JACEK ŁUCZAK

PRODUCT, PROCESS AND SYSTEM RISK MANAGEMENT PROGRAM

INTRODUCTION

Product risk is the inverse of product safety. As risk decrease, safety increase. Thus, a risk management program is, in fact, also a product safety program. The actual use of any medical device always includes some measure of risk to users or patients – no medical device is ever 100% safe.

Risk management is increasingly a requirement posed by the standards, or clients. However, a key practical question is – whether in practice the chosen method of assessment and risk management are useful for ensuring quality and safety of products and processes.

Risk is a measure of the possibility of loss or harm. The regulatory context for medical device risk management is the risk inherent in the use of the device – the risks presented to product users and patients. Product risk involves the combination of two factors, which each play a role in defining the level of risk.

The most important standard to suport a manufacturer's risk management program is ISO 14971:2007 (medical devices case)[1] [2] and ISO 31000:2009[3] [4] [5].

Medical devices are surrounded by special protection in risk management aspects, because the approach to them in this regard may be examples of a model of risk management. Their analysis should be useful for other industries.

It provides an example of a risk management process, describes the essential aspects of a risk management program and specifies particular activities and documentation that must be established.

The main topics in product risk management area: procedure, method of risk assessment, list of hazards etc.

---

[1] IEC 60601-1 – Medical equipment medical electrical equipment, (12-20)

[2] ISO 14971:2007 Medical devices -- Application of risk management to medical devices, (14-17)

[3] ISO 31000:2009 Risk Management – Principles and Guidelines, (3-17)

[4] T.T. Kaczmarek, *Zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Difin, Warszawa 2010, (15-27)

[5] J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2011, (67-70) (236-250)

1. RISK MANAGEMENT BASIC

Generally, risk is a measure of the possibility of loss or harm [6]. The regulatory context for medical device risk management is the risk inherent in the use of the device – the risks presented to product users and patients. Risk management in this context does not apply to business risks, such as financial risks associated with product development or introduction, or projekt development risk, such as scope creep or variable resource levels[7].

Product risk involves the combination of two factors, which each play a role in defining the level of risk. Both factors relate to harm, which is a physical injury or damage to the health of a patient or user or to the surrounding environment or property. A hazard exists relative to each harm (a hazard is a potential source of harm). For the harm to to occur, a scenario or hazardous situation must unfold. The hazardous situation is the sequence of circumstances that must exist to expose people, property, or the environment one or more hazards. Product risk involves the probability (or likelihood) that a particular harm will occur and a severity of that harm. Note that product risk may be defined with qualitative or quantitative measures of probability and severity[8].

Product risk is the inverse of product safety. As risk decrease, safety increase. Thus, a risk management program is, in fact, also a product safety program. The goal of such a program is to ensure that the product is as safe as practical and that the safety of the product is acceptable for a given intended use. The actual use of any medical device always includes some measure of risk to users or patients – no medical device is ever 100% safe.

Working with applicable regulatory authorities, each manufacturer must determine how much risk is acceptable. Establishing an acceptable level of risk depends of the intended use of the device. Intended use includes definitions of:

- particular health conditio of the patient population,
- general cognitive abilities of the patient population,
- skill level of the health practitioners involved,
- their level of direst supervision of the product`s use, and
- the use environment[9].

All these aspects of intended use play a role in determining the level of product risk. For example, paediatric or seriously ill adult patients may have less ability to detect a product malfunction and to notify a health practitioner when a malfunction occurs. And in case of clinic and home use – that same device; a product that is used in both a clinic environment and a home environment may have two different risk levels, given its two different intended uses.

---

[6] J. Gryz, W. Kitler (red.), *Systemy reagowania kryzysowego*, Wydawnictwo Adam Marszałek, Toruń 2007, (9-22)

[7] P. Goodwin, G. Wright, *Analiza decyzji*, Wolters Kluwer Polska, Warszawa 2011, (326-335)

[8] ISO/IEC 27002 Information Technology – Security Techniques – Code of practice for information security management, ISO 2005, (12-15)

[9] M. Molski, M. Łachota, *Przewodnik audytora systemów informatycznych [The IT systems auditor's guide]*, Helion, Gliwice 2007, (120-127)

Risk management is the systematic application of policies, procedures and practices to the tasks of analysing, evaluating, controlling and monitoring risk[10]. In other words, managing risk involves proactive evaluation, control and monitoring of product risk, and reactive response to actual situations that may indicate new of changing product risk.

2. RISK MANAGEMENT PROGRAM CONCEPTION

For sure, the most important standard to suport a manufacturer's risk management program is ISO 14971:2007 (Medical devices – Application of risk management to medical devices. The standard applies to all medical devices and covers the entire life cycles of a product from concept to disposal[11].

FDA first recognized ISO 14971:2000 as a consensus standard in May 2001, adopting the complete standard. In September 2007 FDA updated their consensus standard database to recognize last version in its entirety[12].

ISO 14971:2007 provides an example of a risk management process, describes the essential aspects of a risk management program and specifies particular activities and documentation that must be established. The general approach described by the standard includes establishing a clear statement of intended use for the device, considering risk under normal use scenarios and considering misuse such as incorrect use by a user.

In addition to that standard, numerous technical standards exist to suport risk analysis – e.g. FMEA, fault tree analysis and other.

3. GENERAL CHARACTERISTICS OF SAFETY RISK ASSESSMENT METHODS

In theory and in practice several dozens of methods for risk assessment and evaluation are utilised. These methods can be divided into 3 following groups:

- quantitative methods,
- qualitative methods,
- hybrid methods[13].

---

[10] G. Wieteska, *Zarządzanie ryzykiem w łańcuchu dostaw na rynku B2B*, Wydawnictwo Difin, Warszawa 2011, (78)

[11] M.E. Whitman, H.J. Mattord, *Readings and Cases in the Management of Information Security*, Thomson Course Technology, Boston 2006, (12-28)

[12] T.M. Pelnik, *The Quality System Compendium*, GMP Requirements & Industry Practice, 2nd edition, Arlington, 2007, (2-12)

[13] J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2011, (67-70) (236-250)

Qualitative methods

Qualitative risk assessment is most often a subjective evaluation which is based on best practices and experience. The outcome of such an assessment is a list of threats ranked by their risk level (low, medium, high). Qualitative methods are very flexible and open to various kinds of modifications. Owing to their flexibility and modifiability they provide the organisation with fast and cost-effective results when identifying threats and deploying security measures is concerned. However, because of the flexibility the scope and cost of risk assessment in different organisations can vary to a significant extent. That is why, depending on the available financial resources allotted for this purpose in the budget the scope of risk assessment may change in the course of time.

In qualitative risk analysis all risks and potential effects of their occurrence are presented in a descriptive way. It means using risk scenarios and determining the effects of potential realisation of risk. The scenarios should include numerous details which are helpful in taking specific actions and choosing proper security measures. In widespread use, there are various scales to describe specific situations and incidents.

Quantitative methods

In quantitative risk assessment it is essential to determine two basic parameters; the value of effect and the probability of occurrence of a specific risk.

The potential effects may be determined by evaluating the effects of risk events or extrapolated on the basis of data from the past. The consequences of risk events may be expressed by means of different categories (e.g. financial, technical, operational, human resources).

The overall quality of the analysis depends on the accuracy of indicated values and statistical validation of the deployed model.

Hybrid methods

Both quantitative methods and qualitative methods have some disadvantages. First of all, they are too general. Second, they do not identify all the needs with regard to safety in a precise way. Apart from that, they do not provide the organisation with sufficient information concerning the cost analysis when deploying new security. Because of this, the majority of companies make use of the combination of the two approaches. On one hand, qualitative analysis founded on scenario-based methods is used to identify all risk areas and potential effects of specific risks. On the other, quantitative analysis is used to determine the costs associated with the effects of risk occurrence. This also leads to significant increase in knowledge related to processes realised in an organisation and raises awareness on the potential risks.

3.1. Failure modes and effects analysis — FMEA

The Failure Mode and Effect Analysis (FMEA) is mainly a method to support quality management, however the concept and rules of risk assessment (organisational and technological) may also be applied in case of safety product risk assessment.

3.2. The OCTAVE Method

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a set of guidelines developed at Carnegie-Mellon University in 2001. This method is used, for instance by the US army, and is getting more and more popular in other, especially large, organisations.

3.3. The COBRA Method

The Control Objectives for Risk Analysis (COBRA) is a complete risk analysis method designed for the board and management of an organisation to thoroughly evaluate the profile of risks related to the conducted activity. Particular attention is paid to the security of the image, conformity with applicable legal regulations and laws and to internal control mechanisms.

3.4. The CRAMM Method

The CCTA Risk Analysis and Management Method (CRAMM) is a risk analysis method developed by the British Central Communication and Telecommunication Agency (CCTA) whose name was changed to Office of Government Commerce (OGC). The integral part of this method is a special IT tool for risk assessment (CRAMM). Using the method without the CRAMM software tool can be difficult.

3.5. The MARION Method

The method MARION (Methodology of Analysis of Computer Risks Directed by Levels) was developed by the CLUSIF (Club de la Sécurité de l'Information Français), and the last update was performed in 1998. Nowadays, CLUSIF does not longer finance nor promote the method as the financial resources were reallocated to another, newly developed, method, i.e. MEHARI. However, this method is still used by many organisations.

3.6. Individual methods

It is possible for the organisation to use its own methods which are compiled based on industry knowledge and experience. This approach, however, is only appropriate for large organisations which have proper organisational structures to compile and validate such a method. The biggest advantage of it is being fully

aware of the method as well as the whole risk assessment process by all people involved in the processes related to it. Obviously, there is a danger that the developed method may turn out to be ineffective and that the organisation shall not be granted a recommendation during the certification audit. In consequence, it may also not be awarded a certificate. For this reason, small businesses do not decide to develop their own methods and prefer to choose one of the methods which are already available. Such methods are usually approved of auditors during certification audits. Finally, small businesses do not usually have sufficient human resources to develop their own methods.

4. IMPLEMENTING, KEEPING AND DEVELOPING A RISK MANAGEMENT PROGRAM

Risk management program is typically implemented as an integral aspect of the quality system. Risk based decision occur throughout various quality system processes, and a cohesive approach to risk management exist across the manufacturer's organization. Risk management during product design, during production and after product realise are noticed below.

4.1. Product design risk management aspects

Effective risk management usually starts in conjunction with the design and development planning proces to ensure that the risk management care approach fits within the overall project plan. The key to proactive risk management is initiating the risk management proces at a point in the development life cycle when the results of analyses can affect the design process. Starting too late typically means that designers have progressed past a point where reasonable risk migration features could have been included in the design itself. The possible approaches for reducing risk are typically described as a prioritized list:

- inherent design safety,
- protective measures in the design or manufacturing processes,
- user notification.

A preliminary hazard analysis or risk analysis can be very helpful in ensuring that design inputs are comprehensive and address user needs. Risk analysis often starts with identification of potential hazards, definition of hazardous situations, estimation of the related risks, and evaluation to determine whether the risk is acceptable. For risks that are deemed unacceptable, control measures are planned and implemented.

4.2. Risk management during production and after product realize

As a part of the design transfer proces, production processes are typically planned and developed. Evaluation of potential failure modes or critical control points is often part of the proces developed effort. From a risk point perspective , when the production proces is under development, evaluation of potential hazards that could be introduced or exacerbated by the production proces itself is essential.

Furthermore, during design transfer the manufacturer often determines the type and extent of supplier controls, particularly for suppliers that provide products or services that are related to the essential outputs.

Risk management continues from the time the product is introduced into commercial distribution until the time the product is decommissioned. Each proposed product change must be assessed to evaluate the effect of the change on the product risk.

5. MAIN ELEMENTS OF RISK MANAGEMENT PROCEDURE IN PRODUCTION COMPANY – EXAMPLE

5.1. Qualification of Personnel

Risk Management is ideally carried out using a team and cross-functional approach. Whichever approach is used, all Organization personnel performing risk management tasks shall be trained in risk management techniques. The risk management process typically requires people with expertise in areas such as:

- How the device is constructed
- How the device works
- How the device is intended to be used – also see usability engineering
- How the device is actually used
- Ways in which the device might foresee-ably be misused
- How the device is produced
- How to apply the risk management process
- Clinical/ medical practice

It is permissible that personnel who contribute to risk management activities, for example production personnel taking part in PFMEA, clinical advisors, process experts etc. are not specifically trained in risk management techniques. However the personnel who complete the PFMEA record or guide the PFMEA shall be trained. Likewise design engineers may contribute to brainstorming of hazards but again the person completing the risk analysis activity shall be trained. The persons approving any risk management output shall be trained. The training and qualification of personnel performing risk management tasks shall be recorded according to the method(s) specified for training records by the local Quality Management System.

5.2. Risk Management Plan

All Risk Management activities shall be planned. Planning shall start early in the product's defined life cycle and shall cover the entire product life cycle. All elements of the risk management process should be mapped to the product life cycle. Each manufacturer shall establish and document a risk management plan for each product or group of similar products. The plan shall form part of the risk management file.

Risk Management planning must be completed during the Design and Development planning process. All risk management plans shall include at least the following:

- The identity and description of the medical device being considered, the scope of the planned risk management activities and the life-cycle phases for which each element of the plan is applicable e.g. there may be a single plan or several plans covering the product life-cycle from design through production, distribution, servicing and finally decommissioning. The plan shall clearly identify which variants, accessories and options are included in the risk management activity and cross-refer to the risk management files of any accessory not included:
  - A statement of the intended use of the product or a reference pointing to where the intended use is documented;
  - The inter-relationship(s) between appropriate risk management activities and design and development activities;
  - The key processes which directly affect risk management;
  - The resources needed for risk management, including the appropriate expertise;
  - Responsibilities and authorities;
  - The arrangements for management review of the risk management activities;
  - Criteria for risk acceptability based on the Risk Management Policy;
  - The verification activities that are planned to take place to confirm the effectiveness of the intended risk control measures. This includes planning the resources required for verification;
  - Details of the activities that will take place for the collection and review of relevant production and post-production information.

Top management should ensure the integrity of the risk management plan is maintained when changes to the Risk Management System are planned and implemented.

5.3. Risk Management File

Each product/ product family shall have a documented Risk Management File. The file shall be maintained and kept up to date. The File can be in any form or medium, but if the file is maintained electronically the software used shall be validated for its intended use. The file shall contain the Risk Management Plan, the Risk Management report and provide traceability for each identified hazard to:

- The risk analysis;
- The risk evaluation;
- The risk control measures selected, the review of the effects of those measures i.e. any new hazards or hazardous situations introduced and review for completeness;
- The rationale for acceptance of any residual risks if applicable;
- Risk/ Benefit analysis (if applicable);
- Records of the implementation and verification of risk control measures;
- Evaluation of overall risk acceptability.

The essential performance of the device shall be identified in the Risk Management file, as shall the expected service life. The file shall show where the training records of personnel performing risk management tasks during the project are retained.

The file could contain the documents above or contain references or links to them if held elsewhere in the Quality Management System.

Ownership of the risk management file

The product risk management file shall be created during the New Product Design (NPD) process and shall be owned and managed by the NPD function. Following the completion of design transfer the file shall be transferred to the ownership of the Engineering (product maintenance) function within the Supply Chain. On completion of the expected product life, the ownership of the file shall be transferred to the assigned product owner.

Document control

Documents or records resulting from risk management activities such as reports, procedures etc. may be maintained or referenced in either the risk management file or other appropriate files e.g. Design History files (DHF), Device Master records (DMR) or Process validation files. The local document control and control of records procedures shall apply to these documents and records, wherever they are maintained.

5.4. Risk Analysis

Design and development inputs for a product must include adequate consideration of the intended use of the product and the product's functional, performance, safety and regulatory requirements. Therefore risk analysis shall be conducted during the planning phase of the project and be complete prior to the approval of the design inputs / system requirements. The output from risk analysis shall form one of the design inputs/ system requirements. Early risk analyses may evolve as the design process continues and risk estimates are refined.

If a risk analysis or other relevant information is available for a similar medical device, that analysis or information can be used as the starting point for the new analysis. The degree of relevance depends on the difference between the devices and whether these introduce new hazards or significant differences in outputs, characteristics, performance or results. There must be a systematic evaluation of the effects that the differences have on the development of hazardous situations. If the product is intended to be used in combination with another medical device or equipment, then hazards and control measures should be evaluated for each device individually as well as for the system as a whole.

Risk related data from post production information for the generic type of device must be considered if it is available, for example complaints, adverse incident and MDR reports, competitor information, field safety corrective actions (recalls) etc.

Risk-related information on the production methods should also be considered e.g. PFMEA's.

The Risk Analysis documentation shall include at least the following:

- Description and identification of the product that was analysed, i.e. its unique identification (e.g. Project code);
- Identification of the team who carried out the risk analysis and their roles/ expertise
- Scope and date of the risk analysis (i.e. new product or a revision of an existing Risk analysis); Risk analysis consists of identifying hazards and the potential harms due to those hazards and estimating the risks of those harms occurring. Hazard identification must start by considering the product's intended use and its users, its characteristics and its environment.

Finally the procedure is consist of: risk evaluation, risk acceptability criteria, risk control, residua risk evaluation, risk/ benefit analysis, risk arising from risk control measures, check of completeness of risk control, evaluation of overall residua risk acceptability, risk management report, risk management review.

CONCLUSION

Managing risk involves proactive evaluation, control and monitoring of product risk, and reactive response to actual situations that may indicate new of changing product risk. ISO 14971:2007 provides an example of a risk management process, describes the essential aspects of a risk management program and specifies particular activities and documentation that must be established. The general approach described by the standard includes establishing a clear statement of intended use for the device, considering risk under normal use scenarios and considering misuse such as incorrect use by a user.

Finally is necessary to create the own, individual procedure for risk assessment and management.