Jama software®

WHITEPAPER

Understanding Integrated Risk Management for Medical Devices

Knowledge on best practices, how to integrate risk-based thinking into product development cycles, and the importance of having end-to-end traceability to improve risk management, shared by industry and solution experts.

Understanding Integrated Risk Management for Medical Devices

A level of risk exists with all medical devices, no matter how simple they are. Companies developing medical devices are constantly considering who (or what environment, facility, etc.) could potentially be hurt by a device so they can help reduce risk and meet regulatory requirements. Risk management in the context of ISO 14971 is designed to support medical device manufacturers with these tasks — but not all approaches are equal.

The amount of time it takes to manage risks, connect specific risks to specific requirement tasks, and pull together required documents to respond to an audit varies slightly depending on the approach. The risk management process is an integrated process that not only includes teams in product development, quality, but also many other parts of an organization.

This whitepaper taps into the knowledge of industry and solution experts to uncover best practices, how to integrate risk-based thinking into product development cycles, and the importance of having end-to-end traceability to improve risk management.

Before we dig into integrated risk management, let's first define some key terms.

Risk Management Terms According to ISO 14971

Harm — Harm occurs when people are injured physically or their health is compromised or when property or the environment is damaged.

Hazard — A hazard is a potential source of harm. Annex E.2 categorizes hazards in the following way: energy hazards, chemical hazards, biological hazards, operational hazards, and informational hazards.

Hazardous Situation — A hazardous situation occurs when people are exposed to a hazard or when property or the environment is threatened. A hazardous situation exists when a vulnerable entity is exposed to a hazard.

Risk — According to ISO 14971, the concept of risk combines two variables: the probability of harm and the severity of harm.

For example, if a particular hazardous situation is very likely to cause harm and would be very harmful if it actually occurred, then it would be a high risk situation. Conversely, if it's very unlikely to cause harm and would be only slightly harmful if it actually occurred, then it would be a trivial risk.

Risk Analysis

Risk analysis is a systematic process that is used to identify hazards and to estimate risk. It includes an examination of every reasonably foreseeable sequence or combination of events that could produce a hazardous situation and cause harm.

Risk Assessment

Risk assessment is a process that is, in turn, made up of two interconnected processes: risk analysis and risk evaluation.

Risk Evaluation

Risk evaluation is a process that is used to examine the estimated risk for each hazardous situation and then to use risk acceptability criteria to determine whether or not the estimated risk is acceptable and to decide if risk reduction is required.

Risk Control

Risk control is a process that is used to consider risk control options and to select and implement risk control measures that will reduce risk or maintain risk within specified levels. ISO 14971 expects you to consider the following risk control options and, if possible, to apply them in the following order:

1. Design safety into the product.
2. Establish protective measures.
3. Provide safety information.

Risk Estimation

Risk estimation is a process that is used to assign qualitative or quantitative probability values and severity values to each hazardous situation. These values are then used to estimate risk.

Risk Management

Risk management uses policies, procedures, and practices to systematically analyze, evaluate, control, and monitor risk.

Safety

Safety is freedom from unacceptable risk. Risk acceptability criteria are used to help decide whether or not a risk is unacceptable.

Severity

Severity is a measure of the possible harmful consequences that a hazard could potentially cause.

The Risk Management Process

During risk management — after one defines a device's intended use(s) — risk analysis can begin with identifying all potential hazards, and hazardous situations. Once this is defined, risk can be estimated and can determine the type of appropriate risk control required. Once the risk controls are implemented, residual risk needs to be analyzed to ensure that the benefits outweigh the risks. Let's take a look at what's involved in the risk management process.

Identifying hazards

"Risk" is defined as the severity and probability that harm will occur. Defining the severity of harm requires you to identify all the known and foreseeable hazards for both intended and unintended uses.

For example, let's say you have an infusion pump, and that pump has air in the line, which creates a hazardous situation for the patient. Different levels of patient harm can occur, so it's about uncovering the possible scenarios and the likelihood of a situation's occurring.

Risk Level		Severity				
		S-1	S-2	S-3	S-4	S-5
Probability of Occurance of Harm	0-1	Low	Low	Low	Low	Medium
	0-2	Low	Low	Low	Medium	Medium
	0-3	Low	Low	Medium	Medium	High
	0-4	Low	Medium	Medium	High	High
	0-5	Medium	Medium	High	High	High

Understanding harm

Understanding harm includes both people and property. A medical device that catches fire might threaten property, while an infusion pump with air in the line might threaten human life. Think about what could cause harm to people, like a shark swimming in the water. A shark that attacks a person could create different levels of harm. A few examples include loss of a limb, an infection from getting bitten and loss of life. The various levels of harm result from the hazardous situation, which is the shark in the water.

Harm
Shark attack can result in different levels of harm.

Death | Loss of limb | Bleeding | Infection

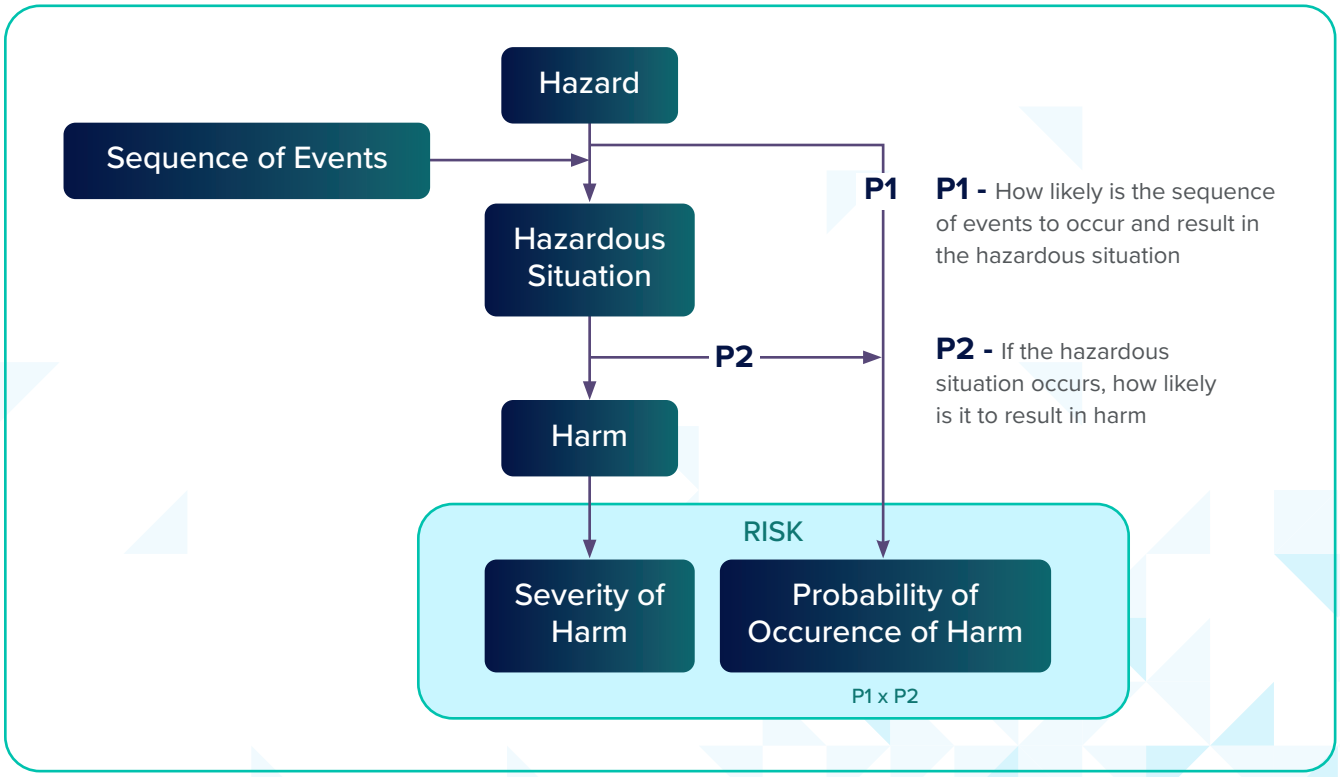
Risk evaluation

Risk evaluation involves comparing an estimated risk against a specific criterion to determine if a risk is acceptable. Five different levels to evaluate risk are common practice, but you can use as many as you'd like. The most severe risk (level five) might include death or impairment. Level one might include no risk to a patient or operator. The levels inbetween include all the other varying degrees of risk.

Sequence of events

A hazardous event includes a number of steps, which is the sequence of events. A risk situation might have two, three, or more steps that, when aligned, create a hazardous event. Risk management tools such as fault trees and failure modes and effects analysis (FMEA) help identify these steps.

Previous version of ISO 14971 used terms like "acceptable" and "unacceptable" to describe risks, but that language has since been removed and the most current version maintains as low as possible (ALAP). The goal of every manufacturer is to lower the risk as much as possible and rethinking how to prioritize risk controls can help.



Analyzing Risk Control Options: How Do We Reduce Risk?

Analyzing risk control options involves making decisions and implementing measures to reduce risk or maintain that risk within specific levels. Risk controls can reduce the probability of occurrence or harm, or both.

When analyzing each risk control option, consider:

- Does the design of the risk control directly reduce or eliminate the risk?
- Do any protective measures safeguard against risk?
- Does the risk control inform the user about any residual risk and provide information to avoid or reduce that risk?

Consider the example of the infusion pump with air in the line. Maybe you design a detector that recognizes there's air in the line and automatically stops treatment. This risk control prevents the risk of embolism, but in eliminating this risk, it introduces a new one – delaying therapy. Of course, stopping treatment is likely a preferable risk compared with having an embolism.

Manufacturers also need to consider if implementing a risk control is technologically and economically feasible. For example, let's say that you could design an airplane that could survive a crash. You discover that, yes, it is technologically possible to do this, but the cost for each ticket would be $1 million – so, it's not economically feasible.

Select the risk controls that reduce risk as much as possible while still being feasible. Re-estimate your risk after selecting the controls, and remember that controls should be translated to requirements that can be verified.

Risk Management Tools

Risk management tools help you take a closer look at all components of a risk and reduce them as much as possible. If you're running a system-level risk and hazard analysis for an infusion system device, for example, you might have the infusion pump, a tubing set, solution bags, and a number of other components to operate the system.

You can look at every element of the system with risk management tools to make sure the elements are as safe as possible. You can answer questions such as "How well does the system detect a hazard?" and "How can you control that hazard?"

Consideration for integration is required to use tools more effectively so that you have a relationship between all the different levels of analysis performance.

Here are some considerations for various tools:

Fault tree analysis

A fault tree analysis is a top-down tool because you start with a top event. For example, consider an event that causes harm, such as an air embolism. You might say, "An air embolism is caused by air infused into the patient." But what causes air to be infused into the patient? Maybe it's piping or some other element.

A fault tree analysis helps you identify specific hazards and the sequence of events that led to those hazards. You need to account for any intended uses — and also reasonable misuses — throughout the entire product lifecycle.

To learn more about ISO TR 24971:2020, the companion document or technical report for ISO 14971, visit this page.

Leading with a Top-Down Approach

Risk management should be practiced as a system-level activity, which is why it's best to lead with a top-down approach. Here's a quick explanation of how top-down and bottom-up approaches can work in synergy.

Top-Down: A top-down approach helps analyse system risk early with only the intended use. You can attempt to mitigate hazards and drive risk controls through requirements that get implemented into the design, so only the system can cause a hazard.

Bottom-Up: Bottom-up analysis, such as FMEA, is still important and valuable to validate what you did during the top-down analysis. But if you're performing only a bottom-up analysis, you're only defining that the system is sequential, not influencing the design of the system.

Hazard analysis

Hazard analysis considers any foreseeable hazards, such as, “The pump will likely fail in 10 years, so preventive maintenance is required.” The analysis is done at the environment level and drives hazard analysis and risk controls – both of which should drive system-level requirements. The goal is to identify a list of “harms,” the hazards that cause those harms, and the users who could be affected by the harms.

FMEA

Risk management is focused on eliminating risk that can cause harm to people or the environment. In contrast, FMEA is focused on preventing failures that can cause customer dissatisfaction.

Not everything included in FMEA causes a risk. Some factors are still important because they impact the customer experience. For example, needing to complete three steps instead of one to use a device could adversely impact the customer experience.

If you do a hazard analysis, you don’t necessarily need to complete an FMEA, but doing so helps with a more robust design. A few types of FMEA to consider include:

- **Use FMEA**. A use FMEA looks at how a user might perform their task and how they can fail to perform that task correctly.
- **Design FMEA**. A design FMEA can be performed at any level, system or subsystem component, and it can be completed during development, before the product is in the field. For example, if you’re using a part in a new application, you might want to perform a design FMEA to see if there are any new failure modes. Even after launch, FMEA should be revisited and updated according to continually manage risk.
- **Software FMEA**. A software FMEA is similar to a design FMEA. Software risk controls are designed to build confidence that the software was developed correctly and ensure the software development process is robust.
- **Process FMEA**. A process FMEA looks at each process step to identify risks and possible errors from many different sources.

Risk management tools help create the safest possible product during the design phase, but most manufacturers know the job doesn’t stop there. Managing post-production risk helps keep safety at the forefront throughout the product life cycle.

Post-production Risk Management

Revisiting your risk management document to address any new concerns during postproduction is a critical part of safety. Maybe you're getting a large number of service calls due to a failing part, or perhaps you have a recall or other corrective actions coming up. Any of these events could trigger a need to update a document in your risk management file.

With the right level of traceability, you can easily determine if an event triggers the need to update other documents. For example, service records might show that you continually need to replace a part due to failure, so you might look at FMEA and increase your probability of occurrence. That change might then increase the probability of occurrence of some hazard at the hazard analysis level. Having the right level of traceability allows you to see what interacts with what, so that you can maintain your risk management file and update the correct documents, given the events.

Traceability

Traceability is critical as you maintain your files, but it's also important for compliance and responding to audits. Manufacturers often don't trace risk controls directly to the requirements. As a result, demonstrating requirements and effectiveness of controls gets challenging. When tracing risk controls to requirements, those requirements should also be traced to verification evidence.

Live Traceability™ is the ability for any engineer at any time to see the most up to date and complete upstream and downstream information for any requirement — no matter the stage of systems development or how many siloed tools and teams it spans. This enables the engineering process to be managed through data, and its performance improved in real time.

Live Traceability of system requirements is required by industry standards to ensure product safety and forms the foundation for digital engineering and model-based systems engineering. It delivers significant productivity improvements, and dramatically reduces the risk of product delays, cost overruns, defects, rework, and recalls — resulting in better product outcomes and faster time to market.

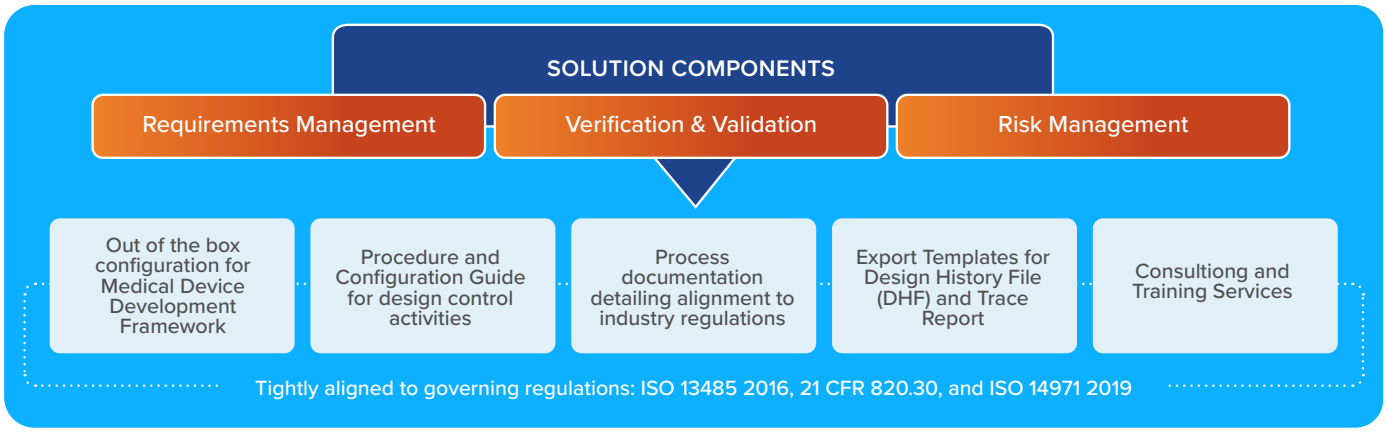
>> Learn More About Live Traceability

The right tools help you keep up to date with compliance and improve your audit readiness. **Jama Connect® for Medical Device Development** is a single platform for managing design controls for device requirements and related risks.

With Jama Connect, you can:

- **Easily demonstrate traceability.** Traceability ensures that design inputs have been met and verified, providing necessary evidence from the design control process. Jama Connect allows you to easily produce traceability documentation required by regulators.
- **Provide design verification and validation.** Seamlessly manage traceability to verifications and validations, providing evidence to comply with government regulations and standards, like 21 CFR Part 820.30.
- **Manage risk analysis.** Manage risk analysis in alignment with ISO 14971:2019. Jama Connect helps teams identify and mitigate risks earlier in development, saving teams from frustrating late-stage design changes and supporting the path to regulatory compliance.
- **Maintain audit trails and export data.** Real-time reporting and baselining allow you to track all changes to information within the system, including timestamps and associated users. Data is easily exported from Jama Connect if your current process dictates storage of documentation in a quality management system.
- **Manage compliance reviews and approvals.** Increase early stakeholder visibility and participation in the review process with e-signatures that are compliant with FDA 21 CFR Part 11.

Jama Connect for Medical Device Development is designed to help you get ramped up quickly, with a platform, training and documentation aligned to industry regulations, plus a proven systems engineering approach to product development.



BASE FEATURES | INTEGRATIONS | PROFESSIONAL SERVICES | ADDITIONAL CAPABILITIES

To learn more about Jama Connect, start a free trial, or speak with one of our industy experts, contact us here.

Jama Software® is focused on maximizing innovation success in multidisciplinary engineering organizations. Numerous firsts for humanity in fields such as fuel cells, electrification, space, software-defined vehicles, surgical robotics, and more all rely on Jama Connect® requirements management software to minimize the risk of defects, rework, cost overruns, and recalls. Using Jama Connect, engineering organizations can now intelligently manage the development process by leveraging Live Traceability™ across best-of-breed tools to measurably improve outcomes. Our rapidly growing customer base spans the automotive, medical device, life sciences, semiconductor, aerospace & defense, industrial manufacturing, consumer electronics, financial services, and insurance industries. To learn more, please visit us at jamasoftware.com.