Design of safety critical systems

Michal Kalinowski TE-MPE-MI

TE-MPE Annual Meeting, 25.01.2024

Machine Interlocks Section

SMP

Safe **M**achine **P**arameter System

PIC

Powering **I**nterlock **C**ontroller

BIS

Beam **I**nterlock **S**ystem

MI

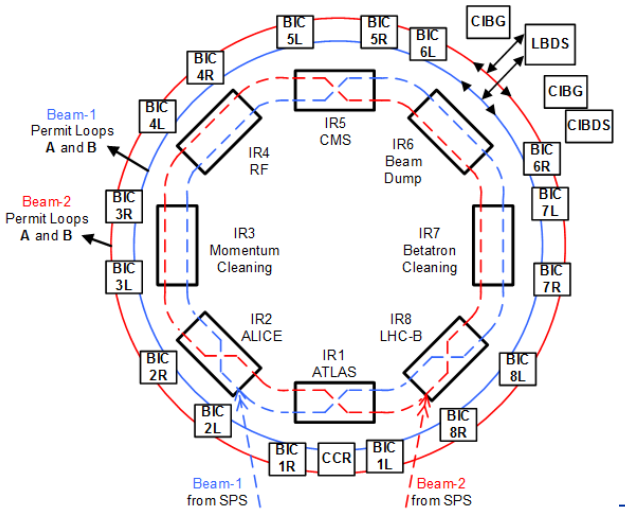
Machine **I**nterlocks Section

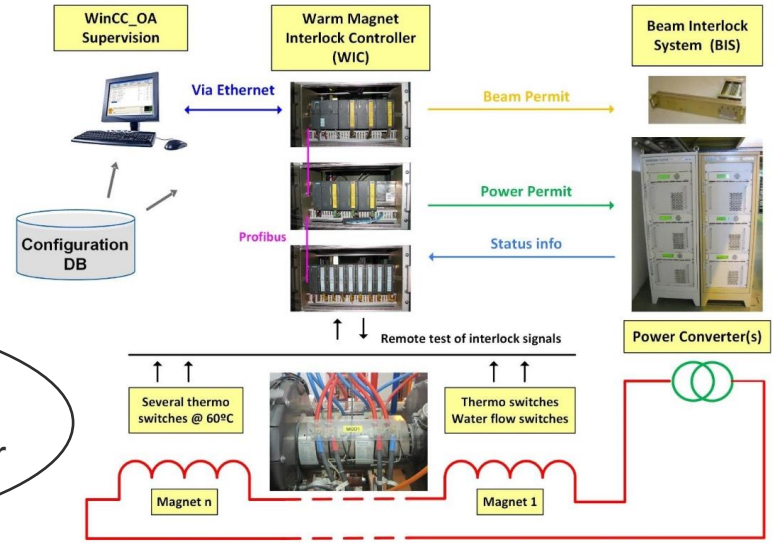
FMCM

Fast **M**agnet **C**urrent change **M**onitors

WIC

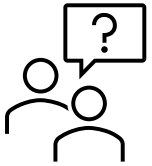
Warm magnet **I**nterlock **C**ontroller





Safety critical system – what it is?

What defines a safety critical system?

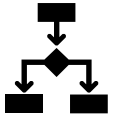


- High consequence of failure (loss of life, injury, environmental damage, high financial loss)



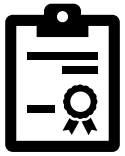
- Thorough risk analysis

- Dependability and availability



- Stringent standards and regulations (e. g. IEC 61508)

- Independent verification and validation

How to design Safety Critical System?

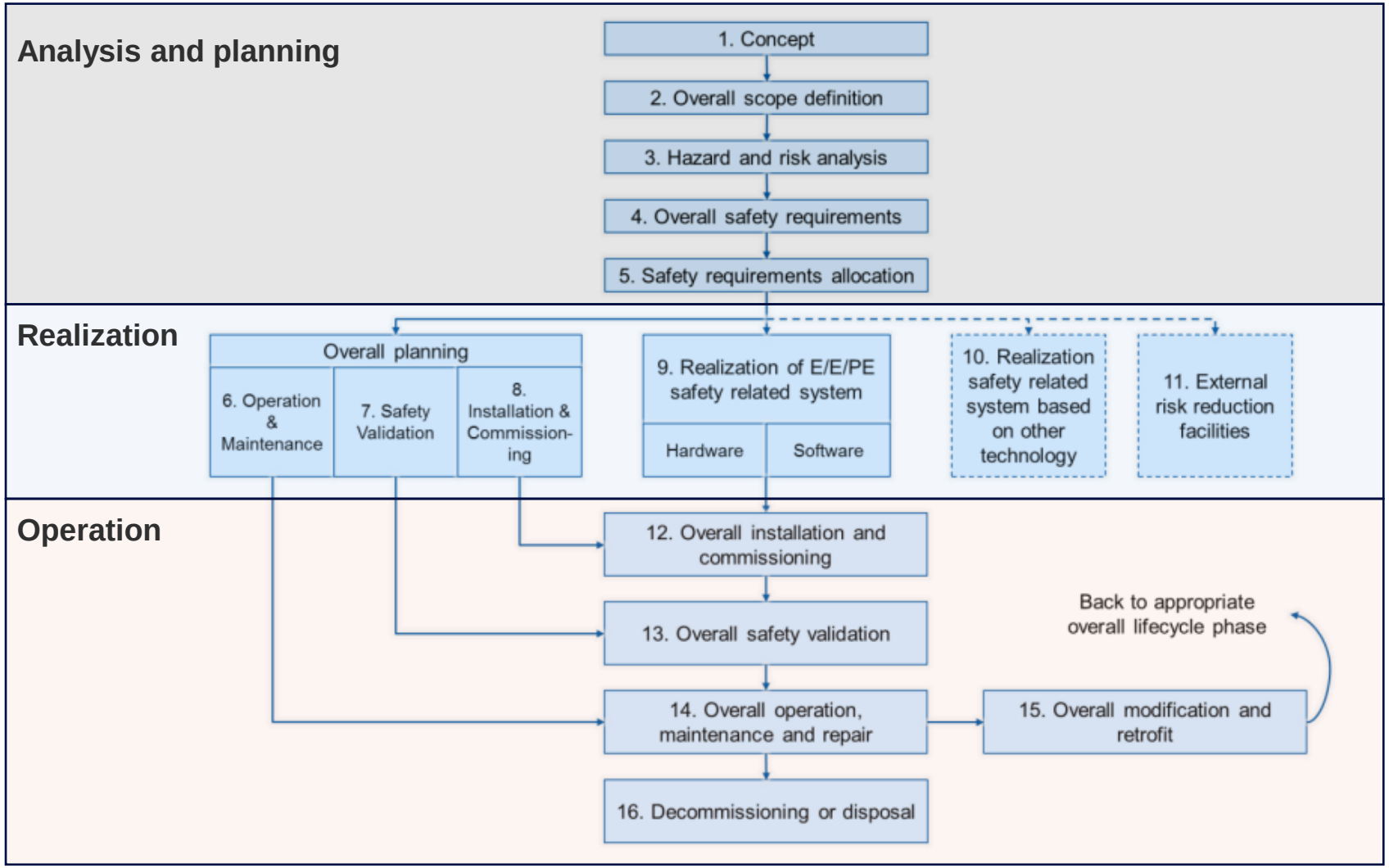


Figure 4-3: Safety Life Cycle (from IEC 61508)

What does the MI do, to ensure the reliability?

Clear and exhaustive specifications of the project

Mars Climate Orbiter (1999)

Metric ≠ Imperial

What does the MI do, to ensure the reliability?

Clear and exhaustive specifications of the project

↓

Thorough risk and hazards analysis, definition of safety requirements

With help of the MPE-CB colleagues

Boeing 737 MAX (2018, 2019)

Single point of failure

What does the MI do, to ensure the reliability?

Clear and exhaustive specifications of the project

↓

Thorough risk and hazards analysis, definition of safety requirements

↓

With help of the MPE-CB colleagues

Design of the system

Reliability analysis → *Dependability*, *Availability*

Space Shuttle Challenger (1986)

Incorrect design of O-ring seal

What does the MI do, to ensure the reliability?

Clear and exhaustive specifications of the project

↓

Thorough risk and hazards analysis, definition of safety requirements

↓

With help of the MPE-CB colleagues

Design of the system

Reliability analysis → *Dependability*, *Availability*

↓

Testing and validation

Continuous integration

↓

Commissioning of the system

Ariane 5 Flight 501 (1996)

Use of previous software version without testing

What does the MI do, to ensure the reliability?

Clear and exhaustive specifications of the project

↓

Thorough risk and hazards analysis, definition of safety requirements

↓

With help of the MPE-CB colleagues

Design of the system

Reliability analysis → *Dependability*, *Availability*

↓

Testing and validation

Continuous integration

↓

Commissioning of the system

↓

Operation and maintenance

Experts' advice — *Trainings*

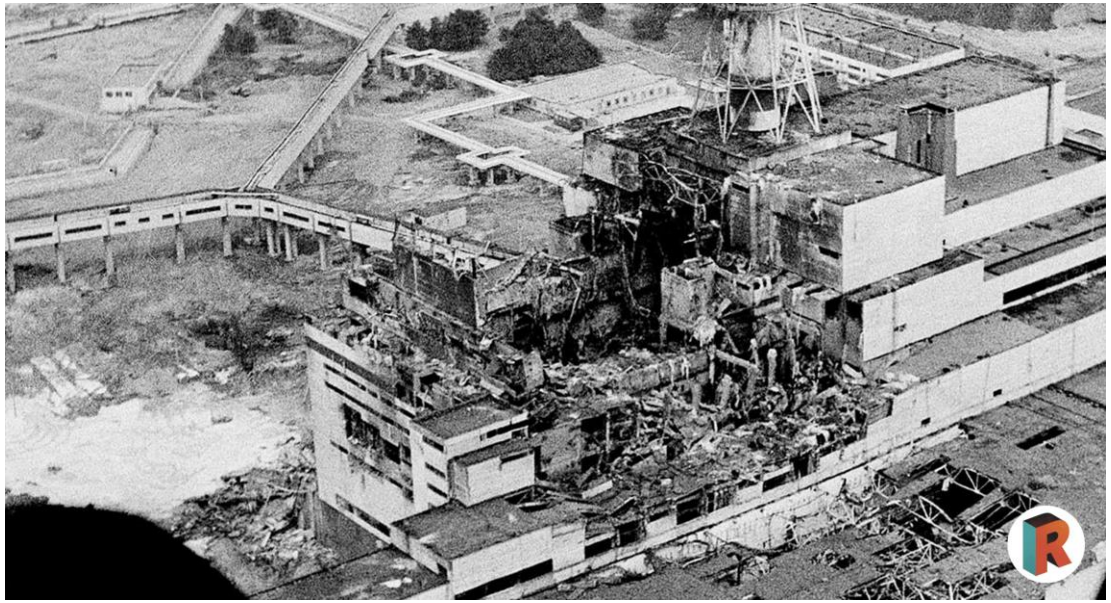
Procedures — *Periodic testing*

Chernobyl Disaster (1986)

Unprepared shift

Not clear procedures

Incorrect advising



What does the MI do, to ensure the reliability?

Clear and exhaustive specifications of the project

↓

Thorough risk and hazards analysis, definition of safety requirements

↓

With help of the MPE-CB colleagues

Design of the system

Reliability analysis → *Dependability*, *Availability*

↓

Testing and validation

Continuous integration

↓

Commissioning of the system

↓

Operation and maintenance

Experts' advice — *Trainings*

Procedures — *Periodic testing*

Conclusions

- A failure of a safety critical system can be catastrophic or in MI case – can destroy parts of the machine
- During development of such a system, it is mandatory to follow a strict procedure
- While designing a system, you should already think about periodic test possibility
- Validation and testing as well as commissioning are crucial
- Clear procedures and well-trained operators reinforce the safe operation


MI
Machine Interlocks
Section
PROTECTING THE MACHINE SINCE
2003

home.cern