SIEMENS
Ingenuity for life

Siemens Digital Industries Software

Medical device design control with Siemens Digital Industries Software

Business best practices

Executive summary

Medical device product development is a highly integrated and regulated process. Implementation of a requirements tracking solution requires attention to a variety of nuanced topics. When presented with the task of tracking the many concept relationships in a project of this type, the initial software solution of choice tends to be a two-dimensional text system such as Microsoft® Excel® or Apple® Numbers®.

In retrospect, however, the choice is most often a very different one due to the multidimensional nature of the logic behind complex requirements. Siemens Digital Industries Software's solution for medical device design control represent a new type of platform designed to model the process relationships and provide a multidimensional, live-linked, relational database solution for today's complex development environments. The solution frees the development staff to establish relationships once, and then move on to more pressing tasks than the constant re-update of the project control paperwork.

Contents

Introduction

The goal of this paper is to discuss each of the nuanced topics of a requirements management and tracking solution in an effort to provide a framework for the development and implementation of the Siemens PLM solution as such a system. A second objective is to explore the broader use of the tool for the management of concepts in general throughout their lifecycle in the highly efficient and effective manner that is so critical in fast-paced development environments.

The Siemens PLM solution is in essence a document creation and management tool used to efficiently author, link and track ideas and concepts. The tool can be used by any company department that deals with the management of complex information throughout life-cycles and across projects spanning disparate teams. Examples include the design and implementation of verification and validation (V&V) testing, quality management systems (compliance with federal registers), and manufacturing processes (compliance with internal company operating procedures). Therefore, any process implementing the tool should consider the larger picture of implementation opportunities, and not limit the view to the development environment at hand, to make sure that the solution is set up in a way to get the best out of its sophisticated functionality, both mid- and long-term.

What does a concept management system do?

Essentially, what a concept management system is designed to do is to break documents down into their essential building blocks. These blocks are then connected on the basis of their definition and logical relationships to constitute workflows that can accomplish given tasks.

For example, in the case of a design proof, a product requirements document could be broken down into user needs, system requirements, mechanical requirements and software requirements. The mechanical requirements are then broken down further into sterilization, packaging, and transit requirements. Because each of these concepts is logically different and tagged independently, they can be sorted and subjected to unique workflows. For instance, the sterilization needs could be copied into a microbiology review, and the user needs could be collected into a validation test. And, each of the workflows can be managed interdependently.

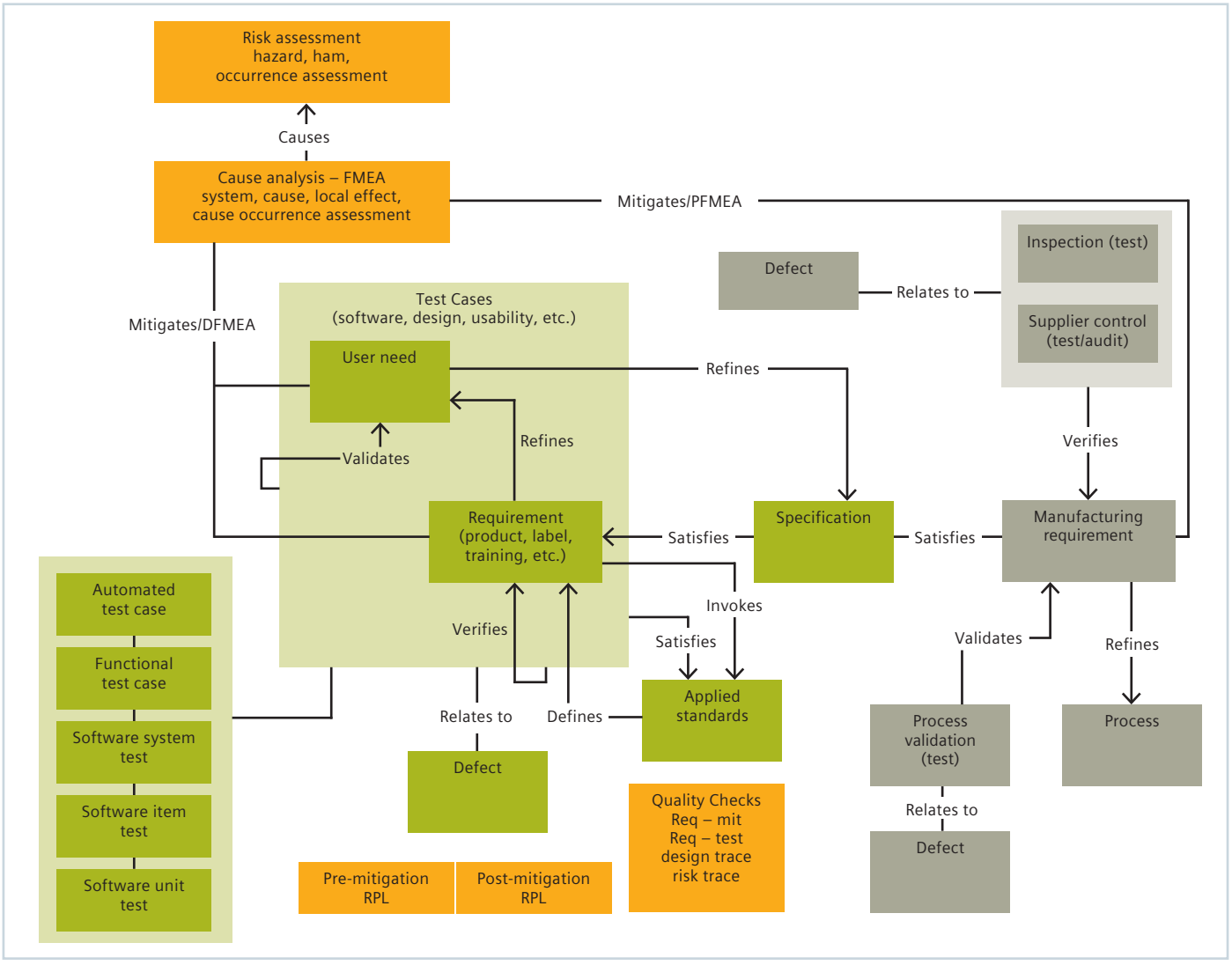
Another example is quality management. For example, when a company receives a register of legal requirements and guidance on system compliance from the government, that can be broken down into its specific legal requirements, which can then be individually satisfied by company standard operating procedures. Because there is clarity in the unique categorization of each individual work item, which is extended through issue, change and variant management, the records proving compliance can be easily verified in an audit, much like a product design verification process.

A key capability of the Siemens PLM solution is that it enables the creation of documents as well as the logic behind them and tracks them interdependently. The concepts including their sophisticated multidimensional relationships can be stored, tracked and released as a complete document resource. Specific reports and documentation for internal reviews as well as external audits can be generated in real time, at any time, to provide the accurate status of your projects.

Traceability matrix

Design V&V

The first task of any product development process is generally to discover, define and link the items of interest for that product. This is typically done in a logic flow diagram, and is the basis for developing the design V&V test plan. In complex development environments, it can be a daunting task. The good news is that templates for typical setups have been completed and made available for use. One example of such a diagram is the SwanVMC comprehensive traceability table (shown below).



Manufacturing

The flow chart is intended to represent the design, manufacturing, and risk management relationships typical in a medical device product development process. It also integrates concepts used in the development process such as standards integration (FDA guidance, ISO, ASTM, etc.), images, text justifications, essential requirements, and standard glossary definitions.

Other artifacts

One of the most powerful leverage points in the use of the Siemens PLM solution is the way ancillary artifacts are referenced throughout the design history file (DHF). One example is the medical device intended use statement. It is convenient to define the text once for approval, and then reference the tagged work item wherever it is used. This ensures consistency in the text, and the ability to establish every point where the standard text is used, which is critical to determine the full impact of a change, and assures that the change is properly propagated to all relevant documents.

Risk management

Conceptually, risk management is not difficult to describe and understand. We have hazards that lead to harms. These hazards should be documented and mitigated to control an outcome to make the use of a device predictable and safe. However, the implementation of such a system is complicated. This is due to a variety of factors including the number of variables needed to describe the relationships between the various system components, options for whether to make these concepts unique and re-usable, many-to-many database relationships and sometimes vague or confusing regulatory expectations. For this reason, the following is offered as exploration on how these various components of the system can be organized.

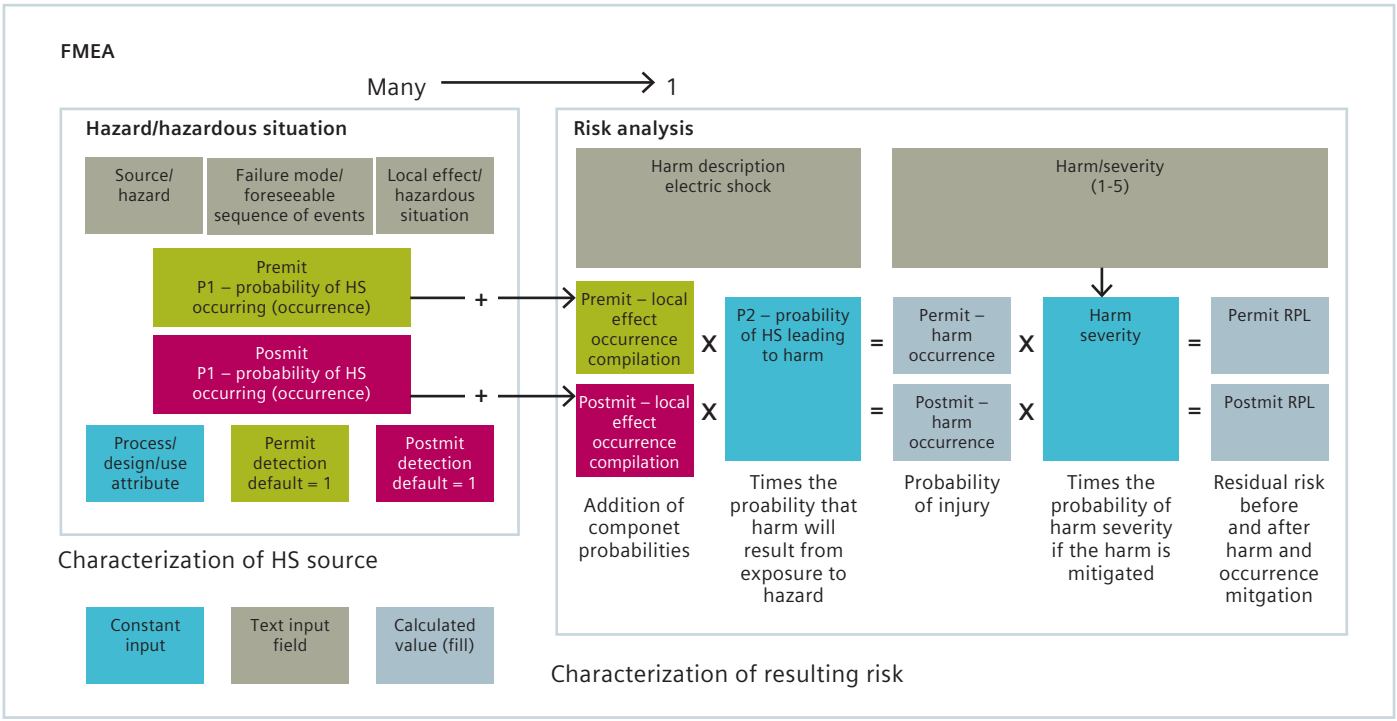
First, the data should be organized by how it will be reviewed. After release of a product to the field post market, surveillance will evaluate the product on the basis of the user harm, the user hazard, and the number or percentage of field occurrences. Our data fields should directly mirror the data returned for easy comparison and response to issues identified in the field.

We 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 us 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.

Second, the data fields should represent common terminology. The regulatory bodies have defined what is meant by a hazard, or hazardous situation. We should build the regulated terminology into our model to provide a system that helps auditors better understand our intent without additional explanation.

Third, the work items should be organized in such a way as to minimize the linking complexity. It is possible to provide so many degrees of freedom in the system that the logic becomes difficult to follow. This can make training of employees on the system and explanation to regulatory authorities difficult.

The following is a flow diagram describing a system compliant with the risk management design prerequisites mentioned above.



The system is organized with two work items.

- Hazardous situation
- Risk analysis

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

This is a convenient grouping due to several factors.

- The work is completed and reviewed (different workflow) for each by different departments. The 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 of a hazardous situation occurring cannot be defined without knowing the hazard, the 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 is convenient to match the work item with the regulatory term for audit clarification.

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, and pre- and post-mitigation detection.

An example of this is:

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

or

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

Risk assessment work item
The risk assessment work item includes a harm description, harm severity, the compiled risk of the occurrence of a group of hazardous situations, both pre- and post-mitigation, the probability that the hazardous situation will lead to the harm, and calculated values for the final harm occurrence and the risk priority level.

To continue the examples outlined above the progression could be:

Electrical shock > Patient death/severity 5

or

Anaphylactic shock > Patient hospitalization 4

Each hazardous situation occurs at a rate. The compilation of multiple hazardous situation occurrences is problematic. When analyzed as a generic problem one cannot know the interrelationships between the different types of hazardous situations. Are the failures sequential (does one only follow another)? Are the failures exclusive (not affected by previous hazardous situations)? Are the hazardous situations dependent (does the occurrence of the first affect the outcome or occurrence of the second)?

For this reason an automated calculation should utilize a worst-case scenario, subject to manual override when engineering deems the change reasonable. Because the occurrence rates are typically low, a summation of all the rates appears to be the most reasonable method.

The calculated value is then multiplied by P2 (probability of the hazardous situation leading to harm). In our example the hazardous situation is energization of the chassis. The harm is electrical shock to the user. The obvious question is then how often will shocking the user lead to user death? Thankfully, one does not always follow the other. This conversion factor is the method we use to reduce the occurrence to the level a user would actually experience.

FMEA

Both the characterization of the hazardous situation and the risk assessment are necessary to complete the FMEA. It is the completion of both that allows us to complete the analysis of how a given failure mode will affect the device end user. This is then converted into the overall Harm > Hazard > Mitigation traceability analysis for final submission.

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 meanings. These scales are only one example of how this can be done. A great variety of different methods are used.

Harm/severity scale

5 – Very serious	4 – Serious	3 – Significant	2 – Marginal	1 – Negligible
May result in death of operator, patient, or bystander. Severe impact on quality that is likely to cause product failures of life-sustaining devices.	May result in permanent impairment or injury to operator, patient, or bystander. Critical impact on product quality including nonconformities likely to cause product failure leading to serious injury.	May result in significant, temporary injury to operator, patient or bystander. Significant impact on product quality including major nonconformities that are likely to cause significant, temporary injury.	May result in damage in the system or process causing process delay with minor, temporary injury. Moderate impact on product quality including minor nonconformities.	May cause minor nuisance to operator or patient without injury, system damage, or process/product impact. Minimal impact on product quality.

Harm occurrence scale

5 – Frequent	4 – Probable	3 – Occational	2 – Remote	1 – Negligible
Greater than 5% (>5/100)	5% Maximum (5/100 Max)	1% Maximum (1/100 Max)	.1% Maximum (1/1,000 Max)	.01% Maximum (1/10,000 Max)

Harm/severity

In the system described below the harm is defined as one of five options:

- Negligible – May cause minor nuisance to operator or patient without injury, system damage, or process/product impact. Minimal impact on product quality.
- Marginal – May result in damage in the system or process causing process delay with minor, temporary injury. Moderate impact on product quality including minor nonconformities.
- Significant – May result in significant, temporary injury to operator patient, or bystander. Significant impact on product quality including major nonconformities that are likely to cause significant, temporary injury.
- Serious – May result in permanent impairment or injury to operator, patient, or bystander. Critical impact on product quality including nonconformities likely to cause product failure leading to serious injury.
- Very serious – May result in death of operator, patient, or bystander. Severe impact on quality that is likely to cause product failures of life-sustaining devices.

Hazard occurrence

The hazard occurrence is broken into the following categories:

1. Negligible (<.01%)
2. Remote (.1 – .01%)
3. Occasional (1 – .1%)
4. Probable (1 – 5%)
5. Frequent (>5%)

Risk priority level (RPL)

The RPL is 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 following is the pick table definition used in this example.

Severity

Occurrence	1	2	3	4	5
1					
2					
3					
4					
5					

Calculation of the risk priority level (RPL)

1	**Low** Verified/Validated to performance level for a low risk level and approved through review
2	**Medium** Verified/Validated to performance level for a medium risk level and approved through review
3	**High** Verified/Validated to performance level for a high risk; redesign or reduction in occurrence typically required

Document definition

The next step is document definition. In this phase, it is determined which documents will be used to contain each of the relevant work items, and how the documents will be approved. Some of the documents expected by regulators are included below:

Regulatory requirements analysis
There are typically two documents used in the development process that are generated by the regulatory department.

Regulatory Analysis – In this analysis the regulatory department analyzes the new product to determine regulatory requirements including:

- Device markets and areas of legal jurisdiction
- Device classification(s)
- Accessory needs
- Other regulatory requirements related specifically to the device in development

Clinical Evaluation Report (CER) – This report has a variety of names, but is a summary of the performance of the device or similar device in the field. It pulls from public and company records to determine the type of user harms/severity found in the general use population, and the frequency of occurrence. This data forms the basis of the initial risk analysis and provides a solid foundation for the design requirements. Regulatory evaluation is a good example of company-generated requirement sources. Other examples include design best practice, legal liability, and standard operating procedures (SOPs) used to reprocess international standards.

Risk management
Risk management is broken down into three documents. The content for the risk analysis is originated in several more:

- **The risk management plan**
- **Risk analysis**
  - DFMEA
  - PFMEA
  - Harms
  - Hazardous situations
  - Harms-based fault tree analysis (FTA)
  - Database traceability table
- **Risk management report**

Some of the structure of the document artifacts is mandated. For example, ISO requires that the risk analysis take a harms-based approach. Consideration should also be given to assure that the documents contain all of the information required by law.

Examples include:

- Risk management plan (EN ISO 14971:2009, The plan shall include the following: Scope of activities... assignment of responsibilities... criteria for acceptability... verification activities... activities related to collection and review)
- Risk management report (EN ISO 14971:2009, The review shall at least ensure 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)

One way to accomplish this would be to pull federal registers into the Siemens PLM solution as requirement documents. These legal requirements would be satisfied by the company SOP requirements, or an ISO standard, which would in turn be satisfied by compliance of the design documents to the company SOP. What better way to establish the audit traceability from the requirement source to the design document evidence? When asked in an audit, the company compliance with a particular paragraph of the FDA Code of Federal Regulation (CFR) or European Medical Device Directives (MDDs) could be directly traced from the legal requirement to the SOP, making identification of the records proving compliance easy.

The proof progression is as follows:

Legal Requirement > Company SOP requirement/ISO standard > All project document records

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 to the user. In such cases, as the risk management file is sorted by harms, it is a rapid process to determine which hazardous situations were predicted to be contributors to the harm at hand, and to 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 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, FTA, evaluation of field clinical use, clinical trials, etc.) should identify hazardous situations and become 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."

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 place 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 is a good way to justify when and where user notifications should be used.

Design

Design inputs (product requirements documents) – The document set should include at least one document, and more likely many, that define the user needs and product requirements. These documents are often developed to mirror the actual development process and the 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, for example. A plan to track satisfaction of all design requirements should be devised. It is seldom necessary to pull every specification into the design control, because depending upon the testing strategy there may not be a need to touch on all of the files.

On the other hand, if all specifications are in the system, testing can be tracked for all data required by the product quality plan (first articles, in-process testing, receiving inspection), providing a more complete picture of the entire device lifecycle. This strategy could effectively set up the manufacturing group for integration of post-market test data into the product history.

Design verification and validation plan (design V&V) – As mentioned above, the ability to search the project file for user needs, product requirements and their test cases is a very powerful functionality.

Manufacturing

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 flow chart provides context for the later discussion of processes and the requirements for each step of the product fabrication. This list is then checked for duplication and becomes the basis for the master validation plan. When a process validation is required, the test case is defined. When it is not, the file contains the justification for non-inclusion.
- **Master (process) validation plan –** This part of the document is a convenient location for a discussion of all of the processes used to construct the product, an identification of all processes which require process validation, and the container for the process validation test work items. The process validation work is a mitigation to potential product hazards and should be linked as such 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 the assurance of product quality with points of product performance verification within the construction plan. These points of verification are also mitigations to 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 gives important consideration as to how the company intends to monitor and collect device manufacturing and field performance. The company quality policy objectives must be evaluated at each quality management review meeting. These objectives include performance of the quality auditing, corrective and preventive action (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 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

Wiki 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 implementation of the tool on a broad data set. Opportunities for customization include:

- **RPL calculation –** Unique methods for calculating the product Risk Priority Level (RPL). A great variety of methods are used (severity * occurrence, severity 2 * occurrence, severity * detection * occurrence) with a great multiplicity of ranking scales: 1-10, 1-5, 1-20, pick lists, equations, and additional variables. There are so many ways to accomplish this function that it can be easily customized to your company 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 the Siemens PLM solution is flexible and supports either approach.
- **Work item terminology –** There are many different terms used for the same logical concept. It is common to require the system to conform with company policy.
- **DFMEA, PFMEA terminology –** 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 an Excel spreadsheet 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 it is evident that this will lead to an ever-expanding workload with a geometric increase in the probability of error.

The Siemens PLM solution is purpose-built to help you manage complex design artifacts and linking relationships. With this tool, established relationships remain without costly maintenance, while program updates can occur in a structured, searchable environment. Contact Siemens Digital Industries Software and start the process of accelerating productivity and innovation, while avoiding errors in your next development project.

Siemens Digital Industries 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
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

About Siemens Digital Industries Software

Siemens Digital Industries Software is driving transformation to enable a digital enterprise where engineering, manufacturing and electronics design meet tomorrow. Our solutions help companies of all sizes create and leverage digital twins that provide organizations with new insights, opportunities and levels of automation to drive innovation. For more information on Siemens Digital Industries Software products and services, visit siemens.com/software or follow us on LinkedIn, Twitter, Facebook and Instagram. Siemens Digital Industries Software – Where today meets tomorrow.

siemens.com/software

55662-C6 9/16 H