Risk management in medical software

Miklos Taliga
Department of Control Engineering and Information Technology, Budapest University of Technology and Economics
Budapest, H-1117 Magyar Tudósok Körútja 2 Hungary

and

Dr. Katalin Balla
Department of Control Engineering and Information Technology, Budapest University of Technology and Economics
Budapest, H-1117 Magyar Tudósok Körútja 2 Hungary

ABSTRACT

In the following article, we aim to examine and analyze the efficacy of product related risk management directives in the development of medical devices, along with the resource requirement and the reliability of risk management. We will also inspect the development methodologies suggested for keeping errors at a low level, detailing measures which help in analyzing and eliminating causes of errors, and in a higher rate of error detection. We focus our attention on a real case and the definition of concepts laid out in related standards. In doing so, we will analyze the adaptability of these concepts and processes based on them to various development methodologies, which are used in the development of medical software. Through the concept of risk and hazard, and using related formulas, we will inspect whether the time and resources allocated to risk management and assessment are proportional to the expected final quality level of a given product. We will summarize the results and propose an optimization algorithm. We will also suggest a way of reducing risk even before development, during the design phase; we investigate how much does a possible risk add to required resources during the development and testing period.

Keywords: Medical software, software testing, standards, technical risk, risk matrix, verification, PEMS, PESS, safety critical environment

1. INTRODUCTION

Devices used in the treatment of patients or the screening of healthy people may contain electronic components. In more advanced devices, hundreds of such components may exist, which are monitored and controlled by a software element or a group of such elements. It is natural to expect devices which may affect human lives and health, to operate safely and reliably. It is, consequentially, important to understand and, if possible, to reduce risks and hazards these devices may pose to their users, their operators or their environment. Most electronic medical devices belong in the category of safety critical devices, so, in the introductory part of the article, we will explain the related definitions, standards, and the stricter requirements towards such devices. Subsequentially, we will describe further complementary measures related to these standards, which serve to reduce the risk of severe errors remaining in a product containing hardware and software elements, when delivered to the customer. We will use a component of an acute dialysis device as an example to explain the steps of risk management and the measures taken to reduce the risk of malfunction. In the following chapters we will examine the methodologies and process which serve to keep error rates low.

2. DEFINITIONS AND STANDARDS

As most electronic devices are capable of inflicting harm and injury on a human being, the concept of risk and hazard are essential. While it may not sound proper to draw together the concept of harm and loss to business, there is a definite connection between the two. Loss to business is an undesirable event which results from the malfunction of a device causing harm, temporary or permanent injury, or, in the worst case, death. Such an event may lead to the loss of current or future contractors. Malfunctioning software may cause a hazardous situation, which qualifies as endangerment. Essentially, it covers the occurrence of a potential hazard which may directly affect human health or the natural, economical or technological environment. The likelihood of a hazard occurring is defined as risk. Hazardous situations can lead to accidents, which should be minimized. The possible scenarios involving hazardous situations and accidents are identified during risk assessment. The likelihood of an accident may be used as a numerical value in the process of risk minimization.

A large number of standards were developed to address different aspects and formulate different requirements towards safety critical systems; Table 1 summarizes such standards.

The circumstances which may lead to death, injury, occupational accidents, or damage to the device, property or to business are detailed in the IEC 50(191) and the MIL-ASTD882B:1984 standards. The IEC 61508/61551 standard describes the concept of hazard as a source of, or a situation involving potential injury or damage. The same standard provides the definition of functional safety as well, which can be used to determine whether an electronic system is free of permissible risks which can be traced back to malfunctions of the electronic system. The definition of functional safety according to IEC 61508/81551: “Safety measures taken during the operation of a device in order to avoid hazards related to the main function of the device”. The process of design control is described in the ISO13485 standard. The standard provides help in establishing development plans and goals, planning development (selecting a software life cycle), and determining verification, delivering and validating the technical plan and in issuing and selling the product. The IEC 60601-1:2005 complementary standard describes processes to be followed

during the development of electric medical devices containing programmable electronic subsystems in order to ensure their safety. This standard also requires documenting these processes. We will also cover measures which serve to detect, avoid and eliminate causes of errors. In the third chapter we will bring examples to measure which help to eliminate causes of errors.

Name	Standard	Description	Effect on medical equipment or standard
Medical equipment management standards	ISO14971 ISO13485	Designates the basics of medical equipment development	Influences the development of medical equipment
Medical equipment process standard	IEC 62304	Provides a detailed guide to the development and maintenance of a secure software system	These standards appear as an input requirement for medical equipment management standards, as they form the basis of these standards these standards also influence the development of medical equipment
Medical equipment product standards	IEC 60601-1	Provides specific guidance to the production of safe medical equipment	These standards influence the realization of medical equipment management standards, and indirectly affect the development of medical equipment
Miscellaneous standards	IEC/ISO 12207 IEC 61508-3 IEC/ISO 90003	Supplementary guidelines, techniques, etc. that may be useful during development	These support the development of medical equipment

Table 1. : Standards affecting the development of medical equipment.

The IEC 60601 standards provide guidelines for risk management processes. The IEC 60601-2-X standard defines extra requirements for a given product, which may modify the requirements of general and complementary standards. The IEC 60601-1-X standard can be used to define structures or chapters, for example in the documentation, and as a part of the IEC 60601-1 general standard, it proposes emergencies, which are to be considered and taken into account. The IEC 60601-1 general standard defines basic safety measures, which are evaluated during risk management.

3. TECHNICAL RISK

According to the expectation of the members of society (or, in a narrower sense, the users and the customer) minimizing technical risk means the development of the software or the electronic device in a technological system which meets the technical requirements for safe operation and can reduce the likelihood of malfunction. There are various types of risks related to electronic devices and their controlling software. The first type of risks are called acceptable (or tolerable) risks, where operation is permitted without the risk being reduced. Such risks are accepted with an agreement of the management, the developer and the customer. The second type is called unacceptable risk. Unacceptable risks must be reduced, or, if possible, eliminated. The remaining group is the smallest one, as it consists of the residual risks, which remain after the reduction of identified risks after the full risk management process. After a successful risk management process, residual risk has to be lower than the acceptable risk. The MIL-ASTD882B:1984 standard interprets the malfunction of the blood-leak detector in an acute dialysis device as a situation which may directly lead to injury or death. Malfunction of this components can be either software or hardware based. If the device is incapable of translating the detection of a bubble to an electronic signal, it is a hardware malfunction. A register storage error is a software malfunction. In the latter case, the sensor cannot save data from the processed signal to the register. All possible malfunctions of the blood leak detector have to be investigated through the standard. These cases will go in the three risk categories. In a normal situation, risk (R) is determined as the product of likelihood (F) and effect severity (C). [4]

$$\boldsymbol{R = C\,x\,F}$$

In software containing multiple subsystems, total risk can be determined using the following formula:

$$\boldsymbol{R = \sum_{i=1}^{n} C_i x\, F}$$

In the formula, the products of likelihoods (F) and effect severities (C) of separate events are unrelated. The aforementioned standard determines functional safety (S) with the

$$\boldsymbol{S = \frac{1}{R}}$$

formula, as the likelihood of a hazard-free state. The desired, or acceptable risk can be determined using the following formula:

$$\boldsymbol{\frac{Fr}{MaxFr} + \frac{Con}{MinC} < 1}$$

According to this formula, the quotient of the frequency (Fr) of an event and the maximum tolerable frequency of negligible events (MaxFr) plus the quotient of the consequence of an event (Con) and the severity of an event (MinC) (which has a negligible likelihood of occurring) must be lower than one. The ALARP (As Low As Reasonably Tolerable) principle (see Fig. 1.) is used to manage hazards, which also allows hazardous situations to be categorized. The ALARP principle can provide further help in determining the level of risk reduction. In that case, there are also three different risk categories: unacceptable, partially acceptable and acceptable. Part of the difference is that revealed risks have to be analyzed in detail. Importantly, risk reduction is only eschewed if it is not feasible or if the cost of risk reduction is disproportionately high compared to the expected results. If the risk is generally acceptable (by risk management, development and the customer), there is no need for further assessment or risk reduction measures.

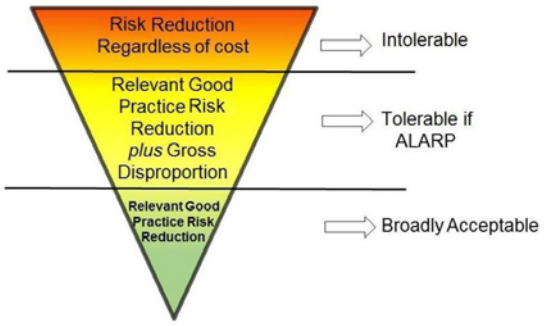

Fig. 1 ALARP Principle [1]

If the numbers of identified risks is higher than acceptable, risk reduction measures and processes must be implemented. We would like to emphasize that this does NOT equal to risk management during the development of test planning, as it happens earlier, as an intervention to and supplementing the testing / development process. Thus, the system has to be expanded with new processes and functions that enable reducing the occurrence or the elimination of a certain error. The final goal is to reduce the number of risks at least below the acceptable level. It is important to note that a completely risk-free state cannot be achieved, but nevertheless, the aim should always be risk-free from as early on as the design phase. The IEC 61508 standard underlines that non acceptable risks always have to be reduced. Every foreseeable circumstance, malfunction and operator error which leads to a hazardous situations (that is, every such series of events) has to be analyzed according to this standard. Series of events leading to hazardous situations are detailed in the following chapter.

3.1. Example: Risk assessment of an acute dialysis device

The latest Diapact CRRT acute dialysis device, manufactured by BBraun, contains a blood leak detector.

Fig. 1 Diapact CRRT [1]

The malfunction of the blood leak detector may directly cause death. The blood flowing in the tubes of the device can be considered continuous and leak-proof only if the number of bubbles in the tubes is minimal. If the number of bubbles exceeds a certain critical value, the blood of the patient is likely to have leaked from the system and was replaced by air. Thus the device for monitoring blood leaks is a critical hardware and software component, and so malfunctions are assumed to be very unlikely and catastrophically severe. A blood leak detector is an electrical medical device. A dialysis device is also a PEMS (Programmable Electrical Medical Device), which is a medical electrical device which contains one or more programmable subsystems. The continuous monitoring of the blood leak detector must be independent from the executive (i.e. control) system. Monitoring can thus be handled by a PESS (Programmable Electronic Subsystem). A PESS is based on one or more central processing units, including software and interfaces. A PEMS may contain one or more PESS, or they may be the same thing. Hardware and software malfunctions and operator errors have to be distinguished during risk assessment. Operator errors can be reduced trough proper education and also through displaying important information on the device. In the case of a blood leak detector, education or informative displays are not necessary, as it is embedded in the device. There are, however, several ways to reduce hardware errors. The first is to create design directives which enable a safe implementation of the hardware element. For example, during the design of the printed circuits, the device has to be checked for interruptions and short circuits. This may be achieved with a diagnostic function of the design software, a real-time instrumental measurement or the constant monitoring of the working device. Monitoring is best done independently from the control system, so that a malfunctioning device still provides feedback. In hybrid safety systems, control and safety software processes run on the same processor. Constant self-testing is an option as well, like the checksum processes (CRC, MD5) on the data stored in the EEPROM register tests during the self-test of the microcontroller, instruction set tests, or power supply tests. The self-tests of analogue signals also belong here if ACD is involved. Reference measurements can be used to detect offset and amplification errors. In case of software malfunctions not general criteria can be laid down not only for expected, but also for erroneous operations. Internal information flow in a software is unidirectional even in case of a malfunction. A software receiving bad or erroneous input data will react with erroneous operation. Consequentially, input data to which the software will react with pre-generated error messages has to be determined. Additionally, coding errors can occur, to which static code analysis software exists; translation errors, which can be analyzed with the debugging method. With respect to software testing, it is important to mention using multiple testing levels, like integration test, system test and user acceptance test.

4. RISK MATRIX

One of the most widely known risk reductions methods is the risk matrix (see Fig. 3.), which is mainly used in identifying unacceptable risks. A risk matrix is a qualitative tool, which can be used to graphically represent the relation between risk frequency and consequence severity (which have been mentioned earlier). This method is highly subjective, as there is no universally accepted approach to either consequence severity, or the frequency. Individual elements of a complex system may appear with different frequencies and consequence

severities, regardless of whether or not they run as components of an integrated system or at the same time.

LIKELIHOOD (probability) How likely is the event to occur at some time in the (Linear Scale time specific matrix)	CONSEQUENCES: What is the Severity of injuries /potential damages / financial impacts (if the risk event actually occurs)? (Logarithmic Scale, property industry specific matrix)				
	Insignificant	Minor	Moderate	Major	Catastrophic
	No Injuries First Aid No Envir Damage << $1,000 Damage	Some First Aid required Low Envir Damage << $10,000 Damage	External Medical Medium Envir Damage <<$100,000 Damage	Extensive Injuries High Envir Damage <<$1,000,000 Damage	Death or Major Injuries Toxic Envir Damage >>$1,000,000 Damage
Almost certain - expected in normal circumstances (100%)	MODERATE RISK	HIGH RISK	HIGH RISK	CRITICAL RISK	CRITICAL RISK
Likely – probably occur in most circumstances (10%)	MODERATE RISK	MODERATE RISK	HIGH RISK	HIGH RISK	CRITICAL RISK
Possible – might occur at some time. (1%)	LOW RISK	MODERATE RISK	HIGH RISK	HIGH RISK	CRITICAL RISK
Unlikely – could occur at some future time (0.1%)	LOW RISK	MODERATE RISK	MODERATE RISK	HIGH RISK	HIGH RISK
Rare - Only in exceptional circumstances 0.01%)	LOW RISK	LOW RISK	MODERATE RISK	MODERATE RISK	HIGH RISK

NOT ACCEPTABLE
TEMPORARY ACCEPTABLE
ACCEPTABLE

Fig. 3 Risk matrix [2]

In the coordinate system defined by the severity of the consequence and the frequency of the event, lines connecting points which belong to the same risk level are called ISO contours. In the coordinate system, ISO contours can be used to discern risk levels. ISO contours projected on a complete matrix display acceptability fields. Using a large numbers of cells in a matrix is best to be avoided, as it tends to hamper consistent scoring. It is usually not advisable to use a scale other than the general unacceptable, partially acceptable and acceptable, again, because it erodes consistency. In case the risk to a critical software or hardware element has been reduced, it may move to the partially acceptable field in a newly made matrix. Movement through the fields must be continuous, so only one field may be passed in a single move. Since the blood leak detector of an acute dialysis device may malfunction in multiple ways, it can have multiple entries on different levels of the risk matrix, the exact position depending on the severity frequency of the malfunction. Thus, the state space of erroneous operation, in which it is possible to realistically model the operation of the blood leak detector has to be covered. Regardless of the necessary measures and processes determined by risk assessment, elements of a blood leak detector may not pass from the unacceptable directly to acceptable. A fundamental rule of the risk matrix is that elements may pass only one field at a time, for example, in the case of the blood leak detector, from unacceptable to partially acceptable.

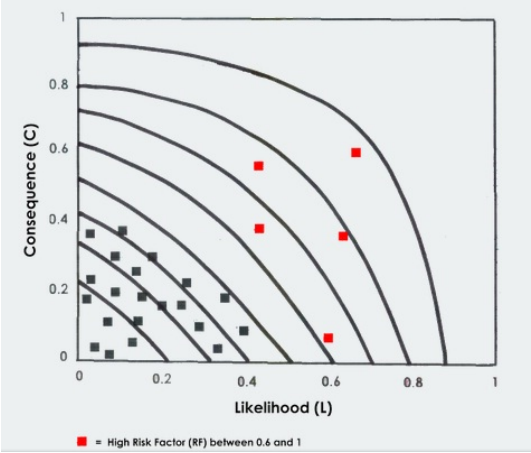

Fig. 4 Risk factors and ISO-contours for a quality process] [3]

The graphical representation of higher likelihoods and consequences is best done on a logarithmic scale, as that way risk contours are one order magnitude easier to interpret [3]. The logarithmic scale is also used to represent units of measurement on a large scale, like in certain physical phenomena (earthquakes) or in human perception (hearing). Similarly, the likelihood and the severity of an event could be best represented on a logarithmic scale.

4.1. Example: Risk management in an acute dialysis device

We have proposed multiple ways to avoid or mitigate software and hardware malfunctions or operator errors, as mentioned in an earlier chapter at risk management. The options all have financial and resource requirements. Education has financial costs, while informative displays on the device requires equipment. Processes to reduce hardware malfunctions do not only require equipment, but also human resources, as trained engineers and calibrated instruments are required to monitor a hardware component. An end user test is of course also necessary before delivery, where real, live operation is tested (for example, through selecting a treatment) comprehensively, to see whether the initial checks and calibration steps are enough to ensure safe operation. This also requires both financial and human resources. Developing a hardware component to be monitored by protection software registers as additional work hours, just like the development of a software-based automated testing process. Additionally, we propose that a device be replaced before it reaches the end of its lifetime. The operation of a server park which supports continuous regressive testing (Jenkins, application server) also demands resources. These conditions (in our case, concerning the blood leak detector) must be accepted by management, development, the test leader and also the user. If an unexpected risk emerges during development or testing (possibly during end user testing), a new risk matrix has to be prepared. Aside from requiring a new matrix, a new risk can add both to work hours and to the budget required for development. Time is also of pivotal importance. The timeframe of developing the product is established before development actually starts during the design phase. An additional error can extend this time and so threatens the deadline for delivery, and my even result in a serious competitive handicap versus similar products of competing companies. Early risk assessment and management are thus very important, even before development, in order to implement

measures which will, in the end, result in the product being better at meeting expectations of quality.

5. CONCLUSIONS

In the present article we have examined the directives for risk management in medical devices with respect to the development process as well as the end product. We can conclude that a risk matrix is a useful tool as long as the risk assessment is done before the development, during the design phase. A risk matrix can be used to reduce the likelihood of malfunction and user to meet demands for safe operation. We have proposed ways to reduce the likelihood of malfunction in the product, testing requirement verification and product utilization. The processes we have described can be adapted to the V-model methodology for the development of medical devices. We have explained the most basic standards and the definitions for related concepts. Hazard and risk have been described. We have used these concepts along with the relevant formulae to examine the creation of a risk matrix for a real product (acute dialysis device blood leak detector). We have found that time and resources allocated to very early, design phase risk assessment and management are proportional to the increase in the expected quality of the product. If, however, a new risk emerges during development or end-user testing, the cost of testing and development is multiplied. Further research is required on ISO contours, which are projected on risk matrices, that is, to find out the general attributes of ISO contours as functions and with which matrices they are usable. Also, further research is required on logarithmic contours. It would be important to know the scale of likelihoods and severities they can be applied to, and to understand how the dependencies of certain ranges influence the properties of the contours.

6. REFERENCES

[1] Jayr Figueiredo de Oliveira, Marcelo Eloy Fernandes , Carlos Roberto Camello Lima, **Information technology management system: an analysis on computational model failures for fleet management,** http://www.scielo.br/scielo.php?pid=S1807-17752013000300577&script=sci_arttext&tlng=es

[2] Risk Management Group Pty Ltd http://www.risk8.com/pentagon/

[3] RISK MANAGEMENT METHODOLOGY FOR QUALITY MANAGEMENT https://www.cognidox.com/2015/06/iso-90012015-how-to-apply-risk-based-thinking-to-quality-processes-part-viii/

[4] Kockázatelemzés alapjai, http://moodle.autolab.uni-pannon.hu/Mecha_tananyag/biztonsagkritikus_rendszerek/ch01.html

[5] Medical device software standard IEC 62304 et al: http://www.chemgineering.com/en/Scientific%20Articles/$/Medical-device-software-standard-IEC-62304-et-al./22

[6] Standards: ISO/IEC 12207:2008. Systems and software engineering -- Software life cycle processes. IEC 62304:2006. Medical device software -- Software life cycle processes. IEC 60601-1 Medical Electrical Equipment Package, 2009. IEC 61508-3 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. ISO 14971:2007. Medical devices -- Application of risk management to medical devices. ISO13485:2003: Medical devices -- Quality management systems -- Requirements for regulatory purposes, IEC 50(191), MIL-ASTD882B:1984, 61508 and 61551 standards .

[7] Sziray J., Majzik I., Benyó B., Pataricza A., Góth J., Kalotai L., Heckenast T., Nagy N.: Szoftver rendszerek minőségbiztosítása és verifikálása. Elektronikus jegyzet, 2000.

[1] [8] Diapact CRRT, BBraun B. Braun Melsungen AG, http://www.bbraun.com/cps/rde/xchg/bbraun-com/hs.xsl/products.html?id=0002074277000000092&prid=PRID00001038