RISK ASSESSMENT OF THE CHOPPER DIPOLE KICKER MAGNETS FOR THE MEDAUSTRON FACILITY

T. Kramer, T. Stadlbauer (EBG MedAustron, Wr. Neustadt),
M.J. Barnes, M. Benedikt, T. Fowler (CERN, Geneva)

Abstract

The MedAustron facility, to be built in Wiener Neustadt (Austria), will provide protons and ions for both cancer therapy and research [1]. Different types of kicker magnets will be used in the accelerator complex, including fast beam chopper dipoles: these allow the beam to be switched on and off for routine operational reasons or in case of emergency. Main requirements for the beam chopper system are safety and reliability. A criticality analysis, to chart the probability of failure modes against the severity of their consequences of the fault, has been carried out for the chopper dipole system. This “Failure Mode, Effects, and Criticality Analysis” (FMECA), has been used to highlight failure modes with relatively high probability and severity of consequences: conservative ratings of critical components and appropriate redundancy, together with measurements and interlocks, have been used to reduce the probability and criticality of faults. This paper gives an overview of the Risk Assessment approach and presents results of the FMECA.

INTRODUCTION

The MedAustron accelerator complex is intended to be used for medical purposes. Thus the requirements for medical devices are to be carefully evaluated. MedAustron envisages constructing the particle accelerator as an “in house product”, hence no commercial availability of the design is planned. MedAustron intends to deliver a state of the art facility: in order to guarantee the highest levels of safety, reliability and availability a Risk Management process has to be established. MedAustron will introduce a Risk Management process following the ISO14971 standard on “application of risk management to medical devices” [2]. The High Energy Beam Transfer (HEBT) beam chopper will be a safety relevant system under direct control of the beam delivery system (BDS). It basically consists of four chopper dipoles (MKC), a dump block, a power converter (PKC) and its controls interface. This paper focuses mainly on the Risk Assessment process carried out for the magnets, but the power converter is briefly discussed as well.

The Principle

All treatment rooms will be able to switch the beam on and off routinely during operation by means of the beam chopper. When the chopper is on it creates a closed-orbit bump that bypasses the dump block, mounted inside the vacuum chamber (Fig. 1). When the chopper is off the beam is stopped by the dump block. The four chopper dipoles are connected electrically in series and fed by a common power supply. Since the four dipoles are located in a common HEBT-section, the bump is “perfectly” closed and the downstream trajectory of the beam is unaffected. Hence the stability and over-shoot of the power supply are not critical issues.

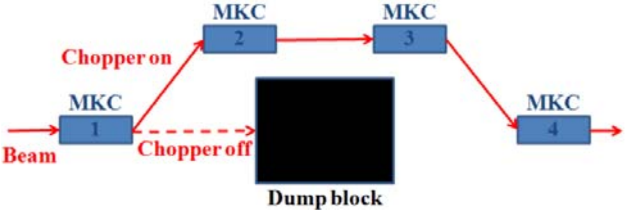


Figure 1: Schematic of the HEBT beam chopper.

The Chopper Dipoles (MKC)

The MKC dipoles have a window frame construction with two water cooled saddle shaped coils (Fig. 2). Each magnet will be housed in a box whose sides, top and bottom are made out of aluminium. End-plates, which act as field clamps, are 12 mm thick and made out of 1 mm thick steel laminations. The MKC requires a maximum current of 630 A. The specified current rise and fall time of the dipoles will allow for operation with a minimum ramp time of 90 µs (2% to 98%), however the baseline for the ramp time is 250 µs due to constraints in the power converter. An important requirement is that a turn off command can be executed at any time even during the ramp up. In this case the ramp down time will be less than the specified fall time. The current flat top can be from 0 s to DC. The design of the MKC has been optimized to achieve a uniformity of the integrated field of better than ±0.2% over an area of 45 mm x 45 mm. The predicted inductance, derived from 3D simulations, is 85 µH per dipole. This permits a fast rise/fall time with a maximum voltage of 3.5 kV per four series dipole magnets.

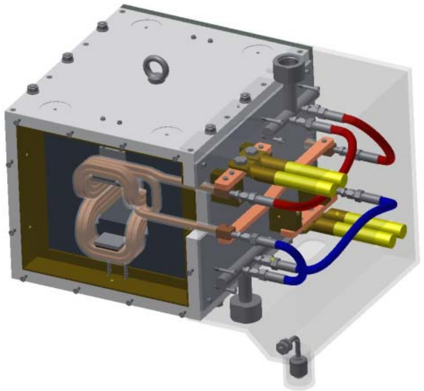


Figure 2: MKC 3D design model (end-plate removed).

Definition of the Risk Assessment Process

As part of the risk management process the MKC system has to undergo a risk assessment procedure. The risk management process has to be maintained throughout the lifecycle and must commence in the design phase. This study uses the term “Risk Assessment” for the discussed process. However this term is only mentioned once in the ISO14971 standard as the definition for an “overall process comprising a risk analysis and a risk evaluation”. The ISO31000 standard [3] gives the definition of Risk Assessment as an “overall process of risk identification, risk analysis and risk evaluation” which is deemed to fit the MedAustron needs in a better way.

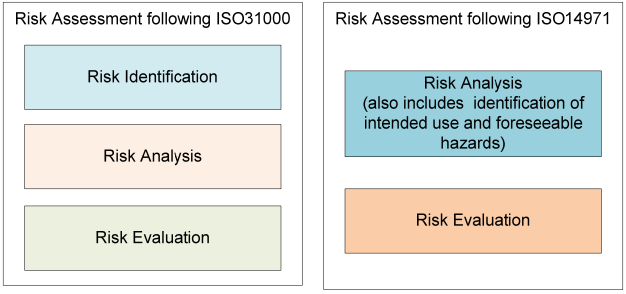

Risk Assessment following ISO31000
Risk Identification
Risk Analysis
Risk Evaluation
Risk Assessment following ISO14971
Risk Analysis
(also includes identification of intended use and foreseeable hazards)
Risk Evaluation

Figure 3: Definition of Risk Assessment outline.

The process introduced below aims to conduct a Risk Assessment on a system level in order to identify the main system risks at an early stage and thus to be able to incorporate provisions in the system design to compensate for potential failures. Furthermore the tendering specifications for subsequent Risk Assessment needs (e.g. on a component level) and control interfaces as well as for certain risk reduction measures will be derived from the process results.

METHODOLOGY OF THE RISK ASSESSMENT

The Risk Assessment process was started on a general level with the identification of the intended use. For the MKC system two main branches have been identified:

- the magnets;
- the power converter with the controls interface.

Hence it was decided to split – where applicable - the assessment into these parts. Several assessment techniques have been evaluated. As an outcome a combination of creative and structured techniques was introduced. The identification of the intended use was the first step followed by a brainstorming session combined with an Ishikawa analysis for risk identification. As a main assessment technique a Failure Mode Effect and Criticality Analysis (FMECA) was selected. This FMECA analysis was combined with a “Risk Matrix” for the final risk evaluation. All used methods are summarized in [4] (Table A.1) where one can readily see the overlap of the strength of the individual techniques in “Risk Identification”, “Risk Analysis” and “Risk Evaluation”. Therefore the developed process chain redundantly covers these areas. The process allows for feedback (also from reviewers outside the assessment groups) and entry of new items at any stage.

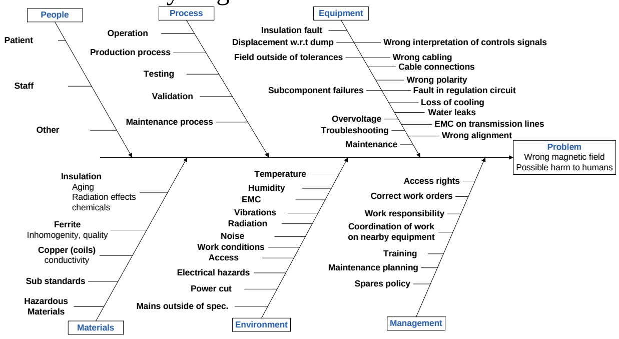


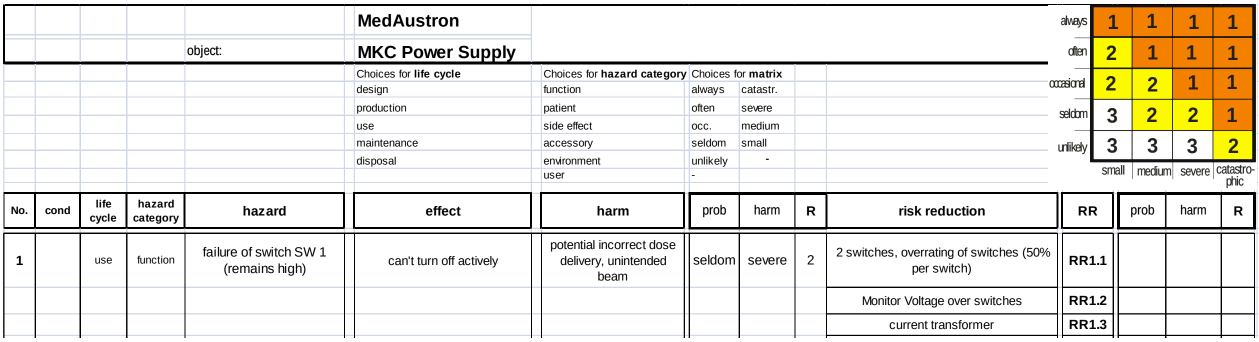
Figure 4: Ishikawa diagram (simplified).

RESULTS

Intended Use

The intended use of the MKC system is to ensure, by fail safe design, that no unintended beam is delivered to the patient and to switch off the beam in emergency situations as well as for clinical and operational reasons:

- Primary use: Start/Stop/Emergency-stop during continuous beam delivery to patient or experiment;
- Secondary use: Start/Stop/Emergency-stop during beam delivery with respiratory gating;
- Tertiary use: Possible beam chopper (few Hz) for experiments or machine development.



MedAustron

object: MKC Power Supply

Choices for **life cycle**	Choices for **hazard category**	Choices for **matrix**	
design	function	always	catastr.
production	patient	often	severe
use	side effect	occ.	medium
maintenance	accessory	seldom	small
disposal	environment	unlikely	-
	user	-	

always	1	1	1	1
often	2	1	1	1
occasional	2	2	1	1
seldom	3	2	2	1
unlikely	3	3	3	2
	small	medium	severe	catastro-phic

No.	cond	life cycle	hazard category	hazard	effect	harm	prob	harm	R	risk reduction	RR	prob	harm	R
1		use	function	failure of switch SW 1 (remains high)	can't turn off actively	potential incorrect dose delivery, unintended beam	seldom	severe	2	2 switches, overrating of switches (50% per switch)	RR1.1			
										Monitor Voltage over switches	RR1.2			
										current transformer	RR1.3			

Figure 5: Simplified example of a FMECA analysis sheet with an integrated risk matrix.

Ishikawa Analysis

An Ishikawa diagram is used to display and structure the brainstorming outcome. The brainstorming sessions have been arranged in 1 hour units to guarantee excellent concentration and to be able to prepare and properly document each meeting. Small groups were formed out of relevant experts according to the concerned fields. Each session was documented and briefly reviewed in the subsequent meeting. Fig. 4 shows an example of a preliminary outcome for one such session (simplified: sub-causes are not displayed).

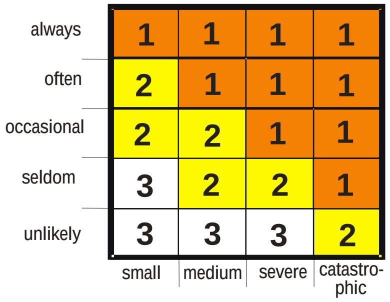
FMECA

The used FMECA concept is closely interfaced with a Risk Matrix. This improved concept was developed together with the Graz Institute of Health Care Engineering (TU-Graz) [5]. Fig. 5 shows the FMECA sheet with one example for the PKC. Each identified risk is categorised concerning fault type, considered life cycle phase and hazard category. The potential hazard effect and harm is discussed during the individual session: the probability of its occurrence and the severity of the harm are assessed which finally yield the position in the risk matrix.

Possible risk reduction measures are evaluated and new probabilities for occurrence and severities of harm are judged. Each risk reduction measure is evaluated concerning the impact on the complete system and possible risks arising from the risk reduction itself.

Risk Matrix

Fig. 6 shows the used 4×5 Risk Matrix in detail: the orange area "1" has highest priority for risk reduction measures and represents risks which are not acceptable at all.



always	1	1	1	1
often	2	1	1	1
occasional	2	2	1	1
seldom	3	2	2	1
unlikely	3	3	3	2
	small	medium	severe	catastro-phic

Figure 6: Used Risk Matrix.

Yellow marked fields ("2") comprise risks which have to be evaluated concerning further risk reduction or, under some circumstances, if the state of the art does not allow for further risk reduction, have to be evaluated concerning their individual risk acceptance. This will be carried out by a Risk/Benefit Analysis and is not part of this study. Fields marked with "3" represent an area of acceptable risks. Nevertheless the ALARP principle (As Low As Reasonably Practicable) applies also for this area and thus risk reduction measures have to be applied where reasonable. The individual residual risks might appear as fairly acceptable however the sum of all residual risks has to be analysed concerning interaction and common mode issues. This is especially important as FMECA studies are mostly suitable for single failure modes.

Example of an Assessment Output

Brainstorming sessions identified the potential hazard of semiconductor failures in the conceptual design of the PKC power stage. A FMECA analysis revealed a hazard for switch SW1 (Fig. 7) that could remain in an on-state with the effect that only "passive turn off" (i.e. non commutated turn-off) would be available and thus some milliseconds of unintended beam passage could lead to patient harm which was rated as "severe" with "seldom" occurrence. Thus only a risk matrix level "2" is achieved with the conceptual design. Possible risk reduction measures have been identified; e.g. two switches in series, each overrated by at least 100%, and voltage and current monitors connected to a fast trigger line to the synchrotron dump system. Redundant and overrated switches would reduce the occurrence and thus yield a new reduced risk matrix level "3".

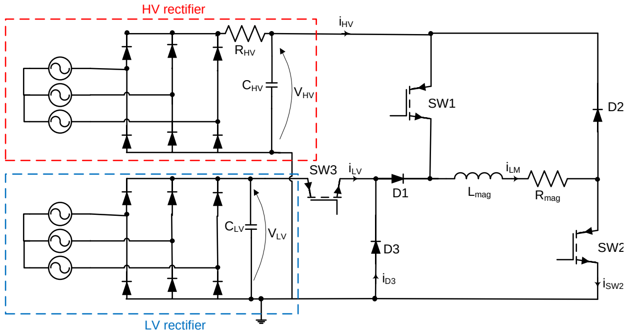


Figure 7: Power stage of the PKC.

CONCLUSIONS

A risk assessment process following the guidelines of ISO 14971 & 31000 has been introduced for the MKC-system. FMECA and Ishikawa analyses yielded initial valuable results for improvement of the conceptual design and specific tendering specification requirements. The process developed will be applied in more detail to all PKC subsystems and interfaces. The harmonization with, and the embedment in, an overall enterprise-wide risk and quality management process is envisaged. An external audit of the process is intended in the future.

REFERENCES

[1] M. Benedikt, A. Wrulich, MedAustron - Project overview and status, Eur. Phys. J. Plus, 2011 126: 69.
[2] ISO 14971 Medical devices –Application of risk management to medical devices, ISO, Geneva, 2007.
[3] ISO 31000 Risk management – Principles and guidelines on implementation, ISO, Geneva, 2009.
[4] ISO 31010 Risk management – Risk assessment techniques, ISO, Geneva, 2009.
[5] Risikomanagement Akte, Minutes of RM meeting, MedAustron, Wr. Neustadt, 2010.