UNIT 1

Concepts of safety – Hazard classification chemical, physical, mechanical, ergonomics, biological and noise hazards – Hazards from utilities like air, water, steam.
Hazard identification - Safety Audits - Checklists - What if Analysis – HAZAN – HAZOP - Vulnerability models - Event tree and Fault tree Analysis - Past accident analysis - Flixborough - Mexico - Bhopal - Madras - Vizag accident analysis.

Concept of safety:

Safety is a state in which hazards and conditions leading to physical, psychological or material harm are controlled in order to preserve the health and well-being of individuals and the community. It is an essential resource for everyday life, needed by individuals and communities to realise their aspirations.

Attaining an optimum level of safety requires individuals, communities, governments and others to create and maintain the following conditions, whichever setting is considered :

- a climate of social cohesion and peace as well as of equity protecting human rights and freedoms, at the family, local, national or international level;
- the prevention and control of injuries and other consequences or harm caused by accidents;
- the respect of the values and the physical, material and psychological integrity of individuals; and
- the provision of effective preventive, control and rehabilitation measures to ensure the presence of the three previous conditions.

These conditions can be assured by initiatives that focus on the **environment** (physical, social, technological, political, economic and organizational) and on **behaviour**.

Hazard classification:

A **hazard** is an agent which has the potential to cause harm to a vulnerable target. The terms "hazard" and "risk" are often used interchangeably. However, in terms of risk assessment, these are two very distinct terms. A hazard is any agent that can cause harm or damage to humans, property, or the environment. Risk is defined as the probability that exposure to a hazard will lead to a negative consequence, or more simply, a hazard poses no risk if there is no exposure to that hazard.

Hazards can be dormant or potential, with only a theoretical probability of harm. An event that is caused by interaction with a hazard is called an The likely severity of the undesirable consequences of an incident associated with a hazard, combined with th of this occurring, constitute the associated risk. If there is no possibility of a hazard contributing towards an incident, there is no risk.

Hazards can be classified as different types in several ways. One of these ways is by specifying the origin of the hazard. One key concept in identifying a hazard is the presence of stored energy that, when released, can cause damage. Stored energy can occur in many forms: chemical, mechanical, thermal, radioactive, electrical, etc. Another class of hazard does not involve release of stored energy, rather it involves the presence of hazardous situations. Examples include confined or limited egress spaces, oxygen-depleted atmospheres, awkward positions, repetitive motions, low-hanging or protruding objects, etc. Hazards may also be classified as natural, anthropogenic, or technological. They may also be classified as health or safety hazards, by the populations that may be affected, and the severity of the associated risk. In most cases a hazard may affect a range of targets, and have little or no effect on others.

Identification of hazards assumes that the potential targets are defined, and is the first step in performing a risk assessment.

CLASSIFICATION OF HAZARD:

Hazards can be classified as different types in several ways. One of these ways is by specifying the origin of the hazard. One key concept in identifying a hazard is the presence of stored energy that, when released, can cause damage. Stored energy can occur in many forms: chemical, mechanical, thermal, radioactive, electrical, etc. Another class of hazard does not involve release of stored energy, rather it involves the presence of hazardous situations. Examples include confined or limited egress spaces, oxygen-depleted atmospheres, awkward positions, repetitive motions, low-hanging or protruding objects, etc.

Hazards may also be classified as natural, anthropogenic, or technological. They may also be classified as health or safety hazards and by the populations that may be affected, and the severity of the associated risk.

In most cases a hazard may affect a range of targets, and have little or no effect on others. Identification of hazards assumes that the potential targets are defined.

CHEMICAL HAZARD

A chemical can be considered a hazard if by virtue of its intrinsic properties it can cause harm or danger to humans, property, or the environment.

Health hazards associated with chemicals are dependent on the dose or amount of the chemical. For example, iodine in the form of potassium iodate is used to produce iodised salt. When applied at a rate of 20 mg of potassium iodate per 1000 mg of table salt, the chemical is beneficial in preventing goiter, while iodine intakes of 1200–9500 mg in one dose have been known to cause death. Some chemicals have a cumulative biological effect, while others are metabolically eliminated over time. Other chemical hazards may depend on concentration or total quantity for their effects.

A variety of chemical hazards (e.g. DDT, atrazine, etc.) have been identified. However, every year companies produce more new chemicals to fill new needs or to take the place of older, less effective chemicals. Laws, such as the Federal Food, Drug, and Cosmetic Act and the Toxic Substances Control Act in the US, require protection of human health and the environment for any new chemical introduced. In the US, the EPA regulates new chemicals that may have environmental impacts (i.e. pesticides or chemicals released during a manufacturing process), while the FDA regulates new chemicals used in foods or as drugs. The potential hazards of these chemicals can be identified by performing a variety of tests prior to the authorization of usage.

The number of tests required and the extent to which the chemicals are tested varies, depending on the desired usage of the chemical. Chemicals designed as new drugs must undergo more rigorous tests that those used as pesticides.

Some harmful chemicals occur naturally in certain geological formations, such as radon gas or arsenic. Other chemicals include products with commercial uses, such as agricultural and industrial chemicals, as well as products developed for home use. Pesticides, which are normally used to control unwanted insects and plants, may cause a variety of negative effects on non-target organisms. DDT can build up, or bioaccumulate, in birds, resulting in thinner-than-normal egg shells which can break in the nest. The organochlorine pesticide dieldrin has been linked to Parkinson's disease. Corrosive chemicals like sulfuric acid, which is found in car batteries and research laboratories, can cause severe skin burns. Many other chemicals used in industrial and laboratory settings can cause respiratory, digestive, or nervous system problems if they are inhaled, ingested, or absorbed through the skin. The negative effects of other chemicals, such as alcohol and nicotine, have been well documented.

PHYSICAL HAZARD

A physical hazard is a naturally occurring process that has the potential to create loss or damage. Physical hazards include earthquakes, floods, fires, and tornadoes. Physical hazards often have both human and natural elements. Flood problems can be affected by the natural elements of climate fluctuations and storm frequency, and by land drainage and building in a flood plain, human elements. Another physical hazard, X-rays, naturally occur from solar radiation, but have also been utilized by humans for medical purposes; however, overexposure can lead to cancer, skin burns, and tissue damage.

MECHANICAL HAZARD

A mechanical hazard is any hazard involving a machine or industrial process. Motor vehicles, aircraft, and air bags pose mechanical hazards. Compressed gases or liquids can also be considered a mechanical hazard.

Hazard identification of new machines and/or industrial processes occurs at various stages in the design of the new machine or process. These hazard identification studies focus mainly on deviations from the intended use or design and the harm that may occur as a result of these deviations. These studies are regulated by various agencies such as the Occupational Safety and Health Administration and the National Highway Traffic Safety Administration.

ERGONOMICS HAZARD

An ergonomic hazard is a physical factor within the environment that harms the musculoskeletal system. Ergonomic hazards include themes such as repetitive movement, manual handling, workplace/job/task design, uncomfortable workstation height and poor body positioning. Ergonomics is the study of how a workplace, the equipment used there and the work environment itself can best be designed for comfort, efficiency, safety and productivity. Often we can improve our levels of comfort and productivity with relatively simple changes.Although ergonomics is a broad field, the main areas of concern for workplaces and employees will often relate to:

- workstations (sitting and standing)
- equipment layout and operation
- computer systems
- noise
- lighting
- thermal comfort
- maintenance tasks performed on plant items.

Ergonomic issues can be associated with a wide range of concerns including the physical design of workstations, workspaces, the working environment, tools, vehicles, computer programs and plant. It can also involve cognitive processes such as those involved with workload, decision making, skilled performance and stress. There are procedures for dealing with all these issues to make sure any difficulties are addressed.

BIOLOGICAL HAZARD

Biological hazards, also known as biohazards, originate in biological processes of living organisms, and refer to agents that pose a threat to the health of living organisms, the security of property, or the health of the environment.

The term and its associated symbol may be used as a warning, so that those potentially exposed to the substances will know to take precautions. The biohazard symbol was developed in 1966 by Charles Baldwin, an environmental-health engineer working for the Dow Chemical Company on the containment products. and is used in the labeling of biological materials that carry a significant health risk, such as viral samples and used hypodermic needles.

Biological hazards include viruses, parasites, bacteria, food, fungi, and foreign toxins.

Many specific biological hazards have been identified. For example, the hazards of naturally-occurring bacteria such as *Escherichia coli* and *Salmonella*, are well known as disease-causing pathogens and a variety of measures have been taken to limit human exposure to these microorganisms through food safety, good personal hygiene and education. However, the potential for new biological hazards exists through the discovery of new microorganisms and through the development of new genetically modified (GM) organisms. Use of new GM organisms is regulated by various governmental agencies. The US Environmental Protection Agency (EPA) controls GM plants that produce or resist pesticides (i.e. Bt corn and Roundup ready crops). The US Food and Drug Administration (FDA) regulates GM plants that will be used as food or for medicinal purposes.

Biological hazards can include medical waste or samples of a microorganism, virus or toxin (from a biological source) that can affect health.

Many biological hazards are associated with food, including certain viruses, parasites, fungi, bacteria, and plant and seafood toxins. Pathogenic *Campylobacter* and *Salmonella*are common foodborne biological hazards. The hazards from these bacteria can be avoided through risk mitigation steps such as proper handling, storing, and cooking of food. Disease in humans can come from biological hazards in the form of infection by bacteria, antigens, viruses, or parasites.

NOISE HAZARD

Noise-related hearing loss is one of the most common occupational health issues. Every year thousands of workers are exposed to workplace noise hazards that result in preventable hearing loss. The Bureau of Labor Statistics (BLS) has reported that since 2004 nearly 125,000 workers have suffered significant, permanent hearing loss. In 2009 alone the BLS reported there were more than 21,000 cases of hearing loss. Exposure to workplace noise hazards (high noise levels) can cause permanent hearing loss that cannot be corrected by surgery or a hearing aid. Even short-term exposure to loud noise can cause a temporary change in hearing. Short-term effects such as feeling like your ears are "stuffed up" or ringing in the ears may go away after leaving the noisy area. However, repeated exposure to noise hazards can lead to permanent tinnitus or hearing loss.

In addition to hearing damage, noise hazards can:

- Create physical and psychological stress
- Reduce productivity
- Interfere with communication and concentration.
- Contribute to workplace accidents and injuries by making it difficult to hear warning signals

HAZARDS FROM UTILITIES

HAZARDS FROM AIR

Hazardous air pollutants, also known as toxic air pollutants or air toxics, are those pollutants that are known or suspected to cause cancer or other serious health effects, such as reproductive effects or birth defects, or adverse environmental effects. EPA is working with state, local, and tribal governments to reduce air emissions of 187 toxic air pollutants to the environment.
Examples of toxic air pollutants include

- benzene, which is found in gasoline;
- perchloroethylene, which is emitted from some dry cleaning facilities; and
- methylene chloride, which is used as a solvent and paint stripper by a number of industries.

Examples of other listed air toxics include dioxin, asbestos, toluene, and metals such as cadmium, mercury, chromium, and lead compounds.

HAZARDS FROM WATER

Water—oceans, seas, storms, and rain—are a source of beauty, inspiration, and recreation for billions of people. As with many natural processes, part of that beauty is seated in the untamed grandness of those systems, which can sometimes turn hazardous. Water hazards have the potential to impact almost everyone on the planet, because roughly half of the world's population lives within 100 miles of a coastline. Those who don't are still at risk for experiencing local or regional flooding events. Natural Hazards at the University of Washington includes scientists and researchers working across water-related hazards, each with their own area of expertise—from extreme precipitation and regional climate change to roadways and mountain snow melt. In partnership with other experts, we are working toward resilient mitigation approaches to water hazards, including tsunamis, coastal threats, floods.

HAZARDS FROM STEAM

Here are the top four dangers of steam systems and how to prevent them:

1. SLIPS AND FALLS

One of the biggest hazards of any steam system is the risk of injury to employees due to slip and fall hazards. On a national scale, slips and falls account for an estimated $70 billion in workers' compensation and medical bills, according to the Centers For Disease Control and Prevention. This data is supported by research from Martindale-Nolo, which found that the average cost of a workers' compensation claim for a slip-and-fall accident is between $17,200 and $27,500.

Prevention tips: Preventive maintenance of steam systems is one of the best ways to prevent slips and falls at a facility. When condensate is released into the atmosphere, it can quickly make the floor slick. Using ultrasound technology, inspectors can pinpoint small leaks before they would otherwise be visible to the naked eye. Then, maintenance staff can take action to repair aging assets before they become a problem. Likewise, slip-resistant footwear can protect employees from hard-to-spot hazards in low-light environments.

2. STEAM LEAKS

In addition to causing slipping hazards, steam leaks can lead to abnormally warm pipes and ambient temperatures, making the facility unsafe for workers. This problem is especially apparent in low-pressure steam systems where feedwater must be heated past the boiling point. Burns caused by steam can severely injure workers and reduce efficiency over the long term.

Prevention tips: Assuring steam traps are functional is one of the top ways to reduce the risk of dangerous leaks. The Ultraprobe 100 and Ultraprobe 3000 are great options for assessing steam traps and preventing asset failure. Both products are easy to use and absolutely essential for facilities managers who want to keep workers safe and control resource costs at the same time.

3. RUPTURED PIPES

A ruptured steam pipe is a serious problem with the potential to cause bodily harm and serious financial risk. When a steam trap fails in the closed position, it can cause condensate to back up, increasing pressure levels and causing water hammer. Steam traps aren't the only culprit, either. Poor maintenance of steam systems can also lead to pipe and valve corrosion, two more precursors to pipe rupture.

Prevention tips: Traps and valves should be monitored regularly for signs of anomalies. The Ultraprobe 2000 can be adapted to test almost any problem in operating equipment, reducing downtime and diagnosing problems before they become safety risks. The Ultraprobe 9000 does all that and more, allowing technicians to store data directly on the device and download the information via USB for easy reporting.

4. FINANCIAL LOSS

If a steam system has never been inspected and isn't subject to a recurring maintenance program, upwards of 50 percent of the system's steam traps could be failed or blowing live steam. That unused energy can severely cut into a facility's operating costs. Managers who want to control costs and conserve precious resources need to implement a preventive maintenance system to protect their assets and employees.

Prevention tips: A annual inspection of a steam system can reduce trap and valve failures by half, and more frequent preventive maintenance will increase efficiency accordingly. Ultimately, the size of a facility and its access to resources will determine the optimal maintenance schedule. For optimal efficiency, the Ultraprobe® 15000 features state-of-the-art technology that takes an entire ultrasonic condition monitoring laboratory and puts it all in a single tool.

To learn more about how preventive maintenance can improve your steam system and protect employees, visit UESystems.comtoday.

HAZARD IDENTIFICATION

One of the "root causes" of workplace injuries, illnesses, and incidents is the failure to identify or recognize hazards that are present, or that could have been anticipated. A critical element of any effective safety and health program is a proactive, ongoing process to identify and assess such hazards.

To identify and assess hazards, employers and workers:

- Collect and review information about the hazards present or likely to be present in the workplace.
- Conduct initial and periodic workplace inspections of the workplace to identify new or recurring hazards.
- Investigate injuries, illnesses, incidents, and close calls/near misses to determine the underlying hazards, their causes, and safety and health program shortcomings.
- Group similar incidents and identify trends in injuries, illnesses, and hazards reported.
- Consider hazards associated with emergency or nonroutine situations.
- Determine the severity and likelihood of incidents that could result for each hazard identified, and use this information to prioritize corrective actions.

Some hazards, such as housekeeping and tripping hazards, can and should be fixed as they are found. Fixing hazards on the spot emphasizes the importance of safety and health and takes advantage of a safety leadership opportunity. To learn more about fixing other hazards identified using the processes described here, see "Hazard Prevention and Control."

Action item 1: Collect existing information about workplace hazards

Action item 2: Inspect the workplace for safety hazards

Action item 3: Identify health hazards

Action item 4: Conduct incident investigations

Action item 5: Identify hazards associated with emergency and nonroutine situations

Action item 6: Characterize the nature of identified hazards, identify interim control measures, and prioritize the hazards for control

Action item 1: Collect existing information about workplace hazards

Information on workplace hazards may already be available to employers and workers, from both internal and external sources.

How to accomplish it

Collect, organize, and review information with workers to determine what types of hazards may be present and which workers may be exposed or potentially exposed. Information available in the workplace may include:

- Equipment and machinery operating manuals.
- Safety Data Sheets (SDS) provided by chemical manufacturers.
- Self-inspection reports and inspection reports from insurance carriers, government agencies, and consultants.
- Records of previous injuries and illnesses, such as OSHA 300 and 301 logs and reports of incident investigations.
- Workers' compensation records and reports.
- Patterns of frequently-occurring injuries and illnesses.
- Exposure monitoring results, industrial hygiene assessments, and medical records (appropriately redacted to ensure patient/worker privacy).
- Existing safety and health programs (lockout/tagout, confined spaces, process safety management, personal protective equipment, etc.).
- Input from workers, including surveys or minutes from safety and health committee meetings.
- Results of job hazard analyses, also known as job safety analyses.

Information about hazards may be available from outside sources, such as:

- OSHA, National Institute for Occupational Safety and Health (NIOSH), and Centers for Disease Control and Prevention (CDC) websites, publications, and alerts.
- Trade associations.
- Labor unions, state and local occupational safety and health committees/coalitions ("COSH groups"), and worker advocacy groups.
- Safety and health consultants.

Action item 2: Inspect the workplace for safety hazards

Hazards can be introduced over time as workstations and processes change, equipment or tools become worn, maintenance is neglected, or housekeeping practices decline. Setting aside time to regularly inspect the workplace for hazards can help identify shortcomings so that they can be addressed before an incident occurs.

How to accomplish it

- Conduct regular inspections of all operations, equipment, work areas and facilities. Have workers participate on the inspection team and talk to them about hazards that they see or report.
- Be sure to document inspections so you can later verify that hazardous conditions are corrected. Take photos or video of problem areas to facilitate later discussion and brainstorming about how to control them, and for use as learning aids.
- Include all areas and activities in these inspections, such as storage and warehousing, facility and equipment maintenance, purchasing and office functions, and the activities of on-site contractors, subcontractors, and temporary employees.
- Regularly inspect both plant vehicles (e.g., forklifts, powered industrial trucks) and transportation vehicles (e.g., cars, trucks).
- Use checklists that highlight things to look for. Typical hazards fall into several major categories, such as those listed below; each workplace will have its own list:
    - General housekeeping
    - Slip, trip, and fall hazards
    - Electrical hazards
    - Equipment operation
    - Equipment maintenance
    - Fire protection
    - Work organization and process flow (including staffing and scheduling)
    - Work practices
    - Workplace violence
    - Ergonomic problems
    - Lack of emergency procedures
- Before changing operations, workstations, or workflow; making major organizational changes; or introducing new equipment, materials, or processes, seek the input of workers and evaluate the planned changes for potential hazards and related risks.

Action item 3: Identify health hazards

Identifying workers' exposure to health hazards is typically more complex than identifying physical safety hazards. For example, gases and vapors may be invisible, often have no odor, and may not have an immediately noticeable harmful health effect. Health hazards include chemical hazards (solvents, adhesives, paints, toxic dusts, etc.), physical hazards (noise, radiation, heat, etc.), biological hazards (infectious diseases), and ergonomic risk factors (heavy lifting, repetitive motions, vibration). Reviewing workers' medical records (appropriately redacted to ensure patient/worker privacy) can be useful in identifying health hazards associated with workplace exposures.

How to accomplish it

- Identify chemical hazards –review SDS and product labels to identify chemicals in your workplace that have low exposure limits, are highly volatile, or are used in large quantities or in unventilated spaces. Identify activities that may result in skin exposure to chemicals.
- Identify physical hazards –identify any exposures to excessive noise (areas where you must raise your voice to be heard by others), elevated heat (indoor and outdoor), or sources of radiation (radioactive materials, X-rays, or radiofrequency radiation).
- Identify biological hazards –determine whether workers may be exposed to sources of infectious diseases, molds, toxic or poisonous plants, or animal materials (fur or scat) capable of causing allergic reactions or occupational asthma.
- Identify ergonomic risk factors –examine work activities that require heavy lifting, work above shoulder height, repetitive motions, or tasks with significant vibration.
- Conduct quantitative exposure assessments –when possible, using air sampling or direct reading instruments.
- Review medical records –to identify cases of musculoskeletal injuries, skin irritation or dermatitis, hearing loss, or lung disease that may be related to workplace exposures.

Action item 4: Conduct incident investigations

Workplace incidents –including injuries, illnesses, close calls/near misses, and reports of other concerns– provide a clear indication of where hazards exist. By thoroughly investigating incidents and reports, you will identify hazards that are likely to cause future harm. The purpose of an investigation must always be to identify the root causes (and there is often more than one) of the incident or concern, in order to prevent future occurrences.

How to accomplish it

- Develop a clear plan and procedure for conducting incident investigations, so that an investigation can begin immediately when an incident occurs. The plan should cover items such as:
    - Who will be involved
    - Lines of communication
    - Materials, equipment, and supplies needed
    - Reporting forms and templates
- Train investigative teams on incident investigation techniques, emphasizing objectivity and open-mindedness throughout the investigation process.
- Conduct investigations with a trained team that includes representatives of both management and workers.
- Investigate close calls/near misses.

- Identify and analyze root causes to address underlying program shortcomings that allowed the incidents to happen.
- Communicate the results of the investigation to managers, supervisors, and workers to prevent recurrence.

Effective incident investigations do not stop at identifying a single factor that triggered an incident. They ask the questions "Why?" and "What led to the failure?" For example, if a piece of equipment fails, a good investigation asks: "Why did it fail?" "Was it maintained properly?" "Was it beyond its service life?" and "How could this failure have been prevented?" Similarly, a good incident investigation does not stop when it concludes that a worker made an error. It asks such questions as: "Was the worker provided with appropriate tools and time to do the work?" "Was the worker adequately trained?" and "Was the worker properly supervised?"

Action item 5: Identify hazards associated with emergency and nonroutine situations

Emergencies present hazards that need to be recognized and understood. Nonroutine or infrequent tasks, including maintenance and startup/shutdown activities, also present potential hazards. Plans and procedures need to be developed for responding appropriately and safely to hazards associated with foreseeable emergency scenarios and nonroutine situations.

How to accomplish it

- Identify foreseeable emergency scenarios and nonroutine tasks, taking into account the types of material and equipment in use and the location within the facility. Scenarios such as the following may be foreseeable:
  - Fires and explosions
  - Chemical releases
  - Hazardous material spills
  - Startups after planned or unplanned equipment shutdowns
  - Nonroutine tasks, such as infrequently performed maintenance activities
  - Structural collapse
  - Disease outbreaks
  - Weather emergencies and natural disasters
  - Medical emergencies
  - Workplace violence

Action item 6: Characterize the nature of identified hazards, identify interim control measures, and prioritize the hazards for control

The next step is to assess and understand the hazards identified and the types of incidents that could result from worker exposure to those hazards. This information can be used to develop interim controls and to prioritize hazards for permanent control.

How to accomplish it

- Evaluate each hazard by considering the severity of potential outcomes, the likelihood that an event or exposure will occur, and the number of workers who might be exposed.
- Use interim control measures to protect workers until more permanent solutions can be implemented.
- Prioritize the hazards so that those presenting the greatest risk are addressed first. Note, however, that employers have an ongoing obligation to control all serious recognized hazards and to protect workers.

SAFETY AUDITS

DEFINITION

Safety auditing is a core safety management activity, providing a means of identifying potential problems before they have an impact on safety. Safety regulatory audit means a systematic and independent examination conducted by, or on behalf of, a national supervisory authority to determine whether complete safety-related arrangements or elements thereof, related to processes and their results, products or services, comply with required safety-related arrangements and whether they are implemented effectively and are suitable to achieve expected results.

OBJECTIVE

Safety audits are conducted in order to assess the degree of compliance with the applicable safety regulatory requirements and with the procedural provisions of a Safety Management System if one is in place. They are intended to provide assurance of the safety management functions, including staffing, compliance with applicable regulations, levels of competency and training.

DESCRIPTION

Safety auditing is an element of safety management which subjects the activities of airline operators/service providers to a systematic critical evaluation. An audit may include one or more components of the total system, such as safety policy, change management, SMS as a whole, operating procedures, emergency procedures, etc. The aim is to disclose the strengths and weaknesses, to identify areas of non-tolerable risk and devise rectification measures. The outcome of the audit will be a report, followed by an action plan prepared by the audited organisation and approved by the regulator/supervisory authority. The implementation of the agreed safety improvement measures shall be monitored by the supervisory authority.

Safety audits are used to ensure that:

- Organisation’s SMS has a sound structure and adequate staffing levels;
- Approved procedures and instructions are complied with;
- The required level of personnel competency and training to operate equipment and facilities, and to maintain their levels of performance, is achieved;
- Equipment performance is adequate for the safety levels of the service provided;

- Effective arrangements exist for promoting safety, monitoring safety performance and processing safety issues;
- Adequate arrangements exist to handle foreseeable emergencies.

Safety audits are carried out by a single individual or a team of people who are competent (adequately qualified, experienced and trained) and have a satisfactory degree of independence from the audited organisation or unit. The frequency of the audits depends on the regulatory/management policy. For example some State authorities may conduct annual safety audits; others may consider that a full safety audit is only necessary at a few years interval. Ad-hoc safety audits may be conducted to verify the compliance of a particular system component or activity, or may be initiated following an incident. In accordance with ICAO Standards and Recommended Practices (SARPs) safety audits are to be conducted on a regular and systematic basis. Usually the frequency and scope of safety audits is fixed in a dedicated annual safety audit (inspection) programme of the responsible authority/organisation. Safety audits are one of the principal methods for fulfilling the safety performance monitoring requirements. Often audits are integrated, i.e. they include not only safety but also other business processes and performance areas, such as quality, capacity, cost efficiency etc.

All audits should be pre-planned and supporting documentation (usually in the form of checklists) of the audit content prepared. Among the first steps in planning an audit will be to verify the feasibility of the proposed schedule and to identify the information that will be needed before commencement of the audit. It will also be necessary to specify the criteria against which the audit will be conducted and to develop a detailed audit plan together with checklists to be used during the audit.

The conduct of the actual audit is essentially a process of inspection or fact-finding. Information from almost any source may be reviewed as part of the audit. The techniques for gathering the information include:

- Review of documentation;
- Interviews with staff;
- Observations by the audit team.

The results from the safety auditing present evidence of the performance and the general condition of the organisation’s SMS. Audits which limit observations to items of regulatory non-compliance are of limited value, because they will not encourage the audited organisation to act proactively. The audit report should be an objective presentation of the results of the safety audit. The key principles to be observed in the development of the audit report are:

- Consistency of observations and recommendations;
- Conclusions substantiated with references;
- Observations and recommendations stated clearly and concisely;
- Avoidance of generalities and vague observations;
- Objectivity of observations;
- Avoidance of criticism of individuals or positions.

According to ICAO Doc 9859 - Safety Management Manual safety auditing is a proactive safety management activity which provides means for identifying potential problems before they have an impact on safety. Therefore, safety auditing has the characteristics attributed to both the safety assurance domain of SMS, and the hazard identification element of risk management.

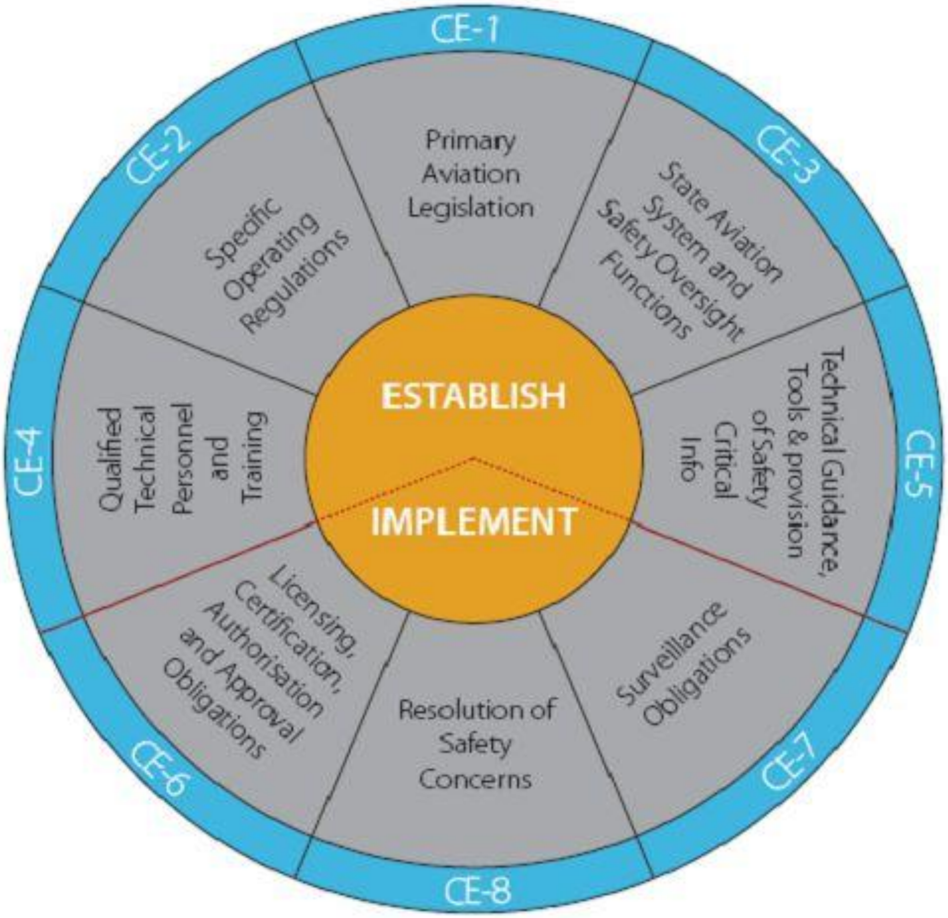
Safety audits may be conducted externally - by the designated State regulatory authority, internally - by the aviation services provider organisation, or by a qualified external safety auditor, for example a consultancy agency. Regardless of the driving force behind the audit, the activities and output from both internal and external audits are similar.

REGULATORY SAFETY AUDITS (*EXTERNAL AUDITING*)

Under the Chicago Convention, States are required to put in place a safety oversight system to promote aviation safety by observing and assessing the compliance of aircraft operators/service providers with the applicable regulations, procedures and recommended practices. This is to be achieved through a mix of activities, including safety audits. Such audits conducted by a safety regulatory authority should take a broad view of the safety management procedures of the audited organisation. The key issues in such audits should be:

- **Surveillance and compliance** - the authority needs to ensure that international, national and local standards are complied with prior to issuing any licence or approval and continue to be complied with afterwards;
- **Areas and degree of risk** - the audit should assess how risks are identified and how any necessary changes are made to ensure that all safety standards are met;
- **Competence** - the audited organisation should have adequately trained staff for all safety related positions
- **Safety management** - ensure that the organisation's SMS is based on sound principles and procedures, and that the organisation is meeting its safety performance targets.

ICAO Document 9734-A - The Establishment and Management of a State's Safety Oversight System defines Eight Critical Elements of a State's Safety Oversight System in - as shown in the diagram below:


CE-1
Primary Aviation Legislation
CE-2
Specific Operating Regulations
CE-3
State Aviation System and Safety Oversight Functions
CE-4
Qualified Technical Personnel and Training
CE-5
Technical Guidance, Tools & provision of Safety Critical Info
CE-6
Licensing, Certification, Authorisation and Approval Obligations
CE-7
Surveillance Obligations
CE-8
Resolution of Safety Concerns
ESTABLISH
IMPLEMENT

ICAO Model
The Eight Critical Elements of a State's Safety Oversight System

Ideally the State regulatory authorities should have established procedures and criteria to focus inspections, audits and surveys (in an annual audit programme) on those areas of greater safety concern or need, as identified by the analysis of operational hazard data and risk areas.

Regulatory audits are independent of internal auditing activities undertaken by the organisation concerned within the framework of its safety management system.

Safety audit is an essential safety oversight tool for international and national regulatory and supervisory authorities. In 1999 ICAO established the Universal Safety Oversight Audit Programme(USOAP) with the objective to oversee the effective application of ICAO standards regarding the development of safety regulatory frameworks by Member States. In the area of Air Traffic Management the EUROCONTROL Permanent Commission approved in November 2002 the establishment of the ESARR Implementation Monitoring and Support (ESIMS) Programme. The ESIMS audits are focused on the States' overall safety oversight, including safety audit capabilities. In Europe, the two safety oversight programmes have been coordinated to achieve an efficient use of avialable resources. ESIMS audits had been carried out for a decade and were replaced by the EASAstandartisation inspections.

THIRD PARTY AUDITS (*EXTERNAL AUDITING*)

The organisation's management or the regulator may decide to have an external agency carry out an independent safety audit. ICAO Doc 9859 specifies that: "External audits of the SMS may be conducted by relevant authorities responsible for acceptance of the service provider's SMS. Additionally, audits may be conducted by industry associations or other third parties selected by the service provider. These external audits enhance the internal audit system as well as provide independent oversight."

An organisation which possesses the necessary expertise and technical experience to verify on behalf of a State authority the compliance of an air navigation service provider with the applicable regulatory requirements is called a qualified entity. An organisation wishing to become qualified entity must be certified by a State authority in accordance with the provisions of the SES Service provision regulation.

INTERNAL SAFETY AUDITS (*SELF AUDITING*)

Internal safety audits and safety surveys should be used by the aviation service providers to assess the level of compliance with the applicable regulatory framework and the organisational SMS processes and procedures, to verify the effectiveness of such processes and procedures and to identify corrective measures if needed. Planning of the audits should take into account the safety significance of the processes to be audited and the results of previous audits. An annual audit program should include:

- Definition of the audits, in terms of criteria, scope, frequency, and methods;
- Description of the processes used to select the auditors;
- The requirement that individuals shall not audit their own work;
- Documented procedures for assignment of responsibilities, planning and conduct of audits, reporting results and maintaining records;
- Audits of contractors and vendors.

According to ICAO Doc 9774 - Manual on Certification of Aerodromes, an aerodrome operator should arrange for an audit of the aerodrome SMS, including an inspection of the aerodrome facilities and equipment. For conducting such a large scale safety audit "the aerodrome operator should also arrange an external audit for the evaluation of aerodrome users, including aircraft operators, ground handling agencies and other organizations" operating at the aerodrome.

CHECKLISTS

A **checklist** is a type of job aid used to reduce failure by compensating for potential limits of human memory and attention. It helps to ensure consistency and completeness in carrying out a task. A basic example is the "to do list." A more advanced checklist would be a schedule, which lays out tasks to be done according to time of day or other factors. A primary task in checklist is documentation of the task and auditing against the documentation.

APPLICATIONS:

- Pre-flight checklists aid in aviation safety to ensure that critical items are not overlooked
- Used in quality assurance of software engineering, to check process compliance, code standardization and error prevention, and others.
- Often used in industry in operations procedures
- In civil litigation to deal with the complexity of discovery and motions practice. An example is the open-source litigation checklist.
- Can aid in mitigating claims of negligence in public liability claims by providing evidence of a risk management system being in place
- Used by some investors as a critical part of their investment process
- An ornithological checklist, a list of birds with standardized names that helps ornithologists communicate with the public without the use of scientific names in Latin
- A popular tool for tracking sports card collections. Randomly inserted in packs, checklist cards provide information on the contents of sports card set.
- The creation of emergency survival kits
- Professional diving, preparation of equipment for a dive

What is an example of an inspection checklist for a manufacturing facility?

The examples outlined below do not list all the possible items for manufacturing facilities. The best checklist for your workplace is one that has been developed for your specific needs. Whatever the format of the checklist, provide space for the inspectors' signatures and the date.

Inspectors:		**Date:**	
	(O)Satisfactory (X) Requires Action		
	Location	Condition	Comments
Training			
Is training provided for each person newly assigned to a job?			
Does initial training include a thorough review of hazards and accidents associated with the job?			
Is adequate instruction in the use of personal protective equipment provided?			
Is training for the use of emergency equipment provided?			
Are workers knowledgeable in the "Right to Refuse" procedures?			
Environment			

Are resources available to deal with very hot or very cold conditions (drinking water, lined gloves, insulated boots)?			
Is the rain/cold weather gear that is provided comfortable, and light enough so as not to constitute a hazard?			
Are work surfaces and grip surfaces safe when wet?			
Do workers know the symptoms of heat cramps/heatstroke, or frost bite/hypothermia?			
Work Process			
Are repetitive motion tasks properly paced and kept to a minimum?			
Are the material safety data sheets placed in locations accessible to all employees?			
Are hazards signalled by signs and tags?			
Have all trucks, forklifts and other equipment been inspected and maintained?			
Are lockout or tagout procedures in place and followed?			
Is ventilation equipment working effectively?			
Is the fume and dust collection hood working effectively?			
Are the safety showers and eye wash stations in the proper locations and in good working condition?			
Fire Emergency Procedures			
Is there a clear fire response plan posted for each work area?			
Do all workers know the plan?			
Are drills held regularly?			
Are fire extinguishers chosen for the type of fire most likely in that area?			
Are there enough extinguishers present to do the job?			
Are extinguisher locations conspicuously marked?			
Are extinguishers properly mounted and easily accessible?			
Are all extinguishers fully charged and operable?			

Are special purpose extinguishers clearly marked?			
Means of Exit			
Are there enough exits to allow prompt escape?			
Do employees have easy access to exits?			
Are exits unlocked to allow egress?			
Are exits clearly marked?			
Are exits and exit routes equipped with emergency lighting?			
Warehouse and Shipping			
Are dock platforms, bumpers, stairs and steps in good condition?			
Are light fixtures in good condition?			
Are all work areas clean and free of debris?			
Are stored materials properly stacked and spaced?			
Are tools kept in their proper place?			
Are there metal containers for oily rags and for rubbish?			
Are floors free of oil spillage or leakage?			
Is absorbent available for immediate clean-up of spills and leaks?			
Are all flammable and combustible products stored appropriately? For example: Are Class I (one) flammable products (as per NFPA or your local fire code) stored in Class I approved buildings or outside the warehouse?			
Loading/Unloading Racks			
Are steps, railings and retractable ramps on raised platforms in good repair?			
Is piping and in-line equipment in good condition and free of leaks?			
Are loading arms operating satisfactorily?			
Do submerged filling two-stage valves operate properly?			

Are bonding and grounding cables free of breaks or damage?			
Are connections tight and sound?			
Is the general condition of wiring and junction boxes, etc. in good condition (visual inspection)?			
Lighting			
Is the level of light adequate for safe and comfortable performance of work?			
Does lighting produce glare on work surfaces, monitors, screens and keyboards?			
Is emergency lighting adequate and regularly tested?			
Machine Guards			
Are all dangerous machine parts adequately guarded?			
Do machine guards meet standards?			
Are lockout procedures followed when performing maintenance with guards removed?			
Electrical			
Is the Canadian Electrical Code adhered to in operation, use, repair and maintenance?			
Are all machines properly grounded?			
Are portable hand tools grounded or double insulated?			
Are junction boxes closed?			
Are extension cords out of the aisles where they can be abused by heavy traffic?			
Is permanent wiring used instead of extension cords?			
Tools and Machinery			
Are manufacturers' manuals kept for all tools and machinery?			
Do power tools conform to standards?			
Are tools properly designed for use by employees?			

Are defective tools tagged and removed from service as part of a regular maintenance program?			
Are tools and machinery used so as to avoid electrical hazards?			
Is proper training given in the safe use of tools and machinery?			
Confined Spaces			
Are the confined space procedures and training available and followed by all involved?			
Are entry and exit procedures adequate?			
Are emergency and rescue procedures in place (e.g. trained safety watchers)?			
Housekeeping			
Is the work area clean and orderly?			
Are floors free from protruding nails, splinters, holes and loose boards?			
Are aisles and passageways kept clear of obstructions?			
Are permanent aisles and passageways clearly marked?			
Are covers or guardrails in place around open pits, tanks and ditches?			
Floor and Wall Openings			
Are ladder-ways and door openings guarded by a railing?			
Do temporary floor openings have standard railings or someone constantly on guard?			
Stairs, Ladders and Platforms			
Are stairs and handrails in good condition?			
Are ladders free of defects?			
Are ladders set up properly before use?			
Are the elevated platforms properly secured and do they have handrails?			

Elevating Devices			
Are elevating devices used only within capacity?			
Are capacities posted on equipment?			
Are they regularly inspected, tested and maintained?			
Are controls of the "dead man" type?			
Are operators trained?			
Sound Level/Noise			
Are regular noise surveys conducted?			
Is hearing protection available and used properly?			
Temporary Work Structures			
Are temporary work structures used only when it is not reasonably practicable to use permanent ones?			
Are excavations properly shored, free of large objects (rocks, etc.) at the edges?			
Employee Facilities			
Are facilities kept clean and sanitary?			
Are facilities in good repair?			
Are cafeteria facilities provided away from toxic chemicals?			
Are hand washing facilities available?			
Medical and First Aid			
Do all employees know how to get first aid assistance when needed?			
Do the first-aiders know when and to which hospital or clinic an injured person should be taken?			
Are there employees trained as first-aid practitioners on each shift worked?			
Are first-aid kits provided as per jurisdiction’s first-aid regulations?			
Are first-aid supplies replenished as they are used?			

Personal Protective Equipment (PPE)			
Is required equipment provided, maintained and used?			
Does equipment meet requirements?			
Is it reliable?			
Is personal protection utilized only when it is not reasonably practicable to eliminate or control the hazardous substance or process?			
Are the areas requiring PPE usage properly identified by warning signs?			
Materials Handling and Storage			
Is there safe clearance for all equipment through aisles and doors?			
Is stored material stable and secure?			
Are storage areas free from tipping hazards?			
Are only trained operators allowed to operate forklifts?			
Is charging of electric batteries performed only in designated areas?			
Are dock boards (bridge plates) used when loading or unloading from dock to truck or dock to rail car?			
Are necessary warning devices and signs in use for railway sidings?			
Are specifications posted for maximum loads which are approved for shelving, floors and roofs?			
Are racks and platforms loaded only within the limits of their capacity?			
Are chain hoists, ropes and slings adequate for the loads and marked accordingly?			
Are slings inspected daily before use?			
Are all new, repaired, or reconditioned alloy steel chain slings proof-tested before use?			
Are pallets and skids the correct type and inspected?			

Do personnel use proper lifting techniques?			
Is the size and condition of containers hazardous to workers?			
Are elevators, hoists, conveyors, balers, etc., properly used with appropriate signals and directional warning signs?			

WHAT IF ANALYSIS

OBJECTIVES

- Introduce What-If Analysis
- Review Process Hazard Analyses Methods
- Examine the Use of Techniques, their Strengthens and Limitations
- Provide Guidance on the Use of What-If Analysis Techniques

INTRODUCTION

What-If Hazard Analysis is a well-established and widely used qualitative method for identifying and analyzing hazards, hazard scenarios, and existing and needed controls.

Although originally developed for chemical and petrochemical process hazard studies, the What-If Hazard Analysis and its variations have become widely used in many other industries including energy, manufacturing, high-tech, food processing, transportation, and healthcare to mention a few.

The method can be applied to a system, process, or operation or at a more specific focus such as a piece of equipment, procedure, or activity.

WHAT-IF APPLICATIONS

- operations that contain hazardous chemical processes
- operations with large refrigeration and chiller systems containing ammonia such as meat packing, food processing and storage
- non-routine activities such as equipment installations, repair, or decommission
- ‘Table top drills’ to develop emergency scenarios and necessary measures for preparedness, disaster recovery, and business continuity
- Design Safety Reviews of new facilities, systems, and equipment
- In operations where ‘Management of Change’ is considered
- Analysis prior to selection and procurement of new technology, equipment, or materials

MANDATED PHAS

OSHA 29 CFR 1910.119 Process Safety Management (PSM) of Highly Hazardous Chemicals standard, established in 1992, requires process hazard analyses for regulated industrial processes containing 10,000 pounds or more of a hazardous chemical for the purpose of protecting the employees working in and around such processes.

EPA 40 CFR PART 68 Chemical Accident Prevention Provisions, Risk Management Plan (RMP) Rule issued in 1994 as a result of the Clean Air Act Amendments of 1990 mirror's the OSHA Process Safety Management requirements for process hazard analyses in regulated facilities for the purpose of protecting the public and the environment from undesired consequences of explosions or releases.

What-If Hazard Analysis is one of several process hazard analysis methodologies referred to in the OSHA Process Safety Management standard and EPA Risk Management Plan Rule as an acceptable method.

Process Hazard Analysis Method	Description
What-If	Uses a multi-skilled team to create and answer a series of "what-if" type questions. This method has a relatively loose structure and is only as effective as the quality of the questions asked and the answers given.
Checklist	Uses established codes, standards and well-understood hazardous operations as a checklist against which to compare a process. A good checklist is dependent on the experience level and knowledge of those who develop it.
What-If/Checklist	A team-based, structured analysis that combines the creative, brainstorming aspects of the What-If with the systematic approach of the Checklist. The combination of techniques can compensate for the weaknesses of each.
Hazard and Operability Study (HAZOP)	A team-based, structured, systematic review of a system or product that identifies risks through the use of 'guide words' which question how the design can fail due to certain limitations and deviations of the operation.
Failure Mode and Effects Analysis (FMEA)	Technique used to identify the ways systems and their components can fail and the resulting effect.
Fault Tree Analysis	Technique used for identifying and analyzing factors that can contribute to a specified undesired event. Causal factors are deductively identified, organized in logical manner and represented pictorially in a tree diagram.

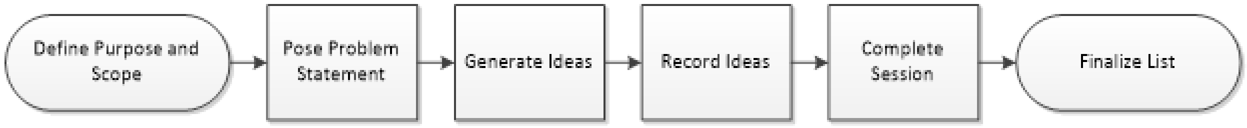
WHAT-IF ANALYSIS AND RELATED METHODS

The primary objectives of the What-If methodology are to identify and analyze: 1) major hazards and hazard exposure scenarios in a system; 2) causes, deviations and weaknesses that can lead to major hazards; 3) control measures in the system; 4) and needed controls to achieve an acceptable risk level. Methods include:

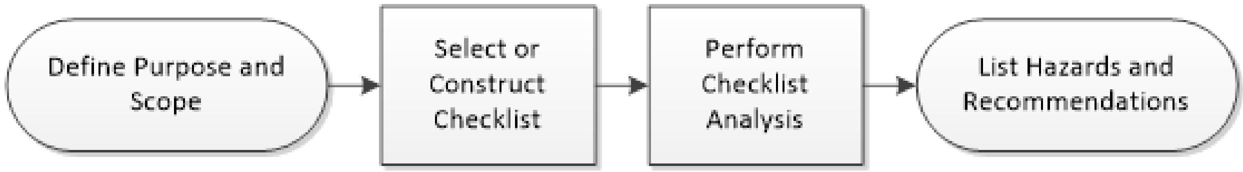
- Brainstorming

- Checklist Analysis
- What-If Hazard Analysis
- What-If Checklist
- Structured What-If Technique (SWIFT)
- Hazard and Operability Study (HAZOP)
-

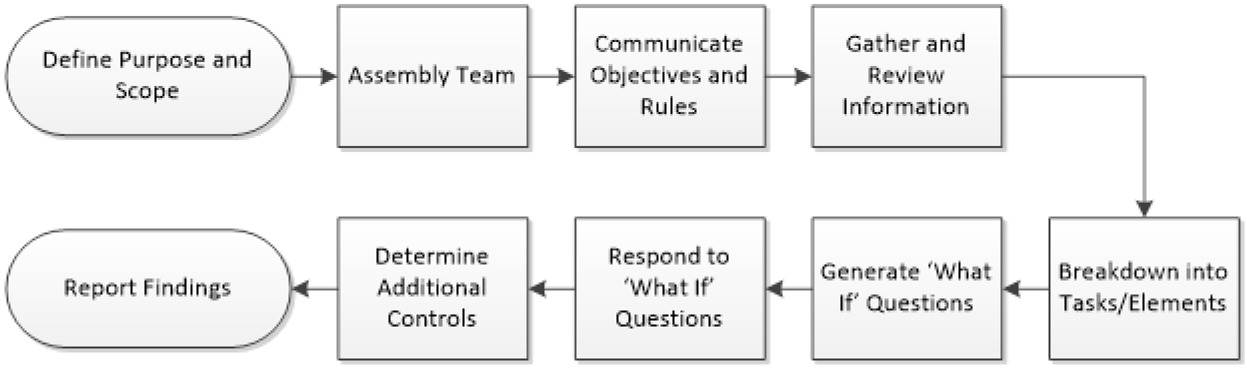
BRAINSTORMING – STRUCTURED AND UNSTRUCTURED



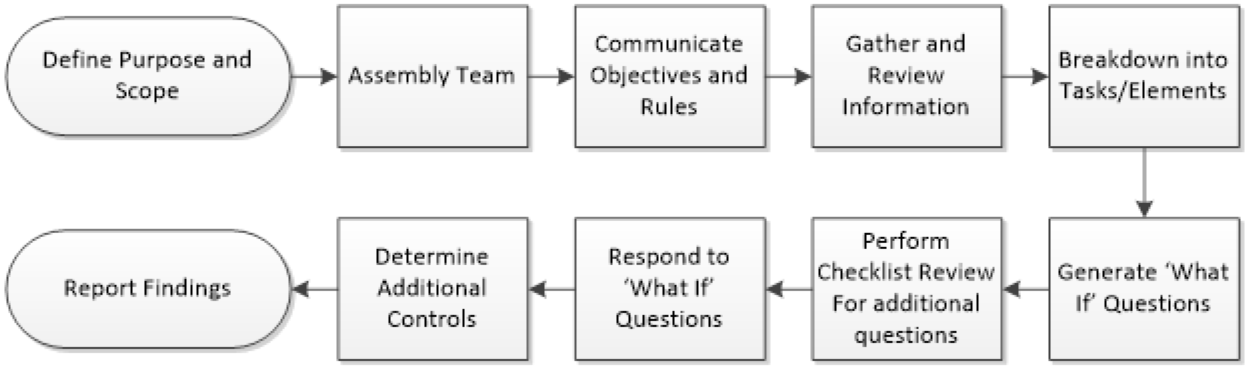
CHECKLIST ANALYSIS


Define Purpose and Scope
Select or Construct Checklist
Perform Checklist Analysis
List Hazards and Recommendations

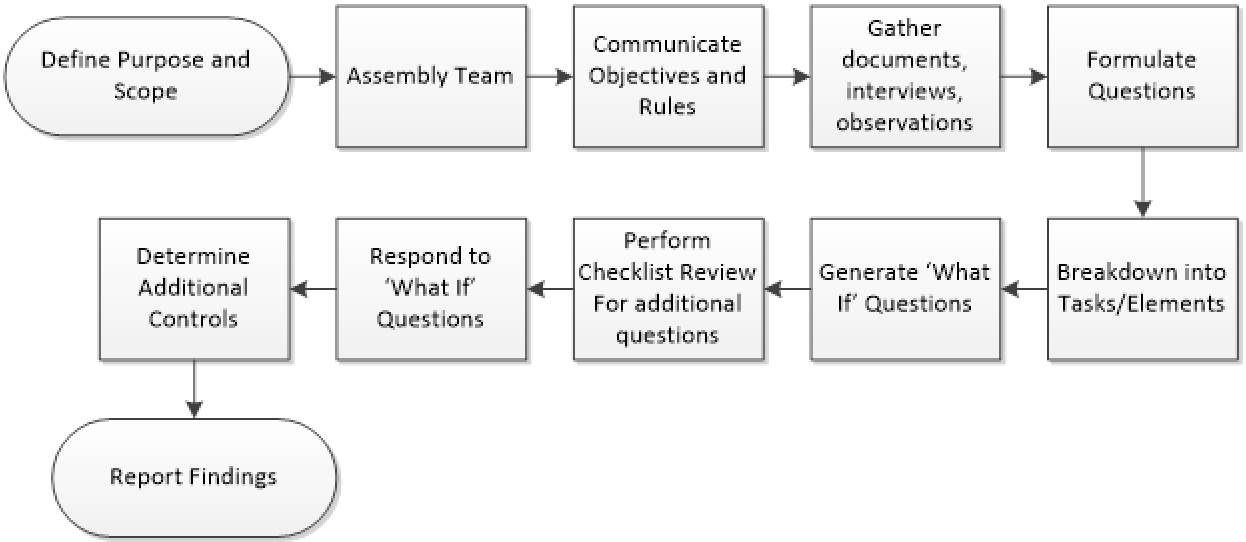
WHAT-IF HAZARD ANALYSIS


Define Purpose and Scope
Assembly Team
Communicate Objectives and Rules
Gather and Review Information
Breakdown into Tasks/Elements
Generate 'What If' Questions
Respond to 'What If' Questions
Determine Additional Controls
Report Findings

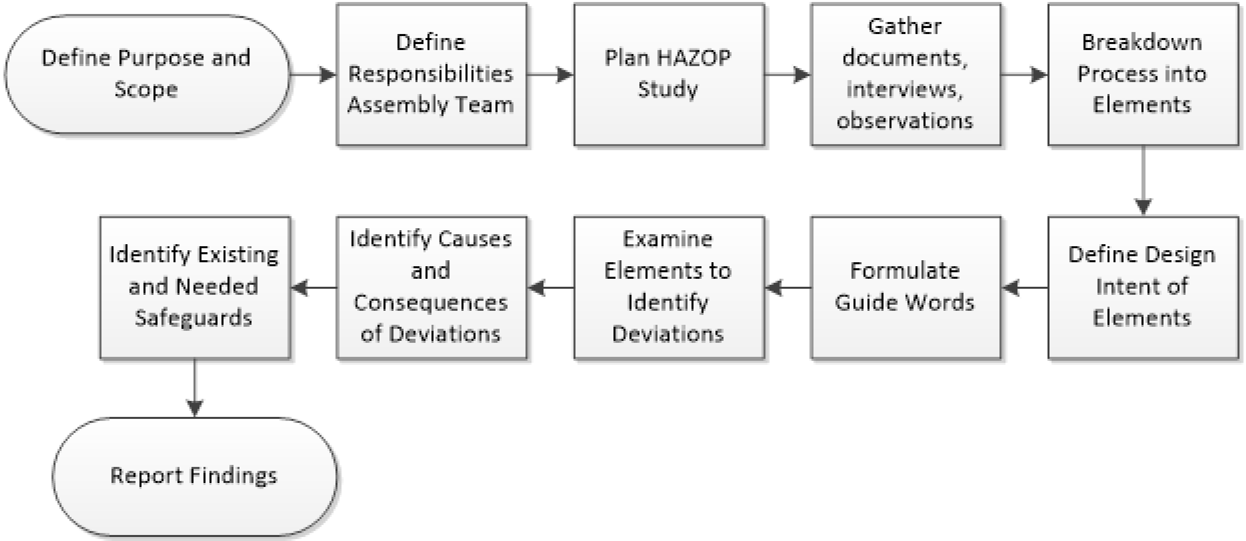
WHAT-IF CHECKLIST


Define Purpose and Scope
Assembly Team
Communicate Objectives and Rules
Gather and Review Information
Breakdown into Tasks/Elements
Generate 'What If' Questions
Perform Checklist Review For additional questions
Respond to 'What If' Questions
Determine Additional Controls
Report Findings

STRUCTURED WHAT-IF TECHNIQUE (SWIFT)


Define Purpose and Scope
Assembly Team
Communicate Objectives and Rules
Gather documents, interviews, observations
Formulate Questions
Breakdown into Tasks/Elements
Generate 'What If' Questions
Perform Checklist Review For additional questions
Respond to 'What If' Questions
Determine Additional Controls
Report Findings

HAZARD AND OPERABILITY STUDY (HAZOP)


Define Purpose and Scope
Define Responsibilities Assembly Team
Plan HAZOP Study
Gather documents, interviews, observations
Breakdown Process into Elements
Define Design Intent of Elements
Formulate Guide Words
Examine Elements to Identify Deviations
Identify Causes and Consequences of Deviations
Identify Existing and Needed Safeguards
Report Findings

RISK SCORING AND RANKING

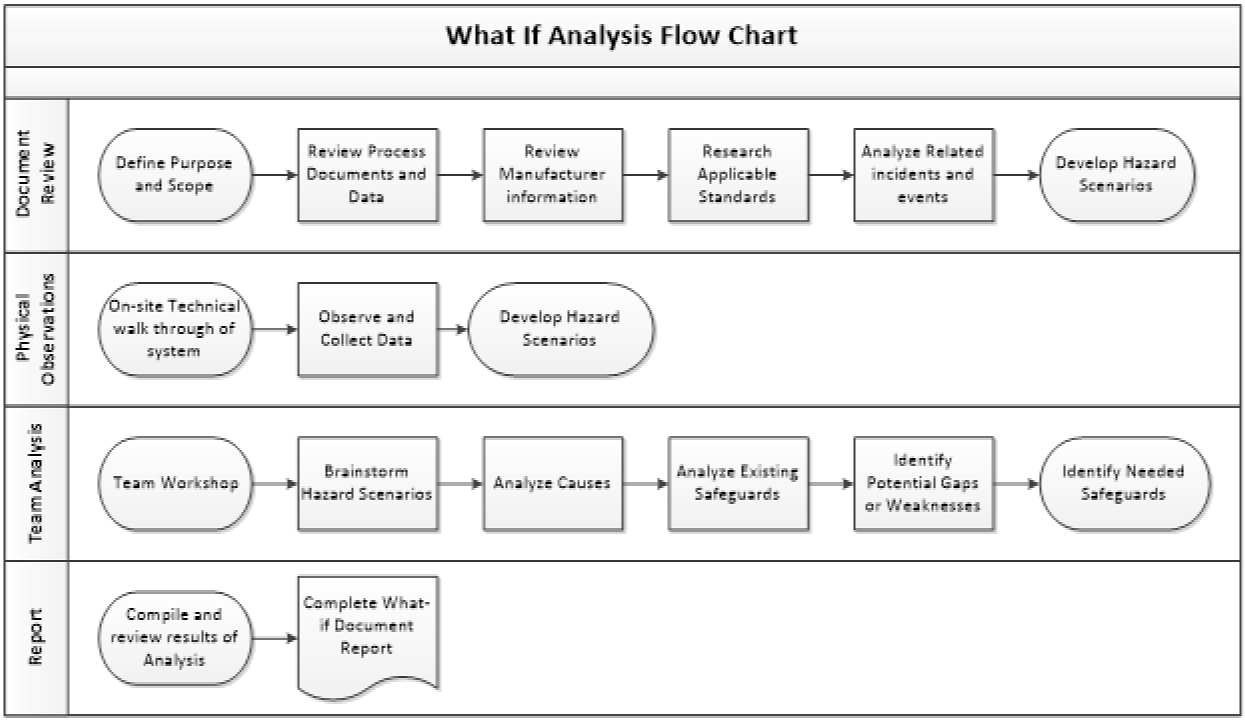
A shortcoming in traditional hazard analysis methods is that they do not include the extra step of estimating risk. Safety professionals are advised to include the risk assessment step in such methods to provide their organizations adequate decision-making information.

Following a What-if analysis, an analysis should be made of each hazard's likelihood of exposure scenario and its severity of consequences to estimate and rank risks for risk reduction.

APPLICATION OF 'WHAT IF

1. The flexibility of the What-If Analysis approach can be applied to nearly any operation, process or activity, either existing or planned.
2. It can be applied to routine and non-routine activities, maintenance and service work, installations and setup activities among others.
3. From a design review standpoint, this method can be used to identify single failures and obvious hazards of proposed changes or new designs.

WHAT-IF ANALYSIS


What If Analysis Flow Chart
Document Review
Define Purpose and Scope
Review Process Documents and Data
Review Manufacturer information
Research Applicable Standards
Analyze Related incidents and events
Develop Hazard Scenarios
Physical Observations
On-site Technical walk through of system
Observe and Collect Data
Develop Hazard Scenarios
Team Analysis
Team Workshop
Brainstorm Hazard Scenarios
Analyze Causes
Analyze Existing Safeguards
Identify Potential Gaps or Weaknesses
Identify Needed Safeguards
Report
Compile and review results of Analysis
Complete What-if Document Report

Structured What-If Technique Analysis

Facility/Operation/Process: Rail Tank Car Cleaning - Vapor Combustion System

Date: June 12-17, 2012	Team: Bruce Lyon, Facilitator; Deane H., Fire Protection Specialist; Tom G., Engineering; Jay P., Safety & Health; Charles T., Environmental; Don B., Maintenance; Kevin S., Production/Tank Car Cleaning

A. Pre-Startup & Flare Purging

ID #	What-If...	Causes	Consequences	Controls	Recommendations
A.1.	Insufficient purging of flare system	Inadequate amount of purge gas used (at least ten system volumes) to drop O_2 level below 8%	Fire or explosion	Operator training in purging procedure	A.1.1 Automatic timing system for purge; (Options: Gauge to show adequate volume of purge gas used; Oxygen testing of flare system after purge to verify) A.1.2 Purge point as close to relief valves as possible.
A.2	Steam is used to purge the flare system	Human error - steam used to purge system	Fire or explosion - steam condenses in piping without displacing air.	Operator training in purging procedure	A.2.1 Physical interlock to prevent steam from being used in purge. A.2.2 Warning signage instructions
A.3	Igniting pilots before air is removed from system	Human error or omission - Inadequate purge; lack of purge	Fire or explosion	Operator training in purging procedure	A.3.1 Procedure to verify purging is complete before ignition.

CONCLUSION

What-If Hazard Analysis is a relatively simple and flexible method of identifying and analyzing hazards in a process, activity or system. It can be applied to a wide range of circumstances in almost all industries. As one of the process hazard analysis methods listed in the OSHA Process Safety Management standard, the What-If method has become a commonly used technique, both in regulated and non-regulated operations.

HAZAN

HAZAN stands for Hazard Analysis and is a technique that focuses on job tasks as a way to identify hazards before they occur. HAZAN takes into account the relationship between the employee, the task to be done, the tools at the workers disposal and the surrounding environment. Once uncontrolled hazards have been identified by a HAZAN analysis, steps can be taken to either eliminate risks or reduce risk to an acceptable level.

Hazan is a hazard analysis and is a term used in safety engineering for the logical, systematic examination of an item, process, condition, facility, or system to identify and analyze the source, causes, and consequences of potential or real unexpected events which can occur. A hazard analysis considers system state (e.g. operating environment) as well as failures or malfunctions. Hazan is the identification of undesired events that lead to the materialization of a hazard, the analysis of the mechanisms by which these undesired events could occur, and, usually, the estimation of the consequences. Every hazard analysis consists of the following three steps.

- Estimating how often the incident will occur.
- Estimating the consequences for the employees, the process, the plant, the public and the environments.
- Comparing the results of first two steps with a target or criterion to decide whether or not action to reduce the probability of occurrence or to minimize the consequences is desirable, or whether the hazard can be ignored, at least for the time being.

Hazan is therefore the essential prerequisite for the complete risk assessment process which includes

(i) analysis of the hazards,

(ii) assessment of the risks which the hazards present, and

(iii) determination of ameliorating measures, if any, required to be taken.

Hazan is the first step in the process used for the assessment of the risk. The result of a hazard analysis is the identification of different type of hazards. A hazard is a potential condition which either exists or not exists (probability is 1 or 0). It may in single existence or in combination with other hazards (sometimes called events) and conditions become an actual functional failure or accident (mishap). The way this exactly happens in one particular sequence is called a scenario. This scenario has a probability (between 1 and 0) of occurrence. Often a system has many potential failure scenarios. It also is assigned a classification, based on the worst case severity of the end condition. Risk is the combination of probability and severity. Preliminary risk levels can be provided in the hazard analysis. The main goal of hazan is to provide the best selection of means of controlling or eliminating the risk.

HAZOP

What is HAZOP: A Hazard and Operability (HAZOP) study is a structured and systematic examination of a planned or existing process or operation in order to identify and evaluate

potential hazards and operability problems. Or to ensure the ability of equipments in accordance with the design intent.The HAZOP analysis technique uses a systematic process to identify possible deviations from normal operations and ensure that appropriate safeguards are in place to help prevent accidents. It uses special adjectives combined with process conditions to systematically consider all credible deviations from normal conditions. The adjectives, called guide words, are a unique feature of HAZOP analysis.
In addition to its utility in Quality Risk Management, HAZOP is also commonly used in risk assessments for industrial and environmental health and safety applications.
Definitions: When describing the HAZOP methodology, the following definitions1 are useful:
Hazard - Potential source of harm. Deviations from design or operational intent may constitute or produce a hazard. Hazards are the focus of HAZOP studies, and it should be noted that a single hazard could potentially lead to multiple forms of harm.
Harm - Physical injury or damage to the health of people or damage to property or the environment. Harm is the consequence of a hazard occurring and may take many forms: patient or user safety, employee safety, business risks, regulatory risks, environmental risks, etc.
Risk - Combination of probability of occurrence of harm and the severity of that harm. In a strict sense, “risk” is not always explicitly identified in HAZOP studies since the core methodology does not require identification (also referred to as rating) of the probability or severity of harm. However, risk assessment teams may choose to rate these factors in order to further quantify and prioritize risks if needed.
Usage: HAZOP is best suited for assessing hazards in facilities, equipment, and processes and is capable of assessing systems from multiple perspectives:
Design: Assessing system design capability to meet user specifications and safety standards. Identifying weaknesses in systems.
Physical and operational environments: Assessing environment to ensure system is appropriately situated, supported, serviced, contained, etc.
Operational and procedural controls: Assessing engineered controls (ex: automation), sequences of operations, procedural controls (ex: human interactions) etc. Assessing different operational modes – start-up, standby, normal operation, steady & unsteady states, normal shutdown, emergency shutdown, etc.

LIMITATION OF THE HAZOP TECHNIQUE:

a.Requires a well-defined system or activity: The HAZOP process is a rigorous analysis tool that systematically analyzes each part of a system or activity. To apply the HAZOP guide words effectively and to address the potential accidents that can result from the guide word deviations, the analysis team must have access to detailed design and operational information. The process systematically identifies specific engineered safeguards (e.g., instrumentation, alarms, and interlocks) that are defined on detailed engineering drawings.

b.Time consuming: The HAZOP process systematically reviews credible deviations, identifies potential accidents that can result from the deviations, investigates engineering and administrative controls to protect against the deviations, and generates recommendations for system improvements. This detailed analysis process requires a substantial commitment of time from both the analysis facilitator and other subject matter experts, such as crew members, engineering personnel, equipment vendors, etc.

c.Focuses on one-event causes of deviations: The HAZOP process focuses on identifying single failures that can result in accidents of interest. If the objective of the analysis is to identify all combinations of events that can lead to accidents of interest, more detailed techniques should be used.

PROCEDURE FOR HAZOP ANALYSIS:

Definition of some useful items:

i. Node: Node is some specific sections of the system in which (the deviations of) the design / process intent are evaluated. A node can be a subsystem, a function group, a function or a sub function.
ii. Deviation: A deviation is a way in which the process conditions may depart from their design / process intent. It is created by combining guide words with process parameters resulting in a possible deviation from design intent.
iii. Process parameters: The process parameters is the relevant parameter for the conditions of the process. For example, voltage, data, direction, etc.
iv. Guide words: The guide words, or secondary keywords, applied in conjunction with a Primary Keyword, these suggest potential deviations or problems. For example, less, more, no, reverse, etc.

  b. Define the system or activity: The system boundaries should be specified and clearly defined. By doing these, analysts can avoid overlooking key elements at interfaces.
  c. Main process of the HAZOP Analysis:
    i. Divide the system into sections and develop credible deviations.
    ii. Determine the cause of the deviation and evaluate the consequences/problems.
    iii. Find the safeguard which help to reduce the occurrence frequency of the deviation or to mitigate its consequences.
    iv. Recommend some actions to against the deviation more effectively,
    v. Record the information.
    vi. Repeat procedure.
    vii. First we should divided the system into several sections and choose one as a node. Of course we should know the design intent of this node so that we could find the process parameters from it. After that we should apply some guide-word to match these parameters and both of them compose a deviation.
    Guide Word + System Parameter = Deviation

HAZOP ABOUT STEPPER MOTOR DEMO

  d. What is Stepper Motor Demo: Stepper Motor Demo is a RTLinux Application which controls the running status of a small stepper motor. Our intent is to analysis the Hazards and Operability of a system by analyzing a actual example on the stepper motor demo.

e. Specify the problems which include some issues: As a system with the motor, it may appear some problems as following:
    i. The motor burn down or cannot rotate forever
    ii. The motor rotate too quick
        1. The motor do contrarily what you want it do, for the direction is reverse
f. Divide the system by interfaces
g. Develop the deviations
h. Analysis the interface 3

VULNERABILITY MODELS

Introduction Vulnerability is not a new or modern concept. Before risks and hazards, vulnerability was used to define the exposure of an individual or of a facility to a potential aggression. An individual could be exposed to illnesses, a house to natural disasters, and a facility to malevolence. So, vulnerability could be divided into: • individual vulnerability which could be:

1. physical-takes into account the genetic aspects and also the acquired work consequences like stressed.

2. social-takes into account the position of the individual on the social ladder, his life goals and expectations, his relationship with colleagues and supervisors.

3. economic vulnerability-if the individual is exposed he would try a strategy in order to find the necessary money. This strategy could be based on own work (to optimize his activity, to work supplementary hours) or could be based on antisocial and malevolent acts (Berkes, 1998). • vulnerability of facilities-here being included from hand tools (being vulnerable to decay if not maintained properly) to complex process installations. Facilities are vulnerable to natural and malevolent aggression. In between they are also vulnerable to decay or damage occurring from work acts;

• vulnerability of community-communities are an aggregate of individuals and facilities .The individuals could lead to a vulnerability profile for the community if they have common characteristics-for example populations from a certain area are more exposed to specific aggressors than other populations. The facilities could have certain characteristics that could also increase the community vulnerability (for example nuclear facilities, process facilities near the houses, etc.).

A community could also be affected by natural disasters like the Katrina (NRS, 2002). Vulnerabilities could be studied, managed and in the end could be prevented and mitigated towards an ALARP level. All this process should be done on a systemic and scientific basis in order to have an appropriate and clear image of what is in place at this moment, what should be

done, etc. A very important aspect is to prevent eliminated vulnerabilities to re-occur. In this respect a continuous control is needed.

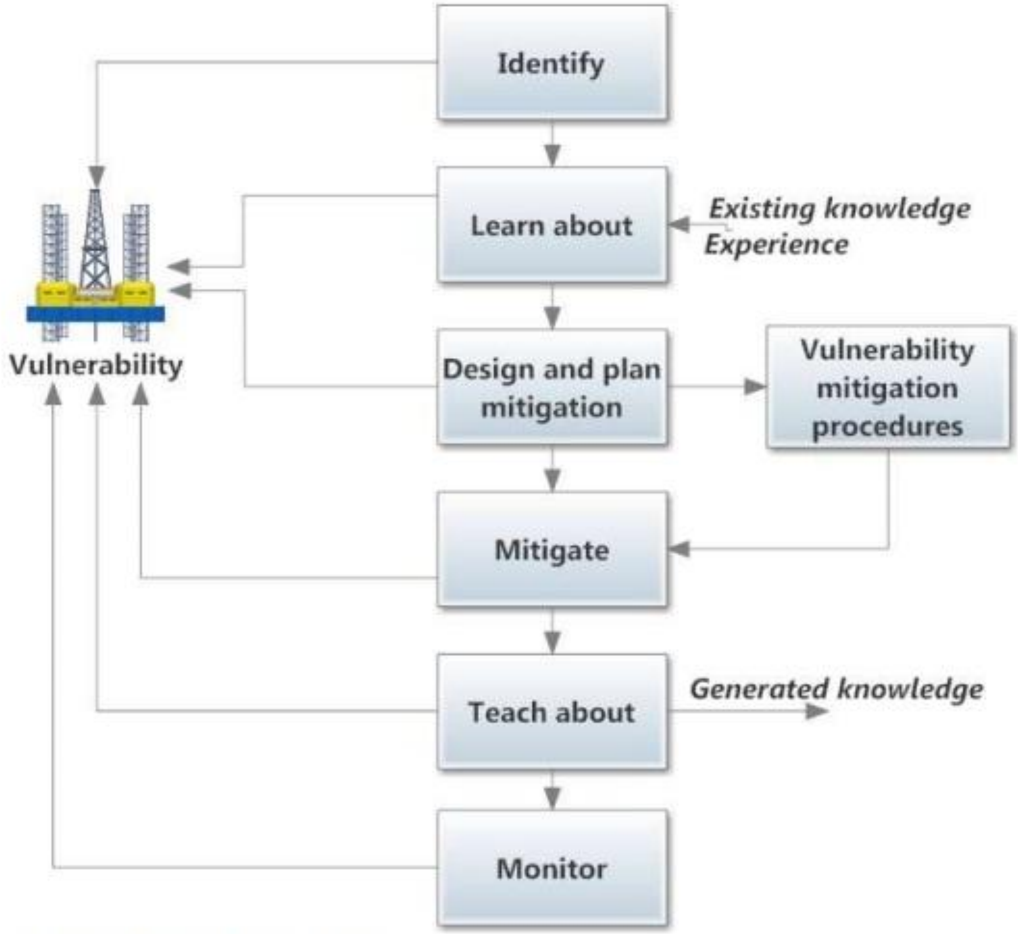


Figure 1 Steps in the treatment of vulnerability

As shown in the figure, vulnerability must initially be identified and we must learn about it. An already identified vulnerabilitywhich is not mitigated- is a very serious problem for every management and a potential major event in happening. A good management would never allow such a vulnerability that is not mitigated below the ALARP level. A vulnerability management includes the usage of existing knowledge (if we don t know nothing about the vulnerability we could not mitigate it) and also the generation of new knowledge in order to improve the mitigation process. The paper shows some research based aspects regarding the usage of vulnerability and its derived concepts- like vulnerability assessment and vulnerability management in occupational risk management. Most of these aspects were developed during the preparation for the course Vulnerability Analysis and Return on Prevention Analysis developed inside the iNTegRisk project.

VULNERABILITY ASSESSMENT — the first step towards an optimal management A vulnerability analysis or assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Examples of systems for which vulnerability assessments are performed could be found in every economic domain- they include, but are not limited to, nuclear power plants, information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems. Why analyse vulnerabilities and not risks? Vulnerability analysis and research could be a preliminary phase of risk analysis. It involves lesser costs and also could be done more quickly and with lesser resources. As risk is more general notion vulnerabilities could be specifically targeted. Usually, the elimination of vulnerability leads to the elimination of the linked risks. If a building is, for example, no more vulnerable to earthquakes then the risk of falling down is eliminated as the risk of being caught under the rubble. The notion of vulnerability, by itself supposes that some actions should be taken in order to eliminate or mitigate the vulnerability. Vulnerability assessment has many things in common with risk assessment. Assessments are typically performed according to the following steps: 1. Distributing assets and capabilities (resources) in a system.2.Assigning quantifiable value (or at least rank order) and importance to those resources 3. Identifying the vulnerabilities or potential threats to each resource 4. Mitigating or eliminating the most serious vulnerabilities for the most valuable resources Vulnerability assessment is an important subset of the risk assessment process (see figure). It can be more prescriptive than risk assessment. Vulnerability assessment involves looking at the system elements and layout and their failure modes based on a given set of threats or .“attacks...” The vulnerability assessment answers the basic question, “what can go wrong should the system be exposed to threats and hazards of concern?” Line managers and technical staff at individual facilities or service provider organizations can perform a vulnerability assessment. Although risk is often calculated using the likelihood-cost equation, risk assessment ends with the judgment of stakeholders at the executive level of government and private companies. The determination of risk starts with the results of the vulnerability assessment and adds consideration of the likelihood of threats coupled with the economic, political and social consequences of the system failure. The end of the risk assessment process is a decision concerning whether or not to take action based on the acceptability of risks identified. The mitigation phase should involve: 1. Collection – The company collects vulnerability reports in two ways: monitoring public sources of vulnerability information and processing reports sent directly to the company. After receiving reports, they perform an initial surface analysis to eliminate duplicates and false alarms, and then catalog the reports in a database. 2. Analysis - Once the vulnerabilities are catalogued, the company determines general severity, considering factors such as the number of affected systems, impact, and attack scenarios. Based on severity and other attributes, they select vulnerabilities for further analysis. The analysis includes background research, runtime and static analyses, reproduction in own test facilities, and consultation with vendors and other experts. 3. Coordination - When handling direct reports, the company works privately with suppliers and clients to address vulnerabilities before widespread public disclosure. 4. Disclosure - After coordinating with all the stakeholders, the company take steps to notify critical audiences and the public about the vulnerabilities. To the best of their ability, they produce accurate, objective technical information focused on solutions and mitigation techniques. Targeting a technical audience (administrators and others who are responsible for securing systems), they provide sufficient information to make an informed decision about risk.

The vulnerability assessment tool — methodology The vulnerability assessment methodology has the following objectives: 1. Understand the facility/organization’s mission and mission-supporting systems and functions 2. Identify mission-threatening vulnerabilities of critical facility systems 3. Understand system design and operation in order to determine failure modes and likelihoods 4. If possible, identify consequences of system failures in terms of down time, effects on people, and any cascading effects on other systems and organizations.(While failure cost analysis is not an explicit part of a vulnerability assessment, such information may flow from return on prevention (ROP) analysis.) (Turner, 2003) 5. Recommend facility improvements to reduce vulnerability The methodology is based upon the Improved Vulnerability Assessment Framework (IVAF) which was developed and improved as a response to the Presidential Decision Directive 63. The Improved Vulnerability Assessment Framework (IVAF) that was developed here would act through a three-step process and will enable an economic entity: • to define its Minimum Essential Infrastructure (MEI), • identify and locate interdependencies and vulnerabilities of MEI; • provide the basis for developing mitigation and management plans. The IVAF has been designed with inherent scalability so that it is applicable to all levels of economic structure. IVAF is based on a holistic approach taking into account the existing experience, mainly at the national level. Main objectives of IVAF are presented next: • The IVAF must apply to enterprise vulnerabilities in both physical and cyber dimensions. • The IVAF must be scalable, capable of being applied by all the enterprise, irrespective of their employee number. • The IVAF must be open and flexible, allowing the user to give emphasis to those areas of the IVAF of greatest importance to its specific enterprise. • The IVAF should incorporate a delivery mechanism that is readily acceptable to both National Authorities and the business world, and not one that would require new government regulation or structures. (The IVAF can be implemented by an auditor, both within the context of business risk assessment, and the growing accountancy requirement to assess risks and adequacy of controls over enterprise.) • The IVAF must be flexible enough to draw from other sources of expertise for updated analytical information. • The IVAF process must be repeatable over time. Today's IVAF outcomes must be valid in tomorrow's investment climate. • The methodology primarily consists of three major steps, as shown in Figure 2. Each step consists of a series of activities, which are outlined in the following paragraphs. Using these assessment steps, the assessment team will compile a list of vulnerabilities for the organization to evaluate and determine appropriate next steps. Next steps include determining the order in which vulnerabilities should be addressed, the resources required, and the level of investment necessary to meet the management's objectives.

EVENT TREE ANALYSIS

Event tree is an inductive analytical diagram in which an event is analyzed using Boolean logic to examine a chronological series of subsequent events or consequences. For example, event tree analysis is a major component of nuclear reactor safety engineering.

ANALYTICAL TOOL

Event tree analysis (**ETA**) is a forward, bottom up, logical modeling technique for both success and failure that explores responses through a single initiating event and lays a path for assessing probabilities of the outcomes and overall system analysis.[1] This analysis technique is used to analyze the effects of functioning or failed systems given that an event has occurred. ETA is a powerful tool that will identify all consequences of a system that have a probability of occurring after an initiating event that can be applied to a wide range of systems including: nuclear power plants, spacecraft, and chemical plants. This Technique may be applied to a system early in the design process to identify potential issues that may arise rather than correcting the issues after they occur.With this forward logic process use of ETA as a tool in risk assessment can help to prevent negative outcomes from occurring by providing a risk assessor with the probability of occurrence. ETA uses a type of modeling technique called event tree, which branches events from one single event using Boolean logic.

Performing a probabilistic risk assessment starts with a set of initiating events that change the state or configuration of the system. An initiating event is an event that starts a reaction, such as the way a spark (initiating event) can start a fire that could lead to other events (intermediate events) such as a tree burning down, and then finally an outcome, for example, the burnt tree no longer provides apples for food. Each initiating event leads to another event and continuing through this path, where each intermediate event's probability of occurrence may be calculated by using fault tree analysis, until an end state is reached (the outcome of a tree no longer providing apples for food). Intermediate events are commonly split into a binary (success/failure or yes/no) but may be split into more than two as long as the events are mutually exclusive, meaning that they can not occur at the same time. If a spark is the initiating event there is a probability that the spark will start a fire or will not start a fire (binary yes or no) as well as the probability that the fire spreads to a tree or does not spread to a tree. End states are classified into groups that can be successes or severity of consequences. An example of a success would be that no fire started and the tree still provided apples for food while the severity of consequence would be that a fire did start and we lose apples as a source of food. Loss end states can be any state at the end of the pathway that is a negative outcome of the initiating event. The loss end state is highly dependent upon the system, for example if you were measuring a quality process in a factory a loss or end state would be that the product has to be reworked or thrown in the trash. Some common loss end states:

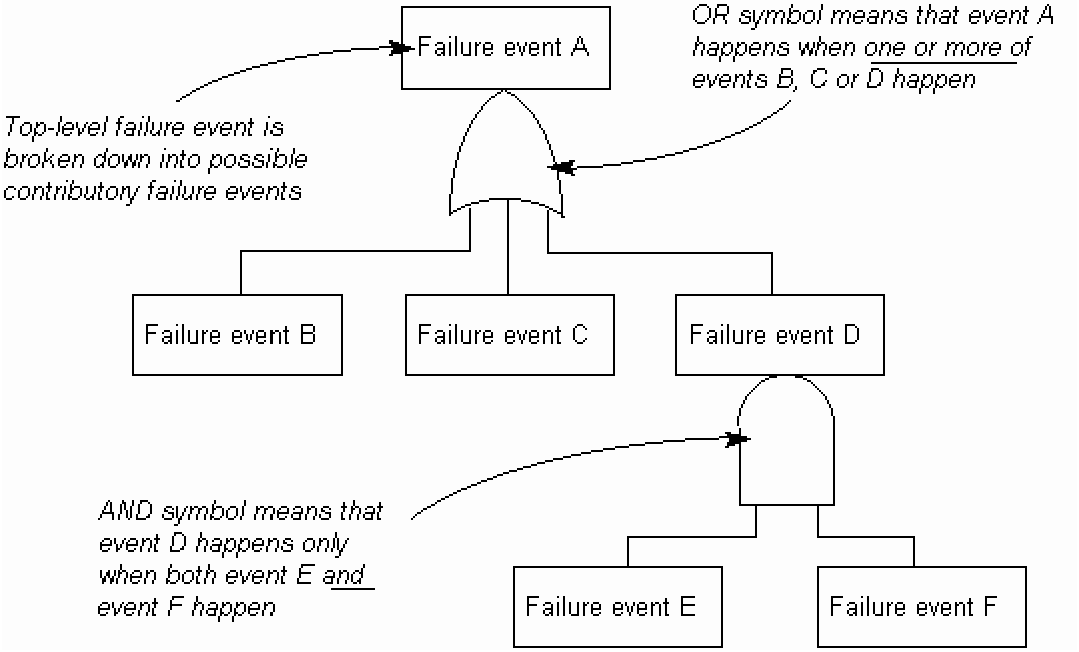
- Loss of Life or Injury/ Illness to personnel
- Damage to or loss of equipment or property (including software)
- Unexpected or collateral damage as a result of tests
- Failure of mission
- Loss of system availability
- Damage to the environment

METHODOLOGY

The overall goal of event tree analysis is to determine the probability of possible negative outcomes that can cause harm and result from the chosen initiating event. It is necessary to use detailed information about a system to understand intermediate events, accident scenarios, and initiating events to construct the event tree diagram. The event tree begins with the initiating event where consequences of this event follow in a binary (success/failure) manner. Each event creates a path in which a series of successes or failures will occur where the overall probability of occurrence for that path can be calculated. The probabilities of failures for intermediate events can be calculated using fault tree analysis and the probability of success can be calculated from 1 = probability of success(ps) + probability of failure (pf). For example, in the equation 1 = (ps) + (pf) if we know that pf=.1 from fault tree analysis then through simple algebra we can solve for ps where ps = (1) - (pf) then we would have ps = (1) - (.1) and ps=.9.

The event tree diagram models all possible pathways from the initiating event. The initiating event starts at the left side as a horizontal line that branches vertically. the vertical branch is representative of the success/failure of the initiating event. At the end of the vertical branch a horizontal line is drawn on each the top and the bottom representing the success or failure of the first event where a description (usually success or failure) is written with a tag that represents the path such as 1s where s is a success and 1 is the event number similarly with 1f where 1 is the event number and f denotes a failure (see attached diagram). This process continues until the end state is reached. When the event tree diagram has reached the end state for all pathways the outcome probability equation is written.

Steps to perform an event tree analysis:


Failure event A
OR symbol means that event A happens when one or more of events B, C or D happen
Top-level failure event is broken down into possible contributory failure events
Failure event B
Failure event C
Failure event D
AND symbol means that event D happens only when both event E and event F happen
Failure event E
Failure event F

1. **Define the system:** Define what needs to be involved or where to draw the boundaries.
2. **Identify the accident scenarios:** Perform a system assessment to find hazards or accident scenarios within the system design.
3. **Identify the initiating events:** Use a hazard analysis to define initiating events.
4. **Identify intermediate events:** Identify countermeasures associated with the specific scenario.
5. **Build the event tree diagram**
6. **Obtain event failure probabilities:** If the failure probability can not be obtained use fault tree analysis to calculate it.
7. **Identify the outcome risk:** Calculate the overall probability of the event paths and determine the risk.
8. **Evaluate the outcome risk:** Evaluate the risk of each path and determine its acceptability.
9. **Recommend corrective action:** If the outcome risk of a path is not acceptable develop design changes that change the risk.
10. **Document the ETA:** Document the entire process on the event tree diagrams and update for new information as needed.

IN RISK ANALYSIS

Event tree analysis can be used in risk assessment by determining the probability that is used to determine the risk when multiplied by the hazard of the event. Event Tree Analysis is a tool that makes easy to see what pathway is creating the greatest probability of failure for a specific system. It is common to find single point failures that do not have any intervening events between the initiating event and a failure. With Event Tree Analysis single point failure can be targeted to include an intervening step that will reduce the overall probability of failure and thus reducing the risk of the system. The idea of adding an intervening event can happen anywhere in the system for any pathway that generates too great of a risk, the added intermediate event can reduce the probability and thus reduce the risk.

ADVANTAGES

- Enables the assessment of multiple, co-existing faults and failures
- Functions simultaneously in cases of failure and success
- No need to anticipate end events
- Areas of single point failure, system vulnerability, and low payoff countermeasures may be identified and assessed to deploy resources properly
- paths in a system that lead to a failure can be identified and traced to display ineffective countermeasures.
- Work can be computerized
- Can be performed on various levels of details
- Visual cause and effect relationship
- Relatively easy to learn and execute
- Models complex systems into an understandable manner
- Follows fault paths across system boundaries
- Combines hardware, software, environment, and human interaction
- Permits probability assessment
- Commercial software is available

LIMITATIONS

- Addresses only one initiating event at a time.
- The initiating challenge must be identified by the analyst·
- Pathways must be identified by the analyst·
- Level of loss for each pathway may not be distinguishable without further analysis·
- Success or failure probabilities are difficult to find.
- Can overlook subtle system differences·
- Partial successes/failures are not distinguishable·
- Requires an analyst with practical training and experience·

FAULT TREE ANALYSIS

Fault tree analysis (FTA) is a top down, deductive failure analysis in which an undesired state of a system is analyzed using Boolean logicto combine a series of lower-level events. This analysis method is mainly used in the fields of safety engineering and reliability engineering to understand how systems can fail, to identify the best ways to reduce risk or to determine (or get a feeling for) event rates of a safety accident or a particular system level (functional) failure. FTA is used in the aerospace, nuclear power, chemical and process, pharmaceutical, petrochemical and other high-hazard industries; but is also used in fields as diverse as risk factor identification relating to social service system failure. FTA is also used in software engineering for debugging purposes and is closely related to cause-elimination technique used to detect bugs.

In aerospace, the more general term "system Failure Condition" is used for the "undesired state" / Top event of the fault tree. These conditions are classified by the severity of their effects. The most severe conditions require the most extensive fault tree analysis. These "system Failure Conditions" and their classification are often previously determined in the functional Hazard analysis.

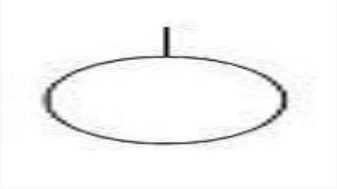
USAGE

Fault tree analysis can be used to:

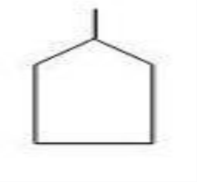
- understand the logic leading to the top event / undesired state.
- show compliance with the (input) system safety / reliability requirements.
- prioritize the contributors leading to the top event - Creating the Critical Equipment/Parts/Events lists for different importance measures.
- monitor and control the safety performance of the complex system (e.g., is a particular aircraft safe to fly when fuel valve *x* malfunctions? For how long is it allowed to fly with the valve malfunction?).
- minimize and optimize resources.
- assist in designing a system. The FTA can be used as a design tool that helps to create (output / lower level) requirements.
- function as a diagnostic tool to identify and correct causes of the top event. It can help with the creation of diagnostic manuals / processes.

EVENT SYMBOLS

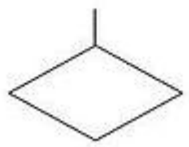
Event symbols are used for *primary events* and *intermediate events*. Primary events are not further developed on the fault tree. Intermediate events are found at the output of a gate. The event symbols are shown below:



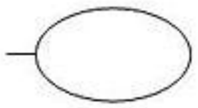
Basic event



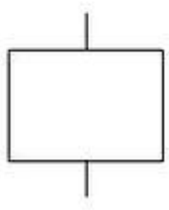
External event



Undeveloped event



Conditioning event



Intermediate event

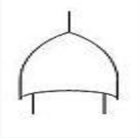
The primary event symbols are typically used as follows:

- **Basic event** - failure or error in a system component or element (example: switch stuck in open position)
- **External event** - normally expected to occur (not of itself a fault)
- **Undeveloped event** - an event about which insufficient information is available, or which is of no consequence
- **Conditioning event** - conditions that restrict or affect logic gates (example: mode of operation in effect)

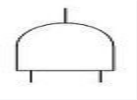
An intermediate event gate can be used immediately above a primary event to provide more room to type the event description. FTA is top-to-bottom approach.

GATE SYMBOLS

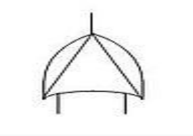
Gate symbols describe the relationship between input and output events. The symbols are derived from Boolean logic symbols:



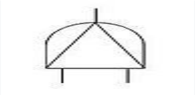
OR gate



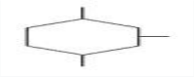
AND gate



Exclusive OR gate



Priority AND gate



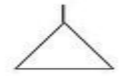
Inhibit gate

The gates work as follows:

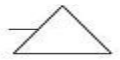
- **OR gate** - the output occurs if any input occurs
- **AND gate** - the output occurs only if all inputs occur (inputs are independent)
- **Exclusive OR gate** - the output occurs if exactly one input occurs
- **Priority AND gate** - the output occurs if the inputs occur in a specific sequence specified by a conditioning event
- **Inhibit gate** - the output occurs if the input occurs under an enabling condition specified by a conditioning event

Transfer Symbols

Transfer symbols are used to connect the inputs and outputs of related fault trees, such as the fault tree of a subsystem to its system. NASA prepared a complete document about FTA through practical incidents.



Transfer in



Transfer out

ANALYSIS

Many different approaches can be used to model a FTA, but the most common and popular way can be summarized in a few steps. A single fault tree is used to analyze one and only one undesired event or top event, which may be subsequently fed into another fault tree as a basic event. Though the nature of the undesired event may vary dramatically, a FTA follows the same procedure for any undesired event; be it a delay of 0.25 ms for the generation of electrical power, an undetected cargo bay fire, or the random, unintended launch of an ICBM. Due to labor cost, FTA is normally only performed for more serious undesired events.

FTA analysis involves five steps:

Define the undesired event to study

Definition of the undesired event can be very hard to catch, although some of the events are very easy and obvious to observe. An engineer with a wide knowledge of the design of the system or a system analyst with an engineering background is the best person who can help define and number the undesired events. Undesired events are used then to make the FTA, one event for one FTA; no two events will be used to make one FTA.

Obtain an understanding of the system

Once the undesired event is selected, all causes with probabilities of affecting the undesired event of 0 or more are studied and analyzed. Getting exact numbers for the probabilities leading to the event is usually impossible for the reason that it may be very costly and time consuming to do so. Computer software is used to study probabilities; this may lead to less costly system analysis.
System analysts can help with understanding the overall system. System designers have full knowledge of the system and this knowledge is very important for not missing any cause affecting the undesired event. For the selected event all causes are then numbered and sequenced in the order of occurrence and then are used for the next step which is drawing or constructing the fault tree.

Construct the fault tree

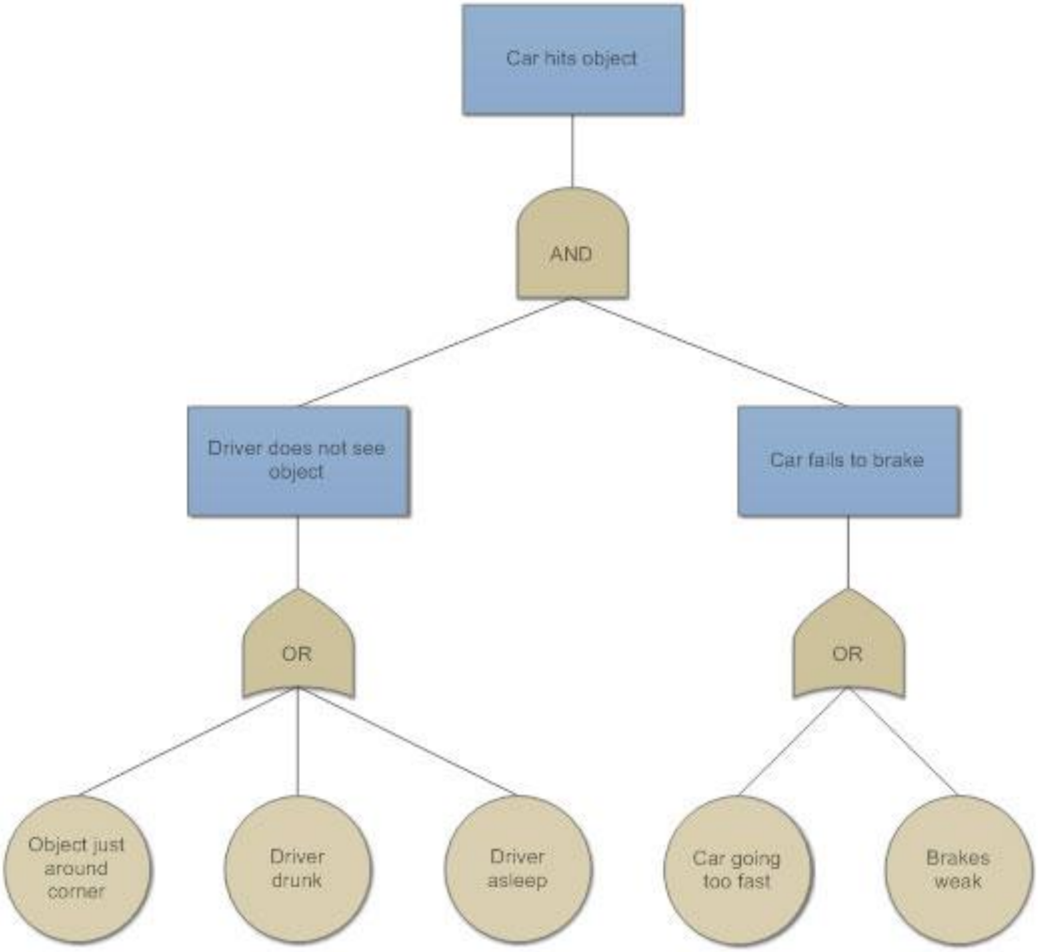
After selecting the undesired event and having analyzed the system so that we know all the causing effects (and if possible their probabilities) we can now construct the fault tree. Fault tree is based on AND and OR gates which define the major characteristics of the fault tree.

Evaluate the fault tree

After the fault tree has been assembled for a specific undesired event, it is evaluated and analyzed for any possible improvement or in other words study the risk management and find ways for system improvement. This step is as an introduction for the final step which will be to control the hazards identified. In short, in this step we identify all possible hazards affecting the system in a direct or indirect way.

Control the hazards identified

This step is very specific and differs largely from one system to another, but the main point will always be that after identifying the hazards all possible methods are pursued to decrease the probability of occurrence.



FLIXBOROUGH DISASTER

The **Flixborough disaster** was an explosion at a chemical plant close to the village of Flixborough, North Lincolnshire, Englandon Saturday, 1 June 1974. It killed 28 people and seriously injured 36 out of a total of 72 people on site at the time. The casualty figures could have been much higher, if the explosion had occurred on a weekday, when the main office area would have been occupied. A contemporary campaigner on process safety wrote "the shock waves rattled the confidence of every chemical engineer in the country".

The disaster involved (and may well have been caused by) a hasty modification. There was no on-site senior manager with mechanical engineering expertise (virtually all the plant management had chemical engineering qualifications); mechanical engineering issues with the modification were overlooked by the managers who approved it, nor was the severity of the potential consequences of its failure appreciated.

Flixborough led to a widespread public outcry over process plant safety. Together with the passage of the Health and Safety at Work Act in the same year it led to (and is often quoted in justification of) a more systematic approach to process safety in UK process industries, and – in conjunction with the Seveso disaster and the consequent EU 'Seveso directives' – to explicit UK government regulation of plant processing or storing large inventories of hazardous materials, currently (2014) by the Control of Major Accident Hazards Regulations 1999 (COMAH).

OVERVIEW

The chemical works, owned by Nypro UK (a joint venture between Dutch State Mines (DSM) and the British National Coal Board (NCB)) had originally produced fertiliser from by-products of the coke ovens of a nearby steelworks. Since 1967, it had instead produced caprolactam, a chemical used in the manufacture of nylon 6. The caprolactam was produced from cyclohexanone. This was originally produced by hydrogenation of phenol, but in 1972 additional capacity was added, built to a DSM design in which hot liquid cyclohexane was partially oxidised by compressed air. The plant was intended to produce 70,000 tpa (tons per annum) of caprolactam but was reaching a rate of only 47,000 tpa in early 1974. Government controls on the price of caprolactam put further financial pressure on the plant.

It was a failure of this plant that led to the disaster. A major leak of liquid from the reactor circuit caused the rapid formation of a large cloud of flammable hydrocarbon. When this met an ignition source (probably a furnace at a nearby hydrogen production plant[B]) there was a massive fuel-air explosion. The plant control room collapsed, killing all 18 occupants. Nine other site workers were killed, and a delivery driver died of a heart attack in his cab. Fires started on-site which were still burning ten days later. Around 1,000 buildings within a mile radius of the site (in Flixborough itself and in the neighbouring villages of Burton upon Stather and Amcotts) were damaged, as were nearly 800 in Scunthorpe (three miles away); the blast was heard over thirty miles away in Grimsby and Hull. Images of the disaster were soon shown on television, filmed by BBC and Yorkshire Television filmstock news crews who had been covering the Appleby-Frodingham Gala in Scunthorpe that afternoon.

The plant was re-built but cyclohexanone was now produced by hydrogenation of phenol (Nypro proposed to produce the hydrogen from LPG. in the absence of timely advice from the Health and Safety Executive (HSE) planning permission for storage of 1200 te LPG at Flixborough was initially granted subject to HSE approval, but HSE objected[8]); as a result of a subsequent collapse in the price of nylon it closed down a few years later. The site was demolished in 1981, although the administration block still remains. The site today is home to the Flixborough Industrial Estate, occupied by various businesses and Glanford Power Station.

The foundations of properties severely damaged by the blast and subsequently demolished can be found on land between the estate and the village, on the route known as Stather Road. A memorial to those who died was erected in front of offices at the rebuilt site in 1977. Cast in bronze, it showed mallards alighting on water. When the plant was closed, the statue was moved to the pond at the parish church in Flixborough. During the early hours of New Year's

Day 1984, the sculpture was stolen. It has never been recovered but the plinth it stood on, with a plaque listing all those who died that day, can still be found outside the church.

The cyclohexane oxidation process is still operated in much the same plant design in the Far East

THE PLANT

In the DSM process, cyclohexane was heated to about 155 °C (311 °F) before passing into a series of six reactors. The reactors were constructed from mild steel with a stainless steel lining; when operating they held in total about 145 tonnes of flammable liquid at a working pressure of 8.6 bar gauge (0.86 MPa gauge; 125 psig). In each of the reactors, compressed air was passed through the cyclohexane, causing a small percentage of the cyclohexane to oxidise and produce cyclohexanone, some cyclohexanol also being produced. Each reactor was slightly (approximately 14 inches, 350 mm) lower than the previous one, so that the reaction mixture flowed from one to the next by gravity through nominal 28-inch bore (DN 700 mm) stub pipes with inset bellows.[C] The inlet to each reactor was baffled so that liquid entered the reactors at a low level; the exiting liquid flowed over a weir whose crest was somewhat higher than the top of the outlet pipe.[9] The mixture exiting reactor 6 was processed to remove reaction products, and the unreacted cyclohexane (only about 6% was reacted in each pass) then returned to the start of the reactor loop.

Although the operating pressure was maintained by an automatically controlled bleed valve once the plant had reached steady state, the valve could not be used during start-up, when there was no air feed, the plant being pressurised with nitrogen. During start-up the bleed valve was normally isolated and there was no route for excess pressure to escape; pressure was kept within acceptable limits (slightly wider that those achieved under automatic control) by operator intervention (manual operation of vent valves). A pressure-relief valve acting at 11 kg/cm^2 (156 psi) gauge was also fitted.

REACTOR 5 LEAKS AND IS BYPASSED

Two months prior to the explosion, the number 5 reactor was discovered to be leaking. When lagging was stripped from it, a crack extending about 6 feet (1.8 m) was visible in the mild steel shell of the reactor. It was decided to install a temporary pipe to bypass the leaking reactor to allow continued operation of the plant while repairs were made. In the absence of 28-inch nominal bore pipe (DN 700 mm), 20-inch nominal bore pipe (DN 500 mm) was used to fabricate the bypass pipe for linking reactor 4 outlet to reactor 6 inlet. The new configuration was tested for leak-tightness at working pressure by pressurisation with nitrogen. For two months after fitting the bypass was operated continuously at temperature and pressure and gave no trouble. At the end of May (by which time the bypass had been lagged) the reactors had to be depressurised and allowed to cool in order to deal with leaks elsewhere. The leaks having been dealt with, early on 1 June attempts began to bring the plant back up to pressure and temperature.

THE EXPLOSION

At about 16:53 on Saturday 1 June 1974, there was a massive release of hot cyclohexane in the area of the missing reactor 5, followed shortly by ignition of the resulting cloud of flammable vapour and a massive explosion in the plant. It virtually demolished the site. Since the accident took place at a weekend there were relatively few people on site: of those on-site at the time, 28 were killed and 36 injured. Fires continued on-site for more than ten days. Off-site there were no fatalities, but 50 injuries were reported and about 2,000 properties damaged.

The occupants of the works laboratory had seen the release and evacuated the building before the release ignited; most survived. None of the 18 occupants of the plant control room survived, nor did any records of plant readings. The explosion appeared to have been in the general area of the reactors and after the accident only two possible sites for leaks before the explosion were identified: "the 20 inch bypass assembly with the bellows at both ends torn asunder was found jack-knifed on the plinth beneath" and there was a 50-inch long split in nearby 8-inch nominal bore stainless steel pipework".

COURT OF INQUIRY

Immediately after the accident, *New Scientist* commented presciently on the normal official response to such events, but hoped that the opportunity would be taken to introduce effective government regulation of hazardous process plants.

Disasters on the scale of last Saturday's tragic explosion ... at Flixborough tend to provoke a brief wave of statements that such things must never happen again. With the passage of time these sentiments are diluted into bland reports about human error and everything being well under control – as happened with the Summerland fire. In the Flixborough case, there is a real chance that the death toll could trigger meaningful changes in a neglected aspect of industrial safety.[13]

The Secretary of State for Employment set up a Court of Inquiry to establish the causes and circumstances of the disaster and identify any immediate lessons to be learned, and also an expert committee to identify major hazard sites and advise on appropriate measures of control for them. The Inquiry sat for 70 days in the period September 1974 – February 1975, and took evidence from over 170 witnesses.[f] In parallel, an Advisory Committee on Major Hazards was set up to look at the longer term issues associated with hazardous process plant.

CIRCUMSTANCES OF THE DISASTER

The report of the court of inquiry was critical of the installation of the bypass pipework on a number of counts: although plant and senior management were chartered engineers(mostly chemical engineers) the post of Works Engineer which had been occupied by a chartered mechanical engineer had been vacant since January 1974 and at the time of the accident there were no professionally qualified engineers in the works engineering department. Nypro had recognised this to be a weakness and identified a senior mechanical engineer in an NCB subsidiary as available to provide advice and support if requested. At a meeting of plant and engineering managers to discuss the failure of Reactor 5, the external mechanical engineer was not present. The emphasis was upon prompt restart and – the inquiry felt – although this did not lead to the deliberate acceptance of hazards, it led to the adoption of a course of action whose hazards (and indeed engineering practicalities) were not adequately considered or understood. The major problem was thought to be getting reactor 5 moved out of the way. Only the plant engineer was concerned about restarting before the reason for the failure was understood, and the other reactors inspected. The difference in elevation between reactor 4 outlet and reactor 6 inlet was not recognised at the meeting. At a working level the offset was accommodated by a dog-leg in the bypass assembly; a section sloping downwards inserted between (and joined with by mitre welds) two horizontal lengths of 20-inch pipe abutting the existing 28-inch stubs. This bypass was supported by scaffolding fitted with supports provided to prevent the bellows having to take the weight of the pipework between them, but with no provision against other loadings.The Inquiry noted on the "design" of the assembly:

No-one appreciated that the pressurised assembly would be subject to a turning moment imposing shear forces on the bellows for which they are not designed. Nor did anyone appreciate that the hydraulic thrust on the bellows (some 38 tonnes at working pressure) would tend to make the pipe buckle at the mitre joints. No calculations were done to ascertain whether the bellows or pipe would withstand these strains; no reference was made to the relevant British Standard, or any other accepted standard; no reference was made to the designer's guide issued by the manufacturers of the bellows; no drawing of the pipe was made, other than in chalk on the workshop floor; no pressure testing either of the pipe or the complete assembly was made before it was fitted.

The Inquiry noted further that "there was no overall control or planning of the design, construction, testing or fitting of the assembly nor was any check made that the operations had been properly carried out". After the assembly was fitted, the plant was tested for leak-tightness by pressurising with nitrogen to 9 kg/cm^2; i.e. roughly operating pressure, but below the pressure at which the system relief valve would lift and below the 30% above design pressure called for by the relevant British Standard.

CAUSE OF THE DISASTER

The 20-inch bypass was therefore clearly not what would have been produced or accepted by a more considered process but controversy developed (and became acrimonious) as to whether its failure was the initiating fault in the disaster (the 20-inch hypothesis, argued by the plant designers (DSM) and the plant constructors; and favoured by the court's technical advisers[3]), or had been triggered by an external explosion resulting from a previous failure of the 8-inch line (argued by experts retained by Nypro and their insurers

THE 20-INCH HYPOTHESIS

Tests on replica bypass assemblies showed that bellows squirm could occur at pressures below the safety valve setting, but that squirm did not lead to a leak (either from damage to the bellows or from damage to the pipe at the mitre welds) until well above the safety valve setting. However theoretical modelling suggested that the expansion of the bellows as a result of squirm would lead to a significant amount of work being done on them by the reactor contents, and there would be considerable shock loading on the bellows when they reached the end of their travel. If the bellows were 'stiff' (resistant to squirm), the shock loading could cause the bellows to tear at pressures below the safety valve setting; it was not impossible that this could occur at pressures experienced during start-up, when pressure was less tightly controlled. (Plant pressures at the time of the accident were unknown since all relevant instruments and records had been destroyed, and all relevant operators killed). The Inquiry concluded that this ("the 20-inch hypothesis") was 'a probability' but one 'which would readily be displaced if some greater probability' could be found.

THE 8-INCH HYPOTHESIS

Detailed analysis suggested that the 8-inch pipe had failed due to creep cavitation at a high temperature while the pipe was under pressure. Failure had been accelerated by contact with molten zinc and there were indications that an elbow in the pipe had been at significantly higher temperature than the rest of the pipe. The hot elbow led to a non-return valve held between two pipe flanges by twelve bolts. After the disaster, two of the twelve bolts were found to be loose; the inquiry concluded that they were probably loose before the disaster. Nypro argued that the bolts had been loose, there had consequently been a slow leak of process fluid onto lagging leading eventually to a lagging fire, which had worsened the leak to the point where a flame had played undetected upon the elbow, burnt away its lagging and exposed the line to molten zinc, the line then failing with a bulk release of process fluid which extinguished the original fire, but subsequently ignited giving a small explosion which had caused failure of the bypass, a second larger release and a larger explosion. Tests failed to produce a lagging fire with leaked process fluid at process temperatures; one advocate of the 8-inch hypothesis then argued instead that there had been a gasket failure giving a leak with sufficient velocity to induce static charges whose discharge had then ignited the leak.

THE INQUIRY CONCLUSION

The 8-inch hypothesis was claimed to be supported by eyewitness accounts and by the apparently anomalous position of some debris post-disaster. The inquiry report took the view that explosions frequently throw debris in unexpected directions and eyewitnesses often have confused recollections. The inquiry identified difficulties at various stages of the accident development in the 8-inch hypothesis, their cumulative effect being considered to be such that the report concluded that overall the 20-inch hypothesis involving 'a single event of low probability' was more credible than the 8-inch hypothesis depending upon 'a succession of events, most of which are improbable'.

LESSONS TO BE LEARNED

The inquiry report identified 'lessons to be learned' which it presented under various headings; 'General observation' (relating to cultural issues underlying the disaster), 'specific lessons' (directly relevant to the disaster, but of general applicability) are reported below; there were also 'general' and 'miscellaneous lessons' of less relevance to the disaster. The report also commented on matters to be covered by the Advisory Committee on Major Hazards.

GENERAL OBSERVATION

- Plant – where possible – should be designed so that failure does not lead to disaster on a timescale too short to permit corrective action.
- Plant should be designed and run to minimise the rate at which critical management decisions arise (particularly those in which production and safety conflict).
- Feedback within the management structure should ensure that top management understand the responsibilities of individuals and can ensure that their workload, capacity and competence allow them to effectively deal with those responsibilities

SPECIFIC LESSONS

The disaster was caused by 'a well designed and constructed plant' undergoing a modification that destroyed its technical integrity.

- Modifications should be designed, constructed, tested and maintained to the same standards as the original plant

When the bypass was installed, there was no works engineer in post and company senior personnel (all chemical engineers) were incapable of recognising the existence of a simple engineering problem, let alone solving it

- When an important post is vacant special care should be taken when decisions have to be taken which would normally be taken by or on the advice of the holder of the vacant post
- All engineers should learn at least the elements of other branches of engineering than their own

MATTERS TO BE REFERRED TO THE ADVISORY COMMITTEE

No one concerned in the design or construction of the plant envisaged the possibility of a major disaster happening instantaneously.[J] It was now apparent that such a possibility exists where large amounts of potentially explosive material are processed or stored. It was 'of the greatest importance that plants at which there is a risk of instant as opposed to escalating disaster be identified. Once identified measures should be taken both to prevent such a disaster so far as is possible and to minimise its consequences should it occur despite all precautions. There should be coordination between planning authorities and the Health and Safety Executive, so that planning authorities could be advised on safety issues before granting planning permission; similarly the emergency services should have information to draw up a disaster plan.

CONCLUSION[

THE INQUIRY SUMMARISED ITS FINDINGS AS FOLLOWS:

We believe, however, that if the steps we recommend are carried out, the risk of any similar disaster, already remote, will be lessened. We use the phrase "already remote" advisedly for we wish to make it plain that we found nothing to suggest that the plant as originally designed and constructed created any unacceptable risk. The disaster was caused wholly by the coincidence of a number of unlikely errors in the design and installation of a modification. Such a combination of errors is very unlikely ever to be repeated. Our recommendations should ensure that no similar combination occurs again and that even if it should do so, the errors would be detected before any serious consequences ensued

RESPONSE TO INQUIRY REPORT

CONTROVERSY AS TO IMMEDIATE CAUSE

Nypro's advisers had put considerable effort into the 8-inch hypothesis, and the inquiry report put considerable effort into discounting it. The critique of the hypothesis spilled over into criticism of its advocates: 'the enthusiasm for the 8-inch hypothesis felt by its proponents has led them to overlook obvious defects which in other circumstances they would not have failed to realise'.] Of one proponent the report noted gratuitously that his examination by the court 'was directed to ensuring that we had correctly appreciated the main steps in the hypothesis some of which appeared to us in conflict with facts which were beyond dispute'.The report thanked him for his work in assembling eyewitness evidence but said his use of it showed 'an approach to the evidence which is wholly unsound'.

The proponent of the 8-inch gasket failure hypothesis responded by arguing that the 20-inch hypothesis had its share of defects which the inquiry report had chosen to overlook, that the 8-inch hypothesis had more in its favour than the report suggested, and that there were important lessons that the inquiry had failed to identify:

[T]he Court's commitment for the 20-inch hypothesis led them to present their conclusions in a way that does not help the reader to assess contrary evidence. The Court could still be right that a single unsatisfactory modification caused the disaster but this is no reason for complacency.

There are many other lessons. It is to be hoped that the respect normally accorded to the findings of a Court of Inquiry will not inhibit chemical engineers in looking beyond the report in their endeavours to improve the already good safety record of the chemical industry.

The Flixborough inquiry findings have not been accorded the normal respect; one critic of them was able to note after a flurry of articles on the 25th anniversary:

POST-ENQUIRY FORENSIC ENGINEERING – TWO-STAGE RUPTURE OF BYPASS

The enquiry noted the existence of a small tear in a bellows fragment, and therefore considered the possibility of a small leak from the bypass having led to an explosion bringing the bypass down. It noted this to be not inconsistent with eyewitness evidence, but ruled out the scenario because pressure tests showed the bellows did not develop tears until well above the safety valve pressure.[t] This hypothesis has however been revived, with the tears being caused by fatigue failure at the top of the reactor 4 outlet bellows because of flow-induced vibration of the unsupported bypass line. finite element analysis has been carried out (and suitable eyewitness evidence adduced) to support this hypothesis.

POST-ENQUIRY FORENSIC ENGINEERING – THE 'WATER HYPOTHESIS'

The reactors were normally mechanically stirred but reactor 4 had operated without a working stirrer since November 1973; free phase water could have settled out in unstirred reactor 4 and the bottom of reactor 4 would reach operating temperature more slowly than the stirred reactors. It was postulated that there had been bulk water in reactor 4 and a disruptive boiling event had occurred when the interface between it and the reaction mixture reached operating temperature. Abnormal pressures and liquor displacement resulting from this (it was argued) could have triggered failure of the 20-inch bypass.

DISSATISFACTION WITH OTHER ASPECTS OF THE INQUIRY REPORT

The plant design had assumed that the worst consequence of a major leak would be a plant fire and to protect against this a fire detection system had been installed. Tests by the Fire Research Establishment had shown this to be less effective than intended. Moreover, fire detection only worked if the leak ignited at the leak site; it gave no protection against a major leak with delayed ignition, and the disaster had shown this could lead to multiple worker fatalities. The plant *as designed* therefore could be destroyed by a single failure and had a much greater risk of killing workers than the designers had intended. Critics of the inquiry report therefore found it hard to accept its characterisation of the plant as 'well-designed'. The HSE (through the Department of Employment) had come up with a 'shopping list' of about 30 recommendations on plant design,[many of which had not been adopted (and a few explicitly rejected) by the Inquiry Report; the HSE inspector who acted as secretary to the inquiry spoke afterwards of making sure that the real lessons were acted upon.undamentally, Trevor Kletz saw the plant as symptomatic of a general failure to consider safety early enough in process plant design, so that designs were inherently safe – instead processes and plant were selected on other grounds then safety systems bolted on to a design with avoidable hazards and unnecessarily high inventory. 'We keep a lion and build a strong cage to keep it in. But before we do so we should ask if a lamb might do.'

If the UK public were largely reassured to be told the accident was a one-off and should never happen again, some UK process safety practitioners were less sanguine. Critics felt that the Flixborough explosion was not the result of multiple basic engineering design errors unlikely to coincide again; the errors were rather multiple instances of one underlying cause: a complete breakdown of plant safety procedures (exacerbated by a lack of relevant engineering expertise, but that lack was also a procedural shortcoming).

ICI Petrochemicals: 'A new world where new methods are needed'

The Petrochemicals Division of Imperial Chemical Industries (ICI) operated many plants with large inventories of flammable chemicals at its Wilton site (including one in which cyclohexane was oxidised to cyclohexanone and cyclohexanol). Historically good process safety performance at Wilton had been marred in the late 1960s by a spate of fatal fires caused by faulty isolations/handovers for maintenance work. Their immediate cause was human error but ICI felt that saying that most accidents were caused by human error was no more useful than saying that most falls are caused by gravity. ICI had not simply reminded operators to be more careful, but issued explicit instructions on the required quality of isolations, and the required quality of its documentation. The more onerous requirements were justified as follows:

Why do we need the HOC rules on the isolation and identification of equipment for maintenance? They were introduced about 2 years ago, but Billingham managed for 45 years without them. During those 45 years there were no doubt many occasions when fitters broke into equipment and found it had not been isolated, or broke into the wrong line because it had not been identified positively. But pipe-lines were mostly small, and the amount of flammable gas or liquid on the plant was not usually large. Now pipe-lines are much larger and the amount of gas or liquid that can leak out is much greater. Several serious incidents in the last 3 years have shown that we dare not risk breaking into lines that are not properly isolated. As plants have got larger we have moved ... into a new world where new methods are needed.

In accordance with this view, post-Flixborough (and without waiting for the Inquiry Report), ICI Petrochemicals instituted a review of how it controlled modifications. It found that major projects requiring financial sanction at a high level were generally well-controlled, but for more (financially) minor modifications there was less control and this had resulted in a past history of 'near-misses' and small-scale accidents, few of which could be blamed on chemical engineers. To remedy this, not only were employees reminded of the principal points to consider when making a modification (both on the quality/compliance of the modification itself and on the effect of the modification on the rest of the plant), but new procedures and documentation were introduced to ensure adequate scrutiny. These requirements applied not only to changes to equipment, but also to process changes. All modifications were to be supported by a formal safety assessment. For major modifications this would include an 'operability study'; for minor modifications a checklist-based safety assessment was to be used, indicating what aspects would be affected, and for each aspect giving a statement of the expected effect. The modification and its supporting safety assessment then had to be approved in writing by the plant manager and engineer. Where instruments or electrical equipment were involved signatures would also be needed from the relative specialist (instrument manager or electrical engineer). A Pipework Code of Practice was introduced specifying standards of design construction and maintenance for pipework – all pipework over 3"nb (DN 75 mm) handling hazardous material would have to be designed by pipework specialists in the design office. The approach was publicised outside ICI; while the Pipework Code of Practice on its own would have combatted the specific fault(s) that led to the Flixborough disaster, the adoption more generally of tighter controls on modifications (and the method by which this was done) were soon recognised to be prudent good practice. In the United

Kingdom, the ICI approach became a *de facto*standard for high-risk plant (partly because the new (1974) Health and Safety at Work Act went beyond specific requirements on employers to state general duties to keep risks to workers as low as reasonably practicable and to avoid risk to the public so far as reasonably practicable; under this new regime the presumption was that recognised good practice would inherently be 'reasonably practicable' and hence should be adopted, partly because key passages in reports of the Advisory Committee on Major Hazards were clearly supportive).

ADVISORY COMMITTEE ON MAJOR HAZARDS

DISSATISFACTION WITH EXISTING REGULATORY REGIME

The terms of reference of the Court of Inquiry did not include any requirement to comment on the regulatory regime under which the plant had been built and operated, but it was clear that it was not satisfactory. Construction of the plant had required planning permission approval by the local council; while "an interdepartmental procedure enabled planning authorities to call upon the advice of Her Majesty's Factory Inspectorate when considering applications for new developments which might involve a major hazard" (there was no requirement for them to do so), since the council had not recognised the hazardous nature of the plant they had not called for advice. As the *New Scientist* commented within a week of the disaster:

There are now probably more than a dozen British petrochemical plants with a similar devastation-potential to the Nypro works at Flixborough. Neither when they were first built, nor now that they are in operation, has any local or government agency exercised effective control over their safety. To build a nuclear power plant, the electricity industry must provide a detailed safety evaluation to the Nuclear Inspectorate before it receives a licence. On the other hand, permission for highly hazardous process plants only involves satisfying a technically unqualified local planning committee, which lacks even the most rudimentary powers once the plant goes on stream. ... The Factory Inspectorate has standing only where it has promulgated specific regulations

TERMS OF REFERENCE AND PERSONNEL

The ACMH's terms of reference were to identify types of (non-nuclear) installations posing a major hazard, and advise on appropriate controls on their establishment, siting, layout, design, operation, maintenance and development (including overall development in their vicinity). Unlike the Court of Inquiry, its personnel (and that of its associated working groups) had significant representation of safety professionals, drawn largely from the nuclear industry and ICI (or ex-ICI)

SUGGESTED REGULATORY FRAMEWORK

In its first report (issued as a basis for consultation and comment in March 1976), the ACMH noted that hazard could not be quantified in the abstract, and that a precise definition of 'major hazard' was therefore impossible. Instead[w] installations with an inventory of flammable fluids above a certain threshold or of toxic materials above a certain 'chlorine equivalent' threshold should be ' *notifiable installations* '. A company operating a notifiable installation should be required to survey its hazard potential, and inform HSE of the hazards identified and the procedures and methods adopted (or to be adopted) to deal with them.

HSE could then chose to – in some cases (generally involving high risk or novel technology) – require[x] submission of a more elaborate assessment, covering (as appropriate) "design, manufacture, construction, commissioning, operation and maintenance, as well as subsequent modifications whether of the design or operational procedures or both". The company would have to show that "it possesses the appropriate management system, safety philosophy, and competent people, that it has effective methods of identifying and evaluating hazards, that it has designed and operates the installation in accordance with appropriate regulations, standards and codes of practice, that it has adequate procedures for dealing with emergencies, and that it makes use of independent checks where appropriate"

For most 'notifiable installations' no further explicit controls should be needed; HSE could advise and if need be enforce improvements under the general powers given it by the 1974 Health and Safety at Work Act (HASAWA), but for a very few sites explicit licensing by HSE might be appropriate; responsibility for safety of the installation remaining however always and totally with the licensee.

Ensuring safety of 'major hazard' installations

HASAWA already required companies to have a safety policy, and a comprehensive plan to implement it. ACMH felt that for major hazard installations the plan should be formal and include

- the regulation by company procedures of safety matters (such as: identification of hazards, control of maintenance (through clearance certificates, permits to work etc.), control of modifications which might affect plant integrity, emergency operating procedures, access control)
- clear safety roles (for e.g. the design and development team, production management, safety officers)
- training for safety, measures to foster awareness of safety, and feedback of information on safety matters

Safety documents were needed both for design and operation. The management of major hazard installations must show that it possessed and used a selection of appropriate hazard recognition techniques,[S] had a proper system for audit of critical safety features, and used independent assessment where appropriate.

The ACMH also called for tight discipline in the operation of major hazard plants:

The rarity of major disasters tends to breed complacency and even a contempt for written instructions. We believe that rules relevant to safety must be everyday working rules and be seen as an essential part of day-to-day work practice. Rules, designed to protect those who drew them up if something goes wrong, are readily ignored in day-to-day work. Where management lays down safety rules, it must also ensure that they are carried out. We believe that to this end considerable formality is essential in relation to such matters as permits to work and clearance certificates to enter vessels or plant areas. In order to keep strong control in the plant, the level of authority for authorisations must be clearly defined. Similarly the level of authority for technical approval for any plant modification must also be clearly defined. To avoid the danger of systems and procedures being disregarded, there should be a requirement for a periodic form of audit of them.

The ACMH's second report (1979) rejected criticisms that since accidents causing multiple fatalities were associated with extensive and expensive plant damage the operators of major hazard sites had every incentive to avoid such accidents and so it was excessive to require major hazard sites to demonstrate their safety to a government body in such detail:

We would not contest that the best run companies achieve high standards of safety, but we believe this is because they have .... achieved what is perhaps best described as technical discipline in all that they do.

We believe that the best practices must be followed by all companies and that we have reached a state of technological development where it is not sufficient in areas of high risk for employers merely to demonstrate to themselves that all is well. They should now be required to demonstrate to the community as a whole that their plants are properly designed, well constructed and safely operated.

The approach advocated by the ACMH was largely followed in subsequent UK legislation and regulatory action, but following the release of chlordioxins by a runaway chemical reaction at Seveso in northern Italy in July 1976, 'major hazard plants' became an EU-wide issue and the UK approach became subsumed in EU-wide initiatives (the Seveso Directive in 1982, superseded by the Seveso II Directive in 1996). A third and final report was issued when the ACMH was disbanded in 1983.