SAFETY AUDIT

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.

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 organization 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 organization 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. 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

EVENT TREE ANALYSIS

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.

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 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 events 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 cannot 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.

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 branch 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

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 counter measures associated with the specific scenario.
5. **Build the event tree diagram**

6. **Obtain event failure probabilities:** If the failure probability cannot 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

6.2 **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
- 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

6.3 **Limitations**

- Addresses only one initiating event at a time.
- The initiating challenge must be identified by the analysis
- 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

Though ETA can be relatively simple, software can be used for more complex systems to build the diagram and perform calculations more quickly with reduction of human errors in the process. There are many types of software available to assist in conducting an ETA. The software available is generally not available from your local store but easily found with an online search. In nuclear industry, Risk Spectrum PSA software is widely used which has both event
tree analysis and fault tree analysis.