RISK ASSESSMENT BY USING FAILURE MODE EFFECTIVE ANALYSIS (FMEA) TOOL: AN OVERVIEW

V Vijayakumar Reddy, Gangadharappa H. V.* and Shashikanth D.

Department of Pharmaceutics, JSS College of Pharmacy, JSS University, SS nagara, Mysuru, Karnataka-570015, India.

ABSTRACT

The use of risk assessment is a growing trend within the pharmaceutical industry. One such analytical method for performing risk assessment is FMEA (Failure Mode Effective Analysis). Risk Management is a process of identifying hazards associated with a product or processes, estimating and evaluating the risks associated, controlling these risks, and monitoring the effectiveness of the control. Failure mode and effects analysis (FMEA) is a method (first developed for systems engineering) that examines potential failures in products or processes. It can be used to evaluate risk management priorities for mitigating known threat vulnerabilities. This article aims to provide detailed study of the risk assessment by using FMEA tool. By this tool severity (S), Probability/Occurrence (P), Detectability (D) numbering for each failure mode was given, RPN can calculate and accordingly the risk level can be classified (Low, Medium, High level). High and medium level risks having potential impact on product quality. Low risks are not likely to affect the overall process very much.

KEYWORDS: Risk assessment, FMEA.

INTRODUCTION

The use of risk assessment in the pharmaceutical industry is becoming not only an increasingly used tool but also an expectation of regulatory authorities. Risk assessment consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards. Risk assessment is an analytic techniques that are used in different situations, depending upon the characteristic of the hazard, the available data, and...
requirements of decision makers. Risk assessments begin with a well-defined problem description or risk question. When the risk in question is well defined, a suitable risk management tool and the types of information needed to address the risk question will be more readily identifiable. Different risk management tools available for risk assessment include Basic risk management facilitation methods (flowcharts, check sheets, etc.), Failure Mode Effects Analysis (FMEA), Failure Mode, Effects and Criticality Analysis (FMECA), Failure Tree Analysis (FTA), Hazard Analysis and Critical Control Points (HACCP), Hazard Operability Analysis (HAZOP), Preliminary Hazard Analysis (PHA), Risk ranking and filtering, Supporting statistical tools. Failure mode and effects analysis (FMEA) is a commonly used method that examines potential failures in products or processes. It can be used to evaluate risk management priorities for mitigating known threat-vulnerabilities.

**Risk Assessment**[1]

Risk assessment can be defined as "A systematic process of organizing information to support a risk decision to be made within a risk management process. It contains the identification of hazards and analysis and evaluation of risks associated with exposure to those hazards". Parts of the risk assessment include risk identification, risk analysis and risk evaluation.

Three basic questions that supportive while evaluating the risk associated with the procedure are.

1. What might go wrong?
2. What is the possibility that it will go wrong?
3. What are the consequences?

**Risk identification** is an organized use of information to identify hazards referring to the risk. Information can include data available, theoretical analysis, and the opinions of stakeholders. Risk identification involves in identifying the possible consequences.

**Risk analysis** is the estimation of the risk associated with the identified hazards. It is either qualitative or quantitative process of linking the probability of occurrence and severity of harms. In some risk management tools including FMEA, the ability to detect the harm (detectability) also factors in the estimation of risk.
**Risk evaluation** compares the identified and analyzed risk against given risk criteria. The strength of evidence for all fundamental questions is considered in risk evaluation.

To complete risk assessment successfully, the robustness of the data set is important because it determines the output quality. Revealing predictions and reasonable sources of uncertainty will help to identify its limitations. Uncertainty is due to a combination of poor knowledge about a process and its expected or unexpected variability. Typical examples for sources of uncertainty include gaps in knowledge gaps in pharmaceutical science and process understanding, sources of harm (e.g., failure modes of a process, sources of variability), and likelihood of detection of problems.

The output of a risk assessment is either a quantitative or a qualitative. When risk is expressed quantitatively, a statistical probability is used. Alternatively, risk can also be expressed using qualitative descriptors, such as “high”, “medium”, or “low”, which should be defined in as much detail as possible. Sometimes a "risk score" is used to further define descriptors in risk ranking. If risk assessment is expressed quantitatively, a risk estimate provides the probability of a specific consequence, given a set of risk-generating situations. Thus, quantitative estimation of risk is useful for one particular consequence at a time. On the other hand, some risk management tools use a relative risk measure to combine multiple levels of severity and probability into an overall estimate of relative risk. The intermediate steps within a scoring process can sometimes employ quantitative risk estimation.

**Failure mode effect analysis (FMEA)** \(^{[2, 3]}\)

Failure mode effect analysis (FMEA) “A systematic process for identifying potential failures in a process or design before they occur, with the intent to eliminate them or minimize the risk associated with them”.

**Objectives**

To identify potential failures in design and process failures before they occur and to minimize the risk of failure by either proposing changes in design or, if these cannot be formulated, proposing changes in operational procedures. Basically the FMEA is to:

- To identify potential failures and consequences in a process or design
- To evaluate the effects on the process of each failure mode individually
- Identify measures for eliminating or mitigating the risks associated with each failure mode identified
To Identify trials and testing necessary to prove the conclusions and
Provide information to the operators so that they understand the capabilities and limitations of the system to achieve best performance.

Description [4]
A Failure Mode Effects Analysis (FMEA) is a method used in product development and operations management for analysis of potential failures within a system for classification by the severity and probability of the failures. A successfully developed FMEA activity helps to identify potential failure modes, based on historical data with similar products or processes. Failure modes are any defects in a process, design, or item, in particular those that affect the quality of the drug product, and can be potential or actual. Effects analysis in FMEA refers to studying the consequences of those potential failures.

Types of FMEA [2]
Normally two types of FMEA’s are used in pharmaceutical industries
i. The Design FMEA (DFMEA) and
ii. The Process FMEA (PFMEA).

The Design FMEA (DFMEA)
The design FMEA is used to analyze products before they are released to production and it focuses on potential failure modes of products, caused by design deficiencies. Design FMEA’s are normally done at three levels – system, sub-system, and component levels.

The Process FMEA (PFMEA)
The process FMEA is normally used to analyze manufacturing and assembly processes at the system, sub-system or component levels. PFMEA focuses on potential failure modes of the process that are caused by manufacturing or assembly process deficiencies. To start, it is necessary to describe the system and its function. Before starting the actual FMEA, a worksheet needs to be prepared, which contains the important information about the system. On this worksheet all the functions of the subject should be listed in a logical manner.

When is an FMEA carried out?
The FMEA should start at the earliest stage that the design and development Program will allow, even to assist at a higher level in identifying potential weaknesses during the conceptual design.
How is the FMEA Process Progressed? \[^{[5]}\]

**Step One: Select a process to assess with FMEA**
Evaluation using FMEA works best on processes that do not have too many sub processes.

**Step Two: Select a multidisciplinary team**
Be sure to include everyone who is involved at any point in the process. Some people may not need to be part of the team throughout the entire analysis, but they should certainly be included in discussions of those steps in the process in which they are involved.

**Step Three: List all the steps in the process**
Assign numbers to each and every step of the process, and be as specific as possible. Depending on the number of steps and the complexity of the process, it may take several meetings for the team to complete this part of the FMEA. Flowcharting can be used for outlining the steps. When you are finished, be sure to obtain consensus from the group. The team should agree that the steps enumerated in the FMEA accurately describe the process.

**Step Four: List failure modes and causes**
For each step in the process, list all possible “failure modes” including minor and rare problems. Then, then identify the possible causes for each failure listed.

**Step Five**
For each failure mode, have the team assign a numeric value (known as the Risk Priority Number, or RPN) for probability of occurrence, detection, and severity. Assigning RPNs helps the team prioritize areas to focus on and can also help in assessing opportunities for improvement. For every failure mode recognized, the team should answer probability of occurrence, detection and severity.

- **Probability of occurrence**: How likely is it that this failure mode will occur? Assign a score between 1 and 4, with 1 meaning “very unlikely to occur” and 4 meaning “very likely to occur.”

- **Probability of detection**: If a failure mode occurs, how likely is it that the failure will be detected? Assign a score between 1 and 4, with 1 meaning “very likely to be detected” and 4 meaning “very unlikely to be detected.”
• **Severity:** If a failure mode occurs, how likely is it that harm will occur? allocate a score between 1 and 4, with 1 meaning “very unlikely that harm will occur” and 4 meaning “very likely that severe harm will occur.”

**Step Six: Evaluate the results**
To calculate the RPN for each failure mode, multiply the three scores (probability of occurrence, detection, and severity) obtained.

**Step Seven: Use Risk priority number to plan improvement efforts**
Failure modes with high RPNs are the most important parts of the process on which one should focus improvement efforts. Failure modes with low RPNs are not likely to affect the overall process, even if eliminated completely.

**Table No. 01: Failure Mode Effective Analysis** [2]

<table>
<thead>
<tr>
<th>Process step/ input</th>
<th>Potential Failure Mode</th>
<th>Potential Cause(s) of Failure</th>
<th>Potential Effect(s) of Failure</th>
<th>S</th>
<th>O</th>
<th>D</th>
<th>RPN= S<em>O</em>D</th>
<th>Actions Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Generalized FMEA was given in the table 1 above which includes severity (S), occurrence / occurrence (O), Detectability (D) rating (1-4 scale) and RPN calculation by multiplying Severity (S), Occurrence (O), Detectability (D). Recommended actions proposed to reduce the undesired event occurred. The table 2, table 3 and table 4 describes the values of severity, occurrence and Detectability for failure/ undesired event occurred.

The table 2, table 3 and table 4 describes the values of severity, occurrence and detectability for failure/ undesired event occurred. [6,7]

**Table No. 02: Severity (Consequences of failure)**

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description with example</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extreme</td>
<td>Predicted to cause severe impact to quality (Product OOS, no 4 expert statement possible)</td>
<td>4</td>
</tr>
<tr>
<td>High</td>
<td>Predicted to cause significant impact on quality (Failure to meet 3 specifications, no stability data, Expert Statement possible)</td>
<td>3</td>
</tr>
<tr>
<td>Moderate</td>
<td>Predicted to cause minor impact on quality (Failure to meet 2 specifications, stability data available)</td>
<td>2</td>
</tr>
<tr>
<td>Low</td>
<td>Predicted to have no/minor impact on quality of the product</td>
<td>1</td>
</tr>
</tbody>
</table>
Table No. 03: Probability/occurrence (Likelihood failure happen)

<table>
<thead>
<tr>
<th>Likelihood failure happen</th>
<th>Description</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular Failures</td>
<td>Expected to happen regularly</td>
<td>4</td>
</tr>
<tr>
<td>Repeated Failures</td>
<td>Expected to happen in a low frequency</td>
<td>3</td>
</tr>
<tr>
<td>Occasional Failures</td>
<td>Expected to happen infrequently</td>
<td>2</td>
</tr>
<tr>
<td>Unlikely Failures</td>
<td>Unlikely to happen</td>
<td>1</td>
</tr>
</tbody>
</table>

Table No. 04: Detectability (Ability to find the failure)

<table>
<thead>
<tr>
<th>Detectability</th>
<th>Description</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normally not detected</td>
<td>Failure very likely to be overlooked (no technical solution, no manual control)</td>
<td>4</td>
</tr>
<tr>
<td>Likely not detected</td>
<td>Failure may be overseen (Manual control, spot checks)</td>
<td>3</td>
</tr>
<tr>
<td>Regularly detected</td>
<td>Failure will normally be detected (manual control, routine work with statistical control)</td>
<td>2</td>
</tr>
<tr>
<td>Always detected</td>
<td>Failure can and will be detected in all cases (monitoring, technical solution available)</td>
<td>1</td>
</tr>
</tbody>
</table>

Table No. 5: Overall risk (RPN)

<table>
<thead>
<tr>
<th>Calculated RPN</th>
<th>Risk</th>
<th>Action required</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥ 16</td>
<td>High</td>
<td>Unacceptable, Significant change required to reduce severity</td>
</tr>
<tr>
<td>6-15</td>
<td>Medium</td>
<td>Risk mitigation required</td>
</tr>
<tr>
<td>1-5</td>
<td>Low</td>
<td>Acceptable risk, no action required</td>
</tr>
</tbody>
</table>

CONCLUSION

An RPN number can be calculated by multiplying the probability of occurrence, probability of detection and severity and the categorization of risk can be done as follows shown in the table no. 5. Risk level can be classified (Low, Medium, High level) based on obtained RPN value. High and medium level risks having potential impact on product quality. low risks are not likely to affect the overall process very much.

REFERENCES


