TLC ENGINEERING SOLUTIONS PTY(LTD)

SOLUTIONS SOFTWARE TECHNOLOGY

Safety and Reliability Engineering in Medical Electronic Products - A Case Study

Terry Cousins, TLC Engineering Solutions (Pty) Ltd

Abstract

Medical products must be engineered to an acceptable reliability and safety standard. International standards for medical equipment such as IEC 60601-1-4 have a number of similarities with IEC 61508 in terms of risk management and assessment. This paper will examine a life cycle case study for medical equipment from design to final certification with particular emphasis on the risk analysis of the control software and safety engineering.

Introduction

Medical devices have to comply with regulations and standards of safety that are among the strictest. Medical devices are used on patients who may be unconscious and unable to respond to hazardous conditions or pain. The equipment is often directly connected electrically to the patient and the failure of the equipment when used for life support may lead to the patient's death.

Engineers who are experienced in equipment design may not be familiar with the relevant safety standards and particular risk assessment requirements for medical equipment. A thorough understanding of the specific requirements and standards at the start of the design will increase product safety, reduce product compliance delays in certification and consequently reduce product development costs.

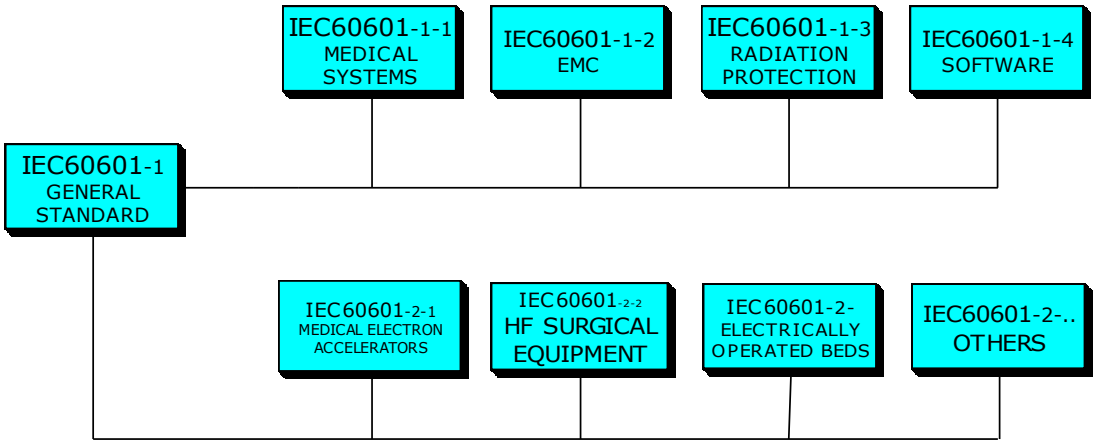
The first part of this paper will examine the applicable safety standards for medical equipment, the design and risk assessment philosophy and the methods for verification, validation and certification of the equipment. The second part will examine the risk assessment of a patient respirator during its design.

PART 1: Medical Equipment Requirements

Applicable Standards

One of the challenges that engineers and regulatory professionals are facing today is the determination of what is considered "medical equipment." Today's complex devices were not anticipated in the late 1980s when the second revision of IEC 60601-1 was published. Further, at that time, the Internet was not developed, and the sharing of diagnostic information and performing operations via the Internet was simply not possible. For this reason, the definition of medical electrical equipment from that time is sometimes interpreted in a much broader way.

The IEC 60601-1 standard, "Medical Electrical Equipment— Part 1: General Requirements for Safety," is the cornerstone document addressing many of the risks associated with electrical medical equipment. The following illustrates the organization of the standard.



In IEC 60601-1:1988 medical electrical equipment is defined as "Electrical equipment provided with not more than one connection to a particular supply mains and intended to diagnose, treat or monitor the patient under medical supervision and which makes physical or electrical contact with the patient and/or transfers energy to or from the patient and/or detects such energy transfer. The equipment includes those accessories as defined by the manufacturer, which are necessary in normal use of the equipment" The general interpretation of the term "particular supply mains" includes internally (battery) powered equipment.

The term "medical supervision" does not mean that a nurse or physician has to be near the patient at all times, but that, in general, a certain degree of supervision is included in the use of the equipment. This can include regular scheduled follow up visits for patients with active implants, or transmission of measurements from a patient to a physician via the Internet.
Based on this definition, a workstation that is placed in a physician's office and which does not come in contact with the patient and is not used in the patient vicinity is not considered to be medical electrical equipment. In cases like this, it may not be necessary to apply the stringent requirements for medical equipment.

The following table lists some of the items that are covered by the IEC60601 standard. For a comprehensive list refer to the standard.

IEC 60601-1 Clause	**Subjects**
1	Scope
2	Definitions
3	General component requirements
6	Identification, marking and documentation
10	Transport and Storage
14	Classification
18	Protective earthing
19	Continuous leakage current
20	Dielectric strength
21	Mechanical Strength
22	Moving Parts
42	Excessive Temperatures
52	Abnormal Operation / Fault Conditions
54	Construction requirements
56	Enclosures and covers
57	Mains parts, components and layout
58	Protective earthing terminals

The underlying philosophy of IEC 60601-1 is that medical equipment must be safe in both normal and single-fault condition

The philosophy in other safety standards, such as IEC 61508 (the standard for functional safety in programmable systems), define a generic approach and a technical framework for dealing systematically with safety related activities. It also provides all the processes to build the understanding of the real needs/expectations in order to meet them. In addition, the standard explicitly addresses the issue of continuous process improvement (as found in the Capability Maturity Model developed by the Software Engineering Institute). This mindset, with the processes for achieving it, is the basis for a total quality in safety-related control systems. And quality is of fundamental importance to safety because it relates to the ability of a system to meet its requirements.

In this respect, IEC 61508 has many common points in terms of quality and process management with other international standards like ISO 9000. For example, the ISO 9000 quality system, defined as "the organizational structure, responsibility, procedures, processes and resources for implementing quality management", is implemented by the IEC 61508 clause which covers the management of functional safety.

The basic principles of quality assurance have as their goal the production of articles that are fit for their intended use. These principles may be stated as follows:

- quality, safety, and effectiveness must be designed and built into the product;
- quality cannot be inspected or tested into the finished product; and,
- each step of the manufacturing process must be controlled to ensure repeatability

Design and Risk Identification Process

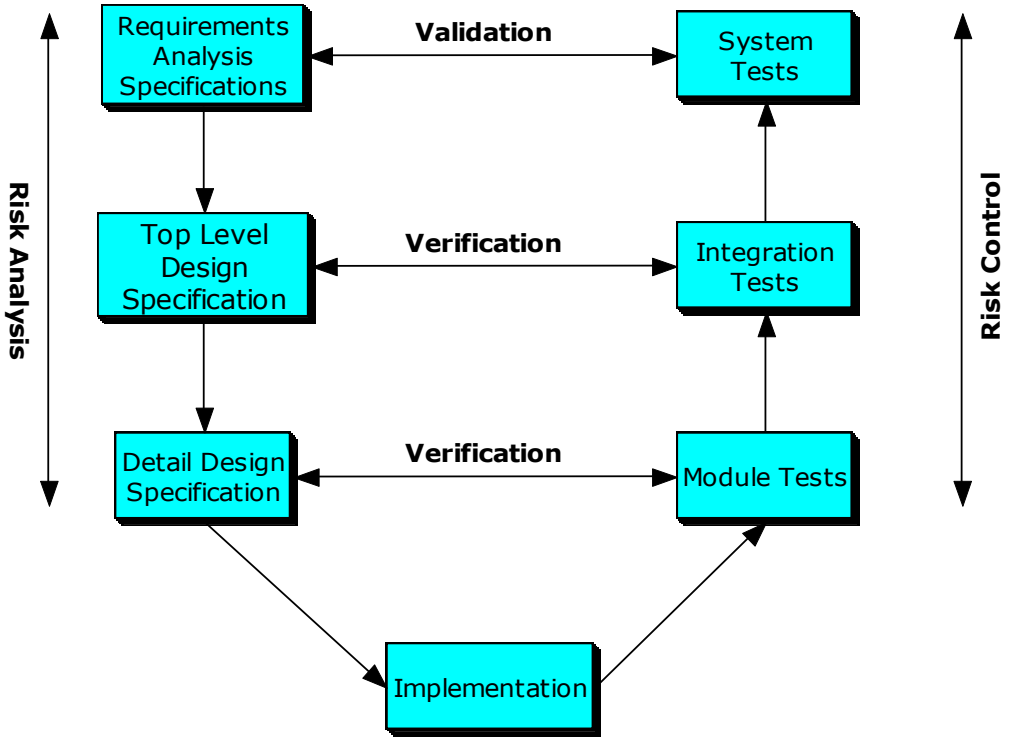
The most important principle of the IEC60601-series is to ensure safety for patients, users and others in normal use and normal condition as well as in a single fault condition. This is specifically important for life supporting and life-sustaining equipment where an interruption could cause a hazard for the patient. Safety of the equipment should be considered part of the overall safety situation, comprised also of the safety of the equipment installation, equipment maintenance and the safety of equipment application. Hazards have to be eliminated as far as reasonably possible, in the following order:

1. Protective precautions incorporated in the design (inherently safe design)
2. Additional protective precautions, such as alarms
3. Restrictions and warnings in instructions and on labels.

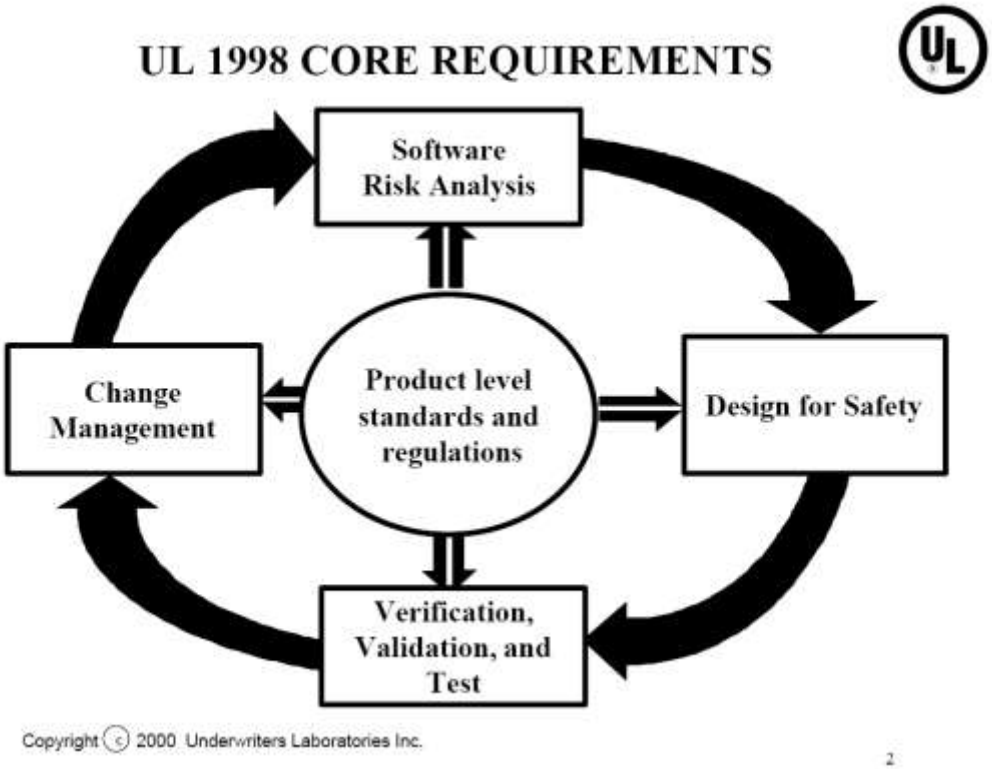
Considerations should also include hazards from electric shock, mechanical failures, unintentional or excessive radiation, excessive temperatures, or abnormal conditions or human error.

Considerations for safety of electrical medical equipment should begin in the early stages of the product creation process. In order to avoid compliance related problems during the product verification and validation phase, applicable requirements need to be identified early and incorporated into the design specifications. As part of this process, aspects related to equipment maintenance and aging of materials should also be addressed. Information can be derived from reliability studies or calculations and, if available, experience with previous products.

The equipment design process should embody a philosophy of risk management at all stages of the design. This is indicated below.



Many medical devices now contain software which requires a "safety" systems mindset during the development. This is also illustrated by the Underwriters Laboratory core requirements.



Designing medical electrical equipment to meet today's complex safety certification requirements can be costly and time consuming for medical device manufacturers. It is essential that these requirements

are considered during the early stages of design. This software development model is similar to the version described in IEC 61508 part 3 which is aimed at operating systems and application software for safety controllers.

Verification and Validation

An essential part of the design process in is to develop test procedures to verify and validate the design.

Verification is the confirmation by examination and testing that specified requirements have been fulfilled. In a software development environment, software verification is confirmation that the output of a particular phase of development meets all of the input requirements for that phase. Software testing is one of several verification activities intended to confirm that the software development output meets its input requirements. Other verification activities could include:

- walk-throughs
- various static and dynamic analyses
- code and document inspections
- module level testing
- integration testing.

Design validation is establishing by testing or other means that device specifications conform with user needs and intended use. Software validation refers to establishing, by acceptance test procedures, that the software conforms with the user needs and intended uses of the device. Software validation is a part of design validation of the finished device. It involves checking for proper operation of the software in its actual or simulated use environment, including integration into the final device where appropriate. Software validation is highly dependent upon comprehensive software testing and other verification tasks previously completed at each stage of the software development life cycle. Planning, verification, traceability, configuration management, and many other aspects of good software engineering are important activities that together help to support a conclusion that software is validated.

The United States Food and Drug Administration (FDA) analysed 3140 medical device recalls between 1992 and 1998 which revealed that 242 of them (7.7%) were attributed to software failures. Of those software related recalls, 192 (or 79%) were caused by software defects that were introduced when changes were made to the software after its initial production and distribution. Validation and other related engineering practices are a principal means of avoiding such defects and resultant recalls.

Verification and validation are difficult because a developer cannot test forever, and it is difficult to judge how much testing is enough. In most cases, validation is a matter of developing a “level of confidence” that the device meets all requirements and user expectations for the functions and features of the device. Measures such as defects found in specifications documents, estimates of defects remaining, testing coverage, and other techniques are all used to develop an acceptable level of confidence before shipping the product. The level of confidence, and therefore the level of software validation, verification, and testing effort needed, will vary depending upon the safety risk (hazard) posed by the automated functions of the device.

Acceptance Testing and Clinical Trials

Once the verification and validation stages have been completed, there will be a high degree of confidence that the equipment is fit for market. Medical equipment has to undergo another set of tests – the clinical trial. This is performed by medical personnel under strict supervision. The test conditions are as would be experienced once the equipment is released to market. These trials are conducted to ensure that there will be no negative impact on the patient should the equipment under trial fail or malfunction. The scope and duration of the trial is determined by the certificating body. Comprehensive records are kept of the performance of the equipment and any problems that the medical operator experienced. On conclusion of the trial the data is analyzed to determine if there are any potential problems that the verification and validation had not identified.

Certification

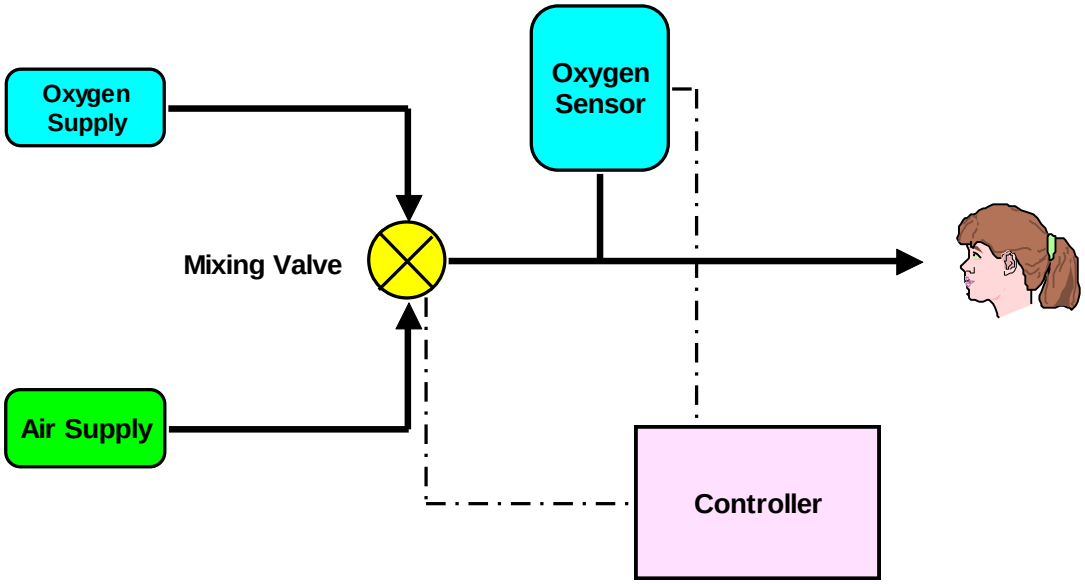
The final step is to provide the certificating body with a document pack. The requirements vary according to its requirements. This would contain detailed data on the design, component specifications, software flowcharts, failure mode analysis, verification and validation test results, clinical trial data and minutes of review meetings.

The origin of the design and manufacture of the medical equipment is not relevant. It is essential that the certification must comply with the regulations of the accrediting body in the country where the equipment is sold. For equipment designed and manufactured in South Africa a CE mark is often required. This may require the services of a European based quality inspector to perform the certification. If the documentation is not to the required standard, the application will be rejected and the exercise becomes very costly to the manufacturer.

Part 2: Case Study – Automatic Oxygen Regulator

Functional Requirements

As way of illustration we will consider the design of the software in a respiratory device which provides an air / oxygen mixture to a patient. The software in this device has to automatically control a blend valve which regulates the mixture to the patient.



PATIENT RESPIRATOR

The basic user requirements for the device are as follows:

- Medical staff to set the required air / oxygen mixture using a front panel control
- Controller to adjust the setpoint to the mixing valve to obtain and maintain the setpoint within a specified tolerance.
- The setpoint and actual mixture values must displayed.
- Audible and visual alarms must be provided for error conditions.

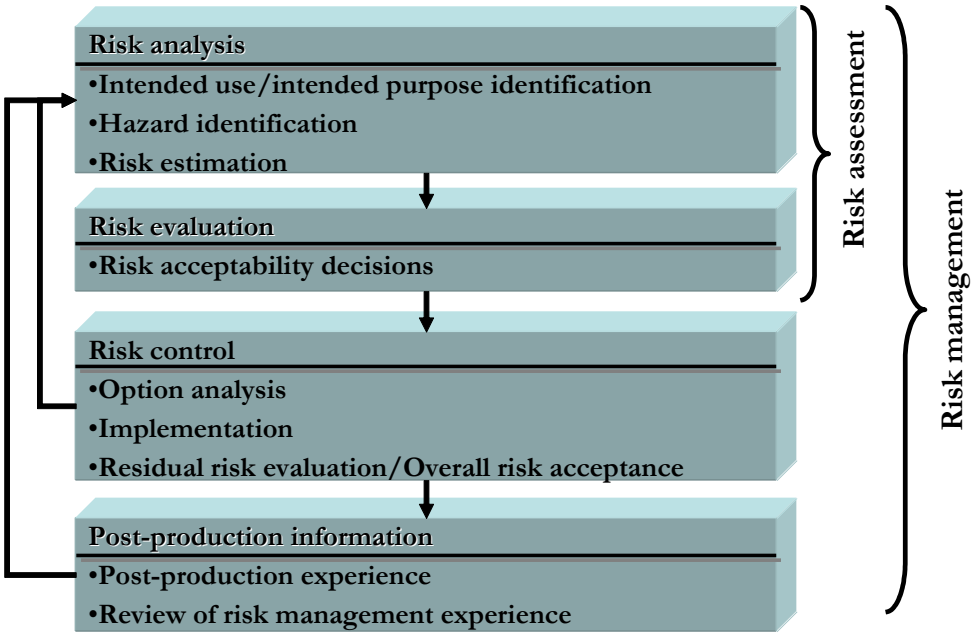
Risk Analysis

The design team must first consider what can go wrong. Basic safety requirements in IEC60101-1 require freedom from unacceptable risk directly caused by hazards when medical equipment is used in normal and single fault condition. It also requires assurance that the absence or degradation of a function would not result in an unacceptable risk.

There are a number of possible single fault conditions that could occur which have to be considered in the design. These include failure or malfunction of:

Oxygen supply
Air supply
Mixing valve
Oxygen sensor
Controller

Risk analysis can be conducted using procedures as described in ISO 14971.



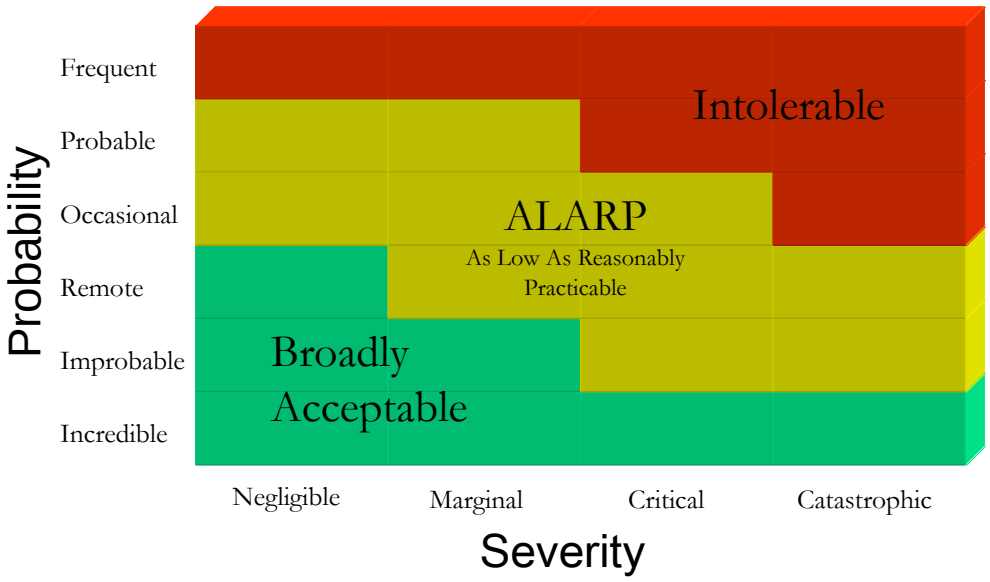
Risk analysis is performed by identifying hazards and estimating their associated probability and severity. A common technique that is used is the failure mode and effects analysis (FMEA). An example is shown below (this is not comprehensive and is used for illustration only).

FUNCTION	POTENTIAL EFFECT (S) OF FAILURE	SEVERITY	CLASS	OCCUR
Oxygen valve control	Failed in arbitrary open position - System shutdown and alarm	9	YC	3
Air valve control	Failed in arbitrary open position - System shutdown and alarm	9	YC	3
User display	No display	1	NC	3
Mains supply	Power checked by external circuit. Failure results in an alarm. Shutdown after 10 mins.	9	YS	3
Keyboard	Cannot mute alarms or/and Cannot input new setpoint or/and Cannot place in standby	5	NC	3
Oxygen sensor	System shut down	9	YC	5

The above table summarises the functions, potential effects of any failure, the severity to the system, failure class and likelihood of occurrence. The failure severity is a number from 1 to 10, with 1 indicating the failure is will have no impact and 10 indicating a hazardous condition which can occur without warning. The failure class code indicates a critical failure (YC), potentially critical (YS) or non-critical (NC). The final column indicates the frequency of occurrence. This is scored on a scale of 0 to 10 with 10 indicating continuous occurrence and 0 indicating no occurrence.

Design Controls

The equipment designer must now identify those conditions that would result in an intolerable or unacceptable situation and then apply design controls to reduce the impact of the hazard to an acceptable risk. ISO 14971 provides a framework to perform this analysis. The table below indicates go / no go areas based on the frequency of occurrence (probability) and the severity This is an example and is used for illustration purposes only. This analysis is similar to the SIL assignments in IEC 61508.



The design team can now plan to implement design controls to reduce those risks that fall into the red or amber zones into the green zone.

The following table has been constructed for patient respirator. (Values used for illustration purposes only)

FUNCTION	CONTROLS	RPN	INDEX AFTER CONTROLS			
			SEV	OCC	DET	RPN
Oxygen valve control	Compare oxygen content from sensor with valve setpoint	27	9	3	0	0
Air valve control	Compare air content from sensor with valve setpoint	27	9	3	0	0
User display	User test	3	1	3	0	0
Power supply	Independent voltage monitor with alarm	27	9	2	0	0
Keyboard	User test	15	5	3	0	0
Oxygen sensor	Calibration test	18	9	2	0	0

The detection (DET) column indicates to what degree we can detect the failure or fault condition after a control has been implemented. A value of 0 indicated 100% detection while 10 indicates unable to detect. The control that is put in place must reduce the probability of occurrence (through service, component inspection etc) or the detection (using user tests, calibration etc). It is very difficult to provide 100% detection using software on its own. By implementing multiple controls, such as a combination of hardware, software and user controls, it is possible to get close to 100% detection.

Unacceptably high values in the risk priority number (RPN) column (severity x occurrence x detection) before the control must be reduced after the control is introduced. Once these values are in place the design can be implemented, verified and validated.

Conclusion

Risk assessment is an essential requirement for both regulatory requirements and for marketing confidence. This process can be time consuming and resource intensive but with due care it is possible to minimise the risk of injury, product recall and potential litigation by customers. The additional cost spent in the design process will be significantly less that correcting for failures in the field.

The risk assessment process should not be performed in isolation. The analysis should be an integral part of the product design methodology. The equipment manufacturer should take advantage of whatever new and better techniques become available to perform this type of analysis.

It is extremely difficult to quantity the likelihood of every failure, but by implementing simple and practical control measures the risk can be reduced to acceptable levels. Once the risks have been quantified and controls put in place to reduce these to an acceptable level, then good design and engineering practice, coupled with a quality system, will ensure the delivery of reliable equipment that is safe to use.

References

European, Canadian And United States Product Safety Standards For Electrical Medical Equipment, Heinz Joerg Steneberg TUV Rheinland of North America, Inc. CONFORMITY®: AUGUST 2003

IEC 60601-1, "Medical Electrical Equipment—Part 1: General Requirements for Safety" (Geneva: International Electrotechnical Commission, 1988).

IEC 60601-1-1, Medical electrical equipment - Part 1-1: General requirements for safety - Collateral standard: Safety requirements for medical electrical systems (Geneva: International Electrotechnical Commission, 2000)

IEC 60601-1-2, Medical electrical equipment - Part 1-2: General requirements for safety - Collateral standard: Electromagnetic compatibility - Requirements and tests (Geneva: International Electrotechnical Commission, 1993)

IEC 60601-1-3, Medical electrical equipment - Part 1: General requirements for safety - 3. Collateral standard: General requirements for radiation protection in diagnostic X-ray equipment (Geneva: International Electrotechnical Commission, 1994)

IEC 60601-1-4, Medical electrical equipment - Part 1-4: General requirements for safety - Collateral Standard: Programmable electrical medical systems (Geneva: International Electrotechnical Commission, 1996)

IEC 60601-2-7, Medical electrical equipment - Part 2-7: Particular requirements for the safety of high-voltage generators of diagnostic X-ray generators (Geneva: International Electrotechnical Commission, 1998)

IEC 60601-2-28, Medical electrical equipment - Part 2: Particular requirements for the safety of X-ray source assemblies and X-ray tube assemblies for medical diagnosis (Geneva: International Electrotechnical Commission, 1993)

IEC 60601-2-32, Medical electrical equipment - Part 2: Particular requirements for the safety of associated equipment of X-ray equipment (Geneva: International Electrotechnical Commission, 1994)

EN 60601-1, “Medical Electrical Equipment—Part 1: General Requirements for Safety” (Brussels: European Committee for Electrotechnical Standardization, 1988).

CSA C22.2 NO 601.1-M90 Medical Electrical Equipment - Part 1: General Requirements for Safety (Canadian Standards Association, 1990)

UL 2601-1, “Medical Electric Equipment, Part 1: General Requirements” (Northbrook, IL: Underwriters Laboratories, 1997).

ISO 14971, “Medical Devices—Application of Risk Management to Medical Devices” (Geneva: International Organization for Standardization, 2000).

United States Code of Federal Regulations (Title 21, Subchapter J) Recognition and Use of Consensus Standards; Final Guidance for Industry and FDA Staff (June 20, 2001) Directive 93/42/EEC – Medical Device Directive

GUIDELINE ON GENERAL PRINCIPLES OF PROCESS VALIDATION May 1987
Prepared by: Center for Drugs and Biologics and Center for Devices and Radiological Health
Food and Drug Administration Maintained by: Division of Manufacturing and Product Quality (HFN-320)

General Principles of Software Validation; Final Guidance for Industry and FDA Staff U.S. Department Of Health and Human Services Food and Drug Administration Center for Devices and Radiological Health Center for Biologics Evaluation and Research

10th Annual AAMI/FDA International Conference on Medical Device Standards and Regulations March 16, 2000