

Safety concept and scope for WP Controls

Fabian Moser
February 5, 2010

Introduction

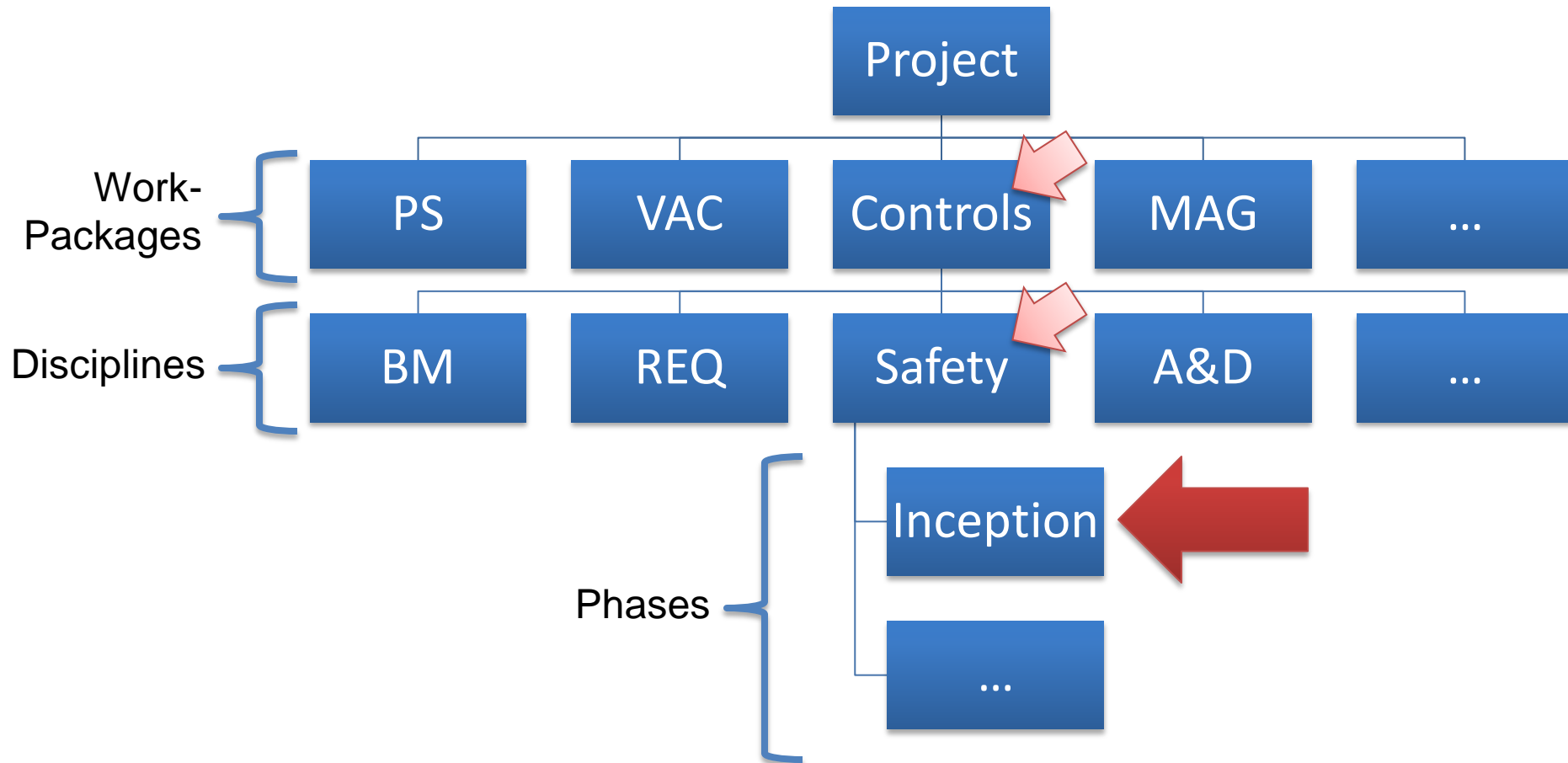
What is this presentation about?

- Preparatory work for strategy on safety in control system
- Identification of required quality assurance level for development of control system
- Preparatory work required for beam verification system

What can audience expect?

- Introduction into control system safety strategy
- Summary of first steps of the process

Relation to overall project



Overview

Safety strategy

- Plan
- Progress

Step 1: Safety Concept

- Overview
- Summary of contents

Step 2: Safety Scope

- Overview
- Summary of contents

Conclusions and Outlook

Safety strategy

Hazard and risk analysis

```
graph TD; A[Hazard and risk analysis] --> B[Safety requirements]; B --> C[Safety-related systems];
```

Safety requirements

Safety-related systems

Hazard and risk analysis

Concept

- Develop understanding of the plant concept and its environment
- *Based on conceptual design information*
- **Identify top-level hazards – emerge from goals** (Preliminary Hazard List)

Scope

- Determine boundary of controlled equipment and control system
- *Specify scope of hazard and risk analysis*
- **Identify system-level hazards – emerge from design** (Preliminary Hazard Analysis)

Analysis

- Determine all hazards and hazardous events
- *Determine the risks associated with the hazards and hazardous events (probability for harms to materialize and severity of their impacts)*
- For all modes of operation
- For all reasonably foreseeable circumstances

Progress

Concept

- Develop understanding of the plant concept and its environment
- *Based on conceptual design information*
- **Identify top-level hazards – emerge from goals** (Preliminary Hazard List)

Scope

- Determine boundary of controlled equipment and control system
- *Specify scope of hazard and risk analysis*
- **Identify system-level hazards – emerge from design** (Preliminary Hazard Analysis)

Analysis

- Determine all hazards and hazardous events
- *Determine the risks associated with the hazards and hazardous events (probability for harms to materialize and severity of their impacts)*
- For all modes of operation
- For all reasonably foreseeable circumstances

Step 1: Safety Concept document

PM-090630-a-FMO

Sources of hazards

- List of physical, biological or chemical agents, properties of the environment or activities

Preliminary Hazard List

- Identifies potential hazards and mishaps
- Structured approach with different perspectives

Safety regulations

- Summary of applicable directives

Sources of hazards

Comprehensive list has been created

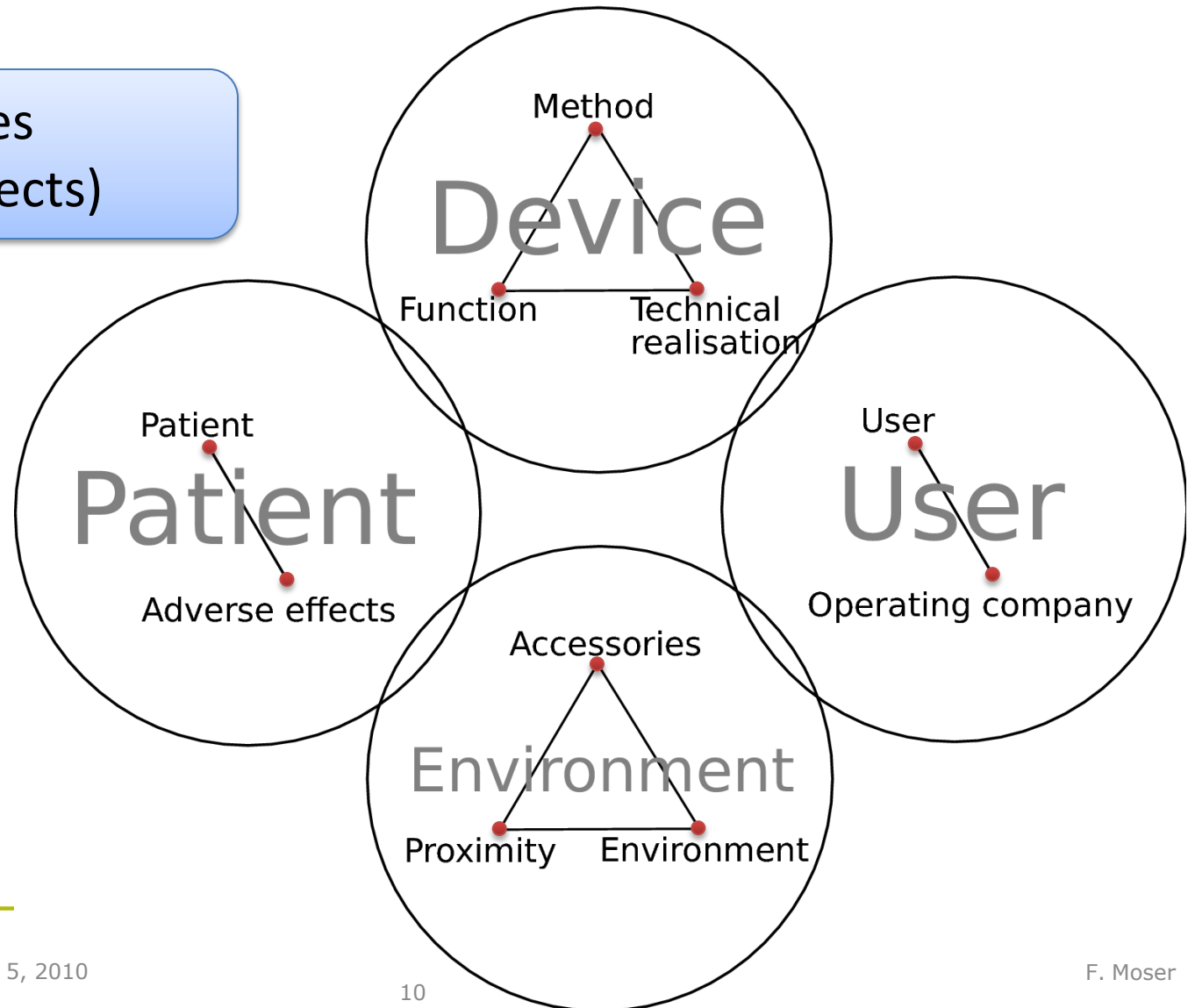
Identified sources (agents), characteristics and defining mishaps

Examples:

Carbon beam (ionizing radiation)	12C^{4+} , 400 MeV/u, 10^9 s^{-1}	Tissue damage
Source cooling system (hydraulic pressure)	20 bar	Blast
Dipole MBV-F (lifted weight)	75000 kg	Strike

Structure of Preliminary Hazard List

Perspectives
(safety aspects)



Content of Preliminary Hazard List

Comprehensive list of top-level hazards

Under normal and single-fault conditions

Examples:

PHL-M01	High energy radiation	NC	Material wear-out, Activation, Electronics damage, Chemical reactions
PHL-T20	Beam stopping failure	SFC	Treatment incorrect, Treatment ineffective, Equipment damage
PHL-P06	Unexpected anatomy	SFC	Treatment incorrect, Treatment ineffective

Safety regulations

Medical device directive applies to all parts whose purpose is medical treatment

- Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, OJ L 169, 12. July 1993, S. 1-43.

Standards serve as conformity guidelines

- EN ISO 14971:2007 Medical devices – Application of risk management to medical devices
- EN ISO 13485:2003 Medical devices – Quality management systems — Requirements for regulatory purposes
- EN ISO 14155:2003 Clinical investigation of medical devices for human subjects

Consequences of the Activity

Basis for identification and separation of safety-relevant subsystems created

Comprehensive list of top-level hazards allowed scope definition

Understood regulatory framework

Development process defined keeping regulatory framework in mind

Quality assurance applied throughout entire lifecycle of control system development

Increased requirements on contractor selection

Step 2: Safety Scope document (REF)

PM-100114-a-FMO

Based on Safety Concept and the Preliminary Hazard List

Selects in-scope hazards from PHL

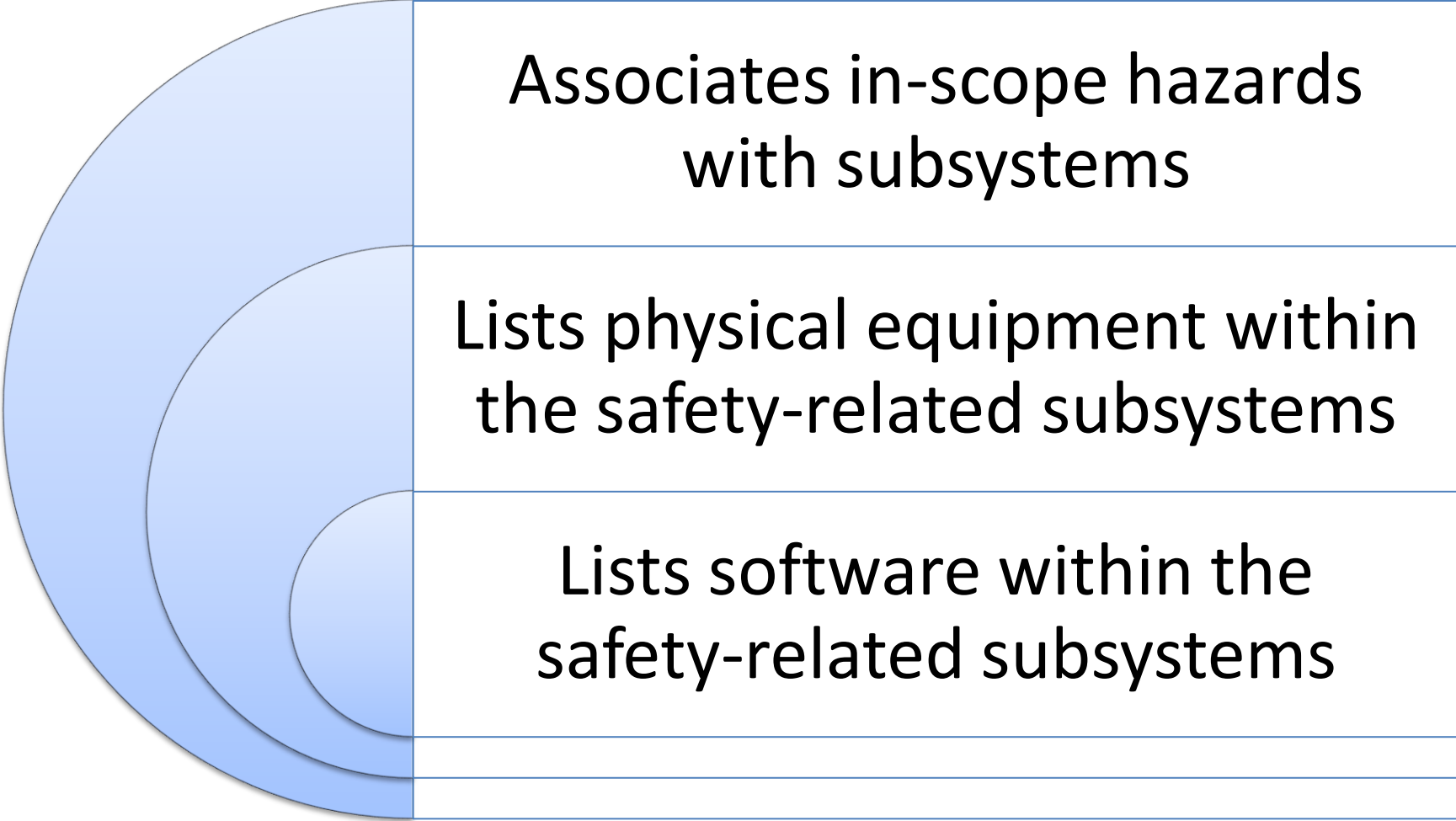
- Hazards that are relevant for medical application

Defines boundary of the Medical Device

- Identifies parts participating in medical treatment and foreseen safety functions

Specifies scope of the hazard and risk analysis

Equipment in scope (ongoing)

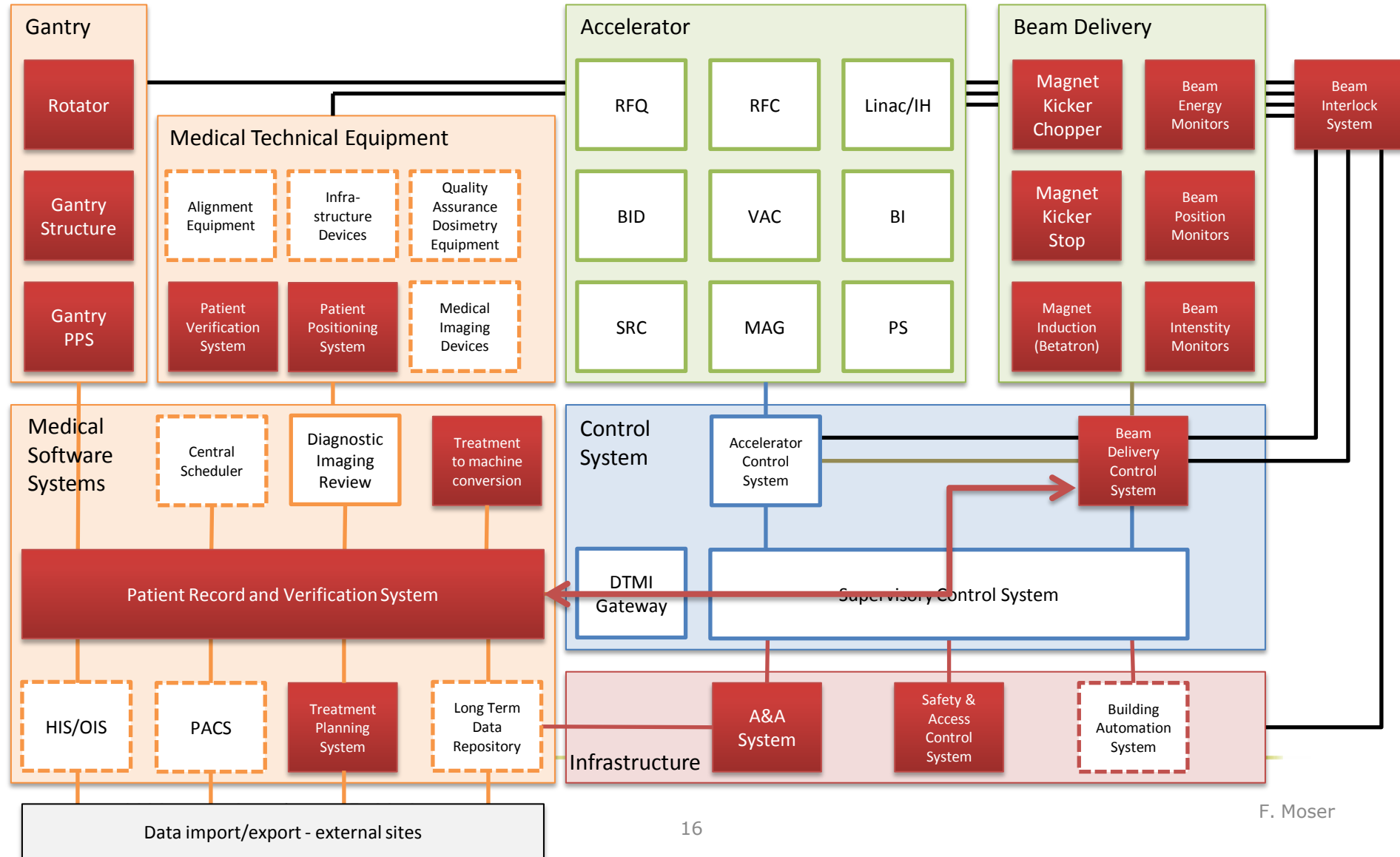


Associates in-scope hazards
with subsystems

Lists physical equipment within
the safety-related subsystems

Lists software within the
safety-related subsystems

Preliminary Scope Map



Events in scope

Comprehensive list of accident-initiating event types

- Component failures
- Configuration faults
- Timing failures
- ...

Comprehensive list of external events

- Electrical power failure
- Patient identification failure
- Ion beam failure
- ...

Required next steps

Check and complement concept & scope

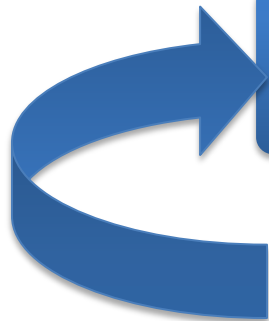
Review and approve concept & scope

Perform risk analysis on existing design

Refine risk analysis

Refine design of safety-related systems

Requires additional manpower



Conclusions

Initiated risk management process

Identified need for top-down approach

- Project-wide WP covering process
- Coordination of individual activities

Performed preparatory work in order to elaborate beam-verification requirements