Risk Management Using Failure Mode and Effect Analysis (FMEA)
Also available from ASQ Quality Press:

*Failure Mode and Effect Analysis: FMEA from Theory to Execution, Second Edition*
D.H. Stamatis

*Advanced Quality Auditing: An Auditor’s Review of Risk Management, Lean Improvement, and Data Analysis*
Lance B. Coleman Sr.

*The Certified Supplier Quality Professional Handbook*
Mark Allen Durivage, editor

*The ASQ Auditing Handbook, Fourth Edition*
J.P. Russell, editor

*Proactive Supplier Management in the Medical Device Industry*
James B. Shore and John A. Freije

*Quality Risk Management in the FDA-Regulated Industry, Second Edition*
José Rodríguez-Pérez

Milton P. Dentch

*The Certified Six Sigma Yellow Belt Handbook*
Govindarajan Ramu

*Handbook of Investigation and Effective CAPA Systems, Second Edition*
José Rodríguez-Pérez

*Practical Design of Experiments (DOE): A Guide for Optimizing Designs and Processes*
Mark Allen Durivage

*The Certified Pharmaceutical GMP Professional Handbook Second Edition*
FDC Division and Mark Allen Durivage, editor

*The Quality Toolbox, Second Edition*
Nancy R. Tague

Risk Management Using Failure Mode and Effect Analysis (FMEA)

D. H. Stamatis

ASQ Quality Press
Milwaukee, Wisconsin
Table of Contents

List of Figures and Tables ......................................................... ix
Preface ...................................................................................... xi
Introduction ............................................................................... xiii

Chapter 1  Risk ........................................................................ 1
  Overview .............................................................................. 1
  In ISO 9001:2015 ................................................................. 3
  In IATF 16949 ...................................................................... 7
  VDA (New FMEA Proposed Standard of 2018) ..................... 7
  Method or Process of Conducting Any Risk Assessment ...... 10
  General Comments ............................................................. 14
  Conclusion ........................................................................... 18

Chapter 2  Reliability and FMEA ............................................ 19
  Overview .............................................................................. 19
  Need to Understand the Concept of Failure ...................... 20
  Design for Reliability ......................................................... 21

Chapter 3  Prerequisites of FMEA .......................................... 23
  Creating an Effective Team ................................................. 23
  The Structure of the FMEA Team ....................................... 23
  Ingredients of a Motivated FMEA Team ......................... 25
  Potential FMEA Team Members ....................................... 26
  Mind-set of Minimizing Failures ....................................... 27

Chapter 4  What Is an FMEA? .................................................. 29
  Definition ............................................................................ 29
  Is FMEA Needed? .............................................................. 30
  Benefits of FMEA .............................................................. 31
  The Process of Conducting an FMEA ............................... 32
  Understanding Your Customers and Their Needs .............. 36
What Happens after Completion of the FMEA? .......... 37
Vocabulary ......................................... 38

Chapter 5 Robustness ................................. 45
  Boundary Diagram ................................ 45
  Interface Matrix ................................... 46
  P-Diagram ......................................... 47

Chapter 6 The FMEA Form and Rankings ............ 49
  Severity Rating ..................................... 50
  Occurrence Rating .................................. 51
  Detection Rating .................................... 51
  Classification and Characteristics ................. 52
  Understanding and Calculating Risk ............... 53
  Driving the Action Plan ............................ 54

Chapter 7 Types of FMEA ......................... 57
  FMEA Challenges ................................ 58

Chapter 8 The Common Types of FMEAs .......... 59
  Concept ............................................ 59
  Design ............................................. 61
  Process ............................................ 66
  Equipment ........................................ 75

Chapter 9 Health FMEA ............................. 85
  Comparison of Root-Cause Analysis and HFMEA ... 86
  The Process of the HFMEA ........................ 87
  Forms and Rankings ................................ 91

Chapter 10 Failure Mode Effects and Criticality
  Analysis (FMECA) .................................. 97
  Definition ......................................... 97
  Possible Sources for Identifying Functions ........ 98
  The Process of Conducting an FMECA ............. 99
  Qualitative Analysis ................................ 101
  Quantitative Approach ............................. 101
  Form .............................................. 108

Chapter 11 Control Plans ............................. 113
  Purpose ........................................... 113
  Benefits .......................................... 114
  Content of a Control Plan ........................ 114
  FMEA/Control Plan Linkage ......................... 115
## Table of Contents

Chapter 12  Linkages .................................................. 119
   DFMEA to PFMEA to Process Flow Diagram
   to Control Plan ............................................. 119

Chapter 13  Tools ................................................... 123
   Overview of Typical Tools Used in FMEA ................ 123

Chapter 14  Troubleshooting an FMEA ........... 141
   After FMEA .................................................. 141

Chapter 15  Typical Concerns When Conducting
   an FMEA ..................................................... 147
   Common Team Problems ................................... 147
   Common Procedural Problems ............................ 147
   Institutionalizing FMEA in Your Company ........... 149

Chapter 16  FMEAs Used in Selected Specific Industries ....... 151
   Automotive ................................................. 151
   Aerospace .................................................. 152
   Software .................................................... 152
   Chemical/Pharmaceutical .............................. 152

Chapter 17  Warranty, Six Sigma, Lean, and FMEA .... 155
   Automotive Perception of Warranty .................... 155
   Six Sigma ................................................... 158
   Lean ......................................................... 159
   After Improvements Are Made .......................... 159

References ......................................................... 161
Selected Bibliography ........................................... 163
Index .................................................................. 165
# List of Figures and Tables

<table>
<thead>
<tr>
<th>Figure/Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.1</td>
<td>VDA-proposed FMEA form</td>
<td>13</td>
</tr>
<tr>
<td>Table 1.1</td>
<td>A typical risk register for a project that includes four steps: identify, analyze, plan response, monitor and control</td>
<td>16</td>
</tr>
<tr>
<td>Figure 4.1</td>
<td>Overview of a DFMEA</td>
<td>34</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>Overview of a PFMEA</td>
<td>35</td>
</tr>
<tr>
<td>Table 5.1</td>
<td>Robustness focus</td>
<td>46</td>
</tr>
<tr>
<td>Figure 5.1</td>
<td>A typical boundary diagram</td>
<td>46</td>
</tr>
<tr>
<td>Table 5.2</td>
<td>Interface matrix</td>
<td>47</td>
</tr>
<tr>
<td>Figure 5.2</td>
<td>A typical P-diagram</td>
<td>48</td>
</tr>
<tr>
<td>Figure 6.1</td>
<td>A typical FMEA form</td>
<td>50</td>
</tr>
<tr>
<td>Figure 6.2</td>
<td>Area chart showing priority levels</td>
<td>53</td>
</tr>
<tr>
<td>Table 7.1</td>
<td>Types of FMEAs</td>
<td>58</td>
</tr>
<tr>
<td>Table 8.1</td>
<td>DFMEA—severity</td>
<td>63</td>
</tr>
<tr>
<td>Table 8.2</td>
<td>DFMEA—occurrence</td>
<td>64</td>
</tr>
<tr>
<td>Table 8.3</td>
<td>DFMEA—detection</td>
<td>65</td>
</tr>
<tr>
<td>Figure 8.1</td>
<td>A typical PFMEA</td>
<td>68</td>
</tr>
<tr>
<td>Table 8.4</td>
<td>PFMEA—severity</td>
<td>69</td>
</tr>
<tr>
<td>Table 8.5</td>
<td>PFMEA—occurrence</td>
<td>70</td>
</tr>
<tr>
<td>Table 8.6</td>
<td>PFMEA—detection</td>
<td>71</td>
</tr>
<tr>
<td>Table 8.7</td>
<td>A typical control matrix for a manufacturing process</td>
<td>72</td>
</tr>
<tr>
<td>Figure 8.2</td>
<td>Explanation of the EFMEA form</td>
<td>79</td>
</tr>
</tbody>
</table>
List of Figures and Tables

Table 9.1 Similarities and differences of RCA and HFMEA ........... 87
Table 9.2 8 wastes and 6S .................................... 88
Table 9.3 A typical comparison of process design and organizational change. ............................ 89
Figure 9.1 A typical HFMEA worksheet ............................ 92
Table 9.4 A typical severity ranking ............................... 93
Table 9.5 A typical matrix showing severity and probability ........... 94
Figure 10.1 A typical qualitative FMECA ......................... 102
Figure 10.2 A typical quantitative FMECA ...................... 109
Figure 11.1 Linkage from DFMEA to CP ......................... 116
Change rarely comes in the form of a whirlwind, despite the currently popular notion to the contrary. Change is not “creative destruction” like we’ve been told. Change that expects us to throw out everything we were and start over isn’t change at all, but a convulsion. A hiccup. The internet did not change everything. Broadband did not change everything. September 11 did not change everything. Nor did Enron, WorldCom, or any other company. Nor will tomorrow’s horror, tomorrow’s amazing breakthrough, or tomorrow’s scandal.

If you follow the cataclysmic theory of change, you will reap a whirlwind indeed. There is a different theory of change that no one talks about but that is much more significant for the wise professional. In the coastlines of any country, state, or territory one can see it every day. The waves may crash against the rocks, but they are a distraction. The real action is the tide. When the tide changes, huge forces are put in motion that cannot be halted. (If you doubt the power of the tide, look at the suburbs of any fair-size town anywhere. A piece of farmland on the edge of most towns is worth its weight in gold. Why? Because it’s where the affluent middle class wants to bunk down every night.)

Risk is everywhere. It does not matter where we are or what we do. It affects us on a personal level, but it also affects us in our world of commerce and our business. No matter if we are focused on identifying and/or analyzing risks, these risks are always balanced with an associated benefit. In the final analysis, all types of risks exist, and they are generated by a variety of factors, such as customer requests, continual improvement philosophy, and competition.

Why do we do a risk analysis? Primarily to answer the following two questions:

1. What can go wrong?
2. If something does go wrong, what is the probability of it happening and what is (are) the consequence(s)?
In the past, these questions were focused on “problem fixing.” The primary analysis was to focus on “who” did it. Of course, the focus on problems assumed that somebody was to blame, and action was taken. In other words, we operated on the principle that “If it’s not broken, don’t touch it.” Today, that paradigm has changed. The focus is on prevention. In other words: “If it is not broken improve it.” The focus is on “how it happened” and “why it happened.”

In this book we explore the evaluation process of risk by utilizing one of the core methodologies available: failure mode and effect analysis (FMEA). Our intent in this book is to make the concepts easy to understand and explain why FMEA is used in many industries with positive results to either eliminate or mitigate risk.

It is not a complete reference on FMEA; rather, it is a summary guide for everyone who wants some fast information regarding failures and how to deal with them. Specifically, we cover the following topics:

- Risk as defined in International Organization for Standardization (ISO), International Automotive Task Force (IATF), and Verband der Automobilindustrie (VDA) standards and/or guidelines
- Reliability and FMEA
- Prerequisites of FMEA
- What an FMEA is
- Robustness
- The FMEA form and rankings
- Types of FMEA
- The common types of FMEAs
- Failure mode effects and criticality analysis (FMECA)
- Health FMEA
- Control plans
- Linkages
- Tools
- Troubleshooting an FMEA
- Getting the most from FMEA
- FMEAs used in selected and specific industries
- Warranty, Six Sigma, and lean
In the past 100 years or so, the United States has been the envy of the world. This country has been the leader in almost every major innovation people have made. The historical trend has been positive indeed. However, what about the future? Can the status quo be retained? Is there anything to worry about? Can the leadership for tomorrow be guaranteed by following past successes?

The United States wants to be among the leaders; it wants to be better; its citizens want to work smart and be efficient. But with leadership and general betterment comes change—change in behavior and technology. The old ways served workers well but not anymore. The following saying describes the situation best.

*If you always do what you always did, you will always get what you always got.*

What the United States has achieved in the past is not good enough anymore as world competition increases; it must improve or it will be left behind as others pursue technological and quality improvements for their products and/or services. In simple terms, this means that the attitude and behavior toward quality must change.

A good starting point is for organizations to use the 6S process (sort-store-shine-standardize-sustain-safety), emphasizing sustain and safety. Both of these areas focus on prevention and will lead to good designs as well as excellent processes.

As with any transformation, this change brings uncertainty and risk. However, this transformation may be successful if the organization has (1) vision, (2) mission, (3) strategy, (4) action plan, and (5) implementation strategy.

The recognition that all well-managed companies are interested in preventing or at least minimizing risk in their operations is the concept of
Introduction

risk management analysis. The requirements for performing such analysis may be extensive and demanding. The elimination, control, or reduction of risk is a total commitment by the entire organization, and it is more often than not the responsibility of the engineering department. In this book we focus only on a small portion of this engineering responsibility—specifically, the FMEA methodology. Here we must emphasize that FMEA is only one methodology of many that can help in the strategy, action plan, and implementation strategy for improvement.
Over the last five or so years, much discussion has been devoted to risk, although the fact is that the “risk concept” is immature in the International Organization for Standardization (ISO) documents. Why? Because of the 157 items in the ISO standards the word “risk” is used in 45 unique definitions, of which 21 specifically address hazards. On the other hand, in the International Automotive Task Force (IATF) 16949 standard, the word “risk” is sprinkled throughout the standard and it is especially emphasized in reference to prevention actions and failure mode and effect analysis (FMEAs).

In both ISO and IATF documents, the definitions are abundant as they consider events with negative outcomes using very specific language. For example, risk is “a function of the probability of occurrence of a given threat and the potential adverse consequences of that threat’s occurrence.”

To be sure, that is a very unique definition. However, it is not all inclusive. For example, the Project Management Body of Knowledge (PMBOK) (2000, ch. 11; 2017, ch. 11) goes further by including concerns that deal with the effect of uncertainty, the combination of the consequences of an event and the associated likelihood of its occurrence, and uncertain events or conditions that, if they occur, have a positive or negative effect on a project’s objectives.

The term risk, used in the ISO standards and the new IATF standard, “pertains to safety and/or performance requirements in the context of meeting applicable regulatory requirements at minimum.” An FMEA is a standard technique used to assess and evaluate potential risks in the design development phase, which continues during production process controls. Other related techniques are fault tree analysis, warranty analysis, SWOT (strengths-weaknesses-opportunities-threats) analysis, event tree analysis, business continuity planning, BPEST (business, political, economic, social, technological) analysis, real option modeling, decision making under conditions of risk and
uncertainty, statistical inference, measures of central tendency and dispersion, and PESTLE (political, economic, social, technical, legal, environmental) analysis. Any of these various risk assessment techniques can also be used to incorporate other aspects of the quality management system (Stamatis 2014). The specific definition, per the ISO standards, includes three related definitions:

1. **Risk definition.** Risk is the potential of gaining or losing something of value. Values (such as physical health, social status, emotional well-being, or financial wealth) can be gained or lost when taking risk resulting from a given action or inaction, foreseen or unforeseen. Risk can also be defined as the intentional interaction with uncertainty (EN ISO 14971:2012, 2.16).

2. **Risk management.** Risk management is the identification, assessment, and prioritization of risks (defined in ISO 31000:2018 as the effect of uncertainty on objectives), followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities (EN ISO 14971:2012, 2.22).

3. **Risk assessment.** Risk assessment is the determination of a quantitative or qualitative estimate of risk related to a well-defined situation and a recognized threat (also called hazard). Quantitative risk assessment requires calculations of two components of risk (R): the magnitude of the potential loss (L) and the probability (p) that the loss will occur (Stamatis 2014).

The need for risk analysis is defined in several clauses of the standard. For example, in ISO 13485:2016, we find that risk is mentioned either directly or indirectly throughout the standard but specifically in sections (clauses) 4.1; 7.4.1; 7.4.2; 8.2; 8.2.1; 8.3; and 8.3.4.

Therefore, the issue of risk has become a very important quality requirement and is viewed as a preventive tool in any quality management system (QMS), Advanced Product Quality Planning (APQP) process, and FMEA of any organization. In fact, for most organizations, there is no need to have a separate section to identify “preventive action” because the concept of preventive action is expressed through a “risk-based” approach in which the QMS requirements are identified and implemented. For example, ISO 9001:2015 makes risk-based thinking a requirement by specifically calling for risks and opportunities to be determined and addressed. This is a very strong statement to demonstrate that risks are to be identified, corrective actions must be planned, and implementation has to be monitored for the specific risks under consideration.

Reading the standards, one concludes without hesitation that their intent as far as risk is concerned is (a) to provide confidence in the organ-
organization’s ability to consistently provide customers with conforming goods and services and (b) to enhance customer satisfaction. The concept of “risk” in the context of the international standards relates to the uncertainty in achieving these objectives.

Since that is the primary concern, the standards articulate the notion of risk-based thinking, which is defined as something we all do automatically and often subconsciously. Although the concept of risk has always been implicit in ISO 9001, the 2015 revision makes it more explicit and builds it into the whole management system. So, risk-based thinking now has become part of the process approach. The intent here is to make sure that risk-based thinking makes preventive action part of the routine process. This is also very true in the FMEA process.

To be sure, risk is often thought of only in the negative sense. However, risk-based thinking can also help to identify opportunities. This can be considered the positive side of risk, which is a relatively recent concept. The result of this thinking is:

- To improve customer confidence and satisfaction
- To ensure consistency of quality of goods and services
- To establish a proactive culture of prevention and improvement
- To have successful companies intuitively take a risk-based approach

**IN ISO 9001:2015**

Risk in ISO 9001:2015 and ISO 14001:2015 is implied throughout the standards as it is referenced wherever the words “planning” or in clause 6.0 “prevention” and “effectiveness” are mentioned. The reason for this general inclusion is because the ISO standards consider risk to be an inherent characteristic in all aspects of a quality management system.

Therefore, in a given organization risk-based thinking must be prevalent in any management review because it is a vital element in the continual improvement process that is focused on prevention. This risk-based thinking must be demonstrated with risk register documentation and must be available for review during audits. A risk register is documented information that validates that an organization has done risk-based thinking.

It must be emphasized here that risk-based thinking is indeed preventive action and unequivocally is everybody’s business! As a consequence, it must become an integral part of the organizational culture.

It is significant to note that ISO 9001:2015 does not automatically require anyone to carry out a full, formal risk assessment or to maintain
a risk register per ISO 31000 (Risk management—Principles and guide-
lines on implementation); although it will be a useful reference, it is not
mandated. On the other hand, the standard requires the proper identifica-
tion of what the risks and opportunities are in your organization, which
depends on context. That is why the active participation of management
is imperative.

The premise of the risk evaluation as a quality management system is
founded in clause 4.4—Quality management system and its processes. Here
we find that the organization must establish, implement, maintain, and
continually improve a quality management system, including the processes
needed and their interactions, in accordance with the requirements of this
ISO standard. The organization must determine the processes needed for
the quality management system and their application throughout the organ-
ization (in subsection (f) we read the risks and opportunities in accordance
with the requirements of 6.1) and then plan and implement the appropriate
actions to address them.

Furthermore, we need to read clause 4.6 (Planning for the quality man-
gagement system) and clause 6.1 (Actions to address risks and opportuni-
ties, specifically, 4.1 and 6.1.1). When planning for the quality management
system, the organization shall consider the issues referred to in 4.1 and the
requirements referred to in 4.2 and determine the risks and opportunities
that need to be addressed to (a) give assurance that the quality management
system can achieve its intended result(s); (b) prevent, or reduce, undesired
effects; and (c) achieve continual improvement.

In section 5 of the standard, Management responsibility, and clause
6.0—Planning—we see specific actions. For example, in 6.1 we find actions
to address risks and opportunities. In 6.1.1 we find that when planning for
the quality management system, the organization shall consider the issues
referred to in 4.1 and the requirements referred to in 4.2 and determine the
risks and opportunities that need to be addressed to (a) give assurance that
the quality management system can achieve its intended result(s); (b) prevent,
or reduce, undesired effects; and (c) achieve continual improvement. Finally,
clause 6.1.2 tells us that the organization shall plan (a) actions to address
these risks and opportunities, and (b) how to, one, integrate and implement
the actions into its quality management system processes (see 4.4) and, two,
evaluate the effectiveness of these actions. Actions taken to address risks and
opportunities shall be proportionate to the potential impact on the conformity
of products and services.

Of course, to appreciate what the ISO standard is requiring is to see the
individual clauses in context. The context should be addressed from at least
the following actions and questions:
• Analyze and prioritize the risks and opportunities in your organization—what is acceptable? What is unacceptable?

• Plan actions to address the risks. How can I avoid or eliminate the risk? How can I mitigate the risk?

• Implement the plan—take action.

• Check the effectiveness of the action. Does it work? Learn from experience (continual improvement).

Overall, the ISO standard presents an outline of requirements for risk-based thinking as specific requirements. For example:

• Risks and opportunities are determined and addressed.

• Actions are implemented to address the specific risk(s) identified.

• There is no requirement for formal methods for risk management or a documented risk management process.

• QMS is considered a preventive tool (as such, there is no need to have a separate clause or sub-clause titled “preventive action”; the concept of preventive action is expressed through a risk-based approach to formulating QMS requirements).

• Risk is defined in ISO 9000 as the effect of uncertainty. (Uncertainty is the state—even partial—of deficiency of information related to the understanding or knowledge of an event, its consequence, or its likelihood. Remember that not all processes have the same level of risk in terms of the organization’s ability to meet its objectives.) Therefore, the consequences of process, product, service, or system nonconformities will not be the same for all organizations.

• Opportunities can arise as a result of a situation favorable to achieving an intended result, which means any opportunity is not the positive side of risk. Rather, an opportunity is a set of circumstances that makes it possible to do something—either from a positive or negative situation. This means that an opportunity presents different levels of risk and appropriate planning, definition, and therefore evaluation must take place, and the earlier the better.

**Goal**

So, generally speaking, ISO’s goal is to make sure that the customer is satisfied with the quality system of the supplier in such a way that it is sufficient
to deliver an acceptable product. In other words, it is a system-oriented standard.

On the other hand, the goal of the automotive QMS standard is an upgrade of ISO to the new IATF 16949 standard as defined on page 7 of it. The new upgrade provides for continual improvement, emphasizing defect prevention and reduction of variation and waste (in the entire supply chain) in much more detail. In essence, the idea is to harmonize the automotive standards globally.

Project

Once the goal has been defined, the next concern is to make sure management understands the perimeters of the project from at least four perspectives (Stamatis 2016, 1998). They are:

1. **Resources**: Of great importance here is to recognize the workload in resource planning.

2. **Timing**: Project plan must be in place with internal and external milestones and critical paths that are practical and realistic to fulfill all the planned resources requirements.

3. **Ability to address customer requirements**: Any success depends on whether the customer requirements are met as defined and expected.

4. **Change**: Change is inevitable. Therefore, the first and perhaps the most important element of any change implementation is the recognition of an effective implementation.

The key new actions in ISO 9001 that address risks and opportunities (in addition to the ones that have already been mentioned) are:

- **6.1.1 Actions to Address Risks and Opportunities**: Planning needs to consider the context (issues) of the organization (4.1) and the interested party expectations (4.2) and address the risks and opportunities to help the QMS achieve “its intended results.”

- **6.1.2 Actions to Address Risks and Opportunities**: Actions need to be developed, integrated, and implemented back into the QMS processes (4.1).

- **9.1.3 Analysis and Evaluation**: Effectiveness of actions on risks and opportunities.

- **9.3 Management Review**: (b) Changes in external and internal issues and (e) effectiveness of actions on risks and opportunities.
• 10.1 (Improvement) General: “Preventing or reducing undesired effects.”

• 10.2 Nonconformity and Corrective Action: “Update risks and opportunities” based on corrective actions.

**IN IATF 16949**

As of September 2018, IATF 16949 is the official automotive requirement replacing the ISO 9001/16949:2015. It has become an official standard and not an engineering specification. In the standard, we find that risk is evident because it is either directly or indirectly mentioned throughout the standard but specifically in sections (clauses) 4.4.1.2; 6.1.2.1; 6.1.2.2; 6.1.2.3; 7.2.3; 8.1.2; 8.3.2.1; 8.7.1.1; 8.7.1.2; and 8.7.1.6.

IATF 16949 supports all the core tools (statistical process control [SPC], measurement system analysis [MSA], FMEA, APQP, production part approval process [PPAP] of the Automotive Industry Action Group [AIAG]) and adds a number of specific risk-related requirements to minimize the chance of failure during new program development and to maximize (not optimize) the chance for realization of planned activities. Key clauses that deal directly with the managing and mitigating risk are 8.1.1; 8.2.2.1; 8.2.3.1.1; 8.2.3.1.3; and 8.6.6.

The comprehensiveness of the new standard is coming to light with further requirements that deal with additional controls for the management of development projects through the cycle, eventually concluding with a product approval process. Key clauses that deal with this area are 8.3.3.1; 8.3.4.2; 8.3.4.3; 8.3.5.1; and 8.3.4.4.

**VDA (NEW FMEA PROPOSED STANDARD OF 2018)**

There is no ambiguity about the relationship of FMEA and risk. The two are very closely related. However, for all industries—except automotive—the requirements of all FMEAs are the same. That is, they follow the specifications of the Society of Automotive Engineers (SAE) J1739, ISO requirements, AIAG, FMEA, and their specific requirements, as appropriate, for their customers.

**Principles**

Generally, there are 12 principles that guide the way that risk management is integrated and deployed in ISO 9001/16949:2015; in IATF:16949:2016; and in Verband der Automobilindustrie (VDA) and ISO 31000:2018:
Chapter One

1. Risk management creates and protects value. Resources expended to mitigate risk should be less than the consequence of inaction.

2. Risk management is an integral part of all organizational processes.

3. Risk management is part of decision making.

4. Risk management explicitly addresses uncertainty and assumptions.

5. Risk management is systematic, structured, and timely.

6. Risk management is based on the best available information.

7. Risk management is tailored to specific tasks.

8. Risk management takes human and cultural factors into account.

9. Risk management is transparent and inclusive.

10. Risk management is dynamic, iterative, and responsive to change.

11. Risk management facilitates continual improvement and enhancement.

12. Risk management demands that organizations continually or periodically reassess their systems.

In the automotive industry, under the leadership of a German consortium, a new standard is pending called the VDA. It is supposed to harmonize the automotive standards worldwide. In the United States the standard has been met with mixed feelings, although the AIAG has given the standard the green light for further clarification and discussion between its members before full implementation. It is expected to be finalized either very late in 2018 or early 2019. However, it is not a mandatory requirement for Ford, General Motors (GM), and Fiat Chrysler (FC). So, it is up to these automakers if they want to use it or continue with the traditional FMEA approach.

The expected benefits are primarily in five areas. They are:

- Supplying German automakers with a good quality product
- Maintaining higher-quality standards than even IATF 16949
- Increasing overall quality of products
- Reducing warranty costs
- Minimizing risk issues/concerns and problems
Model of the Expected VDA Standard: A Six-Step Approach

Step 1: Scope (Problem) Definition
Step 2: Structure Analysis
Step 3: Function Analysis
Step 4: Failure Analysis
Step 5: Risk Analysis
Step 6: Optimization

Specifically, these steps include:

2.1.1 Purpose: The purpose of the design FMEA (DFMEA) Scope Definition is to define what is included and excluded in the FMEA based on the type of analysis being developed (i.e., system, subsystem, or component).

2.2.1 Purpose: The purpose of Design Structure Analysis is to identify and break down the design into system, subsystem, and component parts for technical risk analysis.

2.3.1 Purpose: The purpose of the Design Function Analysis is to ensure that the functions specified by requirements/specifications are appropriately allocated to the system elements.

2.4.1 Purpose: The purpose of the Design Failure Analysis is to identify failure causes, modes, and effects and show their relationships in order to undertake risk assessment.

2.5.1 Purpose: The purpose of Design Risk Analysis is to estimate risk by evaluating severity, occurrence, and detection and prioritize the need for actions.

2.6.1 Purpose: The purpose of the Design Optimization is to determine actions to mitigate risk and assess the effectiveness of those actions. The primary objective of optimization is to develop actions that reduce risk and increase customer satisfaction by improving the design.

Flow

• DFMEA contains information that is useful for process FMEA (PFMEA):
  – Failure causes related to piece-to-piece
Chapter One

– End-user failure effects and severity for the failure causes related to product characteristics

• PFMEA contains information that needs alignment with the DFMEA:
  – Failure effects and severity for failure modes that are also shown in the DFMEA
  • Not all failure causes in a DFMEA are failure modes in a PFMEA.

Action Priority

*High:* The team must either identify an appropriate action to improve prevention and/or detection controls or justify and document why current controls are adequate.

*Medium:* The team should identify appropriate actions to improve prevention and/or detection controls or, at the discretion of the company, justify and document why controls are adequate.

*Low:* The team could identify actions to improve prevention or detection controls.

METHOD OR PROCESS OF CONDUCTING ANY RISK ASSESSMENT

The generic method for a risk analysis of any kind consists of the following elements, performed, more or less, in the following order:

1. Identify, characterize *threats*.
2. Assess the *vulnerability* of critical assets to specific threats.
3. Determine the *risk* (i.e., the expected likelihood and consequences of specific types of attacks on specific assets).
4. Identify ways to reduce those risks.
5. Prioritize risk reduction measures.
General Evaluation Criteria for DFMEA

Severity: Whereas the evaluation criteria for a DFMEA for industries other than automotive still follow the AIAG guidelines (or some modification of them), the automotive industry, by adopting the VDA standard, has quite different proposed criteria. However, since they are not officially published, we can say that the severity is evaluated based on what the end-user experiences.

Occurrence: Whereas the evaluation criteria for a DFMEA for industries other than automotive still follow the AIAG guidelines (or some modification of them), the automotive industry by adopting the VDA standard has quite different proposed criteria. Again, though, since they are not officially published we can say that occurrence will be evaluated based on (a) estimated frequency, (b) product experience, and (c) prevention control.

Detection: Whereas the evaluation criteria for a DFMEA for industries other than automotive still follow the AIAG guidelines (or some modification of them), the automotive industry by adopting the VDA standard has quite different potential criteria. Once more, since they are not officially published we can say that the detection will be based on the activity performed prior to delivery of the design for production.

General Evaluation Criteria for PFMEA

Severity: Whereas the evaluation criteria for a PFMEA for industries other than automotive still follow the AIAG guidelines (or some modification of them), the automotive industry by adopting the VDA standard has quite different proposed criteria. However, since they are not officially published, we can say that the severity is evaluated based on the failure effects rated for manufacturing, assembly, and end user.

Occurrence: Whereas the evaluation criteria for a PFMEA for industries other than automotive still follow the AIAG guidelines (or some modification of them), the automotive industry by adopting the VDA standard has quite different proposed criteria. Again, though, since they are not officially published we can say that the occurrence is evaluated based on (a) estimated frequency, (b) process experience, and (c) prevention control.
**Chapter One**

**Detection:** Whereas the evaluation criteria for a PFMEA for industries other than automotive still follow the AIAG guidelines (or some modification of them), the automotive industry by adopting the VDA standard has quite different proposed criteria. Once more, since they are not officially published we can say that the detection will be based on activities prior to shipment of the product so that nonconformances may be caught.

**Monitoring and System Response (MSR)**

The scope of a supplemental FMEA for monitoring and system response may be established in consultation between customer and supplier. Typical steps are:

1. Scope definition
2. Structure analysis
3. Function analysis
4. Failure analysis
5. Risk analysis
6. Optimization

**FMEA Form**

Whereas the form used for the FMEA for industries other than the automotive industry still follow the classic AIAG format, the automotive industry, by adopting the VDA standard, has modified the form quite extensively (see Figure 1.1).

**Identification**

After establishing the context, the next step in the process of managing risk is to identify potential risks. Risks are about events that, when triggered, cause problems or benefits. Hence, risk identification can start with the source of our problems and those of our competitors (benefit) or with the problem itself. It is important to note here that the problem is recognized at the *actionable root-cause level*. It is also important to identify the problem at the *escape point* (EP). The EP is the place of the process that the root cause could have been caught but it was not. Unless we find the EP, we will have a perpetual problem. We may find out how to fix it but the fixing is going to be continual since the origination of the root cause will not be known.
### DESIGN FAILURE AND EFFECTS ANALYSIS (DFMEA)

<table>
<thead>
<tr>
<th>SUBJECT:</th>
<th>DFMEA ID Number:</th>
<th>DFMEA Start Date:</th>
<th>DFMEA Revision Date:</th>
<th>Design Responsibility:</th>
<th>Security Classification:</th>
<th>FMEA Intast:</th>
<th>FMEA Test:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>COMPANY NAME:</th>
<th>ENGINEERING LOCATION:</th>
<th>CUSTOMER NAME:</th>
<th>MODEL / YEAR / PLATFORM:</th>
<th>FMEA TEAM:</th>
<th>FMEA DUE DATE:</th>
<th></th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>STRUCTURE ANALYSIS</th>
<th>FUNCTION ANALYSIS</th>
<th>FAILURE ANALYSIS</th>
<th>RISK ANALYSIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. System (Item)</td>
<td>1. Function of System and Requirement or Intended Output</td>
<td>1. Failure Effects (FE)</td>
<td>Occurrence (O) of FC</td>
</tr>
<tr>
<td>2. System Element/Interface</td>
<td>2. Function of System Element and Intended Performance Output</td>
<td>2. Failure Mode (FM)</td>
<td>Current Detection Control (DC) of FC or FM</td>
</tr>
<tr>
<td>3. Component Element (Item / Interface)</td>
<td>3. Function of Component Element and Requirement or Intended Output or Characteristic</td>
<td>3. Failure Cause (FC)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OPTIMIZATION</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PREVENTION ACTION</td>
<td>DETECTION ACTION</td>
</tr>
<tr>
<td>RESPONSIBLE PERSON</td>
<td>TARGET COMPLETION DATE</td>
</tr>
<tr>
<td>STATUS (Untouched Under Consideration in Progress Completed Decided)</td>
<td>ACTION TAKEN WITH POINTER TO EVIDENCE</td>
</tr>
<tr>
<td>COMPLETION DATE</td>
<td>SEVERITY (S)</td>
</tr>
</tbody>
</table>

**Figure 1.1** VDA-proposed FMEA form
Chapter One

So, how do we proceed? Depending on the situation there are several options. However, most commonly they fall into two categories:

1. **Source analysis.** Risk sources may be internal or external to the system that is the target of risk management (use mitigation instead of management since, by definition, risk deals with factors of decision making that cannot be managed). Examples of risk sources are owners of a project, employees of a company, customer requirements, legal requirements, or events of nature.

2. **Problem analysis.** Risks are related to identified threats (e.g., the threat of losing money, the threat of abuse of confidential information, or the threat of human errors, accidents, and casualties). The threats may exist with various entities, most important with process owners, customers, and legislative bodies such as the government. When either source or problem is known, the events that a source may trigger or the events that can lead to a problem can be investigated. For example, stakeholders withdrawing during a project may endanger funding of the project; confidential information may be stolen by employees even within a closed network; natural events may result in many casualties.

The chosen method of identifying risks may depend on culture, industry practice, applicable and thorough FMEA, and compliance with appropriate standards and customer specifications.

**GENERAL COMMENTS**

Everything we do in life has a risk. Generally, that risk is evaluated (assessed) based on two considerations:

1. The benefit one gets from performing a task
2. The negative consequences from either performing or not doing the task

In any environment there is always more than one risk involved. So, some options in identifying the available risk options are:

1. Design a new business process with adequate built-in risk control and containment measures from the start.
2. Periodically reassess risks that are accepted in ongoing processes as a normal feature of business operations and modify mitigation measures.
3. Transfer risks to an external agency (e.g., an insurance company).
4. Avoid risks altogether (e.g., by closing down a particular high-risk business area).

The assessment is not always in financial terms. It may be safety, government regulations, customer demands, and so on. If the assessment is a financial one, make sure an appropriate cost-benefit analysis is performed. To be sure that the appropriate assessment is being evaluated, each option requires developing a plan that is implemented and monitored for effectiveness (i.e., reduction or mitigation of risk). Typical guides for this evaluation of increasing seriousness of the risk (ISO 31000:2009, revised with ISO 31000:2018: Risk management—Principles and guidelines on implementation) are:

1. Intensified technical and management reviews of the engineering process
2. Special oversight of designated component engineering
3. Special analysis and testing of critical design items
4. Rapid prototyping and test feedback
5. Consideration of relieving critical design requirements
6. Initiation of fallback parallel developments

Essentially, the key capabilities of a risk-enabled quality management solution include but are not limited to the following:

- **An integrated risk register.** There needs to be a centralized place to record and monitor individual hazards and risk items. The importance here is to demonstrate consistency. At minimum, this document should include dates, description of risk, risk type (business, project, and stage), severity of effect, likelihood of occurrence (Low <30%, Medium 31–75%, or High >75%), countermeasures, status, and any other quantitative value that may be applicable and appropriate. A typical risk register based on the work of Kokcharov (2015) is shown in Table 1.1.

- **Flexible risk tools.** A matrix is needed to be able to activate risk assessment tools, to demonstrate the link between audits to risk deviations or regulatory requirements, and to track the effectiveness of the tools as they are applied to specific risks.

- **Risk-based effectiveness checks.** This requirement is used for verifying corrective action and evaluating improvement requirements.
Chapter One

Risk Management Plan

Select appropriate controls or countermeasures to measure each risk. Risk mitigation needs to be approved by the appropriate level of management. For instance, a risk concerning the image of the organization should have top management decision behind it whereas IT management would have the authority to decide on computer virus risks.

The risk management plan should propose applicable and effective security controls for managing the risks. For example, an observed high risk of computer viruses could be mitigated by acquiring and implementing antivirus software. A good risk management plan should contain a schedule for control implementation and the persons responsible for those actions.

According to ISO/IEC (International Electrotechnical Commission) 27001, the stage immediately after completion of the risk assessment phase consists of preparing a risk treatment plan, which should document the decisions about how each of the identified risks should be handled. Mitigation of risks often means selection of security controls, which should be documented in a statement of applicability that identifies which particular control objectives and controls from the standard have been selected and why.

Potential Risk Treatments

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories (Stamatis 2014; Dorfman 2007):

1. Avoidance (eliminate, withdraw from, or not become involved). This includes not performing an activity that could carry risk. An example would be not buying a machine with high life-cycle costs even though the original price of the machine may be less than a machine with low life-cycle costs, even though the original price may be higher.
2. Reduction (optimize and mitigate). Risk reduction or optimization involves reducing the severity of the loss or the likelihood of the loss from occurring. A classic example of this is whether or not to buy water sprinklers that are designed to put out a fire and therefore reduce the risk of loss by fire. However, by installing the sprinklers you may cause another loss due to water damage, which may be a higher cost and not suitable for the budget of the organization. The result may be in finding another alternative.

Yet another approach to reducing risk is by outsourcing it (Stamatis 2016, 2014; Roehrig 2006). A typical method is to insure the loss through a third party.

3. Sharing (transfer, outsource, or insure). This option is briefly defined as “sharing with another party the burden of loss or the benefit of gain, from a risk, and the measures to reduce a risk.”

The term “risk transfer” is often used in place of risk sharing in the mistaken belief that you can transfer a risk to a third party through insurance or outsourcing. In practice, if the insurance company or contractor go bankrupt or end up in court, the original risk is likely to still revert to the first party. As such, in the terminology of practitioners and scholars alike, the purchase of an insurance contract is often described as a “transfer of risk.”

4. Retention (accept and budget). As unthinkable as it may be, the fact is that risk retention is a reality in everything we do. It involves accepting the loss, or benefit of gain, from a risk when it occurs. In our common language we call it self-insurance. In other words, we will take a chance that the failure will not happen or if it does, it will not be detrimental to our organization. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default.

Ideal use of these risk control strategies may not be possible. Some of them may involve trade-offs that are not acceptable to the organization or person making the risk management decisions. Another source of control may be the approach that the US Department of Defense takes in using the avoid-control-accept-transfer (ACAT) model.

Review and Evaluation of the Plan

Initial risk management plans will never be perfect. This is because we are not able to foresee all risks and all potential problems that may occur in the short or long term. Things happen unexpectedly and when they do, hopefully we learn, adjust, modify, and/or completely change the task, system, or process in the organization. Obviously, practice, experience, and actual loss results will necessitate changes in the plan and contribute information
to allow possible different decisions to be made in dealing with the risks being faced.

Risk analysis results and management plans should be updated periodically for two primary reasons:

1. To evaluate whether the previously selected security controls are still applicable and effective.

2. To evaluate the possible risk-level changes in the business environment. For example, information risks are a good example of rapidly changing business environments.

Limitations

Prioritizing the risk management processes too highly could keep an organization from ever completing a project or even getting started. This is especially true if other work is suspended until the risk management process is considered complete.

It is also important to keep in mind the distinction between risk and uncertainty. Risk can be measured by impacts times probability. If risks are improperly assessed and prioritized, time can be wasted in dealing with risk of losses that are not likely to occur. Spending too much time assessing and managing unlikely risks can divert resources that could be used more profitably. Unlikely events do occur, but if the risk is unlikely enough to occur it may be better to simply retain the risk and deal with the result if the loss does in fact occur. Qualitative risk assessment is subjective and lacks consistency. The primary justification for a formal risk assessment process is legal and bureaucratic.

CONCLUSION

Risk-based thinking is an element in the process approach. That is:

- Risk-based thinking is an input to management review.
- Risk-based thinking is an element in the continual improvement process that is focused on prevention.

Risk-based thinking has been demonstrated during audits; a risk register is documented with information that validates an organization has done risk-based thinking.
OVERVIEW

When one talks about reliability the implication is that there is some specification for a product such that no failures will be present in the system, subsystem, component, or process. Therefore, reliability is an engineering discipline that focuses on prevention of failures by design, people, hardware, production, and maintenance personnel or processes.

It is impossible to create something that is 100% reliable because reliability at time $t$ is equal to 1 minus the failure rate: $R(t) = 1 - F(t)$. Therefore, in practice we achieve acceptable failures only, and only if the risk is mitigated to provide benefits that are within the definition of the acceptability guidelines that the customer and/or the team has identified. This is possible if we have a thorough understanding of all the potential failure modes and then take appropriate steps to prevent them from occurring. Understanding potential failure modes is achieved by analyzing and testing during both the design and the production phases of a project. Of course, there are several ways to do the analysis. Here we focus on the FMEA. Other ways include but are not limited to:

- Reliability-centered maintenance (RCM): program development and implementation
- Equipment criticality analysis
- Reliability engineering analysis and support, including FMEA, failure code development, root-cause analysis, and lean tools such as 6S (sort-store-shine-standardize-sustain-safety)
- Reliability engineering training: processes, methods, and tools
- Preventive maintenance optimization
Predictive maintenance program
Calibration program and optimization
Maintenance engineering staff augmentation: planners, schedulers, work preparers, maintenance supervisors, RCM engineers

NEED TO UNDERSTAND THE CONCEPT OF FAILURE

Criteria
A failure by strict definition is a deviation from a standard and/or specification. However, the criteria for defining a failure are heavily dependent on context of use and may be relative to a particular observer or belief system. A situation considered to be a failure by one might be considered a success by another, particularly in cases of direct competition or a zero-sum game. Similarly, the degree of success or failure in a situation may be viewed differently by distinct observers or participants, such that a situation that one considers to be a failure another might consider to be a success, a qualified success, or a neutral situation.

It may also be difficult or impossible to ascertain whether a situation meets criteria for failure or success due to ambiguous or ill-defined definitions of those criteria. Finding useful and effective criteria, or heuristics, to judge the success or failure of a situation may itself be a significant task. That task depends on clear, simple, and concise operational definition as well as a team that has both knowledge and some ownership (either direct or indirect) of the system, subsystem, or component under consideration.

Therefore, in cases where there is a difference of opinion about the failure, the FMEA team should decide to treat the failure under discussion in the most conservative way. This means that the failure exists for all customers.

Types
Once the criteria for failure have been identified, then the team is ready to proceed with the analysis, always remembering that failure can be differentially perceived from the viewpoint of the evaluator. A person who is only interested in the final outcome of an activity would consider it to be an outcome failure if the core issue has not been resolved or a core need is not met. A failure can also be a process failure, whereby although the activity is completed successfully, a person may still feel dissatisfied if the under-
lying process is perceived to be below an expected standard or benchmark. Fundamentally, there are three types of failures:

1. Failure to perceive
2. Failure to anticipate
3. Failure to carry out a task

The first two generally account for the concept and design FMEAs. The third one accounts for process and service FMEAs.

**DESIGN FOR RELIABILITY**

Reliability is of course an issue of design. Therefore, to minimize failures a good design must have at least the following items evaluated before the release of that design. The reader should note that the steps identified here are indeed part of a detailed FMEA analysis. The steps are:

- Step 1: Design for maintainability.
- Step 2: Perform functional analyses to determine failure modes as well as their consequences, severity, and ways of early detection.
- Step 3: Analyze components with potential failures and determine their failure models.
- Step 4: Determine maintenance tasks, their frequency, and their effectiveness.
- Step 5: Define and optimize maintenance implementation plan.
CREATING AN EFFECTIVE TEAM

Perhaps one of the most important issues in dealing with the FMEA is that this analysis must be done with a team. An FMEA completed by an individual is only that individual’s opinion and does not meet the requirements or the intent of an FMEA.

An effective FMEA team:

- Has expertise in the subject (five to seven individuals)
- Is multilevel/consensus-based
- Includes representatives of all relevant stakeholders (those who have ownership)
- May change membership as work progresses
- Is cross-functional and multidisciplinary (one person doing his or her best cannot approach this level of knowledge)
- Allows appropriate and applicable empowerment
- Includes the operator for PFMEA

THE STRUCTURE OF THE FMEA TEAM

Core Team

The experts of the project and those closest to the project are the core team. They facilitate honest communication and encourage active participation. Support membership may vary depending on the stage of the project. The
leader for the DFMEA should be the design engineer and for the PFMEA the manufacturer engineer.

**Champion/Sponsor**

This team member:

- Provides resources and support
- Attends some meetings
- Supports the rest of the team
- Promotes team efforts and implements recommendations
- Shares authority/power with other team members
- Kicks off the team
- Comes from management (the higher up in management the better)
- Breaks down any bottlenecks that may surface

**Team Leader**

A team leader is the “watchdog” of the project. Typically, this function falls on the lead engineer. A good team leader:

- Possesses good leadership skills
- Is respected by team members
- Leads but does not dominate
- Maintains full team participation

**Recorder**

This person documents the team’s efforts. The recorder is responsible for coordinating meeting rooms and times as well as distributing meeting minutes and agendas.

**Facilitator**

The watchdog of the process, the facilitator keeps the team on track and makes sure that everyone participates. In addition, it is the facilitator’s responsibility to make sure that team dynamics develop in a positive environment. For the facilitator to be effective it is imperative that this indi-
vidual has no stake in the project, possesses FMEA process expertise, and communicates assertively.

**Team Considerations**

- Continuity of members
- Receptiveness and open-mindedness
- Commitment to success
- Empowered by the sponsor
- Cross-functionality
- Multidisciplinary
- Consensus-based
- Positive synergy

**INGREDIENTS OF A MOTIVATED FMEA TEAM**

To motivate people:

- Set realistic agendas.
- Have a good facilitator.
- Keep meetings short.
- Have the right people present.
- Reach decisions based on consensus.
- Have open-minded, self-initiators, and volunteers on the team.
- Offer incentives.
- Establish ground rules.
- Make one individual responsible for coordination and accountability of the FMEA project. Typically for the design, the design engineer is that person, and for the process, the manufacturing engineer accounts for that responsibility.

To make sure the effectiveness of the team is sustained throughout the project, it is imperative that everyone concerned with the project bring useful
information in the process. Useful information may be derived from one’s education, experience, training, or a combination of these factors. At least three areas that are usually underutilized for useful information are (1) background information, (2) surrogate data, and (3) the input of the operator.

1. **Background information and supporting documents** that may be helpful to complete the system, design, or process FMEAs include:
   - Customer specifications (OEMs)
   - Previous or similar FMEAs
   - Historical information on warranty/recalls, etc.
   - Design reviews and verification reports
   - Product drawings/bill of material
   - Process flowcharts/manufacturing routing
   - Test methods
   - Preliminary control and gage plans
   - Maintenance history
   - Process capabilities

2. **Surrogate data** generated from similar projects may help in the initial stages of the FMEA. When surrogate data are used, extra caution should be taken. The surrogate data should be replaced with the actual data as soon as possible.

3. **Operator input** is very essential. As the person the closest to the operation, the operator is most qualified to discuss assignable causes.

**POTENTIAL FMEA TEAM MEMBERS**

The actual team composition for your organization will depend on your individual project and resources. An appropriate team for your project may include any of the following:

- Design engineers
- Manufacturing engineers
- Quality engineers
• Test engineers
• Reliability engineers
• Maintenance personnel
• Operators (from all shifts)
• Equipment suppliers
• Customers
• Suppliers
• Anyone who has a direct or indirect interest in the project:
  – In any FMEA team effort, the individuals must have interaction with manufacturing and/or process engineering while conducting a DFMEA. This is important to ensure that the process will manufacture per design specification.
  – On the other hand, interaction with design engineering while conducting a PFMEA or assembly FMEA is important to ensure that the design is right.
  – In either case, team consensus will identify the high risk areas that must be addressed to ensure that the design and/or process changes are implemented for improved quality and reliability of the product.

Once the team is chosen for the given project, spend 15 to 20 minutes creating a list of the biggest (however you define “biggest”) concerns for this product or process. This list will be used later to make sure we have a complete list of functions.

**MIND-SET OF MINIMIZING FAILURES**

Another prerequisite for conducting an FMEA is to recognize that failures should be eliminated and/or minimized. As noble a goal as that proposition is, we all know that it is difficult to achieve. So, what we often end up doing is minimizing as much as possible the potential for any system, process, subsystem, or component failure. This is a team trade-off that may be difficult to achieve. Remember, a failure is a nonconformance from a standard and/or a specification. These nonconformances may or may not be a concern for the customer and/or design and/or the process. In fact, the design and/or process may indeed operate with a given nonconformance.
Even though the previous statement is correct, it is imperative that all of us should be concerned with failures. Our goal is and should be to have an attitude of failure-free designs and processes. This will facilitate customer satisfaction and improve efficiency within the organization that is undertaking the FMEA practice.

In the end, this translates to more profitability!
DEFINITION

FMEA is an engineering “reliability tool” that:

1. Helps to define, identify, prioritize, and eliminate known and/or potential failures of the system, design, or manufacturing process before they reach the customer. The goal is to eliminate the failure modes or reduce their risks.

2. Provides structure for a cross-functional critique of a design or a process.

3. Facilitates interdepartmental dialogue. (It is much more than a design review.)

4. Creates the mental discipline that “great” engineering teams go through when critiquing what might go wrong with the design, product, or process.

5. Is a living document that reflects the latest design, product, and process actions.

6. Ultimately helps prevent, and not react to, problems.

7. Identifies potential product- or process-related failure modes before they happen.

8. Determines the effect and severity of these failure modes.

9. Identifies the causes and probability of occurrence of the failure modes.

10. Identifies the “controls” and their effectiveness.
11. Quantifies and prioritizes the risks associated with the failure modes.

12. Develops and documents action plans that will occur to reduce risk.

**IS FMEA NEEDED?**

If any answer of the following questions is positive, then you need an FMEA:

- Are customers becoming more quality conscious?
- Are reliability problems becoming a big concern?
- Are regulatory requirements harder to meet?
- Are you doing too much problem solving?
- Are you addicted to problem solving? This is a very important consideration in the application of an active FMEA program because when the thrill and excitement of solving problems become dominant, your organization is addicted to problem solving rather than preventing the problem to begin with. A proper FMEA will help break your addiction by:
  - Reducing the % time to problem solving
  - Increasing the % time in problem prevention
  - Increasing the efficiency of resource allocation

Note: Emphasis is always on reducing complexity and engineering changes.

In more general terms we need an FMEA to emphasize the need to improve our designs and/or processes to be more effective (satisfy our customers) and efficient (optimize our resources). However, the most important reason for conducting an FMEA is the need to improve. This strongly implies that in order to receive all or some of the benefits of an FMEA program, the need to improve must be ingrained in the organization’s culture. If not, the FMEA program will not succeed. Therefore, a successful FMEA is a customer, company, and supplier requirement for a world-class quality. Specifically, any FMEA can help the improvement process in the following areas:

- Superior competitive advantage:
  - Best-in-class value
  - Quality performance
What Is an FMEA?

– Sustainable cost advantage
– Flawless launch at the start of production or commencement of a program

• Superior organizational capability:
  – Brings best-in-class design
  – Uses or achieves breakthrough technology
  – Moves fast

• Superior culture:
  – “Can do” attitude
  – An obsession with continual improvement
  – Team spirit
  – Knowing how to say “no” the right way

This translates into:

• Faster development time
• Reduction of overall cost
• Improved quality throughout the life of the product and/or service

**BENEFITS OF FMEA**

When properly conducted, all types of FMEAs should lead to:

1. Confidence that all (reasonable) risks have been identified early and appropriate actions taken
2. Priorities and rationale for product and process improvement actions
3. Reduction of scrap, rework, and manufacturing costs
4. Preservation of product and process knowledge
5. Reduction of field failures and warranty cost
6. Document risks and actions for future designs and/or processes
THE PROCESS OF CONDUCTING AN FMEA

To conduct an FMEA effectively one must follow a systematic approach. The recommended approach is an eight-step method that facilitates the system, design, product, process, equipment, and service FMEA. The steps are:

1. **Select the team** and brainstorm. Make sure the appropriate individuals are going to participate. The team must be cross-functional and multidisciplined and the team members must be willing to contribute (i.e., share their experience and knowledge).

   After the team has been identified and is in place, the team tries to prioritize the opportunities of improvement. Is the concern in a system, design, product, process, or service? What kind of problems are there and/or what kind of problems are anticipated with a particular situation? Is the customer and/or supplier involved or is continual improvement being pursued independently? If the customer and/or supplier identified specific failures, then the job is much easier because direction has already been given. On the other hand, if continual improvement is being independently pursued, the brainstorm, affinity diagram, storybook method, and/or cause-and-effect diagram may prove to be the best tools to identify some direction.

2. **Create a functional block diagram** and/or process flowchart. For system and design FMEAs, the functional block diagram is applicable. For the process and service FMEAs, the process flowchart is applicable. The idea is to make sure that everyone is on the same wavelength. Does everyone understand the system, design, process, and/or service? Does everyone understand the problems associated with the system, design, process, and/or service?

   The functional block diagram focuses the discussion on the system and design while the process flowchart focuses the discussion on the process and service. Both of these tools also provide an overview and a working model of the relationships and interactions of the systems, subsystems, components, processes, assemblies, and/or services and help in the understanding of the system, design, product, process, and/or service.

3. **Prioritize.** After the team understands the background, the actual analysis begins. Frequent questions are: What part is important? Where should the team begin?

   Sometimes, this step is completely bypassed because the prioritization is de facto. The customer has identified the priority, or due to warranty cost or some other input the determination has been made by management to start at a given point.
4. **Begin data collection.** The team must collect data of the failures and categorize them appropriately. At this point the team begins to fill in the FMEA form. The failures identified are the failure modes of the FMEA.

5. **Analyze the data.** Now the data are utilized for a resolution. Remember, the reason for the data is to gain information that is used to gain knowledge. Ultimately, that knowledge contributes to the decision. This flow can be shown as follows:

<table>
<thead>
<tr>
<th>Data</th>
<th>Information</th>
<th>Knowledge</th>
<th>Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The analysis may be qualitative or quantitative. The team may use brainstorming, cause-and-effect analysis, quality function deployment (QFD), design of experiments (DOE), SPC, another FMEA, mathematical modeling, simulation, reliability analysis, and anything else that team members think is suitable.

Information from this step will be used to fill in the columns of the FMEA form in relationship to the effects of the failure, existing controls, and the estimation of severity, occurrence, and detection.

6. **Record results.** The theme here is *data driven*. Based on the analysis, results are derived. The information from this step will be used to quantify the severity, occurrence, detection, and risk priority number (RPN). The appropriate columns of the FMEA will be completed.

7. **Confirm/evaluate/measure.** After the results have been recorded, it is time to confirm, evaluate, and measure the success or failure. This evaluation takes the form of three basic questions.

   – Is the situation better than before?
   – Is the situation worse than before?
   – Is the situation the same as before?

The information from this step will be used to recommend actions and to see the results of those actions in the corresponding columns of the FMEA form.

8. **Do it all over again.** Regardless of how step 7 is answered, the team must pursue improvement all over again because of the underlying philosophy of FMEA, which is continual improvement.

   The long-term goal is to completely eliminate every single failure. The short-term goal is to minimize the failures if not eliminate them. Of course, the perseverance for those goals has to be taken into consideration in relationship to the needs of the organization, costs, customers, and competition.
The philosophy of continual improvement embedded in the FMEA is that all types of FMEAs are living documents. (Here we must note however that due to the short-term versus long-term expectations, the short-term results may be sufficient; therefore the team may change to a new one so that the long-term results may come to fruition.)

**Getting Started**

As with anything else, before the FMEA begins there are some assumptions and preparations that must be taken care of. These assumptions are:

1. Define the FMEA project and scope.
2. Know your customers and their needs.
3. Know the function.
4. Understand the concept of priority.
5. Develop and evaluate conceptual designs/processes based on your customer’s needs and business strategy.
6. Be committed to continual improvement.
7. Create an effective team.

A general overview of the DFMEA and PFMEA may be seen in Figures 4.1 and 4.2, respectively.

---

**Figure 4.1** Overview of a DFMEA
What Is an FMEA?

Timing

The FMEA should be performed and/or updated whenever:

- A new cycle begins (new product/process).
- Changes are made to the operating conditions.
- A change is made in the design/process.
- New regulations are instituted.
- Customer feedback indicates a problem.

Uses

Among the primary uses of an FMEA are:

- Development of system requirements that minimize the likelihood of failures
- Development of designs and test systems to ensure that the failures have been eliminated or the risk is reduced to acceptable level
- Development and evaluation of diagnostic systems
- To help with design choices (trade-off analysis)
Advantages

The process of conducting an FMEA can:

• Improve the quality, reliability, and safety of a product/process
• Improve a company’s image and competitiveness
• Increase user satisfaction
• Reduce system development time and cost
• Collect information to reduce future failures and capture engineering knowledge
• Reduce the potential for warranty concerns
• Lead to early identification and elimination of potential failure modes
• Emphasize problem prevention
• Minimize late changes and associated cost
• Be a catalyst for teamwork and idea exchange between functions
• Reduce the possibility of same kind of failure in future
• Reduce the impact on a company’s profit margin
• Improve production yield

UNDERSTANDING YOUR CUSTOMERS AND THEIR NEEDS

A product or a process may perform functions flawlessly, but if the functions are not aligned with customer needs, you may be wasting your time. Therefore, you must:

• Determine all (internal and/or external) relevant customers.
• Understand the customer’s needs better than the customers understand their own needs.
• Document the customer’s needs and develop concepts. For example, customers may need:
  – Chewable toothpaste
  – Smokeless cigarettes
What Is an FMEA?

In FMEA, a customer is anyone/thing that has functions/needs from your product or manufacturing process. An easy way to determine customer needs is to understand the Kano model and QFD, especially for design issues.

WHAT HAPPENS AFTER COMPLETION OF THE FMEA?

Generally there are seven steps that the team must follow:

1. **Review the FMEA.** Make sure that the function, purpose, and objective have been met. Make sure that all the loose ends have been addressed and the appropriate action has been recommended and/or implemented. Some helpful hints for this review follow.
   - Is the problem identification specific?
   - Was a root cause, an effect, or a symptom identified?
   - Is the corrective action measurable?
   - Is the corrective action proactive?
   - Is the use of terminology current and consistent?
   - Is the corrective action realistic and sustainable?
   - Has a control plan been developed and linked to the critical as well as significant characteristics in the FMEA?

2. **Highlight the high-risk areas.** A visual inspection of the critical column, the severity column, and the RPN column generally will identify the high-risk areas (see Figure 1.1). In the critical column, the high-risk item may be identified as such; in the severity column the high-risk item usually will have a number higher or equal to 7; and in the RPN column usually a number greater than or equal to 100 (on a 1 to 10 scale) will indicate that there might be a high-risk item. In some industries this is not recognized as a valid identification process for high-risk items. In some cases, the high-risk item is identified by the numerical value of severity regardless of the value of RPN (see step 3).

3. **Identify the critical, significant, and major characteristics.** Upon completion of the FMEA, a visual check of the RPN and critical columns
should identify the critical, significant, and major characteristics. Make sure that there is a direct correlation between the critical column and the effects of the failure and the severity columns. Great care should be taken when reviewing the RPN because these numbers will indicate whether or not action should be taken. Here we must emphasize that even though many industries use the RPN as a clearing point for evaluating risks (the higher the number the riskier the failure mode cause), there is a better way to do the evaluation based on (1) severity, (2) criticality (Severity $\times$ Occurrence), and (3) RPN (Severity $\times$ Occurrence $\times$ Detection).

4. Ensure that a control plan exists and is being followed. As previously mentioned, the idea behind performing an FMEA is to eliminate and/or reduce known and potential failures before they reach the customer. In this step, make sure that all critical, significant, and major characteristics have a documented plan for controlling, improving, and/or handling changes. The control plan is the map that will allow practitioners to make the product and/or service acceptable to the customer. Although the FMEA identifies the vital signs of the process and/or service, the control plan monitors those vital signs of the process and/or service.

5. Conduct capability studies. After the control plan is in place and statistical control has been established, a potential capability or a long-term capability must be performed.

6. Work on processes that have a $C_{pk}$ less than or equal to 1.33. Although the 1.33 generally is accepted as the minimum goal, be aware that some companies require a $P_{pk} = 1.33$ (namely, automotive companies) or even a $C_{pk} = 2.00$ (Motorola). The point is to continually improve the process by eliminating variation. Produce everything around the target.

7. Work on processes that have $C_{pk}$ or a $P_{pk}$ greater than or equal to 1.33. After the minimum standard is reached in step 6, try to go beyond that standard for further improvement. Reduce variation and try to reach or exceed a $C_{pk}$ or $P_{pk}$ greater than or equal to 2.00. Remember, all standards are minimum performance. Consequently, continual improvement dictates that one should at all times try to exceed all standards, including all $C_{pk}$ or $P_{pk}$ targets.

**VOCABULARY**

As in every methodology, including the FMEA, there is special jargon that is used to communicate functions, failures, and appropriate actions to
What Is an FMEA?

remove or minimize these failures. It is imperative therefore to be familiar with the vocabulary and its significance to the FMEA. Following is a list of key terms used in all FMEAs.

*Function*: What is the intent of the design or process? Specifically, the following items should be addressed:

- Describe the design/process intent or engineering requirement.
- Write it in verb-noun measurable format.
- Represent all wants, needs, and requirements, both spoken and unspoken for all customers and systems.

*Failure Mode*: How can this function fail? There are usually six minimum failures for each function. They are:

1. No function. It does not work.
2. Degradation. The function over time fails.
3. Intermittent. The function sometimes works and sometimes does not.
4. Partial. The function does not work at full cycle.
5. Unintended. The function acts in a surprise manner.
6. Over function. The function does more than intended.

*Effect of Failure*: Describe the consequence(s) of failure. Typical considerations for design are:

- Part/sub-component
- Next higher assembly
- System
- Total product (as in vehicle)
- Government regulations
- Customer (internal and end user)

Typical considerations for process are:

- Operator safety
- Next user
- Downstream users
• Machines/equipment
• Total process operation
• Ultimate customer
• Compliance with government regulations

Severity (S): How serious is the effect on the failure mode? Generally the severity is the worst numerical effect value. Severity is a relative ranking within the scope of the individual FMEA. A reduction in severity ranking index can be effected only through a design change.

Classification: If severity values are 9 or 10, that is where safety and/or government regulations are effected. This means that the classification column should reflect the potential critical characteristics. When that happens, the team must:
• Develop a proactive design recommended action.
• Ensure that information is communicated to the PFMEA after causes have been generated.

If the severity is >4, this implies that the item is significant and therefore proactive actions should be recommended. In some industries if the severity is 4–8 and the occurrence is >3, the item is considered to be significant and appropriate proactive actions are necessary.

Possible Cause(s): This is an indication of a design weakness, the consequence of which is the failure mode. In other words: What causes the function to fail? A good source for answering this question may be found in the P-diagram and the interface matrix. For design concerns, a good rule to follow is to assume that:
• The item is manufactured and assembled within engineering specifications.
• The design may include a deficiency that may cause unacceptable variation (e.g., misbuilds, errors, etc.).

For process concerns, a good rule to follow is to ask:
• If incoming parts are correct, what would cause the operation to fail in this manner?
• What incoming sources of variation could cause the operation to fail in this manner?
Common ways to determine causes are:

- Brainstorming.
- 5 Whys method.
- Fishbone diagram.
- Fault tree analysis (FTA). This model uses a tree to show the cause-and-effect relationship between a failure mode and the various contributing causes. The tree illustrates the logical hierarchy branches from the failure at the top to the root causes at the bottom.
- Classic five-step problem-solving process:
  1. What is the problem?
  2. What can I do about it?
  3. Put a star on the “best” plan.
  4. Do the plan!
  5. Did your plan work?
- Kepner Tregoe method (analysis that asks, what is the problem, what is not the problem).
- Discipline (8D).
- Experience:
  - Knowledge of physics and the sciences
  - Knowledge of similar products
- Experiments. When many causes are suspect or specific cause is unknown:
  - Classical
  - Taguchi methods

Occurrence (O): How often does the cause of the function happen? Occurrence is the likelihood that a specific cause/mechanism (listed in the previous column) will occur during the life of the function (design or process). The likelihood of occurrence ranking number has a relative meaning rather than an absolute value. Preventing or controlling the causes/mechanisms of the failure mode through a design change or design process change (e.g., design
checklist, design review, design guide) is the only way a reduction in the occurrence ranking can be effected. At this point the highest S × O (criticality) failure mode–cause combinations determine if an appropriate recommended action can be taken. An action should be posted for any cause that received an occurrence rating of 10 (where the team could not reach consensus or where occurrence could not be estimated).

**Prevention Controls:** This item is for the planning controls in order to avoid the cause from happening or to reduce the rate of occurrence.

**Detection Controls:** This item identifies the effectiveness of the planning controls, which may be analytical, physical methods, before the item is released to production.

**Detection (D):** Detection is the rank associated with the best type of design control from the list in the previous column. Detection is a relative ranking, within the scope of the individual FMEA. To achieve a lower ranking, generally the planned design control (e.g., validation and/or verification activities) has to be improved.

**RPN:** This is the result of S × O × D. Based on the highest number, the priority is set for recommended action. However, RPN is not always the best importance indicator since the severity or occurrence sometimes dominates the RPN factor. A better way to set priorities for a completed FMEA might be to first use the high severity number (9 or 10 and, in some organizations, 5 and higher by agreement of the customer and supplier) followed by the highest criticality indices (S × O) and then the highest RPN numbers. Each failure cause must have its own RPN calculated. Be sure to recognize that some failure modes have the same solution or follow-up activity.

**Recommendations:** These are actions that must be taken to minimize or eliminate the cause of the failure. To be effective the actions must be (1) appropriate, (2) applicable, (3) completed within a reasonable time, and (4) cost-effective. This means that each action must be assigned to an individual with a specific due date. If no action is planned, enter “None” or “None at this time.” All identified corrective actions should first be directed at the highest ranked concerns and critical items. In fact, the aim should be prevention and not increasing detection methods.

**Actions Taken:** Here we identify the specific action that is taken from the list of the recommendations. An FMEA without posi-
tive and effective actions to prevent failures is not of much use. Once the actions have been implemented, the estimated values or “the future” become “the present” and can be incorporated into the left-hand side of the form on the next FMEA. After action has been taken, enter a brief description of the action and its effective or actual completion date. At this point re-rate the severity, occurrence, or detection based on the actions taken and enter into the revised severity, revised occurrence or revised detection columns as applicable.

*New Severity:* In order for a new number to be entered here, some or all the following must happen. (1) Change the design, (2) change standards, (3) change procedures and/or instructions, (4) change policies, and (5) make process changes. Warning! There are two schools of thought here. One is that once the severity is identified it remains the same unless the design is changed. The second is that the severity may change if redundant systems are in place and/or if there is a combination of the five items mentioned.

*New Occurrence:* The number may change if redundant systems or one of the following items is incorporated in the design or process. (1) Change the design, (2) change standards, (3) change procedures and/or instructions, (4) change policies, and (5) make process changes.

*New Detection:* The number may change if controls are added or one of the following items is incorporated in the design or process. (1) Change the design, (2) change standards, (3) change procedures and/or instructions, (4) change policies, and (5) make process changes.

*New RPN:* The number will change if any of the contributing factors change in any way. The factors that make up the RPN are severity, occurrence, and detection. Any change in these will change the RPN.
All FMEAs have a robustness focus. This means that robustness tools are inputs to a good FMEA. A pictorial view is shown in Table 5.1.

**BOUNDARY DIAGRAM**

The idea of a boundary diagram is to identify as well as represent other components in the higher-level assembly. Typically, the boundary diagram includes all system attachments and mechanisms as well as interfaces with:

- Other systems
- Manufacturing/assemble tools
- Servicing/customer adjustment
- All user interfaces

Once that representation has been accomplished then the boundary diagram is constructed, usually with dotted lines around the item of concern for the FMEA. This means that the boundary diagram considers what is best included and excluded in the analysis of the particular FMEA. The boundary in essence has two functions: It is used (1) to aid the identification of the possible effects of failures, and (2) once the scope is defined, to focus the support team in the process of conducting the FMEA. A typical diagram is shown in Figure 5.1.

In this case items G, B, and C will be considered for the FMEA.
The interface matrix is used to identify and prioritize interactions between items of concern and their four parameters. Specifically, an interface matrix:

- Acts as an input to a design FMEA.
- Identifies and quantifies the strength of system interactions by:
  - Showing whether the relationship is necessary or adverse
  - Identifying the type of relationship

A typical interface matrix is shown in Table 5.2.
**P-DIAGRAM**

The P-diagram is a method for identifying the ideal function as well as the parameters that will prevent the ideal function from occurring. It is recommended for the design FMEA because it:

- Is a structured tool to identify intended inputs and outputs for a function
- Describes noise factors, control factors, ideal function, and error states
- Assists in the identification of:
  - Potential Causes for Failure
  - Failure Modes

---

**Table 5.2** Interface matrix.

<table>
<thead>
<tr>
<th>Individual Items of Concern</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>P E P</td>
<td>P E P</td>
<td>P E P</td>
<td>P E P</td>
</tr>
<tr>
<td>I M I M I M I M I M I M I M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>P E P</td>
<td>P E P</td>
<td>P E P</td>
<td>P E P</td>
</tr>
<tr>
<td>I M I M I M I M I M I M I M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>P E P</td>
<td>P E P</td>
<td>P E P</td>
<td>P E P</td>
</tr>
<tr>
<td>I M I M I M I M I M I M I M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>P E P</td>
<td>P E P</td>
<td>P E P</td>
<td>P E P</td>
</tr>
<tr>
<td>I M I M I M I M I M I M I M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Each of the letters may be represented with numbers such as:

- **P** = Physical touching
  - +2 = interaction is necessary
  - +1 = interaction is beneficial but not absolutely necessary for functionality
  - 0 = interaction does not affect functionality
  - −1 = interaction causes negative effects but does not prevent functionality
  - −2 = interaction must be prevented to achieve functionality
– Potential Effects of Failure
– Current Controls
– Recommended Actions

The relationship of input → process → output is the ideal function. This means that all inputs are utilized for the expected output. No waste! The P-diagram is based on the following parameters:

• **Input** refers to the items that are used in the process. They may be manpower, machine, method, material, measurement, or environment.

• **Process** is the “value added” activity under consideration. It is the reason for existence.

• **Output** is the expected result of the process.

• **Errors** are the items that contribute to less than 100% of output—the failures.

• **Control** items are the items that we can have in the process to make sure that the output is at optimum—the actions that mitigate the failures so that the output is reached.

• **Noise** factors are the factors that contribute to customer usage, piece-to-piece variation, external environment, interactions, and changes over time without there being an adverse reaction to the process.

A pictorial view is shown in Figure 5.2.

![P-diagram](image)

**Figure 5.2** A typical P-diagram
The generic form for all types of FMEA is very simple and straightforward. For certain industries, however, this form may be modified to reflect the needs of that industry. Figure 6.1 presents a generic form that identifies all needed information for reducing or eliminating a root cause from either a design and/or a process. The reader should note that the only difference between the design and process forms is the header that identifies whether it is a design or process.

The rankings or criteria as they are commonly known are not standardized. In other words, there are no criteria that everyone is using for all FMEAs and industries. What is important to know is that the criteria must be based on logic, knowledge, and experience about the task at hand. Having said that, it is also important for the reader to recognize that certain industries such as aerospace, nuclear, automotive, and others have indeed recommended criteria lists for severity, occurrence, and detection. If your industry has these guidelines and you want to deviate from them, it is acceptable to do so, but you must attach an addendum with the FMEA to show the different criteria so that when someone else reads the FMEA, they will know the deviations from the suggested guideline.

In the section for DFMEA and PFMEA we will identify criteria that are considered very common and used in several industries. Here we summarize some key items of concern for any FMEA and present a general strategy for reducing risk. A more detailed analysis is covered in the section of the specific FMEAs.
SEVERITY RATING

Severity is a relative rating of the seriousness of the effect. Specifically:

- Severity is a numerical rating of the impact on customers.
- When multiple effects exist for a given failure mode, enter the worst-case severity on the worksheet to calculate risk. (This is the accepted method for the automotive industry and for the SAE J1739 standard. It should also be recognized that some companies, while they will accept this approach, prefer to have individual ratings for each of the effects.)
- In cases where severity varies depending on timing, use the worst-case scenario.

Reducing Severity (or Reducing the Severity of the Failure Mode Effect)

- Design or manufacturing process changes are necessary.
- Focus on reducing severity in order of: changing design, process, standards, procedures, and/or instructions.
OCCURRENCE RATING

This is the estimated number of frequencies or cumulative number of failures (based on experience) that will occur (in our design concepts for a given cause over the “intended life of the design”). Example: The cause of staples falling out is soft wood. The likelihood of occurrence is a 9 if we picked balsa wood but a 2 if we choose oak.

Just like severity, there are standard tables for occurrence for each type of FMEA. The ratings on these tables are estimates based on experience and/or similar products or processes. Nonstandard occurrence tables may also be used, based on specific characteristics. However, reliability expertise is needed to construct occurrence tables. (Typical characteristics may be historical failure frequencies, Cpk’s theoretical distributions, and reliability statistics.)

Reducing Occurrence (or Reducing the Frequency of the Cause)

• Design or manufacturing process changes are necessary.

• Focus on reducing occurrence in order of: changing design, process, standards, procedures, and/or instructions.

DETECTION RATING

Detection rating is a numerical rating of the probability that a given set of controls will discover a specific cause or failure mode to prevent bad parts from leaving the operation/facility or getting to the ultimate customer. Among the key concerns:

• Assuming that the cause of the failure did occur, assess the capabilities of the controls to find the design flaw or prevent the bad part from leaving the operation/facility. In the first case, the DFMEA is at issue. In the second case the PFMEA is of concern.

• When multiple controls exist for a given failure mode, record the best (lowest) to calculate risk.

• In order to evaluate detection, there are appropriate tables for both design and process. Just as before, however, if there is a need to alter them, remember that the change and approval must be done by the FMEA team with consensus.
Reducing Detection (or Increasing the Probability of Detection)

- Improving the detection controls is generally costly, reactive, and does not do much for quality improvement, but it does reduce risk.

- Increased frequency of inspection, for example, should only be used as a last resort. It is not a proactive corrective action.

CLASSIFICATION AND CHARACTERISTICS

These characteristics must be classified according to risk impact:

- Severity 9, 10: Highest Classification (Critical)
  *These kinds of characteristics are product- or process-related that:
  - May affect compliance with government or federal regulations (e.g., EPA, OSHA, FDA, FCC, FAA)
  - May affect safety of the customer
  - Require specific actions or controls during manufacturing to ensure 100% compliance

- Severity between 5–8 and Occurrence Greater than 3: Secondary Classification (Significant)
  *These characteristics are product- or process-related that:
  - Are noncritical items that are important for customer satisfaction (e.g., fit, finish, durability, appearance)
  - Should be identified on drawings, specifications, or process instructions to ensure acceptable levels of capability

- High RPN: Secondary Classification

Product Characteristics/“Root Causes”

- Examples include size, form, location, orientation, or other physical properties such as color, hardness, or strength.

Process Parameters/“Root Causes”

- Examples include pressure, temperature, current, torque, speed, feeds, voltage, nozzle diameter, time, chemical concentrations, cleanliness of incoming part, and ambient temperature.
UNDERSTANDING AND 
CALCULATING RISK

Without risk, there is very little progress! Risk is inevitable in any system, 
design, or manufacturing process.

The FMEA process aids in identifying significant risks, then helps to 
minimize the potential impact of risk. It does that through the risk priority 
number or, as it is commonly known, the RPN index. In the analysis of the 
RPN, make sure to look at risk patterns rather than just a high RPN.

The RPN is the product of severity, occurrence, and detection or:

\[ \text{RISK} = \text{RPN} = S \times O \times D \]

Obviously the higher the number of the RPN the more the concern. 
A good rule of thumb analysis to follow is 95%. That means that you will 
address all failure modes with a 95% confidence. It turns out the magic num-
ber is 50 \([S = 10 \times O = 10 \times D = 10] - (1000 \times .95)\]. This number of course is 
only relative to what the total FMEA is all about and it may change as the 
risk increases in all categories and in all causes.

Special risk priority patterns require special attention through specific 
action plans that will reduce or eliminate the high risk factor. They are 
identified through:

1. High RPN
2. Any RPN with a severity of 9 or 10 and an occurrence >2
3. Area chart

The area chart in Figure 6.2 uses only severity and occurrence, which 
is more proactive.

![Area chart showing priority levels](image-url)
The reader should recognize that this is the traditional and most common method of determining risk. However, there are other ways that are in fact more sensitive and beneficial. For example, the priority may be identified by:

1. Severity ranking of >5
2. Severity 3–4 and occurrence >4 (criticality)
3. RPN

**DRIVING THE ACTION PLAN**

- For each recommended action, the FMEA team must:
  - Plan for implementation of recommendations.
  - Make sure that recommendations are followed, improved, and completed.
- Implementation of action plans requires answering the classic questions:
  - Who (will take the lead)?
  - What (specifically is to be done)?
  - Where (will the work get done)?
  - Why (which should be obvious)?
  - When (should the actions be done)?
  - How (will we start)?
- Accelerate implementation by getting buy-in (ownership).
- Draw out and address objections. When plans address objections in a constructive way, stakeholders feel ownership in plans and actions. Ownership aids in successful implementation!
- Typical questions that begin a fruitful discussion are:
  - Why are we . . . ?
  - Why not this?
  - What about this?
  - What if . . . ?
• Timing and actions must be reviewed on a regular basis to:
  – Maintain a sense of urgency
  – Allow for ongoing facilitation
  – Ensure work is progressing
  – Drive team members to meet commitments
  – Surface new facts that may affect plans

• Fill in the actions taken:
  – The Actions column should not be filled out before the actions are totally complete.

Record final outcomes in the Action Plan and Action Results section of the FMEA form. Remember, because of the actions you have taken you should expect changes in severity, occurrence, detection, RPN, and new characteristic designations.
There are many types of FMEAs, each one specifically relating the causes of failures to the specific industry. For example, one may encounter an FMEA in areas such as pharmaceutical, environmental, industrial, defense, service, healthcare, software, equipment, aerospace, automotive, petroleum, oil/gas, transportation, nuclear, marine, and many other specialized forums.

However, as variable as FMEAs may be, fundamentally they all are the same because they all try to prevent failures from happening or minimize their effect if they do. Because of the similarity in both analysis and reaction approach, these different FMEAs may be categorized primarily in the following categories shown in Table 7.1.

The reader will notice that even though we said that there are many FMEAs only five are identified in the table. The reason is because all others fall into either the design or process category of FMEA. The difference is in the application and specific terminology used for the specific application. For example, in the pharmaceutical industry we may use an FMEA to:

- Implement a plan that introduces redundancy into the process and interventions that are best suited to minimize risks of a product by using multiple stakeholders in the medication use process.

- Prepare strategic contingency plans to respond promptly to Food and Drug Administration (FDA) questions and requests that come late in the approval process.

- Establish a rigorous framework for the underlying approach to risk mitigation in the development of a proposed risk management process for a drug or biologic.

- Assess the risk management process performance through identified safety signals and adverse events of interest to assist in the
overall understanding of how, when, and where those risks may occur and ways to improve either the design and/or the process.

FMEA CHALLENGES

FMEA is a living document and as such it must be reviewed and updated as needed or at least once a year. Because of this constant possibility of review, the process of conducting an FMEA is considered to be a:

- Continuous brainstorming activity
- Lengthy consensus-building process
- Process that may not capture all possible issues
- Team-dependent environment only
- Process that determines and implements actions that drive reduction in risk
- Process that ensures that the high-risk failure modes are addressed
- Process that includes interfaces
There are many types of FMEAs. However, the most common ones are (1) concept, (2) design, and (3) process. All of them, without exception, follow the same methodology except for specific failures in the specific industries. For example, failures in the nuclear industry will be different from the health industry’s failures, and in turn they will be different from the automotive industry’s failures.

**CONCEPT**

**Purpose**

Fundamentally any FMEA analysis is a risk assessment methodology. However, in the case of a concept FMEA (CFMEA), the focus is in the feasibility phase for the new, innovative or updated designs. In a CFMEA only potential customers are considered.

**Use**

A CFMEA is used as part of an early engineering assessment to identify the potential feasibility of a system/subsystem/component.

**Benefit**

The CFMEA is a way to test “what-if situations” for new, revolutionary, innovative ways of doing things. The benefits of an upfront CFMEA are:

- It identifies the success of potentiality of engineering as well as economic feasibility.
• It identifies the necessity for redundant systems in the design.
• It identifies potential interaction and adverse effects of system/subsystem/components.
• It helps in the selection of optimized alternatives for a particular design.
• It helps in identifying as early as possible all potential effects of a proposed concept’s failure modes.
• It identifies potential system-level testing requirements.
• It helps determine the serious and/or catastrophic failures for the system/subsystem/component.

Form and Risk Criteria
For all intents and purposes, the form for the CFMEA is exactly the same as the one used for the DFMEA. However, most CFMEAs are never completed because of timing requirements. They usually stop after identifying major shortcomings in the proposed design, such as safety and/or government regulations. Another reason is that the timing requirements are overlapping with the DFMEAs and therefore the DFMEA is completed instead.

The criteria are also the same as that for the DFMEA. Very seldom they will be different. If they are, it is to accommodate the specific requirements of the industry.

Tools
• Computer simulation
• Functional diagrams
• Mathematical models
• Force field analysis
• Breadboard tests
• Laboratory tests on surrogate elements
• QFD
• Benchmarking
• Internal past corporate knowledge
DESIGN

Purpose
The purpose of a DFMEA is to perform a risk analysis of all reasonable design flows of the proposed product prior to manufacturing. To do this there are two assumptions in determining flaws/failures:

1. Item is manufactured and assembled within engineering specifications.
2. Design may include a deficiency that may cause unacceptable variation (misbuilds, errors, etc.) and may be addressed in the PFMEA.

Use
With an appropriate and applicable team in place, the primary use of DFMEA is to facilitate the following:

• Prevention planning
• Changing requirements
• Cost reduction
• Increased throughput
• Decreased waste
• Decreased warranty costs
• Reduction of non-value-added operations

Benefit
There are many benefits to conducting a DFMEA. Among the key benefits are the following:

• Increases the probability that potential failure modes and their effects have been considered in the design/development process
• Helps in the objective evaluation of design requirements and design alternatives
• Establishes a priority system for design improvements based on potential failure modes ranked according to their effect on the customer—generally the external customer
Chapter Eight

• Provides additional information to help plan thorough and efficient test programs for control
• Helps in the initial design for manufacturing and assembly requirements
• Provides an open issue format for recommending and tracking risk-reducing actions in both design and process
• Provides future reference to aid in analyzing field concerns

Form and Ratings

The form for the DFMEA is the same as the form in Figure 6.1. However, the ratings may differ from industry to industry and organization from organization; the ratings in Tables 8.1–8.3 are very common and can be used as a default guideline.

Special Note: There is nothing special about these guidelines. They may be changed to reflect the industry, the organization, the product/design, and/or process. To modify these guidelines:

1. List the entire range of possible consequences (effects).
2. Force rank the consequences from high to low.
3. Resolve the extreme values (rate 10 and rate 1).
4. Fill in the “other” ratings.
5. Use consensus.

Strategies for Lowering Risk: (Concept/Design)—High Severity or Occurrence

Change the Product Design to:

• Eliminate the failure mode cause or decouple the cause and effect.
• Eliminate or reduce the severity of the effect.
• Make cause less likely or impossible to occur.
• Eliminate function or eliminate part (functional analysis).

“Tools” to Consider

• QFD
• FTA
<table>
<thead>
<tr>
<th>Effect</th>
<th>Description</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No effect noticed by customer. The failure will not have any perceptible effect on the customer.</td>
<td>1</td>
</tr>
<tr>
<td>Very minor</td>
<td>Very minor effect, noticed by discriminating customers. The failure will have little perceptible effect on the discriminating customers.</td>
<td>2</td>
</tr>
<tr>
<td>Minor</td>
<td>Minor effect, noticed by average customers. The failure will have minor perceptible effect on average customers.</td>
<td>3</td>
</tr>
<tr>
<td>Very low</td>
<td>Very low effect, noticed by most customers. The failure will have some small perceptible effect on most customers.</td>
<td>4</td>
</tr>
<tr>
<td>Low</td>
<td>Primary product function is operational, however, at a reduced level of performance. Customer is somewhat dissatisfied.</td>
<td>5</td>
</tr>
<tr>
<td>Moderate</td>
<td>Primary product function operational, however, secondary functions inoperable. Customer is moderately dissatisfied.</td>
<td>6</td>
</tr>
<tr>
<td>High</td>
<td>Failure mode greatly affects product operation. Product or portion of the product is inoperable. Customer is very dissatisfied.</td>
<td>7</td>
</tr>
<tr>
<td>Very high</td>
<td>Primary product function is nonoperational but safe. Customer is very dissatisfied.</td>
<td>8</td>
</tr>
<tr>
<td>Hazard with warning</td>
<td>Failure mode affects safe product operation and/or involves nonconformance with government regulation <em>with</em> warning.</td>
<td>9</td>
</tr>
<tr>
<td>Hazard with no warning</td>
<td>Failure mode affects safe product operation and/or involves nonconformance with government regulation <em>without</em> warning.</td>
<td>10</td>
</tr>
</tbody>
</table>
• Benchmarking
• Brainstorming
• TRIZ (theory of inventive problem solving)

**Evaluate Ideas Using Pugh Concept Selection (Specific Examples)**

• Change material, increase strength, decrease stress.
• Add redundancy.
• Constrain usage (exclude features).
• Develop fail-safe designs and early-warning system.

**Strategies for Lowering Risk: (Concept/Design)—High Detection Rating**

*Change the Evaluation/Verification/Tests to:*

• Make failure mode easier to perceive.
• Detect causes prior to failure.
<table>
<thead>
<tr>
<th>Detection</th>
<th>Description</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost certain</td>
<td>Design control will almost certainly detect the potential cause of subsequent failure modes.</td>
<td>1</td>
</tr>
<tr>
<td>Very high</td>
<td>Very high chance the design control will detect the potential cause of subsequent failure mode.</td>
<td>2</td>
</tr>
<tr>
<td>High</td>
<td>High chance the design control will detect the potential cause of subsequent failure mode.</td>
<td>3</td>
</tr>
<tr>
<td>Moderate high</td>
<td>Moderately high chance the design control will detect the potential cause of subsequent failure mode.</td>
<td>4</td>
</tr>
<tr>
<td>Moderate</td>
<td>Moderate chance the design control will detect the potential cause of subsequent failure mode.</td>
<td>5</td>
</tr>
<tr>
<td>Low</td>
<td>Low chance the design control will detect the potential cause of subsequent failure mode.</td>
<td>6</td>
</tr>
<tr>
<td>Very low</td>
<td>Very low chance the design control will detect the potential cause of subsequent failure mode.</td>
<td>7</td>
</tr>
<tr>
<td>Remote</td>
<td>Remote chance the design control will detect the potential cause of subsequent failure mode.</td>
<td>8</td>
</tr>
<tr>
<td>Very remote</td>
<td>Very remote chance the design control will detect the potential cause of subsequent failure mode.</td>
<td>9</td>
</tr>
<tr>
<td>Very uncertain</td>
<td>There is no design control or the control will not or cannot detect the potential cause of subsequent failure mode.</td>
<td>10</td>
</tr>
</tbody>
</table>
“Tools” to Consider

- Benchmarking
- Brainstorming
- Process control (automatic corrective devices)
- TRIZ

Evaluate Ideas Using Pugh Concept Selection
(Some Specific Examples)

- Change testing and evaluation procedures.
- Increase failure feedback or warning systems.
- Increase sampling in testing or instrumentation.
- Increase redundancy in testing.

Tools

- Reliability modeling
- QFD
- Benchmarking
- Block diagram
- P-diagram
- Interface diagram
- Cause-and-effect diagram
- Function tree

PROCESS

Purpose

The purpose of a PFMEA is to resolve issues/concerns/problems in the process that result in low-quality product being shipped to the customer. Here the customer may be internal or external. There are two assumptions that must always be considered for optimum results:
1. Assuming incoming parts are correct, what would cause the operation to fail in this manner? In other words, the design is okay as is.

2. What incoming sources of variation could cause the operation to fail in this manner? As a last resort, evaluate issues that may be associated with design.

**Use**

Fundamentally, the PFMEA is used to identify each manufacturing step and to determine what functions are associated with each manufacturing process step, and then to ask:

1. What does the process step do to the part?
2. What are you doing to the part/assembly?
3. What is the goal, purpose, or objective of this process step?

There is no standardized form for a PFMEA. You may use the one in Figure 6.1 or a simplified form, such as the one shown in Figure 8.1. Any organization may modify these forms to reflect their own processes and needs.

**Benefit**

A PFMEA brings the following benefits:

- Identifies potential product-related process failure modes
- Assesses the potential customer effects of the failures
- Identifies the potential manufacturing or assembly process causes and identifies process variables on which to focus controls or monitoring
- Develops a ranked list of potential failure modes, establishing a priority system for corrective action considerations
- Documents the results of the manufacturing or assembly process
- Identifies process deficiencies
- Identifies confirmed critical characteristics and/or significant characteristics
- Identifies operator safety concerns
- Feeds information on design changes required and manufacturing feasibility back to the designers
<table>
<thead>
<tr>
<th>Item/function</th>
<th>Potential failure mode</th>
<th>Potential effect(s) of failure</th>
<th>Severity</th>
<th>Class</th>
<th>Potential cause/mechanism of failure</th>
<th>Occurrence</th>
<th>Current process controls (prevent/direct)</th>
<th>Detection</th>
<th>RPN</th>
<th>Recommended action(s)</th>
<th>Responsibility and target completion date</th>
<th>Responsibility for the recommended action</th>
<th>Action results</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the process step?</td>
<td>In what ways does the key input go wrong?</td>
<td>What is the impact on the key output variables (customer requirements) or internal requirements?</td>
<td>How severe is the effect to the customer?</td>
<td>How often does cause of FM occur?</td>
<td>What causes the key input to go wrong?</td>
<td>How often does cause of FM occur?</td>
<td>What are the existing controls and procedures that prevent either the cause or the failure mode?</td>
<td>How well can you detect cause or FM?</td>
<td>What are the actions for reducing the occurrence of the cause, or improving detection?</td>
<td>Who is responsible for the recommended action?</td>
<td>What are the completed actions to take with the recalculated RPM? Be sure to include completion month/year</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 8.1 A typical PFMEA
Ratings

There are no standard or universal criteria for ranking any FMEA. However, typical rating guidelines are shown in Tables 8.4–8.6.

Special Note: There is nothing special about these guidelines. They may be changed to reflect the industry, the organization, the product/

Table 8.4 PFMEA—severity.

<table>
<thead>
<tr>
<th>Effect</th>
<th>Description</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No effect noticed by customer. The failure will not have any effect on the customer.</td>
<td>1</td>
</tr>
<tr>
<td>Very minor</td>
<td>Very minor disruption to production line. A very small portion of the product may have to be reworked. Defect noticed by discriminating customers.</td>
<td>2</td>
</tr>
<tr>
<td>Minor</td>
<td>Minor disruption to production line. A small portion (&lt;5%) of product may have to be reworked online. Process up but minor annoyances.</td>
<td>3</td>
</tr>
<tr>
<td>Very low</td>
<td>Very low disruption to production line. A moderate portion (&lt;10%) of very low product may have to be reworked online. Process up but minor annoyances.</td>
<td>4</td>
</tr>
<tr>
<td>Low</td>
<td>Low disruption to production line. A moderate portion (&lt;15%) of product may have to be reworked online. Process up but some minor annoyances.</td>
<td>5</td>
</tr>
<tr>
<td>Moderate</td>
<td>Moderate disruption to production line. A moderate portion (&gt;20%) of product may have to be scrapped. Process up but some inconveniences.</td>
<td>6</td>
</tr>
<tr>
<td>High</td>
<td>Major disruption to production line. A portion (&gt;30%) of product may have to be scrapped. Process may be stopped. Customer dissatisfied.</td>
<td>7</td>
</tr>
<tr>
<td>Very high</td>
<td>Major disruption to production line. Close to 100% of product may have to be scrapped. Process unreliable. Customer very dissatisfied.</td>
<td>8</td>
</tr>
<tr>
<td>Hazard with warning</td>
<td>May endanger operator or equipment. Severely affects safe process operation and/or involves noncompliance with government regulations. Failure will occur with warning.</td>
<td>9</td>
</tr>
<tr>
<td>Hazard with no warning</td>
<td>May endanger operator or equipment. Severely affects safe process operation and/or involves noncompliance with government regulations. Failure occurs without warning.</td>
<td>10</td>
</tr>
</tbody>
</table>
Chapter Eight

Table 8.5 PFMEA—occurrence.

<table>
<thead>
<tr>
<th>Occurrence</th>
<th>Description</th>
<th>Frequency</th>
<th>$C_{pk}$</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote</td>
<td>Failure is very unlikely, no failures associated to similar processes.</td>
<td>$&lt;1$ in $1,500,000$</td>
<td>$&gt;1.67$</td>
<td>1</td>
</tr>
<tr>
<td>Low</td>
<td>Few failures. Isolated failures associated with like processes.</td>
<td>1 in 150,000</td>
<td>1.50</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 in 15,000</td>
<td>1.33</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 in 2000</td>
<td>1.17</td>
<td>4</td>
</tr>
<tr>
<td>Moderate</td>
<td>Occasional failures associated with similar processes, but not in major proportions.</td>
<td>1 in 400</td>
<td>1.00</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 in 80</td>
<td>0.83</td>
<td>6</td>
</tr>
<tr>
<td>High</td>
<td>Repeated failures. Similar processes have often failed.</td>
<td>1 in 20</td>
<td>0.67</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 in 8</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>Very high</td>
<td>Process failure is almost inevitable.</td>
<td>1 in 3</td>
<td>0.51</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$&gt;1$ in 2</td>
<td>0.33</td>
<td>10</td>
</tr>
</tbody>
</table>

design, and/or process. Keep in mind that to modify these guidelines, you should:

1. List the entire range of possible consequences (effects).
2. Force rank the consequences from high to low.
3. Resolve the extreme values (rate 10 and rate 1).
4. Fill in the “other” ratings.
5. Use consensus.

Manufacturing Process Control Matrix

In any process there are several dominant factors that should be evaluated for failures. Table 8.7 shows some of the factors involved and the appropriate data used in the evaluation and control of these failures.
The Common Types of FMEAs

Manufacturing Process Control Examples

**Statistical Process Control**

- X-bar/R control/charts (variable data)
- Individual X-moving range charts (variable data)
- $p$-, $n$-, $u$-, and $c$-charts (attribute data)

**Nonstatistical Control**

- Check sheets, checklists, setup procedures, operational definitions/instruction sheets
- Preventive maintenance (PM)
  - Tool usage logs/change programs
  - Mistake proofing/error proofing/poka-yoke

Table 8.6 PFMEA—detection.

<table>
<thead>
<tr>
<th>Detection</th>
<th>Description</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost certain</td>
<td>Process control will almost certainly detect or prevent the potential cause of subsequent failure mode.</td>
<td>1</td>
</tr>
<tr>
<td>Very high</td>
<td>Very high chance process control will detect or prevent the potential cause of subsequent failure mode.</td>
<td>2</td>
</tr>
<tr>
<td>High</td>
<td>High chance the process control will detect or prevent the potential cause of subsequent failure mode.</td>
<td>3</td>
</tr>
<tr>
<td>Moderate high</td>
<td>Moderately high chance the process control will detect or prevent the potential cause of subsequent failure mode.</td>
<td>4</td>
</tr>
<tr>
<td>Moderate</td>
<td>Moderate chance the process control will detect or prevent the potential cause of subsequent failure mode.</td>
<td>5</td>
</tr>
<tr>
<td>Low</td>
<td>Low chance the process control will detect or prevent the potential cause of subsequent failure mode.</td>
<td>6</td>
</tr>
<tr>
<td>Very low</td>
<td>Very low chance the process control will detect or prevent the potential cause of subsequent failure mode.</td>
<td>7</td>
</tr>
<tr>
<td>Remote</td>
<td>Remote chance the process control will detect or prevent the potential cause of subsequent failure mode.</td>
<td>8</td>
</tr>
<tr>
<td>Very remote</td>
<td>Very remote chance the process control will detect or prevent the potential cause of subsequent failure mode.</td>
<td>9</td>
</tr>
<tr>
<td>Very uncertain</td>
<td>There is no process control or the control will not or cannot detect the potential cause of subsequent failure mode.</td>
<td>10</td>
</tr>
</tbody>
</table>
It is very important to recognize that inspection is not a very effective control because it is a reactive task and quite often very subjective, especially with attribute data.

<table>
<thead>
<tr>
<th>Dominance Factor</th>
<th>Attribute Data</th>
<th>Variable Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup</td>
<td>Check sheet, Checklist</td>
<td>X-bar/R chart, X-MR chart</td>
</tr>
<tr>
<td>Machine</td>
<td>$p$- or $c$-chart, Check sheet</td>
<td>Run chart, X-bar/R chart, X-MR chart</td>
</tr>
<tr>
<td>Operator</td>
<td>Check sheet, Run chart</td>
<td>X-bar/R chart, X-MR chart</td>
</tr>
<tr>
<td>Component/material</td>
<td>Check sheet, Supplier information</td>
<td>Check sheet, Supplier information</td>
</tr>
<tr>
<td>Tool</td>
<td>Tool logs, Check sheet, $p$- or $c$-chart</td>
<td>Tool logs, Capability study, X-MR chart</td>
</tr>
<tr>
<td>Preventive maintenance</td>
<td>Time to failure chart, Supplier information</td>
<td>Time to failure chart, Supplier information, X-MR chart</td>
</tr>
<tr>
<td>Fixture/pallet/work holding</td>
<td>Time to failure chart, Check sheet, $p$- or $c$-chart</td>
<td>Time to failure chart, X-bar/R chart, X-MR chart</td>
</tr>
<tr>
<td>Environment</td>
<td>Check sheet</td>
<td>Run chart, X-MR Chart</td>
</tr>
</tbody>
</table>

- Training and experience
- Automated inspection
- Visual inspection
Strategies for Lowering Risk: (Manufacturing)—High Severity or Occurrence

*Change the Product or Process Design to:*

- Eliminate the failure *cause* or decouple the *cause and effect*.
- Eliminate or reduce the *severity* of the *effect* (recommend changes in design).

*“Tools” to Consider*

- Benchmarking
- Brainstorming
- Mistake proofing
- TRIZ

*Evaluate Ideas Using Pugh Concept Selection (Specific Examples):*

- Developing a “robust design” (insensitive to manufacturing variations)
- Changing process parameters (time, temperature, etc.)
- Increasing redundancy and adding process steps
- Altering process inputs (materials, components, consumables)
- Using mistake proofing (poka-yoke) to reduce handling

Strategies for Lowering Risk: (Manufacturing)—High Detection Rating

*Change the Process Controls to:*

- Make failure mode easier to perceive.
- Detect causes prior to failure mode.

*“Tools” to Consider*

- Benchmarking
- Brainstorming
Chapter Eight

Evaluate Ideas Using Pugh Concept Selection (Specific Examples)

- Change testing and inspection procedures/equipment.
- Improve failure feedback or warning systems.
- Add sensors/feedback or feed forward systems.
- Increase sampling and/or redundancy in testing.
- Alter decision rules for better capture of causes and failures (i.e., more sophisticated tests).

At this stage, now you are ready to enter a brief description of the recommended actions, including the department and individual responsible for implementation, as well as both the target and finish dates on the FMEA form. If the risk is low and no action is required write “No action needed.”

For each entry that has a designated characteristic in the “class” (identification) column:

- Review the issues that impact cause/occurrence, detection/control, or failure mode.
- Generate recommended actions to reduce risk.
- Examine special RPN patterns. They suggest that certain characteristics/root causes are important risk factors that need special attention.

Guidelines for Process Control System

1. Select the process.
2. Conduct the FMEA on the process.
3. Conduct gauge system analysis.
4. Conduct a process potential study.
5. Develop a control plan.
6. Train operators in control methods.
7. Implement the control plan.
8. Determine long-term process capability.
9. Review the system for continual improvement.
The Common Types of FMEAs

10. Develop an audit system.
11. Institute improvement actions.

Tools

- Mistake proofing
- Inspection
- Cause-and-effect diagram
- Affinity diagram
- Engineering testing (specific to the cause being evaluated)

EQUIPMENT

An equipment FMEA (EFMEA) is a systematic approach that applies the generic form of an FMEA to aid the thought process used by engineers to identify the equipment’s potential failure modes and their effects. The focus however is on the operator’s safety.

Purpose

The basic purposes of any EFMEA are to:

1. Identify potential failure modes and rate the severity of their effects.
2. Rank-order potential design and process deficiencies.
3. Help engineers focus on eliminating equipment design and process concerns and help prevent problems from occurring.

Use

Fundamentally there are three reasons for using EFMEA. They are to:

1. Identify potential failure modes that may adversely affect environment safety.
2. Identify potential failure modes that may adversely affect operator safety.
3. Identify potential design deficiencies before releasing machinery to production.
Benefit

There are at least five basic benefits in completing an EFMEA. They are:

1. Improving the quality, reliability, and safety of the customer’s equipment
2. Improving the company’s image and competitiveness
3. Helping to increase customer satisfaction
4. Reducing equipment development, timing, and cost
5. Documenting and tracking actions taken to reduce risk

General Information about EFMEA

The EFMEA is a special FMEA; as such, some items have to be addressed specifically for equipment:

How is an EFMEA prepared? The equipment supplier is responsible for preparing the initial EFMEA. The customer generally only assists as a team member.

When is an EFMEA started? Generally, there are four points of concern for when the EFMEA should be started. They are:

1. When new systems, subsystems components, equipment, and processes are being designed.
2. When existing equipment or processes are modified in any way.
3. When carryover equipment and/or processes are used in new applications or new environments.
4. After completing a problem-solving methodology (e.g., 8D) to prevent recurrence of a problem.

Who prepares the EFMEA? The EFMEA process is a team effort between the supplier and customer. The team should be cross-functional and multidisciplinary. The responsible equipment engineer is the leader of any EFMEA team. However, the supplier’s equipment design engineer is expected to involve representatives from all affected activities. It is suggested that at a minimum the following representation should be part of an active team:
It is imperative that the team must realize that the team members may change as the equipment matures through the design, build, and test phases. Also, team members may be added as ad hoc personnel to aid in specific issues but not as core team members.

**Who updates the EFMEA?** The supplier’s design engineer is responsible for keeping the EFMEA up to date. It is also the responsibility of suppliers to keep their own copy of the EFMEA.

**When is an EFMEA updated?** There are at least three conditions for updating the EFMEA:

1. Whenever a new machine’s project timeline changes
2. Whenever design modifications or new failure modes are discovered
3. Whenever a change is being considered to a machine’s design, application, environment, material usage, or operational process

**When is an EFMEA completed?** It is considered complete when the equipment is installed, has passed its reliability testing, and is signed off by the plant staff. However, remember that an EFMEA, just like the traditional FMEA, is a living document and must be updated whenever significant changes occur in the equipment’s design and/or application.

**When can an EFMEA be discarded?** Depending on the industry it varies from cradle to grave (nuclear industry) to specific years as defined in the record retention requirement of the organization’s policies and procedures. The retention period is reviewed regularly for effectiveness and appropriateness and is part of the organization’s quality system.

**What is the form that may be used in an EFMEA?** A typical form for the EFMEA is the shown in Figure 8.2. Obviously it may be modified to reflect specific issues with a particular industry and/or equipment.
Form

Figure 8.2 is coded with numbers from 1 to 23. The explanations follow the form.

_FMEA number (1):_ Each FMEA must have a number to help track the document and its information. After all, the FMEA is a controlled document.

_Equipment Name (2):_ It is used to identify the equipment’s name for reference and accountability.

_Design responsibility (3):_ This is the place where the design responsibility is identified. For example, it may be the supplier and/or specific department or group responsible for the design of the particular equipment.

_Prepared by (4):_ This item must identify the name, phone number, and e-mail for the primary contact for the EFMEA.

_Model (5):_ This identifies the model of the equipment, if applicable.

_Review Date (6):_ It is the initial date that the EFMEA started. This date should fall within the design and development phase of the equipment’s life-cycle process. Sometimes this is called original date.

_Page of_: Identifies all pages of the FMEA for reference purpose.

_FMEA Date (7):_ This is the initial date the EFMEA is completed or the revision date.

_Core Team (8):_ This item covers all the team members that participate in the EFMEA. It should identify them by name, department, telephone, e-mail, and address.

_System, Subsystem, Component (9a):_ This is information used to classify the analyzed machine’s subsystem. The intent here is to identify the hierarchy of the machine so that it is quickly formulated and then transferred to the column listing all the subsystems in the appropriate order. (Special Note: The subsystem name column and the function and performance requirements column have the same location. However, to make the distinction easier it is suggested that the two be separated.)

_Function or Performance Requirements (9b):_ This column relates directly to the subsystem name information and lists all the subsystem’s associated functions and the design intent of that system. This column provides information that corresponds to each of the machine’s identified subsystems. In addition, using these four recommended steps to fill out this column simplifies subsystem function identification: (1) brainstorm, (2) evaluate the results of brainstorming, (3) convert to verb-noun format, and (4) establish the appropriate and applicable measurement system.

_Potential Failure Mode (10):_ This is defined as the manner in which the equipment could potentially fail to meet the design intent. These failures are generally the ones that the operator sees. Typically, there are two approaches for identifying these failures: (1) functional, which relates to
<table>
<thead>
<tr>
<th>FMEA number (1)</th>
<th>Prepared by (4)</th>
<th>Page ___ of ___</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment name (2)</td>
<td>Model (5)</td>
<td>FMEA date (7)</td>
</tr>
<tr>
<td>Design responsibility (3)</td>
<td>Review date (6)</td>
<td>Core team (8)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System, subsystem, component (9a)</th>
<th>Function or performance requirements (9b)</th>
<th>Potential failure mode (10)</th>
<th>Severity (12)</th>
<th>Classification (13)</th>
<th>Potential causes of failure (14)</th>
<th>Occurrence (15)</th>
<th>Prevention controls and equipment controls (16)</th>
<th>Current design and equipment controls (17)</th>
<th>Detection (18)</th>
<th>Revised RPN (23)</th>
<th>Action results</th>
</tr>
</thead>
</table>

**Figure 8.2** Explanation of the EFMEA form
some form of loss of function; and (2) hardware, when detailed part designs are available. If the failures are identified as part of a static model that means that the identified failures have no effect on other failures of other subsystems or components under investigation. It is very important for the team to identify as many failures as possible in the design phase because this action will reduce the number of failures that may be seen during the debug phase, start-up, and the useful life of the equipment.

**Potential Effects of Failure (11):** These represent the potential consequences of the failure mode. Typical areas of concern may be breakdowns; reduced cycle time; tooling; setup and adjustments; defective parts; government regulations; idling and minor stoppages; and safety. Of these, special attention must be given to government regulations and safety issues.

**Severity (12):** Represents the seriousness of the effects listed in column 11 and is made up of three components: (1) safety, (2) equipment downtime, and (3) product scrap. Each effect (in column 11) is assigned a ranking between 1 and 10 from the agreed-on criteria and the highest ranking is entered in this column. Only the highest ranking is entered because it represents the most serious effect that may occur, if the failure mode occurs.

**Classification (13):** In the EFMEA the only time that this column is used is if the severity is 9 or 10, which has to do with government regulations or operator safety. If indeed it is used, then action must be taken to correct the problem. Typical designations are OS (for operator safety) and Y (which stands for government regulations).

**Potential Causes of Failure (14):** This column represents design deficiency or process variation that results in the failure mode. To have an effective EFMEA, all first level failure mode causes must be identified and listed in this column. This may be accomplished by considering the following three questions: (1) What would cause the subsystem/component to fail in this manner? (2) What circumstances could cause the subsystem/component to fail to perform its function? (3) What can cause the subsystem/component to fail to deliver its intended function? To help in this identification process the team should consider the causes relating to the highest risk failure modes and then review the following for validating their selected options: (1) historical test reports, (2) warranty data reports, (3) surrogate EFMEAs, (4) concern reports, (5) field reports, and (6) product recalls. The team must remember that all 9 or 10 severity rankings must identify the root cause of the failure mode. A root cause is the underlying reason for a first level cause to occur. To identify the root cause(s) one may use simple or difficult methodologies/tools. Options include a problem-solving methodology such as 8D or DOE, cause-and-effect diagrams, and FTA.

**Occurrence (15):** This column contains the rating relating to the likelihood that a particular failure mode cause will occur within a specific time
period. To identify a reasonable occurrence, the team may use the Poisson distribution for theoretical numbers; historical data; maintenance records; surrogate data; and warranty data. Each cause must have its own occurrence number.

Prevention Controls and Equipment Controls (16): This column documents all the prevention controls that are planned to minimize the risk of the failure mode.

Current Design and Equipment Controls (17): This column documents the effectiveness of the planning controls in column 16. For detection purposes the best control item will be carried over to column 18. For example, if there are four controls with the following individual ratings such as 8, 5, 6, 7, and a 2, then the 2 will be carried over to column 18. The reason is that the control with a 2 rating is the strongest of them all and therefore the most effective.

Detection (18): It is the column indicating the likelihood that the prevention controls (item 17) can detect and prevent the failure from reaching the customer. This evaluation is based on preset criteria that everyone has agreed with. A numerical value of 1 indicates the problem is caught at the source, whereas a 10 indicates the failure reaches the customer.

RPN (19): The RPN is the product of severity, occurrence, and detection. It is very important here to remember that each root cause must have its own RPN. The RPN often is used as a value that determines the priority for either design improvements and/or operational changes.

Recommended Action (20): This column documents all the possible (appropriate) alternatives that may reduce the risk of the failure mode’s RPN. There should be more than one action available. The focus should be on reducing safety concerns, then on modes with high severity and occurrence and finally on the combination of severity, occurrence, and detection (RPN).

Responsible Individual and Target Completion Date (21): This column documents who is assigned the responsibility to review or implement the recommended action—if appropriate. A target date must also be identified. Without a name and/or date, no one is responsible and the due date becomes infinity.

Action Taken (22): This column briefly describes the specific action taken from the alternatives identified in column 20 with the intent to lower the risk of a failure mode. A completed EFMEA is of very limited value without positive actions to eliminate potential injury, safety issues, government regulation violations, and machine downtime or to prevent part defects. The action taken here is essential to implement high failure risk solutions. It must be also mentioned that the primary design responsibility belongs to the supplier and therefore all EFMEA updating remains the supplier’s responsibility, even after installation at the customer’s facilities.
(Obviously, if the design is the responsibility of the customer, then the customer bears the responsibility of the design EFMEA.)

Revised RPN (23): The revised RPN is calculated from the new severity, occurrence, and detection values resulting from the implemented actions in item 22. These new numerical values are a result of the team consensus. If there were no actions taken, then these new columns are left blank. If the actions have indeed reduced any of the three numbers or all of them, then the EFMEA team must repeat steps 20 through 23 on a new EFMEA form and a new revision number must be assigned. A word of caution here is appropriate. In order to change the severity number a design change must occur, otherwise the occurrence and/or the detection may be the only items that will change.

Ratings
Generally, the ratings for the EFMEA are the same as that of the design FMEA.

Tools
As machine builders design new equipment a variety of techniques and tools exist to improve quality, safety, and performance. However, from experience, an effective EFMEA can produce very good results if the EFMEA and FTA are used in combination.

The reader should remember that the EFMEA identifies all the machine’s potential failure modes and their first-level causes. In other words, it tries to identify the breadth of problems with a new design (or a modified one). On the other hand, the FTA is used to analyze the root cause of significant failures and establish the probabilities of each cause. The importance of this approach lies with the fact that in the process of evaluating the probabilities it shows graphically the relationship of each of the causes. In other words, the FTA focuses on the depth of each individual failure. The fundamental question in any FTA is: What are all possible causes for one failure?

Other typical tools that may be used are:

• Block diagrams
• Interface matrix
• P-diagram
• Brainstorming
The Common Types of FMEAs

- Cause-and-effect diagram
- Reliability formulas (for defining failure)
- Poisson distribution (for identifying specific failure rates)
- DOE
- Others (see Chapter 13 on Tools)
References


Selected Bibliography


Index

Note: Page numbers followed by f or t refer to figures or tables, respectively.

A

ACAT (avoid-control-accept-transfer) model, 17
actions taken
definition and description of, 42–43
FMECA, 100
form detailing, 81–82
HFMEA, 90
rankings as basis for, 54–55
records of, 55
timing of, 55
troubleshooting, 145
aerospace industry FMEA, 152
affinity diagrams, 75, 94, 112, 123–24
AIAG. See Automotive Industry Action Group
alpha, 103–4
analytical warranty system (AWS), 156
area charts, 53, 53f
automotive industry
dynamic control plans, 114
FMEA adoption, 151
FMEA form, 12, 13f
goal of QMS, 6
IATF 16949 standard, 1, 6, 7
rankings, 50
SAE standards, 7, 50, 152
VDA standard, 7–10, 11–12, 13f
warranty, 155–58

Automotive Industry Action Group (AIAG)
FMEA form, 12
FMEA guidelines, 151
risk assessment criteria, 11–12
tools, IATF 16949 supporting, 7
VDA standard approval, 8
avoid-control-accept-transfer (ACAT) model, 17
AWS (analytical warranty system), 156

B

bar chart graphs, 132
basics of FMEA
benefits, 31, 36
definition, 29–30
need for, 30–31
post-completion steps, 37–38
process of conducting, 32–36
advantages of, 36
starting, 34, 34f–35f
steps in, 32–34
timing of, 35
uses of, 35
understanding customers and their needs, 36–37
vocabulary, 38–43
benchmarking, 60, 64, 66, 73, 119, 120
beta, 103
block diagrams, 32, 46f, 66, 82
boundary diagrams, 45, 46f, 46r, 120
box plots, 95, 124
BPEST (business, political, economic, social, technological) analysis, 1
brainstorming
cause determination, 41
data analysis, 33
description and use of, 124
DFMEA, 64, 66
EFMEA, 82
FMEA team, 32, 33
FMECA, 112
HFMEA, 94
PFMEA, 73
breadboard tests, 60
business, political, economic, social, technological (BPEST) analysis, 1
business continuity planning, 1
capability studies, 38
cause-and-effect analysis
data analysis, 33
description and use of, 125
DFMEA, 66
EFMEA, 83
fishbone diagrams, 41, 125
FMECA, 112
PFMEA, 75
causes, possible
definition and description of, 40–41
determination of, 41
form detailing, 80
root-cause analysis, 86–87, 87f, 101
root cause of risk, 12, 52
troubleshooting, 143
c-control charts, 71, 72r, 125–26
CFMEA. See concept FMEA changes
actions taken eliciting, 55
to control plans, 116
effective implementation of, 6
classification and ranking based on, 52
PFMEA assessing, 58f, 74
special, control plans monitoring, 113
types of FMEAs assessing, 58f
check sheets/checklists, 46f, 71, 72r, 94, 112
chemical industry FMEA, 152–53
classification
definition and description of, 40
form detailing, 80
ranking of characteristics for, 52
severity, 40, 52, 97, 103, 105–6
troubleshooting, 143
common types of FMEA. See types of FMEA
computer simulation, 33, 60, 112, 125
concept FMEA (CFMEA)
benefits of, 59–60
characteristics assessed, 58f
control plan linkage with, 120, 121
continual improvement goals, 33–34, 38
control chart-c, 71, 72r, 125–26
control chart-median and R, 126
control chart-np, 71, 126
control chart-p, 71, 72r, 127
control chart-u, 71, 127
control chart X-bar and R, 71, 72r, 127–28
control chart X-bar and S, 128
control plans
adherence to, 38
benefits of, 114
content of, 114–15
deficiencies in typical, 116–17
definition of, 113
effectiveness of, 38
FMEA linkage with, 115–17, 119–22
Index 167

purpose of, 113
reaction plans and, 113, 115
risk management, 16–18
statement of applicability, 16
tools for, 117
types of, 114
use of, 113–14
corporate knowledge, 60, 119, 120
correlation analysis, 95
cost per unit (CPU), 156
critical path analysis, 135
cross-functional process maps, 128
customer needs and requirements control plans to meet, 113, 114
risk management project addressing, 6
understanding, 36–37

data collection and analysis, 33
DCOV (Define-Characterize-Optimize-Verify) model, 158
decision making under conditions of risk and uncertainty, 2
decision trees, 95, 128–29
Define-Characterize-Optimize-Verify (DCOV) model, 158
Define-Measure-Analyze-Improve-Control (DMAIC) model, 158
Department of Defense, avoid-control-accept-transfer model, 17
design current, form detailing, 81
design concept input, 119
design concept output, 120
design input, 120
design output, 121
for reliability, 21
for Six Sigma, 158
design FMEA (DFMEA) benefits of, 61–62
characteristics assessed, 58
control plan linkage with, 116, 116f, 119–22
focus of, 58
form, 49, 50f, 62
industry-specific, 151
objective of, 58
overview, 34f
purpose of, 61
rankings, 51, 62–66, 63–65
risk assessment criteria, 11
risk reduction strategies, 62, 64, 66
robustness, 46
tools for, 32, 62, 64, 66
troubleshooting, 143–44
use of, 61
VDA standards, 9–10
design of experiments (DOE), 33, 83, 129
detection of risk actions taken affecting, 55
definition and description of, 42, 97
detection controls, 42, 111
early, for warranty spend reduction, 157–58
FMEA results, 33, 38
form detailing, 81, 111
new, 43, 55
rating or ranking, 51–52, 64, 65, 66, 71
73–74, 94, 111
reduction of, 52
risk assessment for, 11–12
risk priority number based on, 42, 53, 111–12
troubleshooting, 144
DFMEA. See design FMEA
DMAIC (Define-Measure-Analyze-Improve-Control) model, 158
DOE (design of experiments), 33, 83, 129
dot plots, 129–30

effects of failure definition and description of, 39–40, 97
form detailing potential, 80, 110–11
troubleshooting, 142
EFMEA. See equipment FMEA
8 wastes analysis, 87, 88
end-of-the-line (EOL) testing, 111
engineering testing, 75
equipment FMEA (EFMEA)
benefits of, 76
characteristics assessed, 58
completion of, 77
discarding of, 77
FMEA team, 76–77, 78
focus of, 58
form, 77–82, 79
general information, 76–77
method of preparing, 76
objective of, 58
purpose of, 75
rankings, 82
timing of starting/updating, 76, 77
tools for, 82–83
updates to, 77
use of, 75
escape point, 12, 90
event tree analysis, 1

F

facilitators, team, 24–25
failure
causes of, possible, 12, 40–41, 52, 80, 86–87, 87f, 101, 143
criteria for, 20
data on, 33
definition of, 20, 27
detection of, 97, 111 (See also detection of risk)
effects of, 39–40, 80, 97, 110–11, 142
FMECA quantitative analysis of probability of, 105
function, 97
mean time between, 97, 106–7
mindset of minimizing, 27–28
mode of, 39, 78, 80, 97, 104–6, 108, 110, 142
rate of, 104, 107–8
types of, 20–21
understanding concept of, 20–21
failure mode
definition and description of, 39, 97
FMECA quantitative analysis of, 104–6
form detailing potential, 78, 80, 108, 110
troubleshooting, 142
Failure Mode Effects and Criticality Analysis. See FMECA
(Failure Mode Effects and Criticality Analysis)
Failure Mode and Effect Analysis. See FMEA (Failure Mode and Effect Analysis)
fault tree analysis (FTA)
cause determination, 41
description and use of, 130–31
DFMEA, 62
EFMEA, 82
FMECA analysis and, 101, 103
risk assessment, 1
fishbone diagrams, 41, 125
5 Whys method, 41
FMEA (Failure Mode and Effect Analysis)
advantages or benefits of, 31, 36
basics of, 29–43
challenges of, 58
concept FMEA, 58f, 59–60, 120, 121, 151
customer needs and requirements, 36–37
definition of, 1, 29–30, 130
design FMEA (See design FMEA)
equipment FMEA, 58f, 75–83
FMECA extension of, 97–112, 152
form, 12, 13f, 49, 50f, 60, 62, 67, 68f, 77–82, 79f, 91, 92f
health FMEA, 85–95
industry-specific, 49, 50, 57–58, 59, 62, 151–53 (See also specific industries)
institutionalization of, 149
lean methodology, 159
linkages, 46f, 115–17, 119–22
monitoring and system response, 12
need for, 30–31
post-completion steps, 37–38, 159–60
prerequisites of, 23–28
problems and concerns, 147–49, 159–60
process FMEA (See process FMEA)
process of conducting, 32–36
quality management system, 1–6, 15–16, 155–60
rankings (See rankings)
reliability and, 19–21, 29, 51, 120–21
risk and (See risk)
robustness of, 45–48, 121
service FMEA, 32, 58
Six Sigma, 158
starting or beginning, 34, 34–35
system FMEA, 32
teams for, 23–27, 32, 33, 76–77, 78, 89, 147
timing of, 35
tools (See tools)
troubleshooting, 141–45
types of, 57–83 (See also specific types)
uses for, 35, 130
VDA standard, 7–10, 11–12, 13f
vocabulary for, 38–43
warranty, 1, 155–58

FMEA teams
brainstorming by, 32, 33
champions/sponsors of, 24
common problems, 147
considerations for, 25
core, 23–24, 78
creating effective, 23
EFMEA, 76–77, 78
facilitators for, 24–25
HFMEA, 89
leaders of, 24
motivated, 25–26
potential members of, 26–27
recorders for, 24
selection of, 32
structure of, 23–25
useful information for, 25–26

FMECA (Failure Mode Effects and Criticality Analysis)
analysis of significant function, 99–108
qualitative, 101, 102f
quantitative, 101, 103–8, 109f
benefits of, 112
definition of, 97–98
detection of failure, 97, 111
effect of failure identification, 97, 110–11
failure mode analysis and identification, 97, 104–6, 108, 110
failure rate analysis, 104, 107–8
FMEA distinction from, 100
form, 101, 102f, 108, 109f, 110–12
implementation of results, 100
industry-specific, 152
planning and preparation for, 99
process of conducting, 99–101
rankings, 101
risk priority number calculation, 111–12
severity classification, 97, 103, 105–6
significant function analysis in, 100–108
qualitative, 101, 102f
quantitative, 101, 103–8, 109f
sources for identifying functions, 98–99
sustaining, 100
tools for, 112
vocabulary, 97

force field analysis, 60
form
CFMEA, 60
DFMEA, 49, 50f, 62
EFMEA, 77–82, 79f
FMECA, 101, 102f, 108, 109f, 110–12
generic, 49, 50f
HFMEA, 91, 92f
PFMEA, 49, 50f, 67, 68f
VDA standard compliance, 12, 13f
FTA. See fault tree analysis
function
definition and description of, 39, 97
form detailing, 78
significant, FMECA analysis of, 100–108
sources for identifying, 98–99
troubleshooting, 142
functional diagrams, 32, 60
function failure, 97
function trees, 66, 131
Index

G

gage repeatability and reproducibility, 131
gages or indicators, 111
Gantt chart graphs, 132
graphs-bar chart, 132
graphs-Gantt chart, 132
graphs-pie chart, 132

H

hazard analysis, 86–87
health FMEA (HFMEA)
  conducting analysis in, 90
  defining topic of, 88–89
  8 wastes analysis, 87, 88t
  FMEA team, 89
  form, 91, 92t
  graphical description of process, 89–90
  hazard analysis, 86–87
  identifying actions and outcome measures for, 90
  organizational, 88–89, 89t
  overview, 85–86
  process of conducting, 87–91
  process-oriented, 88–89, 89t
  rankings, 91, 93t–94t, 94
  repetition of, 91
  root-cause analysis comparison, 86–87, 87t
  6S goals for, 87, 88t
  tools for, 89–90, 94–95
  histograms, 133

I

IATF (International Automotive Task Force) 16949 standard, 1, 6, 7
identification of risks, 12, 14, 37. See also detection of risk
industry-specific FMEA
  aerospace, 152
  automotive, 151 (See also automotive industry)
chemical/pharmaceutical, 57–58, 152–53
  rankings, 49, 50, 62
  software, 152
  types of, 57–58, 59
inspections, 75, 117
institutionalization of FMEA, 149
insurance, 17
interface matrix, 46, 46t, 47t, 66, 82, 120
internal past corporate knowledge, 60, 119, 120
International Automotive Task Force (IATF) 16949 standard, 1, 6, 7
ISO (International Organization for Standardization) standards
  9000, 5
  9001:2015, 3–5, 6–7
  13485:2016, 2
  14001:2015, 3
  14971:2012, 2
  27001, 16
  31000:2018, 4, 7, 15
  goal of, 5–6
  risk assessment defined, 2
  risk-based thinking, 2–5, 6–7, 15, 16
  risk defined, 1, 2, 5
  risk management defined, 2
  system-oriented, 6

J

jigs, 117
The Joint Commission (TJC), 85

K

Kano model, 37, 133
Kepner Tregoe method, 41
key process input variables (KPIV), 113
key process output variables (KPOV), 113
L

laboratory tests, 60
leaders, team, 24
lean methodology, 159
linkages
design concept input, 119
design concept output, 120
design input, 120
design output, 121
FMEA-control plan, 115–17, 119–22
machinery output, 122
process concept input, 120
process concept output, 120
process input, 121
process output, 122
robustness, 46f, 121
logistical analysis, 101

M

machinery output, 122
mathematical modeling, 33, 60
mean time between failure (MTBF), 97, 106–7
metrics
FMEA, 33
HFMEA, 90
measurement system analysis, 117
measures of central tendency and dispersion, 2
Mil-Std 1629, 91, 103
MIS (months in service), 156
mistake proofing, 71, 73, 75, 111
monitoring and system response (MSR) control plans for, 113–14
FMEA establishment of, 12
risk-based effectiveness checks, 15
months in service (MIS), 156
MTBF (mean time between failure), 97, 106–7

N

new detection of risk, 43, 55
new occurrences of risk, 43, 55
new risk priority number, 43, 55, 82
new severity of risk, 43, 55
np-control charts, 71, 126

O

occurrences of risk
actions taken affecting, 55
classification based on, 52
definition and description of, 41–42, 97
FMEA results, 33, 38
form detailing, 80–81
new, 43, 55
rating or ranking, 51, 62, 64, 64t, 70r, 73, 91, 94r, 101
reduction of, 51
risk assessment of, 11
risk priority number based on, 42, 53, 111–12
troubleshooting, 143–44
operational definitions, 134
opportunity, risk and, 2, 3, 4–5, 6

P

Pareto diagrams, 134
p-control charts, 71, 72r, 127
P-diagrams
DFMEA, 66
EFMEA, 82
linkages, 120, 121
robustness tool, 46f, 47–48, 48f
PERT analysis, 135
PESTLE (political, economic, social, technical, legal, environmental) analysis, 2
PFMEA. See process FMEA
pharmaceutical industry FMEA, 57–58, 152–53
pie chart graphs, 132
Poisson distribution, 83, 105
political, economic, social, technical, legal, environmental (PESTLE) analysis, 2
prerequisites of FMEA
FMEA teams
creating effective, 23
motivated, 25–26
potential members of, 26–27
structure of, 23–25
mindset of minimizing failures, 27–28
prevention controls, 42, 81, 144
prioritization, FMEA, 32
problems and concerns
institutionalization, 149
post-completion evolution, 159–60
problem analysis, in risk assessment, 14
problem-solving process, 41, 123
procedural, 147–48
team, 147
procedural problems, common, 147–48
process concept input, 120
process concept output, 120
process control. See also control plans
DFMEA, 66
nonstatistical, 71–72, 72f
PFMEA, 70–72, 72f, 74–75
statistical, 33, 71, 72f, 94, 117
process flowcharts, 32, 89–90, 94, 117, 119–22, 135
process FMEA (PFMEA)
benefits of, 67
characteristics assessed, 58r, 74
control plan linkage with, 116, 116f, 119–22
focus of, 58r
form, 49, 50f, 67, 68f
industry-specific, 151
objective of, 58r
overview, 35f
process control matrix, 70–72, 72r
process control system guidelines, 74–75
purpose of, 66–67
rankings, 51, 52, 69–70, 69r–71r, 73–74
recommendations, 74
risk assessment criteria, 11–12
risk reduction strategies, 73–74
tools for, 32, 73, 75
troubleshooting, 142
use of, 67
VDA standards, 10
process input, 121
process output, 122
program decision process charts, 135–36
Pugh technique, 64, 66, 73, 74, 136

Q
QFD (quality function deployment), 33, 37, 60, 62, 66, 136–37
QMS. See quality management system qualitative analysis, FMECA, 101, 102f/quality function deployment (QFD), 33, 37, 60, 66, 136–37
quality management system (QMS)
goal of, 5–6
lean methodology, 159
post-FMEA implementation, 159–60
risk-based approach, 2, 3–5, 15–16
Six Sigma, 158
warranty in, 1, 155–58
quantitative analysis, FMECA, 101, 103–8, 109f

R
rankings
CFMEA, 60
classification and characteristics, 52
detection rating, 51–52, 64, 65r, 66, 71r, 73–74, 94, 111
DFMEA, 51, 62–66, 63r–65r
driving action plans, 54–55
EFMEA, 82
FMECA, 101
HFMEA, 91, 93r–94r, 94
industry-specific, 49, 50, 62
not standardized, 49
occurrence rating, 51, 62, 64, 64r, 70r, 73, 91, 94r, 101
PFMEA, 51, 52, 69–70, 69r–71r, 73–74
risk understanding and calculation, 53–54
severity rating, 50, 62, 63r, 64, 69r, 73, 91, 93r–94r, 94, 101
troubleshooting, 145
RCM (reliability-centered maintenance), 103
reaction plans, 113, 115
real option modeling, 1
recommendations
definition and description of, 42
form detailing, 81
linkages output, 122
PFMEA, 74
troubleshooting, 145
recordkeeping, 24, 33, 55
regression analysis, 137
reliability
analysis/modeling, 33, 66, 83, 111, 112, 137
design for, 21
expertise in, for occurrence ratings, 51
FMEA and, 19–21, 29, 51, 120–21
linkages design, 120–21
overview, 19–20
reliability-centered maintenance (RCM), 103
understanding failure, 20–21
repair per 1000 vehicles (R/1000), 156
resource planning, 6
risk
assessment
cost-benefit analysis, 14, 15
defined, 2
identification of risk options, 14–15
method or process of conducting, 10–14
techniques, 1–2 (See also FMEA)
avoidance of, 16
definition of, 1, 2, 5
detection of (See detection of risk)
escape point from, 12, 90
goal of standards for, 5–6
high-risk area identification, 37
IATF 16949 standard, 1, 6, 7
identification of, 12, 14, 37
insurance against, 17
ISO standards, 1–7, 15, 16
management
defined, 2
plans, 16–18
occurrences of (See occurrences of risk)
opportunity and, 2, 3, 4–5, 6
overview, 1–3
problem analysis, 14
project plan for, 6–7, 15, 16–18
QMS addressing, 2, 6–7, 15, 16–18
ranking based on understanding and calculating, 53–54
reduction of, 17, 62, 64, 66, 73–74
retention of, 17
risk-based thinking, 2–5, 6–7, 15, 16, 18
risk priority number (See risk priority number)
 risk register, 3–4, 15, 16r
risk treatment plans, 16–18
root cause of, 12, 52
severity of (See severity of risk)
sharing or transfer of, 17
source analysis, 14
uncertainty and, 1–3, 5, 18
VDA standard, 7–10, 11–12, 13f
risk priority number (RPN)
actions taken affecting, 55
area chart of, 53, 53f
calculation of, 42, 53–54, 111–12
classification based on, 52
definition and description of, 42
FMEA results, 33, 37–38
form including, 81, 82, 111–12
new, 43, 55, 82
rankings in relation to, 53–54
troubleshooting, 144
robustness
boundary diagrams, 45, 46f, 46t
interface matrix, 46, 46r, 47r
linkages process, 46r, 121
P-diagrams, 46r, 47–48, 48f
root cause
analysis, 86–87, 87r, 101
of risk, 12, 52
RPN. See risk priority number
run charts, 137–38
S

SAE. See Society of Automotive Engineers
sampling, 117
scatter plots/diagrams, 95, 138
scenario, FMECA, 112
self-insurance, 17
service FMEA, 32, 58
severity of risk
actions taken affecting, 55
classification based on, 40, 52, 97,
103, 105–6
definition and description of, 40
FMEA results, 33, 37–38
form detailing, 80
new, 43, 55
rating or ranking, 50, 62, 63t, 64,
69t, 73, 91, 93r–94t, 94, 101
reduction of, 50
risk assessment of, 11
risk priority number based on, 42,
53–54, 111–12
troubleshooting, 143
shared and interlocking objectives
matrix, 138
significant function, 100–108
simulation, 33, 60, 112, 125
6S (sort, set in order, shine/sweep,
safety, standardize, sustain)
goals, 87, 88r
Six Sigma, 158
Society of Automotive Engineers (SAE)
ARP5580 standard, 152
J1739 standard, 7, 50, 152
software FMEA, 152
source analysis, 14, 98–99
SPC (statistical process control), 33,
71, 72r, 94, 117
special characteristics, 113
statement of applicability, 16
statistical inference, 2
statistical process control (SPC), 33,
71, 72r, 94, 117
stem and leaf plots, 138
surveys, 139
SWOT (strengths-weaknesses-
opportunities-threats)
analysis, 1
system FMEA, 32

T

teams. See FMEA teams
terminology. See vocabulary
theory of inventive problem solving
(TRIZ), 64, 66, 73
time in service (TIS), 156
time series forecasting, 139
timing
of actions, review of, 55
EFMEA start/update, 76, 77
FMEA, 35
mean time between failure, 97,
106–7
risk management project plan, 6
severity variance based on, 50
TIS (time in service), 156
TJC (The Joint Commission), 85
tools
affinity diagrams, 75, 94, 112,
123–24
area charts, 53, 53f
benchmarking, 60, 64, 66, 73, 119,
120
block diagrams, 32, 46f, 66, 82
boundary diagrams, 45, 46f, 46t, 120
box plots, 95, 124
BPESR analysis, 1
brainstorming, 32, 33, 41, 64, 66,
73, 82, 94, 112, 124
breadboard tests, 60
business continuity planning, 1
cause-and-effect analysis, 33, 41,
66, 75, 83, 112, 125
CFMEA, 60
check sheets/checklists, 46f, 71,
72r, 94, 112
critical path analysis, 135
correlation analysis, 95
critical path analysis, 135
cross-functional process maps, 128
data analysis, 33

data analysis, 33
decision making under conditions of risk and uncertainty, 2
decision trees, 95, 128–29
design of experiments, 33, 83, 129
detection controls, 42, 111
DFMEA, 32, 62, 64, 66
dot plots, 129–30
EFMEA, 82–83
end-of-the-line (EOL) testing, 111
engineering testing, 75
event tree analysis, 1
fault tree analysis, 1, 41, 62, 82, 101, 103, 130–31
fishbone diagrams, 41, 125
flexible risk assessment, 15
FMECA, 112
force field analysis, 60
functional diagrams, 32, 60
function trees, 66, 131
gage repeatability and reproducibility, 131
gages or indicators, 111
dot plots, 129–30
graphs-bar chart, 132
graphs-Gantt chart, 132
graphs-pie chart, 132
HFMEA, 89–90, 94–95
histograms, 133
inspections, 75, 117
interface matrix, 46, 46t, 47t, 66, 82, 120
internal past corporate knowledge, 60, 119, 120
jigs, 117
Kano model, 37, 133
laboratory tests, 60
logistical analysis, 101
mathematical modeling, 33, 60
measurement system analysis, 117
measures of central tendency and dispersion, 2
mistake proofing, 71, 73, 75, 111
operational definitions, 134
Pareto diagrams, 134
P-diagrams, 46t, 47–48, 48f, 66, 82, 120, 121
PERT analysis, 135
PESTLE analysis, 2
PFMEA, 32, 73, 75
Poisson distribution, 83, 105
process control, 33, 66, 70–72, 72t, 74–75, 94, 117
process flowcharts, 32, 89–90, 94, 117, 119–22, 135
program decision process charts, 135–36
Pugh technique, 64, 66, 73, 74, 136
quality function deployment, 33, 37, 60, 62, 66, 136–37
real option modeling, 1
regression analysis, 137
statistical inference, 2
statistical process control, 33, 71, 72t, 94, 117
stem and leaf plots, 138
surveys, 139
SWOT analysis, 1
time series forecasting, 139
tree analysis, 139–40
TRIZ, 64, 66, 73
visual alarms, 111
warranty analysis, 1, 156
warranty spend reduction, 156–58
whisker plots, 124
tree analysis, 139–40. See also
decision trees; event tree analysis; fault tree analysis; function trees
TRIZ (theory of inventive problem solving), 64, 66, 73
troubleshooting an FMEA
actions taken/revised ratings, 145
appropriate controls applied, 144
classification, 143
detection, 144
function/purpose, 142
header, 141–42
occurrences, 143–44
potential causes/mechanisms of failure, 143
potential failure effects, 142
potential failure mode, 142
prevention controls, 144
recommended action, 145
responsibility/target completion date, 145
risk priority number, 144
severity, 143
steps in, 141
types of FMEA. See also specific types of FMEA
challenges for, 58
characteristics assessed, 58–83
common, 59–83
concept, 58, 59–60
design, 58, 61–66
equipment, 58, 75–83
focus of, 58
industry-specific, 57–58, 59
objective of, 58
process, 58, 66–75
service, 58

U
u-control charts, 71, 127
uncertainty, risk and, 1–3, 5, 18

V
VDA (Verband der Automobilindustrie) standard
action priority, 10
benefits of, 8
flow, 9–10
FMEA form in compliance with, 12, 13f
principles of, 7–10
risk assessment criteria, 11–12
six-step model, 9
visual alarms, 111

W
warranty
automotive industry, 155–58
cost, 155
definition of, 155
early detection methodology, 157–58
spend, 156
spend reduction tools, 156–58
standardized model, 158
terminology, 156
warranty analysis, 1, 156
whisker plots, 124

X
X-bar and R charts, 71, 72f, 127–28
X-bar and S charts, 128