Strategies and Predictive Maintenance models wrapped around physical systems for Zero-unexpected-Breakdowns and increased operating life of Factories

Z-BRE4K

Deliverable D3.3
KRI models and tools for FMECA and criticality analysis

Work Package 3
WP3 – Knowledge and Predictive Modelling

Document type: Report
Version: V0.2
Date of issue: 26/03/2019
Dissemination level: PUBLIC
Lead beneficiary: ATLANTIS ENGINEERING SA

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement nº 768869.

The dissemination of results herein reflects only the author’s view and the European Commission is not responsible for any use that may be made of the information it contains.
Executive Summary

| Abstract | From description of Work Package 3, specifically task T3.3, this deliverable D3.3 was following one of the objectives of WP3, incorporating risk analysis, KRIs and FMECA within the predictive maintenance solution of Z-BRE4K system. Particularly, the detailed research on fundamental definitions and FMEA types have been provided within section 3, while section 4 presents various FMECA standards, its characteristic and methodology. Furthermore, section 5 (Criticality Analysis Tool) and section 6 (Key Risk Indicators), identified failures and potential risks respectfully. Finally, open source examples summarized in section 7, that presents the Process Failure Mode and Effect Analysis in production process from ceramics and knitting industries, are completed with the conclusion and next steps to be further followed. |
| Keywords | Failure mode and effects analysis, Failure mode, effects and criticality analysis, Key Risk Indicators, Criticality Analysis Tools, |
### Revision history

<table>
<thead>
<tr>
<th>Version</th>
<th>Author(s)</th>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.0</td>
<td>ATLANTIS</td>
<td>ToC</td>
<td>11/02/2019</td>
</tr>
<tr>
<td>v0.1</td>
<td>ATLANTIS</td>
<td>Section 1, 2, 4</td>
<td>18/02/2019</td>
</tr>
<tr>
<td>v0.2</td>
<td>AIMEN</td>
<td>Section 3, 5, 6</td>
<td>08/03/2019</td>
</tr>
<tr>
<td>v0.3</td>
<td>ATLANTIS</td>
<td>Sub-Section 5.1&amp;6.1, Abbreviation, Summary, Conclusion, Reference, List of Figures/Tables</td>
<td>12/03/2019</td>
</tr>
<tr>
<td>V0.4</td>
<td>AIMEN/BRUNEL</td>
<td>Peer Review</td>
<td>25/03/2019</td>
</tr>
<tr>
<td>V0.5</td>
<td>ATLANTIS</td>
<td>Final Deliverable Version</td>
<td>26/03/2019</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

- **LIST OF FIGURES** ........................................................................................................... 6
- **LIST OF TABLES** ............................................................................................................ 6
- **ABBREVIATIONS** ........................................................................................................... 7
- **SUMMARY** ...................................................................................................................... 8

1. **INTRODUCTION** .......................................................................................................... 9
2. **OBJECTIVES AND SCOPE** ........................................................................................ 9
3. **FMEA** .......................................................................................................................... 10
   - 3.1 Understanding the fundamental definitions and conceptions of FMEA .......... 10
   - 3.2 Types of FMEA ........................................................................................................ 11
   - 3.3 How to perform and FMEA project ........................................................................ 11

4. **FMECA** ....................................................................................................................... 14
   - 4.1 Definition ................................................................................................................ 14
   - 4.2 History and FMECA standards .............................................................................. 14
      - 4.2.1 IEC 60812 ......................................................................................................... 15
      - 4.2.2 MIL-STD-1629A ............................................................................................. 15
      - 4.2.3 ISAE J-1739 .................................................................................................... 16
   - 4.3 Benefits .................................................................................................................. 16
   - 4.4 Characteristics ......................................................................................................... 16
   - 4.5 Redundancy ........................................................................................................... 17
   - 4.6 Failure causes modes and effects ........................................................................ 17
   - 4.7 Failure modes ........................................................................................................ 18
   - 4.8 Methodology ........................................................................................................... 19
   - 4.9 Quantitative and Qualitative FMECA .................................................................. 19

5. **CRITICALITY ANALYSIS TOOLS** ........................................................................... 21
   - 5.1 Cascaded failures .................................................................................................... 22
   - 5.2 Event Tree Analysis (ETA) ..................................................................................... 23
5.3 Fault Tree Analysis (FTA) ................................................................. 24

6 KEY RISK INDICATORS (KRI) ............................................................. 27

6.1 Identifying potential risks ................................................................ 28

6.2 Facing the risk ................................................................................. 30

6.3 Developing Effective Key Risk Indicators ....................................... 31

7 Z-BRE4K EXAMPLE ............................................................................. 33

8 CONCLUSION ...................................................................................... 38

9 REFERENCES ....................................................................................... 39
LIST OF FIGURES

Figure 1: The FMEA level hierarchy (adapted from IEC 60812) .................................................. 10
Figure 2: Deployment of different types of FMECA in the production stages ......................... 11
Figure 3: Sample Process FMEA in the Automotive Industry Action Group (AIGA) FMEA-4 ... 12
Figure 4: Example of risk calculation by FMEA. ................................................................. 13
Figure 5: Relation among failure causes, modes and effects ................................................... 18
Figure 6: Relation among failure causes, modes and effects ................................................... 21
Figure 7: Example of three stage system failure sequence ...................................................... 23
Figure 8: Event Tree. .............................................................................................................. 24
Figure 9: Differences among fault tree and event tree analysis ............................................. 25
Figure 10: Fire secure system example (fault tree analysis) .................................................... 26
Figure 11: Financial pricing model (event tree analysis) ........................................................ 26
Figure 12: KRI development .................................................................................................. 28
Figure 13: Key objectives linked with potential critical risks ................................................... 29
Figure 14: Asset type/failure mode and failure cause window ............................................ 33
Figure 15: Failure effect window ........................................................................................... 34
Figure 16: Process Failure Mode & Effect Analysis in production process of Ceramic tiles ...... 36
Figure 17: Process Failure Mode & Effect Analysis in production process of Knitting industry 37

LIST OF TABLES

Table 1: KRI thresholds ........................................................................................................ 30
Table 2: Table of Severity .................................................................................................... 34
Table 3: Table of Detectability ............................................................................................. 35
# ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMECA</td>
<td>Failure mode, effects and criticality analysis</td>
</tr>
<tr>
<td>FMEA</td>
<td>Failure mode and effects analysis</td>
</tr>
<tr>
<td>KRI</td>
<td>Key Risk Indicator</td>
</tr>
<tr>
<td>RPN</td>
<td>Risk Priority Number</td>
</tr>
<tr>
<td>FM</td>
<td>Failure Mode</td>
</tr>
<tr>
<td>IATF</td>
<td>International Automotive Task Force</td>
</tr>
<tr>
<td>WP</td>
<td>Wok Package</td>
</tr>
<tr>
<td>CA</td>
<td>Criticality Analysis</td>
</tr>
<tr>
<td>NASA</td>
<td>National Aeronautics and Space Administration</td>
</tr>
<tr>
<td>RCM</td>
<td>Reliability-Centred Maintenance</td>
</tr>
<tr>
<td>FTA</td>
<td>Fault Tree Analysis</td>
</tr>
</tbody>
</table>
**SUMMARY**

The FMECA, KRI models and criticality analysis task T3.3, deals with failure modes, respective causes and immediate/final effects providing an automated FME(C)A process with the goal to replace the manual FMECA process. It will analyse Key Risk Indicator (KRI) number in each of the project Z-BRE4Ks pilot cases, applying specific KRI model and applicable risk assessment approach. Each risk will be categorized by a Risk Prioritization Number (RPN) having metrics for both the probability and the severity of each risk, allowing mitigation and contingency actions to lower the probability and the severity, respectively. Basically, FMECA, the automated module of Z-BRE4K, will show ways a machinery system could potentially fail (i.e. Failure Modes (FM)s, respective causes and immediate and final effects) while using both logic diagrams and fault trees for these analyses in the systems background. The approach will determine the indenture level in the machinery system, broken down by subsystems, replaceable units, individual parts, etc., where failure effects identified at the lower level may become FMs at higher level, and the FMs at the lower level may become failure causes at higher level, etc. The IEC60812 standard will be followed while the based classification will consider effects with local or machinery system level scope.
1 INTRODUCTION

Failure Mode and Effect Analysis (FMEA) techniques are used for more than 40 years in the industry business. It was mainly developed by the U.S. automotive industry with its QS-9000 supplier requirements that were established in 1996, with the additional global efforts by the International Automotive Task Force (IATF) to build on QS-9000 (and other international quality standards) with the development of ISO/TS 16949. In 2002 there was a revision of ISO/TS 16949 that incorporates ISO 9001:2000 and defines the quality system requirements (and application of ISO 9001) for automotive production and relevant service part organizations. Because FMEAs are team based, several people need to be involved in the process. Effective FMEAs cannot be done by one person alone filling out the FMEA forms.

In 1974, development of FMECA is sometimes incorrectly attributed to NASA. At the same time as the space program developments, use of FMEA and FMECA was already spreading to civil aviation. In 1967 the Society for Automotive Engineers released the first civil publication to address FMECA. The civil aviation industry now tends to use a combination of FMEA and Fault Tree Analysis in accordance with SAE ARP4761 instead of FMECA, though some helicopter manufacturers continue to use FMECA for civil rotorcraft.

Ford Motor Company\(^1\) began using FMEA in the 1970s after problems experienced with its Pinto model, and by the 1980s FMEA was gaining broad use in the automotive industry. In Europe, the International Electrotechnical Commission published IEC 812 (now IEC 60812) in 1985, addressing both FMEA and FMECA for general use. The British Standards Institute published BS 5760–5 in 1991 for the same purpose.

2 OBJECTIVES AND SCOPE

One of the objectives of WP3 and KNOWLEDGE AND PREDICTIVE MODELLING, is the incorporation of risk analysis, KRIs and FMECA within the predictive maintenance solution of Z-BRE4K system. It is combined with integrated quality-maintenance methods and tools of the system, that effectively share information among different data sources in a secure way. Apart from its prediction and detection capabilities, Z-BRE4K will also provide a better understanding of the failures through its FMECA subsystem based on the trends, standards and patterns with focus on support for decision making in Z-Strategies. Due the evolution of Industry 4.0 and demand of the industry to evaluate risks of machinery, Z-BRE4K will be a pioneer in this area, advancing the SoA by elaborating KRIs and Risk Assessment approaches in the maintenance field of industrial manufacturing. We’ll also capitalize the FMECA/KRIs work in relation to asset, context ontology and related reasoning developed within the WP3, in order to establish the link among FMs, Risks effects and their criticality as well as the predictive analytics modelling and cognitive computing (WP2).

---

3 FMEA

The purpose of FMEA is to study the results or effects of item failure on system operation and to classify each potential failure according to its severity. Potential failure mode is defined as the manner in which the process could potentially fail to meet the process requirements and/or design intent. Potential failure modes should be described in physical or technical terms, not as a symptom noticeable by the customer. Typical failure modes could be: Bent, Cracked, surface too rough, deformed, hole too deep, hole off location etc. The FMEA is a bottom-up method, where the system under analysis is first hierarchically divided into components (Figure 1). The division shall be done in such a way that the failure modes of the components at the bottom level can be identified. The failure effects of the lower level components constitute the failure modes of the upper level components.

![FMEA level hierarchy](image)

*Figure 1: The FMEA level hierarchy (adapted from IEC 60812)*

3.1 Understanding the fundamental definitions and conceptions of FMEA

Failure Modes and Effects Analysis (FMEA) is designed to identify potential failure modes for a product or process before the problem occur, to rank the issues in terms of importance and to identify and carry out corrective actions to address the most serious concerns. Ideally, FMEA’s are conducted in the product design or process development stages, although conducting an FMEA on existing products or processes may also yield benefits.

---

The FMEA team determines, by failure mode analysis, the effect of each failure and identifies single failure points that are crucial. It may also rank each failure according to the criticality of a failure effect and its probability of occurring.

### 3.2 Types of FMEA

According to the standard AIAG FMEA-4 and presented at Figure 2, there is several types of FMEA such as System FMEA, Design FMEA, Process FMEA, Machinery FMEA but the main are:

- **Design FMEA**: This is used to analyse products before they are released to manufacturing. A design focuses on failure modes caused by design deficiencies.
- **Process FMEA**: It can be used to analyse manufacturing and assembly processes. A process FMEA focuses on failure modes caused by process or assembly deficiencies.

![Figure 2: Deployment of different types of FMECA in the production stages.](image)

### 3.3 How to perform and FMEA project

In general, FMEA / FMECA requires the identification of the following basic information:

- Item(s).
- Function(s).
- Failure(s).

---


Effect(s) of Failure.
Cause(s) of Failure.
Current Control(s).
Recommended Action(s).
Other relevant details.

In order to report and collect all the information, the standards provide templates to specify the potential risk. Figure 3 shows an example of a FMEA procedure to meet the specific requirements of product/process.

Figure 3: Sample Process FMEA in the Automotive Industry Action Group (AIGA) FMEA-4.

Most analyses of this type also include some method to assess the risk associated with the issues identified during the analysis and to prioritize corrective actions. Two common methods include:

- **Risk Priority Numbers (RPNs)** and
- **Criticality Analysis (FMEA with Criticality Analysis = FMECA).**

For calculating the risk in FMEA method, risk has three components which are multiplied to produce a risk priority number (RPN):

- To use the Risk Priority Number (RPN)⁵ method to assess risk, the analysis team must:
  - Rate the severity of each effect of failure.
  - Rate the likelihood of occurrence for each cause of failure.
  - Rate the likelihood of prior detection for each cause of failure (i.e. the likelihood of detecting the problem before it reaches the end user or customer).

---

Calculate the RPN by obtaining the product of the three ratings:

\[ \text{RPN} = \text{Severity} \times \text{Occurrence} \times \text{Detection} \]

The RPN can then be used to compare issues within the analysis and to prioritize problems for corrective action. An example of risk calculation is explained with a practical scenario within the Figure 4.

<table>
<thead>
<tr>
<th>Potential failure</th>
<th>Severity (S)</th>
<th>Occurrence (O)</th>
<th>Detection (D)</th>
<th>RPN=S\times O\times D</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>10</td>
<td>5</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>2</td>
<td>5</td>
<td>100</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>100</td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td>5</td>
<td>2</td>
<td>100</td>
</tr>
</tbody>
</table>

*Figure 4: Example of risk calculation by FMEA.*

The first priority will be the potential failure 2 and 4 as we have highest severity ranking there. The potential failures 1 and 3 have same severity ranking 2. But 1 has occurrence 10 higher than 3. So, it should be prioritized next providing the results as:

- First priority............ Potential failure 4.
- Second priority......... Potential failure 2.
- Fourth priority......... Potential failure 3.
4 FMECA

It is familiar that industries are using FMECA reports that consists of system description, ground rules and assumptions, conclusions and recommendations, corrective actions to be followed, and the attached FMECA matrix which may be in spreadsheet, worksheet or database form. Also, according to Federal Aviation Administration (FAA) research report for commercial space transportation, it was reported “Failure Modes, effects, and Criticality Analysis is an excellent hazard analysis and risk assessment tool, but it suffers from other limitations. This alternative does not consider combined failures or typically include software and human interaction considerations. It also usually provides an optimistic estimate of reliability. Therefore, FMECA should be used in conjunction with other analytical tools when developing reliability estimates”⁶. Within the Z-BRE4K, the automated module, FMECA, will be developed to provide information and ways a machinery system could potentially fail defining FMs, respective causes and immediate and final effects.

4.1 Definition

The FMECA is composed of two separate analyses, the Failure Mode and Effects Analysis (FMEA) and the Criticality Analysis (CA). The FMEA analyses different failure modes and their effects on the system while the CA classifies or prioritizes their level of importance based on failure rate and severity of the effect of failure. The ranking process of the CA can be accomplished by utilizing existing failure data or by a subjective ranking procedure conducted by a team of people with an understanding of the system.

Although the analysis can be applied to any type of system, this manual will focus on applying the analysis to a C4ISR facility. The FMECA should be initiated as soon as preliminary design information is available. The FMECA is a living document that is not only beneficial when used during the design phase but also during system use. As more information on the system is available the analysis should be updated in order to provide the most benefit.

4.2 History and FMECA standards

The FMECA was originally developed by the National Aeronautics and Space Administration (NASA) to improve and verify the reliability of space program hardware. The cancelled MIL-STD-785B, entitled Reliability Program for System and Equipment Development and Production, Task 204, Failure Mode, Effects and Criticality Analysis calls out the procedures for performing a FMECA on equipment or systems. The cancelled MIL-STD-1629A is the military standard that establishes requirements and procedures for performing a FMECA, to evaluate and document, by failure mode analysis, the potential impact of each functional or hardware failure on mission success, personnel and system safety, maintainability and system performance⁷.

---

Each potential failure is ranked by the severity of its effect so that corrective actions may be taken to eliminate or control design risk. High risk items are those items whose failure would jeopardize the mission or endanger personnel. The techniques presented in this standard may be applied to any electrical or mechanical equipment or system. Although MIL-STD-1629A has been cancelled, its concepts should be applied during the development phases of all critical systems and equipment whether it is military, commercial or industrial systems/products. Short overview of the used standard is presented in the sub-sections below.

4.2.1 IEC 60812

IEC 60812 published by the International Electrotechnical Commission describes a failure mode and effects analysis, and a failure mode, effects and criticality analysis. The standard gives guidance how the objectives of the analysis can be achieved when using FMEA or FMECA as risk analysis tools. The following information is included in the standard:

- procedural steps necessary to perform an analysis,
- identification of appropriate terms, assumptions, criticality measures, failure modes,
- determining basic principles,
- form for documenting FMEA/FMECA and
- criticality grid to evaluate failure effects.

4.2.2 MIL-STD-1629A

MIL-STD-1629A is dated on November 24th, 1980, and has been published by the United States Department of Defence. The standard establishes requirements and procedures for performing a failure mode, effects, and criticality analysis. In the standard FMECA is presented to systematically evaluate and document the potential impacts of each functional or hardware failure on mission success, personnel and system safety, system performance, maintainability and maintenance requirements. Each potential failure is ranked by the severity of its effect in order that appropriate corrective actions may be taken to eliminate or control the risks of potential failures. The document details the functional block diagram modelling method, defines severity classification and criticality numbers. The following sample formats are provided by the standard:

- failure mode and effects analysis criticality analysis,
- FMECA- maintainability information,
- damage mode and effects analysis,
- failure mode, effects, and criticality analysis plan MIL-STD-1629A was cancelled by the action of the standard authority on August 4th, 1998. Users were referred to use various national and international documents for information regarding failure mode, effects, and criticality analysis.
4.2.3 ISAE J-1739

The document provides guidance on the application of the failure mode and effects analysis technique. The focus is on performing the product, process and plant machinery FMEA. The standard outlines the product and process concepts for performing FMEA on plant machinery and equipment, and provides the format for documenting the study. The following information is included in the document:

- FMEA implementation,
- what is an FMEA?
- format for documenting product/process FMEA on machinery,
- development of a product/process FMEA,
- suggested evaluation criteria for severity, detection and occurrence of failure.

4.3 Benefits

The FMECA will highlight single point failures requiring corrective action; aid in developing test methods and troubleshooting techniques; provide a foundation for qualitative reliability, maintainability, safety and logistics analyses; provide estimates of system critical failure rates; provide a quantitative ranking of system and/or subsystem failure modes relative to mission importance; and identify parts & systems most likely to fail.

Therefore, by developing a FMECA during the design phase of a facility, the overall costs will be minimized by identifying single point failures and other areas of concern prior to construction, or manufacturing. The FMECA will also provide a baseline or a tool for troubleshooting to be used for identifying corrective actions for a given failure. This information can then be used to perform various other analyses such as a Fault Tree Analysis or a Reliability-Centered Maintenance (RCM) analysis.

The Fault Tree Analysis is a tool used for identifying multiple point failures; more than one condition to take place in order for a particular failure to occur. This analysis is typically conducted on areas that would cripple the mission or cause a serious injury to personnel.

The RCM analysis is a process that is used to identify maintenance actions that will reduce the probability of failure at the least amount of cost. This includes utilizing monitoring equipment for predicting failure and for some equipment, allowing it to run to failure. This process relies on up to date operating performance data compiled from a computerized maintenance system. This data is then plugged into a FMECA to rank and identify the failure modes of concern.

4.4 Characteristics

The FMECA should be scheduled and completed concurrently as an integral part of the design process. Ideally this analysis should begin early in the conceptual phase of a design, when the design criteria, mission requirements and performance parameters are being developed. To be effective, the final design should reflect and incorporate the analysis results and
recommendations. However, it is not uncommon to initiate a FMECA after the system is built in order to assess existing risks using this systematic approach.

Since the FMECA is used to support maintainability, safety and logistics analyses, it is important to coordinate the analysis to prevent duplication of effort within the same program. The FMECA is an iterative process. As the design becomes mature, the FMECA must reflect the additional detail. When changes are made to the design, the FMECA must be performed on the redesigned sections. This ensures that the potential failure modes of the revised components will be addressed. The FMECA then becomes an important continuous improvement tool for making program decisions regarding trade-offs affecting design integrity.

4.5 Redundancy

Redundancy means, that there is more than one means for performing a required function. The FMEA considers possible sources when analysing a system that uses redundancy to maintain function to mitigate consequences in the event of failure. The objective of redundancy, is to describe at a high level the distribution of systems and components into redundant groups. High level dependencies and intersections between these groups must be described.

The intended normal operation and operation after relevant single failures (normally one failure at the time) shall also be specified. When redundancy is employed to reduce system vulnerability and increase uptime, failure rates need to be adjusted prior to using the preceding formula. This can be accomplished by using formulas from various locations depending on the application.

Redundancy will be used as binary value. If a redundant system/sub-system/component exists, the redundancy value will be 1 or else, it will be 0.

4.6 Failure causes modes and effects

Failure modes are a key ingredient to FMEA, so it is important to have a good understanding of just what they are and how they are normally derived. The diagram at Figure 5 is visualizing the relationship between a failure mode and its causes and effects.

1. The failure mode happens in the present and it describes the way in which the failure is observed.
2. It is due to the failure cause
3. and it may result in the failure effect.
4.7 Failure modes

When a proper way of decomposing the system under analysis is found the next step is to define the failure modes of the components. For the hardware components this in general is straightforward and can be based on operational experience of the same and similar components. Component manufacturers often give failure modes and frequencies for their products. For the software components such information does not exists and failure modes are unknown (if a failure mode would be known, it would be corrected). Therefore, the definition of failure modes is one of the hardest parts of the FMEA of a software-based system. The analysts have to apply their own knowledge about the software and postulate the relevant failure modes. Reifer (1979)\(^8\) gives the following general list of failure modes based on the analysis of three large software projects:

- Computational.
- Logic.
- Data I/O.
- Data Handling.
- Interface.
- Data Definition.
- Data Base.
- Other.

Ristord et. al. (2001)\(^9\) give the following list of five general purpose failure modes at processing unit level:

- the operating system stops,


the program stops with a clear message,
- the program stops without clear message,
- the program runs, producing obviously wrong results,
- the program runs, producing apparently correct but in fact wrong results.

For each production machine, an **indenture level** (submachines, replaceable units, individual parts, etc.) is defined. To this end, **failure effects** identified at the lower level may become FMs at higher level, and the FMs at the lower level may become failure causes at higher level, etc. Our high-level **FMs classification** distinguishes the following main categories:
- failure during operation,
- failure to operate at prescribed time,
- failure to cease operation at prescribed time,
- premature operation,
- failure due to lower level component.

### 4.8 Methodology

The FMECA is composed of two separate analyses, the FMEA and the Criticality Analysis (CA). The FMEA must be completed prior to performing the CA. It will provide the added benefit of showing the analysts a quantitative ranking of system and/or subsystem failure modes. The Criticality Analysis allows the analysts to identify reliability and severity related concerns with particular components or systems.

### 4.9 Quantitative and Qualitative FMECA

There are two primary types of FMECA. Quantitative and Qualitative FMECA. Both of them, use a defined criticality analysis. They are similar in procedure, with the exception that the Quantitative FMECA uses a Quantitative Criticality Analysis and the Qualitative FMECA uses a Qualitative Criticality Analysis.

One is the “hardware approach”, which lists individual hardware items and analyses their possible failure modes. According to MIL - STD 1629A, the hardware approach is normally utilized in a part level up (bottom - up) approach. The other is the “functional approach,” which recognizes that every item is designed to perform a number of functions that can be classified as outputs.

All FMEAs require identifying and understanding the functions of each item being analysed, regardless of whether the item is a system, subsystem, component, or part. In addition, great care must be taken to address all interfaces between parts, components, subsystems, and users, which usually account for more than half of the potential failure modes.

The first step is to calculate the expected failures for each Item. This is the number of failures estimated to occur based on the reliability/unreliability of the item at a given time. Reliability is
the probability that an item will perform a required function without failure under stated conditions for a stated period of time. Unreliability is one minus reliability.

The “time” for the calculation is most often the target or useful life of the item. With an exponential distribution, expected failures is calculated by multiplying the failure rate by the time (\(\lambda t\)), but it is estimated differently for other distributions. Care must be taken to ensure calculations for reliability/unreliability and expected failures are based on correct failure distributions.

The second step is to identify the Mode Ratio of Unreliability for Each Potential Failure Mode. This is the portion of the item’s unreliability (in terms of expected failures) attributable to each potential failure mode. In other words, this represents the percentage of all failures for the item that will be due to the failure mode under consideration.

The total percentage assigned to all modes must be equal to 100%. The failure mode ratio of unreliability can be based on reliability growth testing data for the current design, field data and/or test data from a similar design, engineering judgment, or apportionment libraries such as MIL – HDBK – 338B.

The third step is to rate the probability of Loss that will result from each failure mode that will occur. This is the probability that a failure of the item under analysis will cause a system failure. The fourth and fifth steps are to calculate the criticality mode for each potential failure mode and to calculate the item criticality for each item.

Qualitative Criticality Analysis does not involve the same rigorous calculations as Quantitative Criticality Analysis. To use Qualitative Criticality Analysis to evaluate risk and prioritize corrective actions:

The first step is to rate the severity of the potential effects of failure. The severity ranking is determined using the unique severity scale for FMECA. The second step is to rate the likelihood of occurrence for each potential failure mode. The occurrence ranking is determined using the unique occurrence scale for FMECA. Compare failure modes using a criticality matrix. The criticality matrix identifies severity on the horizontal axis and occurrence on the vertical axis.
5 CRITICALITY ANALYSIS TOOLS

FMEA\(^{10}\) identifies failure modes of a product or process and their effects, while Critical Analysis ranks those failure modes in order of importance, according to failure rate and severity of failure. CA does not add information to FMEA, however in fact, it is limiting the scope of FMECA to the failure modes identified by FMEA as requiring reliability centred maintenance (RCM).

A typical failure modes and effects analysis incorporates some method to evaluate the risk associated with the potential problems identified through the analysis. The two most common methods are Risk Priority Numbers (described in sub-section 3.3) and Criticality Analysis Method. The MIL-STD-1629A\(^{11}\) document describes two types of criticality analysis: qualitative and quantitative (sub-section 4.9).

To use qualitative criticality analysis to evaluate risk and prioritize corrective actions, the analysis team must a) rate the severity of the potential effects of failure and b) rate the likelihood of occurrence for each potential failure mode. It is then possible to compare failure modes via a Criticality Matrix (Figure 6), which identifies severity on the horizontal axis and occurrence on the vertical axis.

![Criticality Matrix](image)

Figure 6: Relation among failure causes, modes and effects.


To use quantitative criticality analysis, the analysis team considers the reliability/unreliability for each item at a given operating time and identifies the portion of the item’s unreliability that can be attributed to each potential failure mode. For each failure mode, they also rate the probability that it will result in system failure. The team then uses these factors to calculate a quantitative criticality value for each potential failure and for each item.

5.1 Cascaded failures

A cascading failure is a particular type of common-mode failure in which a single event, not necessarily hazardous in itself, can precipitate a series of other failures. The basic characteristic of a cascading failure is the propagation of an initial failure effect throughout the entire system or across and between the different systems.

The nature of cascading failures may vary considerably and it is difficult to provide a common definition or characteristic of such an event that would apply to all possible scenarios. A domino effect is a principal characteristic of cascading failures when an initial event, which has little or no adverse effect, is transmitted downstream and one of the subsequent failures generates hazardous effects. Cascading failures are considered "low-probability high-consequence event".

The "classic" cascading failure is characterized by a rapid propagation of failures. However, the cause-effect chain of events, leading ultimately to a hazardous situation, has to be considered, even if the failure propagation is spread over a large period of operation. Moreover, the triggering event may be a permanent or a temporary fault. Therefore, an important attribute of a cascading failure that requires consideration in the analysis is the time factor.

A cascading failure is a progression and generation of equipment outages, one precipitating another. The basic characteristic of a cascading failure is the propagation of an initial failure effect throughout the entire system or across and between the different systems. A domino effect is a principal characteristic of cascading failures when an initial event, which has little or no adverse effect on the aircraft, is transmitted downstream and one of the subsequent failures generates hazardous effects.

The nature of cascading failures may vary considerably and it is difficult to provide a common definition or characteristic of such an event that would apply to all possible scenarios. The prediction and analysis of cascading failures are complex due to their random dynamic involving continuous and switching operations that suddenly change the system’s configuration. In the progression of time, a Failure Mode comes between a Cause and an Effect. Any Effect that itself has an Effect might also be a Failure Mode. In different contexts, a single event may be a Cause, an Effect, and a Failure Mode.

Cascading failures in production systems normally occur as a result of initial disturbance or faults on various mechanical or electrical elements, closely followed by errors of human operators. The stability and secure operation of the production lines have a great impact on other related systems in a factory. It is vital to identify any disturbances on the critical elements in advance and develop effective protection strategies to alleviate the cascading failures.
A cascading failure is defined as a sequence of component malfunctions that include at least one triggering component malfunction and subsequent tripping the other components. Note that a cascading failure does not necessarily lead to a cascading break down.

5.2 Event Tree Analysis (ETA)

Complementary to other tools of CA, Event tree analysis (ETA)\textsuperscript{12} is a logical model for both failure and success responses from individual factor. The model has a number of pathways for analysing probabilities of results and the analysis of the whole structure. Event tree analysis is used for checking the effects of functions, or any error systems. Event trees are used to investigate the consequences of loss-making events in order to find ways of mitigating, rather than preventing losses. The basic stages to carry out the event tree analysis:

1. Identify the primary event of concern.
2. Identify the controls that are assigned to deal with the primary event such as automatic safety systems, alarms on operator actions.
3. Construct the event tree beginning with the initiating event and proceeding through failures of safety functions.
4. Establish the resulting accident sequences.
5. Identify the critical failures that need to be addressed.

There are a number of ways to construct an event tree. They use binary logic gates that has two options. Each branching point is called a node. Simple event trees tend to be presented at a system level, glossing over the detail. The following Figure 7 is a generic example of how they can be drawn.

The diagram shows an initialising event and the subsequent operation or failure of three systems which would normally operate should the event occur. Each system can either operate or not. Because of a multitude of combinations of success/failure of each system, there are multiple possible final outcomes. The diagram also illustrates the way event trees can be quantified. The initiating event is typically specified as an expected annual frequency and the success for each system as a probability.

5.3 Fault Tree Analysis (FTA)

If it is used as a top-down tool, FMEA may only identify major failure modes in a system. Fault tree analysis (FTA) is better suited for "top-down" analysis. When used as a "bottom-up" tool FMEA can complement FTA and identify many more causes and failure modes resulting in top-level symptoms. It is not able to discover complex failure modes involving multiple failures within a subsystem, or to report expected failure intervals of particular failure modes up to the upper level subsystem or system.

Fault tree analysis (FTA) is a kind of analysis and logic diagram for finding deductive failures in which using logic flows to combine different lower-level factors. It is also used for tracing all possible important factors and branches of events. Normally the more complex the case is, the more extensive the framework of fault tree framework will be. Here you can see an example of showing different pathways for possibilities.

The structure of fault tree and event tree analysis is different. The general direction of an event tree is from left to right laying on the horizontal axis, while fault tree graphs are shown in the up-to-down design. The layout of fault tree analysis is based on the traditional diagram structure of sciences, engineering or some other related subjects. In contrast, the structure design of event tree (Figure 8) easily displays categories with long titles and texts.

![Event Tree Diagram](image)
Although the diagram of fault tree and event tree analysis (Figure 9) seem similar for some parts, there are still differences in terms of their analytical methodology. Both two types involve the identifications and classifications of events and factors, but with opposite focuses on undesired events. The main purpose of fault tree analysis is preventing losses. In contrast, event tree analysis is ideal for mitigating bad results. Or you can say, fault tree analysis is cause-oriented whereas event tree analysis is consequences-oriented. You can see the below diagram for more details.

Both of these two types have helpful uses in reality for different specific fields. Fault tree analysis is ideal for the most of sciences related subjects, especially safety and reliability or software engineering, aerospace, energy, chemical process, pharmaceutical analysis, the design of diagnostic manuals and the fuel power design for aircraft. You can see a fire security system example below (Figure 10) that based on fault tree analysis. $P_1$, $P_2$, and $P_3$ are different probabilities for each pathway. In these cases, fault tree analysis is mainly used for:

- Detecting technical bugs.
- Understanding the overall system framework.
- Optimizing existing resources.
- Identifying methods to decrease functional failures of systems.
Event tree analysis is usually used for financial market analysis, especially those topics related to financial assets pricing and risk analysis. Readers can easily see the probabilities between different pathways of a financial model that based on event tree analysis diagram. Here you can see a financial pricing model sample (Figure 11) for the practical analysis of stock pricing. For simplification, the probabilities in this example only have two values $P_1$ and $P_2$, and the total number of stages (time period) is 3. The Expected Value (EV) for each stage is the outcome of corresponding stock price times their own probabilities.

![Fire secure system example](image1)

Figure 10: Fire secure system example (fault tree analysis).

![Financial pricing model](image2)

Figure 11: Financial pricing model (event tree analysis).
6 KEY RISK INDICATORS (KRIs)

Risk management is a set of actions to recognize or identify risks, errors and their consequences by applying any counter actions. A Risk is defined as the probability of an event that produces a negative effect, directly or indirectly. Risk management corresponds to a set of actions to recognize or identify the risk, to assess the probability of something happening, to evaluate the severity of its consequences and to take the necessary steps.

An indicator becomes «key» when it tracks an especially important risk exposure (key risk), or it does so especially well (key indicator), or ideally both. An Indicator is a numeric value produced through the combination of measures which provides business insight. Key Risk Indicators (KRIs) are critical predictors of unfavorable events that can adversely impact organizations. They monitor changes in the levels of risk exposure and contribute to the early warning signs that enable organizations to report risks, prevent crises and mitigate them in time.

KRIs are born out of high-quality data used to track a specific risk. Developing effective KRIs mandates a thorough understanding of objectives and risk-related events that might affect the achievement of those objectives. While most organizations monitor KRIs that have developed over time, it is essential for these to be regularly evaluated for efficiency and continuously monitored to highlight potential risks. Over time, they must be augmented with new KRIs to meet the dynamic circumstances as newer risks emerge and the older KRIs may be insufficient.

Once the Risk Management team assesses all its risks and scores their severity according to probability (or likelihood) and impact, it is possible to extract and isolate the top risks. It is then possible to define specific data which must be collected regularly to measure the ongoing status of those risks. For each KRI, upper and lower acceptable risk limits (warning thresholds) are defined, allowing management to track evolution and trends for each risk and KRI. This methodology enables the usage of Red, Amber and Green (RAG) limits which are useful since a “soft” amber limit can trigger an action before reaching the “hard” red limit.

Good KRIs share a number of characteristics.

1. **Relevant**: the indicator/data helps identify, quantify, monitor or manage risk and/or risk consequences that are directly associated with key business objectives/KPIs.
2. **Measurable**: the indicator/data is able to be quantified (a number, percentage, etc.) and is reasonably precise, comparable over time, and is meaningful without interpretation.
3. **Predictive**: the indicator/data can predict future problems that management can preemptively act on.
4. **Easy to monitor**: the indicator/data should be simple and cost effective to collect, parse, and report on.
5. **Auditable**: you should be able to verify your indicator/data, the way you sourced it, aggregated it, and reported on it.
6. **Comparable**: it’s important to be able to benchmark your indicator/data, both internally and to industry standards, so you can verify the indicator thresholds.
There are a number of benefits to identifying and using KRIs:

- **Supporting Risk Assessments** - KRIs help in adding more detail and information to risk assessments, making them more reliable and informative to management.

- **Proactive management of emerging risks** - KRIs allow for proactive identification of emerging risks by creating an informative framework in which to scan for what is on the horizon.

- **Tolerance levels and thresholds** - KRIs detail at what level a risk is considered important for attention or for direct intervention.

- **Trending KRIs** - KRIs can help management track trends in risks to the organisation. This can help to identify areas where greater investment may be needed or where opportunities might lie.

### 6.1 Identifying potential risks

There are two types of KRIs:

**Lagging** - monitor data retrospectively to identify changes in the pattern or trend of risk / activities. These types of KRIs ensure that the exposure is minimised as soon as practicable to prevent or reduce further exposure or consequence.

**Leading / predictive** - are used to signal changes in the likelihood of a risk event. They are more likely to aid management in acting in advance of risks materialising.

This graphic at Figure 12 represents the four steps needed for KRI development. An effective set of KRI metrics will provide insight into potential risk that may impact the realisation of objectives or may indicate the presence of new opportunities.

**Figure 12: KRI development.**

In details the KRI development is following:

**Step 1: Identification**

- Concentrate on high risks,
- Identify existing/available metrics,
- Understand the frequency of data availability,
- Determine if there are data gaps or metrics improvements.

**Step 2: Selection**

- Focus on indicators that may track changes in the risk profile
- Leading indicators will provide more predictive view of risk
- Ensure the KRIs are measurable, trackable, predictive and informative,
- A mix of leading and lagging indicators will provide better risk management,
- Determine trigger levels and thresholds, without contradiction to risk appetite.

**Step 3: Reporting**

- Determine frequency of tracking,
- Escalation and reporting framework should be in place,
- KRI reports should indicate trends and movements in risk,
- A dashboard format is often the easiest way to track and report KRIs,

**Step 4: Actions**

- Action plans should be created where KRIs are trending towards highest threshold,
- Target competition dates for actions should be set and included in reporting.

The below diagram (Figure 13) illustrates the identification of four key objectives aligned to the entity purpose. Linked to the objectives are several potential critical risks that may impact on one or more of the objectives. KRIs have been mapped to each critical risk to reduce the likelihood of the risk occurring and information to Senior Management of any risk that could potentially hinder the achievement of the entity objectives and strategy.

![Figure 13: Key objectives linked with potential critical risks.](image)

KRIs are most effective when they are:

- Measurable – are the metrics quantifiable e.g. number of, percentage.
- Trackable – allowing comparisons to be made over time to provide trending.
6.2 Facing the risk

Prior to monitoring KRIs, levels of threshold should be determined by management that will trigger action. This creates a more pro-active approach to the management of risk through the identification of actions that will reduce the likelihood of a risk event occurring and/or limit risk exposure to within risk appetite tolerances. KRI thresholds should be reviewed often to ensure they are set so the lower and upper triggers capture events or trends that serve as predictive indicators. The threshold should not contradict the risk appetite of the entity.

When determining the thresholds and trigger points for KRIs, consider the following:

- Risk appetite and tolerance
- Is there any historical data available on the KRI?
- When does management want to intervene to ensure adequate actions and migrations are put in place?

An example of thresholds is presented in Table 1.

<table>
<thead>
<tr>
<th>KRI</th>
<th>Green</th>
<th>Amber</th>
<th>Red</th>
</tr>
</thead>
<tbody>
<tr>
<td># of key persons voluntary resignations (key persons are those identified as successors to senior roles)</td>
<td>&lt;1 per quarter</td>
<td>1 – 3 per quarter</td>
<td>&gt;3 per quarter</td>
</tr>
</tbody>
</table>

In the above example, data would be available from HR systems and action should be taken at the amber trigger to understand reason for leaving, this could be done via methods such as exit interviews, looking at staff engagement survey results or one on one meetings with key persons.

Using past events to identify leading indicators

Reviewing a risk event that has affected your entity in the past is a great way to determine leading indicators that could assist in identifying a similar emerging risk from happening again.

Consider the root causes of the past event, speak to subject matter experts who managed and implemented actions to minimise the impact of that risk and understand the availability of data that could be used to reduce the likelihood of that risk event reoccurring. The closer the KRI is to the root cause of the risk event, the more likely the KRI will trigger pro-active management and action.
6.3 Developing Effective Key Risk Indicators

A goal of developing an effective set of KRIs is to identify relevant metrics that provide useful insights about potential risks that may have an impact on the achievement of the organization’s objectives. Therefore, the selection and design of effective KRIs starts with a firm grasp of organizational objectives and risk-related events that might affect the achievement of those objectives. Linkage of top risks to core strategies helps pinpoint the most relevant information that might serve as an effective leading indicator of an emerging risk.

An effective method for developing KRIs begins by analysing a risk event that has affected the organization in the past (or present) and then working backwards to pinpoint intermediate and root cause events that led to the ultimate loss or lost opportunity. The goal is to develop key risk indicators that provide valuable leading indications that risks may be emerging. The closer the KRI is to the ultimate root cause of the risk event, the more likely the KRI will provide management time to proactively take action to respond to the risk event.

Virtually all organizations possess existing risk metrics that have evolved over time. These metrics should be carefully evaluated for their efficacy and continue to be employed if found to be valuable in highlighting potential emerging risks. Augmenting these existing KRIs with new metrics is likely to be required, however.

Another important element in designing effective KRIs involves the assurance that all parties involved in collecting and aggregating KRI data are clear about definitions of individual data items to be captured and any conversion or standardization methodology to be utilized. Without confidence in the uniformity of the KRI measurement approach, aggregated information will lack robustness and introduce noise into the ultimate decision process.

An important element of any KRI is the quality of the available data used to monitor a specific risk. Attention must be paid to the source of the information, either internal to the organization or drawn from an external party. Sources of information are likely to exist that can help inform the choice of KRIs to be employed. For example, internal data may be available related to prior risk events that can be informative about potential future exposures. However, internal data is typically unavailable for many risks—especially those that have not been encountered previously. And, often risks likely to have a significant impact may arise from external sources, such as changes in economic conditions, interest rate shifts, or new regulatory requirements or legislation.

Thus, many organizations discover that relevant KRIs are often based on external data, given that many root cause events and intermediate events that affect strategies arise from outside the organization.

External sources such as trade publications and loss registries compiled by independent information providers may be helpful in identifying potential risks not yet experienced by the organization. Discussions with key stakeholders such as customers, employees and suppliers may provide important insights into risks they face that may ultimately create risks for the organization. A careful understanding of regulatory and legal requirements that
must be fulfilled is likely to be helpful in anticipating potential risks and events that precede them. KRI data sourced from external and/or independent parties provides the benefit of objectivity. External/independent parties are not necessarily unaffiliated with the organization, but are removed from the business unit from which the KRI is measured. Almost certainly, trade-offs will be required in this area. Those individuals charged with ongoing management of a particular risk are the least objective source (but at times may be the only available resource for the data required to produce the KRI in question). A careful validation of external sources is desirable to enhance confidence in the ultimate effectiveness of the KRI built from that data.

It is unlikely that a single KRI will adequately capture all facets of a developing risk or risk trend. For this reason, it is helpful to analyse a collection of KRIs simultaneously to help form a better understanding of the risk being monitored. That said, some KRIs are likely to possess superior predictive power over other risk metrics and it will be important to weight each piece of information to reflect its past performance in forecasting a risk event. Some have referred to this process as assembling a mosaic of information that collectively can best provide the early warning of potential threats developing over time. Realistically, substantial judgment and experience must be brought to bear on this process to extract the most meaningful inferences. As the use of KRIs evolves in an organization, opportunities for making these judgments will likely yield improvements in KRI performance.
7 Z-BRE4K EXAMPLE

During the manufacturing processes, it is important to prioritize matters and to determine the order and the time-frame for the predictive actions that will take actions. FMECA s/w has been designed to automate and facilitate FMEA/FMECA process and provide flexible data that can be further used by management and reporting capabilities for caring out the measures to address the most serious concerns. Thus, the FMEA/FMECA methodologies have been used to design and to identify potential failure modes for processes (but also products) before the problems occur, to assess the risk associated with those failure modes and to provide the Risk Priority Number (RPN) values due to occurred errors. Design, development, manufacturing, service and other activities that improve reliability and increase efficiency can be supported with FMEA/FMECA analysis.

It is familiar that FMEA/FMECA techniques are widely used throughout various industries e.g. automotive, aerospace, medical and other manufacturing industries, where the flexible analysis method can be performed at various stages in the product life cycle. The effects analysis within Z-BRE4K considers effects with local or machinery system level with severity levels, detectability scale and probability of failure to occurs within plastic, packing and automotive industry.

When using FMECA within Z-BRE4K (Figure 14), an end user needs to:

1. define and specify an asset type e.g. product, process of production, assembly, service, machine, etc.

When defining the asset type, it is important to have in mind the potential failure that is identified in terms of:

- failure mode (e.g. crack, deformation, short circuit, fracture, etc.),
- failure cause (e.g. inadequate design, poor environmental protection, insufficient lubrication, etc.) and/or failure mechanism (e.g. wear, corrosion, yield, etc.),
- failure effect (Figure 15) e.g. poor appearance, noise, deuteration, etc.
2. assess the seriousness of the effect of the potential failure mode providing the input of severity level presented in Table 2,

### Table 2: Table of Severity

<table>
<thead>
<tr>
<th>RANKING LEVEL</th>
<th>CLASSIFICATION</th>
<th>CRITERIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Insignificant</td>
<td>A FM which could potentially degrade the systems function but will cause no damage to the system and does not constitute a threat to life or injury.</td>
</tr>
<tr>
<td>2</td>
<td>Marginal</td>
<td>A FM which could potentially degrade the systems performance function(s) without appreciable damage to system or threat to life or injury.</td>
</tr>
<tr>
<td>3</td>
<td>Critical</td>
<td>A FM which could potentially result in the future of the systems primary functions and therefore causes considerable damage to the system and its environment, but which does not constitute a serious threat to life or injury.</td>
</tr>
<tr>
<td>4</td>
<td>High</td>
<td>A FM which could potentially result in the future of the systems primary functions and therefore causes serious damages to the system and its environmental and/or personal injury.</td>
</tr>
</tbody>
</table>
3. Define the level of detectability presented in Table 3\textsuperscript{13} and how easy is to detect the potential failure (e.g. through physical tests, mathematical modelling, prototype testing, feasibility reviews etc.),

<table>
<thead>
<tr>
<th>RANKING LEVEL</th>
<th>CLASSIFICATION</th>
<th>CRITERIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Extremely Likely</td>
<td>Almost certainly detection</td>
</tr>
<tr>
<td>2</td>
<td>Very High Likely</td>
<td>Very High probability of detection</td>
</tr>
<tr>
<td>3</td>
<td>High Likely</td>
<td>High probability of detection</td>
</tr>
<tr>
<td>4</td>
<td>Moderately High Likely</td>
<td>Moderately effective detection</td>
</tr>
<tr>
<td>5</td>
<td>Medium Likely</td>
<td>Even chance of detection</td>
</tr>
<tr>
<td>6</td>
<td>Moderately Low Likely</td>
<td>May miss to detect the problem</td>
</tr>
<tr>
<td>7</td>
<td>Low Likely</td>
<td>Likely to miss to detect the problem</td>
</tr>
<tr>
<td>8</td>
<td>Very Low Likely</td>
<td>Poor chance of detection</td>
</tr>
<tr>
<td>9</td>
<td>Unlikely</td>
<td>Unreliable and poor chance for detection</td>
</tr>
<tr>
<td>10</td>
<td>Extremely Unlikely</td>
<td>Controls will not detect</td>
</tr>
</tbody>
</table>

4. Define the probability (%) of the chance that one of the specific cause/mechanisms will occur.

The above information and the effect on the total system is studied and Risk Priority Number (RPN) is automatically provided and listed from high to low. The RPN will be further used by management (decision makers) and DSS software applications, for appropriate correction steps and action that will be taken (or planned) to minimize the probability of failure or to minimize the effect of failure.

Within the Z-BRE4K FMECA we have presented the Process Failure Mode and Effect Analysis in production process of Ceramic tiles that are publicly available\textsuperscript{14}. This company’s objective and purpose were to achieve and make quality controls to the final product for the feasibility of quality standards. The published data were used, RPN was obtained automatically (Figure 14) and FMECA further provides information for upcoming use and analysis approach and estimation and evaluation of risks.

![Figure 16: Process Failure Mode & Effect Analysis in production process of Ceramic tiles.](image)

Furthermore, the case in the knitting industry\textsuperscript{15} was found and the example of fabric was used for presenting the Z-BRE4K FMECA analysis as well. The results are presented below in Figure 15.

It can be stated that with continuous FMECA method, the manufacturing process efficiency of product quality is improved while decreasing the number of defective products and saving of rework cost and time\textsuperscript{13}.

\begin{flushright}
\textsuperscript{14}P. H. Tsarouhas, D. Arampatzaki. Application of Failure Modes and Effects Analysis (FMEA) of a Ceramic Tiles Manufacturing Plant. 1ST OLYMPUS INTERNATIONAL CONFERENCE ON SUPPLY CHAINS, 1-2 OCTOBER, KATERINI, GREECE.
\end{flushright}
Figure 17: Process Failure Mode & Effect Analysis in production process of Knitting industry.
8 CONCLUSION

At the conclusion of the FMECA, critical items/failure modes are identified and corrective action recommendations made based on the criticality list and/or the Criticality Matrix generated by the Criticality Analysis. FMEA/FMECA analysis is a flexible process that can be adapted to meet the particular needs of the industry and/or the organization.

Utilizing the criticality list, the items with the highest criticality number or RPN receive attention first. Utilizing the Criticality Matrix (recommended), items in the uppermost right-hand quadrant will receive attention first. Typical recommendations call for design modifications such as; the use of higher quality components, higher rated components, design in redundancy or other compensating provisions.

Recommendations cited must be fed back into the design process as early as possible in order to minimize iterations of the design. The FMECA is most effective when exercised in a proactive manner to drive design decisions, rather than to respond after the fact.

Future work is to connect the FMECA with the various IDS connectors per user case. After that the data will be consumed automatically, and will not be inputted by hand as it happens now. Also, the FMECA will communicate with the DSS software application (D4.2).


9 REFERENCES


