Using DFMEA and PFMEA to Track Improvements

Posted on September 19, 2018

Introduction

Failure Mode and Effects Analysis (FMEA) is a proactive method for identifying how a product or process might fail before the failure reaches a customer, patient, operator, or downstream operation (American Society for Quality, 2026). It is not merely a form completed for an audit. A useful FMEA brings together people who understand design, manufacturing, quality, maintenance, service, suppliers, and customer requirements. The team defines functions, anticipates failure modes, studies causes and effects, evaluates existing controls, and assigns actions that reduce risk.

Design FMEA (DFMEA) and Process FMEA (PFMEA) apply the same preventive logic at different stages. DFMEA asks whether the product's design can perform its intended functions safely and reliably. PFMEA asks whether the manufacturing, assembly, installation, delivery, or service process can consistently produce the intended result. The two analyses should inform each other. A design that is difficult to manufacture can create process failures, while recurring process data can expose design weaknesses. Used together, DFMEA and PFMEA create a traceable record of risk reduction and continuous improvement.

Purpose and Scope of DFMEA

DFMEA begins with the product or system's intended functions and requirements. The team examines components, interfaces, materials, software, operating environments, user interactions, tolerances, and foreseeable misuse. A failure mode describes how a function could be lost, degraded, delayed, intermittent, or performed incorrectly. The effect explains what happens at the next level and ultimately to the customer. The cause identifies the design mechanism that could produce the failure.

For example, a medical-device enclosure may be required to prevent fluid entry. Possible failure modes include cracking, seal separation, or an opening that permits contamination. Effects could range from degraded performance to electrical hazard or infection risk. Causes might include inadequate material selection, stress concentration, thermal expansion, or a seal geometry that is too sensitive to tolerance variation. Design controls may include simulation, tolerance analysis, prototype testing, environmental testing, peer review, and verification against requirements.

The purpose is not to predict every imaginable event. It is to focus the team on credible risk based on function, physics, prior experience, field data, and intended use. DFMEA should begin early enough to

influence the design. Completing it after drawings and tooling are fixed turns a preventive tool into documentation of decisions that can no longer be changed economically.

Purpose and Scope of PFMEA

PFMEA analyzes the steps used to create or deliver the product or service. The team maps the process and identifies requirements at each operation. Failure modes may include wrong material, incorrect torque, contamination, missing component, improper labeling, measurement error, software configuration error, inadequate curing, or failure to detect a defect. Effects describe what the next operation or customer experiences, while causes explain why the process could produce that failure.

Process controls are divided conceptually into prevention and detection. Prevention controls reduce the likelihood that a cause will occur. Examples include keyed fixtures, automated parameter limits, supplier qualification, error-proof connectors, standardized work, maintenance, and operator certification. Detection controls attempt to find the failure before release, such as inspection, functional testing, vision systems, alarms, and statistical monitoring. Prevention is generally stronger because detection can miss defects, occur too late, or depend on sampling.

PFMEA should be linked with the process flow diagram and control plan. The flow diagram establishes the real sequence, including movement, storage, rework, outsourced steps, and inspection. The PFMEA identifies the risks in that sequence. The control plan translates important prevention and detection controls into operating requirements. When these documents contradict one another, the system is not under control even if each document looks complete in isolation.

From RPN to Action Priority

Traditional FMEA often uses the Risk Priority Number (RPN), calculated by multiplying severity, occurrence, and detection ratings (Stamatis, 2019). RPN can help organize discussion, but it has important limitations. Different combinations can produce the same number while representing very different risks. A low-frequency failure with catastrophic severity may receive the same RPN as a frequent nuisance defect. Teams may also focus on reducing scores rather than reducing actual risk.

The harmonized AIAG and VDA approach uses Action Priority to guide whether additional action is high, medium, or low priority based on the combination of severity, occurrence, and detection (Automotive Industry Action Group, 2022). AIAG describes its FMEA handbook as a structured reference for Design FMEA, Process FMEA, and supplemental FMEA for monitoring and system response. The shift does not mean ratings are unimportant. It means the team should not treat one arithmetic threshold as the sole decision rule. High severity deserves attention even when occurrence appears low, and weak evidence should not be converted into unjustified confidence.

Organizations that still use RPN can improve the method by recording the actual reason for each

action, requiring review of high-severity items, and avoiding arbitrary rules such as “all RPNs below 100 are acceptable.” The decision should consider legal requirements, customer impact, safety, warranty history, detectability, process capability, and the feasibility of stronger controls.

Tracking Improvements

FMEA tracks improvement by preserving the relationship between the initial risk assessment, the action taken, the responsible owner, the completion date, and the revised evaluation. A risk is not reduced merely because an action was proposed. The team needs objective evidence that the action was implemented and effective. Evidence may include test results, capability data, audit findings, field performance, reduced scrap, fewer complaints, or successful verification under worst-case conditions.

Before-and-after ratings can summarize the change, but the narrative is more important. A design team may increase wall thickness, change material, add a protective feature, or revise the architecture so the failure mechanism no longer exists. A process team may introduce poka-yoke, automated parameter control, barcode verification, or 100-percent functional testing. The FMEA should state exactly which cause or control was changed. Vague actions such as “train operator” or “be more careful” rarely provide durable risk reduction unless the underlying problem truly is a knowledge gap and competence is verified.

Improvement tracking also requires version control. The document should identify when it was reviewed, what changed, and why. Lessons from prototypes, pilot production, audits, warranty claims, supplier issues, complaints, and corrective actions should be fed back into the FMEA. A document that has not changed for years despite changes in materials, suppliers, equipment, software, or customer use is unlikely to represent the current risk.

Relationship With ISO 14971 and Other Risk Systems

The original essay compared DFMEA with ISO 14971, the medical-device risk-management standard (International Organization for Standardization, 2019). The concepts overlap but are not identical. ISO 14971 addresses the full lifecycle process for identifying hazards, estimating and evaluating risks, controlling risks, and monitoring the effectiveness of controls. A hazard is a potential source of harm; a hazardous situation is a circumstance in which people, property, or the environment are exposed to a hazard; and harm is the injury or damage that results. FMEA can support this process by identifying failure-related sequences, but not every hazardous situation begins with a component failure. Normal use, usability problems, cybersecurity events, and foreseeable misuse may also create risk.

For this reason, a medical-device organization should not assume that completing a DFMEA satisfies

all risk-management obligations. The risk file should connect hazards, design inputs, usability engineering, cybersecurity, verification, clinical evidence, production controls, complaints, and post-market surveillance. Similar integration is needed in automotive, aerospace, food, and other regulated industries. FMEA is powerful when it is part of a larger management system rather than an isolated spreadsheet.

DFMEA and PFMEA as a Connected Chain

DFMEA and PFMEA should exchange information in both directions. Design characteristics identified as critical or significant may require specific manufacturing controls. A tight dimension, for example, may require capable equipment, measurement-system analysis, and reaction plans. The PFMEA can reveal that the design requires a process that is unstable, expensive, or difficult to inspect. The design team may then widen a tolerance, simplify an interface, reduce the number of parts, or add a feature that prevents incorrect assembly.

This connection is especially important during change management. A supplier change may alter material behavior; a software update may affect test coverage; a new production line may introduce different handling; and a cost-reduction proposal may remove redundancy. Change approval should include review of both FMEAs and the associated validation plan. Otherwise, an improvement in one area can create an unseen risk elsewhere.

Common Weaknesses in FMEA Practice

The most common weakness is treating FMEA as the quality department’s paperwork. When one person completes it without a cross-functional team, causes and controls are usually superficial. Another weakness is copying a previous document without confirming that the functions, interfaces, process steps, and operating conditions are truly comparable. Generic failure modes such as “part fails” provide little guidance for prevention.

Rating inflation and rating manipulation are also problems. Teams may lower occurrence because no complaint has been reported, even though there is little data, or lower detection because an inspection exists without evaluating its capability. Actions may be closed without evidence. In some organizations, the same control is listed as both prevention and detection, or inspection is credited with preventing a cause. These practices make the document look safer without changing the real process.

A useful FMEA is specific, evidence-based, and connected to decisions. It uses clear functions, credible failure mechanisms, customer-oriented effects, and causes that can be acted upon. It challenges assumptions and records uncertainty rather than hiding it.

Practical Improvement Cycle

An effective cycle begins by defining scope and boundaries. The team then studies structure, functions, requirements, failure chains, and current controls. It evaluates priority and selects actions that address the cause or strengthen detection. Owners and deadlines are assigned. After implementation, the team verifies effectiveness and updates the ratings and related documents. Management reviews unresolved high-priority risks and ensures that resources are available.

Metrics should extend beyond the number of completed FMEAs. Organizations can track action closure quality, recurrence of previously identified failure modes, customer complaints linked to known risks, process capability for critical characteristics, and the percentage of changes that received FMEA review. These measures show whether the method is influencing performance rather than merely producing files.

Conclusion

DFMEA and PFMEA are complementary methods for preventing failure and documenting risk reduction. DFMEA focuses on whether a design can meet its functions under expected and foreseeable conditions. PFMEA focuses on whether the process can reliably produce and deliver that design. Both require cross-functional knowledge, traceability, evidence, and timely action.

Tracking improvement involves more than comparing an old and new RPN. The organization must identify the failure mechanism, implement a meaningful control, verify effectiveness, and update the connected design, process, control-plan, and risk documents. When used as a living decision system, FMEA converts experience and uncertainty into preventive action. When used as a static form, it creates the appearance of control without the substance.

References

Automotive Industry Action Group. (2022). AIAG & VDA FMEA Handbook.

American Society for Quality. (2026). Failure Mode and Effects Analysis.

International Organization for Standardization. (2019). *ISO 14971: Medical devices—Application of risk management to medical devices*.

Stamatis, D. H. (2019). *Risk Management Using Failure Mode and Effect Analysis*. ASQ Quality Press.