MedAustron

CHALLENGES IN RISK ASSESSMENT OF PARTICLES ACCELERATORS AS MEDICAL DEVICES

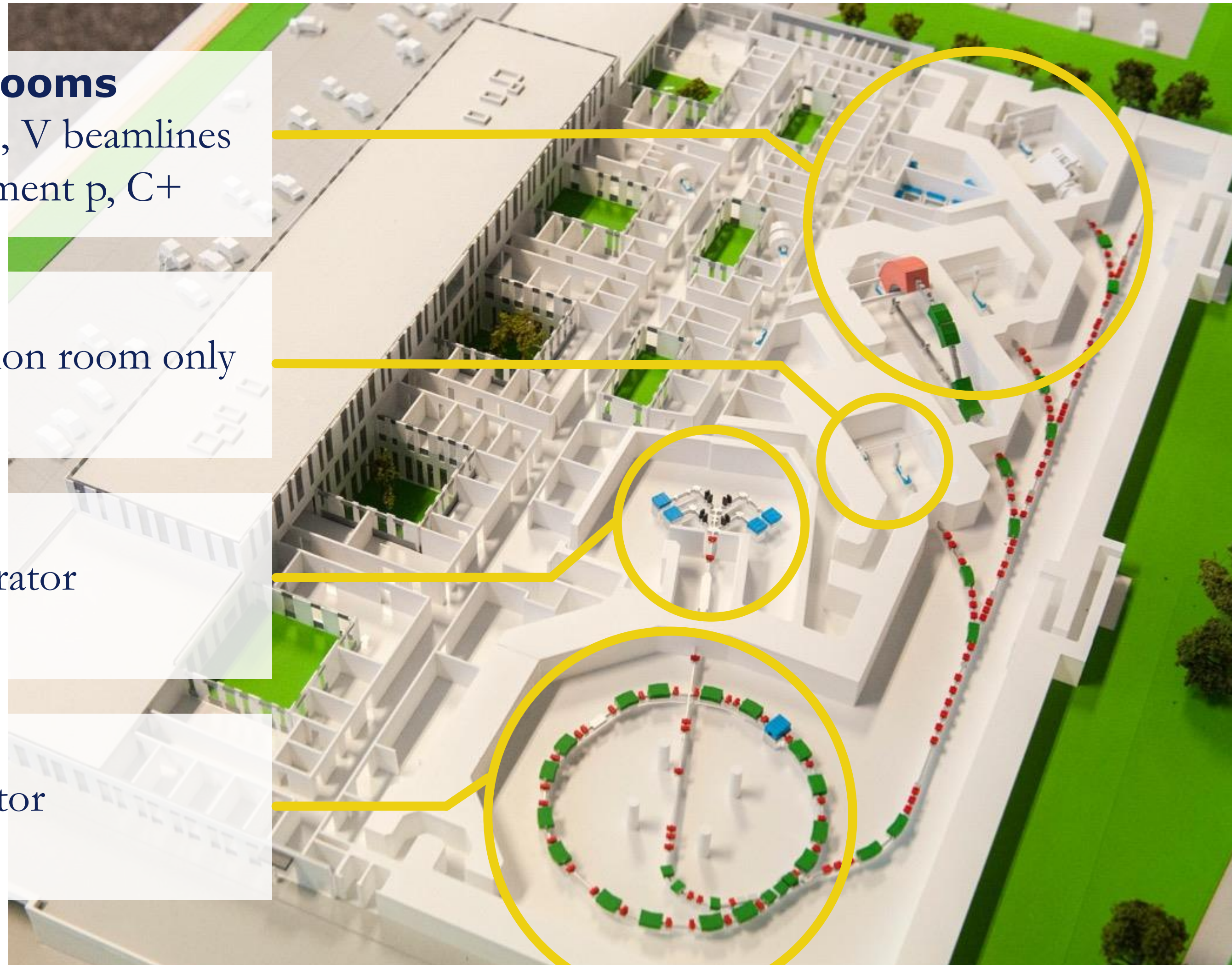
Roberto Filippini

International Conference on Medical Accelerators and Particle Therapy
4-6 September 2019 Seville, Spain

CONTENT

- Introduction
- Risk Management for Medical Devices
- Insights from the MedAustron experience
- Facts and figures
- Challenges and conclusions

MEDAUSTRON FACILITY



Irradiation Rooms
Three rooms H, V beamlines
Gantry for treatment p, C+

Research
Separate irradiation room only for scientific use

Ion Sources
and linear accelerator

Synchrotron
Circular accelerator

RISK MANAGEMENT FOR MD
PARTICLE ACCELERATORS ARE SPECIAL MD

1. **High risk class**
   - IIb in accordance to MDD/MDR
2. **They cannot be entirely administered by the user**
   - Use and Human-Machine interaction is complex
   - Support from operators and technicians
3. **Long lifetime and continuous development processes**
   - Product changes, development and performance improvement

Risk and safety are within the essential requirements in the Medical Device Directive EC/93/42

RISK MANAGEMENT FOR MD
…OUT OF THE ESSENTIAL REQUIREMENTS

- **Risk informed design**
- **Rationale for risk assessment**
  - Hazards and risks
  - Choice of failure models and risk analysis
  - Choice of the risk control options
- **Risk evaluation and risk-benefit analysis**
  - Choice of a risk matrix and acceptability criteria

These issues have to be addressed for the specific MD

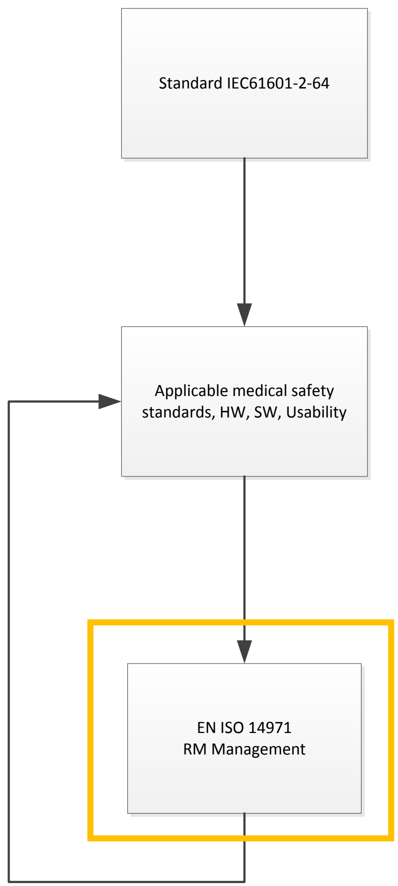
RISK INFORMED DESIGN

…AN EXAMPLE

(1) To be compliant…

(2) To be verifiable…

(3) To be quantifiable…



Basic safety requirements

Means to stop irradiations (automatically, manually)
Means to monitor the beam based on extra-dose limits
Means to prevent the beam to enter an irradiation room
Means to guarantee integrity of clinical parameters

Safety architecture features

Single fault safety principle
Fault tolerance
Failsafe communication
Independence between controls and the safety functions
Software segregation principles
Fault detection and discovery of dormant fault
…

Risk Management process

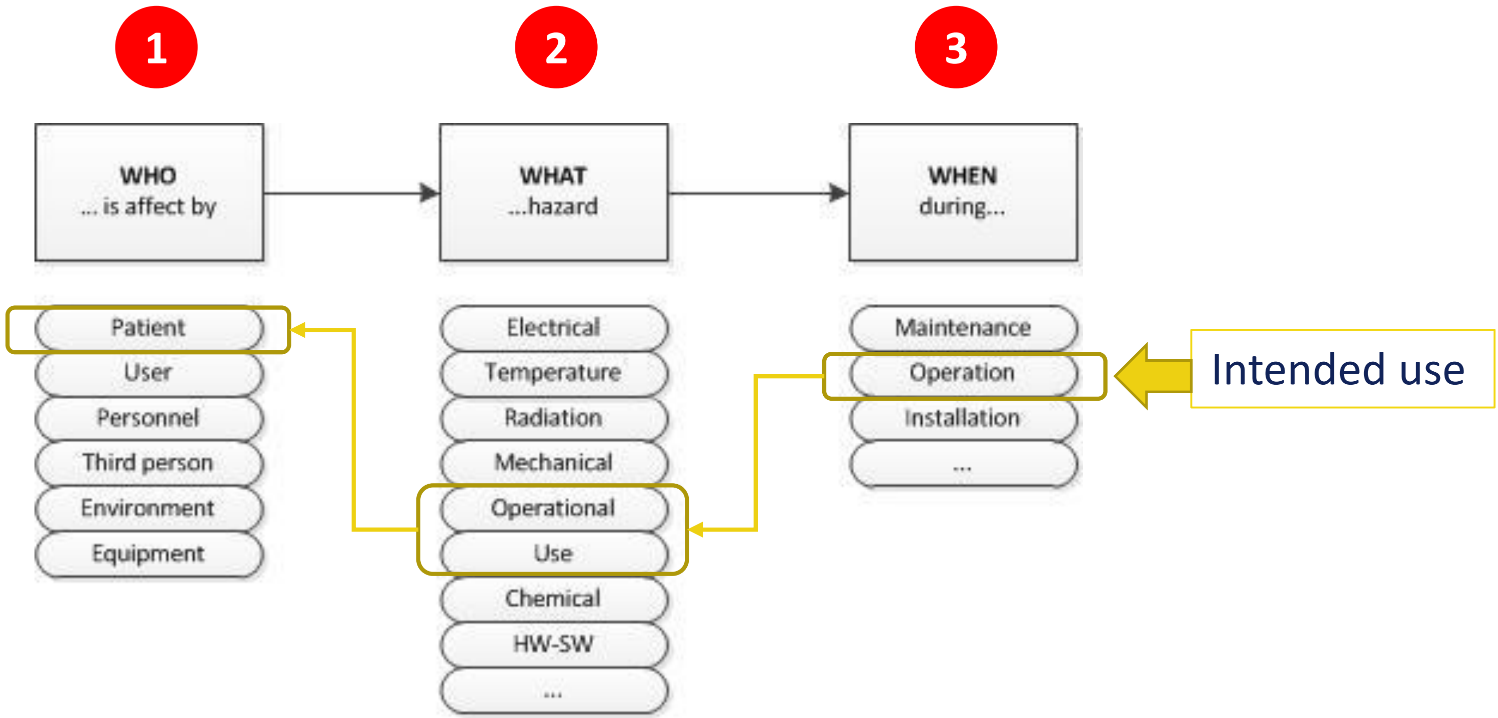
Hazard analysis
Risk analysis
Risk control
Risk evaluation

RISK ASSESSMENT
THE STARTING POINT…

Errors of various nature during design, installation, operation, use and maintenance that can cause harm for the patient, user, personnel, environment, equipment with a certain probability and severity, i.e. **the risk**

All hazards approach, 6 categories are concerned

RISK ASSESSMENT
...THE OVERALL PICTURE



All hazards approach for 6 categories require different professional and technical competences

RISK ASSESSMENT
…AN EXAMPLE: HAZARDS FOR INTENDED USE

Hazards related to beam production, acceleration and delivery for clinical operations

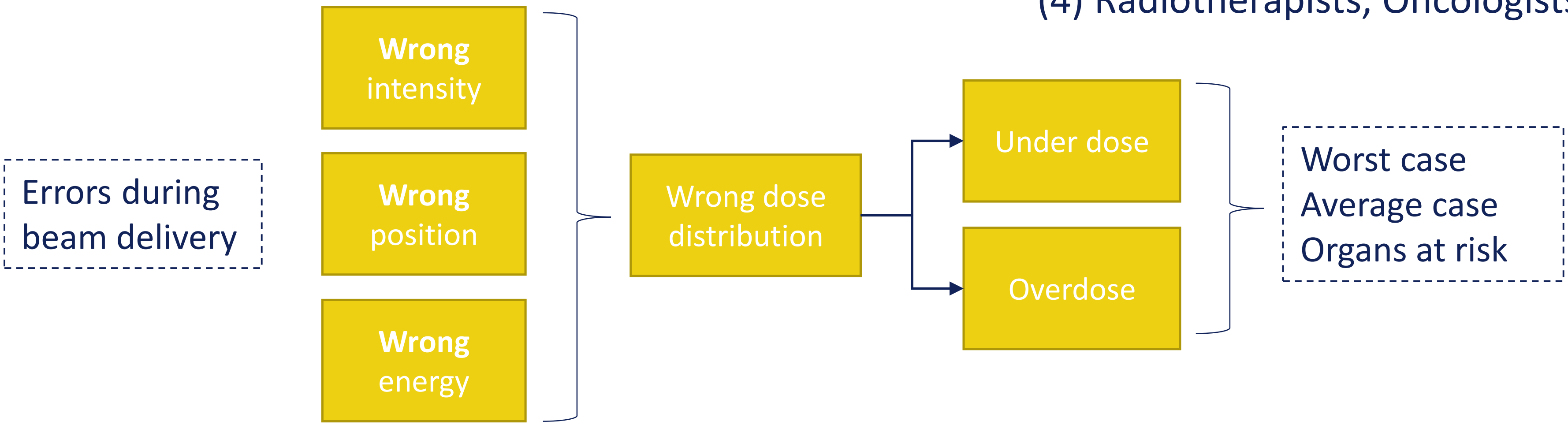
This is a multi-disciplinary **team work**…

(1) Engineers…

(2) Particle accelerator physicists…

(3) Medical physicists…

(4) Radiotherapists, Oncologists



RISK ASSESSMENT
MODELING AND ANALYSIS

What can go wrong?

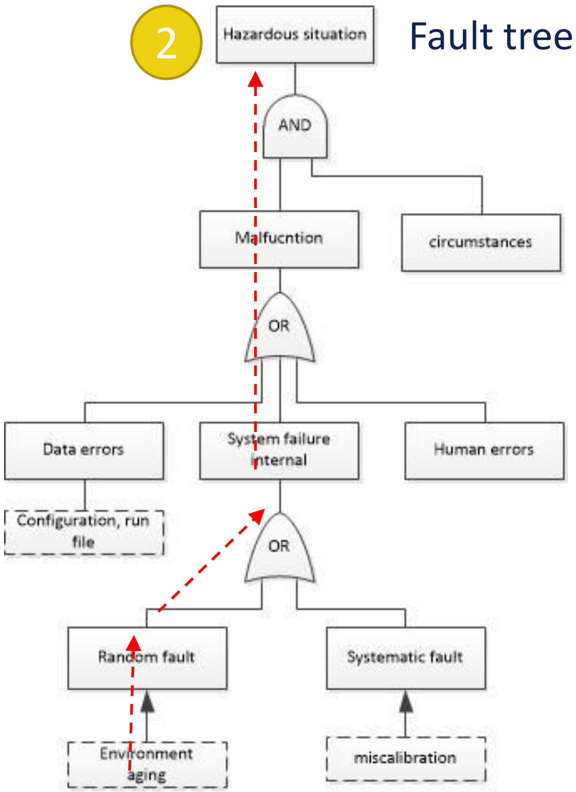
1. Modeling has to capture the **failure process** both logically and dynamically
2. The analysis of the model has to estimate **probability** of the failure event based on the single fault contributors
3. The model has to include the **risk control options**, their effectiveness and the point in time when are demanded

There is not a unique modeling and analysis approach
this freedom needs to be mastered by **suitable guidelines**

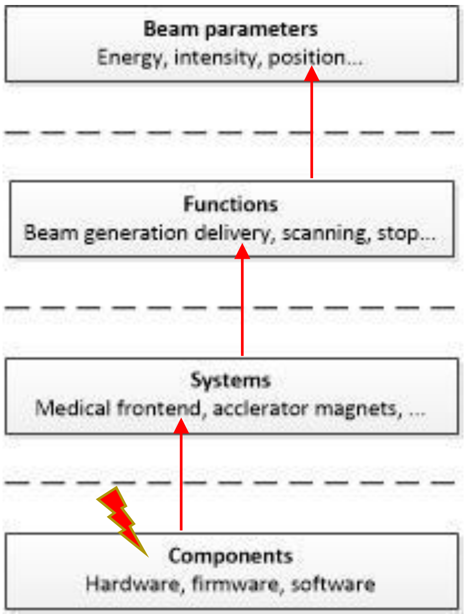
RM ASSESSMENT
FAILURE MODELS...

Guidelines are required to derive failure scenarios from the system architecture

2 Fault tree (logic)



1



3 Failure modes and effect analysis (enumerate)

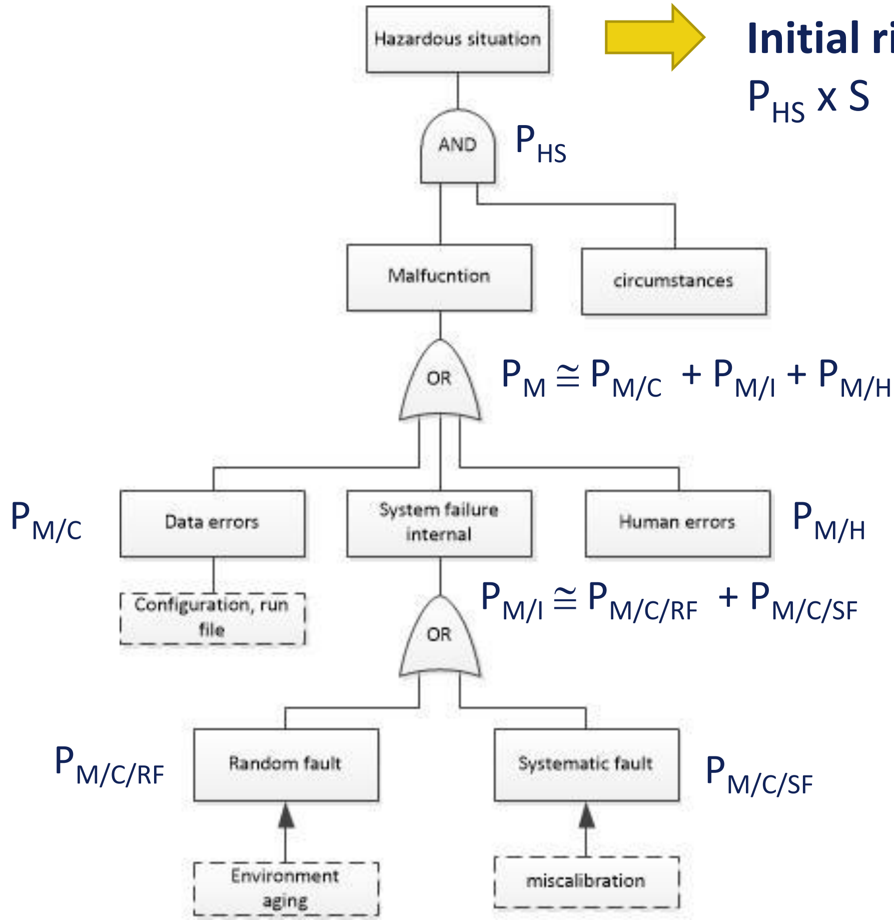
Hazardous situation	Cause	Failure	Effect	Initial risk	...
...					

RM ASSESSMENT
PROBABILITY…

How likely can it occur?

Each fault (HW, SW, human errors) has a probability of occurrence P

Guidelines are required to estimate the probability of failure scenarios



Initial risk

P_{HS} x S

RM ASSESSMENT
RISK CONTROL OPTIONS (1)

How to counteract the failure process?

The RM standard suggests the risk control options, and recommends to use inherent safety, wherever this is possible, as first choice.

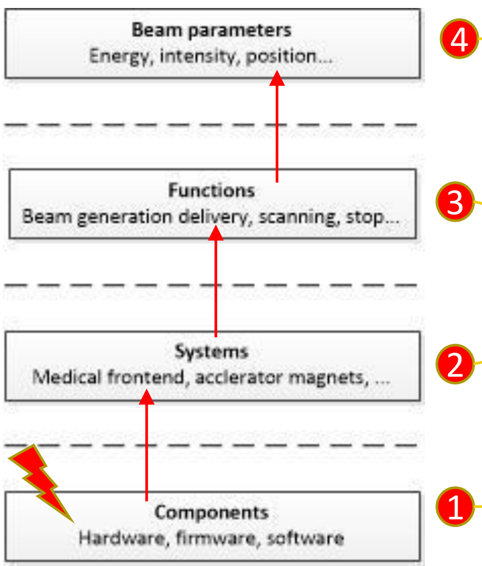
Control option	Effectiveness	Side effects
Inherent safety	Fault avoidance	None
Preventive	Fault detection	False positives
Protective	Beam stop	Extra-dose
Organizational	Periodical checks	Error prone

Guidelines are required for choosing the risk control options i.e. 1) where and 2) when

RM ASSESSMENT

RISK CONTROL OPTIONS (2)

WHERE? in correspondence of a specific cause, fault and malfunction up to the effect on beam parameters



Protective: beam monitors and stoppers
Organizational: QA checks

Inherent safety: fail safe behaviors
Preventive: fault detection and diagnostics, communication checksums, vetoes…

Preventive: fault detection and diagnostics
Organizational: maintenance

RM ASSESSMENT
RISK CONTROL OPTIONS (3)

WHEN? in response to a specific failure event either before or during operation

…the time dimension

Organizational, preventive

Service

QA checks

MP checks

Patient treatment

· · · · · ·

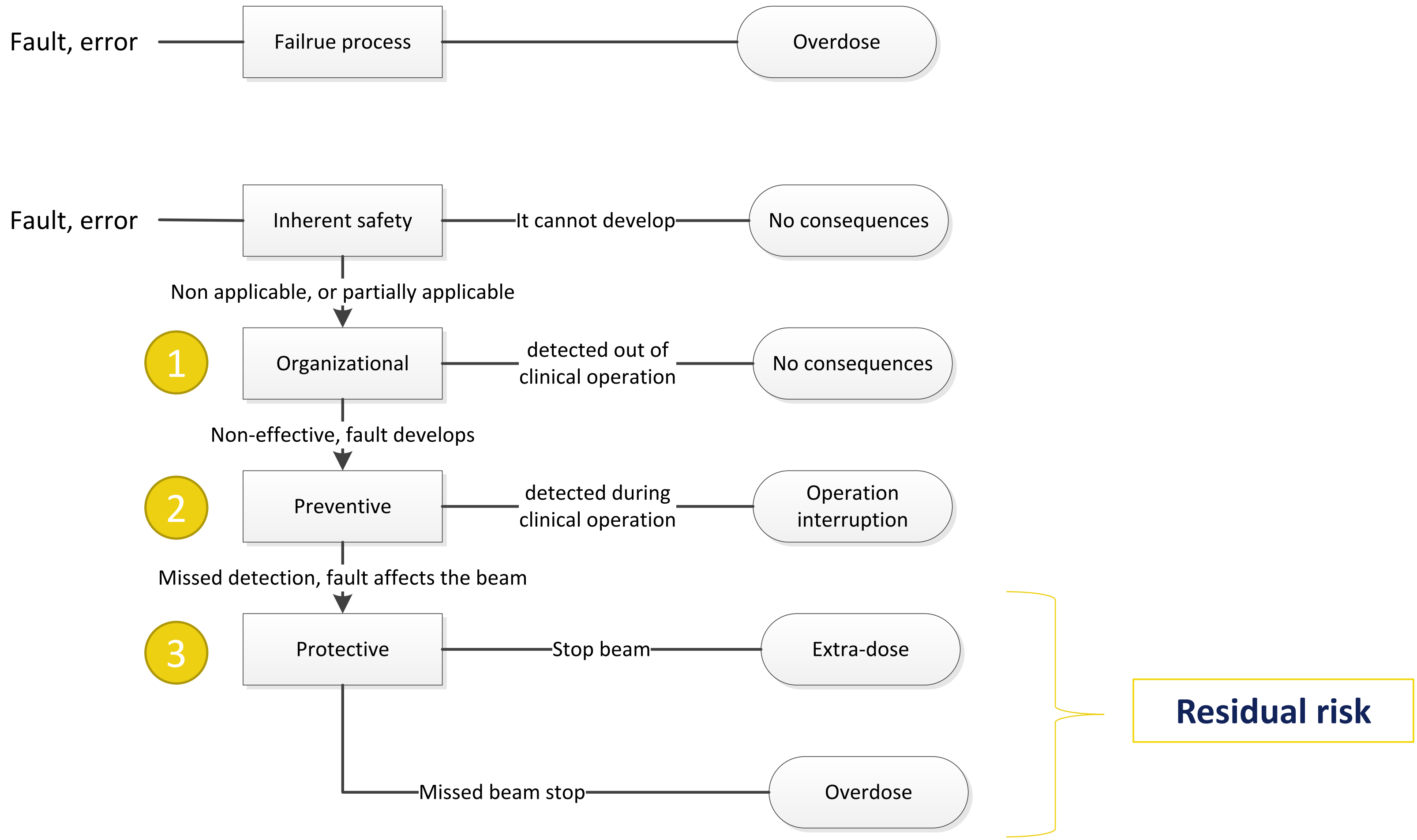
preparation

irradiation

Inherent safety, preventive, protective

Residual risk?

INSIGHTS
RISK REDUCTION PROCESS



RISK EVALUATION
THE RISK METRICS

How to evaluate the risk?
A risk matrix for probability and severity based on frequencies and severity intervals
Risk Priority Number = P x S

Red non acceptable
risk reduction is mandatory

		Severity				
		(1) Negligible	(2) Minor	(3) Moderate	(4) Severe	(5) Catastrophic
Probability of Occurrence	(6) Frequent	6	12	18	24	30
	(5) Often	5	10	15	20	25
	(4) Occasional	4	8	12	16	20
	(3) Seldom	3	6	9	12	15
	(2) Unlikely	2	4	6	8	10
	(1) Incredible	1	2	3	4	5

Green acceptable
no further risk reduction

Yellow
Risk-benefit analysis is mandatory

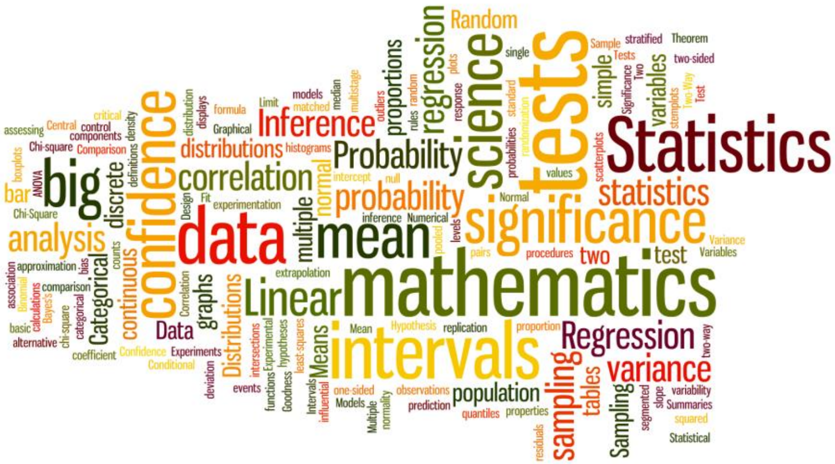
RISK EVALUATION
…IN THREE STEPS

1. Individual risks shall be accepted
2. Overall residual risks shall be accepted
3. Benefits shall be weighted against residual risks
   - It is possible to accept higher risks if benefits are judged as outweighing

The risk benefit analysis is mandatory regardless of the acceptability of the residual risks

FACTS AND FIGURES

- **Hazards in MAPTA**
- **Identified Risks**
- **Risk control measures**



FACTS AND FIGURES

HAZARDS VS. CATEGORIES IN MAPTA

Hazards\Cat. Of risk	PATIENT	USER	PERSONNEL	THIRD PERSON	ENVIRONMENT	EQUIPMENT
Hazards from applicable standards						
Energy-radiation	1 2 5	5 2 6(b)	5 6(b) 2	6(b)	6(b)	6(b)
Energy-EMC	3	3	3	3	3	3
Energy-Electrical	n.a.	4	7	n.a.	n.a.	4 7
Energy-Temperature	n.a.	9 4	9	n.a.	n.a.	9 7
Mechanical	1 4	9 4	9	n.a.	n.a.	9
Mechanical structure	6(a)	6(a)	6(a)	n.a.	n.a.	6(a)
Chemical	4	4	9	n.a.	9	9
Biological	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Operational-function	2	2	9	n.a.	n.a	11
Operational-use	1(a)	1(a)	1(b)	n.a.	n.a	1(b)
Information	1(a)	1(a)	1(b)	n.a.	n.a.	1(b)
HW/SW	1 8	n.a.	9	n.a.	n.a.	11
IT Network	1	n.a.	n.a.	n.a.	n.a.	n.a
Hazards from Ishikawa (6M)						
Milieu	1 2	5	5 9	n.a.	n.a.	9
Material	1	n.a.	n.a.	n.a.	n.a.	1
Measurement	1	n.a.	n.a.	n.a.	n.a.	1
Method	1 10 12	1 10 12	1 10 12	12	12	1 10 12
Man	1	1	1	n.a.	n.a.	1
Machine	1	1	1	n.a.	1	1

Table 1: List of hazards, their applicability to the six categories of risk in MAPTA, and the corresponding assessment framework

Legend: colour based taxonomy

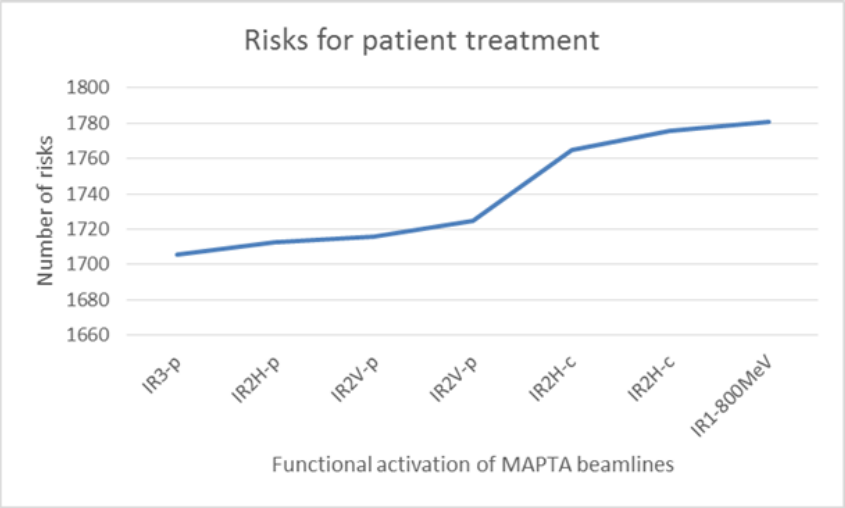
1	EN ISO 14971 RA – (a) user and (b) service manual
2	Functional Safety Concept (FSC)
3	Electromagnetic Compatibility (EMC) Concept
4	EN 60601-1 and IEC 60601-2-64
5	IEC 61508 and derived standards
6	UVP – (a) building and (b) radiation protection
7	OEV/OENORM E 8001-1/EN 61010-1
8	Cause effect analysis
9	CE, applicable standards, HAZOP or RA (EN ISO 14971)
10	Test concept/standard for measurements
11	HAZOP or RA (EN ISO 14971)/Machine protection
12	Review of RA methods by notified bodies

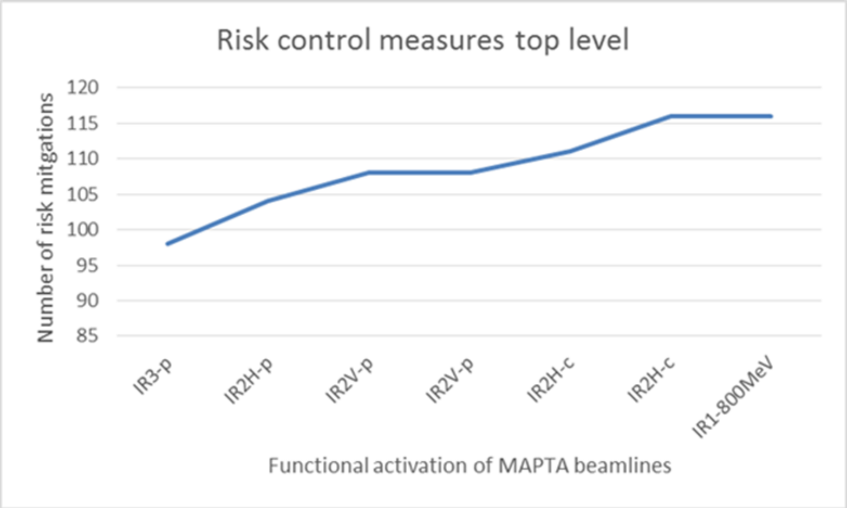
FACTS AND FIGURES
RISK ASSESSMENT INTENDED USE

Number of risks and risk control measures with respect to the activation of beamlines from Dec 2016 to present

⇒ risks from 1706 (dec2016) to 1781

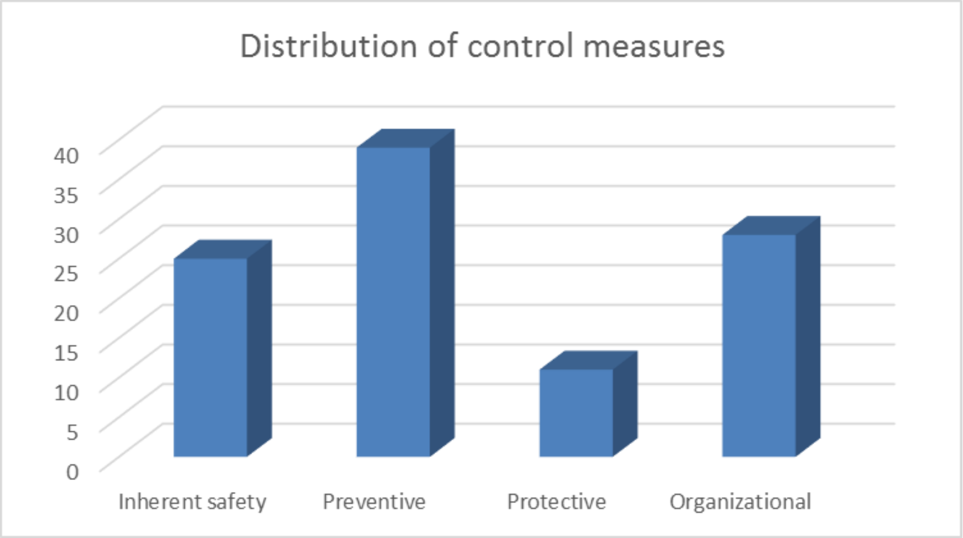
⇒ risk control measures from 97 t0 115 (functional level risk analysis)





FACTS AND FIGURES
DISTRIBUTION OF RISK CONTROL MEASURES

All types of risk control measures are applied to reduce risks in MAPTA, either individually or in combinations



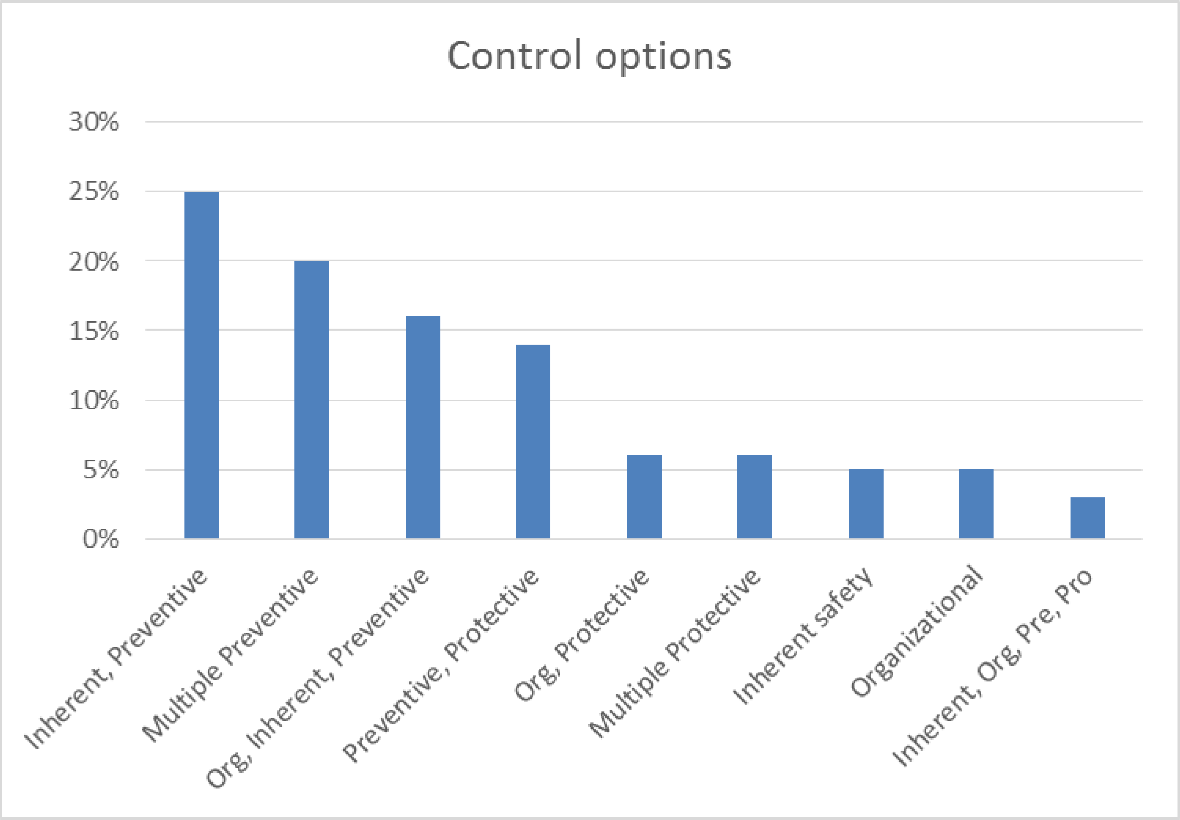
Type	Quantity	instances
Preventive	39	**143**
Inherent safety	22	**111**
Organizational	20	49
Protective	9	39

12%

FACTS AND FIGURES
RISK CONTROL MEASURES (3)

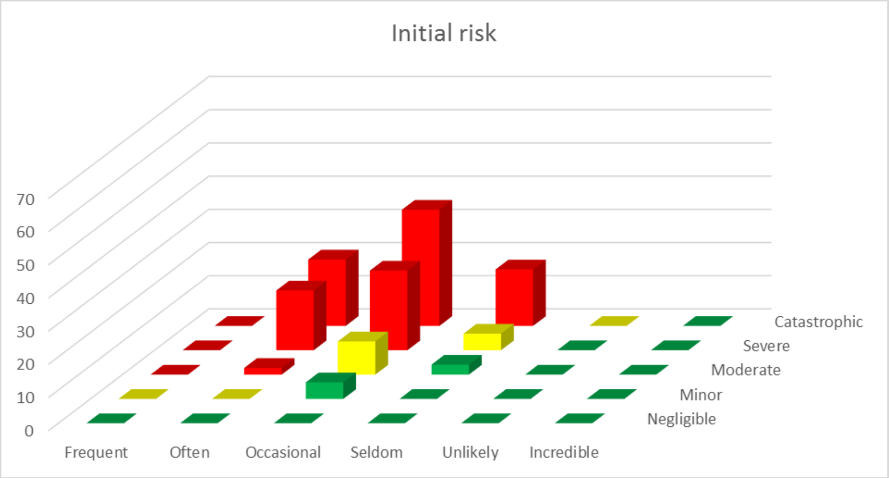
Different combinations of control options
to avoid, prevent, protect

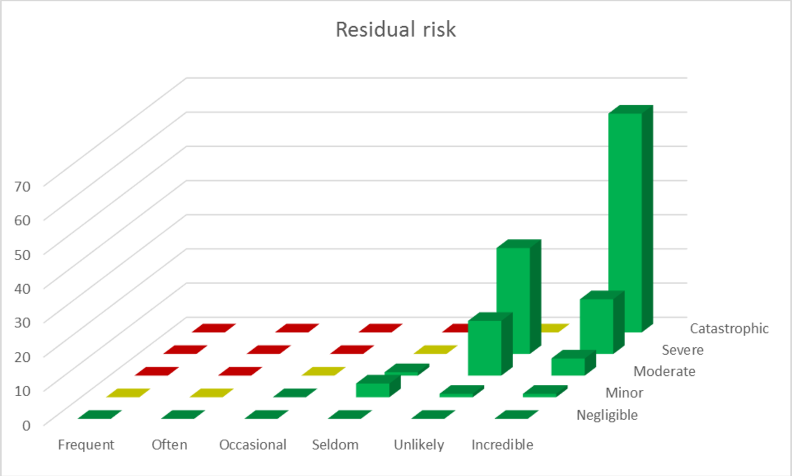
Protective measures alone are for random faults during operation



FACTS AND FIGURES
MAPTA RISK MATRIX

Risks are mapped in the risk matrix (from MAPTA top level risk analysis) before and after risk reduction





RM CHALLENGES
… A FEW TOPICS IN THE SPOTLIGHT

- **Risk assessment**
  - Validate risk estimates by using operation data
- **Trade-off performance vs. risks**
  - Technology bottlenecks (e.g. reaction times of safety systems)
  - False positives $\Rightarrow$ availability
- **RM and post production**
  - Updates of risks as monitoring inputs from different sources, e.g. changes, user feedbacks, development, market…
- **RM and continuous improvements**
  - How to master complexity and at the same time to gain more and more knowledge on risks

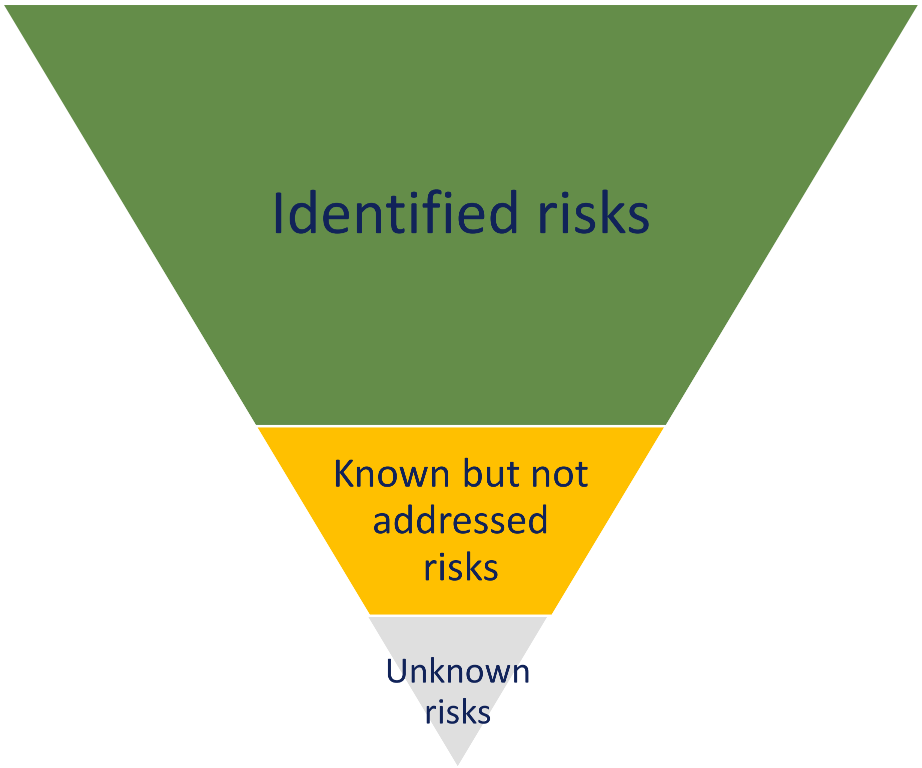
RM CHALLENGES
…CONTINUOUS IMPROVEMENT

At any point in time, the risk knowledge looks like…

1) what is in scope….
Known risks, single fault

2) …what is out of scope
second faults, rare events

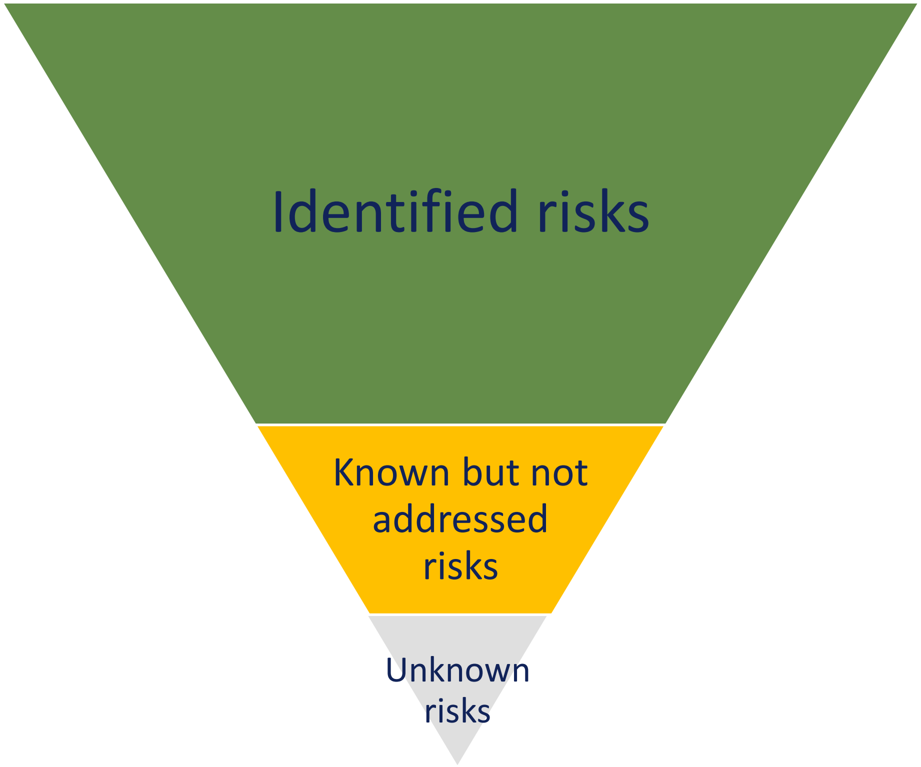
3) and what is left
the “unknown”



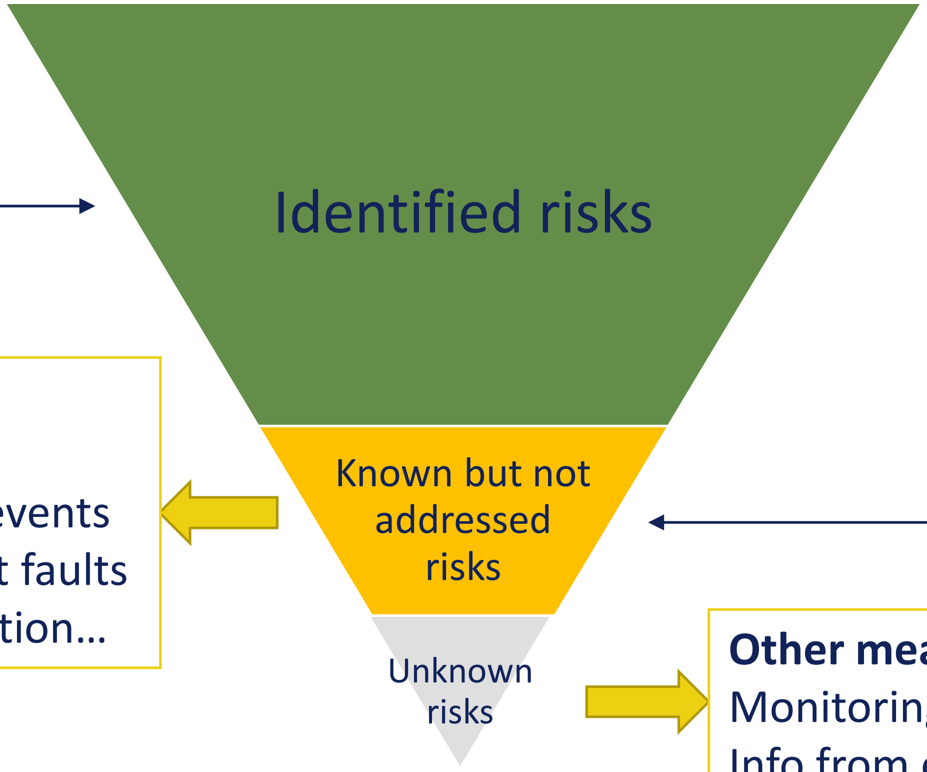
RM CHALLENGES
…CONTINUOUS IMPROVEMENT (2)

Unknown risks have multiple reasons… e.g.
Inaccurate failure models,
lack of risk analysis expertise,
non-homogeneous approaches
…

RM shall aim at keeping the unknown risks **within a tiny % of the total**



RM CHALLENGES
CONTINUOUS IMPROVEMENT (3)



Improve failure models
Common cause failures
Second faults and rare events
Systematic and dormant faults
Interference with operation…

Other means
Monitoring operations
Info from other facilities

CONCLUSIONS AND OUTLOOK

RM in a few recommendations

- To be risk informed RM has to performed from the conceptual design phase
- Risk analysis must have the highest consideration
- Performance increase must consider the available safety technology, and eventually risk-benefit analysis
- Risks related to interplay of MDs shall be analyzed

…and lessons learned

- RM expertise has to be gained within the facility (safety culture), e.g. like for nuclear power plants
- Continuous improvement of RM is essential to maintain the MD effective and safe

CONCLUSIONS AND OUTLOOK

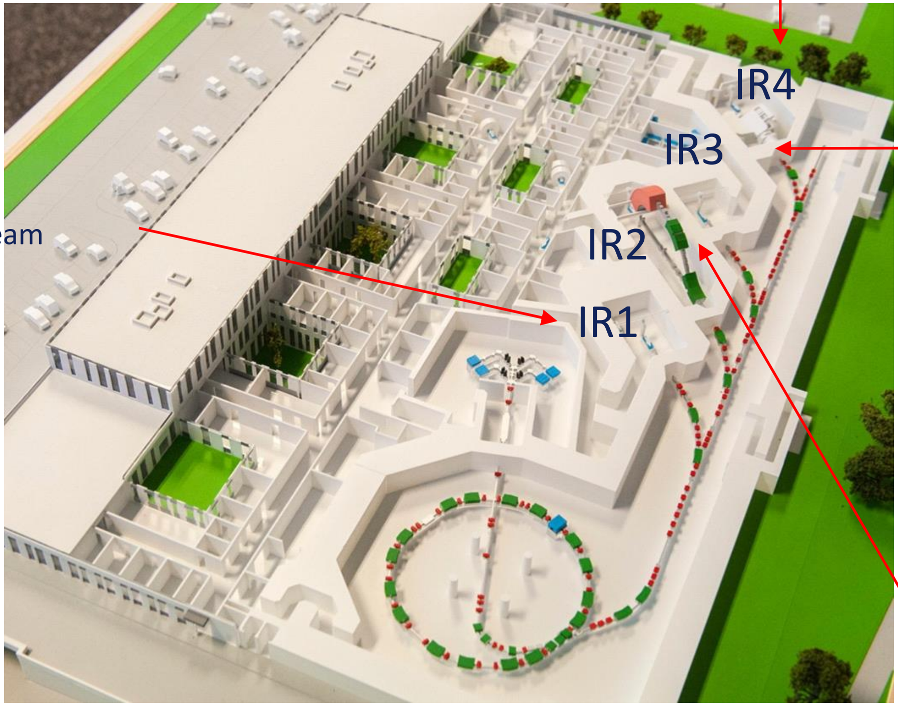
PAST, PRESENT AND FUTURE

***IR4 Gantry**… protons*

IR3 Dec 2016
First patient proton beam

***IR3**… carbon ions*

IR1 NCR
proton and C+ beam



IR2H August 2017
Proton beam
IR2V May 2018
Proton beam
IR2H August 2019
First patient C+

***IR2V**…Carbon ions*

443 patients have been treated since December 2016…

...

Questions?

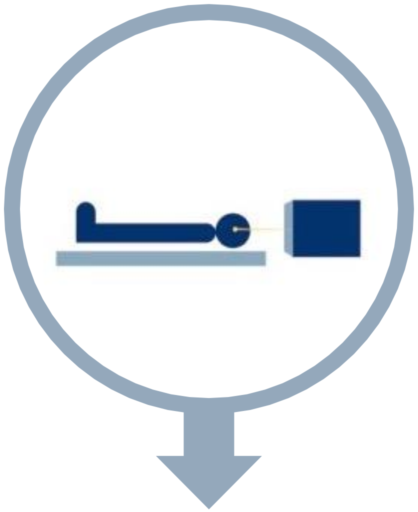
roberto.filippini@medaustron.at

www.medaustron.at

Acknowledgements: Peter Grübling and Mario Schrenk

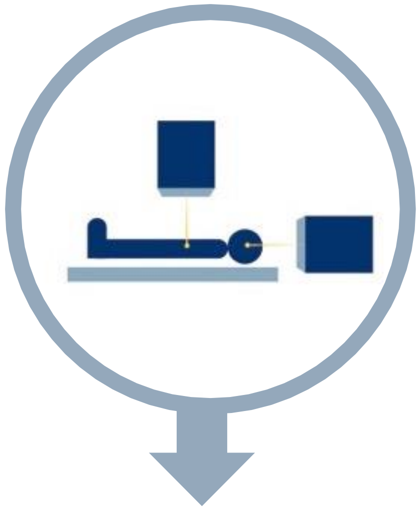
SPARE SLIDES

IRRADIATION ROOMS



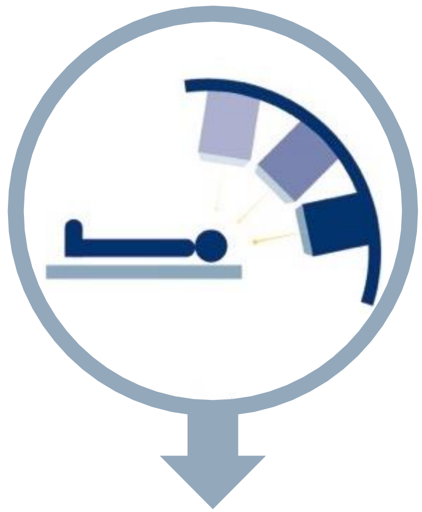
Horizontal fixed beam

Protons & Carbon Ions



Horizontal & vertical fixed beam

Protons & Carbon Ions



Gantry

Protons

Horizontal fixed beam

Protons & Carbon Ions

Patient Treatment

Research

RISK MANAGEMENT FOR MD

THE NORMATIVE FRAMEWORK (1)

EU Medical Device Directive 93/42 and RM...

ESSENTIAL REQUIREMENTS

I. GENERAL REQUIREMENTS

The devices must be designed and manufactured in such a way that, when used under the conditions and for the purposes intended, they will not compromise the clinical condition or the safety of patients, or the safety and health of users or, where applicable, other persons, provided that any risks which may be associated with their intended use constitute acceptable risks when weighed against the benefits to the patient and are compatible with a high level of protection of health and safety.

Safety scope

Risk metrics and criteria

Risk vs. benefits

RISK MANAGEMENT FOR MD
THE NORMATIVE FRAMEWORK (2)

EU Medical Device Directive 93/42 and RM…

Safety by design

The solutions adopted by the manufacturer for the design and construction of the devices must conform to safety principles, taking account of the generally acknowledged state of the art.

In selecting the most appropriate solutions, the manufacturer must apply the following principles in the following order:

— eliminate or reduce risks as far as possible (inherently safe design and construction),

— where appropriate take adequate protection measures including alarms if necessary, in relation to risks that cannot be eliminated,

— inform users of the residual risks due to any shortcomings of the protection measures adopted.

Risk control options

RESIDUAL RISK
INSIGHTS (1)

- **Medical standard IEC 60601-2-64 allows extra dose within 4Gy**
  - The reaction time of the safety chain from error detection to beam stop is crucial…

- **Residual risks for extra dose comes from**
  - Errors in beam delivery within the particle accelerator
  - Errors in the patient positioning system during irradiation (table and robots)

Delivery higher dosage in shorter time shall be compatible with existing patient safety devices

RESIDUAL RISK

INSIGHTS (2)

- **RM standard EN ISO 14971 requires to apply AS Low AS Possible criteria for risk reduction**
  - The reduction of a risk stops when all possible risk mitigations have been applied…
  - This might encourage to control the failure process with several measures, in spite of the residual risk
- **…nonetheless drawbacks have to be considered**
  - Active safety measures that respond to a detectable failure or precursors of failure events can also generate false positives!

Side effect of safety systems to unduly disrupt operation shall be considered as a risk

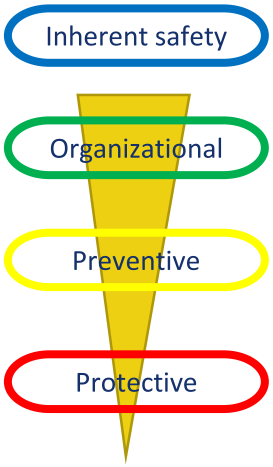
RM CHALLENGES
…POST PRODUCTION

Inputs from several activities/processes…

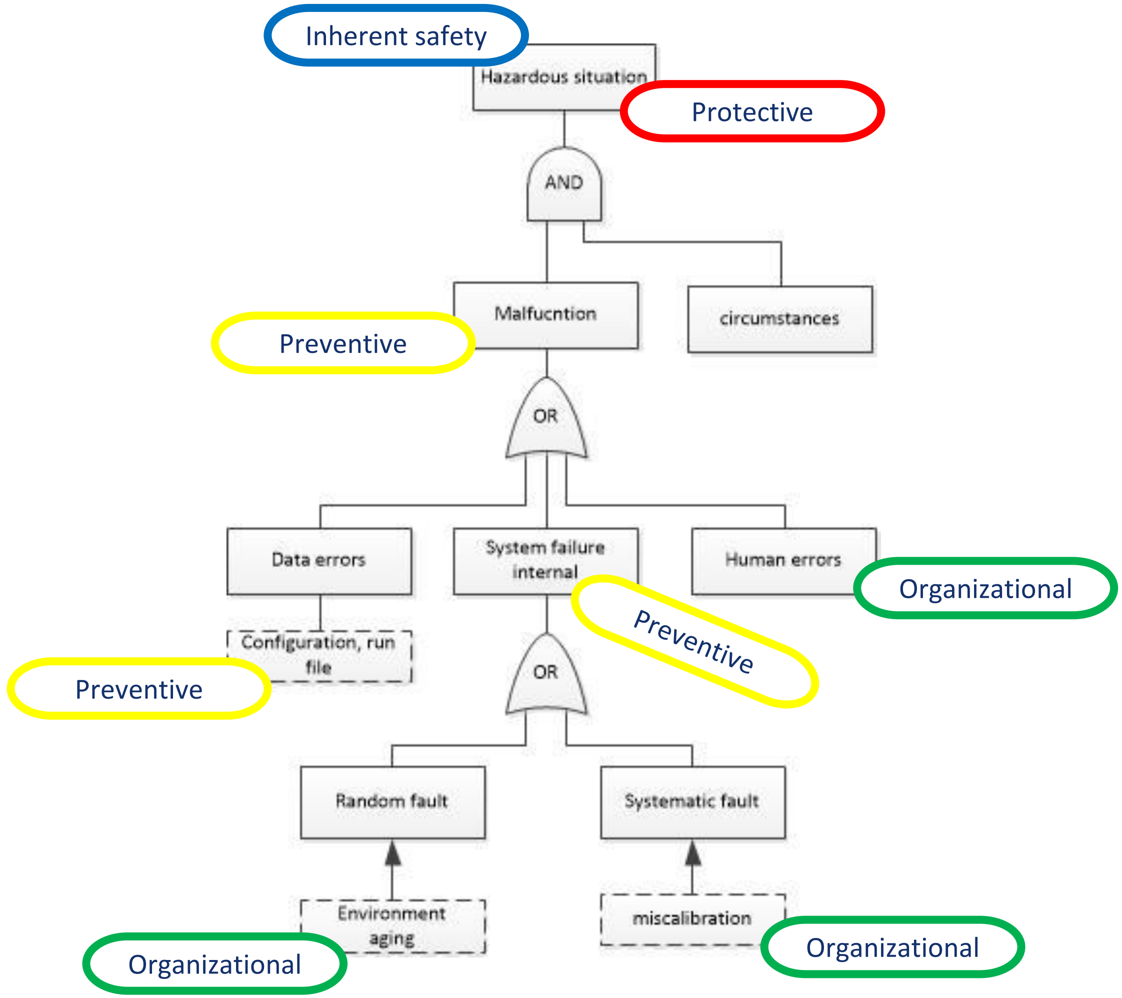
- The user feedbacks process: improve performances within MD safety constraints
- The product changes process: allow changes within a quality controlled MD environment
- The development process: allow integration of new MD components and beamlines after they meet safety requirements
- Market observation: medical development, normative development/ technical state of the art, incidents in related fields

…might change existing risk estimates and/or introduce new risks

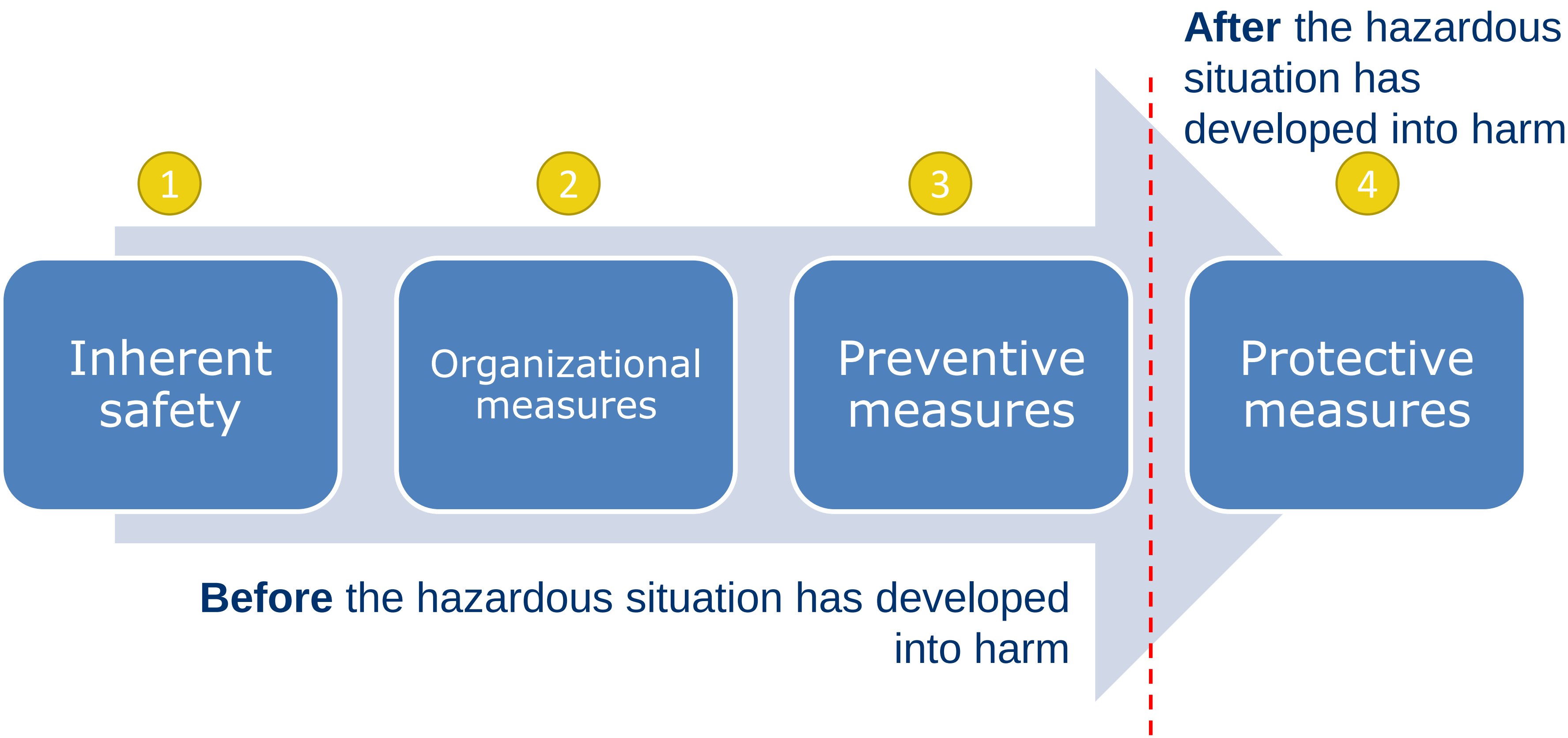
RM PROCESS
HOW TO REDUCE THE RISK (2)



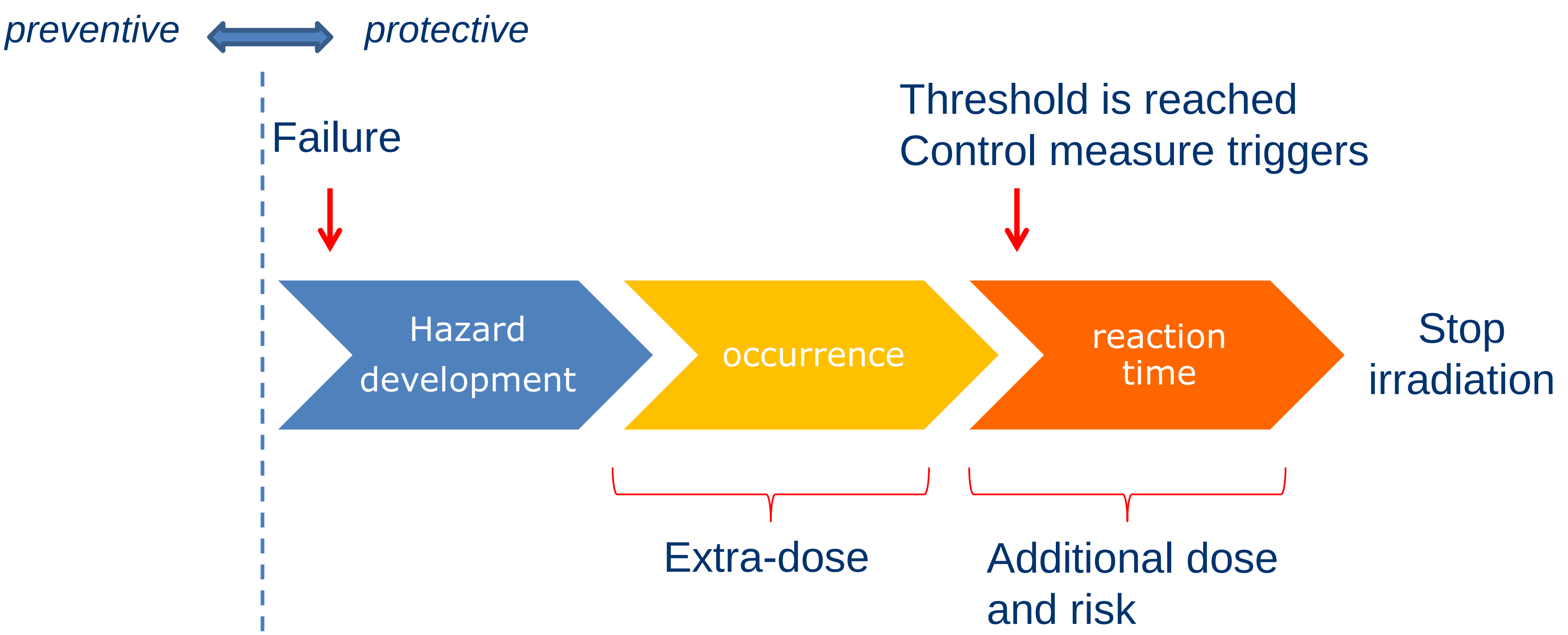
Residual risk



INSIGHTS
RISK CONTROL OPTIONS

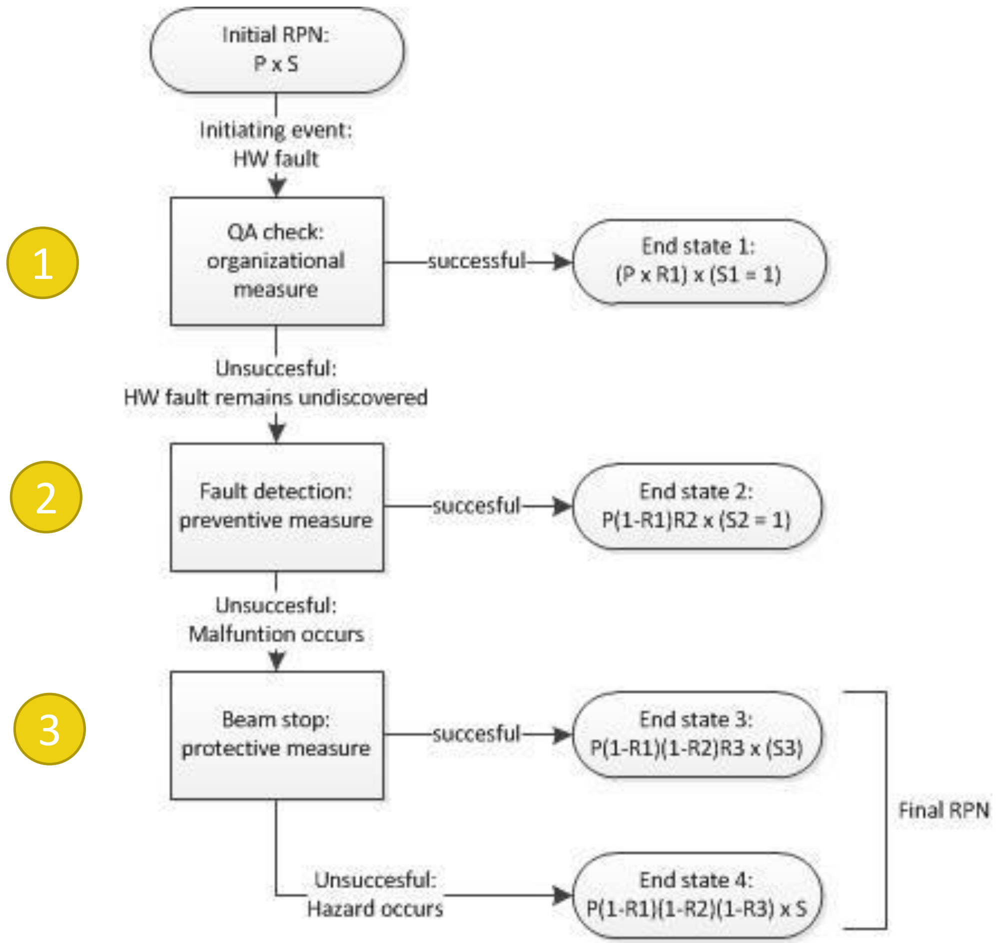


INSIGHTS
PROTECTIVE MEASURES



INSIGHTS
RISK REDUCTION PROCESS

- **Risk mitigations**
  1. Organizational
  2. Preventive
  3. Protective



FACTS AND FIGURES
RISK CONTROL MEASURES

Architecture	Number of instances	%
Inherent safety, preventive	32	25%
Multiple preventive	25	20%
Organizational, Inherent safety, preventive	20	16%
Preventive, protective	18	14%
Organizational, protective	8	6%
Multiple protective	8	6%
Inherent safety	7	5%
Organizational	7	5%
Inherent safety, organizational, preventive, protective	3	3%

RM PROCESS
STEP 3: FMECA

Effect
- Wrong ion species
- Wrong beam intensity, position, energy…
- Unintended beam
- Wrong radiation head

2 – hazardous situation < causal chain>

4 – initial risk

6 – risk control measures

Risk ID	Condition (optional)	Hazard	Cause	Failure Mode	Effect	Harm	Who	Initial Probability	Initial Severity	Initial RPN	Final Probability	Final Severity	Final RPN	Risk mitigation (control) measure	Risk mitigation ID	Type
Chopper-HZ-001…4	Single Fault Condition	Missed beam stop (spot termination fault)	Several causes	Failure of the PKC, current stays ON	Unable to switch the beam off	Overdose	Patient	4	5	20	1	5	5	QA check	Chopper-HZ-001_M01	Organizational measure
														Internal diagnostics by the chopper power converter, which vetoes the chopper to operate in case of detected fault	Chopper-HZ-001_M02	Preventive
														DDS monitors non expected beam and trigger an ILK to the chopper and the beam stopper	Chopper-HZ-001_M03	Protective

1 – Hazardous situation

3 – the harm

5 – residual risk

Cause (single fault)
- Hardware, software
- Communication and synchronization
- Configuration, calibration, settings

Harm

Overdose in the intended area

Wrong dose or dose distribution in the unintended area

<u>Other side effects</u>

Waiting time and treatment interruption

RISK MANAGEMENT FOR MAPTA
SAFETY BY DESIGN AND RISK CONTROL

Single fault safe principle: a single fault cannot lead to an hazardous situation for the patient

- **Risk control options are…**
  - Organizational measures and information for safety
  - Inherent safety by design
  - Preventive measures
  - Protective measures

- **Safety by design**
  - Fail-safe behavior,
  - Independency of risk control measures,
  - Acknowledgement of a safety action,
  - Alternative means or independent back-ups,

RM PROCESS
STEP 1: HAZARDS VS. CATEGORIES OF RISK

- **EN ISO 14971** accounts for 6 categories of risk and several hazards (all hazards approach)

CATEGORIES

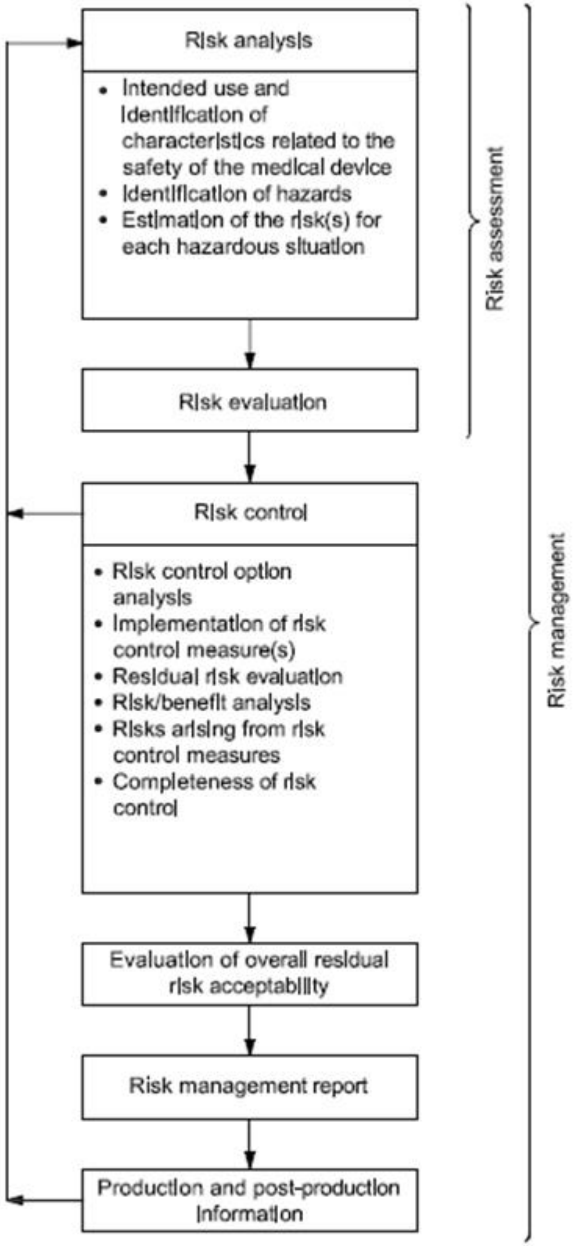
HAZARDS

	Patient	Personnel	User	3rd person	Environment	Equipment
Energy						
Mechanical						
Bio-chemical						
Operation						
Information						
…						

RM PROCESS

Risk is a process of continuous identification of hazards, estimate of related risks and evaluation throughout the MD lifetime

EN ISO 14971:2012
Application of RM to medical devices



INSIGHTS
PROBABILITIES AND SEVERITIES

QA check: organizational

Probability	Severity 1	2	3	4	5
6	4x1	4x2	4x3	4x4	4x5
5	3x1	3x2	3x3	3x4	3x5
4	3x1	3x2	3x3	3x4	**3x5**
3	2x1	2x2	2x3	2x4	2x5
2	1x1	1x2	1x3	1x4	1x5
1	1x1	1x2	1x3	1x4	1x5

Initial risk
RPN = 4 x 5

Diagnostics: preventive

Probability	Severity 1	2	3	4	5
6	3x1	3x2	3x3	3x4	3x5
5	3x1	3x2	3x3	3x4	3x5
4	2x1	2x2	2x3	2x4	2x5
3	2x1	2x2	2x3	2x4	**2x5**
2	1x1	1x2	1x3	1x4	1x5
1	1x1	1x2	1x3	1x4	1x5

Intermediate risk
RPN = 3 x 5

Beam monitor: protective

Probability	Severity 1	2	3	4	5
6	3x1	3x2	3x3	3x4	3x5
5	3x1	3x2	3x3	3x4	3x5
4	2x1	2x2	2x3	2x4	2x5
3	2x1	2x2	2x3	2x4	2x5
2	1x1	1x2	1x3	1x4	**1x5**
1	1x1	1x2	1x3	1x4	1x5

Final risk
RPN = 1 x 5