Meeting international standards for medical device reliability and risk management

METHODS FOR MANAGING PRODUCT RELIABILITY AND RISK IN THE MEDICAL DEVICE FIELD

Introduction

In the design and development of safe, effective medical devices, reducing risk and ensuring reliability are a manufacturer's primary responsibility. Not only are these dimensions of product quality mandated by agencies and organizations like the Federal Food and Drug Administration's (FDA) Center for Devices and Radiological Health (CDRH), and recommended as best practices by the Global Harmonization Task Force (GHTF) and the International Organization for Standardization (ISO), product quality and efficacy are the moral and ethical imperative of all medical device manufacturers.

The advanced technology inherent in medical devices and their production means that all aspects of the system–including mechanics, electronics, software, and hardware–must be evaluated for reliability. What's more, due to the significant impact that a new medical device technology can have on human lives, every aspect of its development–from design and prototyping through manufacture, distribution, disposal, and decommissioning–must adhere to strict quality standards that are documented and traceable to functional and safety requirements. These standards may apply not only to manufacturers, but also to vendors, suppliers, contractors, OEMs, third parties, and others in product development and distribution.

According to various regulations, each of these complex dimensions of medical device safety and reliability must be systematically analyzed in an accurate, documented fashion. When risks are discovered, they must be evaluated for their severity and probability of occurrence, and eliminated or mitigated as appropriate. Then, medical devices must be monitored throughout their useful lives to ensure that no new or unexpected risks arise; and, if they do, additional risk analysis and control measures must be implemented.

Dimensions of medical device risk

Medical devices—which may be defined as any equipment used to diagnose, treat, or monitor patient health—are subject to a variety of complex quality and safety analyses due to the potential significant impact on human lives. Numerous standards throughout the medical device industry require the use of a documented process to identify, analyze, and eliminate or control the risks associated with medical device hardware, software, and electronics. This process, known as risk management, must address potential risks throughout the entire product lifecycle of medical device products, including development, manufacture, maintenance, and disposal or decommissioning.

Not only is the implementation and documentation of a risk management process required for the premarket approval of medical devices, it also helps protect companies against steep liability damages by providing evidence that risk was assessed during product development and that every reasonable measure was taken to control it. Medical device regulations and guidelines ISO 14971 and GHTF/SG3/N15R8 call for the thorough documentation, via a risk management file, of all risk management activities performed by the manufacturer. Not only must they be fully documented, these activities must be traceable to an initial risk management plan, which must adhere to the risk management process required by regulatory bodies.

Assessing and reducing the risks associated with medical devices also helps to reduce the total impact of wide-ranging product recalls, including financial costs as well as reduced customer satisfaction and a damaged company reputation. Most importantly, companies are morally and ethically obligated to know the impact that a product will have on human safety and wellbeing before the product is released to the public.

The following examples describe a few of the many dimensions that an assessment of medical device risk and reliability must consider:

- **Part failures**: The failure of one part or component of a medical device can lead to system failure and may result in patient injury or death. For example, if a feedback mechanism in a therapeutic medication delivery system fails, a patient may receive incorrect or even lethal doses.
- **Process failures**: Fully operational devices can inflict harm when used improperly, such as X-ray machines when proper measures are not taken to protect the patient.
- **Human impact**: The potential harm caused by a part or process failure may extend not only to the patient but to the device operator and others in the environment, as in the case of a highly flammable oxygen source.
- **Device application**: Each device may have many different applications, uses, or environments. For instance, defibrillators are now commonly available in public places for use by nonprofessionals in cases of emergency. These devices require different risk controls when used by different operators. Similarly, a device as simple as a blood pressure cuff can be used in many situations, including emergency, rehabilitative, surgical, and more. Each possible application of a device must be considered during risk analysis.
- **Complex technology**: The advanced technology used in medical devices and in their production requires that all aspects of the system—including mechanics, electronics, software, and hardware—must be evaluated for reliability. Consider the many systems that comprise an ultrasound device, including hardware that comes in direct contact with a patient, sophisticated electronics that emit high-frequency waves, and advanced software transmitting findings to a healthcare professional via computer. If all of these complex systems are not working together properly, the device may fail at its crucial role in patient diagnosis.
- **Product lifecycle**: Every aspect of the product development lifecycle for a medical device—from design, prototyping, and manufacture through distribution, decommissioning, and disposal—must adhere to strict quality standards that are documented and traceable. For example, taking extra care during the design stage to select the most reliable parts cannot prevent errors in device assembly. Therefore, all aspects of product development must be considered and controlled during risk management.

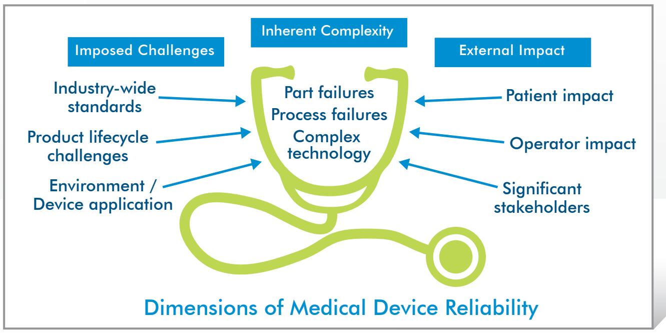


Figure 1: The multiple dimensions of medical device reliability: Imposed Challenges, Inherent Complexities, and External Impact

- **Industry-wide standards**: These standards may apply not only to device manufacturers, but also to their suppliers, contractors, OEMs, third-party manufacturers, and others associated with product development and distribution. If device parts are manufactured by one company, assembled by another, and distributed by a third, all three parties should participate in the risk management process to ensure that every possible risk is managed before the device is sent to market.

- **Significant stakeholders**: A wide range of potential stakeholders are affected by the reliability of a medical device, including medical practitioners, healthcare institutions, government, industry, patients, their family members, and others

What is risk management?

The role of ISO 14971 in defining risk management

Risk management in the medical device field is primarily defined by standard ISO 14971. According to this standard, risk management involves the systematic application of policies, procedures, and practices to the task of analyzing, evaluating, controlling, and monitoring the risk inherent in medical devices. Risk management is an iterative process that should evaluate all aspects of the product's lifecycle and must be implemented and documented over the course of the design, development, prototyping, manufacture, and even postproduction phases of a product's lifecycle to ensure that no new or unexpectedly severe risks go unmanaged.

GHTF/SG3/N15R8: Four phases of reliability management

In an effort to incorporate the requirements of risk management set forth in ISO 14971 into the requirements of a quality management system, the Global Harmonization Task Force (GHTF) defined four main phases of risk management in its guideline GHTF/SG3/N15R8. These four phases may be summarized as follows:

- **Phase 1**: Establishing acceptable and unacceptable levels of risks

- **Phase 2**: Identifying and analyzing the risks associated with the device from all potential sources

- **Phase 3**: Evaluating these risks in light of the definitions of risk acceptability defined in Phase 1

- **Phase 4**: Implementing control measures to eliminate risks or mitigate their effects, and monitoring the effectiveness of these controls once they are implemented

Each phase defined in GHTF/SG3/N15R8 summarizes multiple steps, and their associated definitions, set forth in ISO 14971. Both documents require the creation of a risk management file, which comprises the thorough documentation of each step in the risk management process. All of the steps summarized by the four phases and required in the risk management file documentation are described in full below:

1. **Risk management plan: Defining acceptable/ unacceptable levels of risk**

ISO 14971 requires that a risk management plan be created at the start of the risk management process to fully document how each required step will be carried out by the manufacturer. This plan must include criteria for risk acceptability based on the manufacturer's existing policy for determining acceptable and unacceptable risks. These important criteria will provide the basis for accepting a certain risk when the probability of its occurrence or its potential harm cannot be eliminated, or rejecting the risk as being too hazardous and therefore requiring its elimination or mitigation.

Risk is defined within ISO 14971 as the severity of hazard or harm should an event occur, together with the likelihood of its occurrence. Harm may be defined as physical injury or

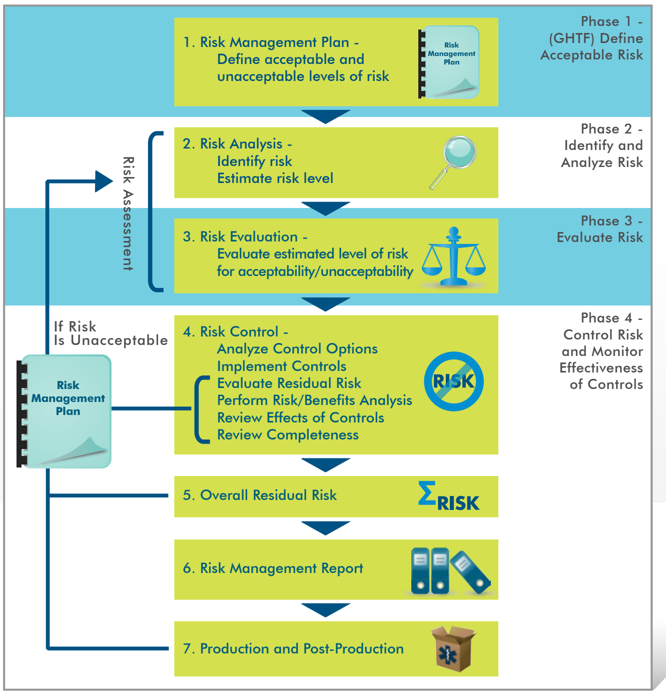


Figure 2: ISO 14971 defines an iterative Risk Management Process in which risks identified at each stage in the process must be evaluated for acceptability or unacceptability based on the standards set forth in the Risk Management Plan.

damage to one's health, property, equipment, or environment, while hazard and hazardous situations may be defined as potential sources of harm. When comparing risk levels, an event that would cause severe harm or hazard but is very unlikely to occur may be deemed less risky than an event that would cause moderate harm or hazard but is very likely to occur.

In weighing acceptable and unacceptable levels of risk, it is crucial to consider the functional requirements of the device. For example, in the case of a heart defibrillator, a secondary risk such as first-degree burns may be deemed acceptable given the significant benefit of saving a life. In other cases, causing a burn may constitute an unacceptable level of risk to the patient that could easily be prevented by designing in control measures, as in the case of a warming blanket for a postoperative patient.

Defining the functional and safety requirements of the device beforehand via a risk management plan is a crucial first step because, to meet regulatory requirements in the case of an audit, each subsequent step in the risk management process must be traceable directly back to device requirements and justifiable based on predefined levels of acceptable and unacceptable risk. The risk management plan also specifies verification activities in which manufacturers must engage to confirm that the requirements of the risk management plan have been fulfilled.

2. Risk analysis: Identifying and estimating risks throughout the product lifecycle

Risk analysis is a systematic, documented process beginning with a description of the device, the person doing the analysis, and the scope and date of the analysis. A description of the intended use and foreseeable misuse of the device follows, to establish a baseline from which potential risks–either from proper or improper use–could emerge.

Next, the analyst identifies all possible risks associated with the lifecycle of the device. For each identified risk, risk estimation takes place. Because risk is defined as the probability of occurrence of harm combined with the severity of that harm, risk estimation is often a quantitative process, which assigns a numerical value to the combined severity and probability of occurrence of the risk.

Often, risk severity is quantified by assigning a numerical value on a relative scale to the varying levels of severity. For example, level one may describe minor patient discomfort that dissipates quickly, while level ten may describe patient death. Using these values during risk analysis can help analysts prioritize the most severe risks and flag those which must be addressed first.

3. Risk evaluation: Comparing estimated risk to acceptable / unacceptable levels of risk

Every risk that is identified and estimated, it must be evaluated with an eye to the criteria for risk acceptability outlined in the original risk management plan. If the risk is deemed unacceptable, it must be eliminated or mitigated using risk control measures. If the risk is deemed acceptable, it must be justified according to these levels of unacceptable and acceptable risks.

4. Risk control: Designing control measures to eliminate or mitigate risks

During this process, decisions are made and measures implemented to reduce or mitigate risk to within the levels specified in the risk management plan. This very important process comprises several distinct steps, which themselves must be documented in the risk management file:

- **Analyze risk control options**: This process considers the available methods that may be used to control the unacceptable risk. Options may include safety by design, which incorporates risk controls into the design of the product; protective measures introduced into the manufacturing process to ensure the safety of the device; and information for safety, which includes use instructions and safety labels.
- **Implement risk control measures**: Once a risk control option is identified, it must be implemented. This step also requires that the effectiveness of the selected measure be verified.
- **Evaluate residual risk**: Residual risk is defined as the risk that remains after risk control measures have been implemented. In other words, any risk that remains after the control measure is introduced must be fed as input back into the risk assessment (risk analysis + risk evaluation) phase of the risk management process and evaluated in terms of its severity, probability of occurrence, and acceptability with regards to the criteria established in the initial risk management plan.
- **Perform a risk/benefits analysis**: If the residual risk resulting from the risk control measures is still deemed unacceptable, the manufacturer may choose to perform a risk/benefit analysis. This consists of gathering literature

and data to determine whether the medical benefits of the device outweigh the residual risk that remains following risk control activities. If the risk is deemed acceptable, the process continues. If not, this information is used as input into the risk assessment phase of the risk management process, and the risk must be estimated, analyzed, and controlled.

- **Review the effects of risk control measures**: In this step, the system with new risk control measures in effect must be assessed for any new risks that may arise as a result of the risk control measures. These new risks must be fed as input back into the risk assessment phase of the risk management process, estimated for severity of harm and probability of occurrence, evaluated for acceptability according to original criteria, and assessed for additional (or alternate) risk control measures if necessary.
- **Review completeness of risk control measures**: This process ensures that risks from all identified hazards have been considered, eliminated or controlled according to the levels of acceptability outlined in the risk management plan, and documented in the risk management file.

5. **Overall residual risk acceptability**

Once the steps for risk assessment, evaluation, and control are performed for each risk identified in a medical device, the overall residual risk of the product must be analyzed for its acceptability in regards to the standards set forth in the risk management plan. If all remaining residual risks are deemed acceptable, they must be documented and disclosed in any information or instructions accompanying the product, as well as in the risk management file. If the overall residual risk is not deemed acceptable, it must be fed back as input into the risk assessment part of the risk management process for reevaluation and control.

6. **Risk management report: Documenting how all required risk Management steps were performed**

Prior to production, a new medical device typically requires approval by national or international regulatory agencies. The production of a risk management report, which documents that all required steps have taken place in accordance with the original risk management plan, is required by these regulatory bodies. This becomes a part of the risk management file.

7. **Production and post-production information: Monitoring the device postmarket for any additional risks**

To gain approval of a medical device for production and distribution, evidence of an established, documented, and maintained system to collect and review information about the device throughout its production and postproduction phases is essential. Although it would appear that risk management activities have all been performed, in reality they have just begun. It is just as important to know that the device will be manufactured in accordance with established standards and perform in accordance with these standards.

As new, unanticipated risks, or unexpectedly severe residual risks, arise during devise production or use, the manufacturer must implement a plan to collect and review this information from significant stakeholders, including the operator, user, or others closely associated with the device–for example, installation technicians, vendors, or maintenance personnel. This plan must include the means to gather and review this information, and compare it to similar devices on the market to determine if previously unrecognized hazards or hazardous situations emerge. If new risks are encountered, they must be documented and fed back as input into the risk management process for analysis, estimation, evaluation, and control. Manufacturers must also evaluate the impact of previously implemented risk management steps, to determine if they truly reduced the risks they were anticipated to control or eliminate in the field.

Both this plan and its execution must be documented in the risk management file, and will be required should the manufacturer be audited.

"Top management has a responsibility to incorporate risk management into the organization." - Global Harmonization Task Force - GHTF/SG3/N15R8

Medical device regulations for risk management

International standards ISO 14971, ISO 13485, and IEC 60601 mandate the documentation of a medical device manufacturer's risk management process. During the Premarket Approval (PMA) process for medical devices, including 510(k) and other PMA documentation requirements, a documented risk analysis process for the hardware, software, and electronic components used in medical devices is required by the FDA. Risk management is reported under these requirements using a risk management file, which contains all of the documents, records, and other supporting materials produced by the risk management process so that the process is both traceable to functional and safety requirements and transparent to regulatory agencies.

ISO 14971

As an internationally recognized standard for medical device manufacturers, ISO 14971 establishes risk management as an essential part of ensuring the safety and reliability of medical devices. Derived from ISO 13485, which requires a documented product realization process, ISO 14971 specifies that this process should include risk management. This standard:

- Specifies a framework manufacturers must use to identify the hazards associated with a medical device, including in vitro diagnostic medical equipment
- Requires companies to conduct and document a risk management process, which it defines fully as described above
- Applies to all stages of the product lifecycle, from its design and development through its decommissioning and disposal
- Calls for the evaluation and assessment of risks to patient, operator, and others; and extends to the equipment itself, other equipment, and the surrounding environment
- Mandates device monitoring throughout production and postmarket use, including the reevaluation of device risks should new or unexpected hazards arise

IEC 60601

This standard identifies required safety standards for electrical medical equipment, which may be defined as equipment connected to a power supply and used in diagnosis, treatment, or monitoring of a patient; which makes physical or electrical contact with the patient, transfers energy to or from the patient, and/or detects energy transfer to or from the patient. This standard also extends to accessories used with such equipment. This standard:

- Sets specific requirements for electromagnetic compatibility, human factors such as the usability of devices, and specific types of applications such as devices used during surgery
- Defines hazards ranging from electrical shock, mechanical sources of harm, radiation, ignition or fire, and excessive energy output
- Requires the use of risk controls including safety by design, protective measures taken during manufacturing, and instructions or labeling information for safety
- Identifies performance requirements—that is, characteristics of a system which are required to maintain residual risk
- Mandates risk analysis activities for specific areas of product design, including protection against shock, protection against the entry of liquids, and the use of flammable materials

Medical Device Standard	Definition
ISO 14971	Establishes the requirements of risk management for ensuring the safety and reliability of medical devices
IEC 60601	Identifies required safety standards for electromedical equipment
ISO/TR 80002	Applies the risk management requirements of ISO 14971 to medical device software
IEC 62304	Defines lifecycle requirements for medical device software to establish a framework for software development and maintenance
21 CFR Part 11	Requires that any software used to develop and manufacturer medical devices meet certain standards for data security and integrity
Verification and Validation	Defines testing procedures to ensure medical device software specifications meet functional needs and software fulfills its design specifications

Figure 3: Several key international standards for medical device reliability and medical device software reliability are outlined above.

Methods for risk analysis, estimation, and control

Several commonly used analysis techniques address the risk management requirements of medical device systems. These methods are used to identify, analyze, control, and monitor medical device safety and risks across the product lifecycle.

Methods to evaluate and mitigate sources of risk

When tracing the possible risks inherent in medical device software or systems, FMEA–or Failure Modes and Effects Analysis–and Fault Tree Analysis are often used.

- **FMEA**: An FMEA is a bottom-up analysis method used to identify each potential failure mode for all of the parts in a system and trace these effects up through the system's hierarchy to identify negative effects at the subassembly, assembly, and system levels
- **Fault Tree**: A Fault Tree is a top-down analysis method, wherein the undesirable end event is identified first and all contributing factors or events are identified next to determine which component or process failures are most critical

When part failures contribute to system risks

To evaluate and mitigate part failures that contribute to risks, reliability prediction analysis and advanced system modeling techniques are often used:

- **Reliability Prediction**: During a reliability prediction analysis, the likely failure rate of a system may be predicted in the design phase. Reliability prediction establishes system performance metrics using information about the parts that comprise the system. This part information is gleaned from extensive libraries of electronic and nonelectronic components and how they react to various environmental stresses. Reliability prediction can also provide insight into alternative, more reliable system designs through trade-off studies that analyze the effects of alternate part designs on overall system reliability.
- **Advanced System Modeling**: When more complex systems are analyzed for reliability, advanced system modeling techniques including reliability block diagrams (RBDs) and optimization and simulation analyses are used to model and predict system behavior. Complex system designs supporting parallel redundancy or part dependency can demonstrate improved reliability, helping to mitigate risks due to system failures.

Methods to monitor and analyze field performance

To fulfill the requirements of medical device regulations to monitor devices during production and postproduction for any additional or unexpectedly severe risks, a CAPA–or Corrective and Preventive Action (also known as Corrective Action / Preventive Action)–is often used, to track part failure data. To ensure this data can be analyzed using statistical methods, a FRACAS (Failure Reporting and Corrective Action System) may be used for data gathering and analysis, together with Weibull for advanced statistical analysis.

- **CAPA and/or FRACAS**: To track system requirements for safety and quality against actual, fielded system performance, a Corrective and Preventive Action system, also known as a FRACAS, or Failure Reporting, Analysis, and Corrective Action System, is often used. When failures or issues arise, they may be collected, organized, and tracked in an automated system, with each issue being addressed by a closed loop system to ensure necessary personnel evaluate the issue for risk, severity, and necessary actions.
- **Weibull**: Used to transform part failure data into key system metrics like failure rate and reliability, Weibull analysis is used to ensure that fielded part performance–and therefore system performance–aligns with predicted values.

Methods to analyze, evaluate, and Mitigate risks

Using a FMEA process

An FMEA is a systematic method for identifying all of the potential failures throughout a system and developing controls to minimize or prevent their occurrence or effects. An FMEA is a bottom-up approach that identifies each failure mode, beginning with the lowest-level components in the system, and examines the effects of their failures on higher levels of the system. In this way, an FMEA can trace the end effects of part failures through to system-level failure and the risks or hazards it can cause. An FMEA can also include an analysis of the criticality of each failure mode: an analysis method often referred to as an FMECA (Failure Mode, Effects, and Criticality Analysis) whereby potential failure modes are classified according to their severity or risk.

An FMEA is an extremely flexible analysis tool, as it may apply to the product itself or to the process of using the medical device. Its flexibility makes this method ideal for meeting the standards imposed by medical device regulations.

There are many types of FMEAs, several of which are described below:

- A **Product FMEA** examines the ways in which hardware or software can fail and the effects that failure can have on product operation
- A **Process FMEA** examines the ways in which manufacturing and assembly processes can affect device operation and product quality; it may also be applied to the way in which the tool is used, systematically identifying the consequences of improper use on device failure and/or potential hazards
- A **Functional FMEA** may be used to focus on the functions that a product or service is designed to fulfill
- An **Interface FMEA** can be used to analyze the interconnections between system elements
- A **Detailed FMEA** is used to ensure that designs comply with requirements for failures that can cause a loss of end-item function

When any of these various types of FMEAs is performed in the design stage to identify and evaluate the potential failure modes of the system and their effects, it is known as a Design FMEA. This type of FMEA uses information about the parts or

Risk Management Activity	Reliability Analysis Method	Application of Reliability Analysis Method
Risk Identification & Analysis	FMEA (Failure Mode & Effects Analysis)	• Perform and document a bottom-up analysis tracing part or process failures through to negative end effects
	Fault Tree Analysis	• Perform and document a top-down analysis tracing negative end effects to all possible sources at the part or process level
Risk Estimation	FMEA	• Assign Risk Priority Numbers to estimate the severity of risks and group by criticality.
	Fault Tree Analysis	• Perform quantitative analysis to calculate risk severity by minimum combination of causal events
	Reliability Prediction System Modeling	• When a risk is the result of a part failure, quantify the probability that the risk will occur.
Risk Control Measures: • Analyze • Implement • Evaluate • Risk/Benefit Analysis • Review New Risks • Completeness of Risk Control Measures	FMEA & Fault Tree Analysis	• Study the bottom-up (FMEA) or top-down (Fault Tree) effects of risk control measures at the part- or process-level
	Reliability Prediction	• Quantify the effects of alternate part designs on improved part reliability and improved product safety
	System Modeling	• Quantify the effects of building in redundancy, dependency, or parallel structure to system design; estimate the efficacy of preventive maintenance or repair activities
Production and post-production monitoring & re-evaluation of found risks	FRACAS (Failure Reporting, Analysis, and Corrective Action System)	• Collect and analyze field data to track new and unexpected risks • Initiate risk evaluation and control plan development for newly detected risks using a closed loop process to ensure all risks are addressed
	Weibull Analysis	• Analyze collected field data to quantify part or system failure behavior • Validate predicted performance by analyzing field data to demonstrate that design and safety requirements are being met

Figure 4: Risk management activities rely on a number of reliability analysis methods to ensure the systematic identification and analysis of risks, estimation of severity and occurrence of risk, implementation and evaluation of risk control measures, and the production and post-production monitoring of devices and their additional risks.

processes which will comprise the system to identify important design problems early in the product development process. By anticipating these problems, design changes can be made to prevent or minimize their consequences. Identifying necessary design changes to minimize risk early in the product development process can amount to significant savings in both cost and resources.

A FMEA offers several ways to incorporate an analysis of criticality and severity of risk:

- In one method, known as mode criticality, a numerical value is calculated and assigned to each failure mode in a FMEA; these values can be linked to the failure rate of the system hardware when part failures contribute to risk
- Another method, criticality rank, allows for the systematic ranking of failure modes, wherein modes are assessed by their severity and probability to identify those that are the most critical to the functioning of the system
- A final method, risk levels, groups failure modes into categories to ensure the most critical ones are evaluated first. FMEA software offers a wide range of output types including graphs and reports to easily track criticality information

Using Fault Tree Analysis

Using a top-down approach, Fault Tree Analysis begins at the system level by identifying the failure or undesired event, and then systematically identifies the lower-level factors or events that contribute to the top-level event.

Fault Tree Analysis offers the distinct advantage of an event-oriented methodology for evaluating the likelihood of occurrence of a system or component failure. As an extremely flexible analysis methodology, fault tree allows for the incorporation of a number of different contributing events, including a combination of software or hardware failures, human errors, and environmental influences all within a single Fault Tree.

By using a logic tree to graphically represent the contributing events, Fault Tree Analysis can employ quantitative or qualitative analysis to determine the criticality of each contributing factor, identify the minimum combination of contributing factors that can lead to the failure, and assist in the development of control measures that would prevent or mitigate the circumstances leading to the top-level failure or event.

Additional quantitative techniques available in Fault Tree Analysis use failure and repair data about lower-level components to calculate the likelihood of the top-level event.

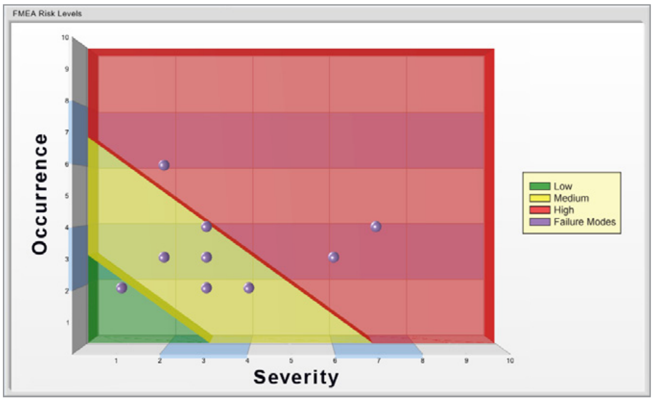
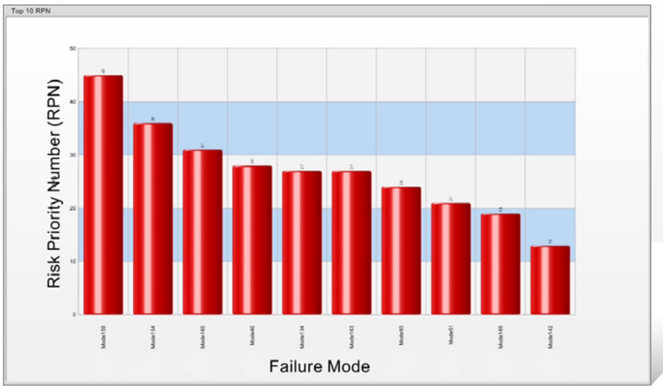


Figure 5: A FMEA Risk Level graph (above) allows for the analysis of events by occurrence and severity in order to quantify risk and prioritize issues to address. A ranking of top Risk Priority Numbers (below) allows for easy review of the top issues by severity, occurrence, and detection.



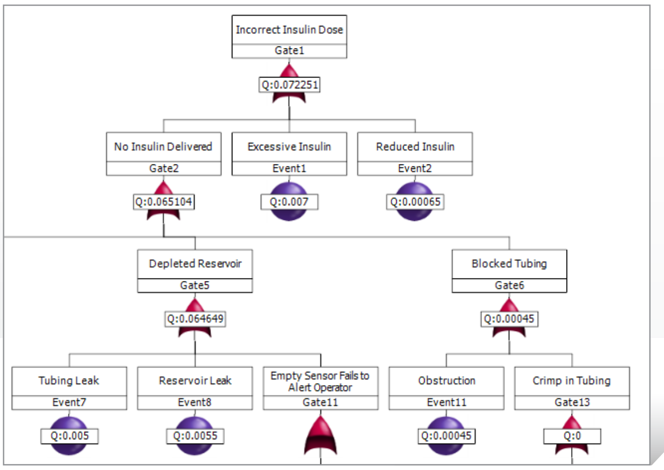
Fault Tree Analysis also incorporates importance measures, which help the analyst determine which contributing factor to improve by identifying the criticality of contributing events, including the probability that the top event is a contributing factor as well as the maximum risk to the system if the contributing factor is failed versus if it is operational.

Comparing FMEA and Fault Tree Analyses

Recall that FMEA is a bottom-up analysis methodology, beginning with the identification of the potential failure modes of component parts and identifying the effects of their failures on subassemblies, assemblies, and, ultimately, the system as a whole. In contrast, Fault Tree Analysis employs a top-down method: beginning with the undesirable top-level event and identifying the events and factors–down to the failure of lowest-level components or processes–that may contribute to the top-level failure. FMEA and Fault Tree analyses can be

	FMEA Tree Item	Hazard	Harm	Cause
6	Reservoir	Leaking	Insulin Loss	bad gasket
7				obstruction
8	Implantable Infusion Set	Disengages	No insulin delivery	Oily skin
9		Leak	Reduced insulin delivery	overpressure
10				bad fitting
11		Deteriorated	Reduced insulin delivery	age
12				chemical exposure
13	Tubing			

Figure 6: Compare the same information evaluated in a FMEA (above) and a Fault Tree (below).



used together. When it is easier to identify an end-level failure and work backward to determine what caused it, Fault Tree is ideal.

From those lower-level failures, a FMEA may be generated to determine other effects they could have throughout the system. Similarly, when a FMEA process has identified system-level failures caused by failures in lower levels of the system, a Fault Tree analysis can be incorporated to identify other sources that may also contribute to the failure.

When part failures contribute to risks

Using Reliability Prediction

A reliability prediction analysis is a crucial step during product development to determine whether product performance under anticipated conditions will match the goals established for it by industry standards or organizational objectives. By modeling the system in a linear fashion, reliability prediction enables the reliability of the system overall to be calculated from the combined reliability parameters of its component parts. Reliability prediction enables the quantification of expected product performance at the very earliest stages of the design process, the comparison of alternative designs which may be used to control or mitigate part failures that can lead to risks, the identification of leading contributors to system failure, the evaluation of the impact of various levels of environmental stresses on a system, and the prediction of accurate system metrics using part data for the exact components used in the system.

Using advanced system modeling techniques

When a system demonstrates the inherent complexity of nonlinear construction—such as redundancy, dependency, various operating profiles, or parallel structure—the system is more commonly modeled using reliability block diagrams (RBDs), which are used to predict system output with sophisticated optimization and simulation calculations. These more sophisticated calculation techniques provide for the modeling of the most complex systems, including their repair procedures, spares needs, and inspection or preventive maintenance intervals.

Methods to track and analyze risks in the field

What is a corrective action system?

An essential component of risk management involves the monitoring of risk control measures after a product has been released into the field and the identification and analysis of additional system failures and unanticipated risks to the patient, operator, equipment, or environment. To log failures or incidents and ensure that each one is analyzed to determine its root cause, a systematic process known as a FRACAS—Failure Reporting, Analysis, and Corrective Action System—is used. Also referred to as a CAPA (Corrective and Preventive Action) or just a Corrective Action system, a FRACAS is used to ensure that failures are addressed using a closed loop process so that every reported failure is resolved. It also ensures that all reported failures and the actions taken to address them are electronically recorded and fully traceable—from logging the failure through failure correction and resolution.

Using Weibull Analysis

Advanced statistical calculations used in Weibull analysis provide the ability to analyze collected field data and identify the characteristic failure behavior, also known as the failure distribution, of a system. This analysis supplies important information about the system, including the probability of Failure or Reliability at a given age, the chances of part failure given survival until a certain age, reliability growth calculations used during product development, and degradation analysis to identify the wear-out behavior of the part at the end of its life.

This data is often collected from a FRACAS process, analyzed using Weibull analysis, and fed back into a reliability prediction analysis or a reliability block diagram analysis, helping to ensure that future performance and safety analyses are accurate for the specific parts and systems being used in medical device production.

The benefits of integrating the analyses

Using a single system to perform an integrated risk analysis

Performing a completely integrated risk analysis over the lifecycle of the product, in which each analysis type is tightly interwoven with the next, helps to ensure visibility into all risk management processes for stakeholders across the organization, and provides for the ready compilation of risk management activities when it comes time to fulfill documentation requirements. Integrating risk management activities and analyses within a single software package also helps to prevent unnecessary redundancy in data entry and the errors that may accompany it.

Linking analyses helps to ensure that data from one analysis type informs the next. For example, the quantitative data generated by reliability prediction or advanced system modeling–including part failure rate–can be linked directly into a FMEA or Fault Tree process to help evaluate the severity of risk based on the probability of a part failing. And when system design is changed to accommodate a risk control measure, the FMEA or Fault Tree can be instantly updated with the failure rate of the new part, eliminating the extra time it takes to re-evaluate the risk with the new part in place. Finally, during production and post-production device monitoring, results recorded in a CAPA or FRACAS can be used to generate a FMEA and evaluate any new risks that may have arisen, as required in standards such as ISO 14971, and inform future system models for more accurate quantitative data tracking the real-world performance of parts and systems.

About Windchill Quality Solutions

Windchill Quality Solutions offers each of these tools in an intuitive, easy-to-use, and uniquely integrated software suite. In addition to automated processes within FMEA, Fault Tree, and FRACAS–and Reliability Prediction methods that streamline analysis activities to dramatically reduce analysis time–Windchill Quality Solutions offer:

- Software solutions that address the medical device reliability standards and regulations discussed here
- Supplied parts libraries containing reliability data information on hundreds of thousands of commonly used electrical and mechanical components
- Fully integrated database construction allowing for the ability to store past reliability analysis information, part information, system configurations, and risk mitigation activities for future analyses
- The ability to assign quantitative values to the severity of risk using RPN, Criticality Rank, or Risk Levels: three common methods in quantifying medical device risks
- Seamless integration of risk analysis activities, allowing part or system performance data generated from a reliability prediction or a reliability block diagram to be figured into a fault tree analysis or a FMEA to determine

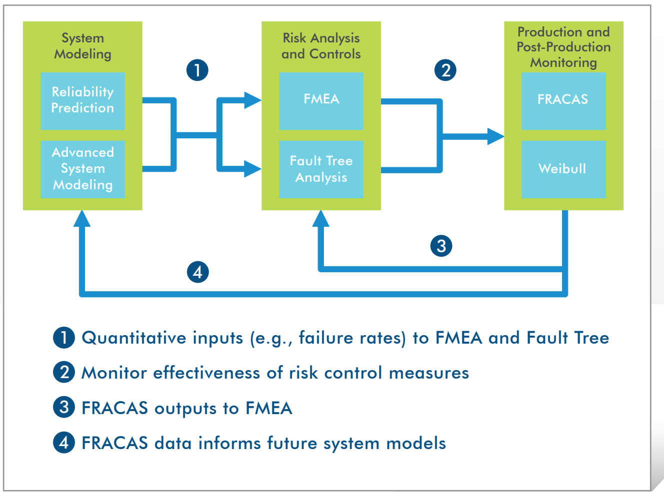


Figure 7: Integrating the analysis types via a single software package eliminates unnecessary redundancy, ensures that quantitative data informs risk analysis, automates risk monitoring in post-production, and feeds found risks back into the risk management process as required by government standards.

part or process risks; the generation of a fault tree from a FMEA for a more complete analysis; and the generation of a FMEA from the incidents recorded in a FRACAS

- Fully configurable workflows enabling identified system risks or part failures to be advanced through a closed loop process to complete essential risk management activities including root cause analysis, risk assessment and evaluation, the design of control measures, review and approval of change requests, documentation of activities in the risk management file, and so on.

Finally, Windchill Quality Solutions adhere to the quality standards for software used in the development and production of medical devices, including 21 CFR Part 11, which requires the use of closed systems, administrator controls to define the level of access for every group or user in the system, password-protected login at the terminal level, and audit tracking capabilities to identify and record each change made to the system. The development team responsible for Windchill Quality Solutions performs the in-depth testing processes required by verification and validation, and can supply the FDA-required documentation of this compliance upon request.

Learn more

For more information about Windchill Quality Solutions, please visit PTC.com/products/windchill/quality.

Bibliography

1. Dhillon, B. S. *Medical Device Reliability and Associated Areas.* 2000. CRC Press: Boca Raton, FL.

2. Eisner, Leonard, Robert M. Brown and Dan Modi. "A Primer for IEC 60601-1." *Medical Device and Diagnostic Industry.* Available December, 2009 at http://www.601help.com/Basic_Concepts/regulatory_outlook.htm.

3. The Global Harmonization Task Force, (2005). *Implementation of risk management principles and activities within a Quality Management System.* GHTF/SG3/N15R8.

4. International Organization for Standards. (2007). *Medical devices–Application of risk management to medical devices.* ISO 14971

5. "Medical Device Exemptions 510(k) and GMP Requirements." *U.S. Department of Health & Human Services.* Available Dec., 2009 at http://www.fda.gov

6. Ozog, Henry. "Risk Management in Medical Device Design." *Medical Device & Diagnostic Industry.* Available December, 2009 at http://www.devicelink.com/mddi/archive/97/10/023.html

7. "Pharmaceutical cGMPS for the 21st Century–A Risk-Based Approach: Second Progress Report and Implementation Plan." *U.S. Department of Health & Human Services.* Available December, 2009 at http://www.fda.gov

8. "Required Submission of Safety and Effectiveness Information for Certain Class III Devices." *U.S. Department of Health & Human Services.* Available December, 2009 at http://www.fda.gov

9. Rudolph, Harvey and Charles Sidebottom. "The Role of Risk Management in the New IEC 60601-1. *Medical Device & Diagnostic Industry.* Available December, 2009 at http://www.devicelink.com/mddi/archive/06/01/013.html.

10. Schmidt, Mike. "The Use and Misuse of FMEA in Risk Analysis." *Medical Device & Diagnostic Industry.* Available December, 2009 at http://www.devicelink.com/mddi/archive/04/03/001.html

11. Tran, Eushiuan. "Verification/Validation/Certification." Carnegie Mellon University. (1999). Available December, 2009 at http://www.ece.cmu.edu/~koopman/des_s99/verification/

12. U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Heath, Center for Biologics Evaluation and Research. *General Principles of Software Validation; Final Guidance for Industry and FDA Staff.* 2002.

6531–Medical–Device–Reliability–WP–EN–0511