SIEMENS
Ingenuity for life

# Improving medical device risk management

This white paper investigates some of the classic challenges of medical device risk management and demonstrates how using Siemens PLM Software's solution significantly improves the process. It provides a robust repository and workflow management solution that simplifies tasks such as requirements management and reporting, while automating deep traceability.

A white paper issued by: Siemens PLM Software

www.siemens.com

# Contents

**Executive summary** ..... **3**

**The challenges of medical device risk management** ..... **4**

**A traceability data model** ..... **6**

**A risk management data model** ..... **9**

**Risk management document definition** ..... **14**

**Conclusion** ..... **18**

# Executive summary

Medical device product development has been a foundational element of the practice and betterment of medicine for about as long as mankind has been trying to heal people. The mortar and pestle were used to prepare medicinal powders more than 6,000 years ago.

Over the millennia our medical devices have become more complex and powerful, and the same can be said for the regulatory environment. Regulations are essential as they help to ensure that medical devices are designed with verification and validation (V&V) so they comply with required specifications and can be used for their intended clinical purposes.

Conceptually, risk management seems simple enough. Given that potentially hazardous situations can lead to harm, these potentially hazardous situations must be documented and mitigated to control outcomes and ensure that a device can be used predictably and safely.

However, as everyone working with compliance knows, things can get complex in a hurry, especially when dealing with multiple regulations, conflicting definitions and the need to track compliance at a digital level. This complexity is caused by a variety of factors, including the number of variables needed to describe the relationships between system components, options for whether to make these concepts unique or re-usable, the many-to-many relationships required to track compliance, and sometimes vague or confusing regulatory expectations.

Tools currently used for the purpose of tracking complexity are not just simple, but simplistic. Although spreadsheets are good for tracking one-to-one relationships, they quickly become far less useful when dealing with the one-to-many and many-to-many relationship tracking required for ensuring regulatory compliance for medical device product development.

Spreadsheets and Microsoft® Word software documents are not really meant for the essential task of achieving traceability. Traceability is at the heart of quality control during the design and development stage, and continues to be essential post release when linking surveillance reports back to specific product requirements and V&V processes.

Fortunately, Siemens PLM Software provides a powerful solution for medical device product development.

# The challenges of medical device risk management

Traditionally, one of the more difficult system development tasks faced by developers is the challenge of implementing effective medical device risk management. The key word is effective, as risk management needs to be a living process that becomes a granular part of the entire process; from first design and manufacturing through post-market surveillance.

Much of the difficulty comes from using old technology – static written documents and spreadsheets – to track the complex and dynamic environment in which applicable standards and other product requirements are tracked over time and through design and development iterations.

Medical device risk management needs to be based on living design elements that can be shared from a central repository to update stakeholder documents and maintain versioning. Without using such automation to trace design element relationships, design intent can be lost across workflows, product changes and requirements updates.

**Incorporating standards**

Medical device product development work is a highly integrated and regulated process. Two key standards incorporated into medical device risk management are International Organization for Standardization (ISO) 14971:2009, which specifies the process for a manufacturer to identify the hazards associated with medical devices; and ISO Technical Information Report (TIR) 24971:2013, which provides guidance in addressing specific areas of ISO 14971 when implementing risk management. Europe has added to the mix with EN ISO 14971:2012, which is different in several important aspects, and is required if a company is selling medical devices into Europe.

The process defined by these standards can be seen in Figure 1.

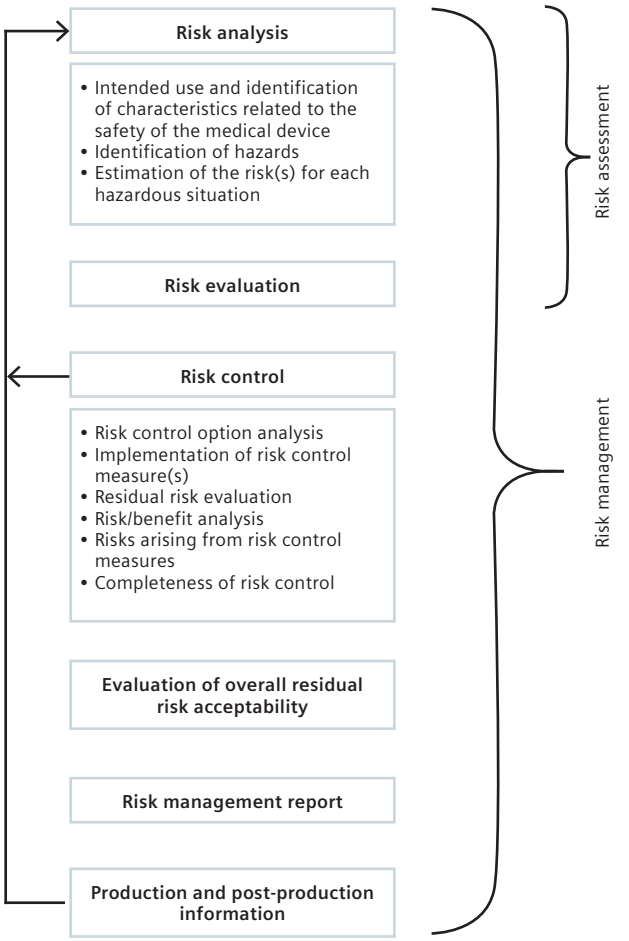


**Figure 1.** Risk management workflow.

**From risk analysis to post-market surveillance**
A complete medical device risk management solution needs to cover the full range of associations, as shown in Figure 1.

The basic logic flow includes:

- **Risk analysis:**
  - Hazards
  - Foreseeable sequence of events (sometimes defined as a sequence of root causes)
  - Hazardous situations
  - Harms
- **Risk evaluation:**
  - Pre- and post-mitigation occurrence values
  - Harm severity
  - Risk priority level
  - Judgment of risk acceptability
- **Risk control:**
  - Design requirements
  - Realization requirements
  - Labeling requirements
  - Verification of implementation
  - Verification of effectiveness
- **Closure and reporting:**
  - Evaluation of product residual risk
  - Evaluation of risk acceptability
- **Post-market surveillance:**
  - Risk trending codes
  - Risk analysis trending code traceability

**Risk management system essentials**
The risk management system should provide information back to the product designers to inform actions, including:

- User impact – How design features affect users
- Hazardous situation control plan – Data to guide development of the hazardous situation control plan, including design, product realization and labeling mitigations
- Field performance – Field performance should be linked to the risk analysis in order to ensure that issues are considered in the analysis, and provide rapid integration of issues discovered during product use
- Mitigation – Performance data, including formulation of requirements to make certain that V&V efforts can be used to ensure that requirements are implemented and effective

**The power of relational data, enforceable workflows and automation**
You can easily be overwhelmed when using spreadsheet-based methodologies to track all of the interdependencies of risk analysis, control, reporting and surveillance. Using Siemens PLM Software's solution for medical devices, with its relational data structure, enforceable workflows, automations, traceability and reporting, makes it easy to track and report against whatever risk management information is required. And the solution's central repository ensures that everyone is using the same data sets. Identifying harms and other artifacts is as simple as pressing a button to run reports against the work items that have been systematically populated with the relevant data.

# A traceability data model

Traceability is at the foundation of medical device risk management. From design, development and manufacturing execution through post-market surveillance, organizations need the ability to precisely trace interrelated work items and their relations to design and regulatory requirements, test cases, V&V processes, build controls, hazards, harms and mitigations. Some of the basic building blocks of traceability are seen in the Siemens PLM Software's medical device template's comprehensive traceability table, as shown in Figure 2. The flow diagram shows elements that provide the basis for developing the design V&V test plan and risk management framework.

**Comprehensive traceability**

The complexity of this interrelation can't be reasonably tracked by spreadsheets or written documents. For example, early in the design process you might specify user needs in a document created using Word. With each user need listed, you may place a number at the end of the sentence for tracking. When writing a separate product requirements document, you can reference each requirement back to the user need it fulfills. The numerical link can then be placed into a spreadsheet in an attempt to trace between user needs and product requirements.

But during design, it is unlikely you will have every design output, including subassemblies, linked to each user need or product requirement.

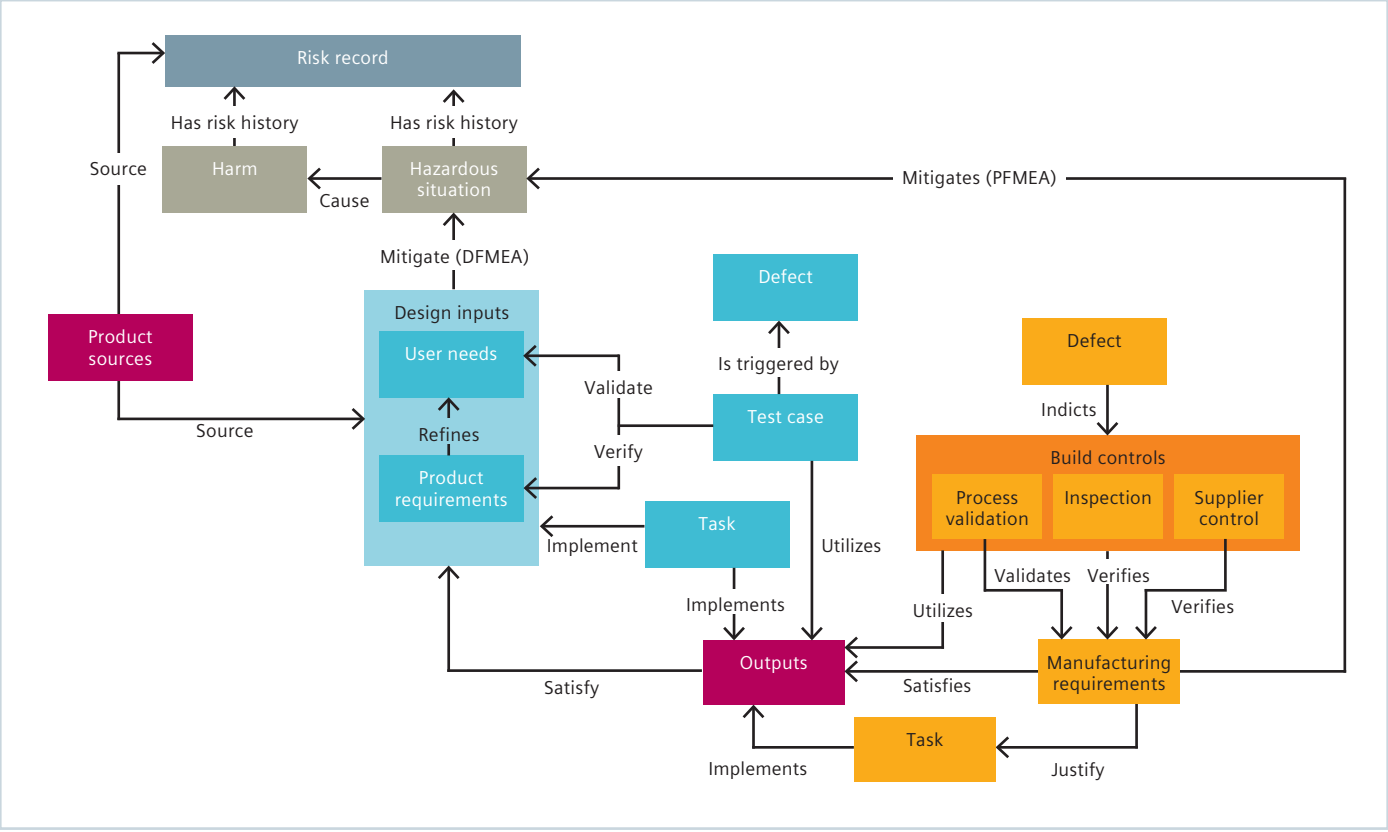


**Figure 2.** Comprehensive traceability table.

Tracing gets more complicated when design file outputs are handed off to production, which typically creates a product realization plan and a spreadsheet to track its own production concerns. So to establish what your traceability is from user needs, product requirements and outputs to manufacturing requirements, you will need to open all these documents. They may or may not have been updated, stored centrally and have version controls, and you're going to have to manually find the elements and decipher the traceability for each one.

This lack of efficient traceability adds a lot of pain and delay for teams attempting to respond to corrective action preventative action (CAPA) needs.

### User requirement and product requirement testing

An efficient solution for managing product requirements should make it easy to associate user needs with product and software requirements and the relevant testing, as shown in Figure 3.

For example, the first entries in the Figure 3 table show that user need 1010-3873 (the device will be sterile) is matched with product requirement 1010-3874 (the device will be ethylene oxide sterilized per ISO 11135), and references the test (1010-3821).

A robust requirements management solution supports workflows and traceability throughout the design, manufacturing and risk management relationships typical in a medical device product development process. The solution should support integration of concepts used in the development process, such as standards integration, United States Food and Drug Administration (FDA) guidance, ISO, American Society for Testing and Materials (ASTM) and all other applicable compliance data, as well as images and text-based justifications.

### Tracking ancillary artifacts

One of the most powerful leverage points in the use of a solid requirements management tool is the way ancillary artifacts can be referenced throughout the design history file (DHF).

Consider, for example, the medical device intended use statement. Your tool should support the approved definition so it can reference a tagged work item wherever it is used. This ensures consistency in the text, and the ability to establish a point wherever the standard text is used. This can be critical to determining the full impact of a change, and ensuring a change is properly propagated to all relevant documents.

Robust tracking and traceability are required for the documentation and mitigation of hazardous situations to control outcomes and ensure that a device is predictable and safe.

| User requirements | Product requirements | Tests |
|---|---|---|
| 1010-3873 - The device will be sterile | 1010-3874 - The device will be EO sterilized per ISO 11135 | 1010-3821 - This is a test case for the requirement |
| 1010-3875 - The device will seal vessels up to and including 5 mm | | |
| 1010-3931 - The software shall generate alerts for the user. | | |
| 1010-4016 - The user will visualize the data | 1010-4017 - The device will have a touch screen | 1010-4019 - Login into Portal |
| 1010-4165 - All Devices and Labels shall indicate to the user that it is sterile | | |
| 1010-4290 - User need for the requirement | 1010-4291 - New requirement for display | |
| 1010-4361 - This is a new user need | 1010-4362 - This is a refining requirement | |
| 1010-4470 - The device will seal vessels up to and including 5 mm | | |
| 1010-4472 - The device will be sterile | 1010-4473 - The device will be EO sterilized per ISO 11135 | |
| 1010-4475 - User need for the requirement | 1010-4476 - New requirement for display | |
| 1010-4477 - This is a new user need | 1010-4478 - This is a refining requirement | |
| 1010-4479 - The user will visualize the data | 1010-4480 - The device will have a touch screen | |
| 1010-4489 - The software shall generate alerts for the user. | | |
| 1010-4765 - This is a new user need | 1010-4766 - This is a refining requirement | |
| 1010-4767 - The device will be sterile | | |
| 1010-4771 - The device will withstand clinical environment | | |

**Figure 3.** User requirement and product requirement test.

**Best practices**

As we've seen, the implementation of an efficient and effective risk management system – especially one based on traditional spreadsheets and static documents – is complicated and challenging.

As noted earlier, this is due to a variety of factors, including:

- The number of variables needed to describe the relationships between system components
- Options for whether to make these concepts unique and re-usable
- The ability to support many-to-many data relationships
- Sometimes vague or confusing regulatory expectations

Some best practices for organizing components of the system to support post-market surveillance include:

- Organize data by how it will be reviewed: After release of a product to the field, post-market surveillance is used to evaluate the product on the basis of user harm, user hazard and the number or percentage of field occurrences. Your data fields should link directly with the data returned for easy comparison and response to issues identified in the field. You should be able to see the occurrence of a harm in the field and directly compare it with the risk management process. This will allow you to immediately evaluate whether the factor used to determine how often the hazardous situation results in a harm is correct, or whether the probability of the hazardous situation occurring has been improperly assessed.
- Use common terminology for data fields: Regulatory bodies have defined what is meant by a hazard, or hazardous situation. You should build that regulated terminology into your model to provide a system that helps auditors better understand your intent without additional explanation.
- Minimize linking complexity: Work items should be organized in such a way as to minimize linking complexity. It is possible to provide so many degrees of freedom (DOF) in the system that the logic becomes difficult to follow. This can make it difficult to train employees on the system, as well as explain your processes to regulatory authorities.

# A risk management data model

Risk management methods are often poorly understood and imprecisely defined, making it all the more important to have a solid risk management model.

A well-designed, comprehensive risk management tool should be able to support a risk management data model that ensures consistent use of definitions, work items and workflows to identify and mitigate harms and hazards.

Your risk management tool should support logic flows such as the one in Figure 4, which is derived from ISO 14971 Annex E, and is required for compliance with both the United States and European medical device approval systems. It addresses measuring elements such as sequence of events, and the probability of a hazardous situation occurring, and the probability of a hazardous situation leading to harm.

A risk management data model brings precision to your operations. It allows you to set definitions – based upon whatever design or regulatory requirements you are dealing with – and then enforce consistency of use to greatly enhance data quality.

### Enforceable workflows

Creating a risk management data model using Siemens PLM Software's solution for medical devices gives you the ability to develop enforceable workflows so all team members, regardless of their geographic location and other variables, use the same defined workflows. Your organization can create whatever workflows it needs. The key is that once it is designed, you are able to ensure that it is used consistently.

This provides a unifying framework that helps ensure that tasks can be completed without leaving anything out, and introduces variables caused by casual definitions or incomplete tasks.

The process of defining your workflows in an enforceable framework brings clarity to the work of identifying potential hazards and harms and determining optimal mitigation strategies.

The framework also enables automation. Once you've established your framework, you're going to create the work items. You go through the same evaluation process to identify hazards and harms as you would if working from a spreadsheet, but now all the interrelationships are managed. This greatly reduces the amount of time that's required to perform calculations, tracings and other normally time-intensive tasks. Re-using the requirements and relationships on similar future products also provides a compelling reduction in workload.

It's important to underscore the fact that a spreadsheet isn't a framework. It's just a collection of cells that can't be used for enforcing workflows or working with relational data.

### The need for consistency

The framework and its supporting environment provided with the Siemens PLM solution, also gives you the ability to enforce consistency for other elements, including definitions, terminology and spelling. Although enforcing consistent spelling and terminology might seem inconsequential at first glance, the absence of consistency can sap the strength of your data.

If you were searching a database for a harm such as perforated bowel, you would only see a portion of such incidents if the word perforated was misspelled in 30 percent of your spreadsheet entries. With a risk management tool that can enforce consistent spelling, a search would result in identifying all incidents.

Enforcing consistent terminology is needed for the same reasons. For example, if you are working with arterial balloon hazards, some incidents might be described as a dislodged balloon, while others define the same incident as a deflated balloon, and there could be a spectrum of variations. By agreeing on proper terminology at the outset, your framework can enforce consistent use of it, while providing the flexibility to accommodate and properly document incident variations.

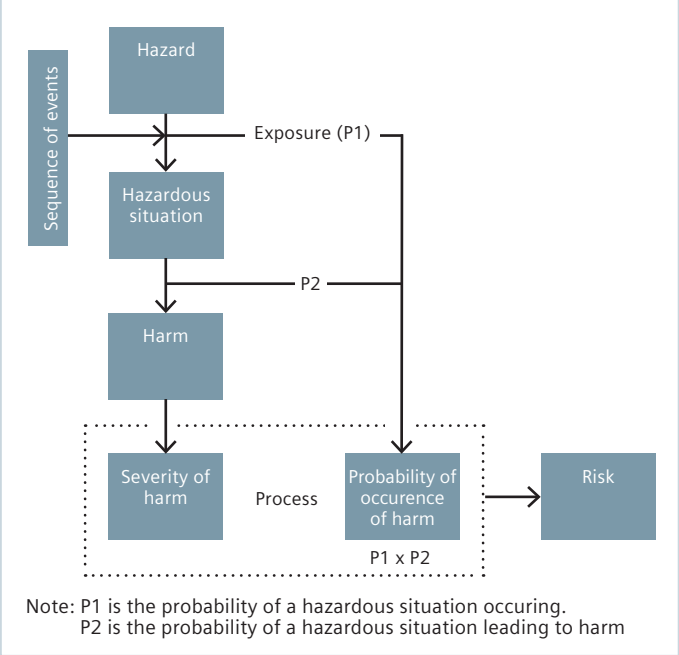


**Figure 4.** Risk management logic flow based on ISO 14971 Annex E.

### Risk evaluation work items

Implementing systematic risk management logic flow requires that multiple work items and commensurate variables must be defined in order to logically organize the analysis. Figure 5 provides an example of a flow diagram of a system compliant with the risk management flow chart shown earlier in Figure 4. The system is organized with three work items: risk record, harm and hazardous situation.

The overall system analysis is in the form of a traditional failure mode and effects analysis (FMEA).

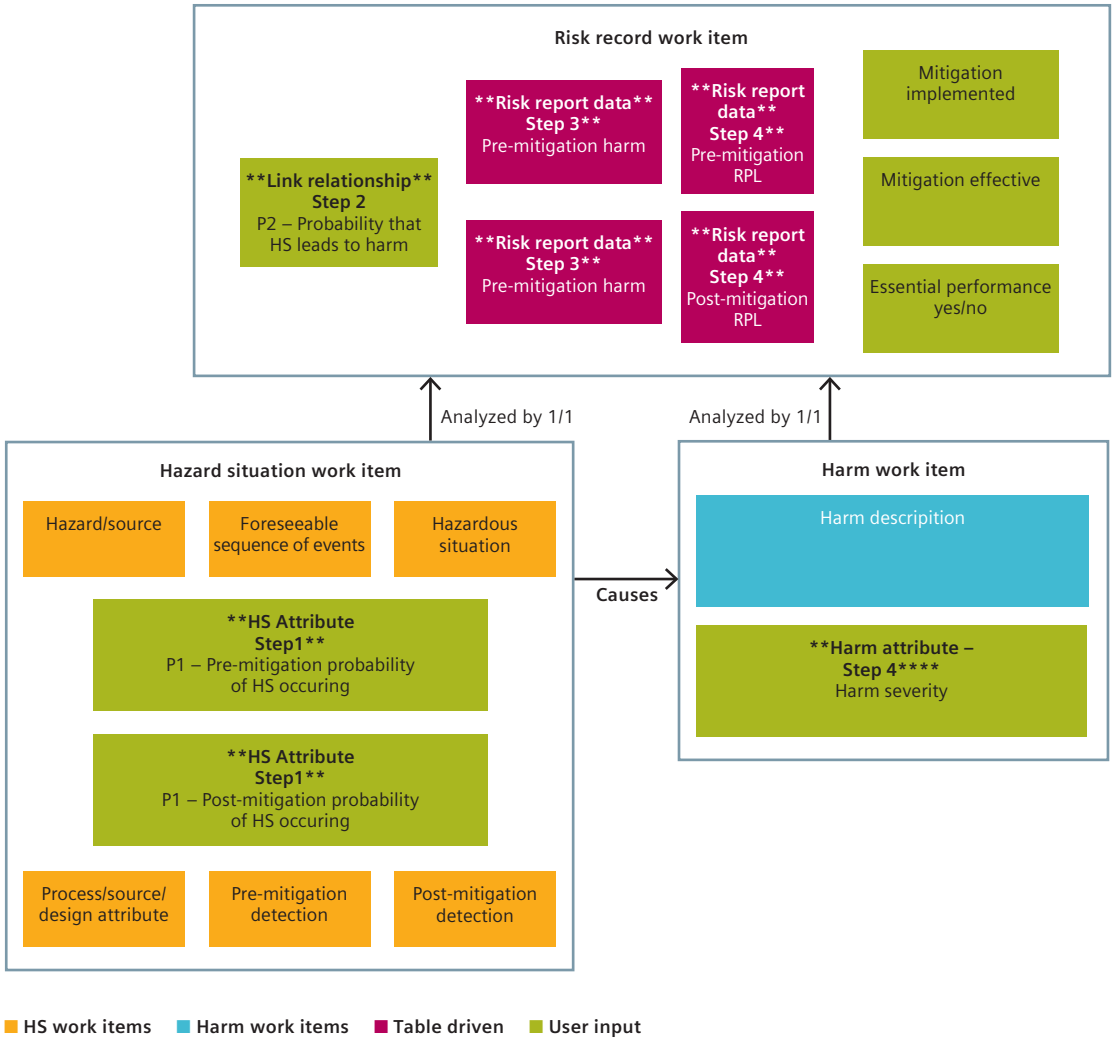


**Figure 5.** Risk evaluation work items.

This is a convenient grouping due to several factors, including:

- The work is completed and reviewed by different departments, each using their appropriate workflow. This bifurcation is logical because a hazardous situation is largely an engineering exercise, while risk analysis tends to be done by risk management professionals and clinical staff.
- The conversion/probability variables cannot be defined without the components described by the work item: for example, the probability that a hazardous situation occurring cannot be defined without knowing the hazard, foreseeable sequence of events and the resulting hazardous situation. In risk analysis the probability that a hazardous situation will lead to patient harm cannot be known without an accumulation of the occurrence of the hazardous situation, and a characterization of the harm.
- The hazardous situation term, for example, is discussed in regulatory documents (ISO 14971) and it's convenient to match the work item with the regulatory term for audit clarification.

**Work item examples**
Work items types can be defined to meet a range of needs. As noted above, three basics include a harm work item, hazardous situation work item and a risk record work item.

**Harm work item**
The risk assessment work item includes a harm description and harm severity. For example, a harm description for anaphylactic shock might be assigned a severity of four on a scale of one to five.

**Hazardous situation work item**
The fully characterized hazardous situation includes the source from which the failure mode originated (hazard), the failure mode description (foreseeable sequence of events) and the local effect (hazardous situation). Variable input includes the pre- and post-mitigation probability of hazardous situation occurrence (P1), and pre- and post-mitigation detection.

An example of this is:

- Electromagnetic radiation > 1) cut insulation, 2) conductor touches case > electrification of the cabinet chassis

  Or

- Biocompatibility, allergenicity > 1) Syringe tip hole out of specification, large, 2) excessive dosage applied > patient overdosed

**Risk record work item**
The risk record work item combines a single hazardous situation with a harm so they can be analyzed as a pair. Several operations are completed in this stage to complete the risk assessment.

The P2 factor is defined as a relationship between the hazardous situation and the harm (probability of the hazardous situation leading to harm). In our above example, the hazardous situation is electrification of the chassis. The harm is electrical shock to the user. The obvious question is how often will shocking the user lead to user death? Thankfully, one does not always follow the other. This P2 conversion factor is the method we use to reduce the occurrence to a level the user would experience.

The P1 and P2 factors are then combined to determine the occurrence of the harm.

The final P factor is then used along with the harm severity to determine the harm/hazardous situation risk index.

The risk priority level, or risk index, is calculated to determine the effect of the risk on the product and company systems.

## Grading scales

Whenever a risk management system is defined, it is also necessary to develop the grading scales. The following is a discussion of each scale and their meaning. The scales are just examples of how this can be done.

### Harm/severity

In the system described in Figure 6, harm severity is defined as one of five levels, on a scale of one to five.

**Harm severity characterization**

| Level | Definitions |
|---|---|
| Minor (1) | Results in temporary injury or impairment that does not require professional medical intervention; inconvenience |
| Moderate (2) | Temporary injury or impairment that requires minor professional medical intervention |
| Serious (3) | Results in injury or impairment requiring major professional medical intervention |
| Critical (4) | Results in permanent impairment or life threating injury |
| Catastrophic (5) | Results in patient death |

**Figure 6.** Harm severity characterization on a scale of one to five.

### Hazardous situation occurrence (P1)

The hazardous situation occurrence is ranked on the basis of probability. The table shown in Figure 7 provides an example of such a ranking system.

### Probability that hazardous situation will lead to harm (P2)

The likelihood that the hazardous situation will lead to a harm is also ranked by probability. An example of this is shown in Figure 8.

### Probability of harm occurrence

By factoring the P1 and P2 occurrence values defined above, you can estimate the probability of harm occurrence, as shown in Figure 9.

**Probability of occurrence of a hazardous situation (P1)**

| Level | Frequency |
|---|---|
| Frequent (5) | >1/100 and <=1 |
| Proable (4) | >1/1000 and <=1 |
| Occasional (3) | >1/10K and <=1/1000 |
| Remote (2) | >1/100K and <=1/10K |
| Unlikely (1) | >0 and <=1/100K |

**Figure 7.** Hazardous situation occurrence probability.

**Probability the hazardous situation will result in harm (P2)**

| Level | Definitions | Probability of harm |
|---|---|---|
| Extremely unlikely (1) | <=5% | Injury would be rare |
| Unlikely but possible (2) | 6 – 25% | Injury is conceivble but not likely |
| Likely (3) | 26 – 75% | Injury may occur |
| Very likely (4) | 76 – 95% | Injury is expected to occur |
| Extremely likely (5) | >=96% | Injury will occur |

**Figure 8.** Probability that a hazardous situation will result in harm.

**P1 – Probability of occurrence of a hazardous situation**

| P2 – Probability of hazardous situation leading to harm | Unlikely (1) | Remote (2) | Occasional (3) | Probable (4) | Frequent (5) |
|---|---|---|---|---|---|
| Extremely unlikely (1) | 1 | 1 | 1 | 1 | 2 |
| Unlikely but possible (2) | 1 | 1 | 1 | 1 | 3 |
| Likely (1) | 1 | 1 | 1 | 2 | 4 |
| Very likely (4) | 1 | 2 | 2 | 3 | 5 |
| Extremely likely (5) | 1 | 2 | 3 | 4 | 5 |

**Figure 9.** Probability of a hazardous situation occurring.

## Risk priority level

The risk priority level (RPL) can be calculated from the severity and occurrence levels established in the previous tables. It can be derived either from a pick table or a variety of calculation methods. The pick table definition is shown in Figure 10.

**Severity of harm**

| Occurrence of harm ($p_1 x P_2$) | | Minor 1 | Moderate 2 | Serious 3 | Critical 4 | Catastrophic 5 |
|---|---|---|---|---|---|---|
| | 1 | D | D | C | C | B |
| | 2 | D | D | C | B | B |
| | 3 | D | C | B | B | A |
| | 4 | C | C | B | A | A |
| | 5 | C | B | A | A | A |

**Figure 10.** Probability of a hazardous situation occurring.

## Report example

Once the characterization is completed for each hazard/harm combination, a risk management and mitigation assessment report can be generated. A partial screenshot of such a report is shown in Figure 11.

**FMEA analysis – harm/hazard and mitigation assessment**

| Risk Record | Hazard | Hazard ID | Hazardous Situation | Essential Performance | Harm | Source | FMEA ID (line item) | POSSIBLE CAUSE | PRE-MITIGATION | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | SEV | P1 | P2 | P | Risk Index |
| 1010-5016 | | ??? | 1010-4364 - Sterile barrier bag allows for bacteria migration | No | 1010-4080 - Infection of the surgical site from a non-sterile instrument | | | Testing field | 4 - Critical | 5 - Frequent | 3 - Likely | 4 - Probable | A |
| 1010-5011 | Bacteria | ??? | 1010-3839 - Sterilization cycle sub-lethal due to use of un-validated manufacturing process | Yes | 1010-4080 - Infection of the surgical site from a non-sterile instrument | 1010-5025 - ISO 5840 - paragraph 5.2.3 - valve performance | PFMEA line 32 | Testing field | 4 - Critical | 3 - Occasional | 2 - Unlikely but Possible | 1 - Improbable | C |
| 1010-5014 | Bacteria | ??? | 1010-3841 - Sterile barrier bag leaks due to un-validated seal manufacturing process at first... | Yes | 1010-4080 - Infection of the surgical site from a non-sterile instrument | 1010-5026 - ISO 5840 Testing requirement | | Testing field | 4 - Critical | 4 - Probable | 4 - Very Likely | 3 - Occasional | B |
| 1010-5015 | Motor | ??? | 1010-3842 - Sterile barrier bag leaks due to un-validated seal manufacturing process at bag... | Yes | 1010-4080 - Infection of the surgical site from a non-sterile instrument | 1010-5027 - ISO 5840 Risk Management requirement | | Testing field | 4 - Critical | 4 - Probable | 4 - Very Likely | 3 - Occasional | B |
| 1010-5013 | | ??? | 1010-4368 - Doctor misuses device | No | 1010-4369 - Instrument perforates bowel | | | | 5 - Catastrophic | 0 - Unanalyzed | 2 - Unlikely but Possible | 0 - Unanalyzed | |

**Figure 11.** Harm/hazard and mitigation assessment report.

# Risk management document definition

Definitions are essential throughout the process of medical device risk management, including defining structure and contents of required documents, such as the risk management plan, risk analysis and risk management report.

Some of the structure of document artifacts is mandated. Of course, special attention must be paid to ensure that the documents contain all of the information required by law.

**Risk management plan**
The risk management plan, as defined by EN ISO 14971:2009, should include:

- Scope of activities
- Assignment of responsibilities
- Criteria for acceptability
- Verification activities
- Activities related to collection and review

**Risk analysis**
The ISO requires that risk analysis documents take a harms-based approach. Elements of risk analysis include:

- Device failure mode and effects analysis (DFMEA)
- Process failure mode and effects analysis (PFMEA)
- Use failure mode and effects analysis (UseFMEA)
- Harms
- Hazardous situations
- Harms-based fault tree analysis (FTA): database traceability table

**Risk management report**
The risk management report, as defined by EN ISO 14971:2009, should help ensure that:

- The risk management plan has been appropriately implemented
- The overall residual risk is acceptable
- Methods are in place to obtain relevant production and post-production information

Using Siemens PLM Software's solution, you can pull information from United States Federal Registers into the tool as requirement documents, and link them to company standard operating procedure (SOP) requirements. Joining the two helps ensure legal requirements are satisfied by the company's SOP requirements or an ISO standard, which would in turn support compliance with the company SOP for design documents.

This process establishes audit traceability from the requirement source to the design document evidence. During an audit, the company could demonstrate compliance with a particular paragraph of the FDA Code of Federal Regulations (CFR) or European Medical Device Directive (MDD) by directly tracing from the legal requirement to the SOP, making it easy to identify records that prove compliance.

This provides a proof progression of:

**Legal requirement →**
**Company SOP requirement/ISO standard →**
**All project document records →**
**Product realization data →**
**Post-market surveillance data**

**Document integration**
Your risk management documents should provide proper integration of well-defined elements, including:

- Harms: Harms should be at the top of the comprehensive product risk analysis. Aside from the regulatory desire for this to be the case, it provides a convenient post-market audit trail. When adverse events occur in the field, they are most often associated with harm(s) to the user. In such cases, as the risk management file is sorted by harms, you can rapidly determine which hazardous situations were predicted to be contributors to the harm at hand, and see all of the mitigations used for control. This provides a concise way to identify whether the root cause of the issue was considered, and what is needed to correct the problem in the field. It also can be used to quickly identify the design V&V testing associated with the design feature and what testing would need to be repeated in the event that design changes are necessary.
- Hazardous situations: Hazards and hazardous situations should be analyzed in every way possible to determine the potential problems in the design, manufacture and use of the device. All of these methods (DFMEA, PFMEA, UseFMEA, fault tree, evaluation of field clinical use, clinical trials and others) should be used to identify hazardous situations and make them visible in the harms-based analysis as potential causes of the user harm.
- Mitigations: Every mitigation of a hazard at the disposal of the company should be listed in the harms-based fault tree analysis. User needs, product requirements and manufacturing requirements should all be considered legitimate mitigations to a hazardous situation. This is in part due to the ISO 14971:2012 Annex Z requirement that labeling should not be used to decrease the occurrence of a hazard. We need as comprehensive a strategy as possible to control product use when it is not possible to control use with device design. When mitigating a hazardous situation, we need every tool available to the company to reduce the risk, in the words of ISO 14971:2012, "as much as is possible."
- Product labeling: The risk mitigation strategy is also the best source of data for product labeling. Instead of using a similar device currently sold in the market or a board of physicians to define risks in need of precaution, warning or contraindication, what better way to develop a comprehensive list of potential issues than from the risk analysis? When the high/medium risk is identified, one of the mitigations should be the use of product labeling. While the label cannot be used to decrease the occurrence of the hazard, from a product liability standpoint it's a terrific way to justify when and where user notifications should be used.

**Document design**
When planning your total documentation package, you'll want to be sure to include documentation on:

- Design inputs: The document set should include at least one document, and more likely many, that define user needs as well as product requirements, as in the product requirements document (PRD). These documents are often developed to mirror the development process and suppliers used in the development process. Thought should be given to how the documents will be organized in the project contractual environment.
- Design outputs (specifications): Specifications come in a variety of forms, including prints, code and manufacturing work instructions. A plan to track satisfaction with all design requirements should be devised. It is often unnecessary to pull every specification into the design control; depending on the testing strategy, you may not need to touch all files. On the other hand, if all specifications are in the system, testing could be tracked for all data required by the product quality plan (first article inspection, in-process testing, receiving inspection), providing a more complete picture of the entire device lifecycle. This strategy could be used to enable the manufacturing group to integrate post-market test data into the product history.
- Design verification and validation plan: As noted earlier, the ability to search the project file for user needs, product requirements and the test case is powerful functionality.

**Manufacturing documents**
You should have a robust collection of manufacturing documents, including:

- Product realization plan – This plan is used to define how to construct the product. Often a company will break up this list into more than one document.
- Product construction flow chart – The flowchart provides context for the later discussion of processes and the requirements for each step of product fabrication. This list is then checked for duplication and becomes the basis for the master validation plan. When process validation is required, the test case is defined. When it is not, the file contains the justification for noninclusion.
- Master (process) validation plan – This part of the document is a convenient location for discussing all of the processes used to construct the product, identifying all processes that require validation and placing the container for the process validation test work items. The process validation work is a mitigation to potential product hazards and should be linked to the hazard for display in the harms-based fault tree analysis.
- Quality management plan – Once the construction progression is established, the quality management plan is used to provide assurance of product quality with points of product performance verification in the construction plan. These points of verification mitigate potential product hazards, and should be listed in the harms-based fault-tree analysis.
- Design transfer plan – Once product development and testing are complete and approved, the design must be transferred to manufacturing as a product approved to be built for outside use.

This plan also provides important considerations for how the company intends to monitor and collect device manufacturing and field performance data.

**Evaluating quality policy objectives**
The company quality policy objectives must be evaluated at each quality management review meeting. These objectives include performance of quality auditing, CAPA, complaint and manufacturing systems. Ideally, the design mitigation strategy would set up the framework to determine the areas of greatest risk, and provide checkpoints for control.

Examples of control checkpoints include:

- Internal audits
- Third-party audits
- Receiving inspection
- First article inspection
- In-process inspection
- Product complaints
- Field failures

If these tests are included in the design control framework, the data from the tests would naturally propagate into the management review process. Occurrence of hazards would be tabulated, making a review of the field harm/hazard risk simple and intuitive.

**Customization**
Visual reporting tools give the program manager ultimate flexibility in determining the format and data needed for every reporting need. With this flexibility comes the powerful ability to change reporting and data structures with unexpected or complicated results. Report output and background data manipulation should be carefully analyzed and changes tested before implementing the tool on a broad data set.

Opportunities for customization include:

- RPL calculation – Unique methods for calculating the product risk priority level. A great variety of methods can be used for RPL. Severity X occurrence, severity 2 X occurrence, severity X detection X occurrence, with a great multiplicity of ranking scales: 1 to 10, 1 to 5, 1 to 20, pick lists, equations and additional variables. In fact, there are so many ways to accomplish this function that you may want to create your own customized RPL to meet your company's specific needs.
- Link relationships – Some people build the system from the product needs up to the harm, some from the harm down to the mitigations. If your internal system is fixed, you may need to rebuild the relationships in a way that is compatible with your company SOPs. The good news is that Siemens PLM Software's solution is flexible and supports either approach.
- Work item terminology – There frequently can be many different terms used for the same logical concept. It is common to require the system to conform with your company policy.
- DFMEA, PFMEA terminology – The FMEA has been around for quite some time, but use of the tool varies widely in different industries, and sometimes the use of different methodologies bleeds into the medical device industry. Some consideration should be given to how the FMEA is presented and disseminated into the design control file.
- Design traceability report – The design traceability report is a depiction of the design proof. The format of the report and the linkages represented would need to be changed if any of the building components (work items, linking relationships, background data) are changed. Work item approval workflows are a good example.

# Conclusion

It is no wonder that a program manager can quickly become overwhelmed by the system architecture required to successfully complete a medical device development project. Initially, it may be tempting to say, "How hard could this be? I will just make a list," and start the process using something like Excel® spreadsheet software for design inputs, and Word for the first pass at the product requirements document. However, with only a cursory investigation into the complexity of the development process, one can see this will lead to an ever expanding workload with a geometric increase in the probability of error.

Siemens PLM Software's solution is built to help you manage complex design artifacts and link relationships. With this solution, established relationships remain without costly maintenance, while program updates can occur in a structured, searchable environment.

**Siemens PLM Software**

**Headquarters**
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

**Americas**
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

**Europe**
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

**Asia-Pacific**
Suites 4301-4302, 43/F
AIA Kowloon Tower,
Landmark East
100 How Ming Street
Kwun Tong, Kowloon
Hong Kong
+852 2230 3308

## About Siemens PLM Software

Siemens PLM Software, a business unit of the Siemens Digital Factory Division, is a leading global provider of product lifecycle management (PLM) and manufacturing operations management (MOM) software, systems and services with over 15 million licensed seats and more than 140,000 customers worldwide. Headquartered in Plano, Texas, Siemens PLM Software works collaboratively with its customers to provide industry software solutions that help companies everywhere achieve a sustainable competitive advantage by making real the innovations that matter. For more information on Siemens PLM Software products and services, visit www.siemens.com/plm.

**www.siemens.com/plm**



58607-A7 3/17 F