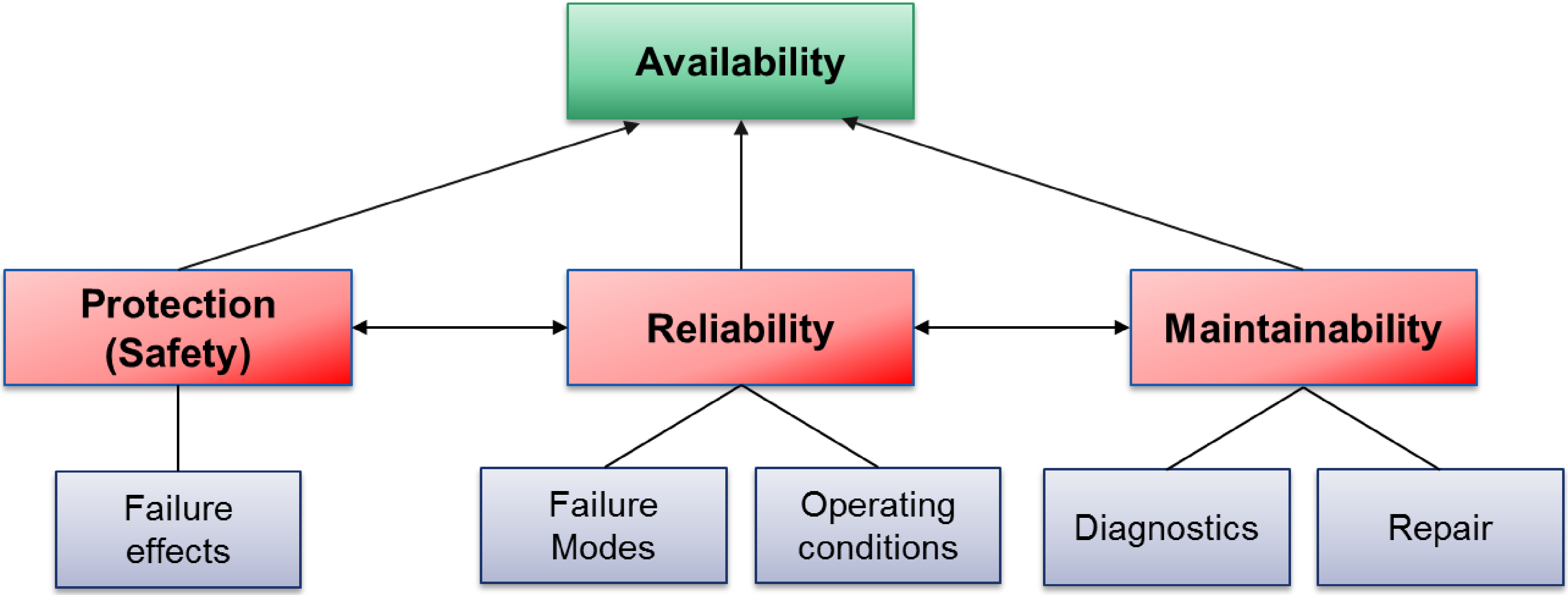
Reliability and Availability of Particle Accelerators: Concepts, Lessons, Strategy

A. Apollonio
CERN Machine Protection Group (TE-MPE)
Xbeam Strategy Workshop– 15/02/2017
andrea.apollonio@cern.ch

Acknowledgements: R. Schmidt, B. Todd, M. Kwiatkowski, F. Bouly, A. Lechner, A. Niemi, J. Gutleber.

RAMS/Outline



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

Basic Definitions

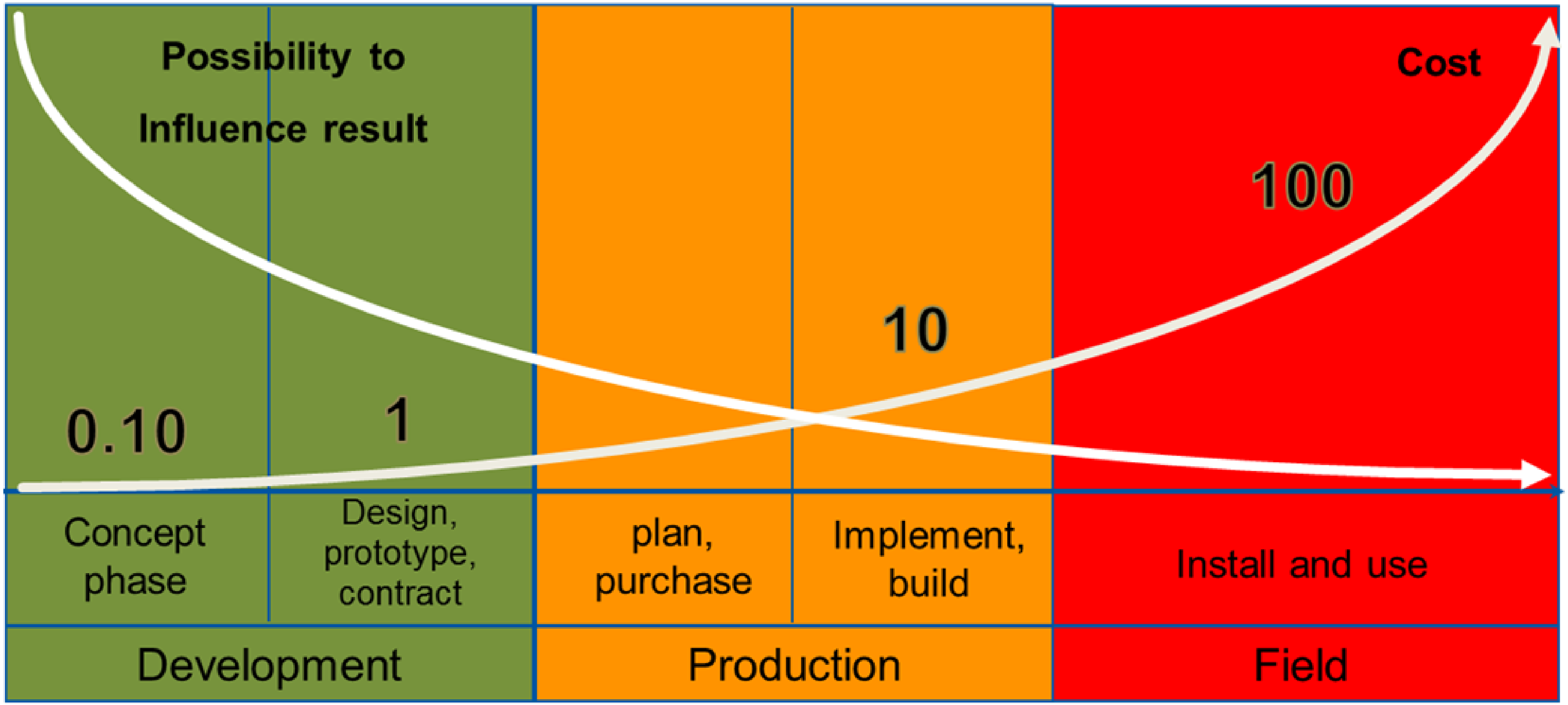
- **Reliability (0-1)** is the probability that a system does not fail during a defined period of time under given functional and environmental conditions
  - Example of reliability specification: “An accelerator must have a reliability of 60 % after 100 h in operation, at an operating current of 40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

Importance of Reliability Analyses

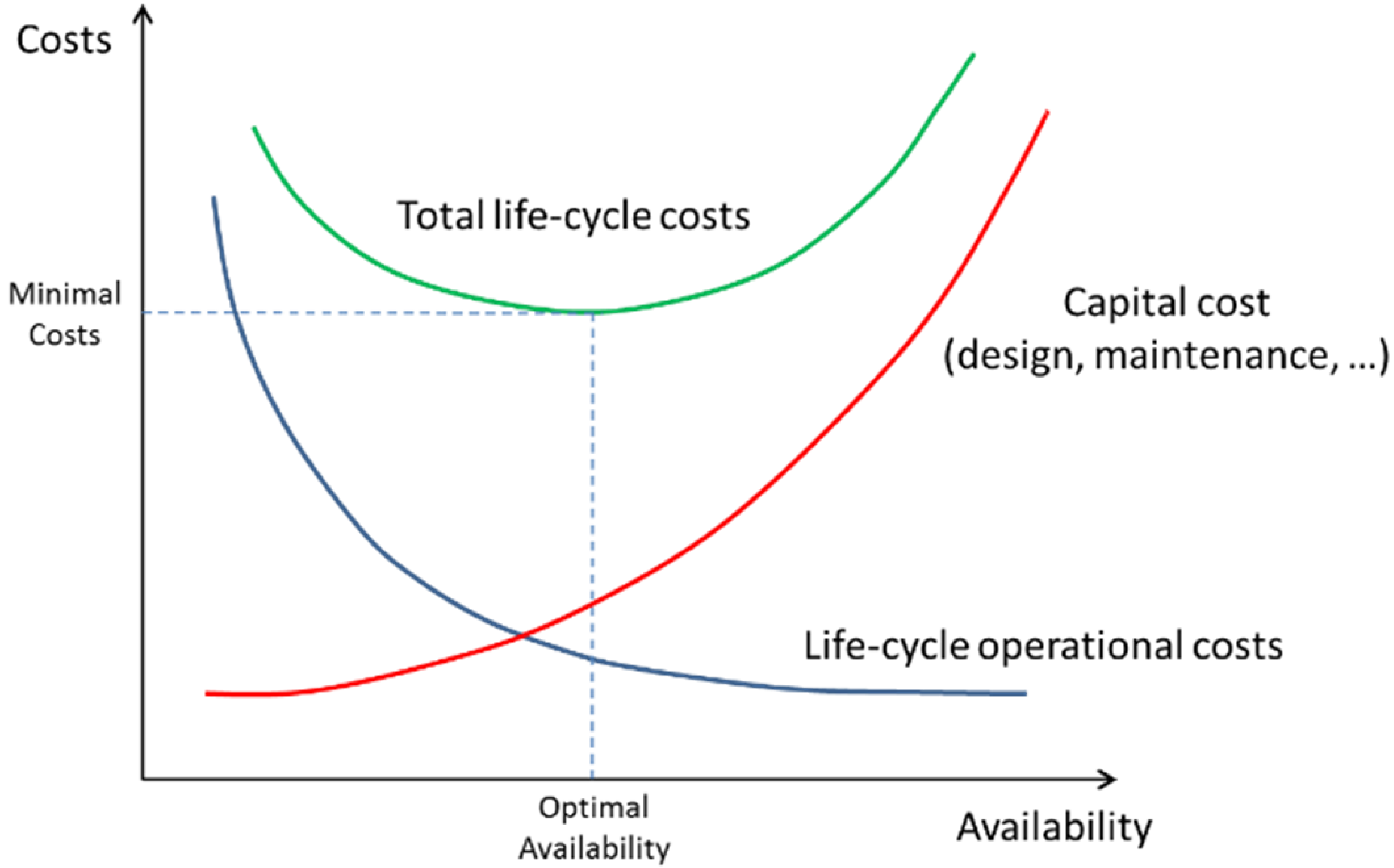
Prof. Dr. B. Bertsche, Dr. P. Zeiler, T. Herzig, IMA, Universität Stuttgart, CERN Reliability Training, 2016

- 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 operational costs must be found

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

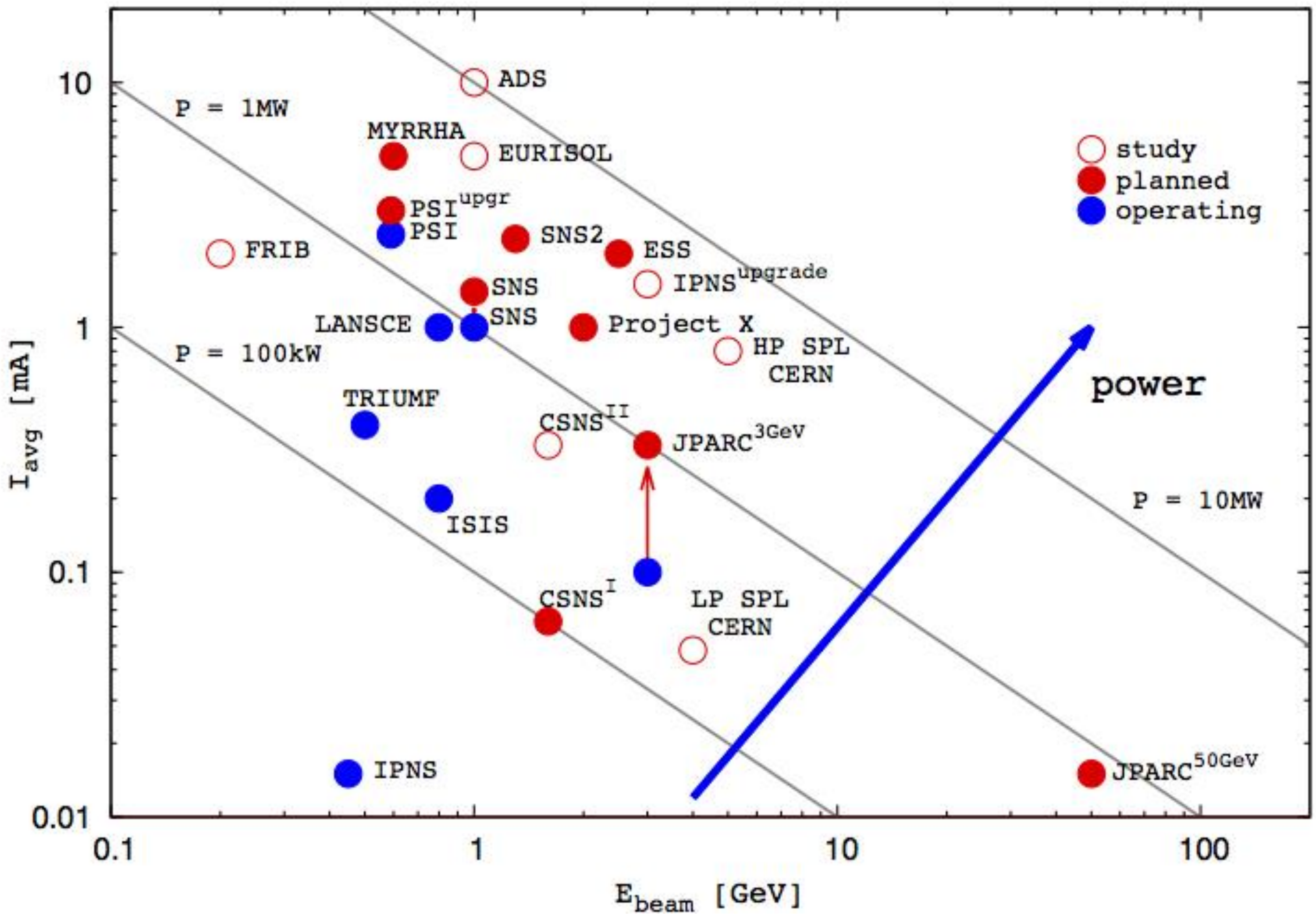
Stored energy per beam is 360 MJ

Stored energy in the magnet circuits is 9 GJoule

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

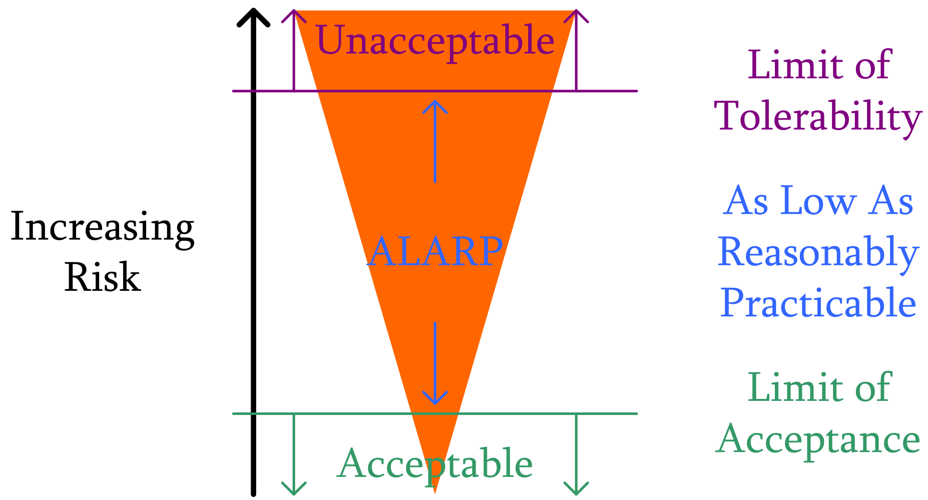
....can melt 14 tons of copper

Spallation Sources + High Intensity Accelerators



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

Machine Protection Concern — IMPACT — Availability Concern

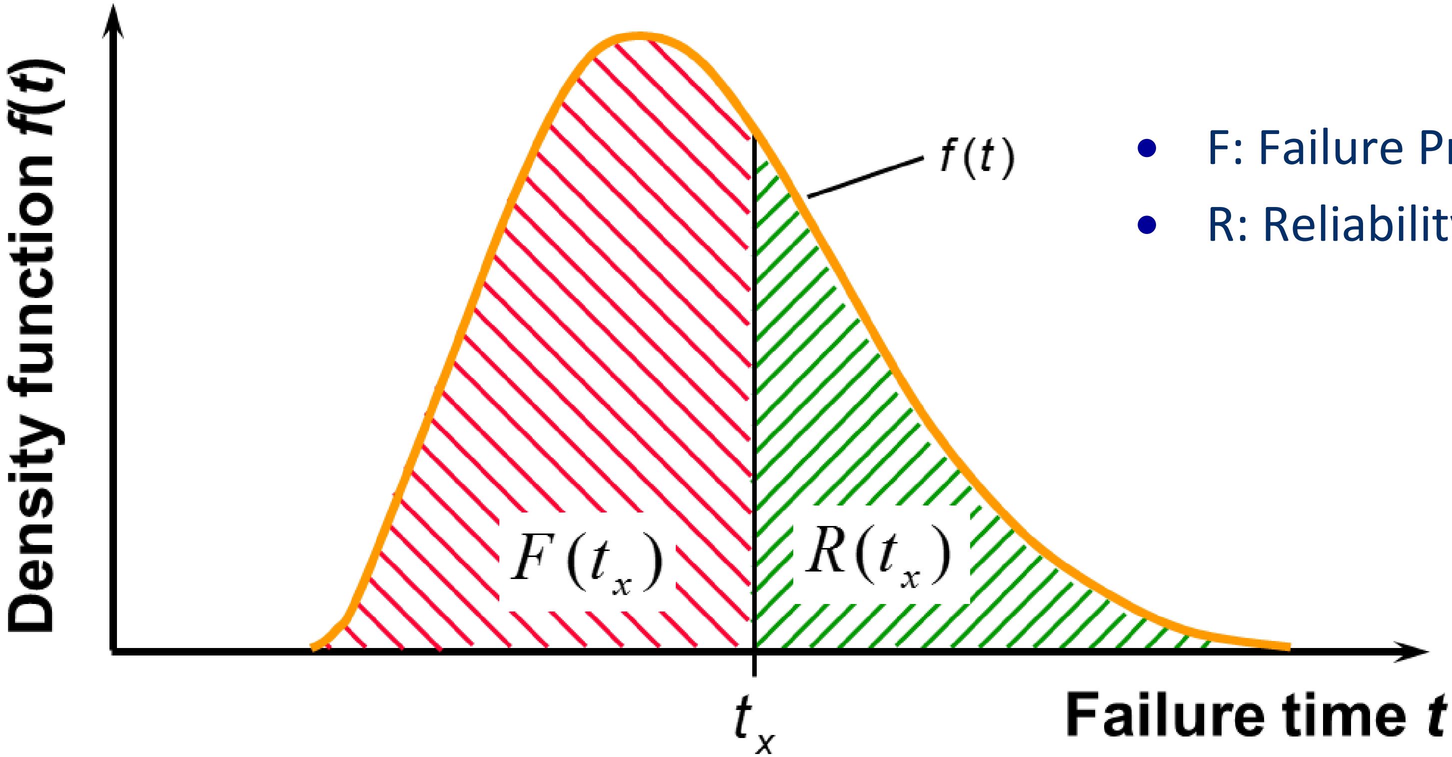
FREQUENCY	1/year	Catastrophic	Major	Moderate	Low	Very Low
Very likely	10					
Frequent	1					
Probable	0.1					
Occasional	0.01					
Remote	0.001					
Improbable	0.0001					
Cost [MCHF]		> 50	1-50	0.1-1	0.01-0.1	0-0.01
Downtime [days]		> 180	20-180	3-20	1-3	0-1

- **IMPORTANT**: this matrix depends on the application!

Failure Frequency

Failure Behaviour of Components

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

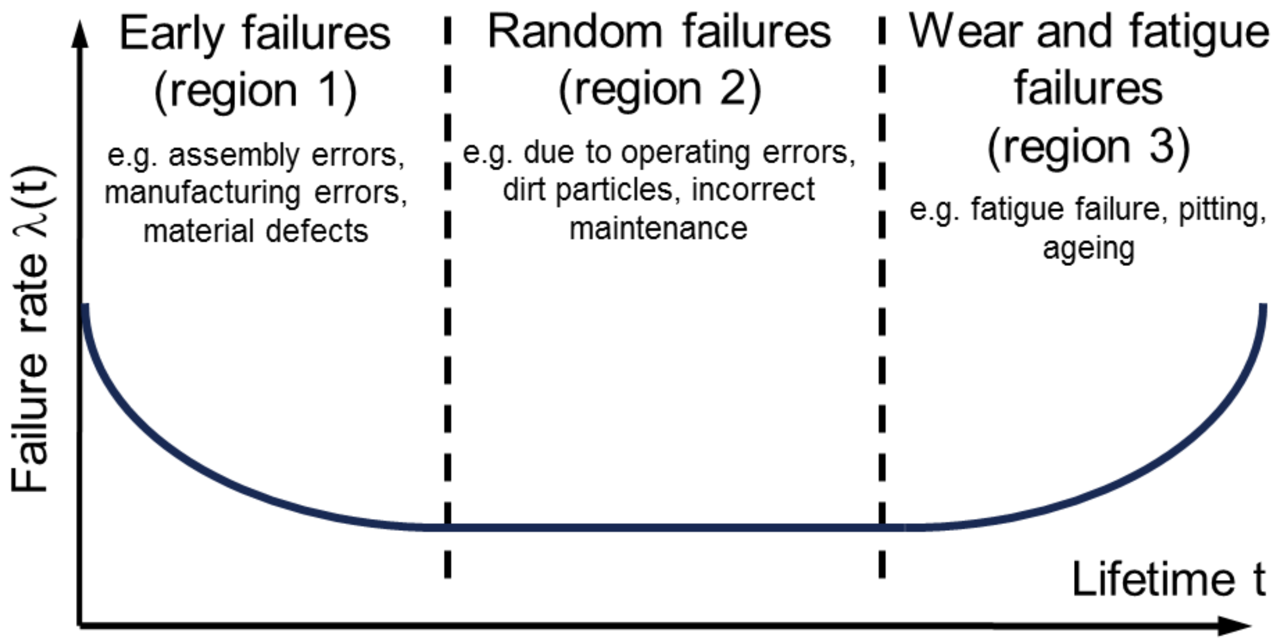


- F: Failure Probability
- R: Reliability

- 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

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



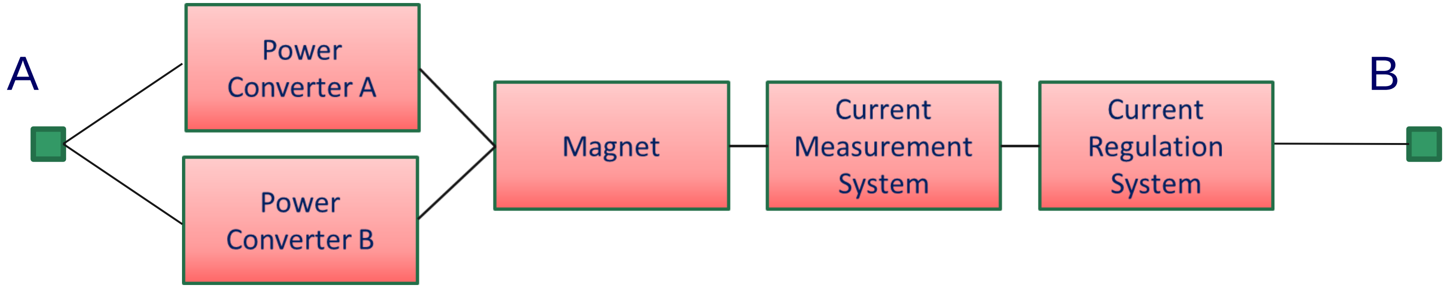
- In practice, it is often assumed that failures occur randomly, i.e. they are described by an exponential density function → **constant failure rate λ**
- Only in the latter case Mean Time Between Failures (MTBF) = 1/λ
- Clearly a **simplification** in some cases…

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

Description of System Failure Behaviour

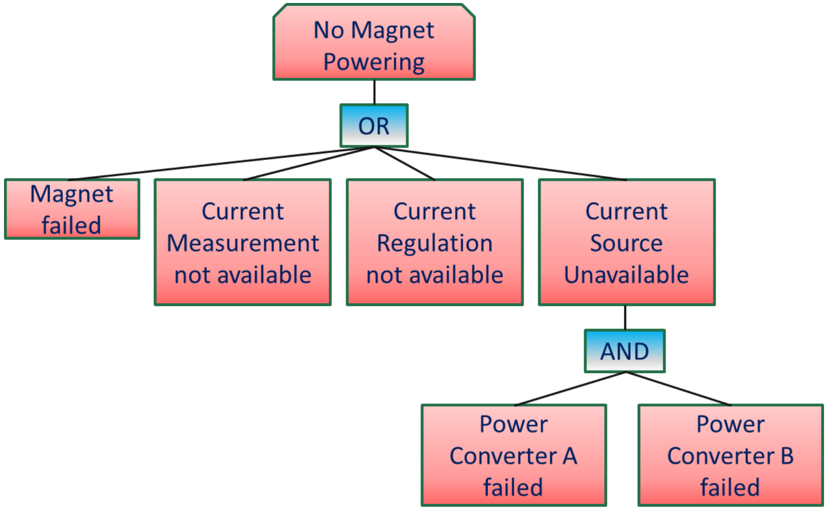
- Reliability Block Diagram:

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?



Boolean Algebra allows calculating system reliability from component reliability

Component Failure Rate Estimates

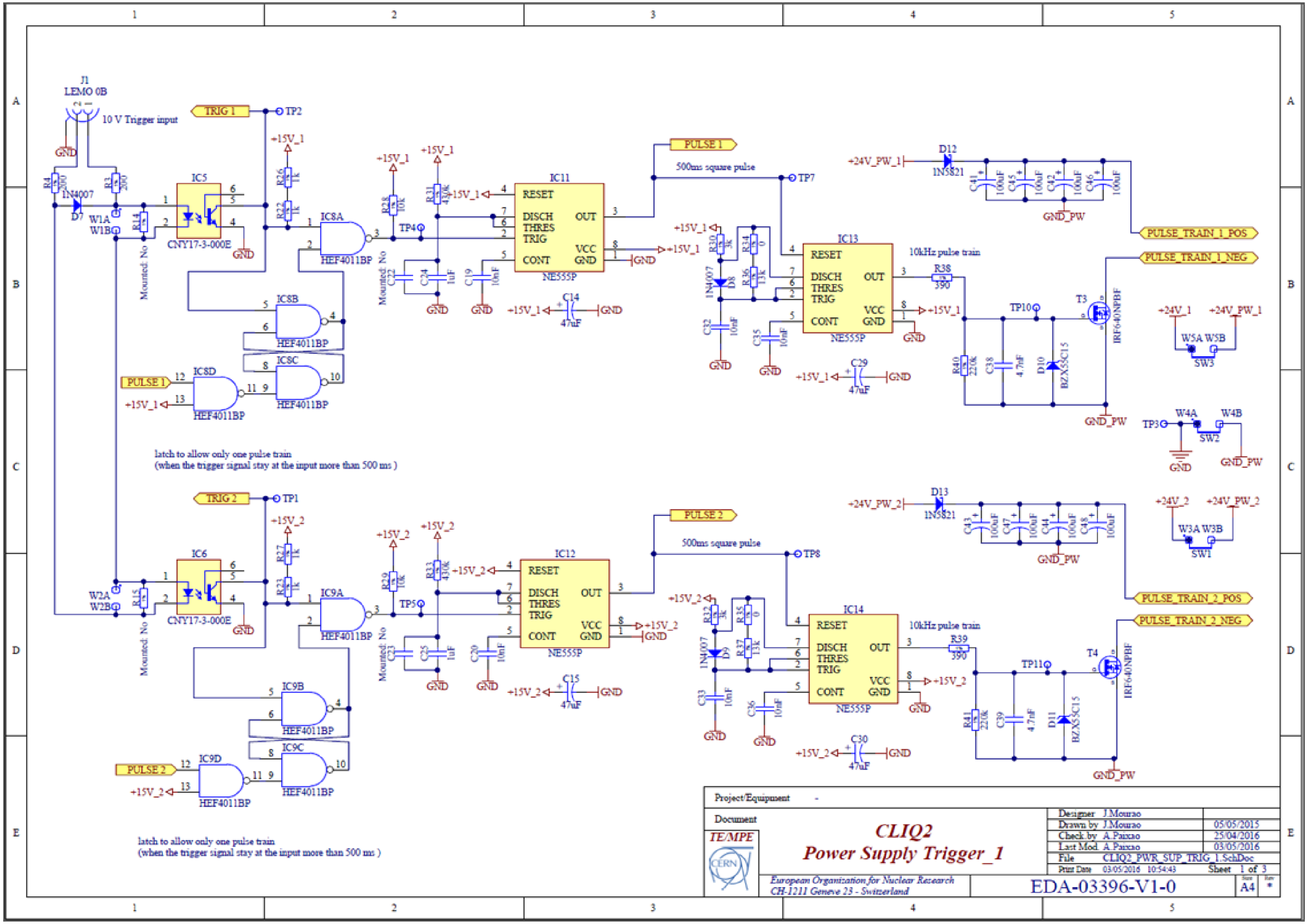
- Tests:
  - Large number of samples to be tested / long time for testing
  - May be impractical in some cases
  - Accelerated lifetime tests (if applicable)

- Experts' estimates
  - Big uncertainties on boundary conditions
  - Good approximation for known technologies
  - Good for preliminary estimates

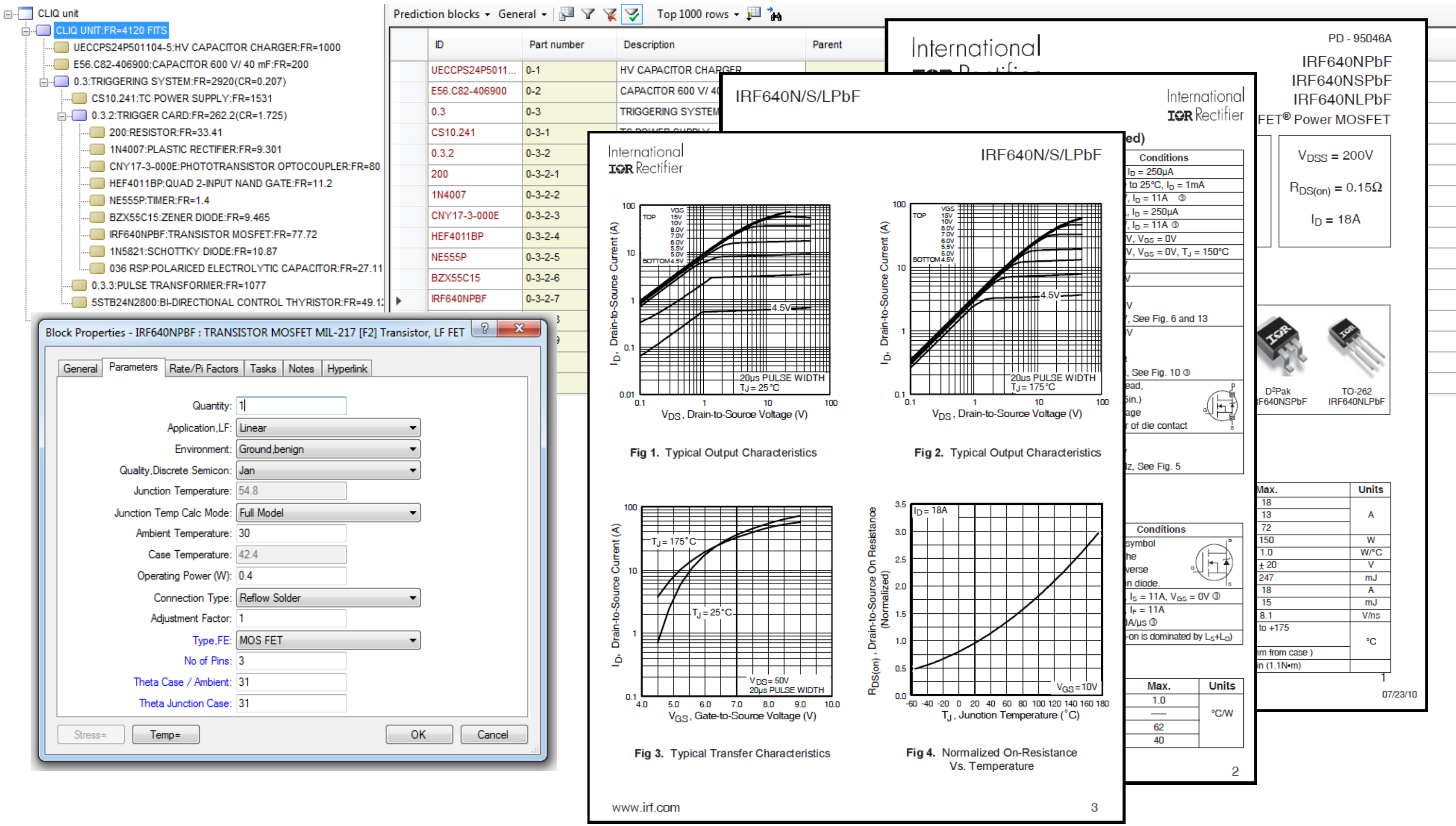
- Using Standards (Mil. Handbooks for electronic components)
  - Very systematic approach
  - Boundary conditions can be taken into account (quality of components, environment)
  - Difficult to follow technology advancements (e.g. electronics)

IMPORTANT: The power of these 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

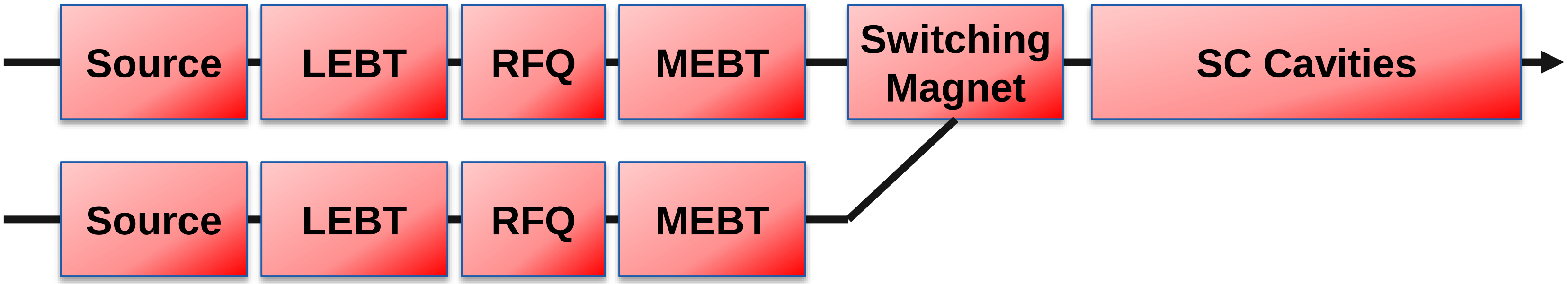
Example of Failure Rate Calculations



Example of Failure Rate Calculations



Redundancy: Example from MYRRHA



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)

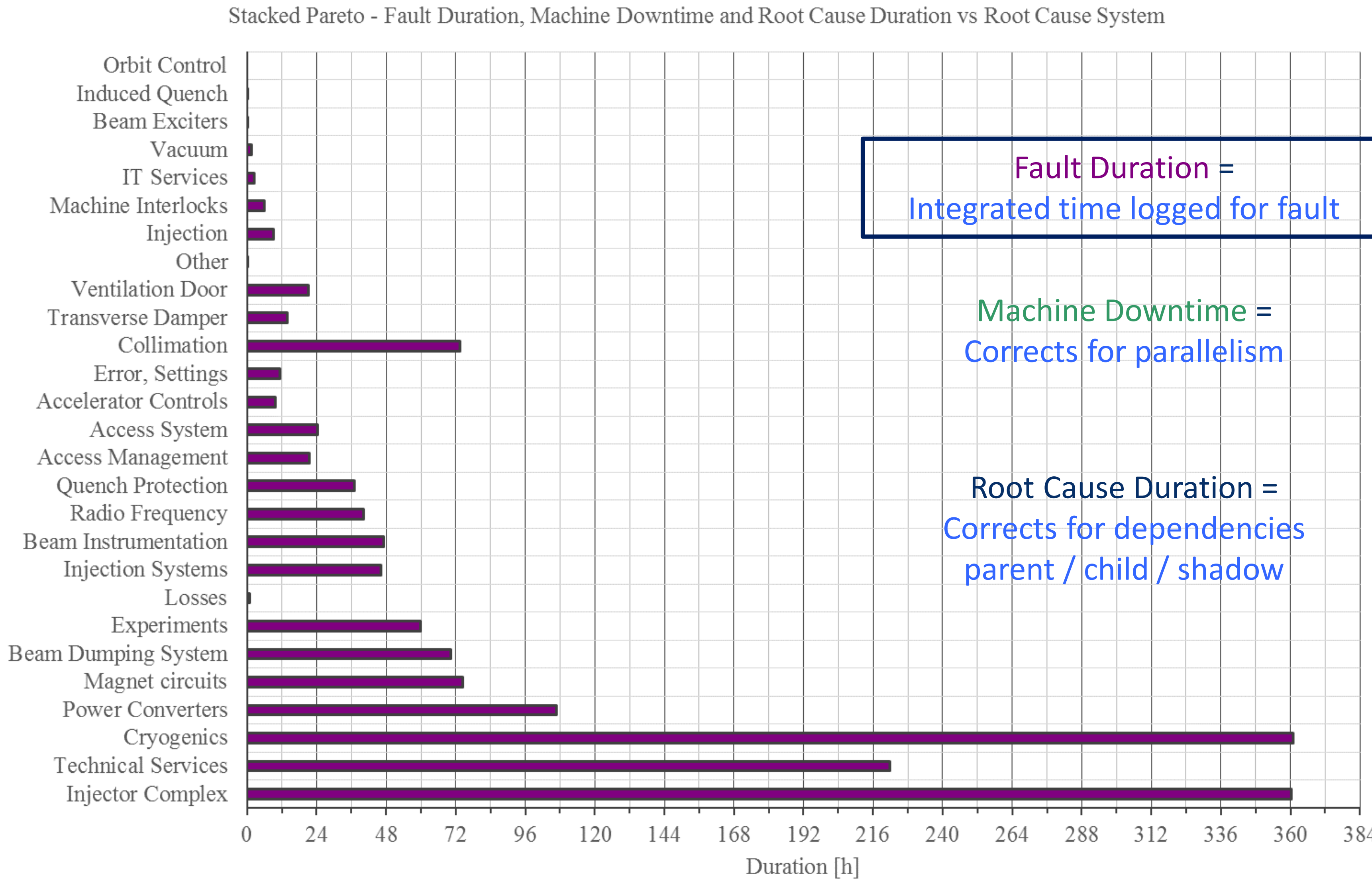
When introducing redundancy, think about remaining single points of failure!

Failure Impact: Downtime

Accelerator Downtime

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

Faults

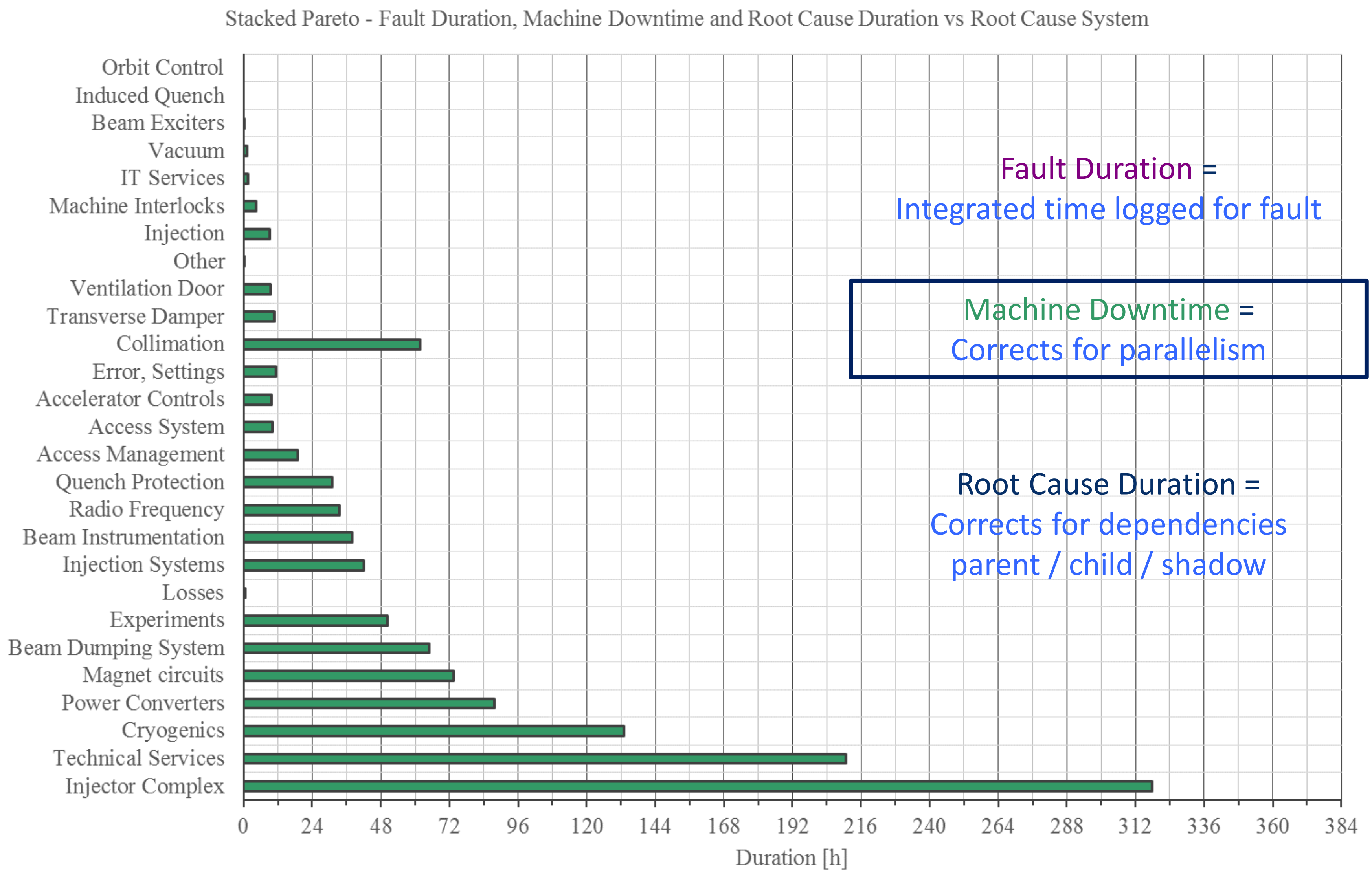


Fault Duration =
Integrated time logged for fault

Machine Downtime =
Corrects for parallelism

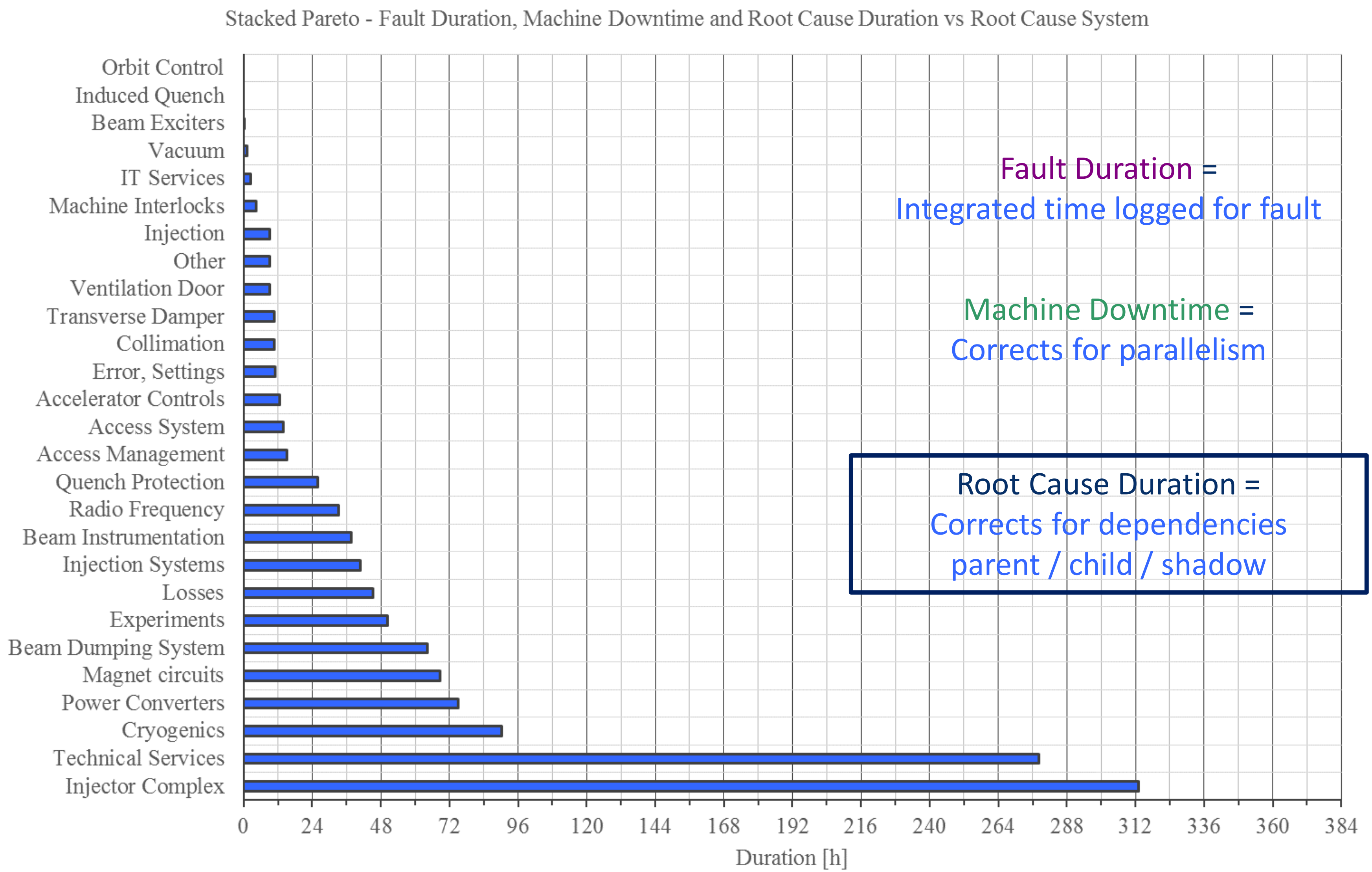
Root Cause Duration =
Corrects for dependencies
parent / child / shadow

Faults



Stacked Pareto - Fault Duration, Machine Downtime and Root Cause Duration vs Root Cause System
Orbit Control
Induced Quench
Beam Exciters
Vacuum
IT Services
Machine Interlocks
Injection
Other
Ventilation Door
Transverse Damper
Collimation
Error, Settings
Accelerator Controls
Access System
Access Management
Quench Protection
Radio Frequency
Beam Instrumentation
Injection Systems
Losses
Experiments
Beam Dumping System
Magnet circuits
Power Converters
Cryogenics
Technical Services
Injector Complex
0
24
48
72
96
120
144
168
192
216
240
264
288
312
336
360
384
Duration [h]
Fault Duration =
Integrated time logged for fault
Machine Downtime =
Corrects for parallelism
Root Cause Duration =
Corrects for dependencies
parent / child / shadow

Faults

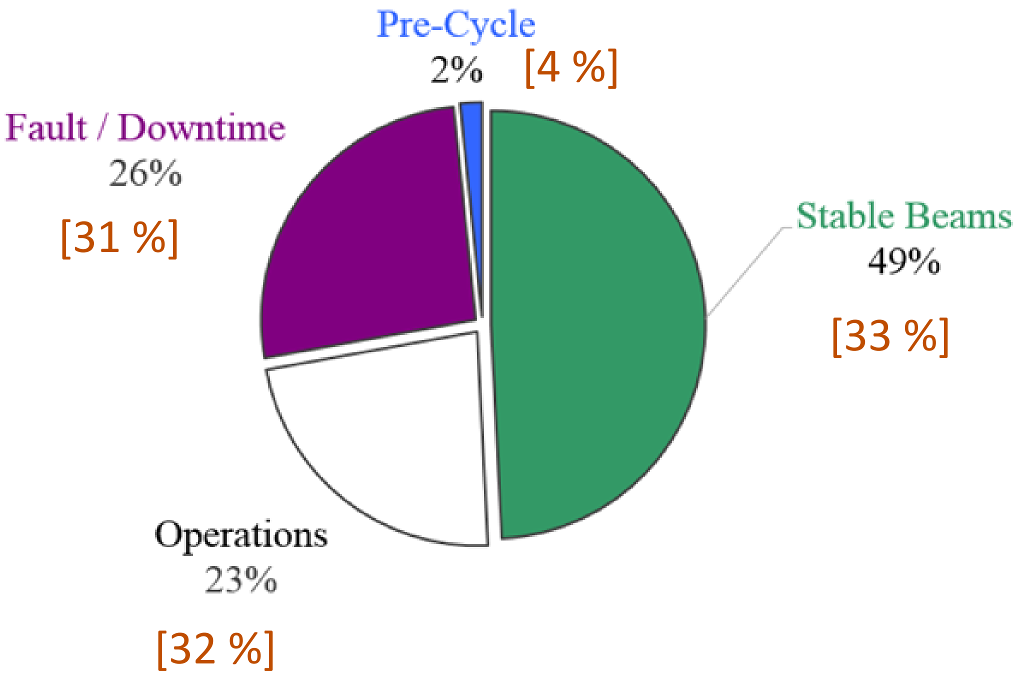


Stacked Pareto - Fault Duration, Machine Downtime and Root Cause Duration vs Root Cause System
Orbit Control
Induced Quench
Beam Exciters
Vacuum
IT Services
Machine Interlocks
Injection
Other
Ventilation Door
Transverse Damper
Collimation
Error, Settings
Accelerator Controls
Access System
Access Management
Quench Protection
Radio Frequency
Beam Instrumentation
Injection Systems
Losses
Experiments
Beam Dumping System
Magnet circuits
Power Converters
Cryogenics
Technical Services
Injector Complex
0
24
48
72
96
120
144
168
192
216
240
264
288
312
336
360
384
Duration [h]
Fault Duration =
Integrated time logged for fault
Machine Downtime =
Corrects for parallelism
Root Cause Duration =
Corrects for dependencies
parent / child / shadow

Mode Breakdown

153 days physics ≈ 3738.7 hours

	Duration [h]
Stable Beams	1839.5
Fault / Downtime	980.0
Operations	857.9
Pre-Cycle	61.3
	= 3738.7

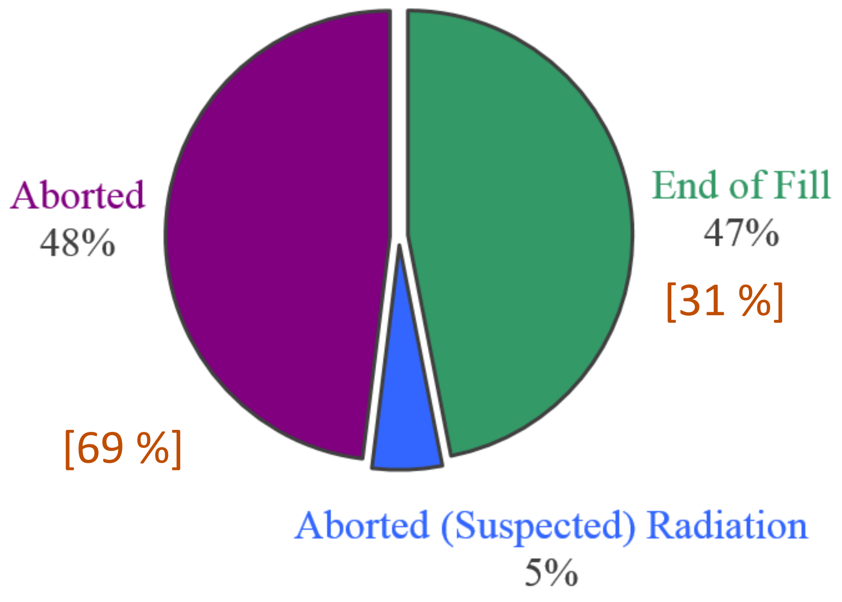


Operations contains nominal cycle + extra measurements (116h) + injection setting-up (23h) + some loss maps (35h) + planned accesses

[25 ns Run in 2015]

Physics Beam Aborts

	[#]
Total Fills	762
Fills with Stable Beams	175
Fills with Physics in Adjust	4
→ End of Fill	84
→ Aborted	86
→ Aborted (suspected) R2E	9

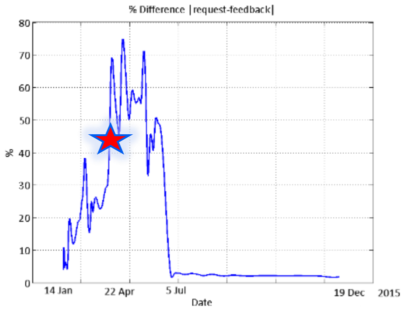


[25 ns Run in 2015]

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,…)

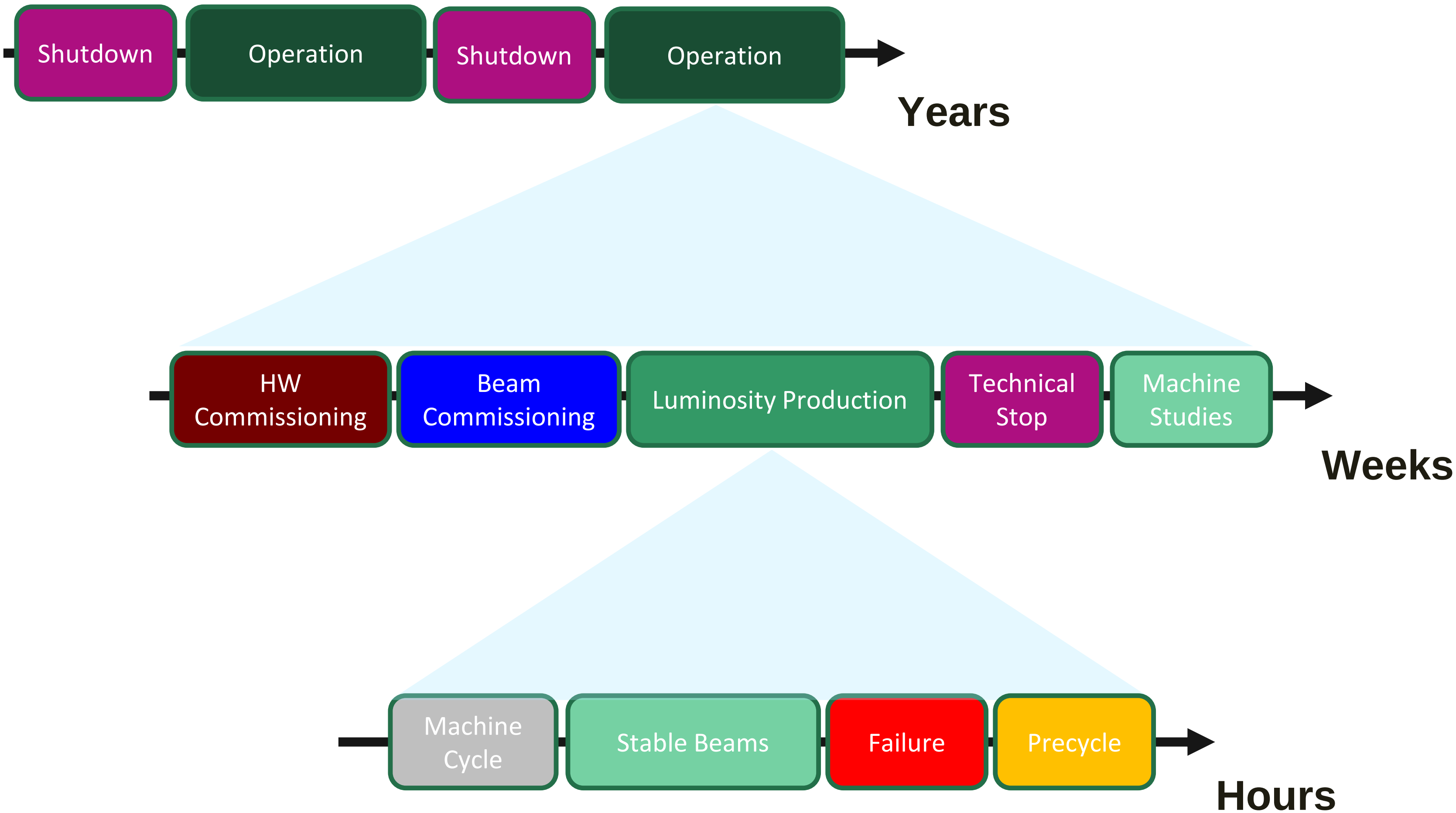
andrea.apollonio@cern.ch

Maintenance and Operability

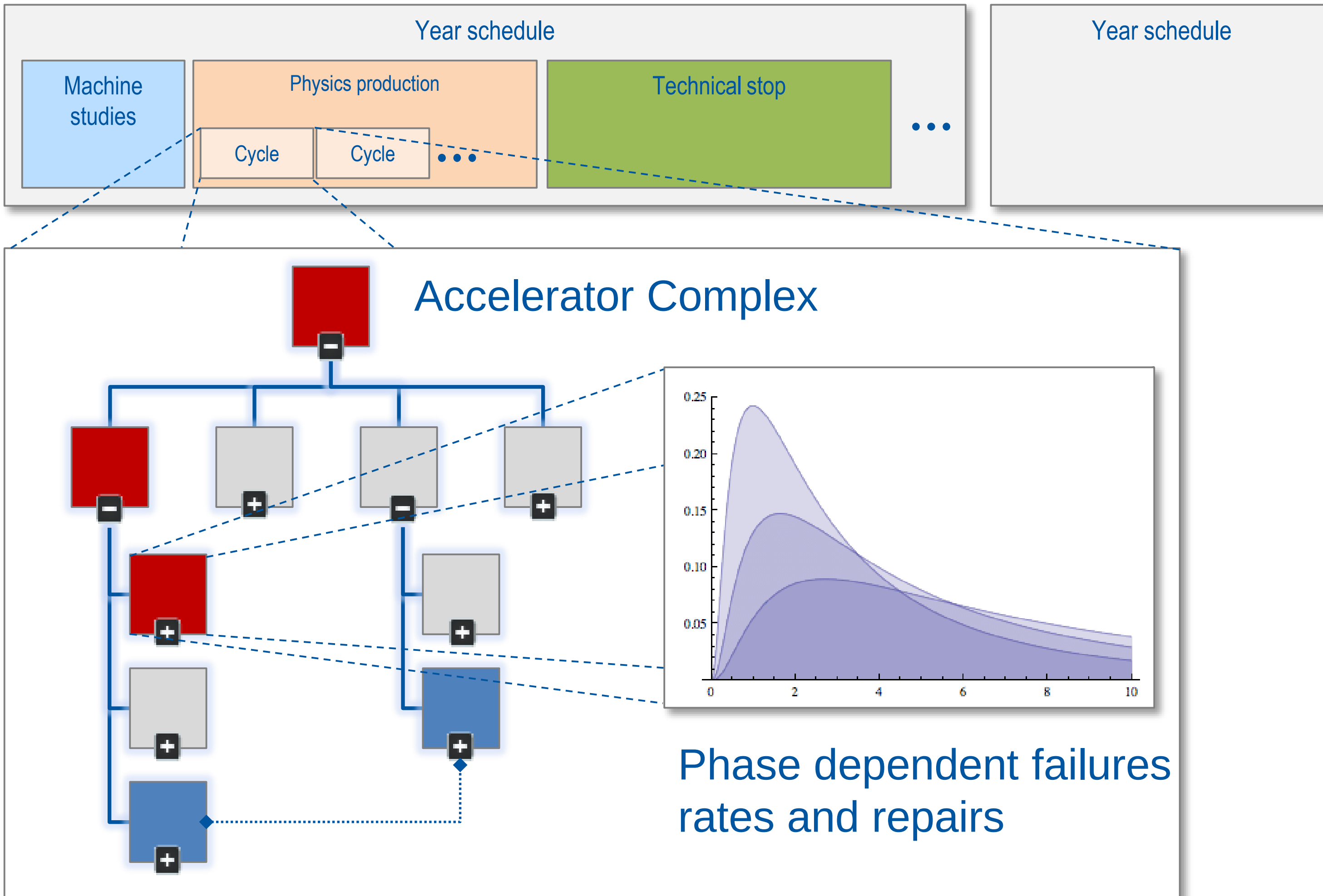
- Maintenance and operability should be considered from **early design** phases of the accelerator
- System **architectures** can strongly influence maintainability
- **Modular designs** help optimizing maintenance tasks and commissioning
- **Accessibility** of equipment (when possible) ensures faster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

From Reliability Data to Availability Modelling

Accelerator Schedule

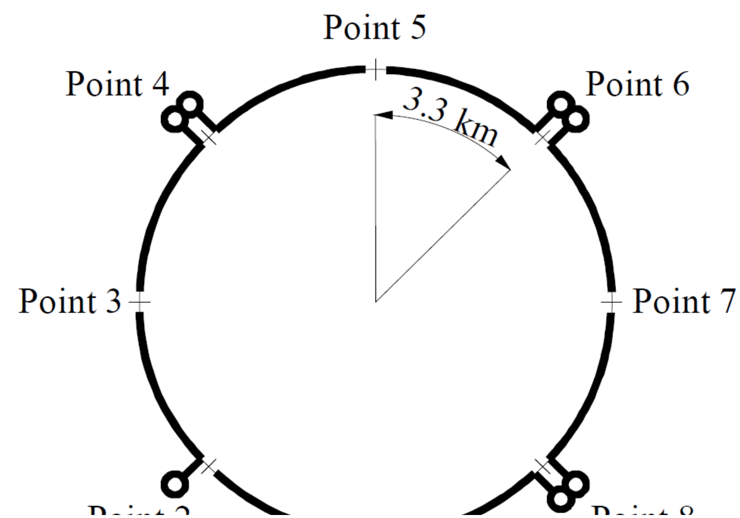


Modelling Concept



Cryogenics Example

- Goal: Define faults that lead to loss of cryogenic conditions
- Built in collaboration with Cryo experts + E. Rogova from TU Delft
- Basis for current Cryo fault categories in logbooks

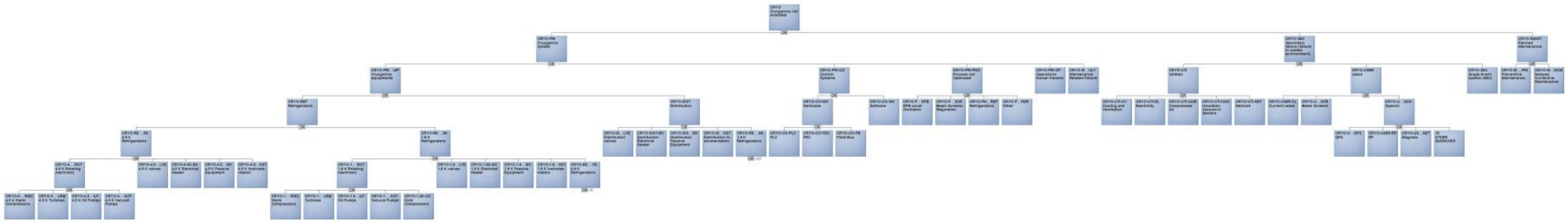


Cryogenics system

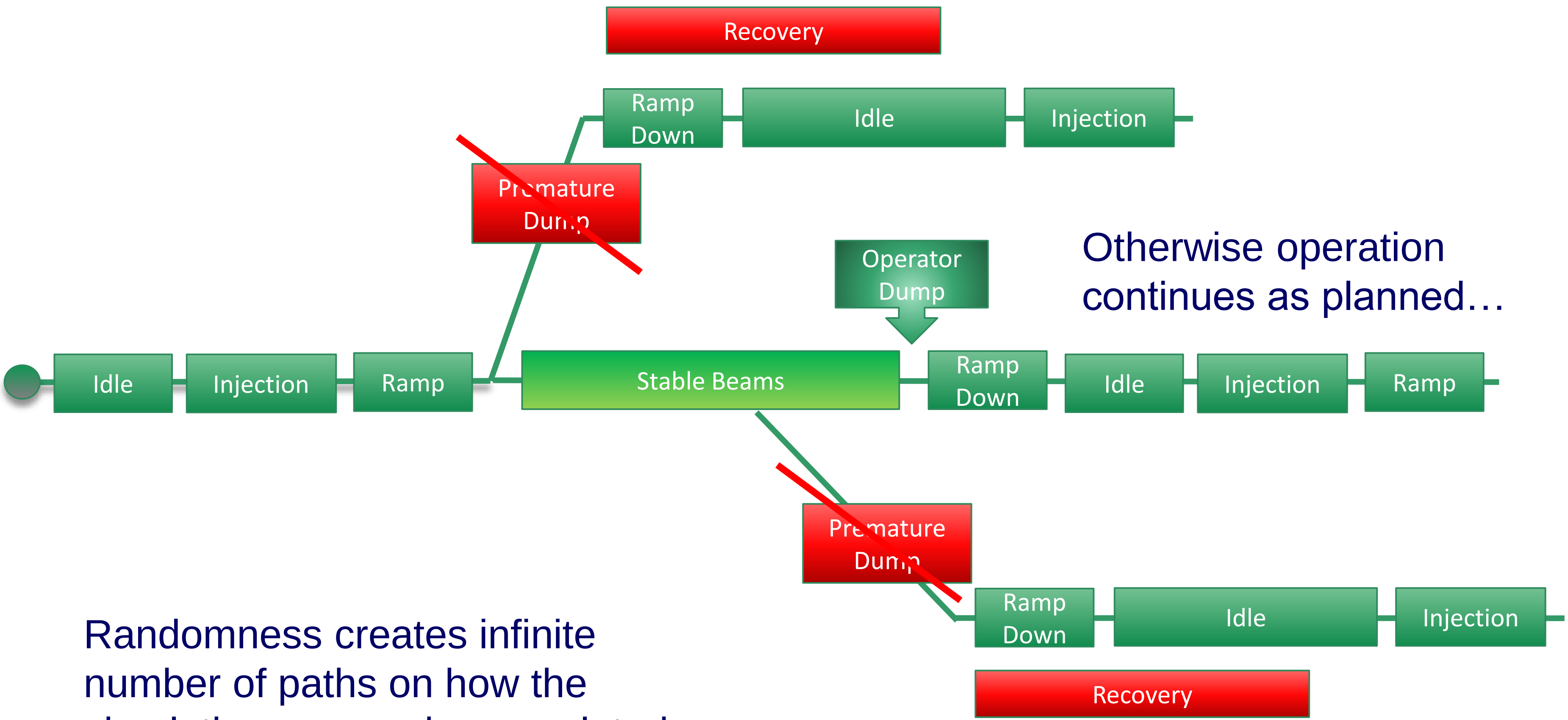
Primary faults

Secondary faults

- Users related failures
- Utility related failures



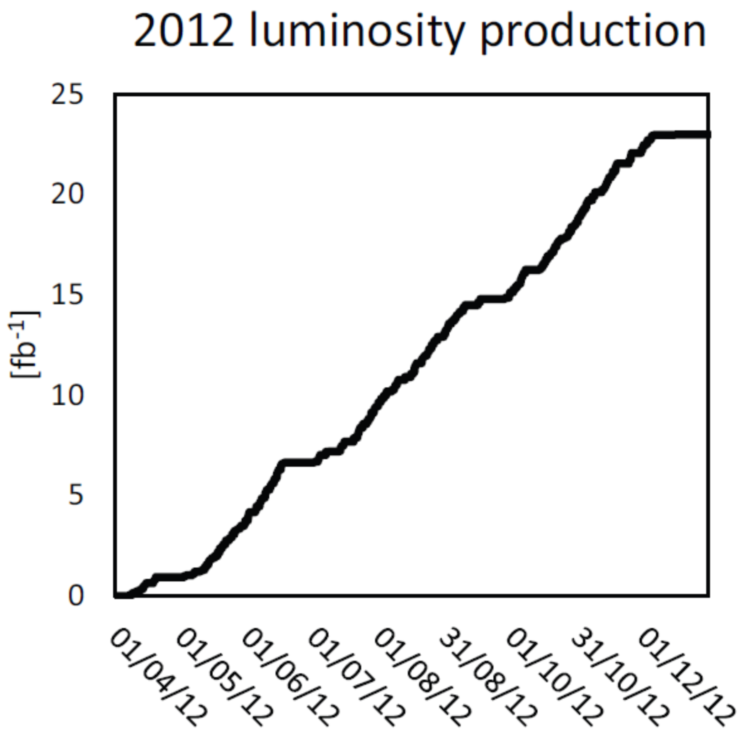
Monte Carlo Simulation Concept

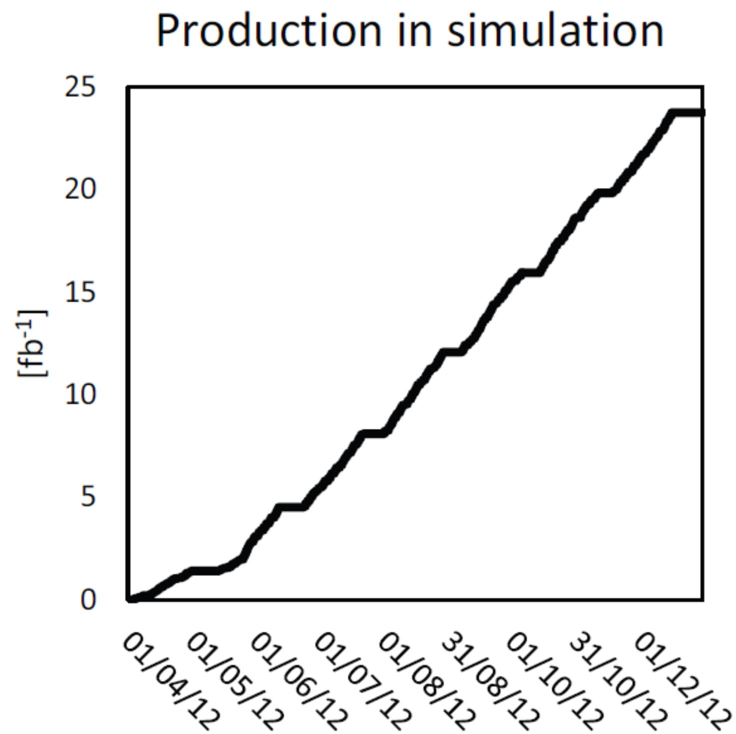


Otherwise operation continues as planned…

Randomness creates infinite number of paths on how the simulation run can be completed

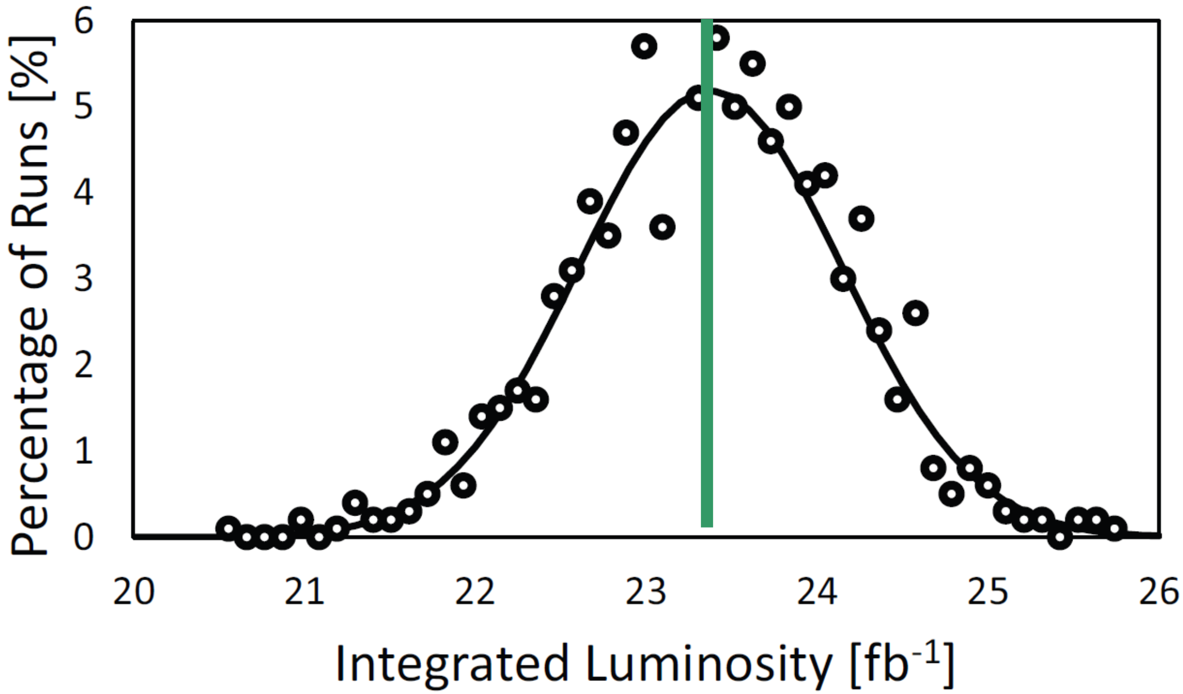
Results: Model Validation





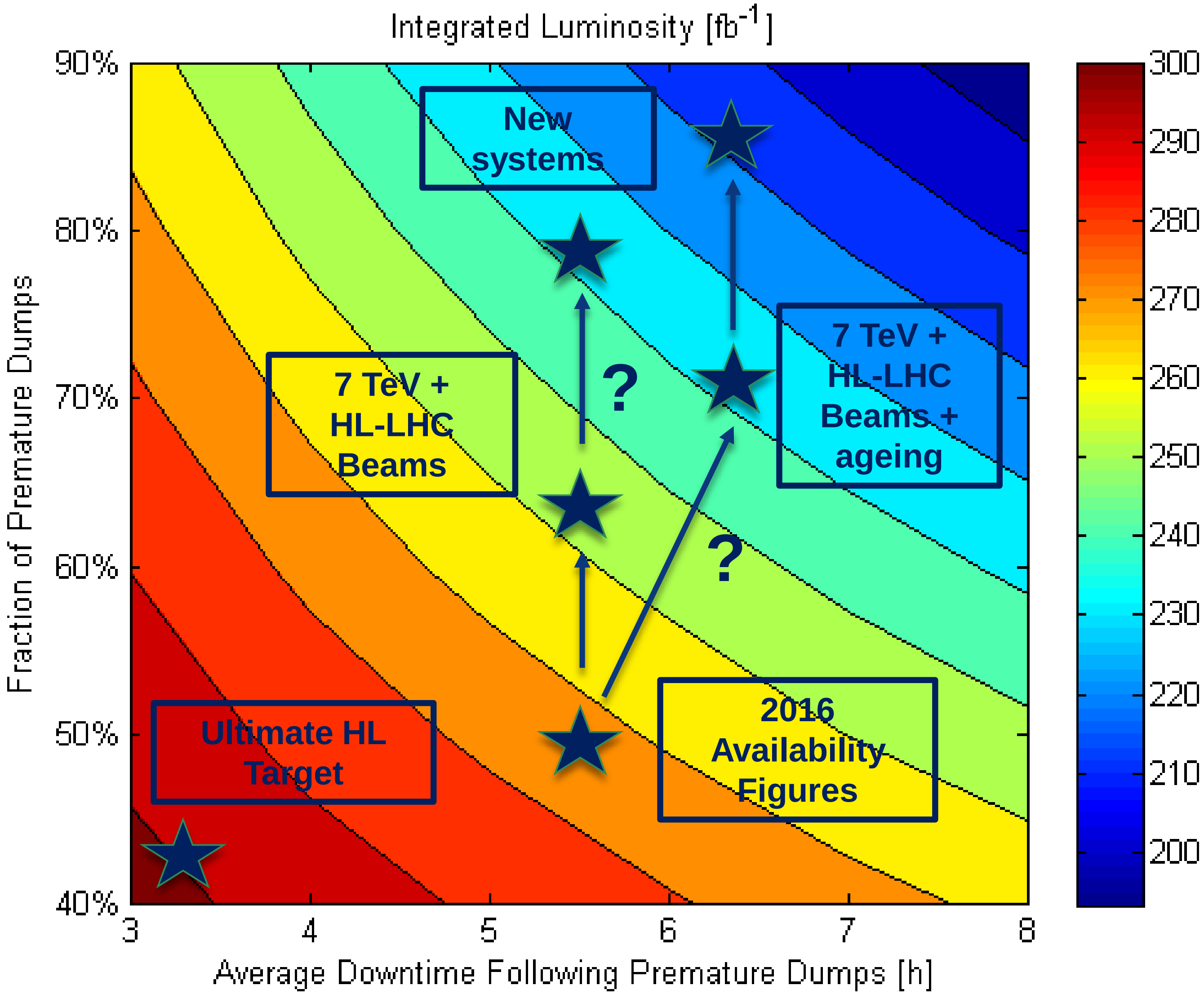
- Actual production vs. one model round
- Note the intensity ramp up at start of the year
- Assumptions: e.g. constant time between TS → Visual differences in actual and modelled productions

Results: Model Validation



- Luminosity production distribution based on 1000 simulation rounds
- Simulation result: 23.38 fb^{-1} sufficiently close to actual production 23.27 fb^{-1}

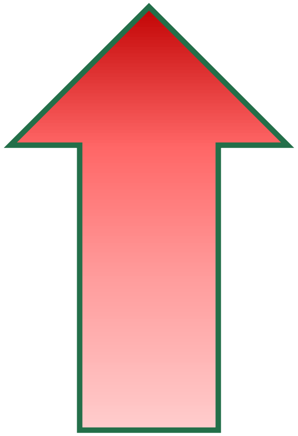
Sensitivity Analysis: HL-LHC



Machine Protection

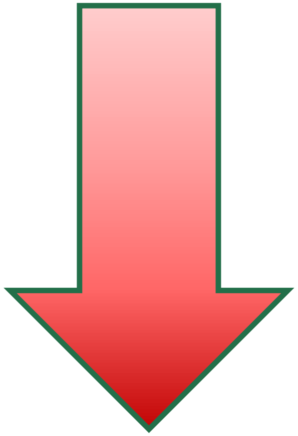
Hazard Analysis: Top-Down or Bottom-Up?

Consequences of component failure on system behaviour



Component Level

Definition of high level accidents / failure scenarios



Identification of causal factors leading to accidents

- **Maybe impractical for large projects**
- **Limited to ‘component failures’**

- **Suitable for increasing complexity**
- **Extends further than ‘component failures’**

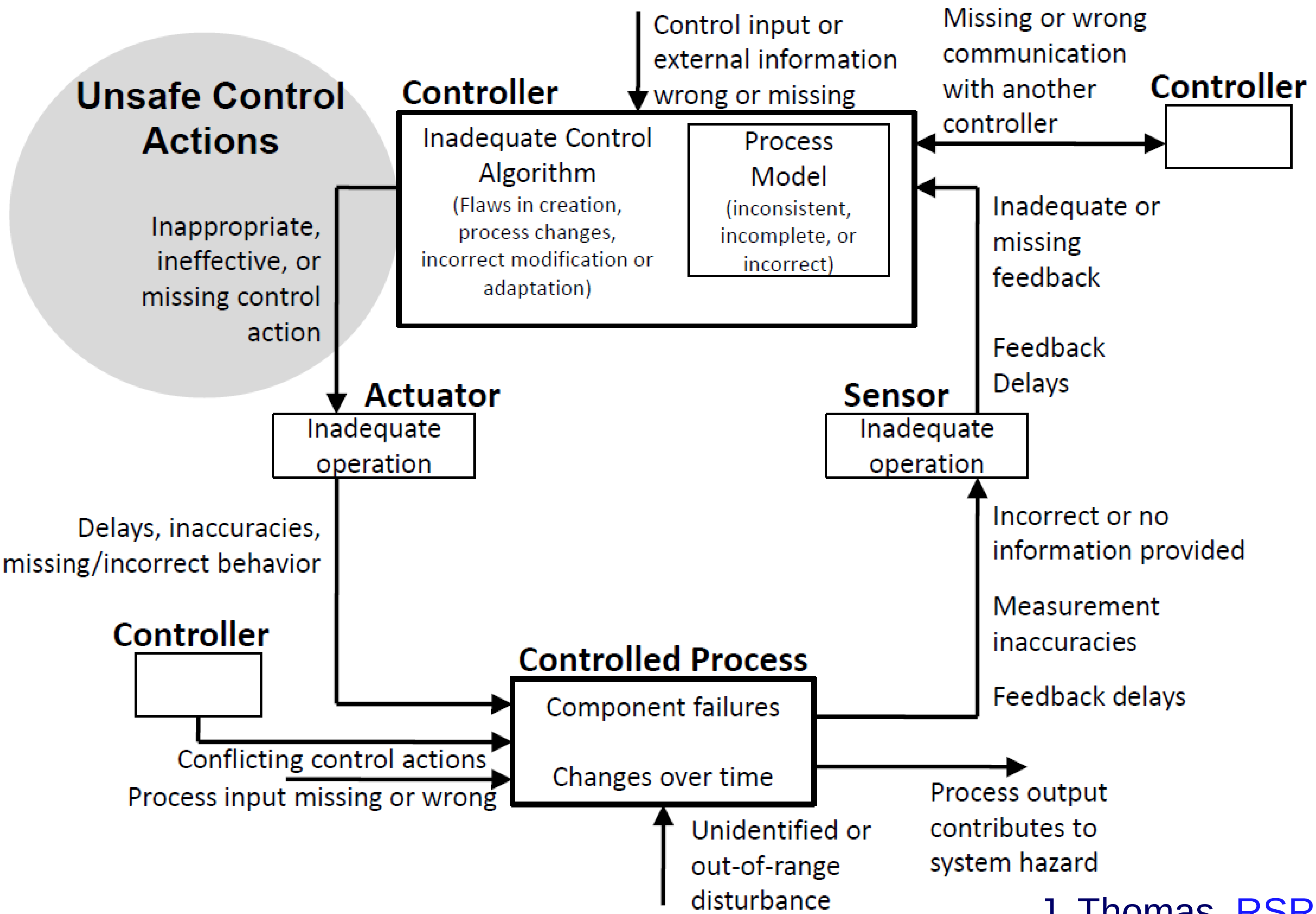
System-Theoretic Process Analysis

- Increasing **accelerator complexity** requires a systematic approach for identification of machine protection requirements
  - Address and optimize **contradictory requirements** (safety vs availability)
  - Applicable from **early design** stages (not applied to a given design)
  - Results should not regard only the **system architecture**, but also provide recommendations for correct **operation and management** of the accelerator

- Long-term goal:
  - Identify suitable method for the design of machine protection systems for the **next generation** of particle accelerators

- As a start…
  - Apply method for the **first time to a small accelerator** to verify its suitability → Linac4

Identify Causal Factors



J. Thomas, [RSRA2015]

Step 4: Causal Factors

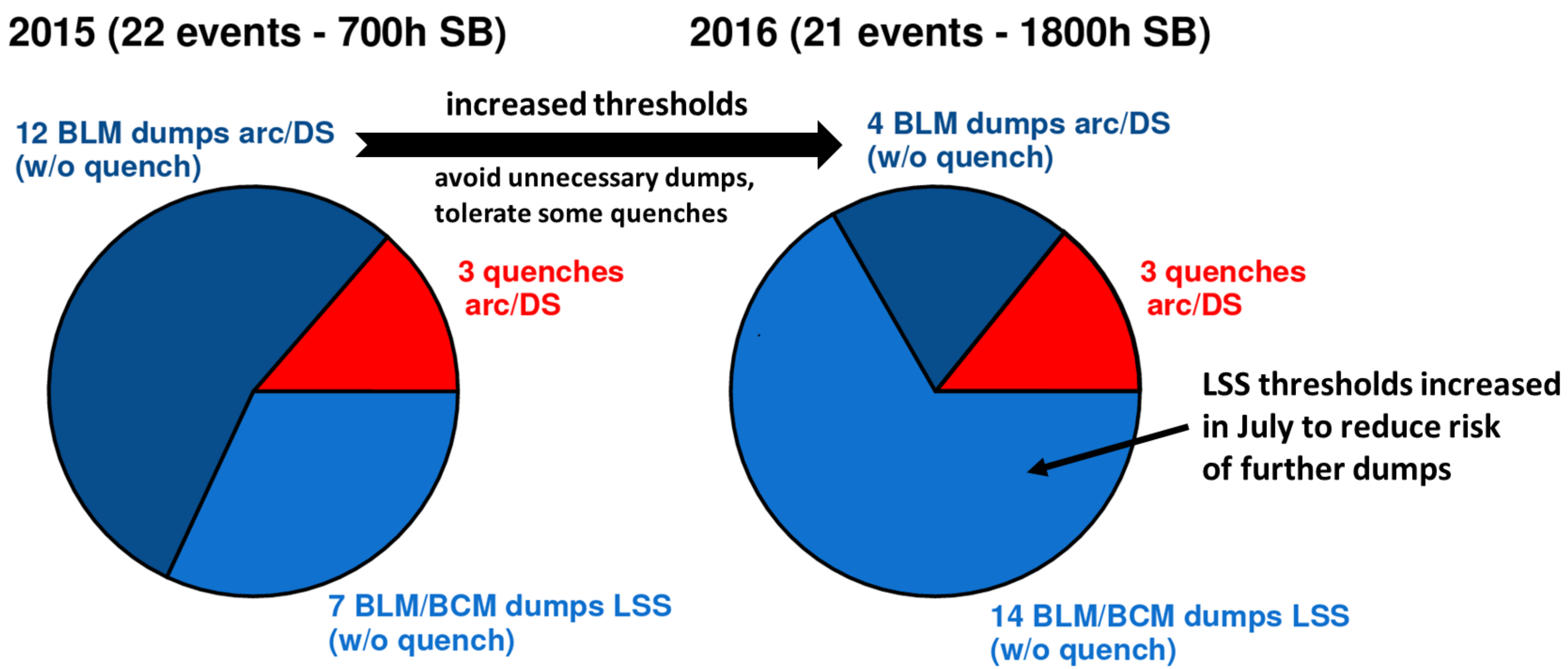
UCA: a beam stop is executed when it is not necessary			
Scenario	Associated Causal Factors	Notes	Requirements
[Control input or external information wrong or missing] Operators trigger an unnecessary beam stop	Operators accidentally act on the physical device connected to the controller	The emergrncy button in the control room is accidentally pushed	Protect the physical device from accidental contact
	Operators misinterpret feedback from instrumentation and trigger the beam stop	The operator misinterprets a singnal judging it as a relevant deviation from the nominal configuration and decides to stop the beam for safety reasons	Train operators to use softwares and processes running in the control room
	Operators act on a command that triggers a dangerous situation and thus a beam stop	The operator tries to compensate a beam or hardware setting but this leads to a dangerous state that requires a beam stop	Train operators to use softwares and processes running in the control room
	Technical personnel tries to access the linac while it is working, causing a beam stop	Techincal personnel is unaware that the machine is running and tries to access it	Require authorization from the control room for machine access
[Sensor - Inadequate or missing feedback] The sensor feedback is wrong and automatically triggers a beam stop	Sensor is faulty and causes a beam stop	A sensor signals its faulty state and determines a beam stop, even if no direct machine harm exists	A dedicated reliability analysis can assess what is the ideal number and type of sensors to be used to minimize the occurrence of false or missed detections (see chapter on calculation of intelock loop architectures)
	Spurious trigger of a sensor causing a beam stop	A sensor signals a hazardous operating condition due to a spurious failure (e.g. radiation-induced)	Consider adding redundancy. When possible, locate sensors and instrumentation far from radiation-exposed areas

- **'Practical' measures**
- **Managerial and organizational measures**
- **Procedural measures**
- **Technical requirements: trigger further analyses with traditional methods**

Protection vs Availability

UFO-induced Dumps & Quenches in 2015/16

A. Lechner



- Number of dumps & quenches depends on:
  - BLM threshold settings
  - UFO rates -> strong conditioning observed since Oct 2015, rates much lower in 2016 than in 2015

BLM threshold strategy for UFOs

A. Lechner

- Arcs and dispersion suppressors:

  If we try to prevent quenches, unnecessary dumps are unavoidable

  For availability it is better to avoid unnecessary dumps, tolerate some quenches, as confirmed by 2016 experience:

	Actual 2016 - Thresholds 3x above quench level	If we would have applied a quench-preventing strategy
Dumps	**4***	**71****
Quenches	**3**	**1** (UFO too fast)

*3 out of 4 dumps were in S12 (temporary reduction of thresholds due to suspected inter-turn short)

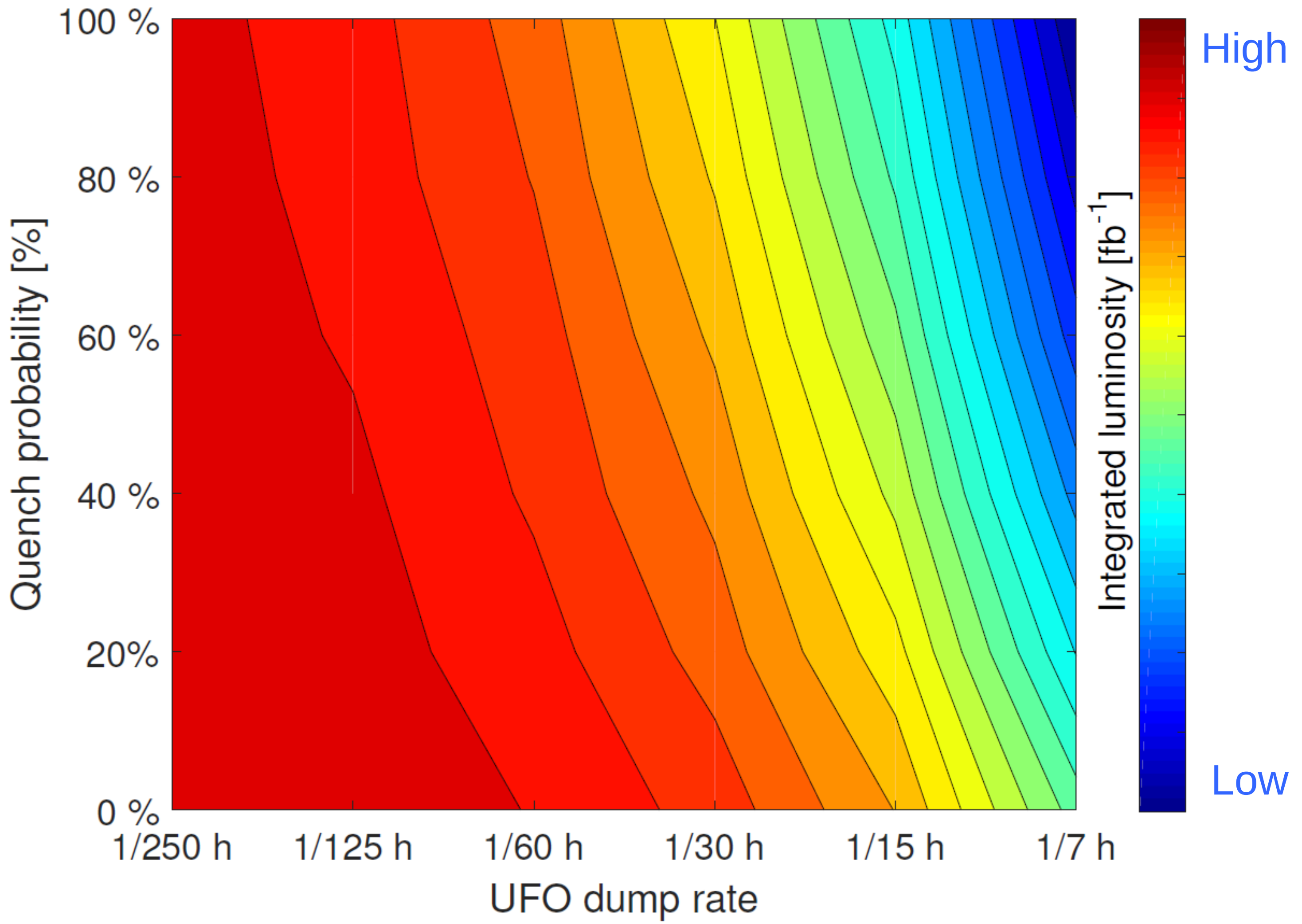
** Simple count of 2016 fills which would have been prematurely dumped if tenfold lower thresholds would have been applied in all sectors throughout the whole year. Multiple occurrences per fill are only counted once.

  Would adopt same strategy at 7 TeV -> "only" consequence is increased risk of quenches

- Long straight sections:

  Expect that local UFO hot spots can be mitigated with threshold increase (as done in 2015 and 2016)

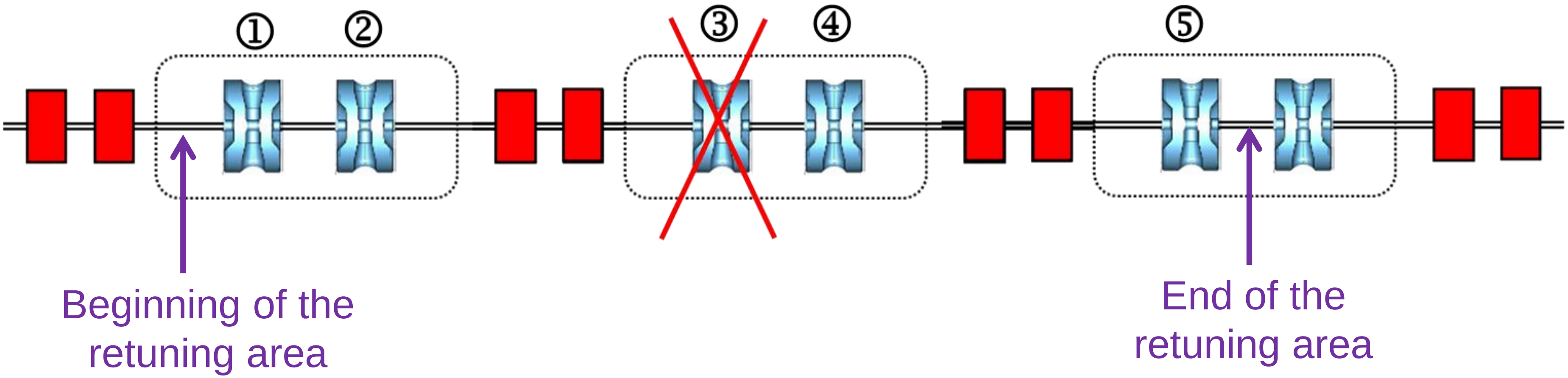
BLM Thresholds and UFOs



ADS: An Exceptional Case

- In most of the accelerators it is frequent to experience **preventive shutdowns** of accelerator operation in case of equipment failures
- A preventive shutdown for ADS is considered to be a **SCRAM**
- Huge **thermal stresses** induced in the reactor following a SCRAM
- In addition, ~24 h needed for recovery of operating conditions due to legal procedures
- Limited number of SCRAMs tolerated → avoid ‘false failures’
- For example: for MYRRHA all failures in the accelerator lasting more than 3 s potentially lead to a SCRAM

Solution: Dynamic Failure Compensation



- **<u>1st criterion</u>**: recover the same transfer matrix of the retuned area than in nominal condition
- **<u>2nd criterion</u>**: the total Energy gain should remain the same than in the nominal case
- **<u>3rd criterion</u>**: the time of flight should remain the same than in the nominal case

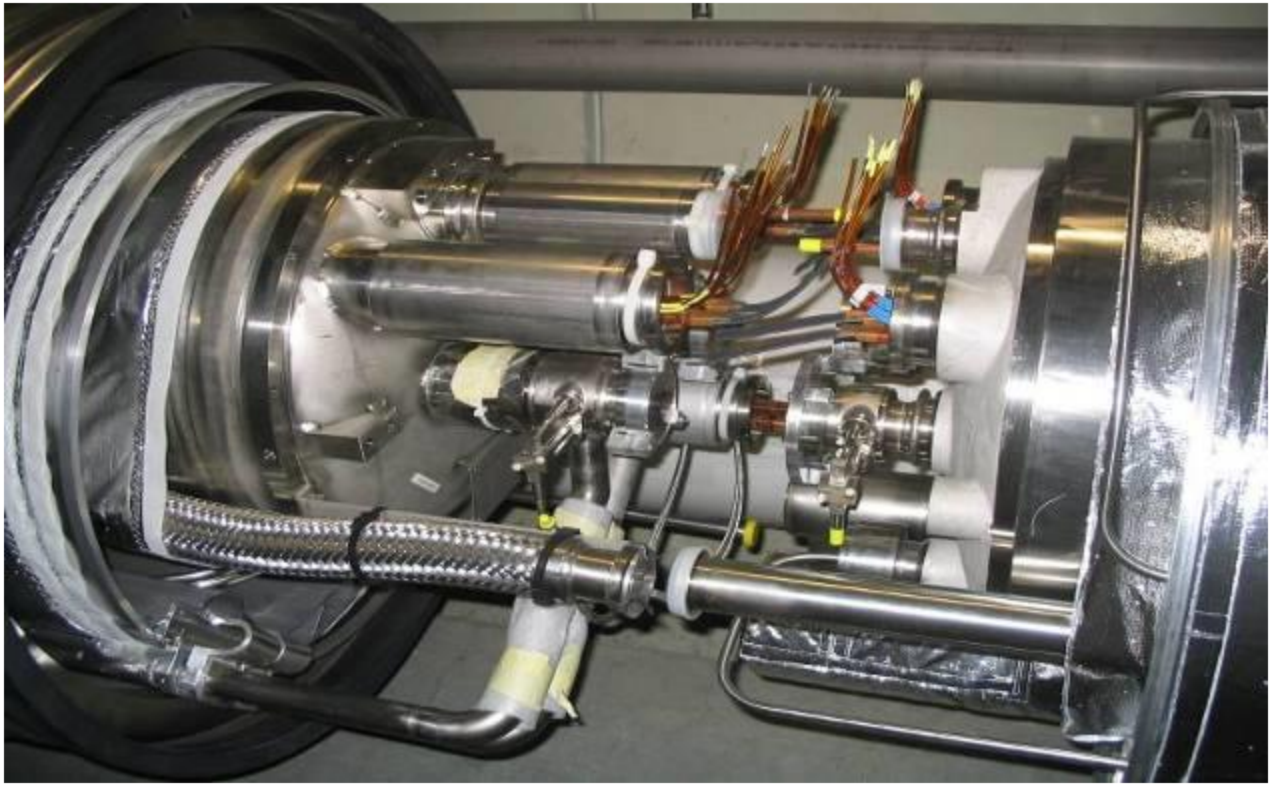
To be done in less than 3 seconds for MYRRHA…

Courtesy F. Bouly, MYRTE WP2 Meeting, October 2016

Additional Factors Influencing the Achieved Protection Level

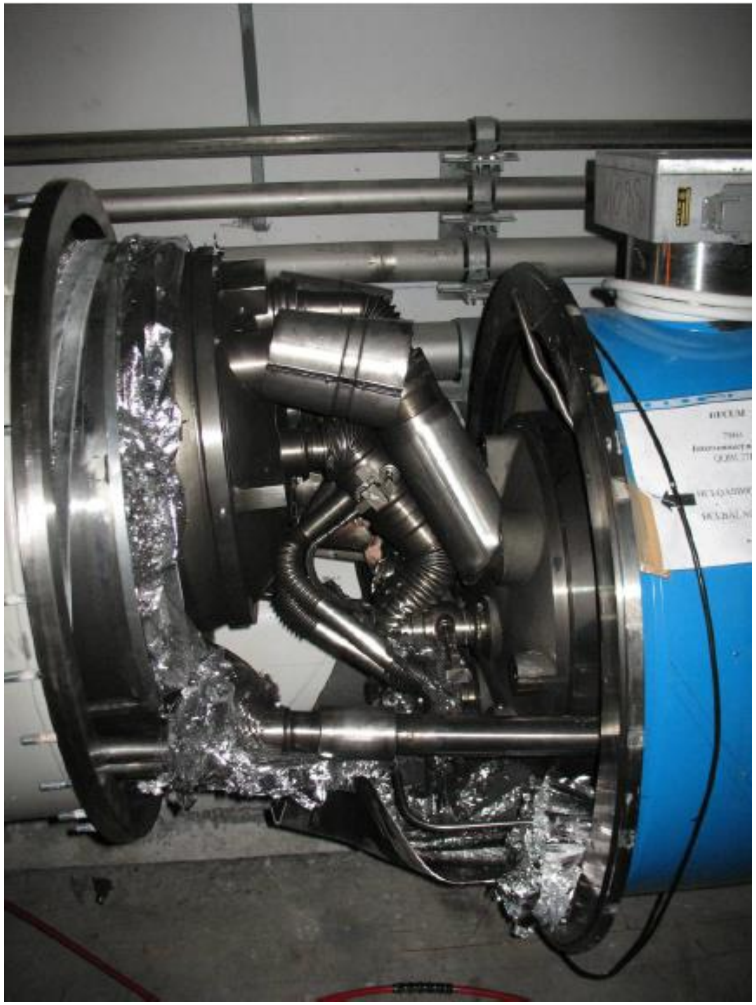
The incident of 19 September 2008

- **10000** high current superconducting **cable joints** – all soldered in situ in the tunnel and **one** of these connections was **defective**



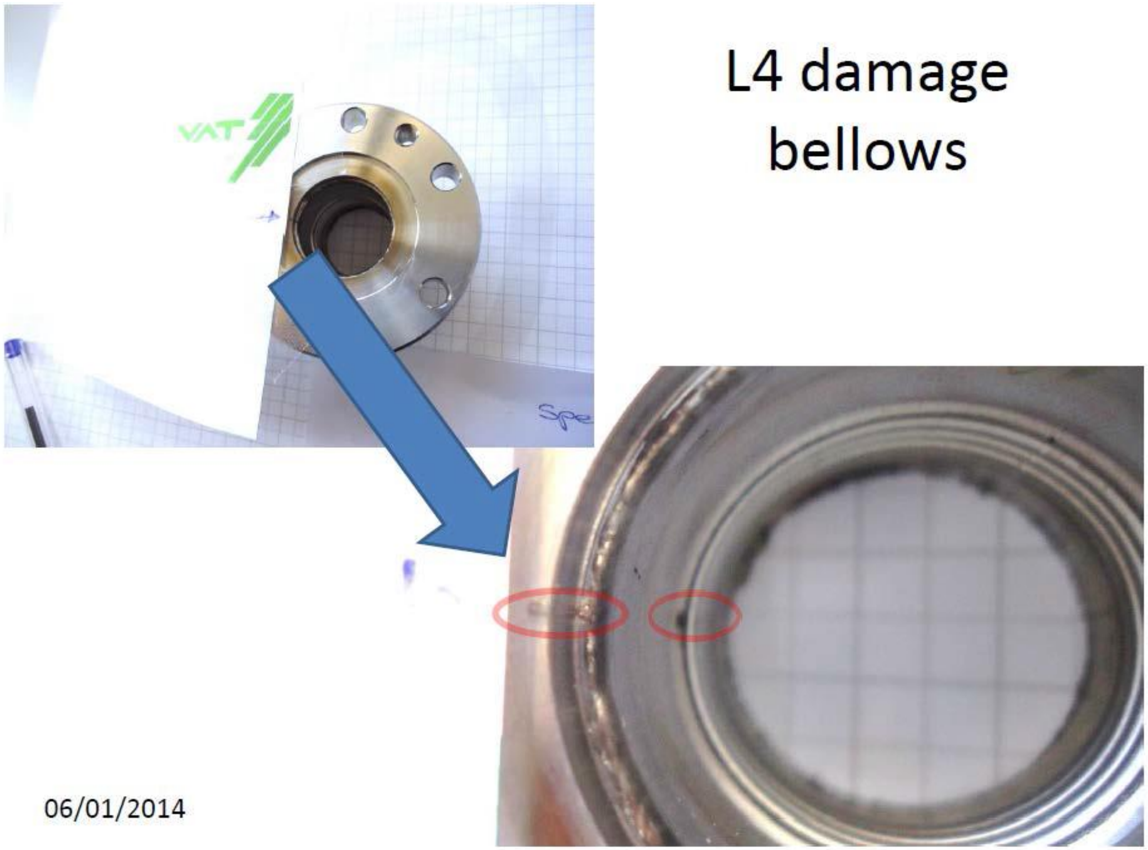
- **One joint ruptured, with 600 MJ stored in the magnets – 70% of this energy was dissipated in the tunnel, electric arcs, vaporizing material, and moving magnets around**

The incident of 19 September 2008



Other factors play a role: quality assurance, time constraints,…

Damage to Linac4 Vacuum Bellow

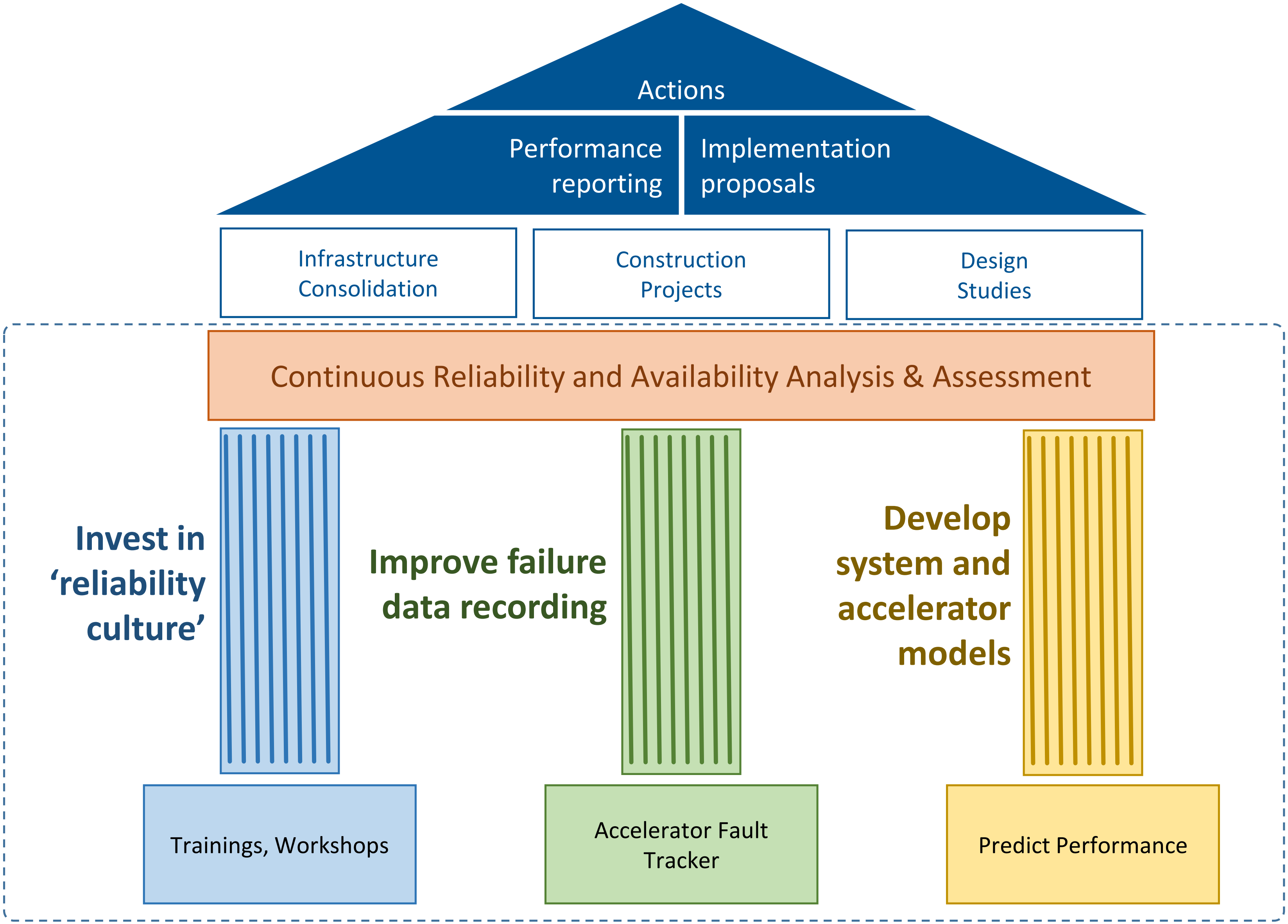


1) Severe misalignment between the RFQ and the MEBT
2) Optic that favoured amplification of this misalignment (test)
3) Phase advance such that the loss occurred on the “wave” of the bellow (200 µm) and it is an aperture limitation

Accidents might occur due to a combination of different factors (change of boundary conditions, non-standard operation, design flaws, human intervention,…)

Conclusion

3 Pillars


Actions
Performance reporting
Implementation proposals
Infrastructure Consolidation
Construction Projects
Design Studies
Continuous Reliability and Availability Analysis & Assessment
Invest in ‘reliability culture’
Improve failure data recording
Develop system and accelerator models
Trainings, Workshops
Accelerator Fault Tracker
Predict Performance

Ideas for the Future

- Protection for future High-Power / High-Energy accelerators will be fundamental to prevent long stops due to equipment damage
  - Evaluate methods for the design of the future generation of Machine Protection Systems

- Limiting maintenance actions on accelerator equipment will be a key factor for the success of the next generation of large-scale accelerators
  - Conceive from the design phase systems with a high degree of redundancy and flexibility
  - Reduce only to 'essential' equipment located in the tunnel
  - Invest in advanced diagnostic techniques (e.g. failure prediction via pattern recognition,…)
  - Explore the potential of developments in robotics for remote maintenance

- Optimize accelerator schedules
  - Today for the LHC only ~150 days per year are allocated for luminosity production
  - Design systems thinking about faster commissioning (with and without beam)
  - Limit the number of technical stops (synchronize with injectors)

Thanks a lot for your attention!!