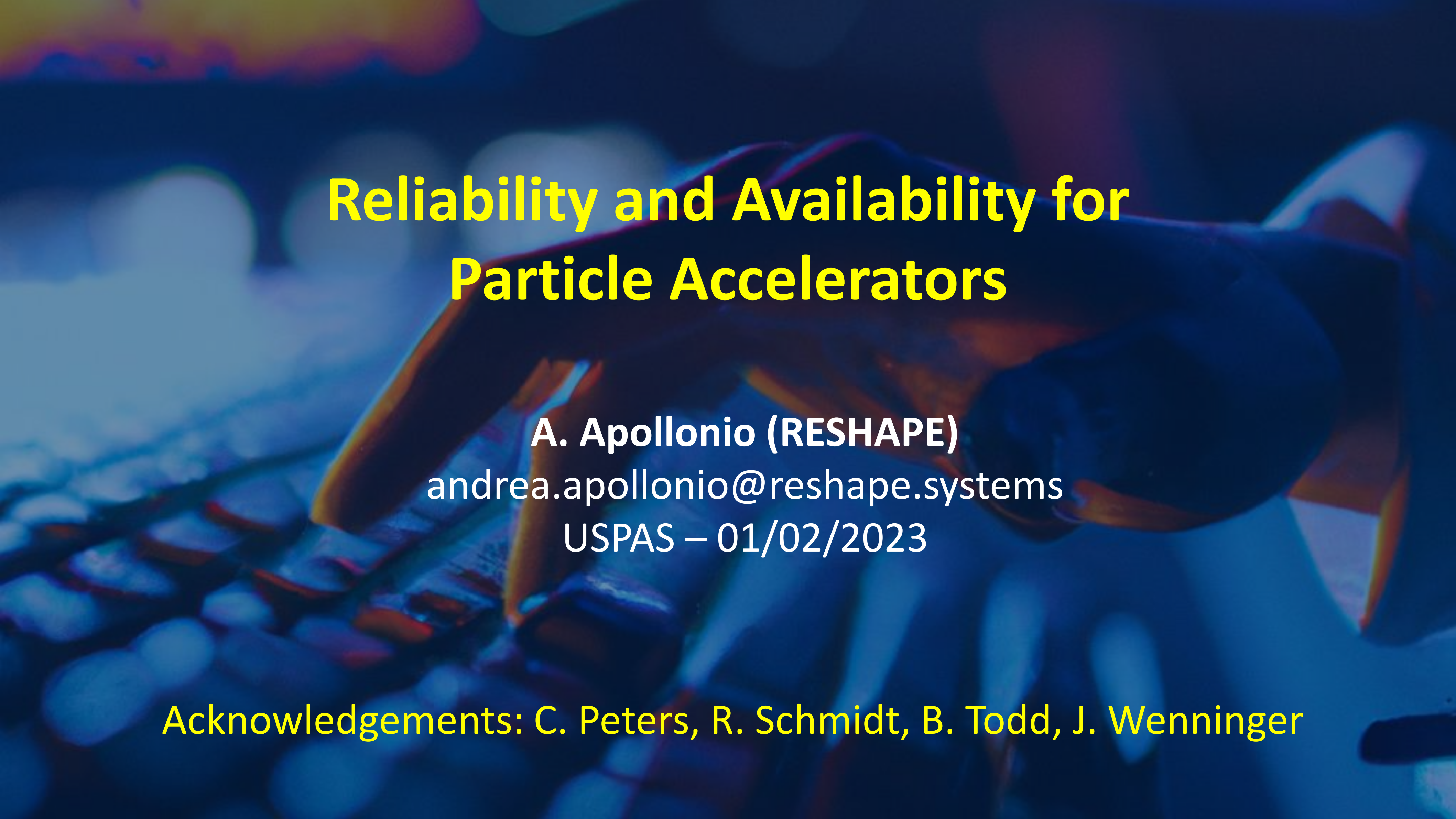


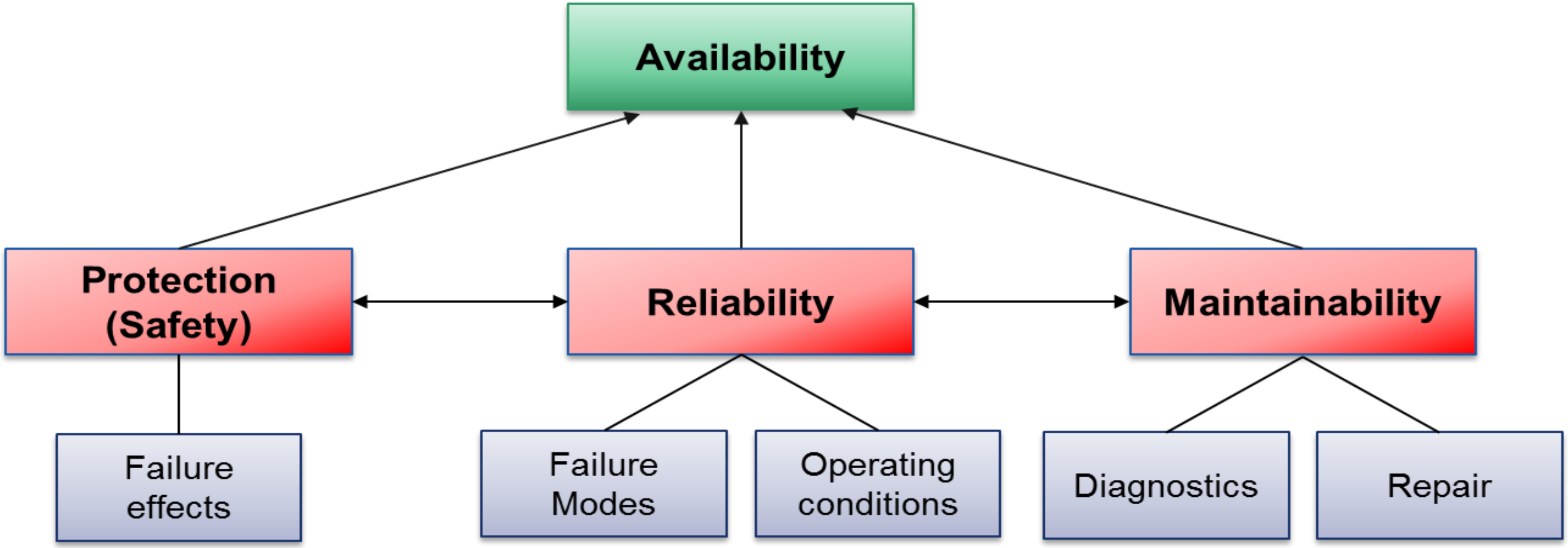
Reliability and Availability for Particle Accelerators

A. Apollonio (RESHAPE)
andrea.apollonio@reshape.systems

USPAS – 01/02/2023

Acknowledgements: C. Peters, R. Schmidt, B. Todd, J. Wenninger

RAMS/Outline



NB: in the context of particle accelerators, we speak about 'Protection' rather than 'Safety', if no personnel is involved

Basic Definitions

- **Reliability (0-1)** is the probability that a system does not fail during a defined period of time under given functional and environmental conditions
  - Example of reliability specification: “An accelerator must have a reliability of 60 % after 100 h in operation, at a current of 40 mA”

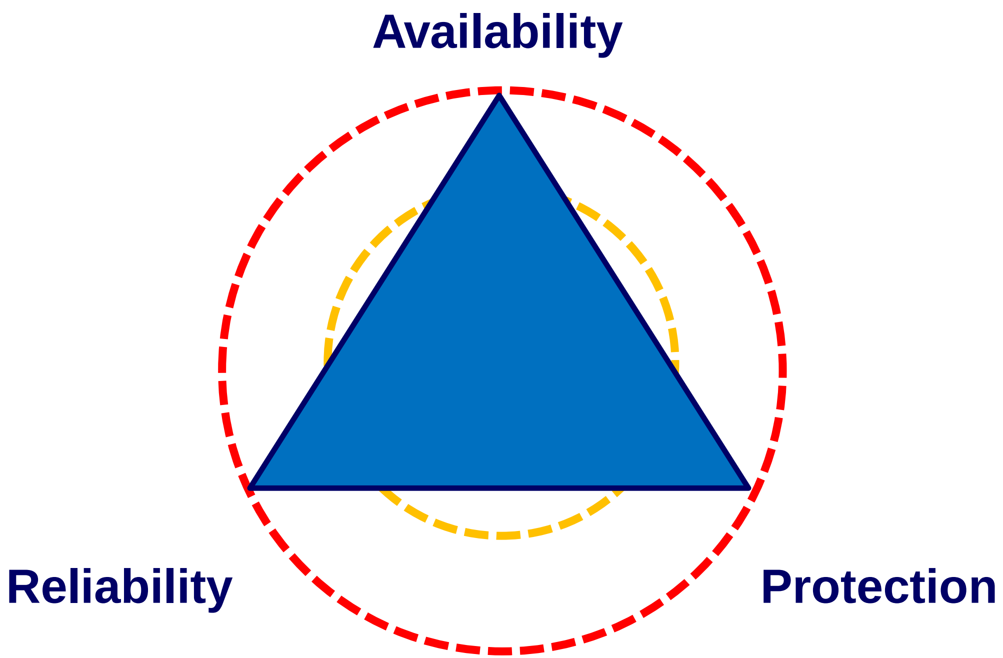
- **Availability (0-1)** is the probability that a system in a functional state at given point in time
  - Example of availability specification: “An accelerator must ensure beam delivery to a target for 90 % of the scheduled time for operation”

Clearly we want highly available and highly reliable accelerators → questions to be answered in this lecture:

What are the factors that limit their reliability and availability?

How can these be quantified systematically?

Metrics



Availability

Reliability

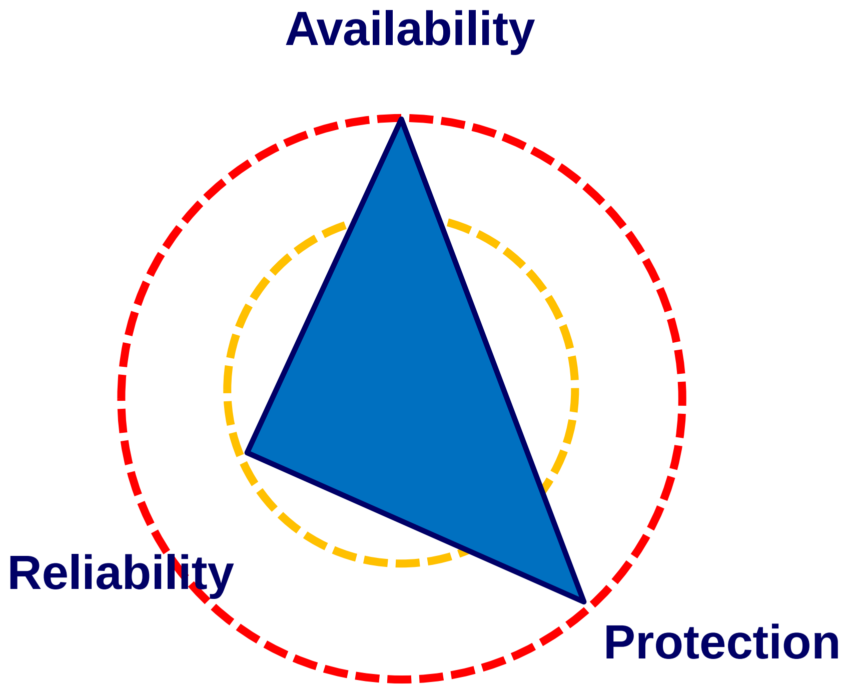
Protection

Low Importance

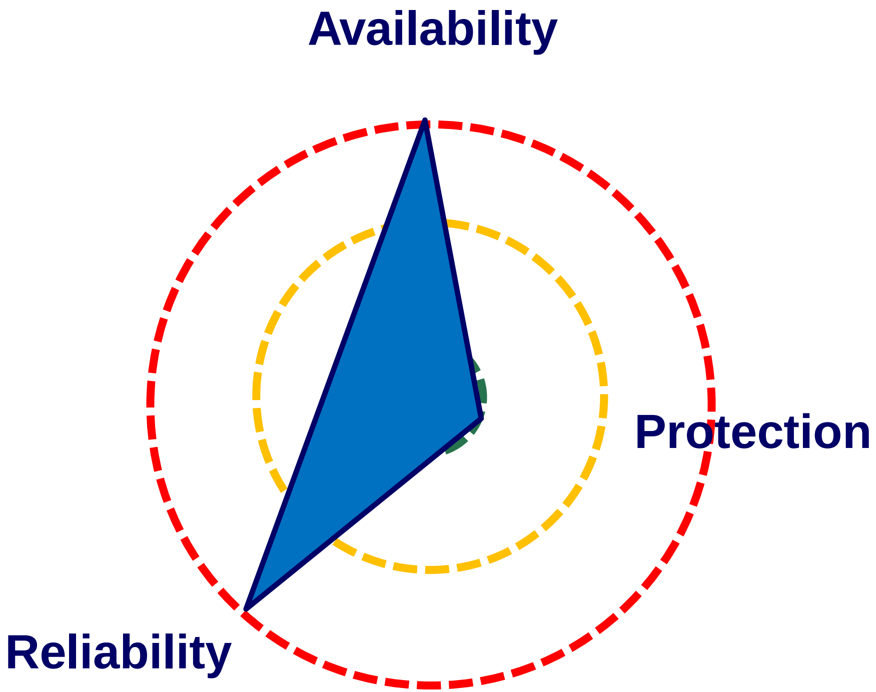
Relative Importance

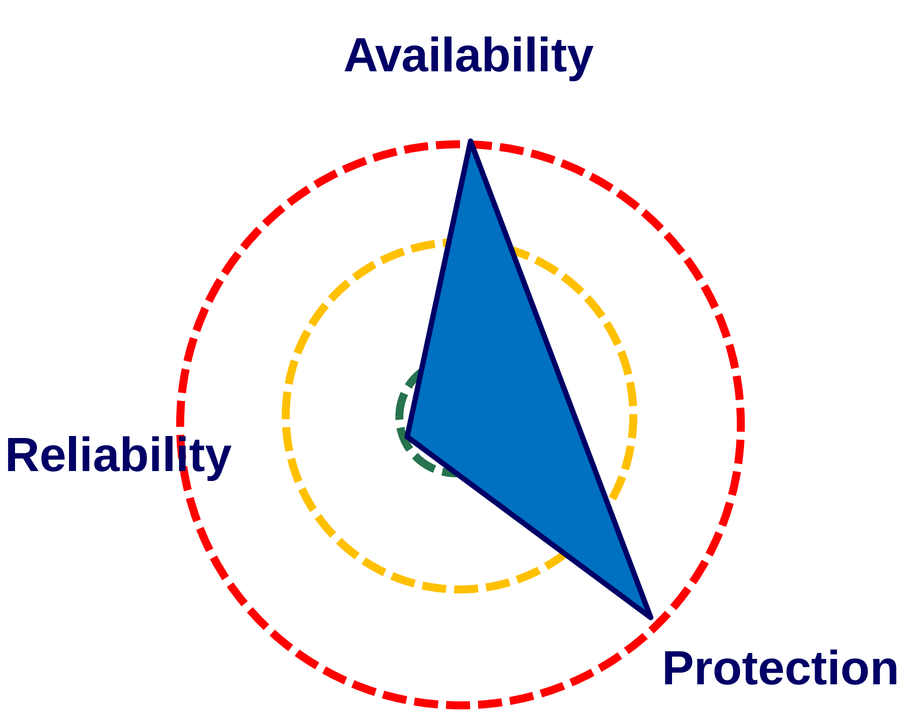
High Importance

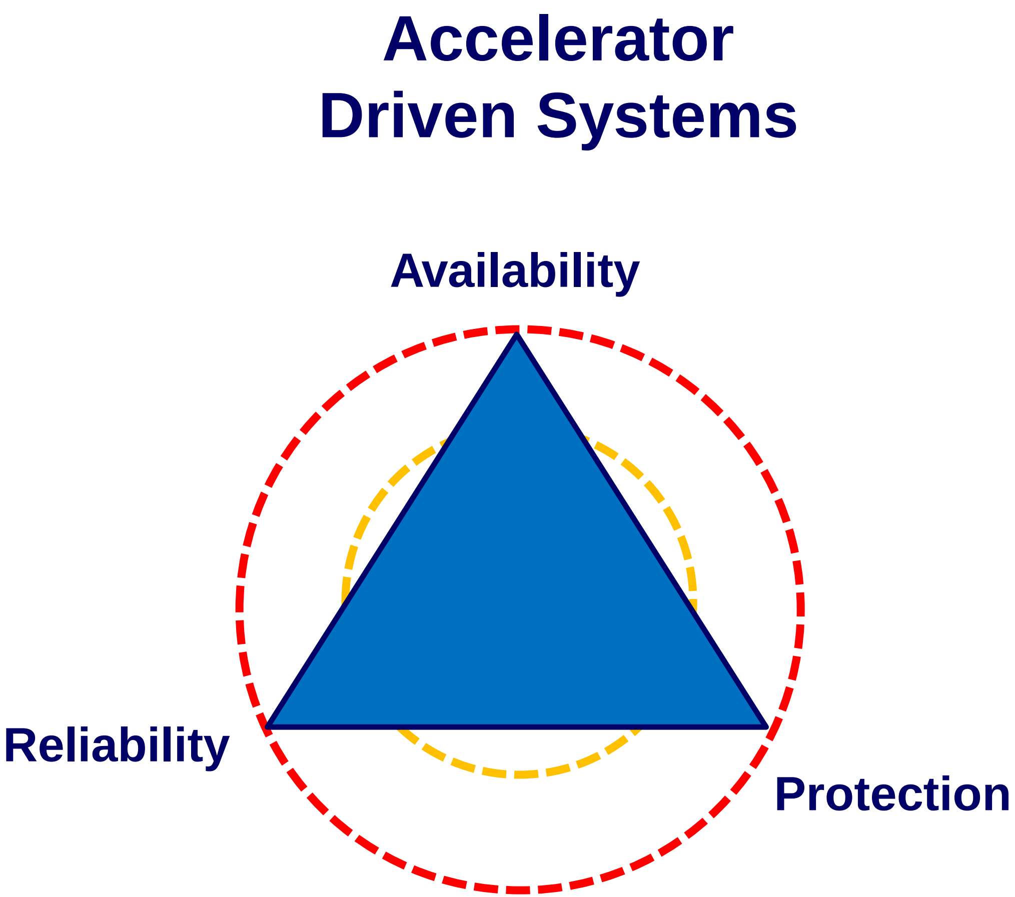
Large-Scale Colliders



Synchrotron Light Sources



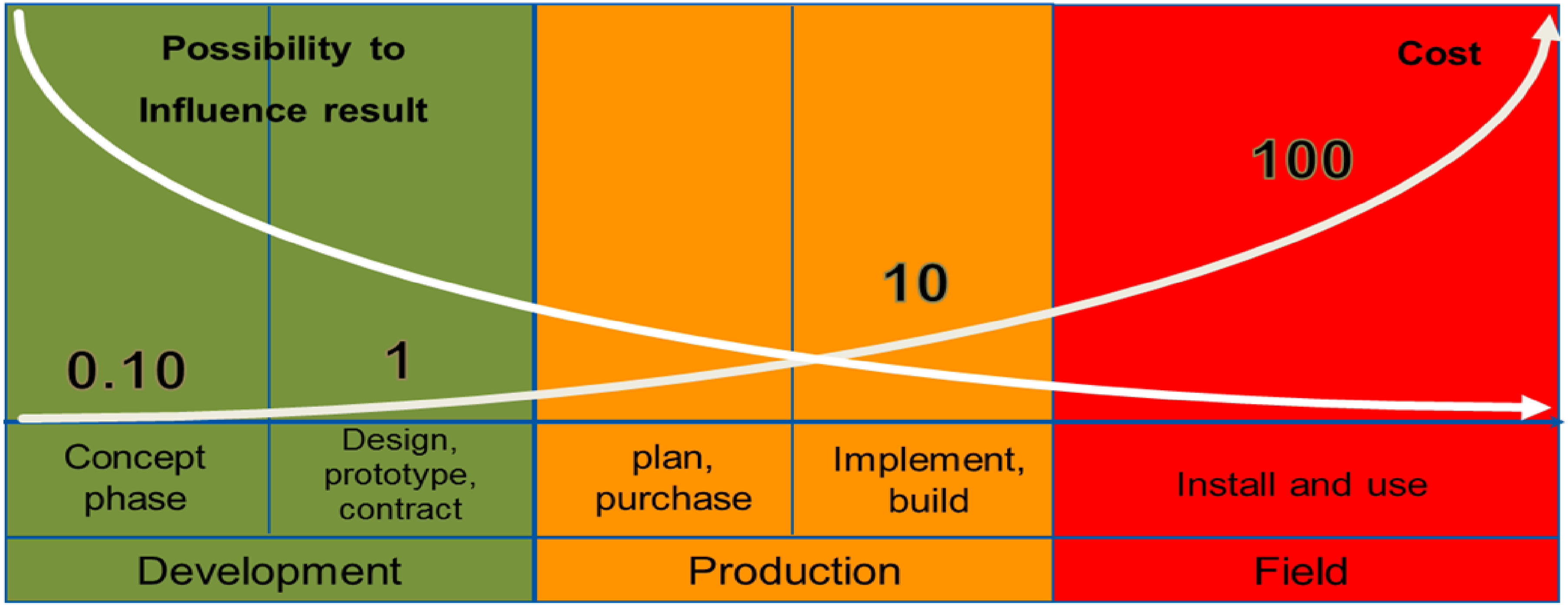

Spallation Neutron Sources
Availability
Reliability
Protection


Accelerator Driven Systems
Availability
Reliability
Protection

Importance of Reliability Analyses

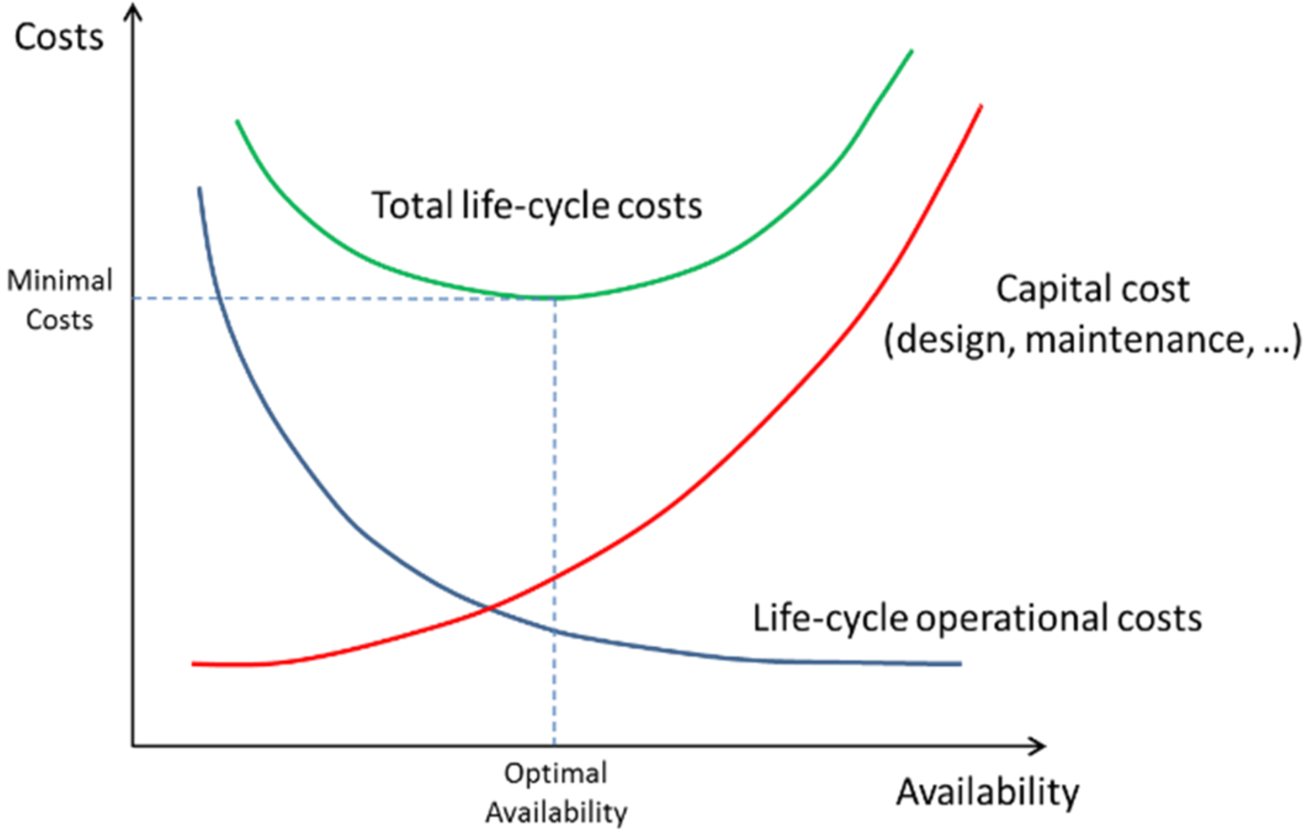
Prof. Dr. B. Bertsche, Dr. P. Zeiler, T. Herzig, IMA, Universität Stuttgart, CERN Reliability Training, 2016

- Product/Accelerator Lifecycle



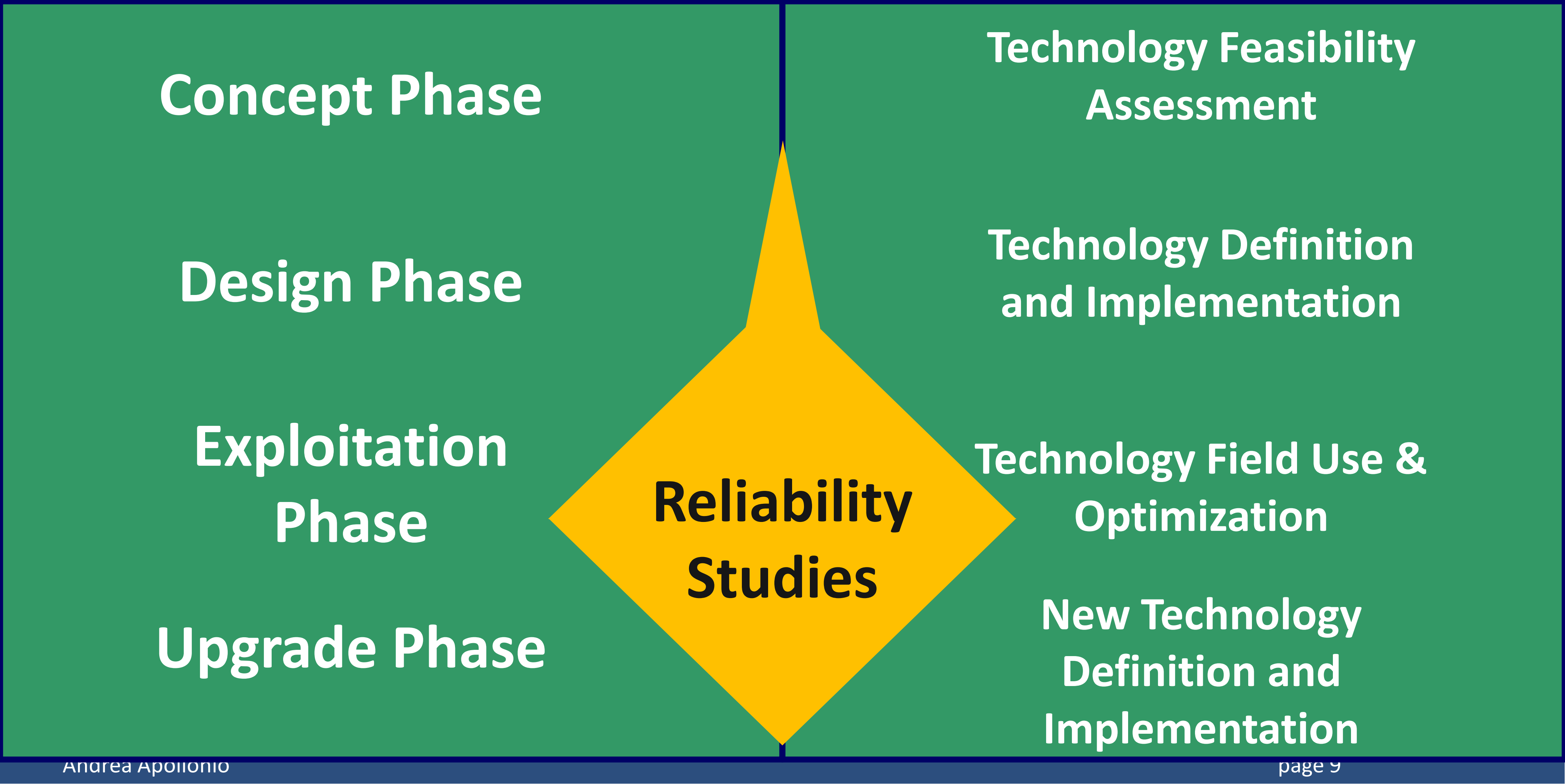
- The earlier reliability constraints are included in the design, the more effective the resulting measures will be

Importance of Reliability Analyses



- Given a target performance reach (neutron fluence, number of patients treated, luminosity production, …), an **optimal balance between capital costs and operation costs** must be found

Today: Dependability Studies



Concept Phase

Design Phase

Exploitation Phase

Upgrade Phase

Reliability Studies

Technology Feasibility Assessment

Technology Definition and Implementation

Technology Field Use & Optimization

New Technology Definition and Implementation

Future: Dependability Studies

Reliability Studies

Concept Phase — Technology Feasibility Assessment

Design Phase — Technology Definition and Implementation

Exploitation Phase — Technology Field Use & Optimization

Upgrade Phase — New Technology Definition and Implementation

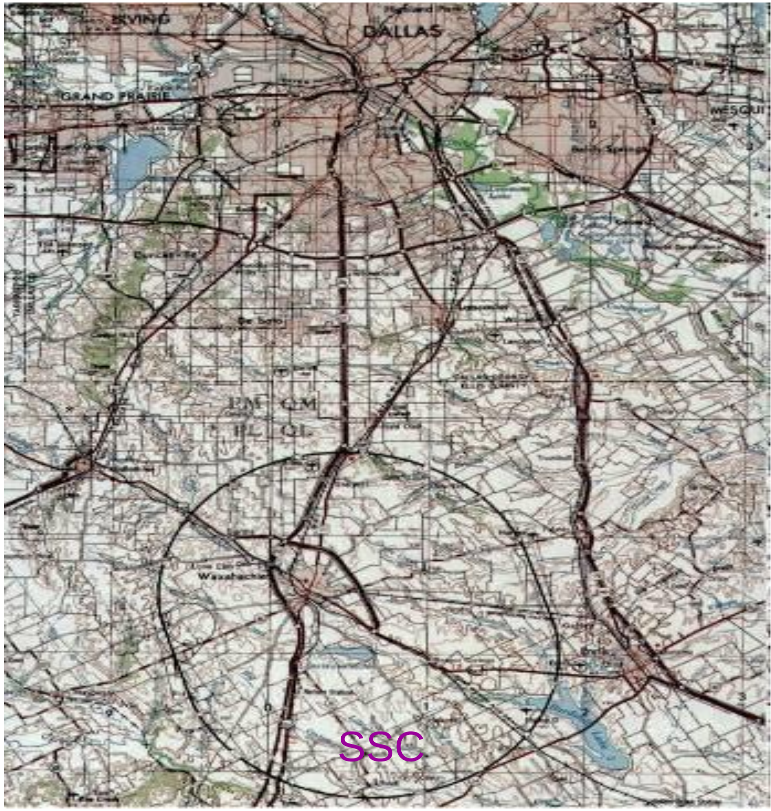
Risk

Risks for Particle Accelerators

- **Not to complete** the construction of the accelerator
  - Happened to other projects, the most expensive was the Superconducting Super Collider in Texas / USA with a length of ~80 km
  - Cost increase from 4.4 Billion US$ to 12 Billion US$, US congress stopped the project in 1993 after having invested more the 2 Billion US$

- **Not** to be able **to operate** the accelerator

- **Damage** to the accelerator **beyond repair** due to an accident



Energy stored in the LHC

Picture source: http://en.wikipedia.org/wiki/File:Alstom_AGV_Cerhenice_img_0365.jpg
Shared as: http://creativecommons.org/licenses/by-sa/3.0/deed.en

Picture source: http://militarytimes.com/blogs/scoopdeck/2010/07/07/the-airstrike-that-never-happened/
Shared as: public domain

$3 \cdot 10^{14}$ protons in each beam

Kinetic Energy of 200 m Train at 155 km/h ≈ 360 MJoule

Stored energy per beam is 360 MJ

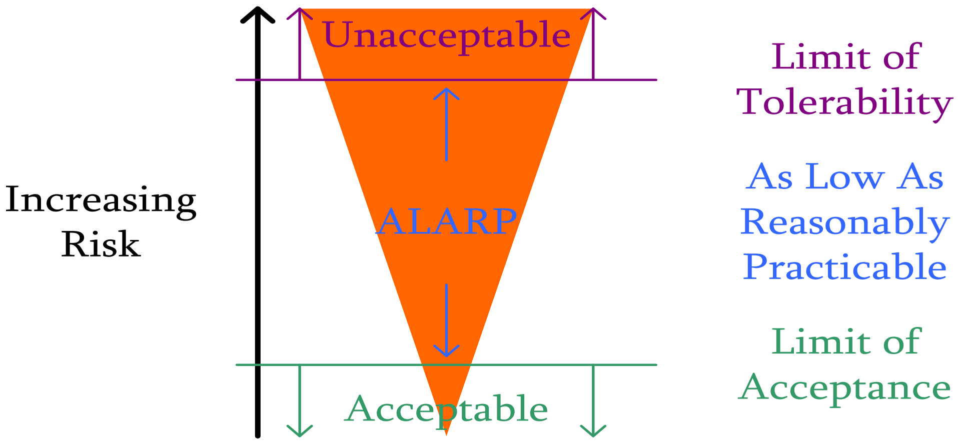
Stored energy in the magnet circuits is 9 GJoule

Kinetic Energy of Aircraft Carrier at 50 km/h ≈ 9 GJoule

….can melt 14 tons of copper

Risk Assessment (1/2)

B. Todd, M. Kwiatkowski, "Risk and Machine Protection for Stored Magnetic and Beam Energies"



- Risk is the product of the probability of occurrence of an undesired event x its impact (financial, reputation, downtime,…)
- 'Acceptable' or 'Unacceptable' risk depends on the context!

Different for user-oriented facilities, medical accelerators, fundamental research,…

Risk Assessment: Example (2/2)

IMPACT

FREQUENCY

Risk Assessment: Example (2/2)

IMPACT

FREQUENCY

	Catastrophic	Major	Moderate	Low
Cost [MCHF]	> 50	1-50	0.1-1	0-0.1
Downtime [days]	> 180	20-180	3-20	0-3

Risk Assessment: Example (2/2)

			IMPACT			
		Per year	Catastrophic	Major	Moderate	Low
FREQUENCY	Frequent	1				
	Probable	0.1				
	Occasional	0.01				
	Remote	0.001				
	Improbable	0.0001				
	Not credible	0.00001				
	Cost [MCHF]		> 50	1-50	0.1-1	0-0.1
	Downtime [days]		> 180	20-180	3-20	0-3

Risk Assessment: Example (2/2)

IMPACT

FREQUENCY

	Per year	Catastrophic	Major	Moderate	Low
Frequent	1				
Probable	0.1				
Occasional	0.01				
Remote	0.001				
Improbable	0.0001				
Not credible	0.00001				
Cost [MCHF]		> 50	1-50	0.1-1	0-0.1
Downtime [days]		> 180	20-180	3-20	0-3

- Assessment of the required level of risk reduction (1-4) for different failure scenarios

Risk Assessment: Example (2/2)

			IMPACT			
		Per year	Catastrophic	Major	Moderate	Low
FREQUENCY	Frequent	1				
	Probable	0.1				
	Occasional	0.01				
	Remote	0.001				
	Improbable	0.0001				
	Not credible	0.00001				0
	Cost [MCHF]		> 50	1-50	0.1-1	0-0.1
	Downtime [days]		> 180	20-180	3-20	0-3

- Assessment of the required level of risk reduction (1-4) for different failure scenarios

Risk Assessment: Example (2/2)

			IMPACT			
		Per year	**Catastrophic**	**Major**	**Moderate**	**Low**
FREQUENCY	Frequent	1	4			
	Probable	0.1				
	Occasional	0.01				
	Remote	0.001				
	Improbable	0.0001				
	Not credible	0.00001				0
	Cost [MCHF]		> 50	1-50	0.1-1	0-0.1
	Downtime [days]		> 180	20-180	3-20	0-3

- Assessment of the required level of risk reduction (1-4) for different failure scenarios

Risk Assessment: Example (2/2)

Machine Protection Concern IMPACT Availability Concern

FREQUENCY

	Per year	Catastrophic	Major	Moderate	Low
Frequent	1	4	3	3	2
Probable	0.1	3	3	3	2
Occasional	0.01	3	3	2	1
Remote	0.001	3	2	2	1
Improbable	0.0001	3	2	1	0
Not credible	0.00001	2	1	0	0
Cost [MCHF]		> 50	1-50	0.1-1	0-0.1
Downtime [days]		> 180	20-180	3-20	0-3

- Assessment of the required level of risk reduction (0-4) for different failure scenarios

Risk Assessment: Example (2/2)

Machine Protection Concern IMPACT Availability Concern

FREQUENCY

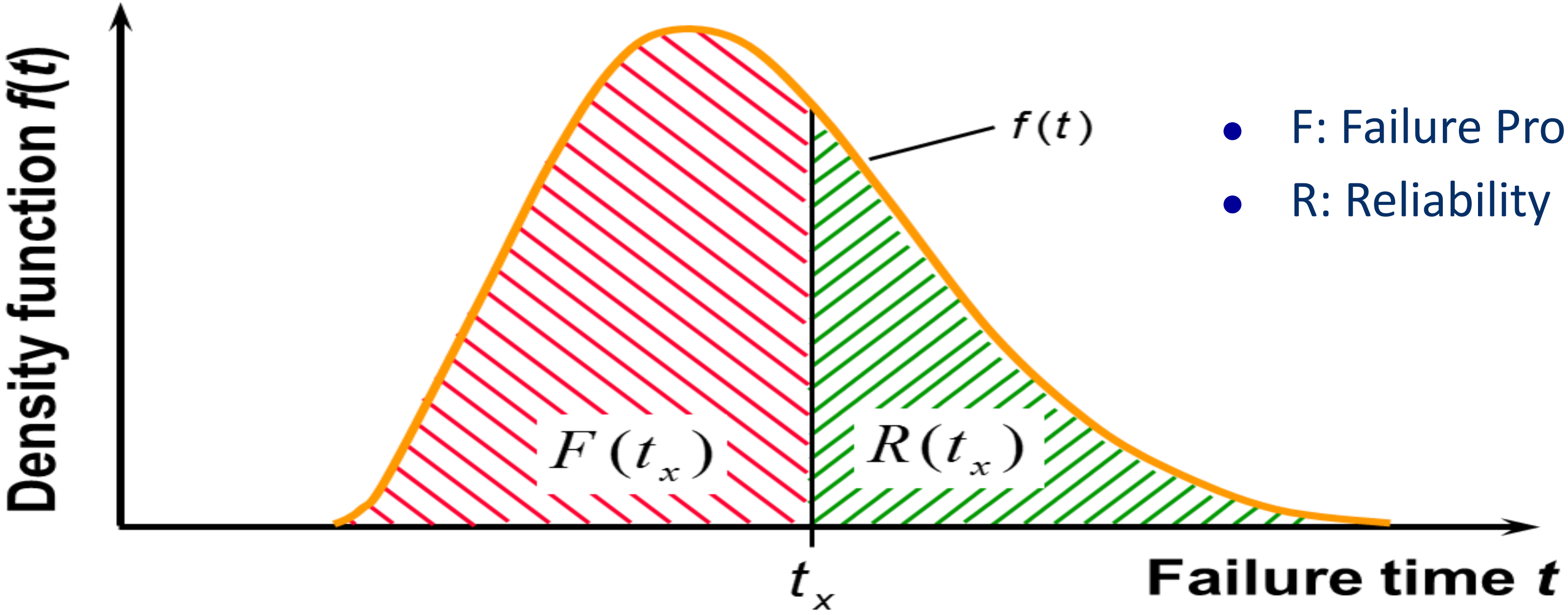
	Per year	Catastrophic	Major	Moderate	Low
Frequent	1	4	3	3	2
Probable	0.1	3	3	3	2
Occasional	0.01	3	3	2	1
Remote	0.001	3	2	2	1
Improbable	0.0001	3	2	1	0
Not credible	0.00001	2	1	0	0
Cost [MCHF]		> 50	1-50	0.1-1	0-0.1
Downtime [days]		> 180	20-180	3-20	0-3

- New approach: ‘Data-driven risk matrices for CERN’s accelerators’, IPAC’21

Failure Frequency

Failure Behaviour of Components

Prof. Dr. B. Bertsche, Dr. P. Zeiler, T. Herzig, IMA, Universität Stuttgart, CERN Reliability Training, 2016

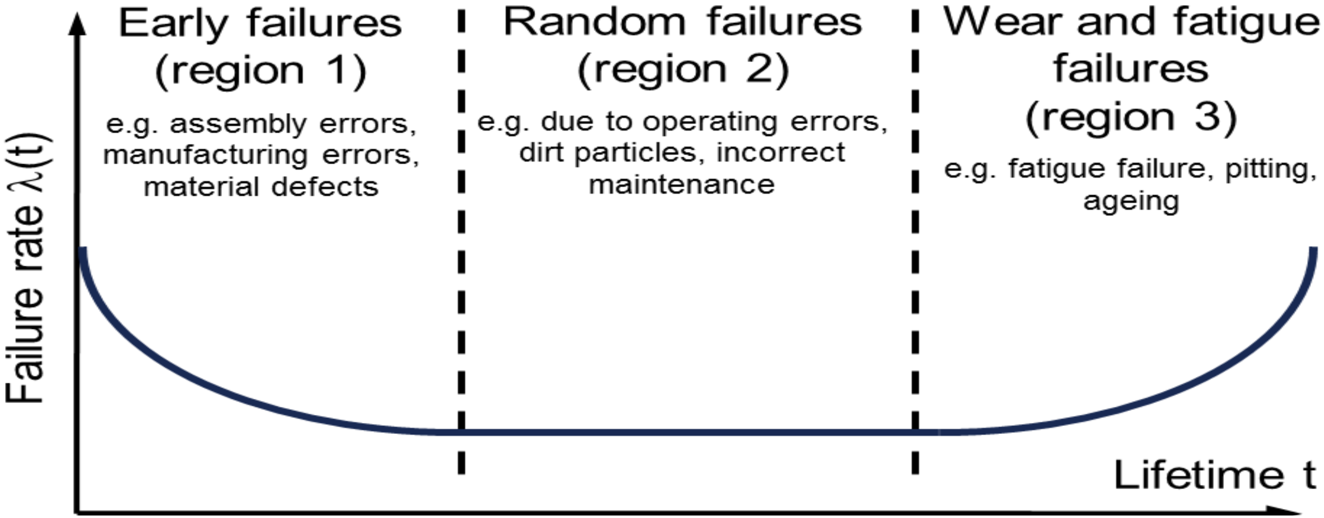


- F: Failure Probability
- R: Reliability

- The failure behaviour of a component is described by a density function
- Its integral over a certain time t_x gives the failure probability
- Reliability is the complement to 1 of the Failure Probability (‘Survival’ Probability)

Failure Rate and Bathtub Curve

$$\lambda(t) = \frac{\text{Failures}}{\text{Total number of units still intact}} = \frac{f(t)}{R(t)}$$



Early failures (region 1)
e.g. assembly errors, manufacturing errors, material defects
Random failures (region 2)
e.g. due to operating errors, dirt particles, incorrect maintenance
Wear and fatigue failures (region 3)
e.g. fatigue failure, pitting, ageing
Failure rate λ(t)
Lifetime t

- In practice, it is often assumed that failures occur randomly, i.e. they are described by an exponential density function → **constant failure rate λ**
- Only in the latter case Mean Time Between Failures (MTBF) = 1/λ
- Clearly a **simplification** in some cases…

Prof. Dr. B. Bertsche, Dr. P. Zeiler, T. Herzig, IMA, Universität Stuttgart, CERN Reliability Training, 2016

Component Failure Rate Estimates

TESTS

Accurate results

Cost + Time

Accelerated lifetime tests (if applicable)

EXPERT ESTIMATES

Big uncertainties on boundary conditions

Good for known technologies

Good for preliminary estimates

STANDARDS

Very systematic

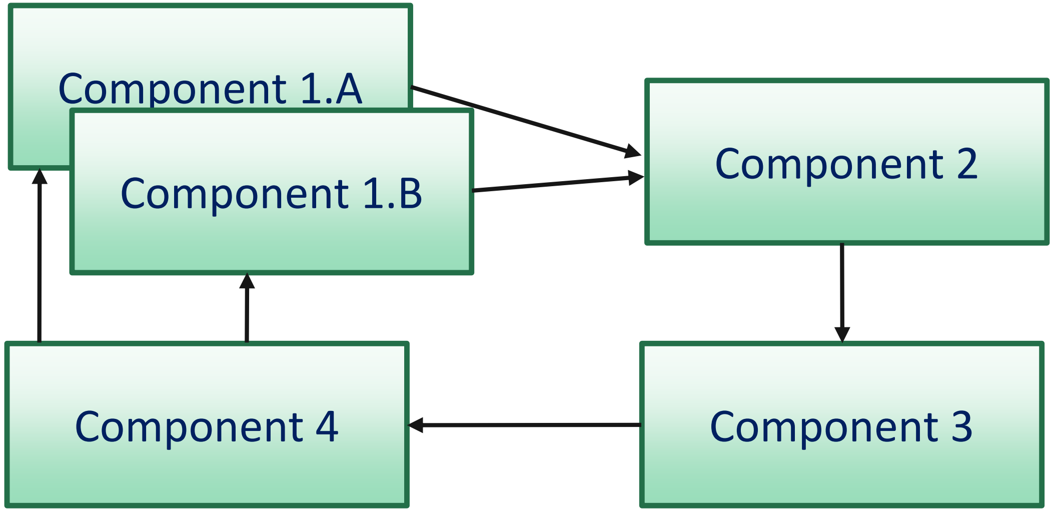
Boundary conditions taken into account

Technology advancements

IMPORTANT: The power of reliability analysis methods is not in the accuracy of failure rate estimates, but in the possibility to **compare architectures** and show the **sensitivity** of system performance on reliability figures

Description of System Failure Behaviour

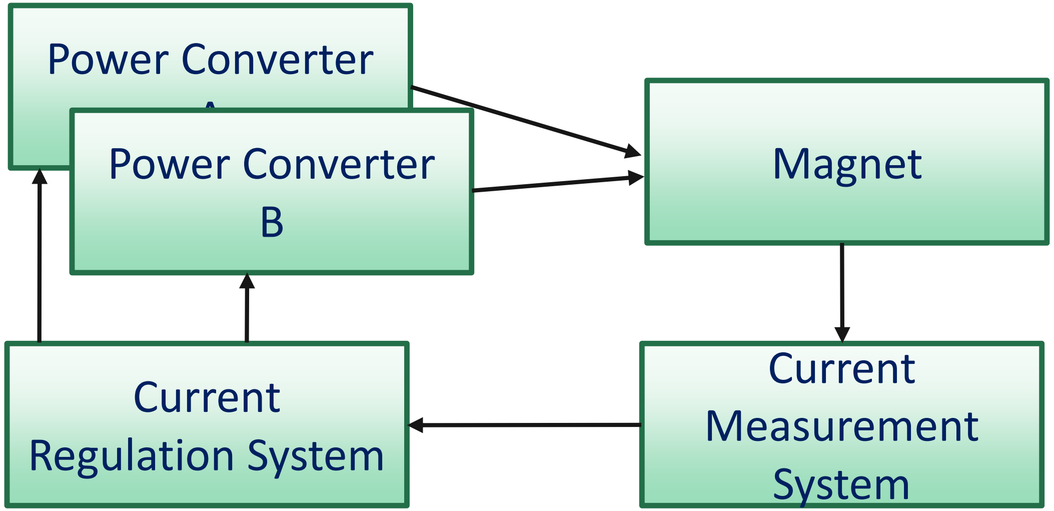
- Functional Block Diagram



Description of System Failure Behaviour

- Example: Redundant magnet powering with current regulation:

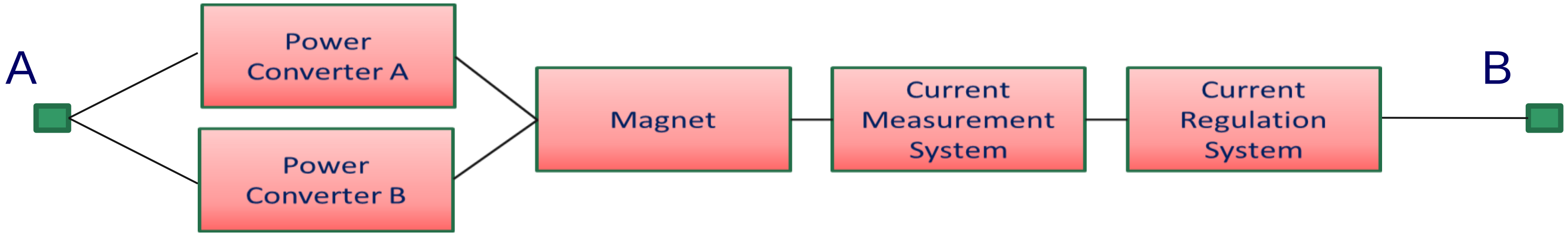
  Function: provide stable current to the magnet, based on the feedback of the current measurement. Each power converter can supply all the current to the magnet



Description of System Failure Behaviour

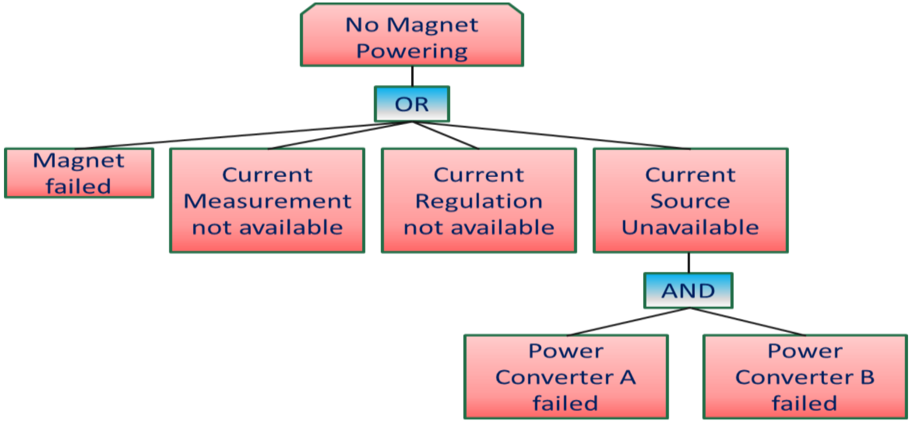
- Reliability Block Diagram:

Question: what is the minimum set of components that allows fulfilling the system functionality?



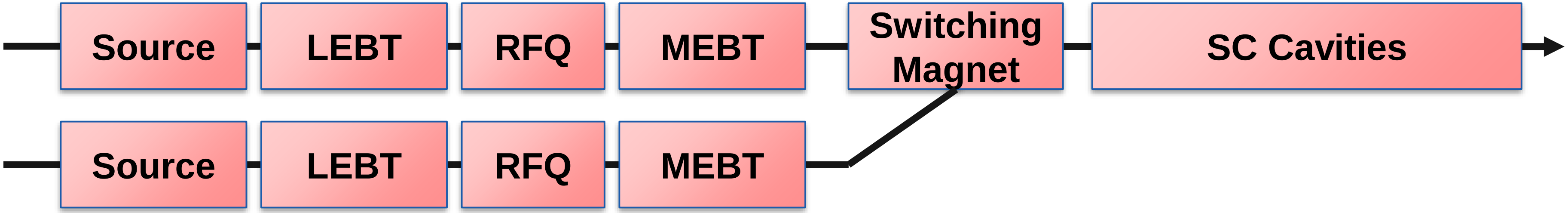
- Fault Tree:

Question: what are the combinations of failures that lead to a system failure?


No Magnet Powering
OR
Magnet failed
Current Measurement not available
Current Regulation not available
Current Source Unavailable
AND
Power Converter A failed
Power Converter B failed

Boolean Algebra allows calculating system reliability from component reliability

Redundancy



The switching magnet becomes the reliability bottleneck in this architecture

- It should be designed for high reliability
- How should it be operated? (only when required, at predefined times,…)

A strategy has to be defined on how to operate the 'spare' Linac:

- Continuously running – 'hot spare' (quantify operation costs)
- When required (consider additional time to recover nominal operation)

When introducing redundancy, think about remaining single points of failure!

Failure Impact

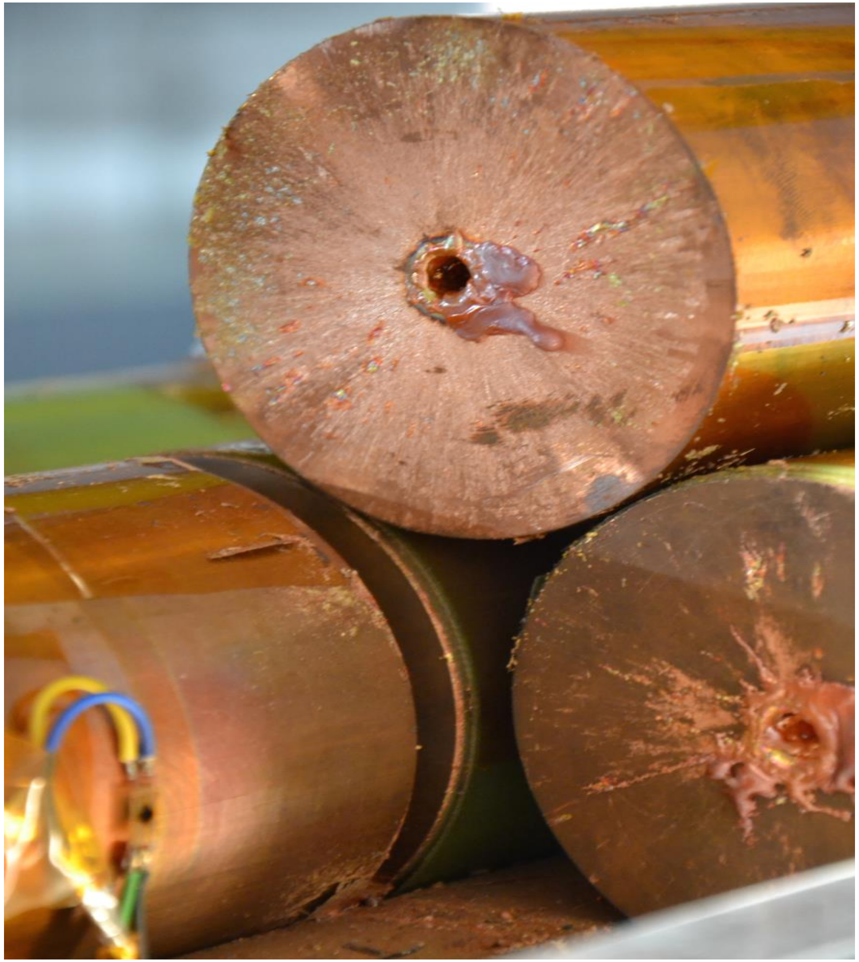
Impact on Accelerator Operation

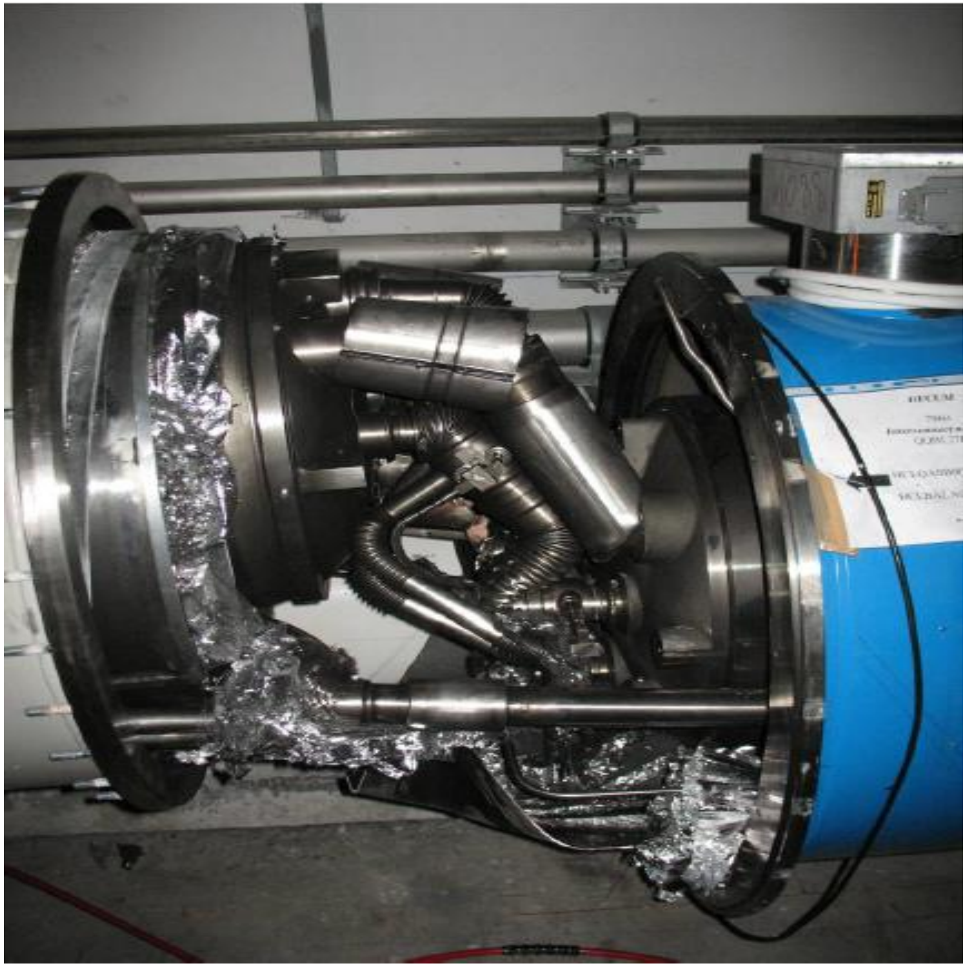
- Failures of accelerator components can lead to:
  - **Damage of the accelerator** (if no suitable protection is in place)
  - Requires significant interventions on the accelerator to restore operating conditions, typically involving experts from different fields
  - Order of magnitude: Several weeks/months

  - **Downtime of the accelerator** (no damage thanks to machine protection systems, but impossibility to operate the accelerator)
  - Requires a corrective action to restore operating conditions (**Maintenance**), typically only involving experts of the failed equipment
  - Order of magnitude: Hours/days

Failure Impact: Damage

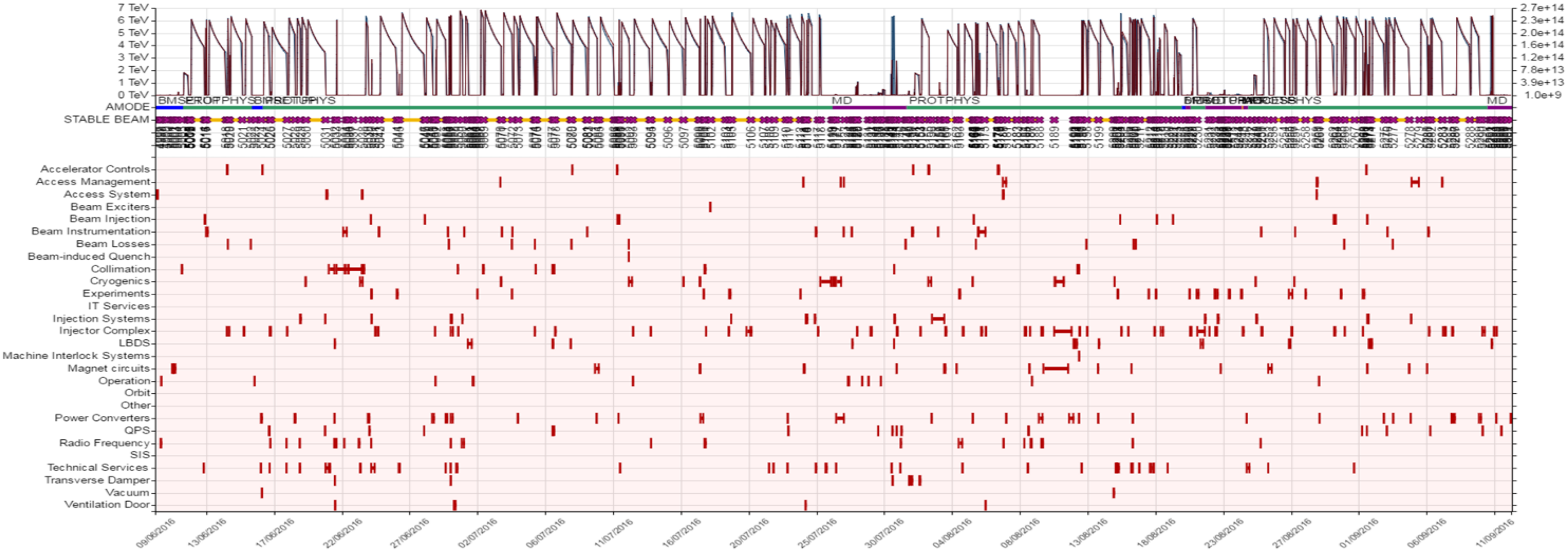
Damage in High-Power Accelerators





Failure Impact: Downtime

Accelerator Downtime

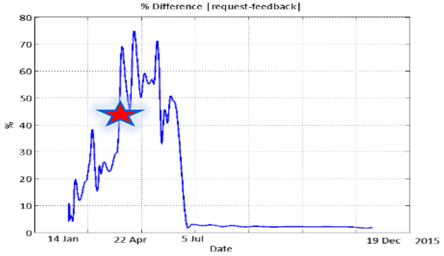


Systematic follow-up of failures → learn from experience → possible reduction of recovery times (faster diagnostics, faster repairs, management of spare parts,…)

Failure Duration

Failure Duration

Identification



Diagnostics

Logistics

Repair

- **Mean Time to Repair (MTTR)**: the average time required to repair a failed component or device.
- In addition, some time might be required to recover nominal operating conditions (e.g. beam-recommissioning, source stabilization, magnetic pre-cycles,…)

Definitions

Maintenance signifies methods for the **determination and evaluation of the current status** as well as for the **preservation and reestablishment of the nominal status** of facilities, machines and components.

- **Corrective maintenance** methods are required for partial and total failures of facilities, devices and components. Such methods serve to the **reestablishment of the nominal condition**.
- **Preventive maintenance** deals with maintenance methods which are carried out preventively, that is, **at a predetermined time** or **periodically** after a certain amount of operational hours.
- **Condition-based maintenance avoids exact inspection and overhauling intervals** and thus avoids the periodical renewal of fully functional components and assemblies.

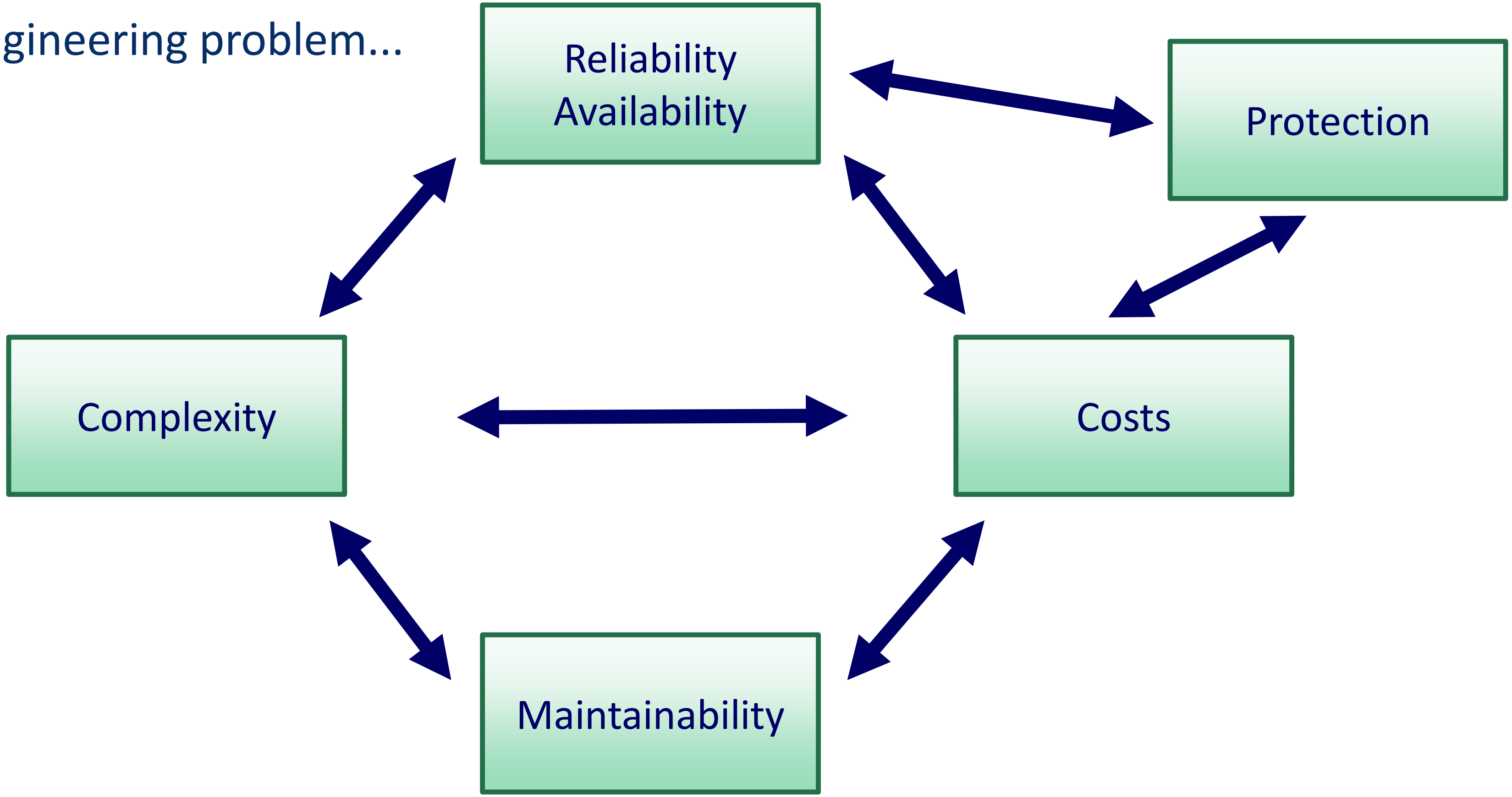
Prof. Dr. B. Bertsche, Dr. P. Zeiler, T. Herzig, IMA, Universität Stuttgart, CERN Reliability Training, 2016

Maintenance and Operability

- Maintenance and operability should be considered from **early design** phases of the accelerator
- System **architectures** can strongly influence maintainability
- **Modular designs** help optimizing maintenance tasks and commissioning
- **Accessibility** of equipment (when possible) ensures faster recoveries after failures
- Advanced **diagnostics** capabilities help identifying – and possibly anticipate – failures → invest in **machine learning for failure prediction**
- Important: reliability analyses provide the means for **spare part management**

Trade-Off

A complex engineering problem...



For each application, the optimal working point has to be chosen!

Thanks a lot for your attention!!