CRitical S**YST**em Engineering **A**cce**L**eration

UC 4.2

Safety layer of an interventional X-ray system

D402.010

DOCUMENT INFORMATION

Project	CRYSTAL
Grant Agreement No.	ARTEMIS-2012-1-332830
Deliverable Title	**Safety layer of an interventional X-ray system**
Deliverable No.	D402.010
Dissemination Level	CO
Confidentiality	R
Document Version	V 1.0
Date	2013-15-11
Contact	H.E.P. Cruts
Organization	Philips Healthcare
Phone	+31-402764507
E-Mail	bert.cruts@philips.com

AUTHORS TABLE

Name	Company	E-Mail
H.E.P. Cruts	Philips Healthcare	bert.cruts@philips.com

CHANGE HISTORY

Version	Date	Reason for Change	Pages Affected
0	1-nov-2013	initial version	
V 1.0	15-nov-2013	update after internal/external review; added details of use case process; added details of engineering method	

CONTENT

Content of Tables

Content of Figures

Content of Appendix

No table of contents entries found.

1 Introduction

1.1 Role of deliverable

This document has the following major purposes:

- Define of the overall use case, including a detailed description of the underlying development processes and the set of involved process activities and engineering methods
- Provide input to SP6 in general and to WP601 (IOS Development) required to derive specific IOS-related requirements
- Provide input to WP602 (Platform Builder) required to derive adequate meta models
- Provide input to WP604 (Tools for safety engineering) required to derive requirements for safety engineering tools
- Establish the technology baseline with respect to the use-case, and the expected progress beyond (existing functionalities vs. functionalities that are expected to be developed in CRYSTAL)

1.2 Relationship to other CRYSTAL Documents

1.3 Structure of this document

2 Use Case Process Description

2.1 Rationales

Healthcare systems are subject to strict regulations from ISO, IEC and FDA regarding safety of operators and patients [Ref ISO/IEC/FDA norms]. A well-defined development process needs to be defined including harm and hazard analysis, risk management and extensive documentation for that purpose. The development process is typically following the 'traditional' V-model; Figure 1 (left) outlines this V-model while Figure 1(right) maps this onto the documentation.

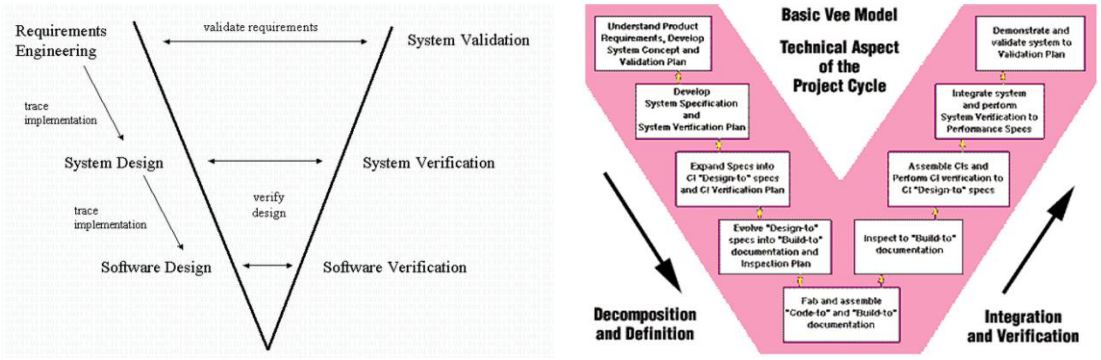


Figure 2-1: *The V-model showing the process (left) and the documentation (right). (Pictures are borrowed from internet sources and Mouz et. al. (1996,2000))*

V-Model: Advantages of linearly following the V-model, in particular for safety, include the well-documented record and audit-trail of process and products, and the 'push-forward' nature of obtaining the final product, which fits engineers quite well. Among the downsides are a lack of incremental approaches, the late system integration and the extensive documentation (which must be updated upon every change and for every different member of a product family). A particular consequence of the late integration is that negative effects of design decisions and safety measures on usability are observed only in a very late stage, or even only in the field. In practice this leads to much manual effort in producing documentation and defining tests.

New challenges: Safety-critical systems engineering faces also new challenges. The complexity of systems is ever increasing due to higher customer demands, more advanced functionality and integration with other medical equipment. System components, in particular software components, become COTS rather than proprietary and, since many safety aspects are software defined, new methods are needed for guaranteeing safety for component-based systems. In addition, systems have to be compliant with updated and new regulatory norms. Because of this, and because of error corrections and changing requirements, updates in the field have to be performed. Finally, in order to maintain a competitive edge, time-to-market must be kept as small as possible or at least predictable.

Improvements: Although current systems do satisfy the safety requirements, there is a need to improve on the following aspects:

1. The call-rate due to a mismatch between user needs and final implementation.
2. The development effort and lack of early impact consequences of additional functional requirements.
3. High release effort due to late integration and manual testing.
4. Large effort to show complete requirements traceability for regulatory affairs audits

The goal of this use case within the CRYSTAL project is to improve these four metrics through a change in the engineering process but more importantly, in the tool support. At the same time these four are the respective drivers of the three use cases of Philips in the healthcare domain in CRYSTAL.

2.2 The safety risk management process

2.2.1 Introduction

Whereas use cases WP4.1 and WP4.3 focus on improving the development process itself, use case WP4.2 is about improving the *safety risk management process*. In general, the *safety risk management process* is running in parallel to the *development process*. In short, the *safety risk management process* takes into account the system requirements and the system design and analyses whether additional risk control measures need to be implemented to fulfil safety requirements.

The requirements for the *safety risk management process* are defined in ISO 14971: "*Medical devices – Application of risk management to medical devices*". The general requirement is as follows:

ISO 14971: clause 3.1 Risk management process

The manufacturer shall establish, document and maintain throughout the life-cycle an ongoing process for identifying hazards associated with a medical device, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls. This process shall include the following elements:

- risk analysis
- risk evaluation
- risk control
- production and post-production information.

2.2.2 Definition of terms

The terms used in this document are aligned with the definitions in ISO 14971:2007.

ISO 14971: clause 2 Terms and definitions

term	definition (the number refers to the corresponding clause in ISO 14971:2007)
Harm	(2.2) physical injury or damage to the health of people, or damage to property or the environment.
Hazard	(2.3) potential source of harm.
Hazardous situation	(2.4) circumstance in which people, property, or the environment are exposed to one or more hazard(s).
Severity	(2.25) measure of the possible consequences of a hazard.
Risk	(2.16) combination of the probability of occurrence of harm and the severity of that harm.
Residual risk	(2.15) risk remaining after risk control measures have been taken.
Safety	(2.24) freedom from unacceptable risk.

Risk estimation	(2.20) process used to assign values to the probability of occurrence of harm and the severity of that harm.
Risk analysis	(2.17) systematic use of available information to identify hazards and to estimate the risk.
Risk evaluation	(2.21) process of comparing the estimated risk against given risk criteria to determine the acceptability of the risk
Risk assessment	(2.18) overall process comprising a risk analysis and a risk evaluation.
Risk control	(2.19) process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels.

A graphical representation of the terms is shown in figure 2-2.

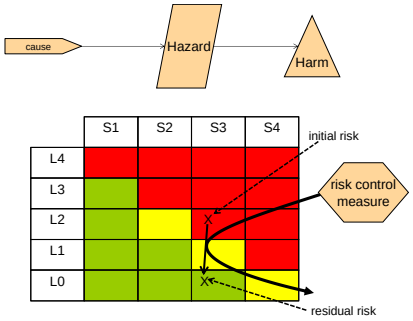


Figure 2-2: *Graphical representation of terms used within the risk management process.*

2.2.3 Description of safety risk management process

The implementation of this process is as follows:

Product risk management is a continuous process throughout the lifetime of a product addressing all risk management activities related to the health, safety, privacy and security of people. This includes product design, manufacturing, distribution, installation, service (maintenance, repair), de-installation, surveillance and where necessary timely corrective actions.

Two phases are distinguished:

• *pre market*: activities during design and release of the product (project execution)

• *post market*: activities after release of the product.

Pre Market:

- The product risk management plan (*RMP*) describes all product safety risk related activities, roles and responsibilities during the project execution. The deliverable of this plan is the Risk Management File (*RMF*). Usually, the *RMP* describes an incremental adaptation of the *RMF* from the previous product generation. The *RMF* is regularly updated during the project execution process and is completed and approved before the release of the product. After the release of the product, the RMF becomes part of the Risk Management Maintenance File (*RMMF*), which is maintained throughout the whole lifecycle of the product.
- The Project Architect defines which additional risk management surveillance activities are required after release of the product. These additional activities are included in the risk management *surveillance plan* of the product family. This plan describes all the product risk related activities after release of the product. These activities are referred to as risk management surveillance trending.

Post Market:

The purpose of risk management surveillance trending is threefold:

- Measure and monitor whether the assumptions made in the Risk Management Matrix (*RMM*) are and remain valid, i.e., actively guard that the residual risk of a released product remains within acceptable limits.
- Identify and assess risks which were unknown at the release of a product. Symptoms that signal a potential or actual change in risk are triggers to execute a risk assessment. Routinely

complaints, including service work orders, the Maude[1] database and changes in standards and regulations are assessed.

- Identify whether or not the defined Essential Performance is still correct after releasing the product.

An overview of the interrelations between the parts of the current *safety risk management process* is depicted in the figure below. In the next section, each part in this figure is described in detail.

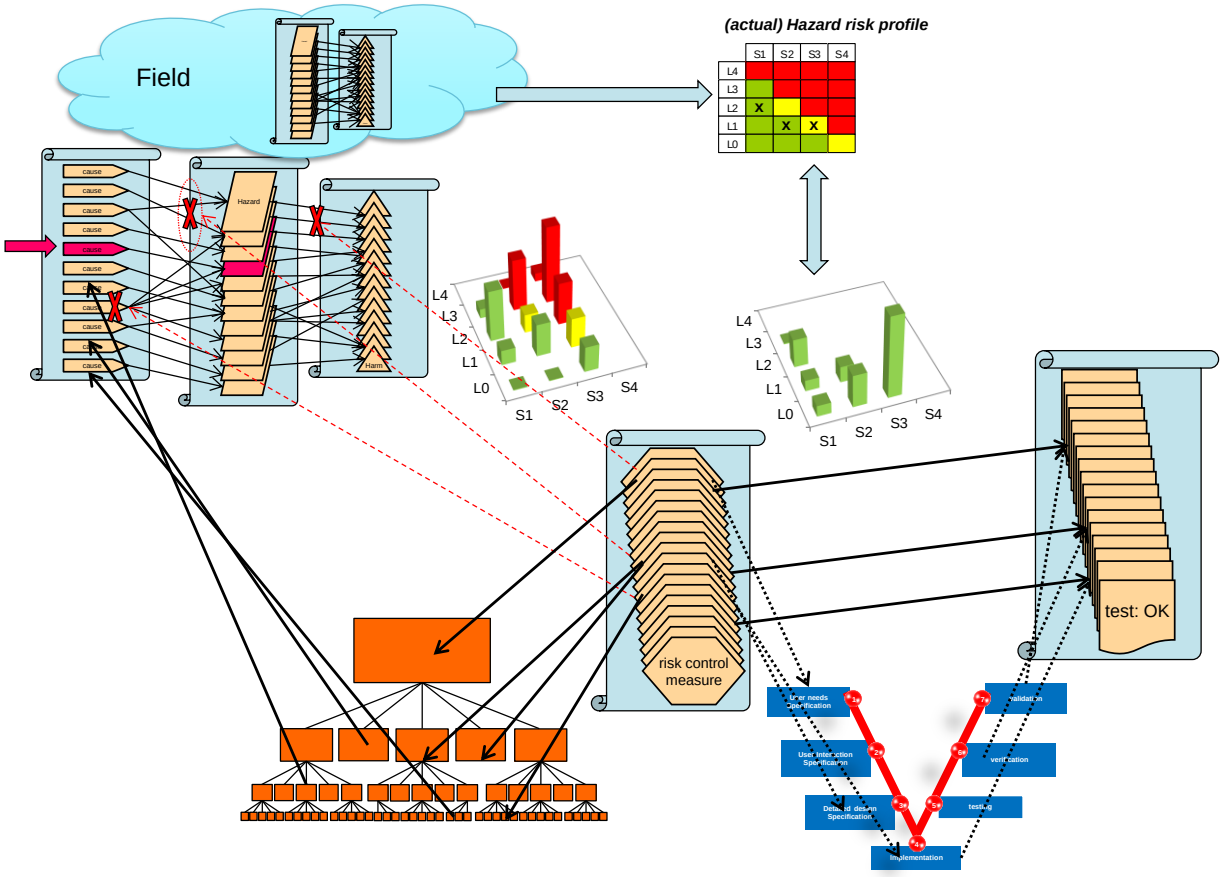
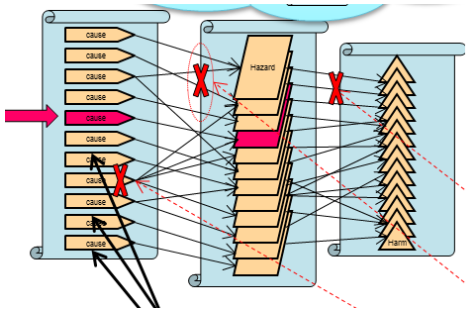


Figure 2-3: *Overview of interrelations between parts of the safety risk management process.*

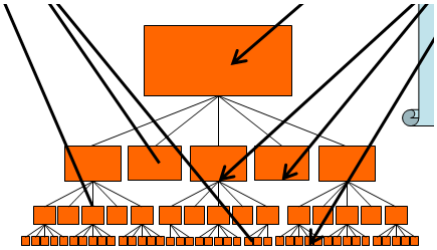
In figure 2-3, the following parts can be distinguished:



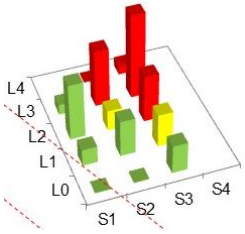
product safety risk assessment: This represents the *sequence of events* that can produce hazardous situations and harm. The indicated sequence is from cause to hazard to harm. As indicated in the figure, one cause can result in more than one hazard and in more than one harm. One harm can be caused by more than on cause. This results in a m-to-n relationship between causes, hazards and harms.

The red-crosses are entry points for risk control measures.

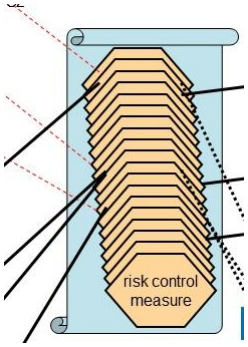
[1] MAUDE: "Manufacture And User facility Device Experience" database of FDA containing reports of adverse events involving medical devices.



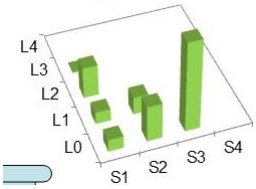
system design: The system is build up from hardware and software components and units. The corresponding design choices directly affect the possible causes for hazards and harms. The diagram represents the hierarchical build-up of the system design.



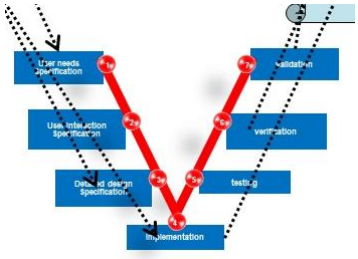
initial risk profile: based upon the *severity* of harm and *likelihood* of occurrence of the hazards, a risk profile of the complete product can be compiled. Sequences of events resulting in harms with high severity (e.g. S4) and high likelihood (e.g. L4) are unacceptable.



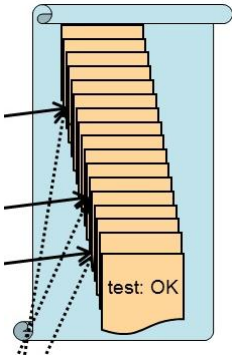
risk control measure: Within the *risk management process* risk control measures are defined and implemented to reduce the risk(s) to an acceptable level. As indicated with the connecting lines, risk control measures are preferable defined as safety concepts and specified in the top level of the system design. Other risk control measures are defined and implemented on unit level.



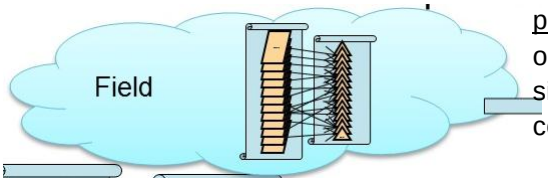
residual risk profile: This is the risk profile after implementing the risk control measures. The risk analysis process is repeated until sufficient risk control measures have been defined and implemented to reduce the risks to an acceptable level.



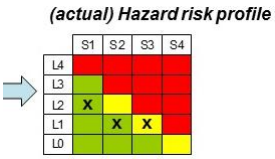
development process: The risk control measures are realized via the development process. Note that some measures have impact at the overall system requirements and design level and some only at the low-level detailed design level. For each *risk control measure*, test and verification results are collected at the corresponding design levels.



test evidence: For all risk control measures, test and verification evidence is collected from the development process.



post market analysis: customer complaints and service work orders are analysed with respect to occurrence of hazardous situations and adverse events. When needed additional risk control measures are defined and implemented.



actual risk profile: using the data from the post market analysis, the actual product risk profile is compiled. This profile is compared to the estimated residual risk profile.

2.2.4 Tools used in the safety risk management process

The tools used in the current *risk management process* are indicated in figure 2-4. The relations between causes, hazards, harms and risk control measures are maintained in an Excel-file. Various manual actions and checks are required to keep the data consistent with design changes and with data collected from the field.

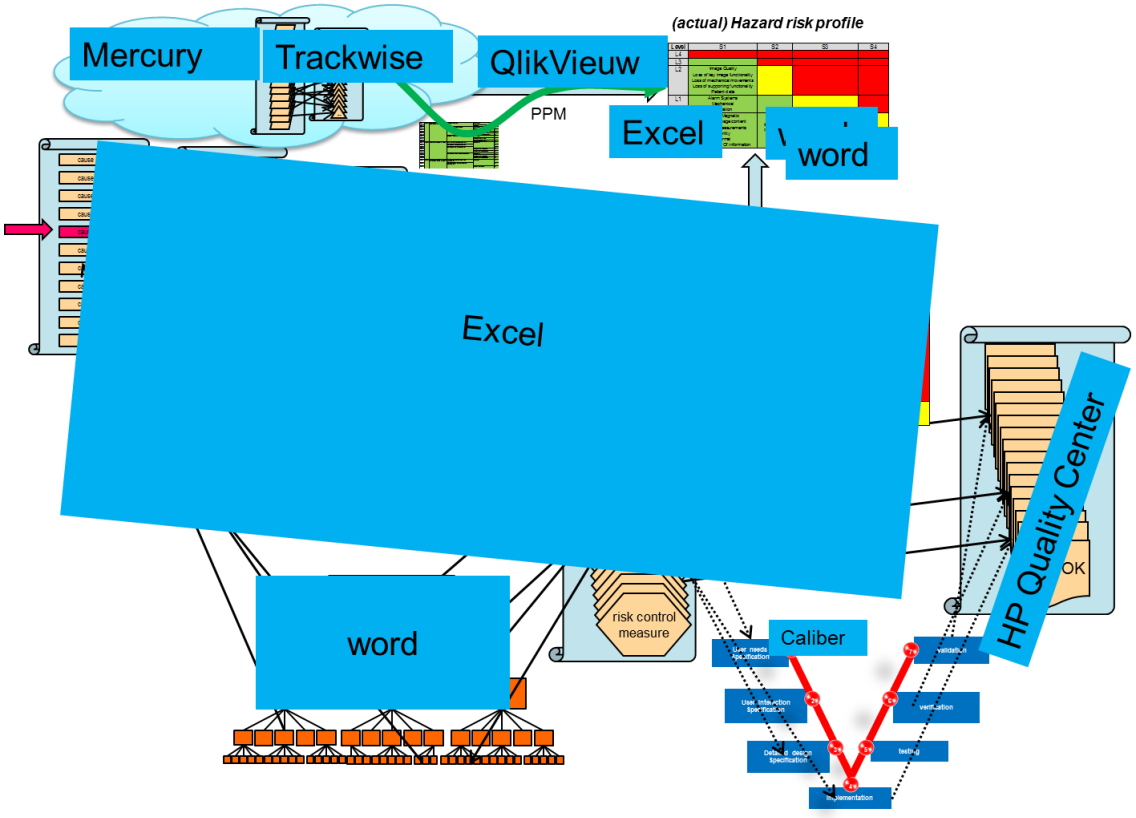


Figure 2-4: *Tools used within the safety risk management process*

In the following paragraphs, areas of improvement are illustrated using a number of case studies.

2.3 Case studies

2.3.1 Case study 1: analysing risk profile related to an adverse event

When an adverse event or hazardous situation is reported using the systems in the field, it should be analysed whether the corresponding *risk* is at a unacceptable or acceptable level. As a start, the cause of the event needs to be investigated. The next step is to check whether the sequence of events from cause to hazard and harm is already included in the risk analysis.

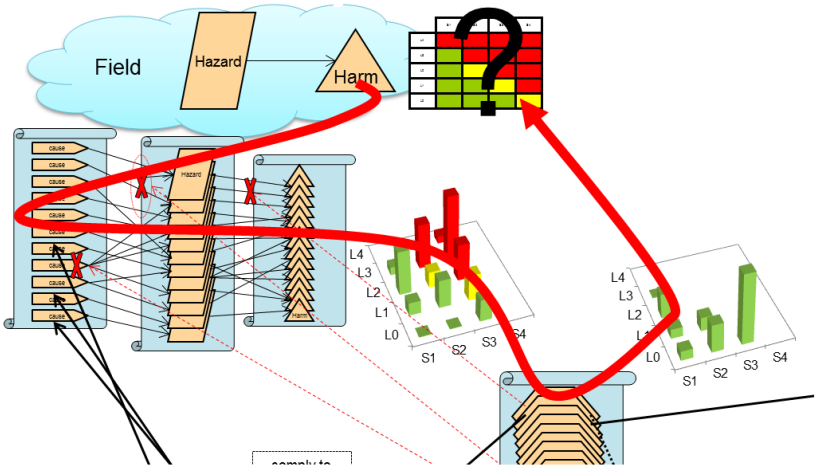


Figure 2-5: *Analysing events reported from the field.*

Current practice to determine the corresponding risk level is to count the number of similar events reported from the field. The corresponding severity of the possible harm is determined during a brainstorm with a member of the application group (clinical marketing).

Possible improvements:

- using a structured description of the event as it occurred at the customer site (*story telling*) and linking the event to a (pre-defined) list of hazardous situations improves the efficiency of analysing the events.
- insight and easy access of the *product safety risk assessment* avoids executing the same safety risk assessment several times for similar events.

2.3.2 Case study 2: impact analysis of design changes

While developing a new version of the product, part of the risk analysis has to be redone, because changing components and units may result in changes in cause-hazard-harm relations. In addition, possible new risk control measures have to be defined and implemented or different implementations of existing risk control measures are required. Currently, a number of manual steps have to be executed:

- identify the role of a unit to be modified within the risk management file:
  * what causes are linked to this unit?
  * what risk control measures are linked to this unit (i.e. implemented by the unit)?
- analyze impact of new unit on causes and risk control measures:
  * is likelihood of occurrence of causes changed?
  * are new causes introduced?
  * can all risk control measures linked to the previous version of the unit be implementd by the new unit?
- analyze the impact in the initial and residual risk profile
  * are all risks in the updated residual risk profile within the acceptable region?
  * are additional risk control measures required?
  * what risk control measures can be removed?
- identify what test evidence for risk control measures needs to be renewed?

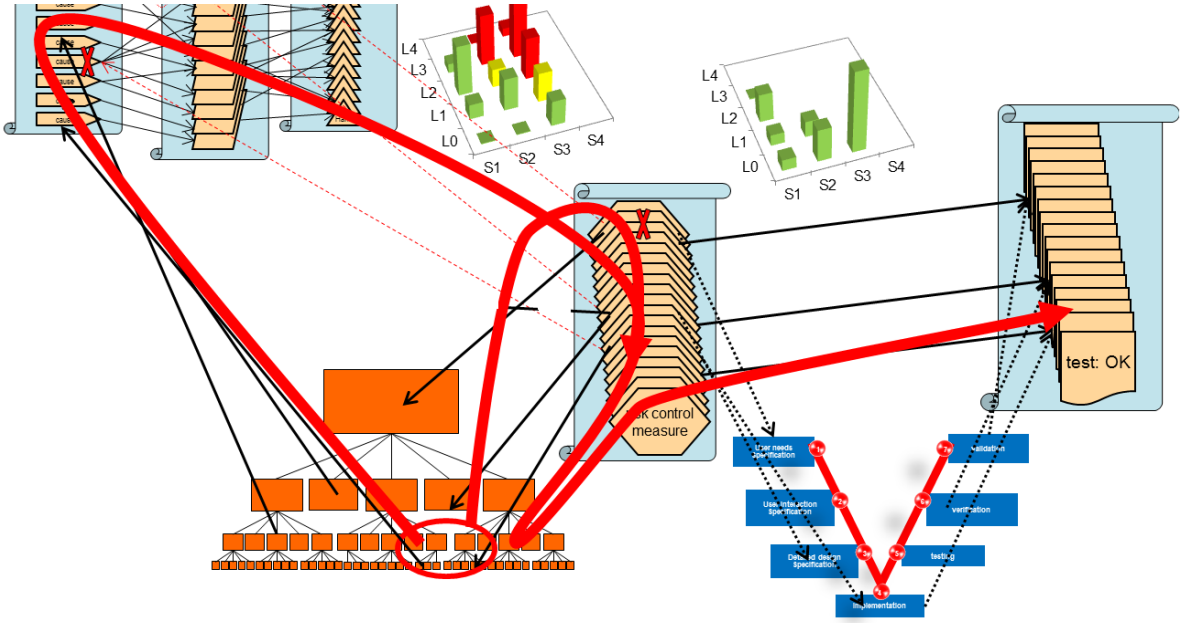


Figure 2-6: *Impact analysis of design changes.*

Possible improvements:

- fewer manual steps in impact analysis
- automation in maintaining relations between design, cause, hazard, harm, risk control measures, test evidence and experience
- automatic generation of (impact on) initial and residual risk profile.
- split up of the *product safety risk assessment* in a technical part and clinical part:
  - *technical part*: incorporating sequence of events from cause to hazardous situation and estimation of likelihood of occurrence. This incorporates technical reliability data.

- *clinical part*: incorporating sequence of events from hazardous situation to harm. This incorporates clinical usage of the system, critical parts of an examination and clinical actions to reduce harm.

As an example:

- *technical part*: uncontrolled tilt movement of the patient support.
- *clinical part*: patient shifts of table and hits floor; severity of harm depends on patient condition, and personel able to prevent patient from sliding of the patient support; likelihood and severity distribution depends on number of examinations with a patient in horizontal position on the patient support without fixation or hand grips.

2.3.3 Case study 3: comparing actual risk profile to residual risk profile (trending)

Using the data of events/reports from the field as entered in the Trackwise system, an *actual risk profile* of the product in the field is generated at regular times. A combination of QlikView and Excel is used to monitor the trend. The *actual risk profile* needs to be compared to the *residual risk profile* as determined during the pre-market phase.

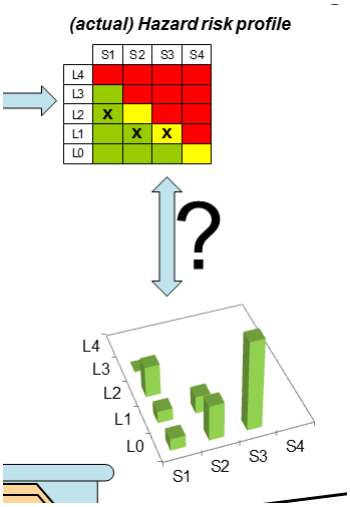


Figure 2-7: *Comparing actual risk profile to residual risk profile.*

Possible improvements:

- Alligning *hazardous situations* as identified in the pre-market fase with the *hazardous situations* as used during the post-market fase improves the mapping between the pre- and post-market risk analysis.
- uniform representation of profiles: express likelihood of occurrence in terms of number of harms per 1.000.000 examinations (ppm) and add up ppm's from causes that result in the same harm.
- take into account the differences between reports from the field and the pre-market analysis:
    - the pre-market analysis is *cause* related. It either starts with the cause or tries to find possible causes of hazards and harms
    - the post-market report are *event* related. It reports how the customer sees a certain *event* and the actual cause is not relevant or not clear for the customer.

  Both viewpoints may result in a structural difference between residual risk profile and actual risk profile.

3 Detailed Description of the Use Case Process

An overview of the *safety risk management* process is presented in figure 3-1.

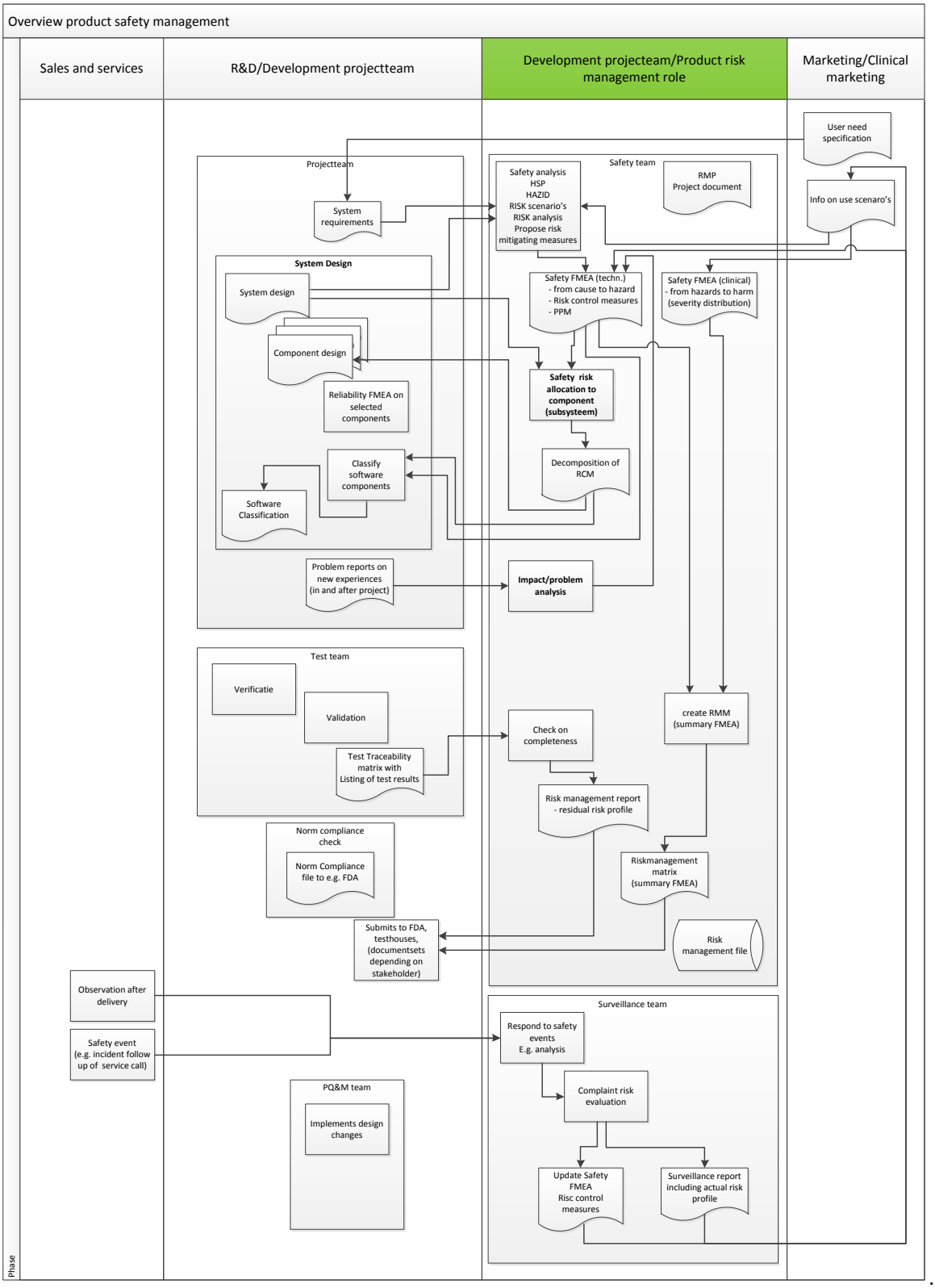


Figure 3-1: *Overview of Risk Management Process.*

Within the *risk management process*, the following artefacts play an important role:

- ***Risk Management File***

> **ISO 14971:2007 clause 3.5: Risk management file**
>
> For the particular medical device being considered, the manufacturer shall establish and maintain a *risk management file*. In addition to the requirements of other clauses of this International Standard, the *risk management file* shall provide traceability for each identified hazard to:
>
> * the risk analysis;
> * the risk evaluation;
> * the implementation and verification of the risk control measures;
> * the assessment of the acceptability of any residual risk(s).
>
> *NOTE 1: The records and other documents that make up the risk management file can form part of other documents and files required, for example, by a manufacturer's quality management system. The risk management file need not physically contain all the records and other documents; however, it should contain at least references or pointers to all required documentation. The manufacturer should be able to assemble the information referenced in the risk management file in a timely fashion.*
>
> *NOTE 2: The risk management file can be in any form or type of medium.*

- ***Safety FMEA***: containing the details of the risk analysis. The following parts are distinguished:
  * *safety FMEA (techn.)*: This represents the *technical* part of the risk analysis. It incorporates the sequence(s) of events from causes to hazards without looking at harm. The likelihood of occurrence is expressed in terms of PPM (= number of occurrences per 1.000.000 examinations). Two PPM values are included: *initial* and *residual* (after risk mitigation via risk control measures). For each sequence of events, references to the corresponding risk control measures are included.
  * *safety FMEA (clinical)*: This represents the *clinical* part of the risk analysis. It incorporates the clinical use of the systems and the resulting propagation from hazards to the various severity levels of harm.
  * *risk control measures*: incorporating description and allocation of risk control measures
  * *test traceability matrix (TTM)*: traceability between test execution and risk control measures.

In detail, the *safety FMEA (techn.)* contains the following items:

item		description
Hazard		The Hazard category, as defined in *Product Risk Management Procedure*
Cause Tag		Unique tag, identifying the Cause.
Cause Description		Description of the root cause/sequence of events that lead to the hazardous situation.
Usability		this attribute classifies the root cause within the usability categories (related to IEC62366).
Cause Related Component		Technical component that contributes to the cause.
SWc		Checked if Software could contribute to the hazardous situation (for IEC62304 Clause 7.1: hazardous situation direct result of software failure)
caused by:	*Medical Device User*	Checked if the Medical Device user contributes to the root-cause.
	Patient	Checked if the patient contributes to the root-cause
	Medical Device (tech)	Checked if the Medical Device itself contributes to the root-cause (usually technical causes)
	Manufacturing	Checked if the manufacturing process of the Medical Device contributes to the root-cause (Manufacturing includes installation of the system until first hand-over to the customer at which point Service starts).
	Service	Checked if the service performed on the Medical Device contributes to the root-cause
	Environmental factors	Checked if environmental factors of the Medical Device contribute to the root-cause
Initial Probability		The estimated PPM value of the probability of the cause to occur per exam. Assumed is that: - The system is used for 1000 examinations per year - The lifetime of the system is 10 years. - The Risk Control Measures have not been implemented.
Risk Control Measure Tag		reference to *risk control measure(s)*.
Residual Probability		The estimated PPM value of the probability of the cause to occur per exam. Assumed is that: - The system is used for 1000 examinations per year - The lifetime of the system is 10 years. - All Risk Control Measures have been implemented.

In detail, the list of *risk control measures* contains the following items:

item	description
Risk Control Measure Tag	Tag by which each safety requirement (risk control measure) is uniquely identified.
Risk Control Measure Description	Description of the Risk Control Measure.
SRS Requirement Tag	Reference to the related SRS requirement (Used for generation of the RMM overview.)
SWm	Checked if Software plays a part in the implementation of the Risk Control Measure (for IEC62304 Clause 7.2).
Design Measure	Checked if the measure is implemented in design
Manufacturing Measure	Checked if the measure is implemented in the manufacturing process
Service Measure	Checked if the measure is implemented in service process
User Measure	Checked if the measure is implemented by the Medical Device user.
Meas. Rel. Comp.	The component that is directly involved in the realization of the Risk Control Measure. *note*: When the safety requirement means compliance to a standard (IEC, HHS, etc.) the Measure Related Component is 'project'. The system release project is responsible for defining and proving compliance to standards.

The engineering methods indicated in the process diagram are described in the next chapter.

4 Identification of Engineering Methods

	Input	Output	Tools
Safety analysis (analyze risk scenario's; intended use; foreseeable misuse; identify hazards; risk estimation; risk evaluation; propose risk mitigating measures)	- System Requirements Spec. - System Design Specification - info on use scenario's - Safety FMEA (clinical)	Safety FMEA (techn.)	Excel (file create) Agile DHF (PLM) Word (SRS/SDS)
Safety risk allocation to component (subsysteem)	- Safety FMEA (techn.) (risk control measures) - system design specification	Decomposition of Risk Control Measures (allocated to components)	Excel
Impact/problem analysis (redo part of safety analysis)	- problem report	Safety FMEA (techn.)	ClearQuest Excel
Check on completeness (all testcase for risk control measures executed with "passed" test result)	- Test Traceability with test results - Safety FMEA	Risk management report (*RMR*)	Word (file create) Excel
create RMM (summary FMEA)	- Safety FMEA (techn.) - Safety FMEA (clinical)	Risk Management Matrix (*RMM*)	Word (file create) Excel
Complaint risk evaluation (analyze complaint information; identify hazard; risk estimation; cause identification; update safety FMEA)	- Complaint description - System Design Specification - Safety FMEA (techn.) - Safety FMEA (clinical)	Safety FMEA (techn.) (update) Safety FMEA (clinical) (update)	TrackWise ClearQuest Word Agile DHF (PLM) Excel

Refer to chapter 7 Annex I: Detailed Descriptions of the Engineering Methods for a detailed description of the engineering method *complaint risk evaluation*.

5 Terms, Abbreviations and Definitions

also refer to definitions in paragraph 2.2.2 Definition of terms.

Table 5-1: *Terms, Abbreviations and Definitions*

6 References

European Directive [MDD]	Council directive concerning medical devices (Medical Device Directive, MDD) Annex I – Essential Requirements. (93/42/EEC 1993-06-14; upto and including amendent 5: 2007/47/EC 2007-09-05)
USA federal Regulations [FDA]	Code of Federal Regulations, Title 21, Subchapter J, Part 1010: *Performance standards for electronic products: general* (2012-04-01) Part 1020: *Performance standards for ionizing radiation emitting products* .30: *Diagnostic X-ray systems and their major components* (2012-04-01) .31: *Radiographic equipment* (2012-04-01) .32: *Fluoroscopic equipment* (2012-04-01)
[IEC60601-1:2005]	Medical electrical equipment – part 1: General requirements for basic safety and essential performance (edition 3.0: 2005-12)
[ISO14971:2007]	Medical devices – Application of risk management to medical devices (second edition: 2007-03-01; corrected edition 2007-10-01)
IEC62366:2007	Medical devices. Application of usability engineering to medical devices (edition 1.0: 2007-10).
IEC62304:2006	Medical device software – Software life cycle processes (first edition: 2006-05)

7 Annex I: Detailed Descriptions of the Engineering Methods

In this section the engineering method: ***Complaint Risk evaluation*** is decribed in detail.

Pre-Condition	Engineering Activity as Steps	Post-Condition
- complaint in TrackWise	1. Collect and analyze data from customer (using Customer story, logfiles, interviews,..) 2. Convert input to *structured problem description* and *cause description* in PCI-form *Tools: e-mails, word, log-file analysis, Trackwise*	- complaint description and additional data in Trackwise - structured problem and cause description in PCI-form (using word)
- complaint in TrackWise - Hazard Harm Matrix (HHM) - HHM mapping	Complaint Evaluation for Risk Assessment: - identify applicable HHM code - determine corresponding Hazard category *Tools: PCI-form (word), HHM (Excel), HHM mapping (Excel), TrackWise*	- PCI form indicates yes/no hazard involved. - HHM code added to complaint in TrackWise and PCI-form (word)
- complaint in TrackWise - Hazard Harm Matrix (HHM) - Safety FMEA (techn.) - Safety FMEA (clinical)	Hazard Severity Evaluation: - determine severity of Hazard in Complaint - determine related worst case severity according Safety FMEA - determine trend of Hazard category *Tools: PCI-form (word), HHM (Excel), Safety FMEA (excel), Hazard trend (TrackWise, QlikView)*	- PCI form indicates yes/no risk assessment required - PCI form contains hazard trend.
- complaint in TrackWise - system design - component design	Cause investigation: - investigate cause (design issue, part failure) - trend graph in case of part failure - investigation documented in TrackWise or ClearQuest and results copied to PCI-form. *Tools: PCI-form (word), part failure trend (SAP, TrackWise, QlikView), ClearQuest, design documents (word), log-file analysis*	- cause analysis documented in TrackWise or ClearQuest - summary of cause analysis in PCI form (word)
- complaint in TrackWise - cause investigation in TrackWise or ClearQuest - Safety FMEA - system usage profile	risk assessment and impact on safety FMEA: - design issue contributed to potential harm? - sequence of events from cause to hazard incorporated in Safety FMEA? - related sequence(s) of events incorporated in Safety FMEA? - ppm estimations correct? - sufficient risk control measures? - effectiviness of risk control measures as expected? - update of use scenario's needed? *Tools: PCI-form (word), HHM (Excel), Safety FMEA (Excel), Hazard trend (TrackWise, QlikView)*	- updated safety FMEA (techn.) (Excel) - updated use scenario's - updated safety FMEA (clinical) (Excel)

Table 7-1: *detailed description of complaint risk evaluation*

note: the activities as listed above only represent the risk management part of *complaint handling*. Other activities are executed to correct the problem in the field and when needed a component redesign is executed to prevent the problem from re-occurring.

8 Annex II: Technology Base Line & Progress Beyond

This information will be collected globally, and the respective part will be inserted here. Basically it could be something like a table with a row for each engineering method and a column for the current functionality, which is the technology baseline (e.g., “data has to be transferred by hand”), and a column for the expected progress in CRYSTAL (e.g., to be implemented in CRYSYTAL / “future work”).

The exact content of this section will be defined in the next technical Board Meeting.