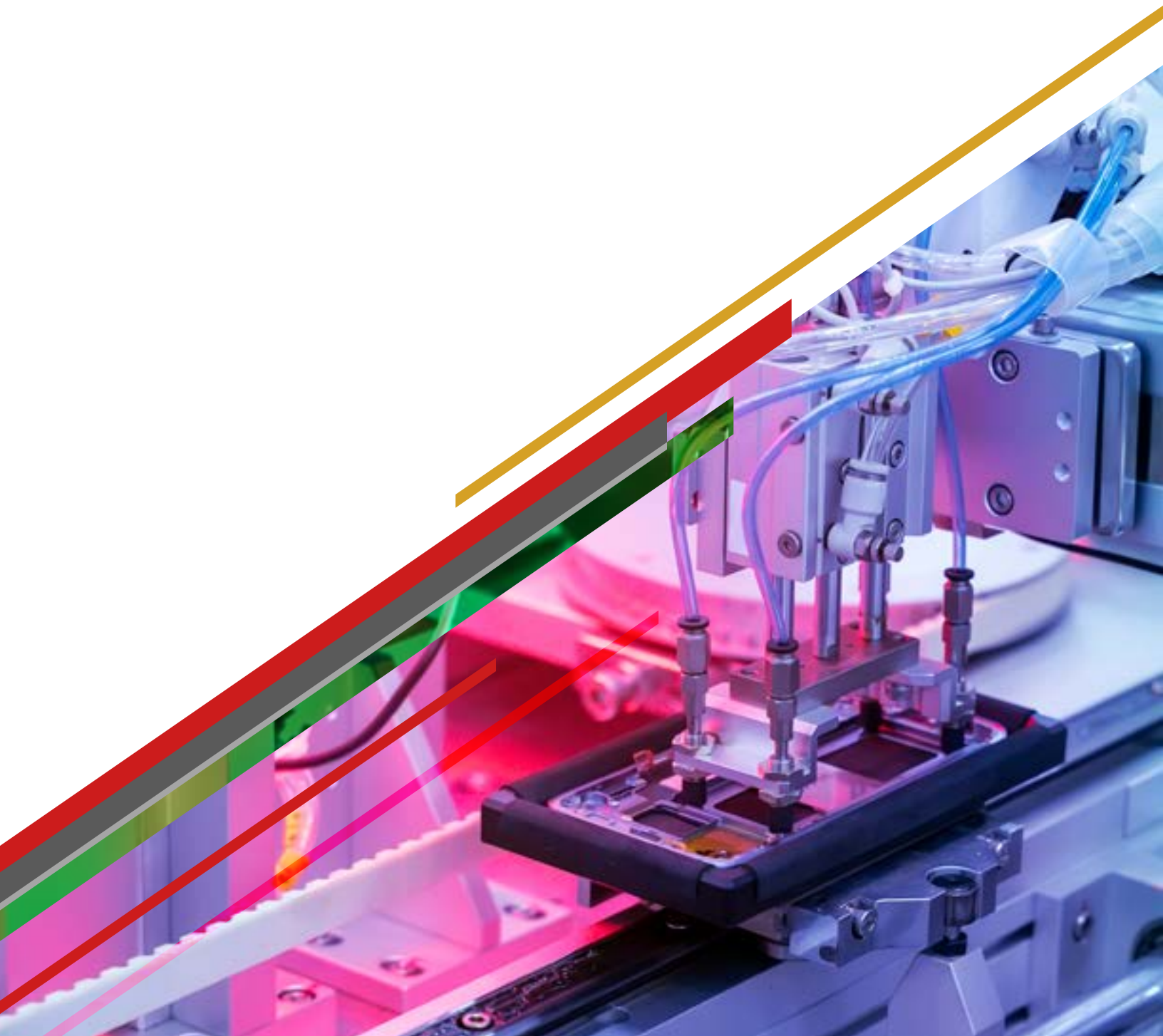
WHITE PAPER

Risk Management in Medical Device Development



ENSURING SAFETY AND EFFICACY FOR THE MEDICAL DEVICE ECOSYSTEM

In the development and marketing of medical devices, a special case of risk management arises which involves designing, ensuring, and certifying the safety of these devices for human interaction in various settings such as daily patient care, invasive or non-invasive diagnostic procedures, or scientific research. The risks may extend to other patients, operators, external equipment or the environment on a micro or macro scale. Developers have the obligation to identify, understand, and mitigate or accept risk on behalf of all stakeholders—users and operators of the device, company officials who certify compliance, and shareholders of interest in the profitability of the company.

CHALLENGES

The journey to design a device for certification is getting increasingly perilous, with many factors, some old, but many new to the practice such as an ever-expanding global market, software as a device, telemedicine and home health, and the ever shrinking or miniaturization of products to meet environmental and usability requirements. Is the "tricorder' of Star Trek legend here or just over the horizon? Any or all of these factors are risks and opportunities that must be identified, analyzed, accepted, mitigated or exploited early in the design process.

If the design team is unable to mitigate risk, they are:

A. in danger of non-compliance and certification for marketing of the product,
B. may face lawsuits from malfunctioning product, and shareholder wrath if the company's image is adversely affected.

Failure to properly identify and mitigate risk may result in product failures related to poor documentation, product malfunctions stemming from insufficient testing or simulation, as most of the simple medical devices have already been perfected. Most of today's devices have a software component and, in many cases, software is the entirety or bulk of the delivered functionality, or finally manufacturing issues not properly identified. See article here for a more thorough discussion of product failures: "Products Fail; four Ways to Mitigate It".

BENEFITS

On the other hand, there are many benefits to Risk Management. The risk management process aims to reduce risks to their lowest possible level to prevent harm to the patient, operators or other stakeholders. Ensuring safety for patients and operators and other stakeholders is the primary reason for risk management in medical devices. Risk Management is a regulatory requirement and in order to get FDA or the European MDR approval for marketing your product, you need to have a documented risk management process in place.

REALITIES

In a perfect world, all risk could be avoided through careful assessment and mitigation. The reality is we need to reduce the risks to as low as possible but there may still be residual risk and we must assess if the benefit outweighs the risk. For example, an x-ray machine radiation can cause cancer so we try to minimize the risk for x-ray operators with lead screens, but we cannot remove radiation because it is how we actually see inside the body so the benefit of seeing inside the body is greater than the risk of radiation.

Risk management is not a one-time event but continues throughout the entire lifecycle of a product. Things change. New environmental factors, technology, or studies can cause a reassessment. An example: 5G is a new technology and we may need to do a risk assessment to see if 5G interferes with heart monitors. 5G may not have been a technology when the heart monitor was released in the market so we could not do a risk assessment for this at that time but now we can. Products may also change over their lifecycle and as the product changes, a reassessment of risks is required. Your risk management documentation must reflect the changes and the updated risk assessment, and in the case of an audit, be able to report why the adjustments occurred.

REDUCING RISK

Various approaches may be employed to mitigate risk in medical devices.[1] These include:

Inherent safety through better design:

- Use specific connectors that cannot be connected to the wrong component.
- Remove features that can be mistakenly selected or eliminate an interaction when it could lead to use error.
- Improve the detectability or readability of controls, labels, and displays.
- Automate device functions that are prone to use error when users perform the task manually.

Protective measures:

- Incorporate safety mechanisms such as physical safety guards, shielded elements, or software or hardware interlocks.
- Include warning screens to advise the user of essential conditions that should exist prior to proceeding with device use, such as specific data entry.
- Use alerts for hazardous conditions, such as a "low battery" alert when an unexpected loss of the device's operation could cause harm or death.
- Use device technologies that require less maintenance or are "maintenance free."

Safety Information:

- Provide written information, such as warning or caution statements in the user manual that highlight and clearly discuss the use-related hazard.
- Train users to avoid the use error.

HOW IS IT MANAGED TODAY?

An obvious question is how is risk management accomplished in today's medical device companies? Unfortunately, many companies are still paper based. Different domains and different processes create content and data resulting from their individual tasks, decisions, and goals. The data exists in Word or Excel files, in home grown Access databases, or other home-grown systems. Content and data that live in widely dispersed emails, laptops, desktops, and remote servers not under change management or control. Those tasked with creating the actual risk assessment for sign offs and submittals to governing agencies, not a one man show but a group of experts, attempt to collate the current view into a binder comprising the Risk Management File containing the risk Management Report that is supposed to describe reality.

In general, the Risk Management Report contains the following information:

- Identifies risk by breaking down the hazards associated with the intended use or misuse of the product, the hazardous situations this can present, and the associated harm that may occur.
- An assessment of the risk s achieved by calculating the level of risk by first assessing the probability of occurrence and secondly the severity of the harm. This will determine the risk level.
- Proposed actions to mitigate the risk. These can include inherent safety through better design, protective measures, or safety Information.
- Final statement of risks that cannot be mitigated. Management must decide to accept the risk or demand further changes or mitigation.

All of the above are adjusted throughout the development process and continue through the lifecycle of the product of product in use as reported and aggregated.

GOVERNING STANDARD—ISO 14971

"Application of Risk Management to Medical Devices" ISO 14971 is a voluntary standard for the application of risk management within medical devices. It is a nine-part standard which establishes a framework for risk analysis, evaluation, control, and review, and also specifies a procedure for review and monitoring during production and post-production. It establishes objective criteria for risk acceptability but does not specify acceptable risk levels. The standard provides that a manufacturer must establish, document and retain a risk management process from conception to decommissioning.

- Reviewing the intended use (intended purpose) of the medical device
- Identification of hazards (known and foreseeable) related to:
  - biocompatibility
  - data and systems security
  - electricity
  - moving parts
  - radiation
  - usability
- Estimation of the probability of occurrence of harm
- Estimation of the severity of each hazard and its harm
- Evaluation of associated risks (decision making)
- Control of these risks
- Monitoring the effectiveness of controls throughout the whole lifecycle of a medical device.

HOW CAN WE DO BETTER?

It is clear than any effort at risk management, and risk management compliance, must have the goal of delivering a correct and current analysis of risks, mitigation measures, controls, and ongoing processes to monitor ongoing product risks. The idea that content and data held in isolated data islands under no unified controls, is unrealistic. There is no concept of traceability, how data, decisions, and results are related. No assurance that the data reflects current realities or outlooks. This is the reality faced by anyone attempting to deliver a report for management signature or compliance approval.

A paper-based process resulting in a document snapshot captured in a binder reporting the aggregation of disparate sources cannot be trusted to represent the process of determining the current state, the history of risk management and mitigation it describes, the relationship between the disconnected data, or the record of what actions were taken; their purpose or reasoning of mitigation actions taken. Such results are prone to error

including dead links, deleted data, and insufficient artifacts to describe the certainty for approvals. Paper-based systems are also time consuming representing an effort in "herding cats', to produce a report. Ultimately, such a system poses risks to end users, stakeholders, and the company relying on the risk management process and results to bring a product safely to market.

In order to alleviate many if not most of the above negative issues there are three basic strategies, technologies, or methodologies to accomplish accurate and up to date risk management processes and reporting. A modern Product Lifecycle Management (PLM) offering can provide a comprehensive solution for first putting change under control. Findings, decisions, and actions are not taken or approved without known workflows, decision verifications, and mitigating actions under formal enterprise control. This ensures that authorized people act at the right time. Secondly, all content created by the risk management process needs to be connected, from the source of the risk to the risk, to the mitigation or control developed, and to any associated evidence. Connection should not be by constant action to be taken by participants but inherently and automatically by the system. And thirdly the first two solutions, change under control and connected content and data, result in traceability, or the ability to look backwards and see how you arrived at your current state.

Change Control is enabled by:

- Enterprise change management including affected data types beyond risk management documents, risk management and its results are not isolated while occurring in multiple domains but are part of an enterprise system of control.
- Dynamic workflows and content approval cycles configured specifically for risk management processes. An FMEA process that is automated, signatories are known, easily identified, and their status is obvious.
- Change processes that encourage coordination between departments. Risk management is not performed by a single person or department but by many experts in many different domains.

Which results in:

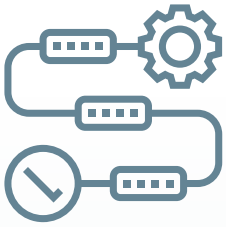
- Synchronization of the risk management processes with product configuration management, aligning and coordinating with the broader product development team.
- Targeted workflows for specific risk management analysis, decisions, and actions.
- Adaptability to future requirements. New product types, software systems replacing mechanical systems, mergers and acquisitions, and ever-changing governance and regulatory requirements all speak to the need to evolve and adapt.

Connected is enabled by:

- Controlled access to all related risk management content and data.

Which results in:

- Use and reuse of risk data and content supporting multiple instances, situations, domains, and disciplines.
- Automation of repetitive content creation processes. Data can be isolated and captured automatically, greatly reducing the effort for risk reporting
- Simplified validation that content accurately reflects current situations and current product data and states
- Efficient exchange of risk management data with external stakeholders including governing agencies and consumers.



Traceability is enabled by:

- Inherently interconnected data structures. Risk management data, decisions, and mitigation actions are all interconnected within the practice as well as with ongoing product development and changes.
- Easy creation of semantically meaningful relationships between risk management content and product data.
- Configurable relationship behaviors to handle different use cases and data maturity levels

Which results in:

- Digital Thread connectivity of risk content across domains and processes
- Simple navigation and visualization of relationships between risk content, operational data, and product data
- Automatic consistency of links between versions of controlled data. Assurance that reported content is consistent with current situations and product states.

SUMMARY

Risk is reality. For everyday life but in particular for the development and marketing of medical devices. Risk must be managed for patients, operators, external equipment, and the environment. Risk management is only becoming more difficult as product complexity evolves. Software replaces many mechanical functions, markets are increasing worldwide, telemedicine and home health are becoming common, and products shrink to meet usability and mobility requirements. Governing entities are never satisfied with current regulations.

ISO 14971 speaks specifically to the "Application of risk management to Medical Devices". As such it provides a nine-part standard for risk analysis, evaluation, control, and review. It establishes objective criteria for risk acceptability but does not specify acceptable risk levels. Risk levels are determined by the individual companies depending on the type of product being developed and markets to be exploited.

There are many benefits to risk management. This process aims to reduce risks to their lowest possible level to prevent harm to the patient, operators, or other stakeholders. Ensuring safety for everyone is the primary reason for risk management in medical devices. Risk management is a regulatory requirement, and in order to get FDA or the European MDR approval for bringing your product to market, you need to have a documented risk management process in place.

A modern Product Lifecycle Management (PLM) offering can provide a comprehensive solution for first putting change under control. Secondly, all content created by the risk management process needs to be connected, not by constant action to be taken by participants but inherently and automatically by the system. And thirdly the first two solutions, change under control and related content and data, result in traceability, or the ability to look backward and see how you arrived at your current state.

1. "Applying Human Factors and Usability Engineering to Medical Devices" (PDF). U.S. Department of Health and Human Services Food and Drug Administration. February 3, 2016. This article incorporates text from this source, which is in the public domain.

Aras provides the most powerful low-code platform with applications to design, build, and operate complex products. It's technology enables the rapid delivery of flexible, upgradeable solutions that build business resilience. Aras' platform and product lifecycle management applications connect users in all disciplines and functions to critical product data and processes across the lifecycle and throughout the extended supply chain. Airbus, Audi, DENSO, Honda, Kawasaki, Microsoft, Mitsubishi, and Nissan are using the platform to manage complex change and traceability. Visit www.aras.com to learn more and follow us on Twitter and LinkedIn.