Accident and Incident Investigation

Objectives of this Section

- To define the reasons for investigating accident and incidents.
- To outline the process for effectively investigating accidents and incidents.
- To facilitate an effective investigation.

Accident Investigation

- Important part of any safety management system. Highlights the reasons why accidents occur and how to prevent them.
- The primary purpose of accident investigations is to improve health and safety performance by:
  - Exploring the reasons for the event and identifying both the immediate and underlying causes;
  - Identifying remedies to improve the health and safety management system by improving risk control, preventing a recurrence and reducing financial losses.

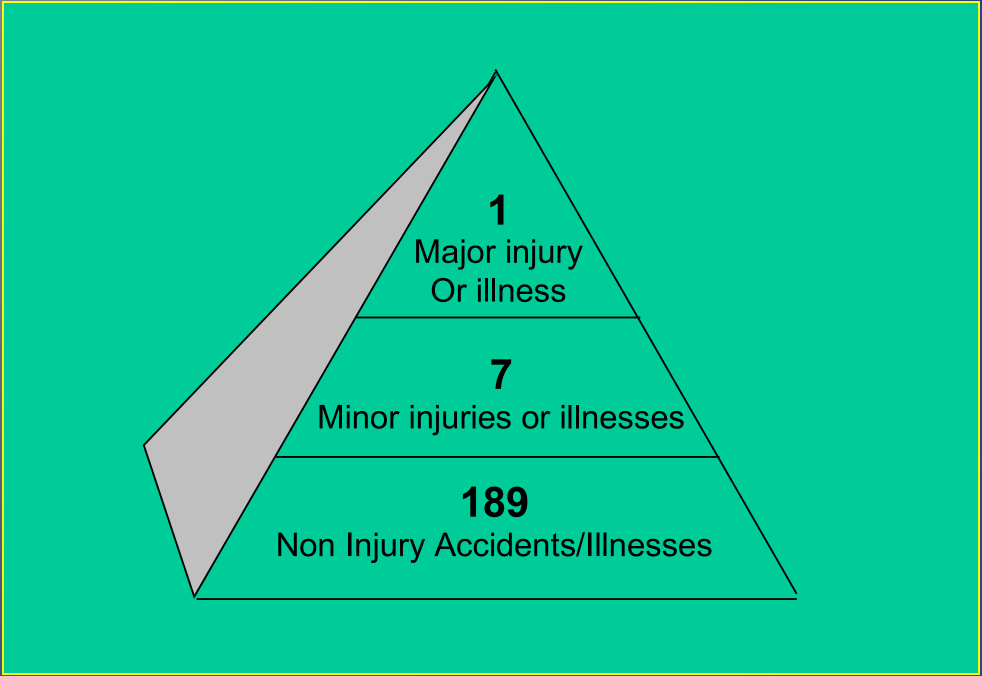
What to Investigate?

- All accidents whether major or minor are caused.

- Serious accidents have the same root causes as minor accidents as do incidents with a potential for serious loss. It is these root causes that bring about the accident, the severity is often a matter of chance.

- Accident studies have shown that there is a consistently greater number of less serious accidents than serious accidents and in the same way a greater number of incidents then accidents.

Many accident ratio studies have been undertaken and the one shown below is based on studies carried out by the Health & Safety Executive.



Accident Studies

- In all cases the 'non injury' incidents had the potential to become events with more serious consequences.
- Such ratios clearly demonstrate that safety effort should be aimed at all accidents including unsafe practices at the bottom of the pyramid, with a resulting improvement in upper tiers.
- Peterson (1978) in defining the principles of safety management says that "*an unsafe act, an unsafe condition, an accident are symptoms of something wrong within the management's system.*"

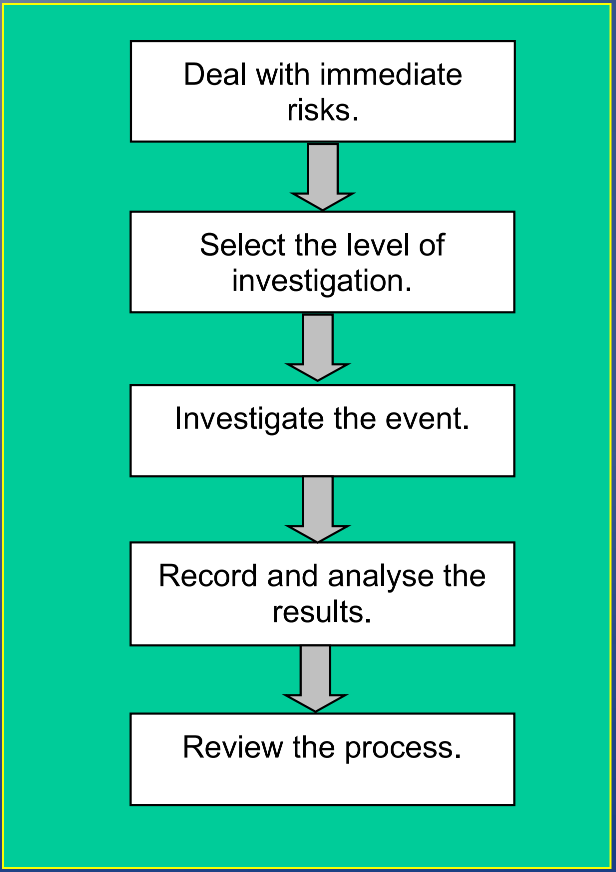
Accident Studies

- All events represent a degree of failure in control and are potential learning experiences. It therefore follows that all accidents should be investigated to some extent.

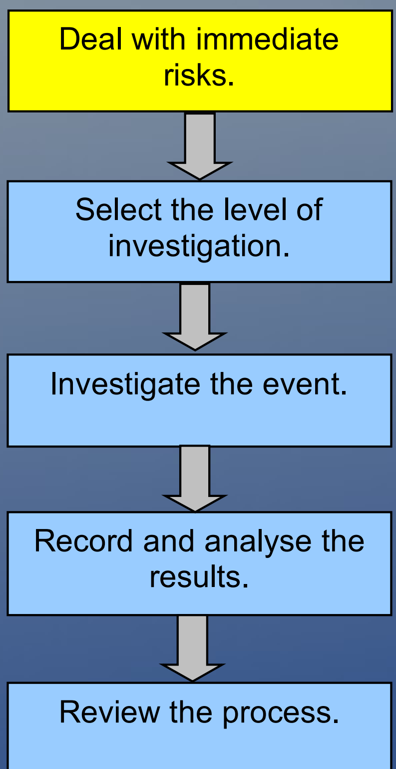
- This extent should be determined by the loss potential, rather then just the immediate effect.

Stages in an Accident/Incident Investigation

The stages in an accident/incident investigation are shown in the following diagram.



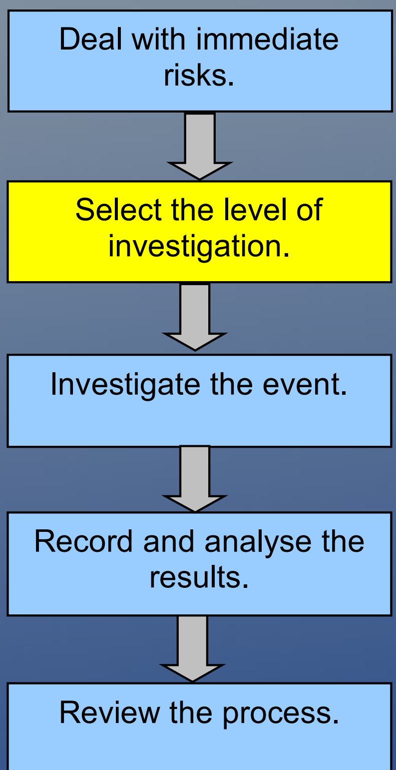
Dealing with Immediate Risks



- When accidents and incidents occur immediate action may be necessary to:
  - Make the situation safe and prevent further injury.
  - Help, treat and if necessary rescue injured persons.

- An effective response can only be made if it has been planned for in advance.

Selecting the level of investigation



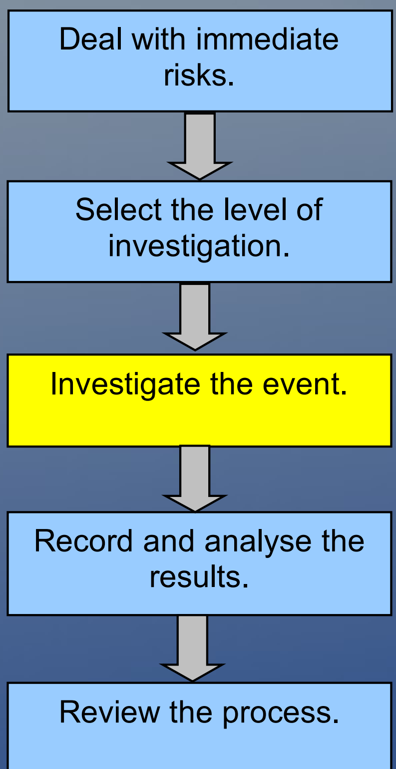
The greatest effort should be put into:

- Those involving severe injuries, ill-health or loss.
- Those which could have caused much greater harm or damage.

These types of accidents and incidents demand more careful investigation and management time. This can usually be achieved by:

- Looking more closely at the underlying causes of significant events.
- Assigning the responsibility for the investigation of more significant events to more senior managers.

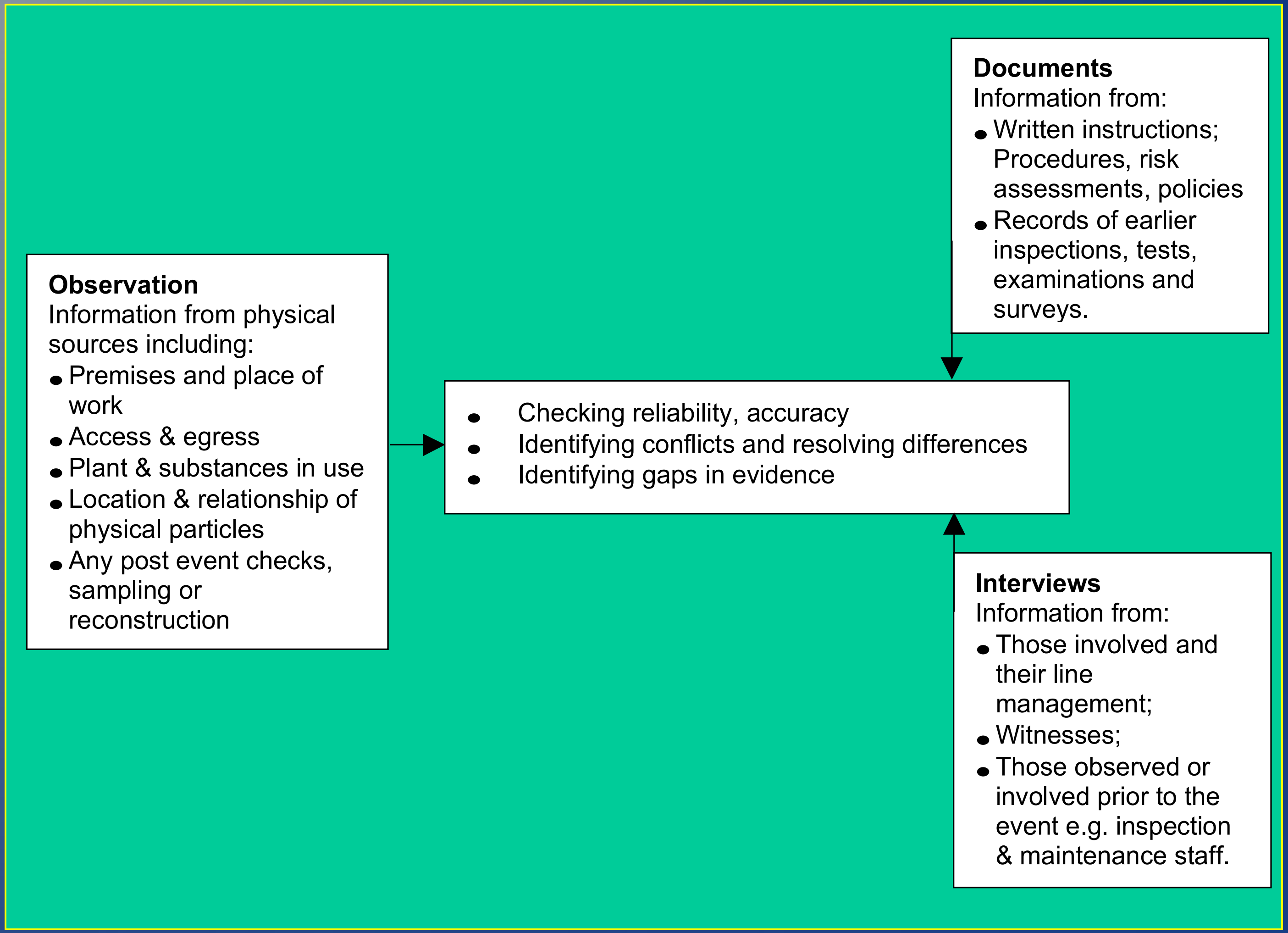
Investigating the Event



The purpose of investigations is to establish:

- The way things were and how they came to be.
- What happened – the sequence of events that led to the outcome.
- Why things happened as they did analysing both the immediate and underlying causes.
- What needs to be done to avoid a repetition and how this can be achieved.

A few sources should give the investigator all that is needed to know.



Interviews

- Interviewing the person(s) involved and witnesses to the accident is of prime importance, ideally in familiar surroundings so as not to make the person uncomfortable.
- The interview style is important with emphasis on prevention rather than blame.
- The person(s) should give an account of what happened in their terms rather than the investigators.

Interviews

- Interviews should be separate to stop people from influencing each other.
- Questions when asked should not be intimidating as the investigator will be seen as aggressive and reflecting a blame culture.

Observation

The accident site should be inspected as soon as possible after the accident. Particular attention should/must be given to:

- Positions of people.
- Personnel protective equipment (PPE).
- Tools and equipment, plant or substances in use.
- Orderliness/Tidiness.

Documents

Documentation to be looked at includes:

- Written instructions, procedures and risk assessments which should have been in operation and followed. The validity of these documents may need to be checked by interview. The main points to look for are:
    - Are they adequate/satisfactory?
    - Were they followed on this occasion?
    - Were people trained/competent to follow it?
- Records of inspections, tests, examination and surveys undertaken before the event. These provide information on how and why the circumstances leading to the event arose.

Determining Causes

- Collect all information and facts which surround the accident.
- Immediate causes are obvious and easy to find. They are brought about by unsafe acts and conditions and are the **ACTIVE FAILURES**. Unsafe acts show poor safety attitudes and indicate a lack of proper training.
- These unsafe acts and conditions are brought about by the so called ‘root causes’. These are the **LATENT FAILURES** and are brought about by failures in organisation and the management’s safety system.

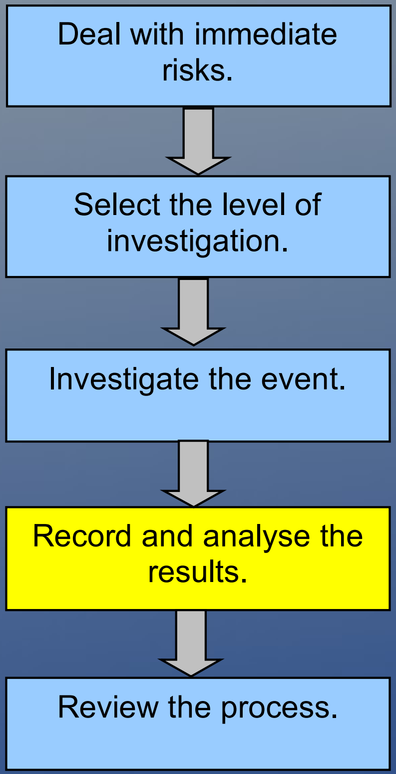
Determine what changes are needed

The investigation should determine what control measures were absent, inadequate or not implemented and so generate remedial action for implementation to correct this.

Generally, remedial actions should follow the hierarchy of risk control:

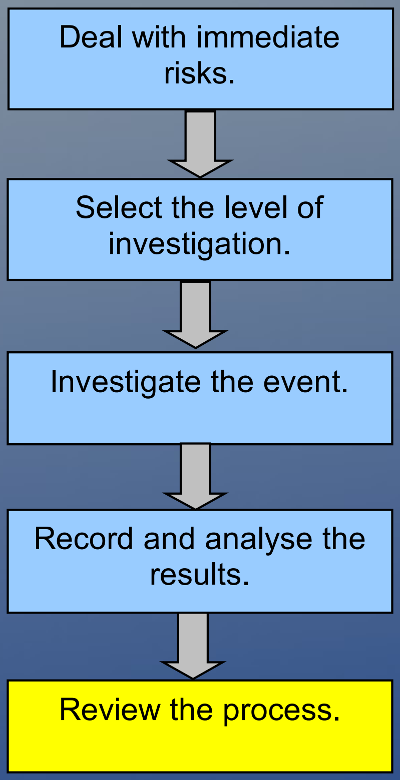
- *Eliminate Risks by substituting the dangerous by the inherently less dangerous.*
- *Combat risks at source by engineering controls and giving collective protective measures priority.*
- *Minimise risk by designing suitable systems of working.*
- *Use PPE as a last resort.*

Recording & Analysing the Results



- Recorded in a similar and systematic manner.
- Provides a historical record of the accident.
- Analysis of the causes and recommended preventative protective measures should be listed.
- Completed as soon after the accident as possible.
- Information on the accident and remedial actions should be passed to all supervisors.
- Appropriate preventative measures may also have to be implemented by such supervisors.
- Investigation reports and accident statistics should be analysed from time to time to identify common causes, features and trends not be apparent from looking at events in isolation.

Reviewing the Process



Reviewing the accident/incident investigation process should consider:

- The results of investigations and analysis.
- The operation of the investigation system (in terms of quality and effectiveness).

Line managers should follow through and action the findings of investigations and analysis. Follow up systems should be established where necessary to keep progress under control.

The investigation system should be examined from time to time to check that it consistently delivers information in accordance with the stated objectives and standards. This usually requires:

- Checking samples of investigation forms to verify the standard of investigation and the judgements made about causation and prioritisation of remedial actions.
- Checking the numbers of incidents, near misses, injury and ill-health events;
- Checking that all events are being reported.

What is your definition of an “Accident”?

What is an Accident

- an unplanned event

- an unplanned incident involving injury or fatality

- a series of events culminating in an unplanned and unforeseen event

How do Accidents occur?

- Accidents (with or without injuries) occur when a series of unrelated events coincide at a certain time and space.

-This can be from a few events to a series of a dozen or more

(Because the coincidence of the series of events is a matter of luck, actual accidents only happen infrequently)

Unsafe Acts

- An unsafe act occurs in approx 85%- 95% of all analyzed accidents with injuries
- An unsafe act is usually the last of a series of events before the accident occurs (it could occur at any step of the event)
- By stopping or eliminating the unsafe act, we can stop the accident from occurring

What is an Accident Investigation?

- A systematic approach to the identification of causal factors and implementation of corrective actions **without placing blame** on or finding personal fault. The information collected during an investigation is essential to determine trends and taking appropriate steps to prevent future accidents.

Which Accidents should be Recorded or Reported?

ALL accidents (including illnesses) shall be recorded and reported through the established procedures and guidance as provided by NOAA Safety Division

Why Investigate Accidents?

- Determine the cause
- Develop and implement corrective actions
- Document the events
- Meet legal requirements

Primary Focus:

PREVENT REOCCURENCE!!!
PREVENT REOCCURENCE!!!
PREVENT REOCCURENCE!!!

Accident vs. Near-Miss

Accident :

Any undesired, unplanned event arising out of a given work-related task which results in physical injury/ illness or damage to property.

Near-Miss :

Events which did not result in injury/illness or damage but had the potential to do so.

Accident Ratio Study

1	Serious or Disabling
10	Minor Injuries
30	Property Damage
600	Accidents with no visible injury or damage
6000	Unsafe Acts or Conditions

Accident Causes

- Unsafe Act

  - an act by the injured person or another person (or both) which caused the accident,

and/or

- Unsafe Condition

  - some environmental or hazardous situation which caused the accident independent of the employee

Accident Causation Model

- **Results of the accident**
  - physical harm
  - property damage
- **Incident Occurrence**
  - contact with
  - type
- **Immediate causes**
  - practices
  - conditions
- **Basic causes**
  - personal factors
  - job factors
  - supervisory performance
  - management policy and decisions

Results of the Accident

- **Physical Harm**
  - catastrophic (multiple deaths)
  - single death
  - disabling
  - serious
  - minor
- **Property Damage**
  - catastrophic
  - major
  - serious
  - minor

Incident Occurrence

- **Type**

  - struck by - struck against
  - slip, trip - fell from
  - caught on - fell on same level
  - caught in - overexertion

- **Contact with**

  - electricity - equipment
  - noise - vibration
  - hazmat - heat/cold
  - radiation - animals/insects

Immediate Causes

- **Practices**

  - operating without authority

  - use equipment improperly

  - not using PPE when required

  - correct lifting procedures not established

  - drinking or drug use

  - horseplay

  - equipment not properly secured

Immediate Causes (cont'd)

- **Conditions**

  - ineffective guards

  - unserviceable tools and equipment

  - inadequate warning systems

  - bad housekeeping practices

  - poor work space illumination

  - unhealthy work environment

Basic Causes

- **Personal Factors**
  - lack of knowledge or skill
  - improper motivation
  - physical or mental condition
  - literacy or ability

- **Job Factors**
  - Physical environment
  - sub-standard equipment
  - abnormal usage
  - wear and tear
  - inadequate standards
  - design and maintenance

Basic Causes (cont'd)

- **Supervisory Performance**
  - inadequate instructions
  - failure of SOPs
  - rules not enforced
  - hazards not corrected
  - devices not provided

- **Management Policy and Decisions**
  - set measurable standards
  - measure work in progress
  - evaluate work vs. standards
  - correct performance

No animals were hurt as a result of this accident

Severity of Incident

(NOAA Safety Policy NAO-209-1)

- **Major**
  - Employee fatality,
  - Hospitalization of 3 or more employees,
  - Permanent employee disability,
  - Five or more lost workdays,
  - Conditions that could pose an imminent and threat of serious injury/illness to other employees
  - Property losses in excess of $1 Million

- **Minor**
  - All other (less serious) incidents and unsafe conditions reported by employees

Who Investigates?

- **Major Accidents**
  - NOAA “GO TEAM” Investigation Team
  - LO Representative
  - Other agencies such as NTSB, USCG, OSHA

- **Minor Accidents**
  - First-Line Supervisor
  - Site Director or Manager
  - Site Safety Representative
  - NOAA SECO (if needed)

Investigator’s Qualifications

- Technical knowledge
- Objectivity
- Analytical approach
- Familiarity with the job, process or operation
- Tact in communicating
- Intellectual honesty
- Inquisitiveness and curiosity

When to Investigate?

- Immediately after incident
  - Witness memories fade
  - Equipment and clues are moved
- Finish investigation quickly

What to Investigate?

- All accidents and near-misses
  - Conduct investigation upon first notification
  - Keeping the scene in-tact and recording witnesses statements early is key to a successful investigation

Accident Investigation Kit

May Include:

- Digital Camera
- Report forms, clipboard, pens
- Barricade tape
- Flashlight
- Tape measure
- Tape recorder
- Personal Protective Equipment (as appropriate)

The Accident Occurs

- Employee or co-worker immediately reports the accident to a supervisor
- Supervisor secures/assesses the scene to prevent additional injuries to other employees, before assisting the injured employee
- Supervisor treats the injury or seeks medical treatment for the injured
- The accident scene is left intact
- Site safety rep is contacted to assist the supervisor in the investigation of the accident.

Beginning the Investigation

- Gather investigation members and kit
- Report to the scene
- Look at the big picture
- Record initial observations
- Take pictures

What's Involved?

- Who was injured?
- Medication, drugs, or alcohol?
- Was employee ill or fatigued?
- Environmental conditions?

Witnesses

- Who witnessed the accident?
- Was a supervisor or Team Lead nearby?
- Where were other employees?
- Why didn't anyone witness the accident (working alone, remote areas)?

Interviewing Tips

- Discuss what happened leading up to and after the accident
- Encourage witnesses to describe the accident in their own words
- Don’t be defensive or judgmental
- Use open-ended questions
- Do not interrupt the witness

What was Involved?

- Machine, tool, or equipment
- Chemicals
- Environmental conditions
- Field season prep operations

Time of Accident

- Date and time?
- Normal shift or working hours?
- Employee coming off a vacation?

Accident Location

- Work area
- On, under, in, near
- Off-site address
- Doing normal job duties
- Performing non-routine or routine tasks (i.e., properly trained)

Employee's Activity

- Motion conducted at time of accident
- Repetitive motion?
- Type of material being handled

Accident Narrative

- Describe the details so the reader can clearly picture the accident
- Specific body parts affected
- Specific motions

of injured employee

just before,

during, and

after accident

Causal Factors

- Try not to accept single cause theory
- Identify underlying causes (root)
- Primary cause
- Secondary causes
  - Contributing causes
  - Effects

Corrective Actions Taken

- Include immediate interim controls implemented at the time of accident
- Recommended corrective actions
  - Employee training
  - Preventive maintenance activities
  - Better operating procedures
  - Hazard recognition (ORM)
  - **Management awareness of risks involved**

Immediate Notification

- Supervisor shall complete the NOAA Web Based Accident/ Illness Report Form and submit within 24 hours of incident occurrence (8 hours for major incidents).

Accident Analysis Summary

- Investigate accident immediately
- Determine who was involved and who witnessed it
- Ascertain what items or equipment were involved
- Record detailed description
- Determine causal factors
- Implement corrective actions

Questions ??

Quiz

1. What is an Accident Investigation?

   a. A systematic approach to the identification of causal factors and implementation of corrective actions.
   b. Finding personal fault and placing blame.
   c. The appropriate steps to prevent future actions.
   d. The essential step to determine trends and taking action against person or persons at fault.

2. Which Accidents should be Recorded or Reported?

   a. Only on the job accidents.
   b. ALL accidents (including illnesses) shall be recorded and reported.
   c. Only on the job accidents on illnesses that occur on the job and reported within 8 hours.
   d. All accidents shall be recorded and reported.

3. Why Investigate Accidents?

a. To develop and implement corrective actions.
b. To document the events.
c. The Primary Focus is to PREVENT REOCCURENCE!!!
d. To determine the cause.

4. Accident vs. Near-Miss?

a. Any unplanned event arising out of work that resulted in injury vs. Any event which did not result in injury but had potential to do so.
b. Any unsafe work habit vs. Any Hazardous working conditions.
c. Any event which warns us of a problem vs. Any circumstances that result in injury or property damage.

5. Which of the following are the basic areas that are looked at in an Accident Investigation.

   a. Policies.
   b. Equipment.
   c. Training.
   d. All of the above.

Accident Investigation

Accident analysis is carried out in order to determine the cause or causes of an accident or series of accidents so as to prevent further incidents of a similar kind. It is also known as accident investigation.

Accident Investigation

It may be performed by a range of experts, including forensic scientists, forensic engineers or health and safety advisers. Accident investigators, particularly those in the aircraft industry, are colloquially known as "tin-kickers".

Sequence

Accident analysis is performed in four steps:

Fact gathering: After an accident happened a forensic process starts to gather all possibly relevant facts that may contribute to understanding the accident.

Sequence
Fact Analysis:

After the forensic process has been completed or at least delivered some results, the facts are put together to give a "big picture." The history of the accident is reconstructed and checked for consistency and plausibility.

Sequence
Conclusion Drawing:

If the accident history is sufficiently informative, conclusions can be drawn about causation and contributing factors.

Sequence
Counter-measures:

In some cases the development of counter-measures is desired or recommendations have to be issued to prevent further accidents of the same kind.

Methods

There exist numerous forms of Accident Analysis methods. These can be divided into three categories:

Methods
Causal Analysis

Causal Analysis uses the principle of causality to determine the course of events. Though people casually speak of a "chain of events", results from Causal Analysis usually have the form of directed a-cyclic graphs-the nodes being events and the edges the cause-effect relations. Methods of Causal Analysis differ in their respective notion of causation.

Methods
Expert Analysis

Expert Analysis relies on the knowledge and experience of field experts. This form of analysis usually lacks a rigorous (formal/semiformal) methodological approach.
This usually affects falsify-ability and objectivity of analyses. This is of importance when conclusions are heavily disputed among experts.

Methods
Organizational Analysis

Organizational Analysis relies on systemic theories of organization. Most theories imply that if a system's behaviour stayed within the bounds of the ideal organization then no accidents can occur.

Methods
Organizational Analysis

Organizational Analysis can be falsified and results from analyses can be checked for objectivity. Choosing an organizational theory for accident analysis comes from the assumption that the system to be analysed conforms to that theory.

Using Digital Photographs to Extract Evidence

Once all available data has been collected by accident scene investigators and law enforcement officers, camera matching, photogrammetry or rectification can be used to determine the exact location of physical evidence shown in the accident scene photos.

Camera matching:

Camera matching uses accident scene photos that show various points of evidence. The technique uses CAD software to create a 3-dimensional model of the accident site and roadway surface.

Camera matching:

All survey data and photos are then imported into a three dimensional software package like 3D Studio Max.
A virtual camera can be then be positioned relative to the 3D roadway surface.
Physical evidence is then mapped from the photos onto the 3D roadway to create a three dimensional accident scene drawing.

Photogrammetry

Photogrammetry is used to determine the three-dimensional geometry of an object on the accident scene from the original two dimensional photos.

Photogrammetry

The photographs can be used to extract evidence that may be lost after the accident is cleared. Photographs from several viewpoints are imported into software like PhotoModeler.

Photogrammetry

The forensic engineer can then choose points common to each photo. The software will calculate the location of each point in a three dimensional coordinate system.

Rectification

Photographic rectification is also used to analyze evidence that may not have been measured at the accident scene. Two dimensional rectification transforms a single photograph into a top-down view. Software like PC-Rect can be used to rectify a digital photograph.

Failure mode and effects analysis

Failure mode and effects analysis

Failure Mode and Effects Analysis (FMEA) was one of the first systematic techniques for failure analysis.

It was developed by reliability engineers in the 1950s to study problems that might arise from malfunctions of military systems.

Failure mode and effects analysis

A FMEA is often the first step of a system reliability study. It involves reviewing as many components, assemblies, and subsystems as possible to identify failure modes, and their causes and effects.

Failure mode and effects analysis

For each component, the failure modes and their resulting effects on the rest of the system are recorded in a specific FMEA worksheet.
There are numerous variations of such worksheets.
A FMEA is mainly a qualitative analysis.

Failure mode and effects analysis

A few different types of FMEA analysis exist, like

- Functional,
- Design, and
- Process FMEA.

Failure mode and effects analysis

Sometimes the FMEA is called FMECA to indicate that Criticality analysis is performed also.

Failure mode and effects analysis

An FMEA is an inductive reasoning (forward logic) single point of failure analysis and is a core task in reliability engineering, safety engineering and quality engineering.
Quality engineering is specially concerned with the "Process" (Manufacturing and Assembly) type of FMEA.

Failure mode and effects analysis

A successful FMEA activity helps to identify potential failure modes based on experience with similar products and processes - or based on common physics of failure logic.

Failure mode and effects analysis

It is widely used in development and manufacturing industries in various phases of the product life cycle.
Effects analysis refers to studying the consequences of those failures on different system levels.

Failure mode and effects analysis

Functional analyses are needed as an input to determine correct failure modes, at all system levels, both for functional FMEA or Piece-Part (hardware) FMEA.

Failure mode and effects analysis

A FMEA is used to structure Mitigation for Risk reduction based on either failure (mode) effect severity reduction or based on lowering the probability of failure or both.

Failure mode and effects analysis

The FMEA is in principle a full inductive (forward logic) analysis, however the failure probability can only be estimated or reduced by understanding the failure mechanism.

Failure mode and effects analysis

Ideally this probability shall be lowered to "impossible to occur" by eliminating the (root) causes. It is therefore important to include in the FMEA an appropriate depth of information on the causes of failure (deductive analysis).

Failure mode and effects analysis

The FME(C)A is a design tool used to systematically analyze postulated component failures and identify the resultant effects on system operations. The analysis is sometimes characterized as consisting of two sub-analyses, the first being the failure modes and effects analysis (FMEA), and the second, the criticality analysis (CA).

Failure mode and effects analysis

Successful development of an FMEA requires that the analyst include all significant failure modes for each contributing element or part in the system. FMEAs can be performed at the system, subsystem, assembly, subassembly or part level.

Failure mode and effects analysis

The FMECA should be a living document during development of a hardware design. It should be scheduled and completed concurrently with the design. If completed in a timely manner, the FMECA can help guide design decisions. The usefulness of the FMECA as a design tool and in the decision making process is dependent on the effectiveness and timeliness with which design problems are identified.

Failure mode and effects analysis

Timeliness is probably the most important consideration. In the extreme case, the FMECA would be of little value to the design decision process if the analysis is performed after the hardware is built.

Failure mode and effects analysis

While the FMECA identifies all part failure modes, its primary benefit is the early identification of all critical and catastrophic subsystem or system failure modes so they can be eliminated or minimized through design modification at the earliest point in the development effort.

Failure mode and effects analysis

Therefore, the FMECA should be performed at the system level as soon as preliminary design information is available and extended to the lower levels as the detail design progresses.

Failure mode and effects analysis

Remark: For more complete scenario modelling other type of Reliability analysis may be considered, for example fault tree analysis(FTA); a deductive (backward logic) failure analysis that may handle multiple failures within the item and/or external to the item including maintenance and logistics. It starts at higher functional / system level. A FTA may use the basic failure mode FMEA records or an effect summary as one of its inputs (the basic events). Interface hazard analysis, Human error analysis and others may be added for completion in scenario modelling.

Functional analysis

The analysis may be performed at the functional level until the design has matured sufficiently to identify specific hardware that will perform the functions; then the analysis should be extended to the hardware level. When performing the hardware level FMECA, interfacing hardware is considered to be operating within specification. In addition, each part failure postulated is considered to be the only failure in the system (i.e., it is a single failure analysis).

Functional analysis

In addition to the FMEAs done on systems to evaluate the impact lower level failures have on system operation, several other FMEAs are done. Special attention is paid to interfaces between systems and in fact at all functional interfaces. The purpose of these FMEAs is to assure that irreversible physical and/or functional damage is not propagated across the interface as a result of failures in one of the interfacing units.

Functional analysis

These analyses are done to the piece part level for the circuits that directly interface with the other units. The FMEA can be accomplished without a CA, but a CA requires that the FMEA has previously identified system level critical failures. When both steps are done, the total process is called a FMECA.

Ground rules

The ground rules of each FMEA include a set of project selected procedures; the assumptions on which the analysis is based; the hardware that has been included and excluded from the analysis and the rationale for the exclusions. The ground rules also describe the indenture level of the analysis, the basic hardware status, and the criteria for system and mission success.

Ground rules

Every effort should be made to define all ground rules before the FMEA begins; however, the ground rules may be expanded and clarified as the analysis proceeds. A typical set of ground rules (assumptions) follows:

Ground rules

- Only one failure mode exists at a time.
- All inputs (including software commands) to the item being analyzed are present and at nominal values.
- All consumables are present in sufficient quantities.
- Nominal power is available

Benefits

Major benefits derived from a properly implemented FMECA effort are as follows:

Benefits

It provides a documented method for selecting a design with a high probability of successful operation and safety.

Benefits

A documented uniform method of assessing potential failure mechanisms, failure modes and their impact on system operation, resulting in a list of failure modes ranked according to the seriousness of their system impact and likelihood of occurrence.

Benefits

Early identification of single failure points (SFPS) and system interface problems, which may be critical to mission success and/or safety. They also provide a method of verifying that switching between redundant elements is not jeopardized by postulated single failures.

Benefits

An effective method for evaluating the effect of proposed changes to the design and/or operational procedures on mission success and safety.

Benefits

A basis for in-flight troubleshooting procedures and for locating performance monitoring and fault-detection devices.

Benefits

Criteria for early planning of tests.

Basic terms

The following covers some basic FMEA terminology.

Failure

The loss under stated conditions.

Basic terms
Failure mode

The specific manner or way by which a failure occurs in terms of failure of the item (being a part or (sub) system) function under investigation; it may generally describe the way the failure occurs. It shall at least clearly describe a (end) failure state of the item (or function in case of a Functional FMEA) under consideration. It is the result of the failure mechanism (cause of the failure mode). For example; a fully fractured axle, a deformed axle or a fully open or fully closed electrical contact are each a separate failure mode.

Basic terms
Failure cause and/or mechanism

Defects in requirements, design, process, quality control, handling or part application, which are the underlying cause or sequence of causes that initiate a process (mechanism) that leads to a failure mode over a certain time. A failure mode may have more causes.

Basic terms
Failure cause and/or mechanism

For example; "fatigue or corrosion of a structural beam" or "fretting corrosion in a electrical contact" is a failure mechanism and in itself (likely) not a failure mode. The related failure mode (end state) is a "full fracture of structural beam" or "an open electrical contact". The initial Cause might have been "Improper application of corrosion protection layer (paint)" and /or "(abnormal) vibration input from another (possible failed) system".

Basic terms / Failure effect

Immediate consequences of a failure on operation, function or functionality, or status of some item.

Indenture levels (bill of material or functional breakdown)

An identifier for system level and thereby item complexity. Complexity increases as levels are closer to one.

Local effect

The failure effect as it applies to the item under analysis.

Next higher level effect

The failure effect as it applies at the next higher indenture level.

End effect

The failure effect at the highest indenture level or total system.

Detection

The means of detection of the failure mode by maintainer, operator or built in detection system, including estimated dormancy period (if applicable)

Risk Priority Number (RPN)

Cost (of the event) * Probability (of the event occurring) * Detection (Probability that the event would not be detected before the user was aware of it)

Severity

The consequences of a failure mode. Severity considers the worst potential consequence of a failure, determined by the degree of injury, property damage, system damage and/or time lost to repair the failure.

Remarks / mitigation / actions

Additional info, including the proposed mitigation or actions used to lower a risk or justify a risk level or scenario.

Example FMEA Worksheet

FMEA Ref.	Item	Potential failure mode	Potential cause(s) / mechanism	Mission Phase	Local effects of failure	Next higher level effect	System Level End Effect	(P) Probability (estimate)	(S) Severity	Detection (Indications to Operator, Maintainer)	(D) Detection Dormancy Period	Risk Level P*S (+D)	Actions for further Investigation / evidence	Mitigation / Requirements
1.1.1	Brake Manifold Ref. Designator 2b, channel A, O-ring	Internal Leakage from Channel A to B	a) O-ring Compression Set (Creep) failure b) surface damage during assembly	Landing	Decreased pressure to main brake hose	No Left Wheel Braking	Severely Reduced Aircraft deceleration on ground and side drift. Partial loss of runway position control. Risk of collision	(C) Moderate	(VI) Catastrophic (this is the worst case)	(1) Flight Computer and Maintenance Computer will indicate "Left Main Brake, Pressure Low"	Built-In Test interval is 1 minute	Unacceptable	Check Dormancy Period and probability of failure	Require redundant independent brake hydraulic channels and/or Require redundant sealing and Classify O-ring as Critical Part Class 1

Probability (P)

In this step it is necessary to look at the cause of a failure mode and the likelihood of occurrence. This can be done by analysis, calculations / FEM, looking at similar items or processes and the failure modes that have been documented for them in the past. A failure cause is looked upon as a design weakness. All the potential causes for a failure mode should be identified and documented.

Probability (P)

This should be in technical terms. Examples of causes are: Human errors in handling, Manufacturing induced faults, Fatigue, Creep, Abrasive wear, erroneous algorithms, excessive voltage or improper operating conditions or use (depending on the used ground rules). A failure mode is given an Probability Ranking.

Probability (P)

Rating	Meaning
A	Extremely Unlikely (Virtually impossible or No known occurrences on similar products or processes, with many running hours)
B	Remote (relatively few failures)
C	Occasional (occasional failures)
D	Reasonably Possible (repeated failures)
E	Frequent (failure is almost inevitable)

Severity (S)

Determine the Severity for the worst case scenario adverse end effect (state). It is convenient to write these effects down in terms of what the user might see or experience in terms of functional failures. Examples of these end effects are: full loss of function x, degraded performance, functions in reversed mode, too late functioning, erratic functioning, etc.

Severity (S)

Each end effect is given a Severity number (S) from, say, I (no effect) to VI (catastrophic), based on cost and/or loss of life or quality of life. These numbers prioritize the failure modes (together with probability and detectability). Below a typical classification is given. Other classifications are possible. See also hazard analysis.

Severity (S)

Rating	Meaning
I	No relevant effect on reliability or safety
II	Very minor, no damage, no injuries, only results in a maintenance action (only noticed by discriminating customers)
III	Minor, low damage, light injuries (affects very little of the system, noticed by average customer)
IV	Moderate, moderate damage, injuries possible (most customers are annoyed, mostly financial damage)
V	Critical (causes a loss of primary function; Loss of all safety Margins, 1 failure away from a catastrophe, severe damage, severe injuries, max 1 possible death)
VI	Catastrophic (product becomes inoperative; the failure may result complete unsafe operation and possible multiple deaths)

Detection (D)

Rating	Meaning
I	No relevant effect on reliability or safety
II	Very minor, no damage, no injuries, only results in a maintenance action (only noticed by discriminating customers)
III	Minor, low damage, light injuries (affects very little of the system, noticed by average customer)
IV	Moderate, moderate damage, injuries possible (most customers are annoyed, mostly financial damage)
V	Critical (causes a loss of primary function; Loss of all safety Margins, 1 failure away from a catastrophe, severe damage, severe injuries, max 1 possible death)
VI	Catastrophic (product becomes inoperative; the failure may result complete unsafe operation and possible multiple deaths)

Detection (D)

The means or method by which a failure is detected, isolated by operator and/or maintainer and the time it may take. This is important for maintainability control (Availability of the system) and it is specially important for multiple failure scenarios.

Detection (D)

This may involve dormant failure modes (e.g. No direct system effect, while a redundant system / item automatic takes over or when the failure only is problematic during specific mission or system states) or latent failures (e.g. deterioration failure mechanisms, like a metal growing crack, but not a critical length).

Detection (D)

It should be made clear how the failure mode or cause can be discovered by an operator under normal system operation or if it can be discovered by the maintenance crew by some diagnostic action or automatic built in system test. A dormancy and/or latency period may be entered.

Detection (D)

Rating	Meaning
1	Certain - fault will be caught on test
2	Almost certain
3	High
4	Moderate
5	Low
6	Fault is undetected by Operators or Maintainers

Detection (D)

DORMANCY or LATENCY PERIOD The average time that a failure mode may be undetected may be entered if known. For example:

During aircraft C Block inspection, preventive or predictive maintenance, X months or X flight hours

During aircraft B Block inspection, preventive or predictive maintenance, X months or X flight hours

During Turn-Around Inspection before or after flight (e.g. 8 hours average)

During in-built system functional test, X minutes

Continuously monitored, X seconds