Award project full title: **Dual cobot system for safe motion therapy**

Award project Acronym: **DOROTHY**

Award Agreement - Realistic Trial ID no.: **RRD7218.02.03**

Deliverable no.: **D1.1**

Title: **Risk assessment document of a dual cobot rehabilitation system**

Contractual Date of Delivery	Project Month 4 - August 13, 2020
Actual Date of Delivery	Project Month 5 – September 13, 2020
Organisation Short Name of Deliverable Leading Partner	DARPAMotion Ltd.
Organisation Short Name of Other Participants	BME
Authors	Hong Son Chu, Milan Lovasi, Kata Szakal, Mark Otto Bauer, Andras Toth, Gyorgy Herke
Editors	Tamas Pilissy, Andras Toth
External Review	
Version	1
WPs contributing to this deliverable	WP1
Dissemination Level (*)	PU
Total number of pages (including cover page)	**51**

(*) Dissemination Level

PU Public

PP Restricted to other programme participants (including the Commission Services)

RE Restricted to a group specified by the consortium (including the Commission Services)

CO Confidential, only for members of the consortium (including the Commission Services)

Award Project Abstract

The DOROTHY proposers accumulated knowledge on how to tackle the issues of design for safety throughout the incremental design, development, and testing process of the REHAROB Therapeutic System in the last two decades. Just as we did with REHAROB, other developers of healthcare robots including rehabilitation robots had to adhere to a number intertwining laws and standards: the MDD, the MDR, the ISO13485, the IEC60601, the internal rules and guidebooks of the Notified Bodies, and the same documents of the Test Organisations. Making a product out of an idea was a real nightmare.

The members of the DOROTHY consortium discontinue to revise the REHAROB Therapeutic System on industrial robot basis by changing the existing ABB IRB140 and ABB IRB 1600 force-controlled industrial robots to open control cobots of Universal Robots: UR5e and UR10e. The UR10e via a two robotic finger hand module will move the hand while the UR5e will move the elbow.

According to the IEC 80601-2-78:2019 standard for the basic safety and essential performance of medical robots for rehabilitation, assessment, compensation or alleviation (RACA) the REHAROB 2.0 rehabilitation robot is classified as “arm type RACA robot for upper extremities”. With the help of the COVR Award the DOROTHY project will introduce the RACA standard into the re-design of the REHAROB 2.0 rehabilitation robot. The Awards will also investigate if the use of cobots already certified according to ISO/TS 15066 in a RACA cobot system brings a technical or time advantage over a genuine design. The risk assessment document of using the RACA standard in the design for and assessment of the safety of a concrete rehabilitation robot under development will be the outcome of the Award work in the period until Milestone 1.

In the second part of the DOROTHY Award project a test method to assess the safety performance of the RACA rehabilitation robot will be developed in alliance with the COVR core team. Candidate functions to test are the shared control and the situation awareness subsystems (e.g. work is ongoing on full upper extremity anatomical and kinematical parameter identification purely from the data received from the two cobots, i.e. without using any external sensor system). This outcome can lead to a COVR best practice case study for risk assessment of rehabilitation robots including the recommendations on PLs and SILs.

Table of Contents

AWARD PROJECT ABSTRACT **2**
TABLE OF CONTENTS **3**
LIST OF ACRONYMS **5**
EXECUTIVE SUMMARY **6**
1 SCOPE **7**
2 INTRODUCTION TO THE OPERATION OF REHAROB **7**
3 DEFININITION **7**
3.1 TERMS AND DEFINITIONS: 7
3.2 TYPE OF HAZARDS: 8
4 PRINCIPLES **9**
4.1 PROBABILITY OF OCCURRENCE OF HARM 10
4.2 SEVERITY 11
4.3 RISK EVULATION MATRIX 11
5 RISK ANALYSIS **12**
5.1 RISK ANALYSIS PROCESS 12
5.2 INTENDED USE AND IDENTIFICATION OF CHARACTERISTICS RELATED TO SAFETY OF THE MEDICAL DEVICES 13
5.3 IDENTIFICATION OF HAZARDS AND HAZARDOUS SITUATIONS 18
5.4 ESTIMATION OF RISKS OF EACH HAZARD 21
6 RISK EVULATION **27**
7 RISK CONTROL **27**
7.1 RISK CONTROL MEASURES 27
7.2 RISK CONTROL OPTION ANALYSIS 27
7.3 RESIDUAL RISK EVULATION 35
7.4 RISK/BENEFIT ANALYSIS 40
7.5 RISKS ARISING FROM RISK CONTROL MEASURES 41
7.6 COMPLETION OF RISK CONTROL 41
8 EVALUATION OF OVERALL RESIDUAL RISK ACCEPTABILITY **41**
9 RISK MANAGEMENT REPORT **41**
10 SOURCES **41**
ATTACHMENT - RISK MANAGEMENT PLAN **42**
11 INTRODUCTION **43**
12 DESCRIPTION AND CHARACTERISTIC OF MEDICAL ELECTRONIC EQUIPMENT (ME EQUIPEMENT) **43**
13 DEFINITION OF PEOPLE AND RESPONSIBILITIES **44**
14 CRITERIA TO ANALYZE AND EVALUTE THE ACCEPTABILITY OF RISK **44**

14.1 SEVERITY OF HARM 44
14.2 PROBABILITY OF HARM 45
14.3 CRITERIA FOR THE ACCEPTABILITY OF RISKS 45
15 CONTROLLING OF THE RISK 46

List of acronyms

The following abbreviations are used in this report:

DMRF: DarpaMotion Robot Fingers

Cobot: Collaborative robot

Executive Summary

This document presents the risk assessment process of a dual cobot based motion therapy system according to ISO 24971:2020 by applying it to the the REHAROB 3.0 motion therapy system.

The document goes through the steps of risk analysis (Intended use and identification of characteristics related to safety and the identification of hazards and hazardous situations and the estimation of their risks) and of risk control measures to be in accordance with the current standards of ISO 24971:2020 and ISO 14971, respectively.

The Annex contains the Risk Management Plan to give a complete picture about the risk assessment process.

1 Scope

This document was prepared using REHAROB 3.0. The process of risk analysis can be properly followed, repeated and validated.
The purpose of the risk analysis completed here is:

- Intended use and identification of characteristics related to the safety of the medical equipment
- Identification of hazards
- Estimation of the risk for each hazardous situation

2 Introduction to the Operation of REHAROB

The structure, function and operating principle of the structure can be found in the User's Manual.

3 Defininition

3.1 Terms and Definitions:

Terms	Definition
Harm	Injury or damage to the health of people, or damage to property or the environment Source: (1) definition 3.3
Hazard	Potential source of harm. Source: (1) definition 3.4
Hazardous Situation	circumstance in which people, property or the environment is/are exposed to one or more hazard(s). Source: (1) definition 3.5
Residual Risk	Risk remaining after risk control measures have been implemented. Source: (1) definition 3.17
Risk	Combination of the probability of occurrence of harm and the severity of that harm. Source: (1) definition 3.18
Risk Analysis	Systematic use of available information to identify hazards and to estimate the risk. Source: (1) definition 3.19
Risk Assessment	Overall process comprising a risk analysis and a risk evaluation. Source: (1) definition 3.20
Risk Control	Process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels. Source: (1) definition 3.21

Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the acceptability of the risk. Source: (1) definition 3.23
Risk Management	Systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling and monitoring risk. Source: (1) definition 3.24
Risk Management File	Set of records and other documents that are produced by risk management. Source: (1) definition 3.25
Safety	Freedom from unacceptable risk. Source: (1) definition 3.26
Severity	Measure of the possible consequences of a hazard. Source: (1) definition 3.27

Table 1. Terms and Definition based on EN ISO 14971:2019

3.2 Type of hazards:

Types	Example
Biological hazards	These include bio-contamination, bio-incompatibility, allergenicity, re-and/or cross-infection, inability to maintain hygienic safety.
Environmental hazards	These include electromagnetic fields, susceptibility to electromagnetic interface, emissions of electromagnetic interference, inadequate supply of power, inadequate supply of coolant, storage or operation outside prescribed environmental conditions, incompatibility with other devices with which it is intended to be use, accidental mechanical damage, contamination due to waste products and/ or medical device disposal.
Physical & Mechanical hazards	Hazards arising from functional failure, maintenance and ageing and contributory factors. These include erroneous data transfer, lack of, or inadequate specification for maintenance including inadequate specification of post-maintenance functional checks, inadequate maintenance, lack of adequate determination of the end of life of the medical device, loss of electrical/ mechanical integrity, inadequate packaging (contamination and/ or deterioration of the medical device), re-use and/ or improper re-use, deterioration in function (e.g. gradual occlusion of fluids/ gas path, or change in resistance to flow, electrical conductivity) as a result of repeated use.
Others	Hazards resulting from incorrect output of energy and substances. These include electricity, radiation, volume, pressure, supply of medical gases, and supply of anesthetic agents. Hazards related to the use of the medical device and contributory factors. These include inadequate labeling, use by unskilled/ untrained personnel, sharp edges or points etc. Energy hazards. These include electricity, heat, mechanical force, vibration, magnetic fields etc.

	Hazards due to inappropriate, inadequate or over-complicated user interface (man/ machine communication). These include mistakes and judgment errors, complex or confusing control system, ambiguous or unclear device state, insufficient visibility, audibility or tactility etc.

4 Principles

The risk management process will be conducted following the Standard ISO 14971:2019 clause 4.1, in figure 1 as below:

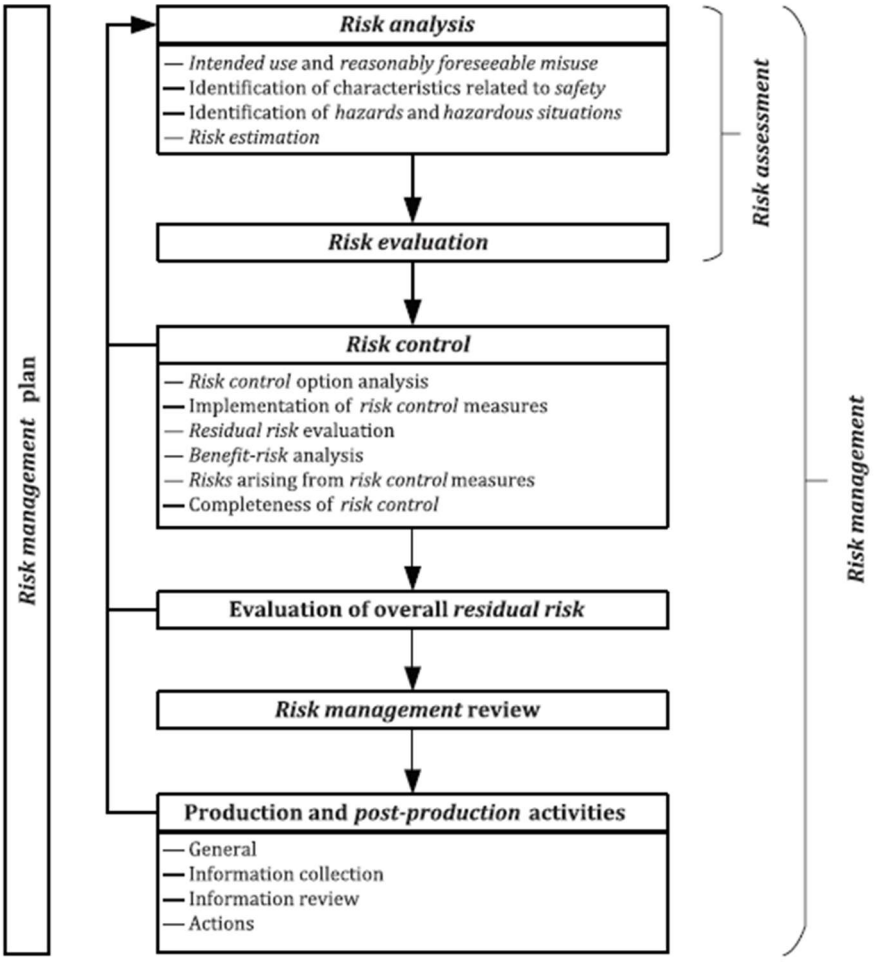


Figure 1. A schematic representation of the risk management process

The magnitude of the risk is given by the probability of occurrence of the threat factor (frequency) and the extent of the caused damage (severity). The information required

for risk analysis consists of the assessment of threats and vulnerabilities and the examination of the prevalence of impacts.

This risk analysis document:

⇒ lists all foreseeable potential (potential) threats,

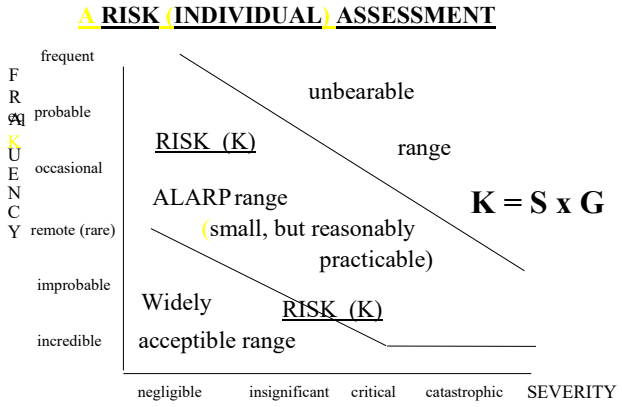
⇒ estimates the severity (**S**) and frequency (**G**) of each potential hazard and then determines the degree of risk as a function of these (**K** = **S** x **G**),

⇒ takes risk mitigation measures where appropriate; and

⇒ assesses the degree of risk before and after the introduction of the measure.

Severity, frequency, risk:

The relationship between the three concepts (graphically) is illustrated in the figure below:



The degree of risk (**K**) is determined by the product of severity (**S**) and frequency (**G**):

$$K = S \times G$$

4.1 Probability of occurrence of harm

The frequency (G) can be estimated from the following table (the rightmost column shows the number of malfunctions, accidents and injuries estimated during 100,000 applications):

Frequency of Occurrence (G)		***Rate***	***Estimation***
Improbable	Although the error may in principle occur, it is highly improbable. The construction is similar as before when no such error was reported.	**1**	$P < 10^{-6}$
Remote (rare)	The construction is similar as before when such error was rarely reported.	**2**	$10^{-6} \leq P < 10^{-5}$
Occasional	The construction is similar as before when such error was occasionally reported.	**3**	$10^{-5} \leq P < 10^{-4}$

Probable	The construction is usually similar to one that has caused difficulties again in the past.	**4**	$10^{-4} \leq P < 10^{-3}$
Frequent	There is almost certainly a significant number of errors	**5**	$P \geq 10^{-3}$

Table 2: Probability of occurrence of harm (per use)

4.2 Severity

Estimation and determination of Severity (S):

	Consequences for the patient, therapist or third party	***Rank***
Negligible	No risk of injury. The user does not even notice the possible error. „Background function" (eg self-test) may be damaged.	**1**
Minor	Slight customer inconvenience; little to no effect on product performance, non-vital fault	**2**
Serious	Short-term injury or impairment requiring additional medical intervention to correct (e.g. reoperation). Moderate defects, e.g. loss of some sub-functions.	**3**
Critical	Severe, long-term injury; potential disability. A serious fault that can cause a complete malfunction.	**4**
Catastrophic	Results in death or life-threatening injury	**5**

4.3 Risk evulation matrix

From the **G** and **S** values – analogous to the figure – for the degree of risk (**K**) the following overview table can be compiled:

Rate of Frequency, **G**		***Rate of Severity,*** **S**				
		Negligible	***Minor***	***Serious***	***Critical***	***Catastrophic***
		1	**2**	**3**	**4**	**5**
frequent	**5**	**5**	**10**	**15**	**20**	**25**
probable	**4**	**4**	**8**	**12**	**16**	**20**
occasional	**3**	**3**	**6**	**9**	**12**	**15**
remote (rare)	**2**	**2**	**4**	**6**	**8**	**10**
improbable	**1**	**1**	**2**	**3**	**4**	**5**

The evaluation matrix above is used for evaluating risks with reference to ISO 24971.

The evaluation and classification of the resulting **K** risk is summarized in the following table:

Low	**0-4**	Widely accepted risk. It does not pose a danger to the patient, the operator or the equipment.
Medium	**5-14**	***ALARP (As Low As Reasonably Practicable) range with just "tolerated" risk (small but still reasonably practicable*).** Further measures can reduce the risk to a more acceptable level.
High	**15-25**	***UNBEARABLE RISK*.** Fatal risk, appropriate measures must be taken to avoid hazards.

A possible risk control measure may reduce the severity (**S**) of the event, either the frequency or occurrence of the event or a combination of both. The incidence is marked with **G1** at baseline and **G2** after the measure is introduced. Similarly, the degree of severity is marked with **S1** in the initial state and with **S2** in the state after the introduction of the risk management measure. Similarly, the original (initial) risk mark is **K1**, while the residual risk sign after the introduction of the risk mitigation measure is **K2**.

5 Risk analysis

5.1 Risk analysis process

A Risk analysis was performed as described according to ISO 14971, clause 5.2 to 5.5. The implementation of the planned risk analysis activities and the results of the risk analysis were recorded in the risk management file.

5.2 Intended use and identification of characteristics related to safety of the medical devices

(a) Questions:

The following questions can aid the person in identifying all the characteristics of the medical device that could affect safety. (according to ISO 24971)

Items	Questions	Answer/ Comments
A.2.1	What is the intended use, and how is the medical device to be used?	The REHAROB Physiotherapy Equipment is designed for upper limb therapy of hemiparetic patients. The physiotherapist teaches the equipment by exercising the patient. The physiotherapist therefore uses the same physiotherapy exercises to teach the system as they use in their daily work. The therapeutic program thus completed can be repeated by the REHAROB Physiotherapy Equipment in an unlimited number, without the supervision of additional nursing staff.
A.2.2	Is the medical device intended to be implanted?	No, they are not intended to be implanted.
A.2.3	Is the medical device intended to be in contact with the patient or other persons?	Yes, applied parts, the orthoses are in contact with the patient during the therapy. Actuated applied parts like the orthoses and the robot arms are in contact with the therapist during walk through programming. .
A.2.4	What materials or components are utilized in the medical device or are used with, or are in contact with, the medical device?	The materials & components used are listed in BOM (bill of material).

A.2.5	Is energy delivered to or extracted from the patient?	(Yes, kinetic energy delivered to the patient in a controlled way)
A.2.6	Are substances delivered to or extracted from the patient?	No substances are delivered to or extracted from the patient.
A.2.7	Are biological materials processed by the medical device for subsequent reuse, transfusion, or transplantation?	No biological materials process used
A.2.8	Is the medical device supplied sterile or intended to be sterilized by the user, or are other microbiological controls applicable?	No.
A.2.9	Is the medical device intended to be routinely cleaned and disinfected by the user?	Yes, the cleaning of the orthoses has to be done by the therapist.
A.2.10	Does the medical device modify the patient environment?	No modification of the patient environment function
A.2.11	Are measurements taken?	No
A.2.12	Is the medical device interpretative?	No data interpretative
A.2.13	Is the medical device intended for use in conjunction with other medical devices, medicines or other medical technologies?	No, they are not.
A.2.14	Are there unwanted outputs of energy or substances?	No
A.2.15	Is the medical device susceptible to environmental influences?	Yes, it may be influenced by temperature, humidity, vibrations
A.2.16	Does the medical device influence the environment?	Yes, they may influence temperature
A.2.17	Does the medical device require consumables or accessories?	No
A.2.18	Is maintenance or calibration necessary?	Yes
A.2.19	Does the medical device contain software?	Yes
A.2.20	Does the medical device allow access to the information?	No
A.2.21	Does the medical device store data critical to patient care?	No

A.2.22	Does the medical device have a restricted shelf life?	No
A.2.23	Are there any delayed or long-term use effects?	No
A.2.24	To what mechanical forces will the medical device be subjected?	The robot system is subjected to such mechanical hazards as gravity (or instability), impact, and drop.
A.2.25	What determines the lifetime of the medical device?	The service life is based on previous records and model
A.2.26	Is the medical device intended for single use?	This device not intended for single use.
A.2.27	Is safe decommissioning or disposal of the medical device necessary?	Yes, This device needs safe decommissioning or disposal.
A.2.28	Does installation or use of the medical device require special training or special skills?	Yes, installation of the system done by engineers and User Manual will be provided for use of the medical device
A.2.29	How will information for safety be provided?	Product specification or product data sheet Safety instructions will be provided according to IEC 60601-1:2005
A.2.30	Are new manufacturing processes established or introduced?	No
A.2.31	Is successful application of the medical device dependent on the usability of the user interface?	No
A.2.31.1	Can the user interface design features contribute to use error?	No
A.2.31.2	Is the medical device used in an environment where distractions can cause use error?	No
A.2.31.3	Does the medical device have connecting parts or accessories?	Yes, the robot system connected to PC
A.2.31.4	Does the medical device have a control interface?	Yes

A.2.31.5	Does the medical device display information?	Yes, the patients nickname or name and their previous therapy record
A.2.31.6	Is the medical device controlled by a menu?	Yes
A.2.31.7	Is the successful use of the medical device dependent on a user's knowledge, skills and abilities?	Yes, but dependent on the knowledge of the therapist and not on the patients
A.2.31.8	Will the medical device be used by persons with specific needs?	No
A.2.31.9	Can the user interface be used to initiate unauthorized actions?	No
A.2.32	Does the medical device include an alarm system?	Yes
A.2.33	In what ways might the medical device be misused (deliberately or not)?	Neglect of manufacturer's recommended maintenance, unauthorized access to the medical device, incorrect use of connectors
A.2.34	Is the medical device intended to be mobile or portable?	Yes (by wheels)
A.2.35	Does the use of the medical device depend on the essential performance?	No
A.2.36	Does the medical device have a degree of autonomy?	Yes, collaborative robots are used in the system
A.2.37	Does the medical device produce an output that is used as an input in determining clinical action?	No

(b) Intended use and most unfavourable maximum working load condition

REHAROB 3.0 Physiotherapy Equipment is used for the clinical physiotherapy of the upper limb of hemiparetic patients. The physiotherapist teaches the equipment by exercising the patient. The physiotherapist therefore uses the same physiotherapy exercises to teach the system as they use in their daily work. During training, the system remembers the physiotherapy, for

example, the series of movements of the upper arm and forearm, based on the signals from the built-in sensors. The sample program and the associated safety data, which only allows the safe repetition of the given physiotherapy, are generated automatically by the system. The physiotherapist can determine and change the parameters of the taught exercises, e.g. the speed, the number of repetitions, the order of the exercises. The therapeutic program thus completed can be repeated by the REHAROB Physiotherapy Equipment in an unlimited number, without the supervision of additional nursing staff.

The equipment is only permitted for indoor use at room temperature. The cable connector is only compatible with the EU mains connector and with the corresponding voltage and frequency (230 VAC, 50 Hz). The voltage from the transformer of Universal Robots robot is 48 V, and the voltage from DarpaMotion Robot Finger (hereinafter “DMRF”) is 24 V.

Target Group

REHAROB 3.0 is used for the upper limb treatment of hemiparetic (unilateral paralytic) patients. The gender and age of the patients do not affect the suitability for treatment, only the anatomical dimensions (patient arm length, arm thickness, patient height,...) Patients come from the 5-95 percentile size range.

The following persons may come into contact with REHAROB 3.0:

patient: a patient in need of physiotherapy
physiotherapist: a therapist who supervises physiotherapy and operates the system
engineer: the person who installs and maintains the equipment
third party: e.g. cleaning staff

Reasonably foreseeable misuse listed as in the below table

Item	Foreseeable misuse and hazard/hazardous situation identification
A1	Device subjected to force
A2	Device subjected to impact
A3	Inadequate storage, transport
A4	Inadequate fixation
A5	Premature or Excessive cleaning
A5	Ortheses exposed to excessive temperature or direct heat
A6	Ortheses dropped
A7	Device (e.g. DMRF) dropped

A8	An unauthorized (third) person is in the robot workspace.
A9	Prototype: A person who does not speak English can misunderstand things.
A10	Output overload of power supply
A11	Output short of power supply
A12	The slope of the floor surrounding the unit poses a risk of an accident.
A13	Patients with vasoconstriction may develop decubitus over a longer period of time.
A14	Improper placement of the orthoses and improper physiotherapy can harm the patient.
A15	An unauthorized person get access to the computer and cause privacy risk.
A16	If the velcro becomes unclean, it will loosen or release during physiotherapy.
A17	Unintended movement related to shared control
A18	Unintended movement related to start up, restart or normal stop
A19	If lack or loss of SITUATION AWARNESS results in hazardous situations.

5.3 Identification of hazards and hazardous situations

The following list contains identification of hazards for the medical equipment (Note: the evaluation of possible hazards base in engineering judgement, ISO 14971:2019 and ISO 24971:2020)

Item	Hazard/hazardous situation identification	Hazard type – Harm
B1	Line voltage from mains to cause a hazard.	Electric energy – Electric Shock
B2	Touch current (Enclosure leakage current) of accessible parts to cause hazards.	Electric energy – Leakage current
B3	Touch current (Output leakage current) of an accessible part to cause a hazard .	Electric energy – Leakage current
B4	Stored energy to cause a hazard	Electric energy – Electric Shock
B5	Input current of Label less than rated value of ME equipment may cause a hazard	Functionality – Labeling (Inadequate description of performance characteristics)
B6	Fuse may not operate to cause a fire hazard	Electric energy – Electric Shock
B7	Critical component fault to cause a fire hazard	Electric energy – Electric Shock
		Thermal energy – High temperature
B8	Unsuitable rating of a critical component to cause a fire hazard.	Electric energy – Electric Shock

		Thermal energy – High temperature
B9	Critical component or wires displaced to cause a hazard	Mechanical energy – Moving parts
		Mechanical energy – Vibration
		Electric energy – Electric Shock
B10	Physically equipment unstable in normal use to cause hazard	Mechanical energy – Falling
B11	Openings of enclosure to cause fire hazard	Thermal energy – High temperature
B12	Markings of Label were not clearly readable to cause hazard	Functionality – Labeling (Inadequate description of performance characteristics)
B13	Instructions or technical description document not provided to cause hazard.	Functionality – Labeling (Inadequate description of performance characteristics)
B14	Information of instructions not enough to cause hazard.	Functionality – Labeling (Inadequate description of performance characteristics)
B15	The Instruction not included the disposal of waste products, residues, etc. to cause hazard	Functionality – Labeling (Inadequate description of performance characteristics)
B16	User modified the ME equipment to cause hazard	Functionality – Labeling (Inadequate disclosure of limitations)
B17	Components of equipment, the unwanted movement or vibration to cause hazard.	Mechanical energy – Moving parts
B18	The accidental detachment of wiring to cause hazard.	Mechanical energy – Vibration
B19	Wiring contact with a moving part or from friction at sharp corners and edges to cause hazard	Mechanical energy – Sharp edges
B20	Rough surfaces, sharp corners and edges of ME equipment to cause hazard.	Mechanical energy – Torsion, shear and tensile
B21	Constructional of Fire Enclosure not meet IEC 60601-1, 3rd to cause hazard	Thermal energy – High temperature
B22	Rating misused for Component	Electric energy – Electric Shock
		Thermal energy – High temperature

B23	If power failure occurs and then the power returns, the continued movement of the robot – due to the unidentifiable position of the controls – is a danger to the patient.	Functionality – Critical performance
B24	Too much force or torque during exercises (during therapy).	Functionality – Critical performance
B25	The Watchdog computer crashes and the uncontrolled continuation of robotic movement after crashing poses a danger to the patient.	Functionality – Critical performance
B26	DMFR applies too much torque to the patient's hands.	Functionality – Critical performance
B27	Collision of robotic arms.	Functionality – Critical performance
B28	The robots should not suddenly cover too great a distance.	Functionality – Critical performance
B29	Due to improper trajectory calculation, the robots can perform movements that move the patient's hand to an unnatural position.	Functionality – Critical performance
B30	In case of signal loss, the robot skips any steps and causes hazardous situation.	Data – Transfer
B31	Exposed surfaces of applied parts reach a temperature over 41°C.	Thermal energy – High temperature
B32	While teaching the exercises, an occurring robot-patient collision does pose a danger to the patient.	Functionality – Critical performance
B33	While teaching the exercises, an occurring robot-physiotherapist collision does pose a danger to the physiotherapist.	Functionality – Critical performance
B34	The force or torque exceeding the load capacity can damage the robot itself, the patient or the operator.	Functionality – Critical performance
B35	The electromagnetic disturbing effect of outside spaces can result in uncertain operation.	Electric energy—Electric fields
		Electric energy – Magnetic fields
B36	In case of "emergency stop", the patient's exercised limb remains temporarily in a painful position and cause psychological stress in the patient.	Functionality – Critical performance
B37	Cross-contamination and recontamination might possible from applied parts(orthoses).	Biological agents
B38	The asynchronous movement of two robotic arms, one robotic movement lags behind the other.	Functionality – Critical performance

B39	Faulty data transmission results in incorrect safety limits.	Data – Transfer
B40	Unintended movement related to unexpected release of energy	Mechanical energy – Moving parts
B41	Unintended movement related to protective stop	Mechanical energy – Moving parts

5.4 Estimation of risks of each hazard

The decision of each hazardous risk was referred to in the recommendation of ISO 14971, ISO 24971 and the requirement of IEC 60601-1.

Item	Risk	Initial Risk estimation		
		P1	S1	R1
A1	Device subjected to force	4	4	16 (unacceptable)
A2	Device subjected to impact	4	4	16 (unacceptable)
A3	Inadequate storage, transport	4	3	12 (Risk Control recommended)
A4	Inadequate fixation	3	5	15 (unacceptable)
A5	Premature or Excessive cleaning	4	4	16 (unacceptable)
A5	Ortheses exposed to excessive temperature or direct heat	4	2	8 (Risk Control recommended)
A6	Orhteses dropped	5	3	15 (unacceptable)
A7	Device (e.g. DMRF) dropped	4	4	16 (unacceptable)
A8	An unauthorized (third) person is in the robot workspace.	4	4	16 (unacceptable)

A9	Prototype: A person who does not speak English can misunderstand things.	4	3	12 (Risk Control recommended)
A10	Output overload of power supply	4	4	16 (unacceptable)
A11	Output short of power supply	4	3	12 (Risk Control recommended)
A12	The slope of the floor surrounding the unit poses a risk of accident.	4	3	12 (Risk Control recommended)
A13	Patients with vasoconstriction may develop decubitus over a longer period of time.	4	3	12 (Risk Control recommended)
A14	Improper placement of the orthosis and improper physiotherapy can harm the patient.	3	3	9 (Risk Control recommended)
A15	An unauthorized person get access to the computer and cause privacy risk.	4	2	8 (Risk Control recommended)
A16	If the velcro becomes unclean, it will loosen or release during physiotherapy.	4	2	8 (Risk Control recommended)
A17	Unintended movement related to shared control	3	4	12 (Risk Control recommended)
A18	Unintended movement related to start up, restart or normal stop	2	4	8 (Risk Control recommended)
A19	If lack or loss of SITUATION	4	3	12

	AWARNESS results in hazardous situations.			(Risk Control recommended)
B1	Line voltage from mains to cause hazard.	3	5	15 (unacceptable)
B2	Touch current (Enclosure leakage current) of accessible parts to cause hazard.	3	5	15 (unacceptable)
B3	Touch current (Output leakage current) of accessible part to cause hazard .	5	4	20 (unacceptable)
B4	Stored energy to cause hazard	5	3	15 (unacceptable)
B5	Input current of Label less than rated value of ME equipment may cause hazard	4	4	16 (unacceptable)
B6	Fuse may not operate to cause fire hazard	3	3	9 (unacceptable)
B7	Critical component fault to cause fire hazard	5	4	20 (unacceptable)
B8	Unsuitable rating of critical component to cause fire hazard.	5	4	20 (unacceptable)
B9	Critical component or wires displaced to cause hazard	4	4	16 (unacceptable)
B10	Physically equipment unstable in normal use to cause hazard	3	3	9 (Risk Control recommended)
B11	Openings of enclosure to cause fire hazard	5	3	15 (unacceptable)
B12	Markings of Label were not clearly readable to cause hazard	4	3	12 (Risk Control recommended)

B13	Instructions or technical description document not provided to cause hazard.	4	3	12 (Risk Control recommended)
B14	Information of instructions not enough to cause hazard.	3	3	9 (Risk Control recommended)
B15	The Instruction not included the disposal of waste products, residues, etc to cause hazard	3	3	9 (Risk Control recommended)
B16	User modified the ME equipment to cause hazard	3	3	9 (Risk Control recommended)
B17	Components of equipment, the unwanted movement or vibration to cause hazard.	4	4	16 (unacceptable)
B18	The accidental detachment of wiring to cause hazard.	3	3	9 (Risk Control recommended)
B19	Wiring contact with a moving part or from friction at sharp corners and edges to cause hazard	4	3	12 (Risk Control recommended)
B20	Rough surfaces, sharp corners and edges of ME equipment to cause hazard.	4	3	12 (Risk Control recommended)
B21	Constructional of Fire Enclosure not meet IEC 60601-1, 3rd to cause hazard	4	3	12 (Risk Control recommended)
B22	Rating misused for Component	4	4	16 (unacceptable)

B23	If power failure occurs and then the power returns, the continued movement of the robot - due to the unidentifiable position of the controls - is a danger to the patient.	4	3	12 (Risk Control recommended)
B24	Too much force or torque during exercises (during therapy).	4	3	12 (Risk Control recommended)
B25	The Watchdog computer crashes am the uncontrolled continuation of robotic movement after crashing poses a danger to the patient.	3	3	9 (Risk Control recommended)
B26	DMFR applies too much torque to the patient's hands.	3	3	9
B27	Collision of robotic arms.	2	3	6 (Risk Control recommended)
B28	The robots should not suddenly cover too great a distance.	3	4	12 (Risk Control recommended)
B29	Due to improper trajectory calculation, the robots can perform movements that move the patient's hand to an unnatural position.	3	4	12 (Risk Control recommended)
B30	In case of signal loss, the robot skips any steps and cause hazardous situation.	3	3	9 (Risk Control recommended)
B31	Exposed surfaces of applied parts reach a	3	2	6

	temperature over 41°C.			(Risk Control recommended)
B32	While teaching the exercises, an occurring robot-patient collision does pose a danger to the patient.	3	3	9 (Risk Control recommended)
B33	While teaching the exercises, an occurring robot-physiotherapist collision does pose a danger to the physiotherapist.	3	3	9 (Risk Control recommended)
B34	The force or torque exceeding the load capacity can damage the robot itself, the patient or the operator.	3	3	9 (Risk Control recommended)
B35	The electromagnetic disturbing effect of outside spaces can result in uncertain operation.	3	2	6 (Risk Control recommended)
B36	In case of “emergency stop”, the patient’s exercised limb remains temporarily in a painful position and cause psychological stress in the patient .	3	2	6 (Risk Control recommended)
B37	Cross-contamination and recontamination might possible from applied parts(orthoses).	3	3	9 (Risk Control recommended)
B38	The asynchronous movement of two robotic arms, one	4	3	12 (Risk Control recommended)

	robotic movement lags behind the other.			
B39	Faulty data transmission results in incorrect safety limits.	4	2	8 (Risk Control recommended)
B40	Unintended movement related to unexpected release of energy	2	4	8 (Risk Control recommended)
B41	Unintended movement related to protective stop	2	4	8 (Risk Control recommended)

6 Risk evaluation

For each identified hazardous situation, the manufacturer shall decide, using the criteria defined in the risk management plan, if risk reduction is required.

If risk reduction is not required, the requirements given in 6.2 to 6.6 do not apply for this hazardous situation.

The results of this risk evaluation were recorded as above.

7 Risk control

7.1 Risk control measures

Risk control measures were taken according to ISO 14971, clause 7.2 to 7.6

7.2 Risk control option analysis

One of the following risk control options apply:

a) inherently safe design and manufacturing;

b) protective measures in the medical device itself or in the manufacturing process;

c) information for safety and, where appropriate, training to users

Item	Risk	Risk control option analysis	Note
A1	Device subjected to static force coming from a person bracing onto or leaning onto it	a) inherently safe design and manufacturing	Provided a solid and hard enclosure to covered unit to Comply with IEC 60601-1, clause 15.3, enclosure mechanical strength test requirement
A2	Device subjected to impact	a) inherently safe design and manufacturing	Provided a solid and hard enclosure to covered unit to Comply with IEC 60601-1, clause 15.3, drop impact test requirement.
A3	Inadequate storage, transport	a) inherently safe design and manufacturing	User Manual describes environmental conditions for transport and storage according to IEC 60601-1 clause 7.2.17, ISO 780 and ISO15223
A4	Inadequate fixation	a) inherently safe design and manufacturing	Warning in the instruction manual (User Manual)
A5	Premature or Excessive cleaning	a) inherently safe design and manufacturing	Provided method of cleaning into User Manual according to IEC 60601-1 7.9.2.12
A5	Ortheses exposed to excessive temperature or direct heat	a) inherently safe design and manufacturing	Provided method of storing and using into User Manual according to IEC 60601-1, ISO 780 and ISO15223
A6	Ortheses dropped	a) inherently safe design and manufacturing	The ortheses are made from durable material
A7	Device (e.g. DMRF) dropped	c) information for safety and, where appropriate, training to users	Warning in the instruction manual (User Manual): Handle the device carefully; never hand it over to the patient.
A8	An unauthorized (third) person is in the robot workspace.	c) information for safety and, where appropriate, training to users	Supervision of the area by the physiotherapist and warning sign. (COBOT safety features will stop the robot in case of impact)
A9	Prototype: A person who does not speak English can misunderstand things.	a) inherently safe design and manufacturing	The communication signs on the screen will be in Hungarian according to 13.7 of Annex 1 in 4/2009. (III. 17.) (the prototype is in English in case of a possible danger, a physiotherapist who does not understand English must be trained to obey.)

A10	Output overload of power supply	a) inherently safe design and manufacturing	Used with IEC 60601-1 certificated power supply. The specified power supply were designed regulating network of OVP, OCP into circuit to Comply with IEC 60601-1, clause 13, single fault conditions test requirement.
A11	Output short of power supply	a) inherently safe design and manufacturing	Used with IEC 60601-1 certified power supply. The specified power supply were designed regulating network of OVP, OCP into circuit to Comply with IEC 60601-1, clause 13, single fault conditions test requirement.
A12	The slope of the floor surrounding the unit poses a risk of accident.	c) information for safety and, where appropriate, training to users	Black / yellow painting to draw attention to the danger.
A13	Patients with vasoconstriction may develop decubitus over a longer period of time.	c) information for safety and, where appropriate, training to users	Warning in the User's Manual: The duration of treatment should not exceed one hour per day.
A14	Improper placement of the orthosis and improper physiotherapy can harm the patient.	c) information for safety and, where appropriate, training to users	Warning in the User's Manual: a trained and authorized person may only perform physiotherapy with orthoses.
A15	An unauthorized person get access to the computer and cause privacy risk.	c) information for safety and, where appropriate, training to users	Presence of physiotherapist and warning signs
A16	If the velcro becomes unclean, it will loosen or release during physiotherapy.	c) information for safety and, where appropriate, training to users	Warning in the User's Manual: Unclean, worn-out velcro should be cleaned as described.
A17	Unintended movement related to shared control	a) inherently safe design and manufacturing	Continuous monitoring of positions to comply with IEC 80901-2-78, clause 201.9.2.3.1.102.
A18	Unintended movement related to start up, restart or normal stop	a) inherently safe design and manufacturing	The robot arms stay in the zero position and mechanical brakes are on until the permitting pedal is activated to comply with IEC 80901-2-78, clause 201.9.2.3.1.104.
A19	If lack or loss of SITUATION AWARNESS	a) inherently safe design and manufacturing	RACA robot designed with various auditory/visual/tactile signals, such as

	results in hazardous situations.		alarms/indicators/displays to meet IEC 80901-2-7, clause 201.4.2.3.102 situation awareness requirements.
B1	Line voltage from mains to cause hazard.	a) inherently safe design and manufacturing	Used with IEC 60601-1 certificated power supply. The specified power adaptor was provided a solid enclosure to covered unit. (And provided Double/Reinforced insulation and two MOPP) between primary and secondary according to IEC 60601-1.
B2	Touch current (Enclosure leakage current) of accessible parts to cause hazard.	a) inherently safe design and manufacturing	Used with IEC 60601-1 certified power supply. The touch current for the output of supply were met require of IEC 60601-1 clause 8.7, leakage current test requirement.
B3	Touch current (Output leakage current) of accessible part to cause hazard.	a) inherently safe design and manufacturing	Used with IEC 60601-1 certified power supply. The touch current for the outer enclosure of supply were met requirement of IEC 60601-1.
B4	Stored energy to cause hazard	a) inherently safe design and manufacturing	Used with IEC 60601-1 certified power supply. The discharge of AC inlet pins was met requirement of IEC 60601-1 clause 8.7, leakage current test requirement.
B5	Input current of Label less than rated value of ME equipment may cause hazard	a) inherently safe design and manufacturing	Provided rating information on label drawing of unit to Comply with IEC 60601-1, clause 4.11, power input test requirement.
B6	Fuse may not operate to cause fire hazard	a) inherently safe design and manufacturing	Used with IEC 60601-1 certified power supply. (The specified power supply provided with main fuse, the fuse with IEC60127 standard approved to Comply with IEC 60601-1, clause 13, single fault conditions test requirement.)
B7	Critical component fault to cause fire hazard	a) inherently safe design and manufacturing	AC power supply Comply with IEC 60601-1, clause 13, single fault conditions test requirement. All components and wiring are used with their specified ratings.

B8	Unsuitable rating of critical component to cause fire hazard.	a) inherently safe design and manufacturing	All components and wiring are used with their specified ratings according to IEC 60601-1 clause 4.8.
B9	Critical component or wires displaced to cause hazard	a) inherently safe design and manufacturing	The equipment designed according to IEC 60601-1, clause 9.3 requirement
B10	Physically equipment unstable in normal use to cause hazard	a) inherently safe design and manufacturing	Designed steady and solid enclosure to covered unit. According to IEC 60601-1 clause 9.4.3. requirement.
B11	Openings of enclosure to cause fire hazard	a) inherently safe design and manufacturing	Provided a solid and hard enclosure without openings to covered unit to Comply with IEC 60601-1 clause 11.3 requirement
B12	Markings of Label were not clearly readable to cause hazard	a) inherently safe design and manufacturing	Used Waterproof Labels material to Comply with IEC 60601-1, clause 7.1.3, durability of marking test requirement.
B13	Instructions or technical description document not provided to cause hazard.	a) inherently safe design and manufacturing	Instruction manual (User Manual) will be provided according to IEC 60601-1 clause 7.
B14	Information of instructions not enough to cause hazard.	a) inherently safe design and manufacturing	The instructions shall be according to IEC 60601-1, clause 7.9.2.5 provided following information: a. brief description of the ME equipment b. how the ME equipment functions c. the significant physical and performance characteristics of the ME equipment d. conditions of safe operation, transport and storage
B15	The Instruction does not include the disposal of waste products, residues, etc to cause hazard	a) inherently safe design and manufacturing	The user manual provided production recycling information to user according to IEC 60601-1 clause 7.
B16	User modified the ME equipment to cause hazard	a) inherently safe design and manufacturing	The instructions shall be according to IEC 60601-1, clause 7.9.3.1 provided following information: “WARING: No modification of this equipment is allowed”.
B17	Components of equipment, the	a) inherently safe design and manufacturing	The movable components will provide two fixings (mechanically securing,

	unwanted movement or vibration to cause hazard.		physical fit, enclosure) to prevent such movement to meet IEC 60601-1 clause 8.8.4.1 requirement.
B18	The accidental detachment of wiring to cause hazard.	a) inherently safe design and manufacturing	The internal wires will be provided two fixings (mechanically securing, physical fit, enclosure) to prevent such accidental detachment to meet IEC 60601-1 clause 8.10.1 requirement
B19	Wiring contact with a moving part or from friction at sharp corners and edges to cause hazard	a) inherently safe design and manufacturing	Designed wire-way of internal wire shall be smooth and free from sharp edges. Wires shall be protected so that they do not come into contact with burrs, cooling fins, moving parts, etc to meet IEC 60601-1 clause 8.10.1 requirement
B20	Rough surfaces, sharp corners and edges of ME equipment to cause hazard.	a) inherently safe design and manufacturing	Designed smooth chamfer and surfaces for outer enclosure to meet IEC 60601-1 clause 9.3 requirement
B21	Constructional of Fire Enclosure not meet IEC 60601-1, 3rd to cause hazard	a) inherently safe design and manufacturing	Used metal material for enclosure and designed on openings to meet IEC 60601-1, clause 11.3 requirement.
B22	Rating misused for Component	a) inherently safe design and manufacturing	All components and wiring are used within their specified ratings and comply with components standard according to IEC 60601-1, clause 4.8 requirement.
B23	If power failure occurs and then the power returns, the continued movement of the robot - due to the unidentifiable position of the controls - is a danger to the patient.	a) inherently safe design and manufacturing	The system is locked and by protective stop can only be restarted manually by turning it on according to IEC 80901-2-78, clause 201.9.2.101. Teaching the exercises should also be repeated.
B24	Too much force or torque during exercises (during therapy).	a) inherently safe design and manufacturing	Robot speed is drastically limited compared to industry to meet IEC 80601-2-78, clause 201.4.2.3.101. Thoughtful limitations based on a careful series of experiments

B25	The Watchdog computer crashes and the uncontrolled continuation of robotic movement after crashing poses a danger to the patient.	a) inherently safe design and manufacturing	The Watchdog PC is powered from an uninterruptible power source. Pressing the emergency stop button by the patient or operator (physiotherapist) will result in immediate shutdown and sufficient PATIENT training instructions according to IEC 809001-2-78, clause 201.9.2.4.
B26	DMFR applies too much torque to the patient's hands.	b) protective measures in the medical device itself or in the manufacturing process	Checking and regulating torque calculated from engine current.
B27	Collision of robotic arms.	b) protective measures in the medical device itself or in the manufacturing process	Continuous monitoring of robotic arm positions with control.
B28	The robots suddenly cover too great a distance.	b) protective measures in the medical device itself or in the manufacturing process	Application of a collaborative robotic system
B29	Due to improper trajectory calculation, the robots can perform movements that move the patient's hand to an unnatural position.	b) protective measures in the medical device itself or in the manufacturing process	Application of a collaborative robotic system
B30	In case of signal loss, the robot skips any steps and causes hazardous situation.	b) protective measures in the medical device itself or in the manufacturing process	Continuous monitoring of positions.
B31	Exposed surfaces of applied parts reach a temperature over 41°C.	a) inherently safe design and manufacturing	Applied part temperatures cannot be affected by operation of the equipment and complies with IEC 60601-1 clause 11.1.2
B32	While teaching the exercises, an occurring robot-patient collision does pose a danger to the patient.	a) inherently safe design and manufacturing	The careful training of the physiotherapist minimizes the chance of an event occurring, or causes the robot to stop in the event of a collision exceeding the limits of force or torque when using a collaborative robot.
B33	While teaching the exercises, an occurring	a) inherently safe design and manufacturing	The careful training of the physiotherapist minimizes the chance

	robot- physiotherapist collision does pose a danger to the physiotherapist.		of an event occurring, or causes the robot to stop in the event of a collision exceeding the limits of force or torqe when using a collaborative robot.
B34	The force or torque exceeding the load capacity can damage the robot itself, the patient or the operator.	a) inherently safe design and manufacturing	Collaborative robot ensures that when the force or torque is exceeded, the robot stops and an emergency condition is declared. (Both during training and replay.) Output force and torque are limited according to IEC 80901-2-78, clause 201.9.2.3.101 and 201.12.101
B35	The electromagnetic disturbing effect of outside spaces can result in uncertain operation.	a) inherently safe design and manufacturing	Based on EMC tests performed by UR (AoC no. 1645), the robot units meet the standard requirements.
B36	In case of “emergency stop”, the patient’s exercised limb remains temporarily in a painful position and cause psychological stress in the patient.	c) information for safety and, where appropriate, training to users	The physiotherapist should be trained to begin “releasing” the patient by dissolving the orthoses to comply with IEC 80901-2-78, clause 201.9.2.5.
B37	Cross-contamination and recontamination might possible from applied parts(orthoses).	a) inherently safe design and manufacturing	Orthoses must be cleaned after used with proper cleaning agents. The material of the orthoses should be made with an antibacterial material. A detailed description of the disinfection procedure can be found in the User’s Manual.
B38	The asynchronous movement of two robotic arms, one robotic movement lags behind the other.	b) protective measures in the medical device itself or in the manufacturing process	Continuous monitoring and correction of robot arm positions with control, stops further movement if necessary.
B39	Faulty data transmission results in incorrect safety limits.	b) protective measures in the medical device itself or in the manufacturing process	Built-in "self-test" function reduces the incidence of faulty signals to a fraction (virtually zero) by detecting converter faults.

B40	Unintended movement related to unexpected release of energy	a) inherently safe design and manufacturing	No loaded springs, pressurized vessels, flywheels found in the system's drive and met with IEC 80901-2-78, clause 201.9.2.3.1.103 requirement.
B41	Unintended movement related to protective stop	a) inherently safe design and manufacturing	During the protective stop the robot arms are held in a position by the motor brakes to comply with IEC 80901-2-78, clause 201.9.2.3.1.105 requirement.

7.3 Residual risk evaluation

According to procedure, all residual risks are judged acceptable. No further risk control measures shall be applied after the risk control measures are applied, See below table for details.

Item	Risk	Initial Risk Estimation (Before Risk Control)			Risk Estimation (After Risk Control)		
		Probability P1	Severity S1	Risk level R1	Probability P2	Severity S2	Risk level R2
A1	Device subjected to force	4	4	16 (unacceptable)	4	1	4 (acceptable)
A2	Device subjected to impact	4	4	16 (unacceptable)	4	1	4 (acceptable)
A3	Inadequate storage, transport	4	3	12 (Risk Control recommended)	2	1	2 (acceptable)
A4	Inadequate fixation	3	5	15 (unacceptable)	2	2	4 (acceptable)
A5	Premature or Excessive cleaning	4	4	16 (unacceptable)	2	1	2 (acceptable)
A5	Ortheses exposed to excessive temperature or direct heat	4	2	8 (Risk Control recommended)	2	1	2 (acceptable)
A6	Orhteses dropped	5	3	15 (unacceptable)	3	1	3 (acceptable)
A7	Device (e.g. DMRF) dropped	4	4	16 (unacceptable)	1	3	3 (acceptable)

A8	An unauthorized (third) person is in the robot workspace.	4	4	16 (unacceptable)	1	2	2 (acceptable)
A9	Prototype: A person who does not speak English can misunderstand things.	4	3	12 (Risk Control recommended)	1	1	1 (acceptable)
A10	Output overload of power supply	4	4	16 (unacceptable)	2	2	4 (acceptable)
A11	Output short of power supply	4	3	12 (Risk Control recommended)	2	2	4 (acceptable)
A12	The slope of the floor surrounding the unit does pose a risk of accident.	4	3	12 (Risk Control recommended)	2	2	4 (acceptable)
A13	Patients with vasoconstriction may develop decubitus over a longer period of time.	4	3	12 (Risk Control recommended)	2	2	4 (acceptable)
A14	Improper placement of the orthosis and improper physiotherapy can harm the patient.	3	3	9 (Risk Control recommended)	2	1	2 (acceptable)
A15	An unauthorized person get access to the computer and cause privacy risk.	4	2	8 (Risk Control recommended)	1	2	2 (acceptable)
A16	If the velcro becomes unclean, it will loosen or release during physiotherapy.	4	2	8 (Risk Control recommended)	2	1	2 (acceptable)
A17	Unintended movement related to shared control	3	4	12 (Risk Control recommended)	2	1	2 (acceptable)
A18	Unintended movement related to start up, restart or normal stop	2	4	8 (Risk Control recommended)	1	1	1 (acceptable)
A19	If lack or loss of SITUATION AWARNESS	4	3	12 (Risk Control recommended)	2	1	2 (acceptable)

	results in hazardous situations.						
B1	Line voltage from mains to cause hazard.	3	5	15 (unacceptable)	1	1	2 (acceptable)
B2	Touch current (Enclosure leakage current) of accessible parts to cause hazard.	3	5	15 (unacceptable)	1	2	2 (acceptable)
B3	Touch current (Output leakage current) of accessible part to cause hazard .	5	4	20 (unacceptable)	1	2	2 (acceptable)
B4	Stored energy to cause hazard	5	3	15 (unacceptable)	1	2	2 (acceptable)
B5	Input current of Label less than rated value of ME equipment may cause hazard	4	4	16 (unacceptable)	1	2	2 (acceptable)
B6	Fuse may not operate to cause fire hazard	3	3	9 (unacceptable)	1	2	2 (acceptable)
B7	Critical component fault to cause fire hazard	5	4	20 (unacceptable)	2	2	4 (acceptable)
B8	Unsuitable rating of critical component to cause fire hazard.	5	4	20 (unacceptable)	1	1	1 (acceptable)
B9	Critical component or wires displaced to cause hazard	4	4	16 (unacceptable)	2	1	2 (acceptable)
B10	Physically equipment unstable in normal use to cause hazard	3	3	9 (Risk Control recommended)	2	2	4 (acceptable)
B11	Openings of enclosure to cause fire hazard	5	3	15 (unacceptable)	1	2	2 (acceptable)
B12	Markings of Label were not clearly readable to cause hazard	4	3	12 (Risk Control recommended)	1	2	2 (acceptable)
B13	Instructions or technical description document not provided to cause hazard.	4	3	12 (Risk Control recommended)	1	1	1 (acceptable)

B14	Information of instructions not enough to cause hazard.	3	3	9 (Risk Control recommended)	1	1	1 (acceptable)
B15	The Instruction not included the disposal of waste products, residues, etc to cause hazard	3	3	9 (Risk Control recommended)	1	2	2 (acceptable)
B16	User modified the ME equipment to cause hazard	3	3	9 (Risk Control recommended)	1	1	1 (acceptable)
B17	Components of equipment, the unwanted movement or vibration to cause hazard.	4	4	16 (unacceptable)	1	4	4 (acceptable)
B18	The accidental detachment of wiring to cause hazard.	3	3	9 (Risk Control recommended)	3	1	3 (acceptable)
B19	Wiring contact with a moving part or from friction at sharp corners and edges to cause hazard	4	3	12 (Risk Control recommended)	1	2	2 (acceptable)
B20	Rough surfaces, sharp corners and edges of ME equipment to cause hazard.	4	3	12 (Risk Control recommended)	3	1	3 (acceptable)
B21	Constructional of Fire Enclosure not meet IEC 60601-1, 3rd to cause hazard	4	3	12 (Risk Control recommended)	4	1	4 (acceptable)
B22	Rating misused for Component	4	4	16 (unacceptable)	2	1	2 (acceptable)
B23	If power failure occurs and then the power returns, the continued movement of the robot - due to the unidentifiable position of the controls - is a danger to the patient.	4	3	12 (Risk Control recommended)	2	1	2 (acceptable)

B24	Too much force or torque during exercises (during therapy).	4	3	12 (Risk Control recommended)	1	2	2 (acceptable)
B25	The Watchdog computer crashes am the uncontrolled continuation of robotic movement after crashing poses a danger to the patient.	3	3	9 (Risk Control recommended)	2	2	4 (acceptable)
B26	DMFR applies too much torque to the patient's hands.	3	3	9	1	2	2 (acceptable)
B27	Collision of robotic arms.	2	3	6 (Risk Control recommended)	1	2	2 (acceptable)
B28	The robots suddenly cover too great a distance.	3	4	12 (Risk Control recommended)	1	2	2 (acceptable)
B29	Due to improper trajectory calculation, the robots can perform movements that move the patient's hand to an unnatural position.	3	4	12 (Risk Control recommended)	1	2	2 (acceptable)
B30	In case of signal loss, the robot skips any steps and cause hazardous situation.	3	3	9 (Risk Control recommended)	2	2	4 (acceptable)
B31	Exposed surfaces of applied parts reach a temperature over 41°C.	3	2	6 (Risk Control recommended)	2	1	2 (acceptable)
B32	While teaching the exercises, an occurring robot-patient collision does pose a danger to the patient.	3	3	9 (Risk Control recommended)	2	1	2
B33	While teaching the exercises, an occurring robot- physiotherapist collision does pose a	3	3	9 (Risk Control recommended)	2	1	2 (acceptable)

	danger to the physiotherapist.						
B34	The force or torque exceeding the load capacity can damage the robot itself, the patient or the operator.	3	3	9 (Risk Control recommended)	2	2	4 (acceptable)
B35	The electromagnetic disturbing effect of outside spaces can result in uncertain operation.	3	2	6 (Risk Control recommended)	3	1	3 (acceptable)
B36	In case of “emergency stop”, the patient’s exercised limb remains temporarily in a painful position and cause psychological stress in the patient.	3	2	6 (Risk Control recommended)	1	2	2 (acceptable)
B37	Cross-contamination and recontamination might possible from applied parts(orthoses).	3	3	9 (Risk Control recommended)	2	1	2 (acceptable)
B38	The asynchronous movement of two robotic arms, one robotic movement lags behind the other.	4	3	12 (Risk Control recommended)	2	1	2 (acceptable)
B39	Faulty data transmission results in incorrect safety limits.	4	2	8 (Risk Control recommended)	2	1	2 (acceptable)
B40	Unintended movement related to unexpected release of energy	2	4	8 (Risk Control recommended)	1	1	1 (acceptable)
B41	Unintended movement related to protective stop	2	4	8 (Risk Control recommended)	1	1	1 (acceptable)

7.4 Risk/benefit analysis

According to procedure, there is no need to perform a risk/benefit analysis because all residual risks are judged acceptable after risk control.

7.5 Risks arising from risk control measures

There are no new hazards or hazardous situations arising from risk control measures because all risk control measures are an inherent design in equipment before the process of risk management and the result of these control measures are acceptable.

7.6 Completion of risk control

All identified hazardous situations have been considered.

8 Evaluation of overall residual risk acceptability

After all risk control measures have been implemented and verified, the overall residual risk posed by the equipment is acceptable using the criteria defined in the risk management plan.

9 Risk management report

The report is intended to ensure that the risk management plan was properly implemented. The overall residual risk is acceptable, and there are appropriate methods in place to collect and analyze production and post-production information.

10 Sources

[1] ISO 14971:2019, Medical devices – Application of risk management to medical devices

[2] ISO/TR 24971:2020, Medical devices – Guidance on the application of ISO 14971

[3] IEC 60601-1:2005, Medical electrical equipment – Part 1: General requirements for basic safety and essential performance

[4] ISO/PDTS 15066, Robots and robotic devices – Collaborative robots

[5] IEC/FDIS 80601-2-78, Medical electrical equipment —Part 2-78: Particular requirements for basic safety and essential performance of medical robots for rehabilitation, assessment, compensation or alleviation

Annex - Risk Management Plan

11 Introduction

The *risk management plan* has been prepared in accordance with the international standard EN ISO 14971, considering its further amendments.

The *risk management plan* has been prepared in accordance with the requirements of the international standard EN ISO 24971 and follows it accordingly in the task of describing *the risk management process* for the following product:

REHAROB 3.0,

to determine and identify potential risks; evaluate, reduce and control them accordingly. This document describes the *risk management process* for the manufacturer of the medical device mentioned above

DarpaMotion Kft.

The document covers the entire life cycle of the product, including the concept, storage and product disposal in accordance with EN ISO 24971.

The *risk management plan* covers the following areas

– Description and operating characteristics of the medical device
– Definition of persons and responsibilities during the *risk management process*
– Criteria for the acceptability of risks
– *Risk management process* flowchart

12 Description and characteristic of medical electrical equipment (ME equipement)

Specific Properties and Intended Use:

The REHAROB Physiotherapy Equipment designed for upper limb therapy of hemiparetic patients. The physiotherapist teaches the equipment by exercising the patient. The physiotherapist therefore uses the same physiotherapy exercises to teach the system as they use in their daily work. The REHAROB equipment and the power supply must not be used outdoors. The therapeutic program thus completed can be repeated by the REHAROB Physiotherapy Equipment in an unlimited number, without the supervision of additional nursing staff.

Product life:
The average life of the product is 25.000 hours.

13 Definition of people and responsibilities

Designated Responsibility	Designated Person	Responsibilities throughout the Process
Risk management Analyst	Chu, Hong Son	- Responsible for carrying out the Risk Management report - Responsible for document
President	Bauer, Ottó Márk	– Responsibilities as below – Ensuring the provision of adequate resources – Ensuring the assignment of qualified personnel for risk management.

14 Criteria to Analyze and Evalute the Acceptability of Risk

Criteria for risk acceptability has defined based upon applicable national or regional regulations and relevant International Standards, and taken into account available information such as the generally accepted state of the art and known stakeholder concerns.

Based on the guidelines being set up by the company management the identified risks will be evaluated in the risk management worksheet and reported in annual risk management reports as follows (according to ISO 14971):

14.1 Severity of Harm

	Consequences for the patient, therapist or third party	***Rank***
Negligible	No risk of injury. The user does not even notice the possible error. „Background function" (eg, self-test) may be damaged.	**1**
Minor	Slight customer inconvenience; little to no effect on product performance, non-vital fault	**2**
Serious	Short-term injury or impairment requiring or life-threatening injury additional medical intervention to correct (e.g reoperation). Moderate defects, e.g. loss of some sub-functions.	**3**
Critical	Severe, long-term injury; potential disability. A serious fault that can cause a complete malfunction.	**4**
Catastrophic	Results in death or life-threatening injury	**5**

14.2 Probability of Harm

Frequency of Occurrence (G)		*Rate*	*Estimation*
Improbable	Although the error may in principle occur, it is highly improbable. The construction is similar as before when no such error was reported.	**1**	$P < 10^{-6}$
Remote (rare)	The construction is similar as before when such error was rarely reported.	**2**	$10^{-6} \leq P < 10^{-5}$
Occasional	The construction is similar as before when such error was occasionally reported.	**3**	$10^{-5} \leq P < 10^{-4}$
Probable	The construction is usually similar to one that has caused difficulties again in the past.	**4**	$10^{-4} \leq P < 10^{-3}$
Frequent	There is almost certainly a significant number of errors	**5**	P 10^{-3}

14.3 Criteria for the Acceptability of Risks

Risk Evaluation Matrix
From the **G**- and **S**-values – analogously to the figure – the degree of risk (for K) can be compiled by the following overview table:

***Rate of Frequency,* G**		***Rate of Severity,* S**				
		Negligible	***Minor***	***Serious***	***Critical***	***Catastrophic***
		1	**2**	**3**	**4**	**5**
Frequent	**5**	**5**	**10**	**15**	**20**	**25**
Probable	**4**	**4**	**8**	**12**	**16**	**20**
Occasional	**3**	**3**	**6**	**9**	**12**	**15**
Remote (rare)	**2**	**2**	**4**	**6**	**8**	**10**
Improbable	**1**	**1**	**2**	**3**	**4**	**5**

The following table summarizes the evaluation and classification of the resulting **K** risk:

Low	**0-4**	Widely accepted risk. It does not pose a danger to the patient, the operator or the equipment.
Medium	**5-14**	**ALARP (As Low As Reasonably Practicable) range with just "tolerated" risk (small but still reasonably practicable).** Further measures can reduce the risk to a more acceptable level.
High	**15-25**	***UNBEARABLE RISK*.** Fatal risk, appropriate measures must be taken to avoid hazards.

The following criteria will be used according to IEC 60601-1:2005+ CORR. 1 (2006) + CORR. 2 (2007), IEC 60601-1:2012 and IEC 60601-1-2

Electromagnetic Energy Hazards

Humidity, cleaning, harmful ingress of liquids could affect the integrity of electrical insulation. Assessment criteria in determining if the resulting risk is acceptable include:

- no signs of wetting the hazardous parts; or
- the leakage current measurements to evaluate the accessibility to the hazardous parts, the dielectric strength test to evaluate the integrity of electrical insulation and measurement of electrical insulation coordination such as creepage distance and air clearances.

Mechanical Energy Hazards

Mechanical stress (caused by pushing, impact and rough handling) of the product could affect the integrity of electrical insulation and assessment criteria in determining if the resulting risk is acceptable include:

- no structural damages; or
- the dielectric strength test to evaluate the integrity of electrical insulation and measurement of electrical insulation coordination such as creepage distance and air clearances.

Thermal Energy Hazards

Molding stress (during fabrication of enclosure) could affect the integrity of mechanical strength and assessment criteria in determining if the resulting risk is acceptable include:

- no deformation of enclosure; or
- the dielectric strength test to evaluate the integrity of electrical insulation and measurement of electrical insulation coordination such as creepage distance and air clearances.

Fire Hazards

Assessment criteria in determining if the resulting risk is acceptable include:

– not exceeding maximum temperature; or
– no emission of flames, molten metal, poisonous or ignitable substance in hazardous quantities.

15 Controlling of the Risk

The below flow chart describes the levels of realization of the management process and designates single steps for the risk analysis, risk evaluation, action management and the risk controlling.

(The flowchart can be found on the next page)

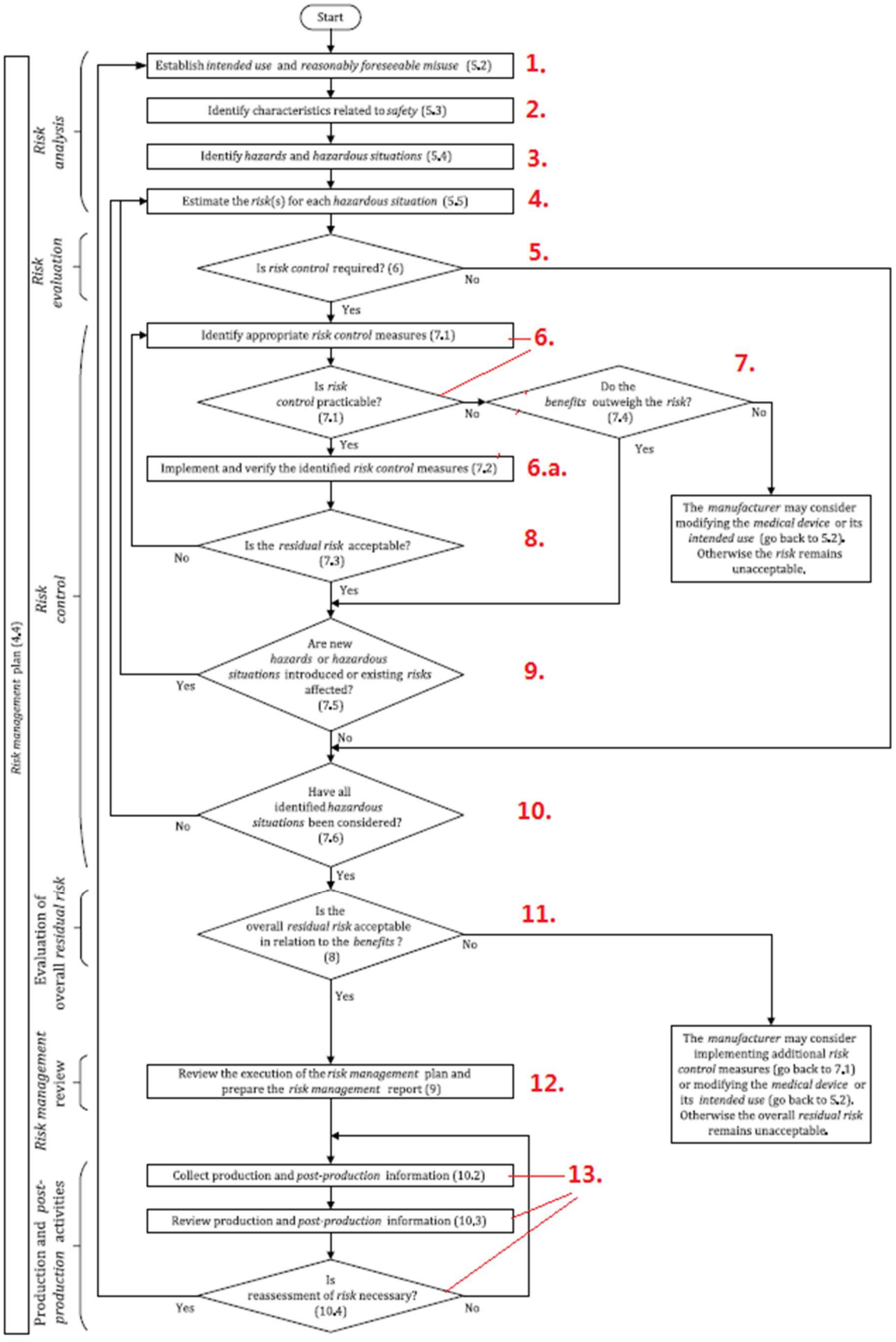


Figure 1: Flow chart of the Risk Management Process Source: ISO 14971:2019

Step 1: Intended Use and reasonably foreseeable misuse
The intended use and each reasonably imaginable and foreseeable misuse will be described in the risk management plan together.

Step 2: Identification of Characteristics Related to the Safety of the Medical Device
The product performance properties, which may influence the safety of the medical device will be described. Then, the performance properties will be taken over into the risk management worksheet and the risks will be evaluated which occur if these performance properties are not achieved. For describing the features of the medical device and its environment in which it is used, ISO 24971 is applied.

Step 3: Identification of Hazards and Hazardous Situation
All known and foreseeable failures / dysfunctions / hazards, which infringe the function and safety of the medical device, will be identified. For this the medical device will be analyzed in its regular mode, failure mode, (also in case of reasonably foreseeable misuse). Moreover already earlier discovered hazards, incidents or situations will be considered. Starting point is always the identified features mentioned in Step 2, as well as the hazards listed in the tables of ISO 14971. These tables are listed in the appendix of the risk management plan and are to be considered accordingly within the risk management worksheet.

Step 4: Estimation of the Risk(s) for Each Hazardous Situation
For each defined or assumed hazard of Step 3 the implied risk will be assessed. The expected damage or severity of harm, and probability of occurrence.
Reasonably foreseeable sequences or combinations of events that can result in a hazardous situation will be considered and the resulting hazardous situation(s) will be recorded.

Step 5: Risk Evaluation
After that each risk will be evaluated, whether it is acceptable or not and whether a risk reduction is required. The criteria to evaluate the acceptability are listed in the risk management plan.

Step 6: Risk Control Option Analysis
For risks that are within the acceptable area no actions of risk control will be taken. Risks, which are outside this area, will be treated case by case. Any risk control measures have the goal to reach at least the „ALARP acceptance level“(As Low As Reasonably Practicable).

Step 6.a: Implementation of Risk Control Measures
The execution of the actions of Step 6, and the effectiveness of the risk control measures taken will be evaluated/verified and recorded in the risk management worksheet.

Step 7: Risk / Benefit Analysis
Not acceptable risks can be accepted in exceptional cases, if a particularly high benefit is to be expected for the patient, and alternative products or treatment measures with minor risks are not available.

Step 8: Residual Risk Evaluation
The residual risks will be evaluated and documented in the risk management worksheet. In case a residual risk is not acceptable, Step 6 will be repeated.

Step 9: Risks Arising from Risk Control Measures
In this step whether the actions of risk control and/or risk reduction would introduce new hazards or hazardous situations will be evaluated. In this case Step 4 has to be repeated.

Step 10: Completeness of Risk Control
In this step, whether all relevant risks have been considered and whether the risk evaluation process is complete will be checked. In case the risk evaluation is acknowledged as complete, the term “no further action” is stated in the risk management worksheet or if this is not true, appropriate descriptions of proposed risk control measures have to be stated.

Step 11: Evaluation of Overall Residual Risk Acceptability
After the completion of all risk control measures, the whole residual risks as well as the acceptability of the residual risks will be evaluated. The evaluation of the residual risks will be performed analogically to the evaluation of the basic risks.

Step 12: Risk Management Report
There will be a summarizing risk management report. It will summarize the risk analysis, risk evaluation and management of preventive respectively risk control measures. This risk management report will be set up and released at least once per year by the management or its deputy.

Step 13: Production and Post-Production Information
Experience and information, which are collected during production and during the post
production phase, are evaluated, starting with step 4.
In each case the insights obtained during the risk management process will be implemented in any applicable product-related documents (e.g. instructions for use, labels and packaging).

Annex – Example FMEA of the REHAROB 3.0 MEE

This annex shows an excerpt of the Failure Mode and Effects Analysis table .

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Folyamatlé-pés azonosító	Folyamatlépés	Elvárt jellemző, tulajdonság, jelenség	Hibaesemény leírása	Hibaesemény következménye	S	O	D	RPN	Hozott intézkedés leírása	S	O	D	RPN
2	10	Páciens kerekesszékben mozog a laborban	Akadálymentes mozgás	Burkolati hibák, kábel, pedál, bútorzat, egyéb eszközök állják a szabad utat	Páciens kiesik a székből, ezáltal személyi sérülés	7	4	2	56					
3			Vízszintes talaj kerekesszék csatlakozásához	Ferde, egyenletlen talaj	Páciens kiesik a székből, ezáltal személyi sérülés	7	4	4	112	Akadálymentes környezet tervezése a rendszerhez (felvéve, még nincs átbeszélve)	7	2	2	28
4			Csúszásmentes padló	Csúszós, ragadós padló	Páciens kiesik a székből, ezáltal személyi sérülés	7	4	4	112	Akadálymentes környezet tervezése a rendszerhez (felvéve, még nincs átbeszélve)	7	2	2	28
5	15	Beteg átülése a rendszerre tervezett kerekesszékbe	Vezetett páciens mozgás	Szabad páciens mozgás	Páciens elesik a székbe üléskor, ezáltal személyi sérülés	7	3	4	84					
6					Páciens a berendezésbe támaszkodik a székbe üléskor, berendezés sérülése, páciens túlterhelése	7	5	3	105	Kerekesszékhez karfa tervezése, melyben a beteg támaszkodhat a be- és kiszállásnál	7	3	3	63
7			Akadálymentes padló	Burkolati hibák, kábel, pedál, bútorzat, egyéb eszközök állják a szabad utat	Páciens elesik a székbe üléskor, ezáltal személyi sérülés	7	4	3	84					
8	20	Kerekesszék pozícionálása gyógytornához	Stabil, kényelmes elhelyezkedés	Kényelmetlen karpozíció	Páciens karjának túlzott terhelése, ezáltal személyi sérülés	7	3	3	63					
9			Fix tér a lábnak	Berendezés és az emberi láb ütközése	Személy és berendezés sérülése	5	5	4	100	Lábtámasz tervezése a kerekesszékhez	5	3	3	45
10			Ütközesmentes üzem	Robot ütközése robottal, emberrel, székkel, asztallal	Személy és berendezés sérülése	7	5	4	140	Robotelrendezés és az eszközök megtervezése az alkalmazott gyakorlatokhoz igazítva	7	3	4	84
			Összefogott haj	Szabadon lógó haj	Személyi sérülés	5	4	2	40					

Figure 2: Detail of the FMEA analysis for the patient.

Note: The FMEA table is currently available in Hungarian.

The heading and two rows have been translated into English:

Process #	Process element	Expected features, properties, phenomenon	Potential Failure Mode	Potential effect of Failure	S	O	D	RPN	Applied Risk Control Measure	S	O	D	RPN
10	Patient moves using wheelchair	Unobstructed movement	Cables, cladding errors (cracks,…)	Wheelchair overturn or falling out of the wheelchair leading to injury	7	4	2	56	Obstacle free route to the system	7	2	2	28
		Horizontal floor for the wheelchair	Steep, uneven floor	Wheelchair overturn or falling out of the wheelchair	7	4	4	112	Obstacle free route to the system	7	2	2	28

				leading to injury									
		Non slippery floor	Slippery floor	Wheelchair overturn or falling out of the wheelchair leading to injury	7	4	4	112	Obstacle free route to the system	7	2	2	28
20	Positoning and fixing of the wheelchair	Stabile, comfortable position for the patient	Uncomfortable position	Overloading the patient's arm during therapy leading to injury	7	3	3	63	t.b.d.				
		Limitation of the workspace for the patient's leg	Collision between the device and patient	Injury and/or damage of the device	5	5	4	100	Provision of footrest for the wheelchair	5	3	3	45