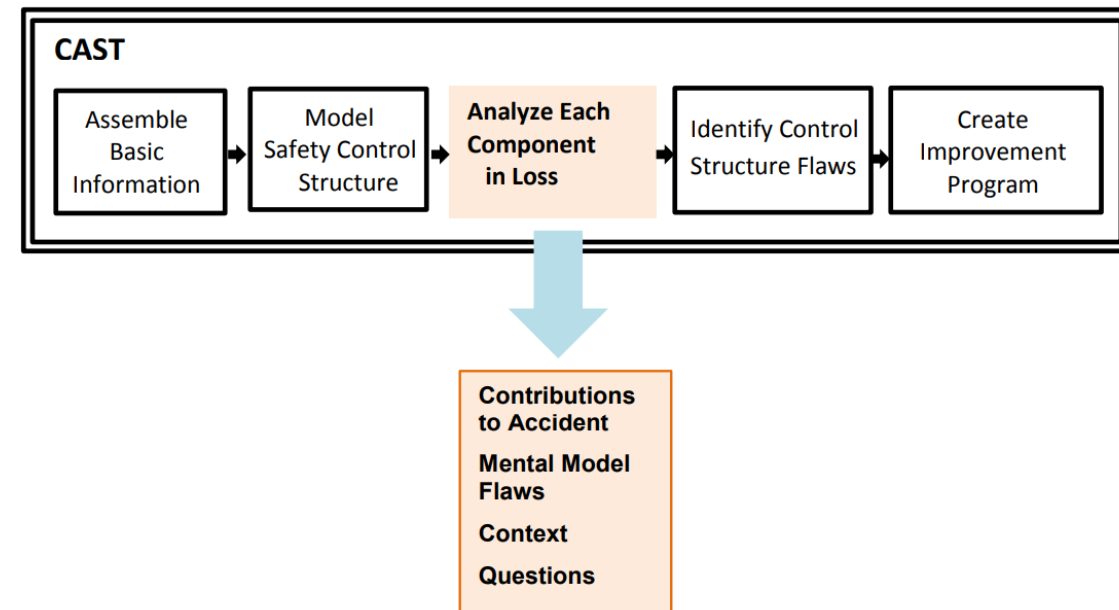
---

## CAST Analysis

### Regulatory Agencies

**Contextual factors explaining the actions, decisions, and process model flaws:**

Pressure for airlines /manufacturers to effectively address safety issues in a way that minimizes costs

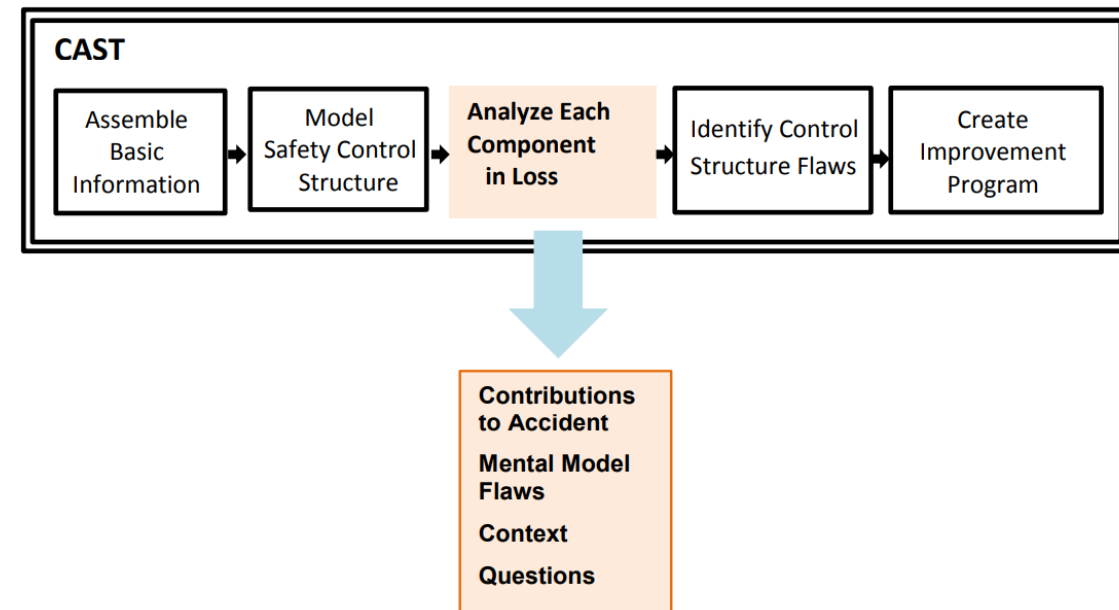


# Case Studies and Best Practices

---

## **CAST Analysis** **Operations Management** **Safety Related Responsibilities**

Develop company operating procedures that ensure safety, provide aircrew training on safety, and update operations procedures to meet regulatory requirements



# Case Studies and Best Practices

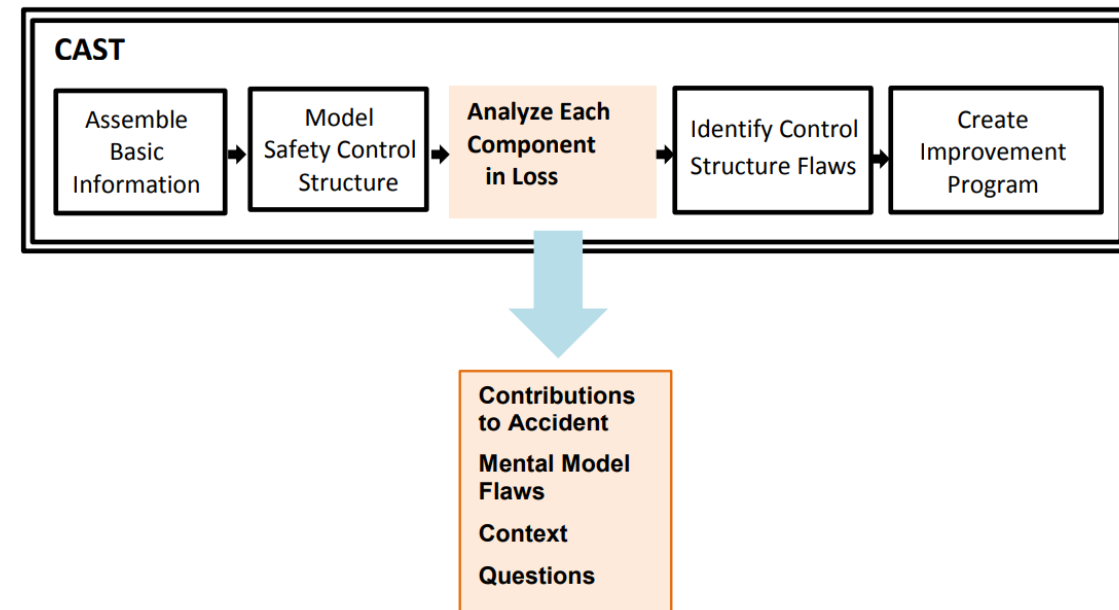
---

## CAST Analysis

## Operations Management

**Contribution (actions, lack of actions, decisions) to the hazardous state:**

Pressure on pilots to minimize delays, and there were no ATC constraints in the training simulators



# Case Studies and Best Practices

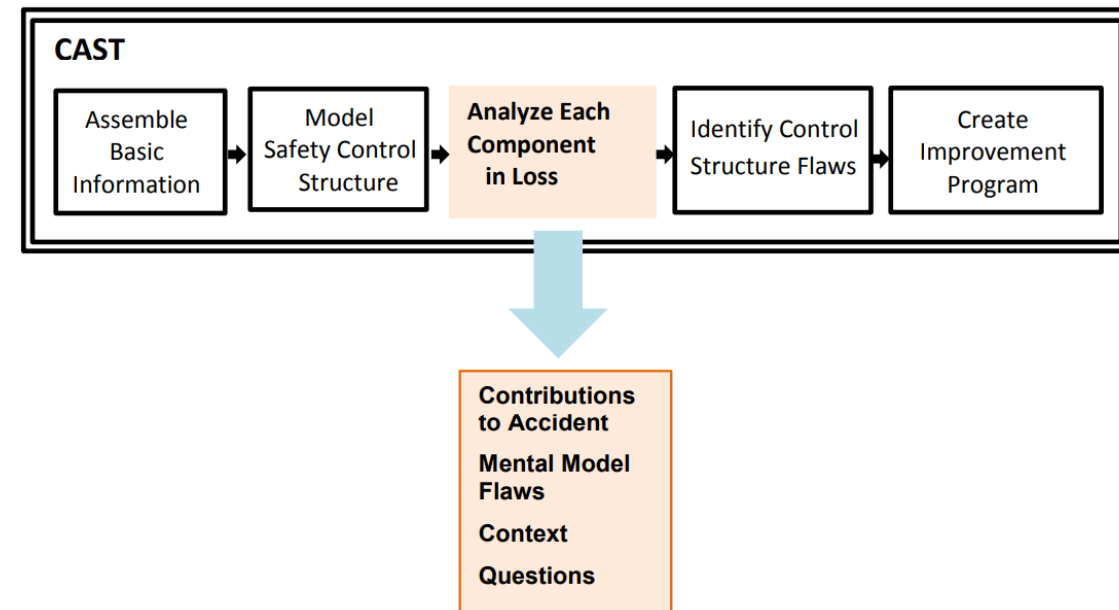
---

## CAST Analysis

### Operations Management

**Flaws in the mental/process model contributing to the actions:**

Focused on efficiency, poor feedback from aircrews on safety, and assumption that compliance with regulations ensures safety



# Case Studies and Best Practices

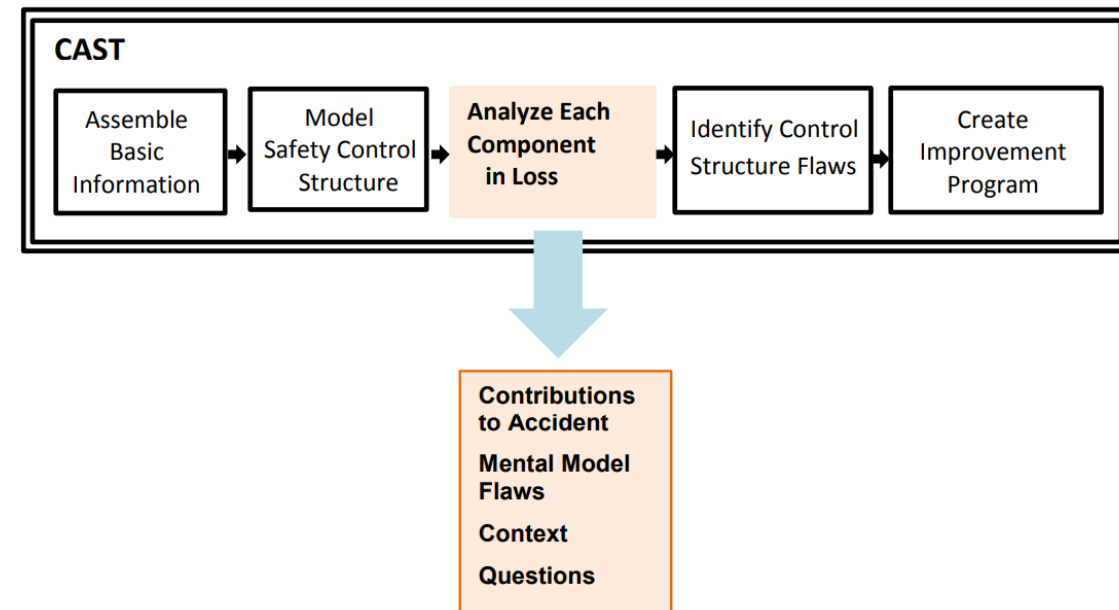
---

## CAST Analysis

## Operations Management

**Contextual factors explaining the actions, decisions, and process model flaws:**

Under pressure and all operating procedures must meet or exceed regulatory requirements to ensure efficiency



# Case Studies and Best Practices

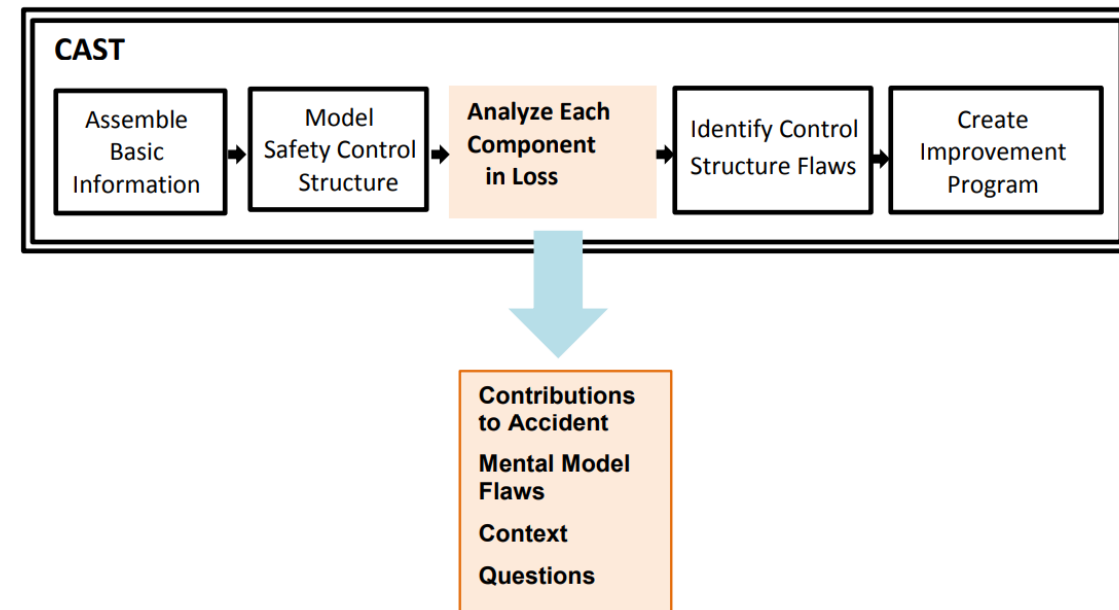
---

## CAST Analysis

### Air Traffic Controllers

### Safety Related Responsibilities

Maintain aircraft separation, inform pilots of weather in area (ATIS) and PIREPs, efficiently prioritize and move aircraft and assist in emergency landings and procedures



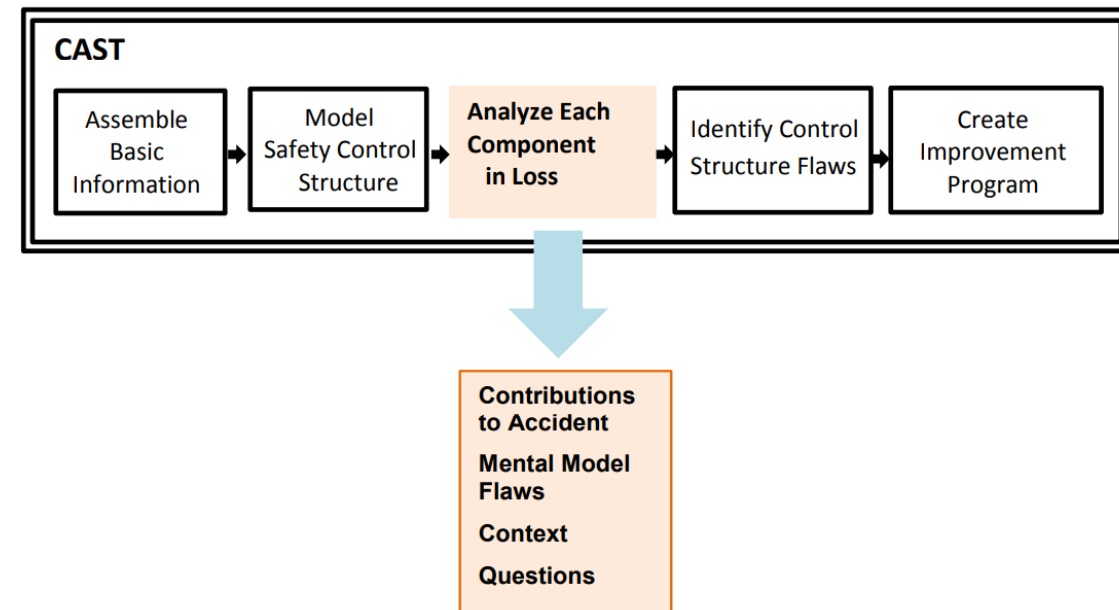
# Case Studies and Best Practices

## CAST Analysis

### Air Traffic Controllers

**Contribution (actions, lack of actions, decisions) to the hazardous state:**

Made a quick decision due to time pressure, ground controller and approach controller used different frequency, poor use of English on the radio





# Case Studies and Best Practices

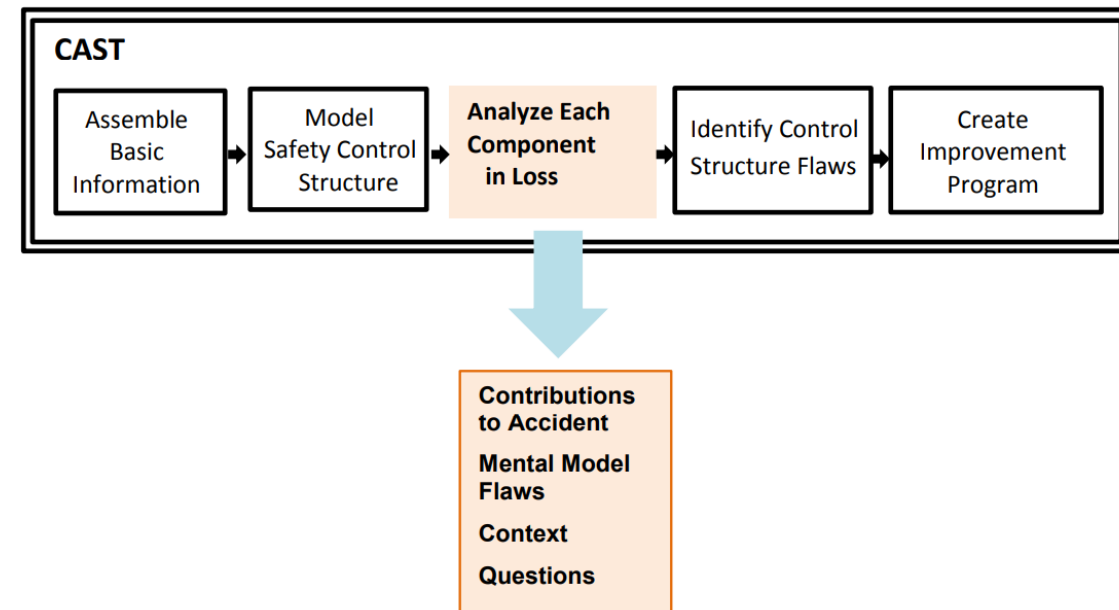
---

## CAST Analysis

### Air Traffic Controllers

**Flaws in the mental/process model contributing to the actions:**

Believed that KLM aircraft could execute the takeoff



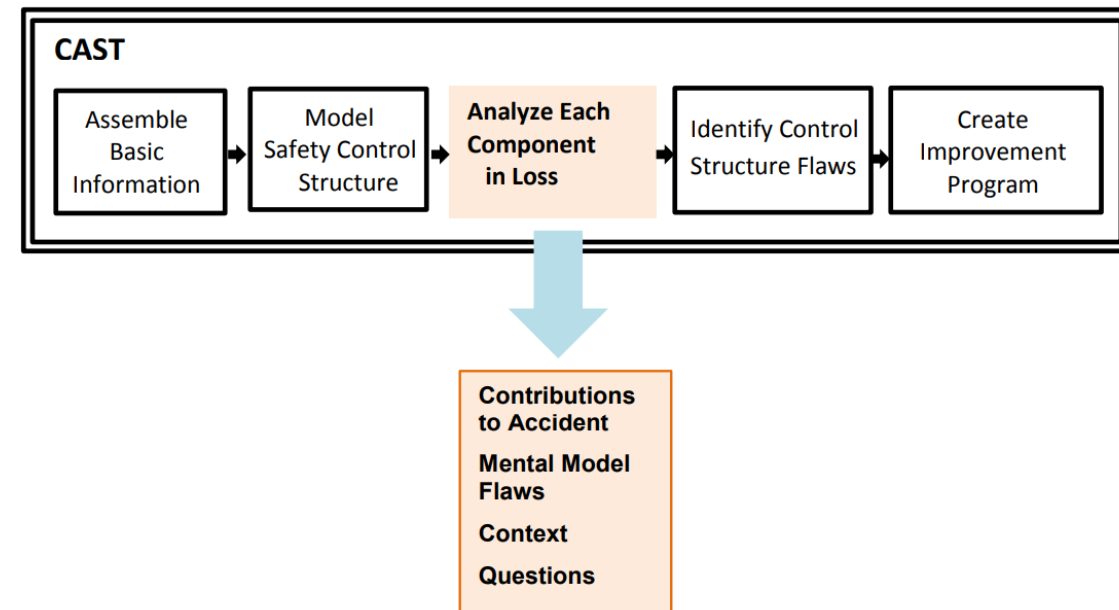
# Case Studies and Best Practices

## CAST Analysis

### Air Traffic Controllers

**Contextual factors explaining the actions, decisions, and process model flaws:**

Mist at the runway, a single runway in use, pressured to expedite operations, knew KLM and Pan Am aircraft executing an emergency landing, unsure of the situation, air traffic control was provided by two controllers (ground and approach), airport facility does not have ground radar, and so the controllers were required to provide aircraft, the airport did not designate the taxiways by numbers, separation under deplorable visibility conditions, and controllers were stressed



# Case Studies and Best Practices

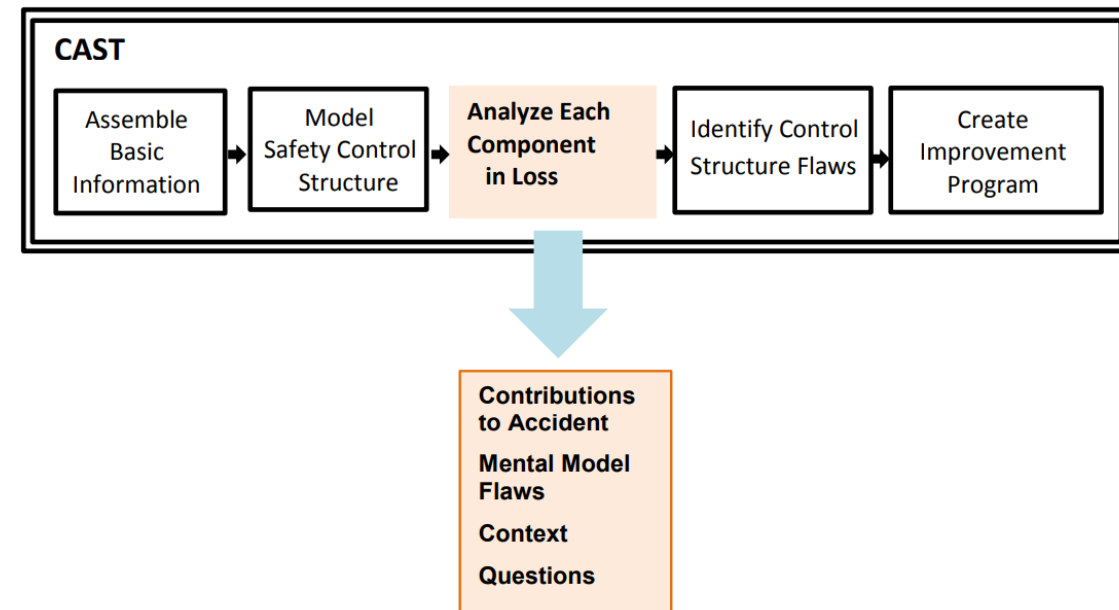
---

## CAST Analysis

### Pilots

### Safety Related Responsibilities

Maintain safe flight, follow emergency procedures, report status inconsistencies, report safety hazards and challenge other pilots on checklists /decisions



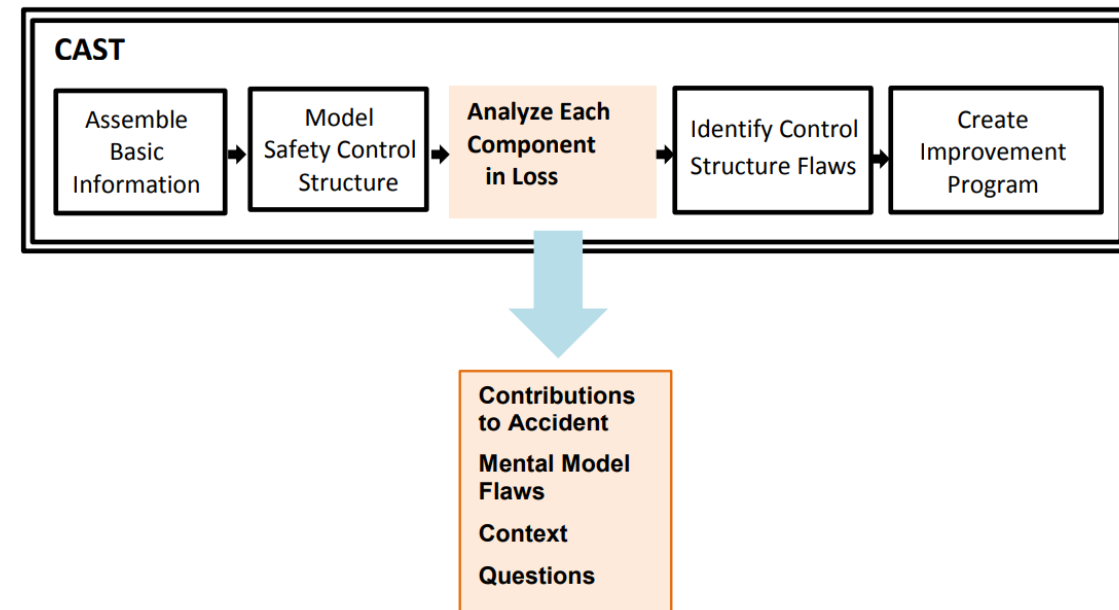
# Case Studies and Best Practices

## CAST Analysis

### Pilots

**Contribution (actions, lack of actions, decisions) to the hazardous state:**

KLM aircraft captain called ground control for start clearance instead of 1st officer, KLM captain called for clearance before checklist was complete, taxi on the runway under heavy mist, poor communication between air traffic controllers and pilots at both aircraft, KLM captain made a quick decision to take-off, and the KLM pilots dismissed KLM flight engineer's question



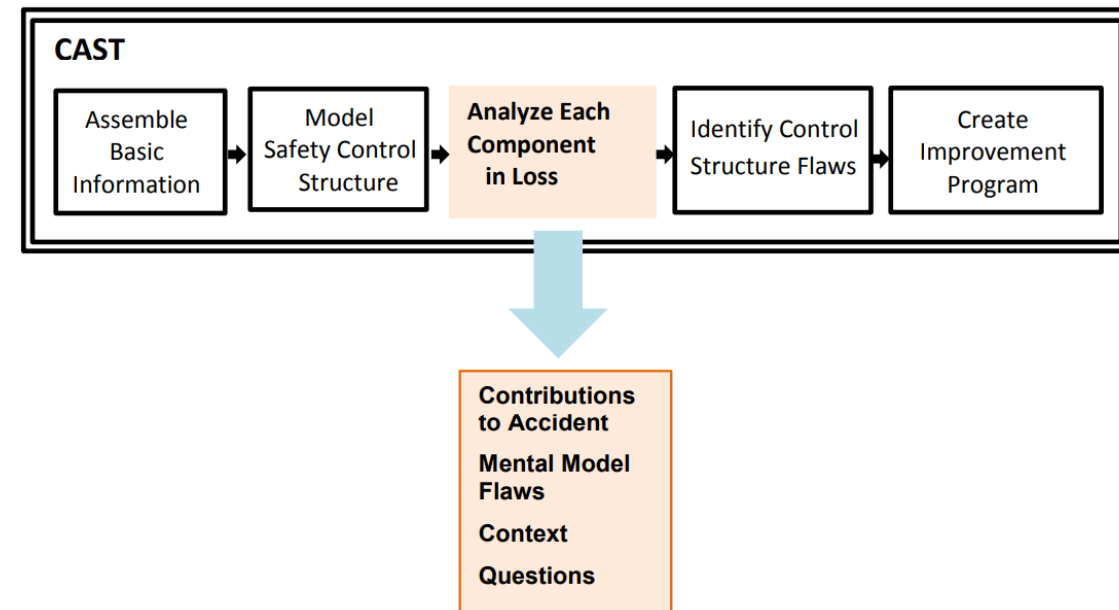
# Case Studies and Best Practices

## CAST Analysis

### Pilots

#### Flaws in the mental/process model contributing to the actions:

Believed that could execute the rapid take-off, Pan Am aircraft captain expressed the desire to hold short of the runway and wait for the KLM to take-off. However, the tower never received that information, believed that controllers provided the correct instructions, and Pan Am did not receive any information from the ATC regarding the exit 3rd taxiway. In contrast, they informed the caption on the 1st and 2nd ones



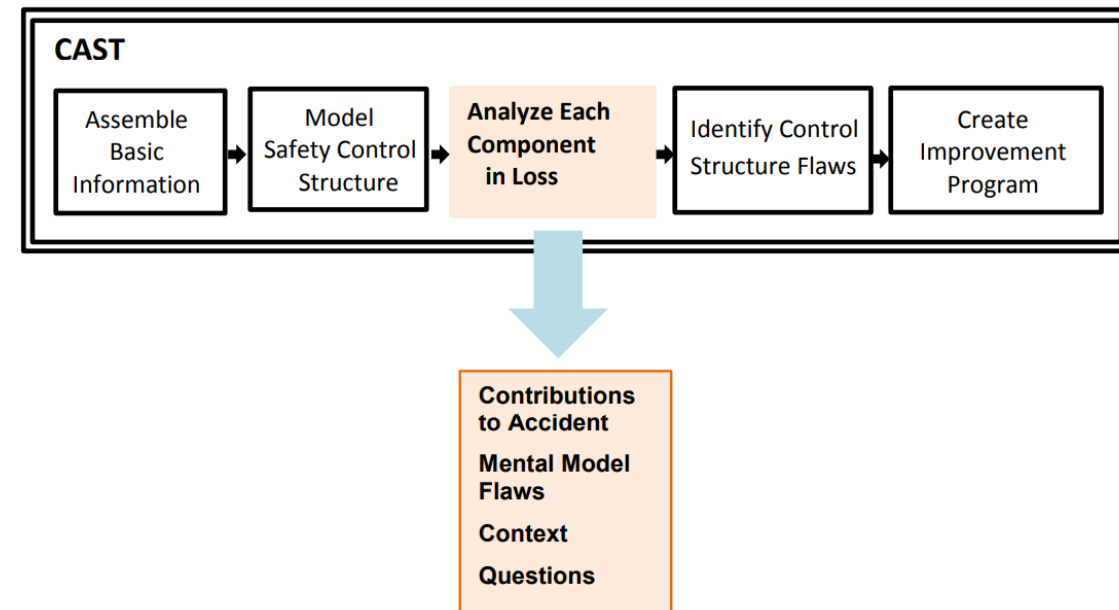
# Case Studies and Best Practices

## CAST Analysis

### Pilots

**Contextual factors explaining the actions, decisions, and process model flaws:**

Highly experienced/ confidence, pushed to minimize delays/avoid missed approaches, mist, unsure of the situation, stressed, pilots were unfamiliar with the airport, and KLM aircraft took fuel prior to the accident.



# Case Studies and Best Practices

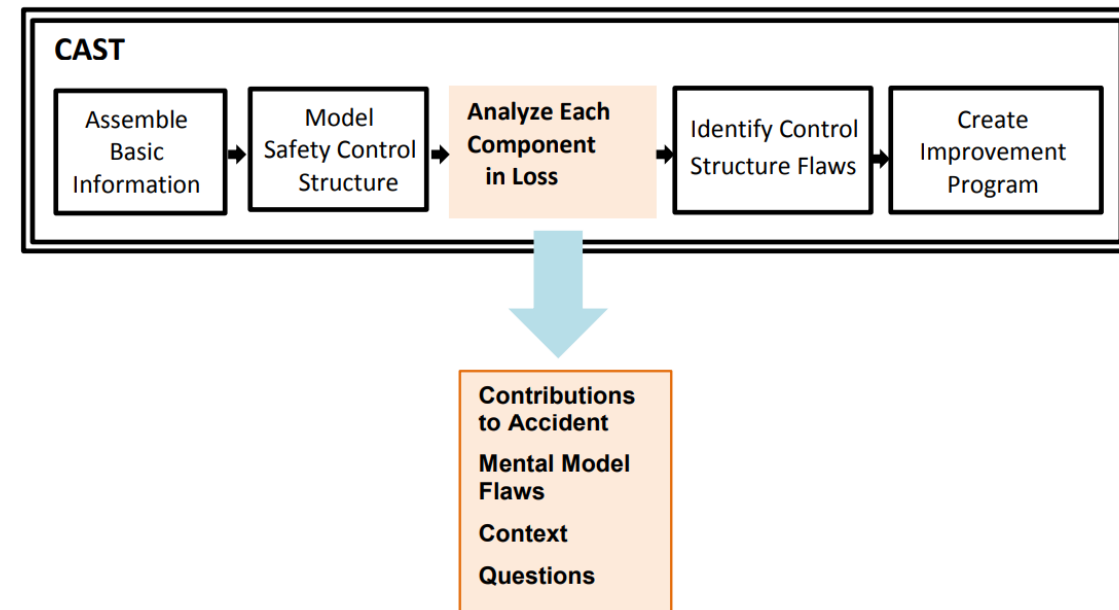
---

## CAST Analysis

### Aircraft

### Safety Related Responsibilities

Maintainability to navigate, remain within airport operating limitations, inform passengers of emergency state and procedures, execute emergency procedures, and safely egress



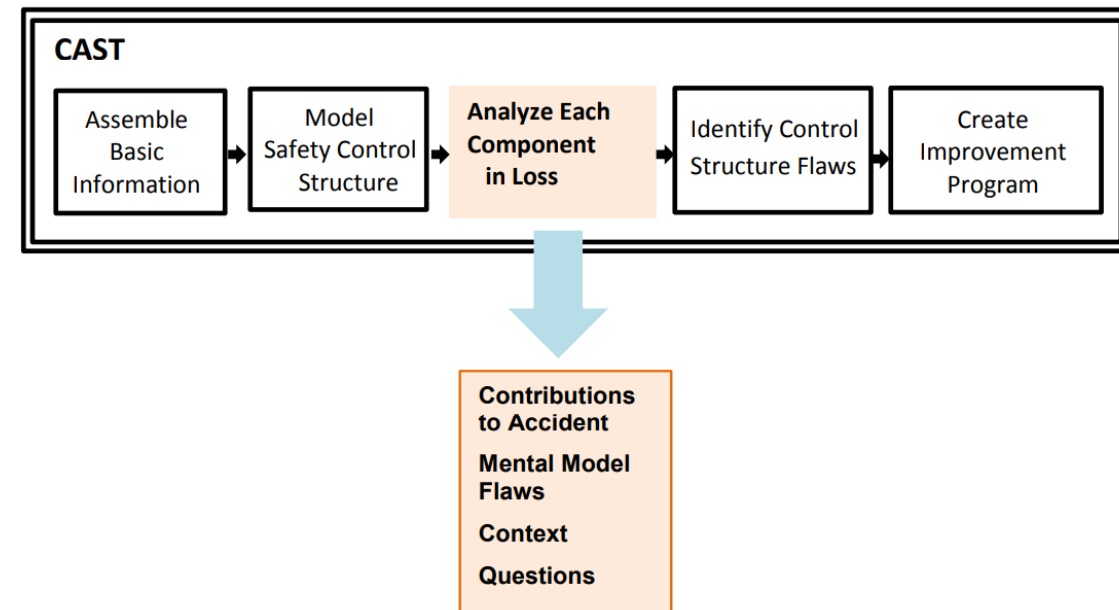
# Case Studies and Best Practices

## CAST Analysis

### Aircraft

**Contribution (actions, lack of actions, decisions) to the hazardous state:**

Inadequate navigation tools to maintain situational awareness, inadequate information concerning conditions at the runway, inadequate protection against weather condition, inadequate specificity with a warning system, and no emergency brake, and on the KLM CVR, the tone of the controller's voice was distorted





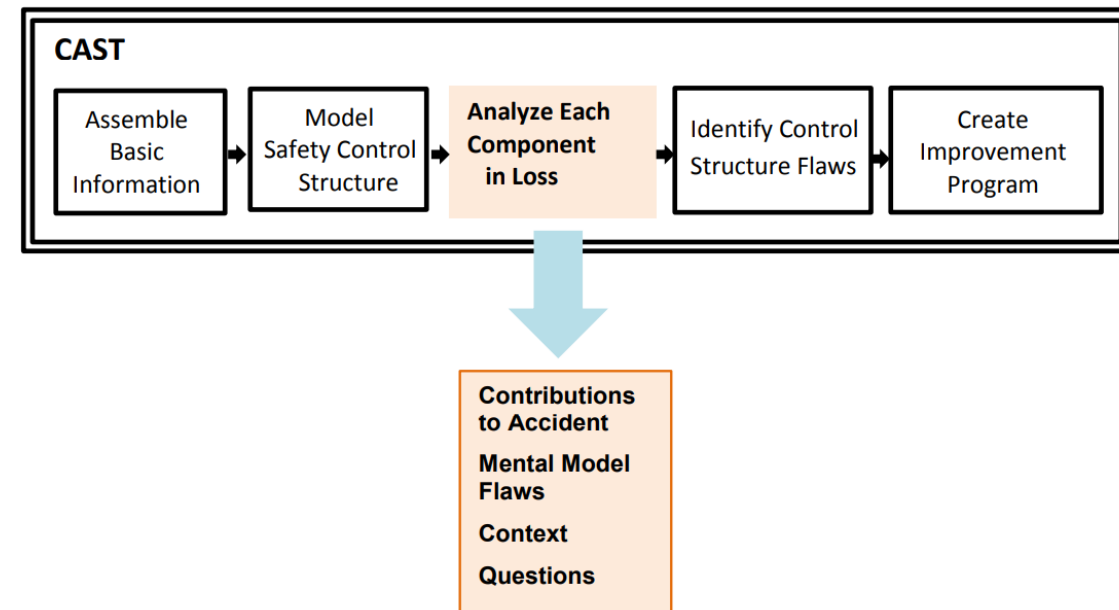
# Case Studies and Best Practices

## CAST Analysis

### Aircraft

**Contextual factors explaining the actions, decisions, and process model flaws:**

Crew emergency procedure training, passenger emergency procedure pre-flight summary, passenger emergency exit procedure card and emergency procedure checklists.

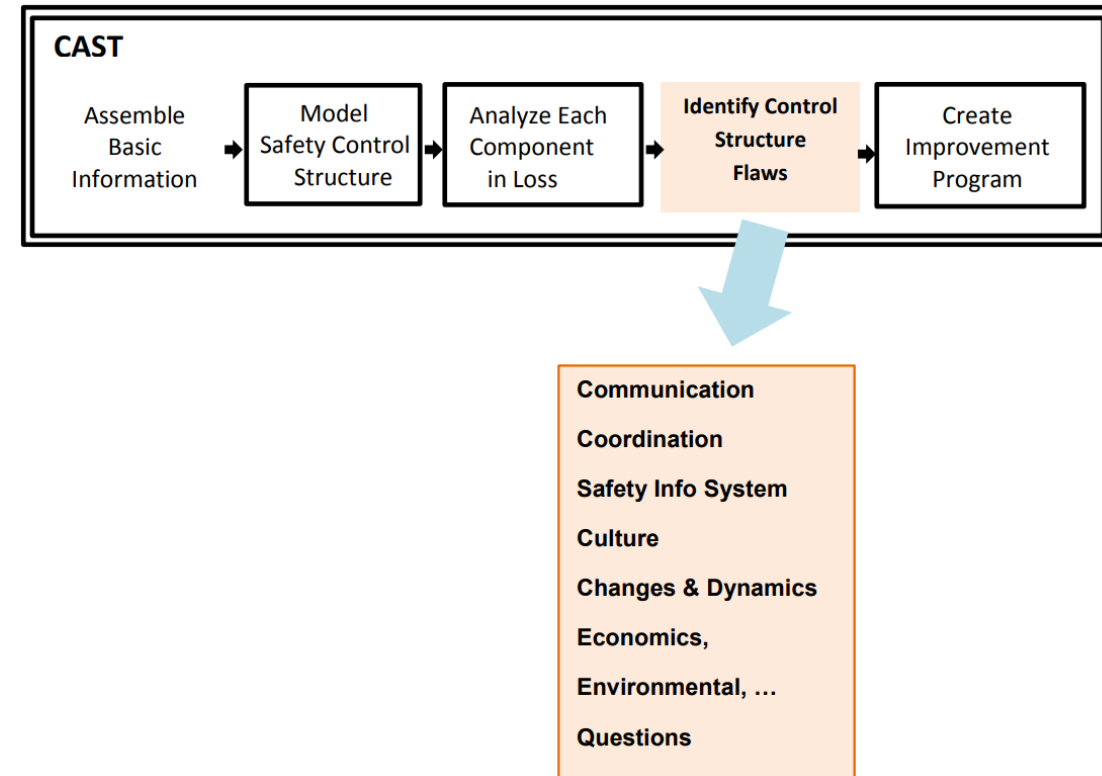


# Case Studies and Best Practices

## CAST Analysis

This part of CAST looks at the control structure as a whole and the systemic factors that led to the ineffectiveness of the designed controls.

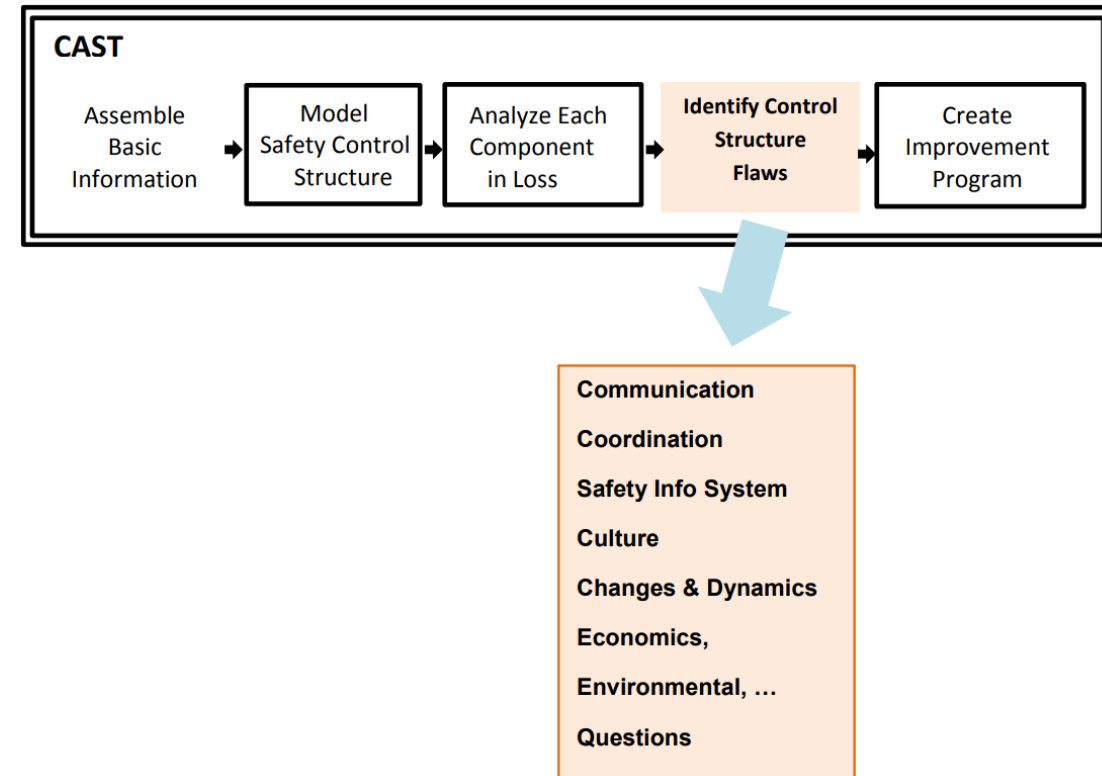
By looking at the system as a whole, rather than individual components, we can identify causal factors that impact how the various safety control structure components interact. These systemic factors provide another way to understand why the individual components may not fulfill their individual safety responsibilities and why together their behavior did not satisfy the system safety constraints.



# Case Studies and Best Practices

## CAST Analysis

This is the truly unique part of a systems approach to accident analysis that is omitted from event-based models, such as the Swiss Cheese or domino models. There are causal factors that can prevent all the barriers from operating correctly and simultaneously cause “holes” in all the protections and cheesecakes that were created to prevent accidents.

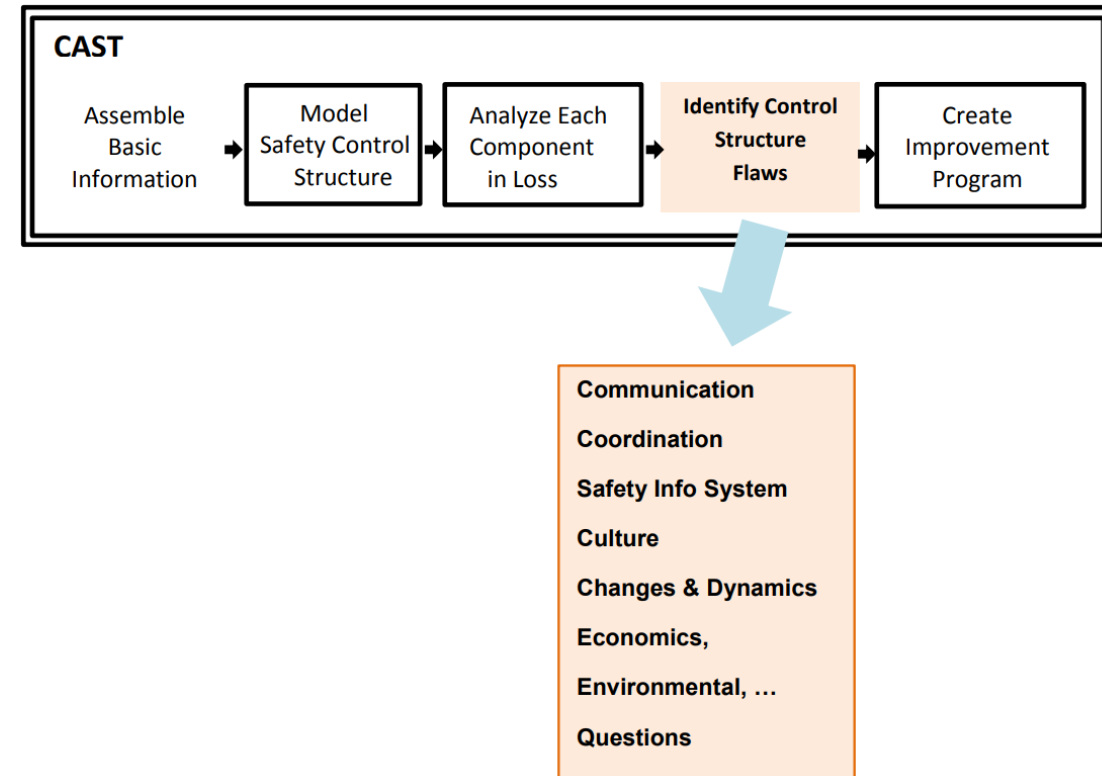


# Case Studies and Best Practices

## CAST Analysis

The following are some of the systemic factors that might be considered

- Communication and coordination
- The safety information system
- Safety culture
- Design of the safety management system
- Changes and dynamics over time: in the system and in the environment
- Internal and external economic and related factors in the system environment not covered previously in the analysis.



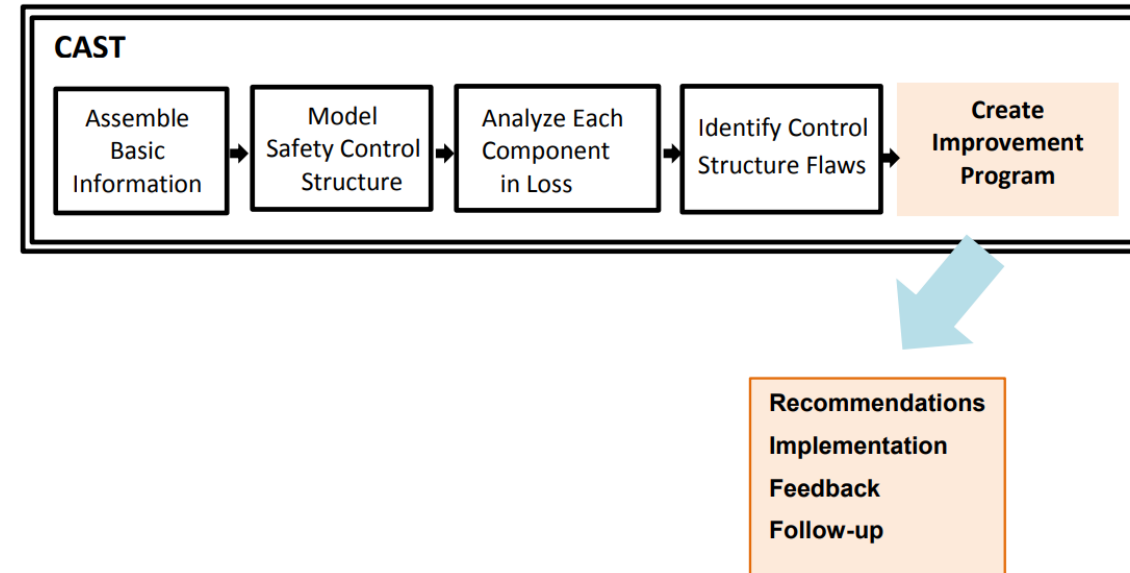
# Case Studies and Best Practices

## CAST Analysis

Once the other parts of the analysis are completed, generating recommendations should be straightforward.

Essentially there are three requirements:

1. Assigning responsibility for implementing the recommendations
2. Checking that they have been implemented
3. Establishing a feedback system to determine whether they were effective in strengthening the controls

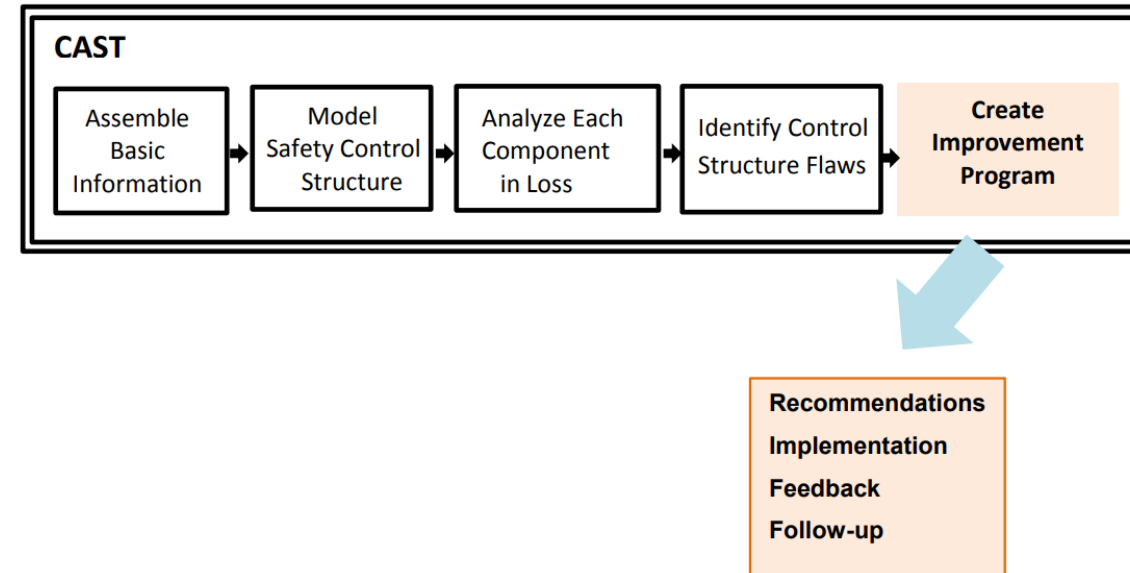


# Case Studies and Best Practices

---

## CAST Analysis

The CAST method was able to detect 50 different causal scenarios. Among these, 14 causes were related to organizational, 31 to human, 16 technology and 5 environmental factors



# Case Studies and Best Practices

---

## Final Conclusions

In this Case study, Tenerife aircraft accident was analyzed by using FTA, FMEA and CAST. The findings indicate that the CAST application provided the most comprehensive analysis, yet there were some overlappings on the findings from different methods. For instance, all methods identified a lack of communication as a primary cause for the accident.

All methods predominantly identified human-related causes. This was due to the nature of the accident and the analysis as focusing on the actions taken by the pilots and air traffic controllers.

# Case Studies and Best Practices

---

## Final Conclusions

However, different methods had different approaches when identifying human-related causes. For instance, FTA application referred to it as “human error”, and FMEA explained it as part of a “wrong action”. In contrast, CAST provided a scenario where unsafe human actions were provided due to inadequate controls in the system.

It is noteworthy that FTA and FMEA aim to reveal the causes of failures that contribute to accidents, whereas CAST aims to identify inadequate controls leading to the accident.



# Case Studies and Best Practices

---

## **Final Conclusions**

This Case study demonstrated that the CAST application was able to cover all failure modes that were identified in FTA and FMEA applications. Additionally, while all methods have value in analyzing accidents, CAST appears to be more useful and convenient to analyze major accidents.

# Preguntas

---



**Manuel Muñoz**

**[haborym@outlook.com](mailto:haborym@outlook.com)**

**+57 313-871-8320**



**[www.airlearningcenter.com](http://www.airlearningcenter.com)**

**[info@airlearningcenter.com](mailto:info@airlearningcenter.com)**

**+593-998-930-107**