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

A. Apollonio
CERN Machine Protection Group (TE-MPE)
IPAC'18 – 04/05/2018
andrea.apollonio@cern.ch

Acknowledgements: TE-MPE Group, CERN Availability Working Group, Accelerator Fault Tracking team.

= Particle Accelerator Community

Decades of experience designing accelerator systems without formal reliability engineering studies

Reliability Engineering applied to particle accelerators is a relatively new discipline, based on industry best practices and methods

Developed very consistently over the last years – why?

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 70 % after 100 h in operation, at an operating current of 80 mA”

- **Availability (0-1)** is the probability that a system in a functional state at a 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”

- Discussions are ongoing in the particle accelerator community to tailor these definitions to different machines (Accelerator Reliability Workshop)

Accelerators Applications and Availability

Fundamental Physics
(e.g. LHC, CERN, Geneva)

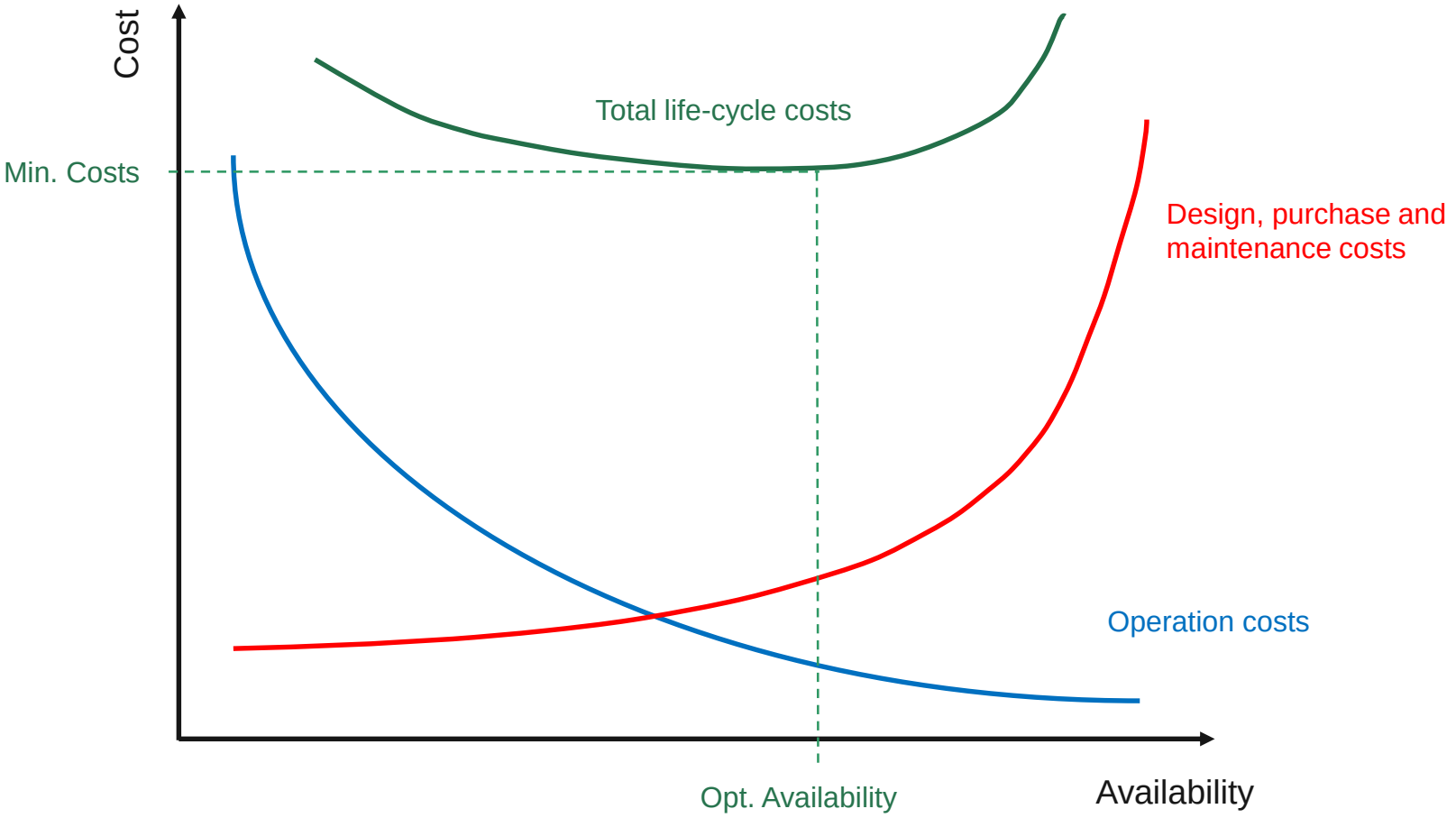
Why is availability a concern for these facilities?

- Money
- Reputation
- Damage potential

Medical Accelerators
(e.g. CNAO, Pavia)

User-oriented facilities
(e.g. Soleil, France)

Cost vs Availability

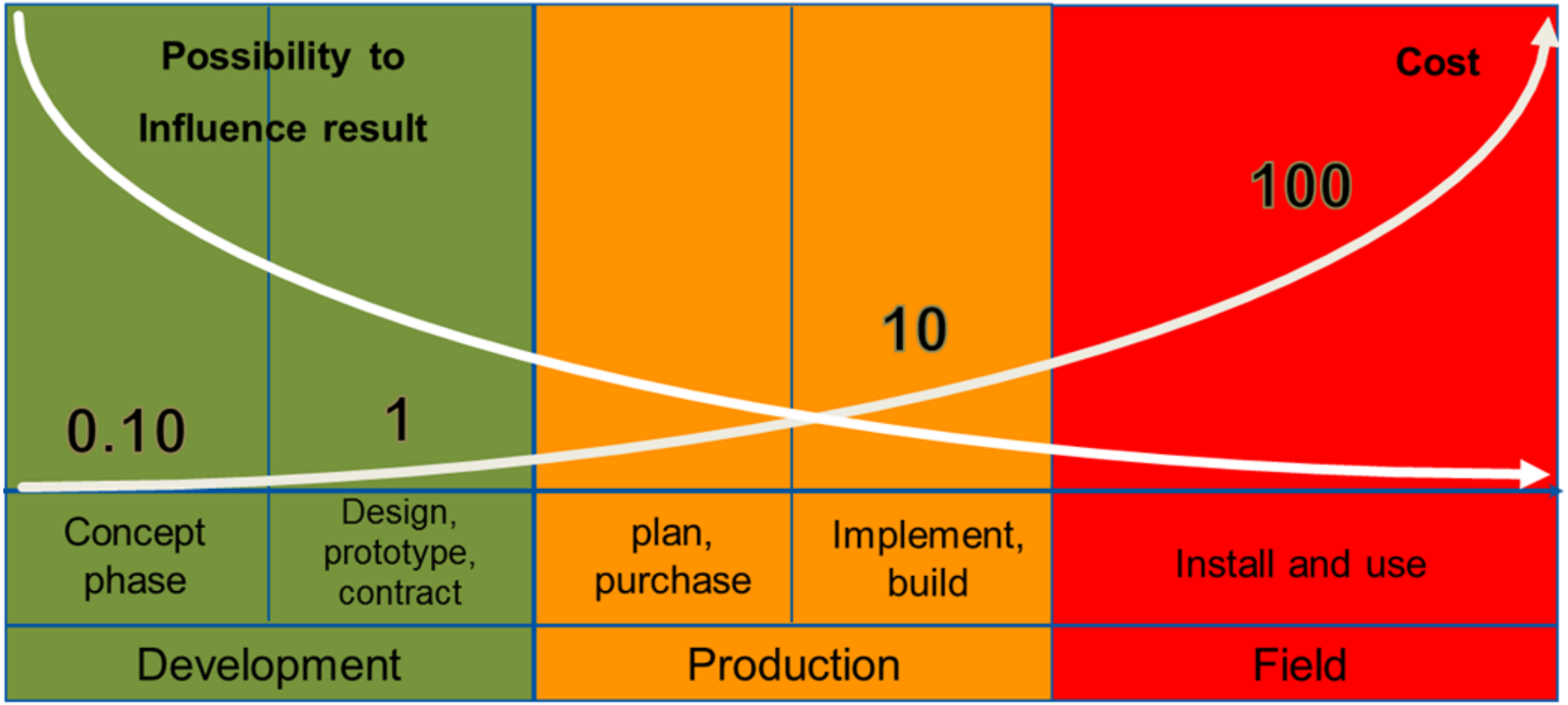


- Given a target performance reach (neutron fluence, number of patients treated, luminosity production, …), an optimal balance between capital costs and operation costs must be found
- This is an **absolute MUST** for the feasibility of next-generation machines

Reliability Studies: if yes, when?

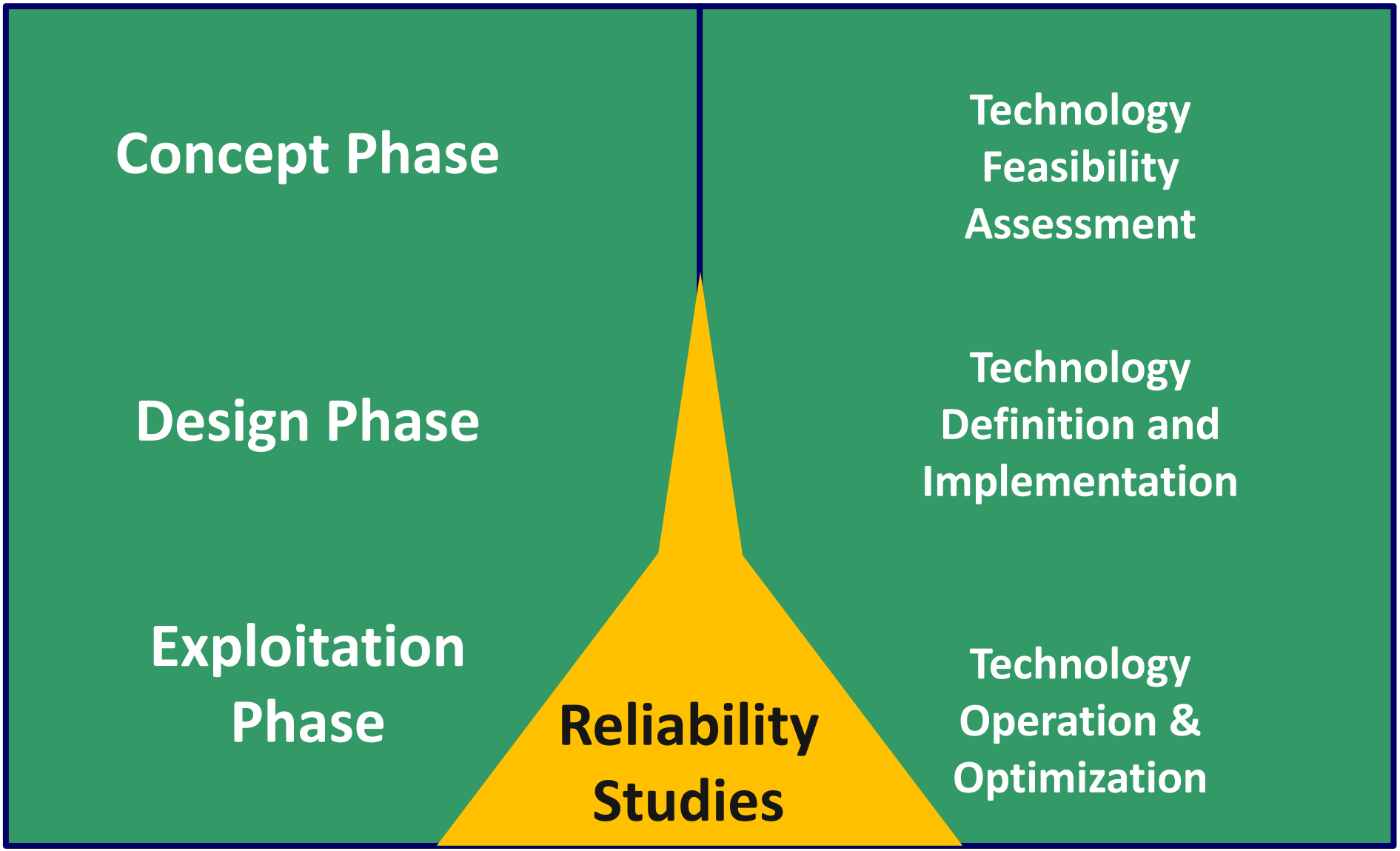
Prof. Dr. B. Bertsche, Dr. P. Zeiler, T. Herzig, IMA, Universität Stuttgart, CERN Reliability Training, 2016

- Product Lifecycle: 'Power-of-10 Law'

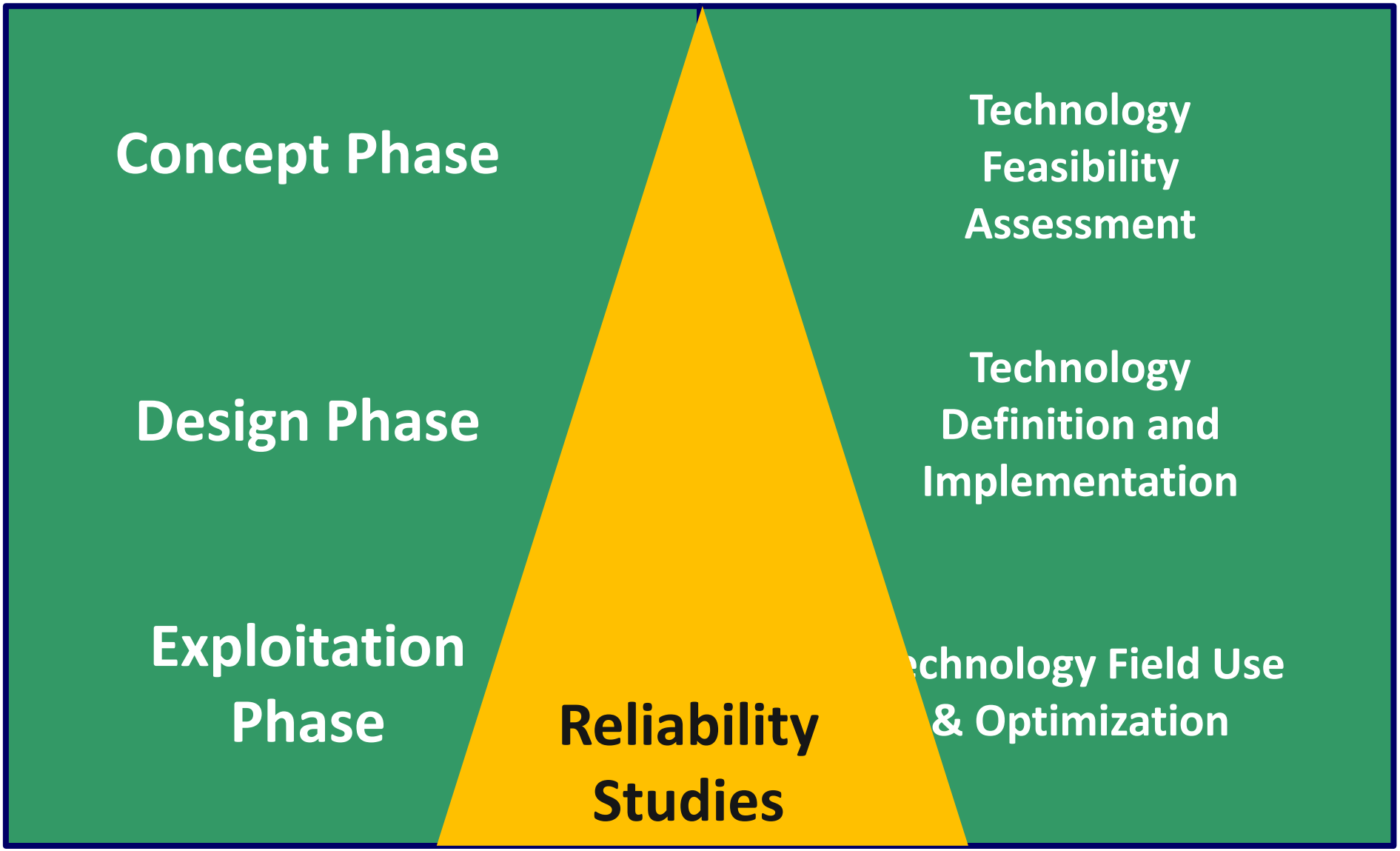


- The earlier reliability constraints are included in the design, the more effective the resulting measures will be

Today: Reliability Studies for Accelerators



Future: Reliability Studies for Accelerators



Reliability Analyses of Accelerator Systems

If *no explicit reliability target* is set for a given system/accelerator, reliability analysis could (should!) still be performed. Most design/architecture flaws can be intercepted already by a **qualitative reliability analysis** (e.g. *Failure Mode and Effect Analysis*)
Result: documentation on expected weak points of the design, recommendations (priorities) on possible changes

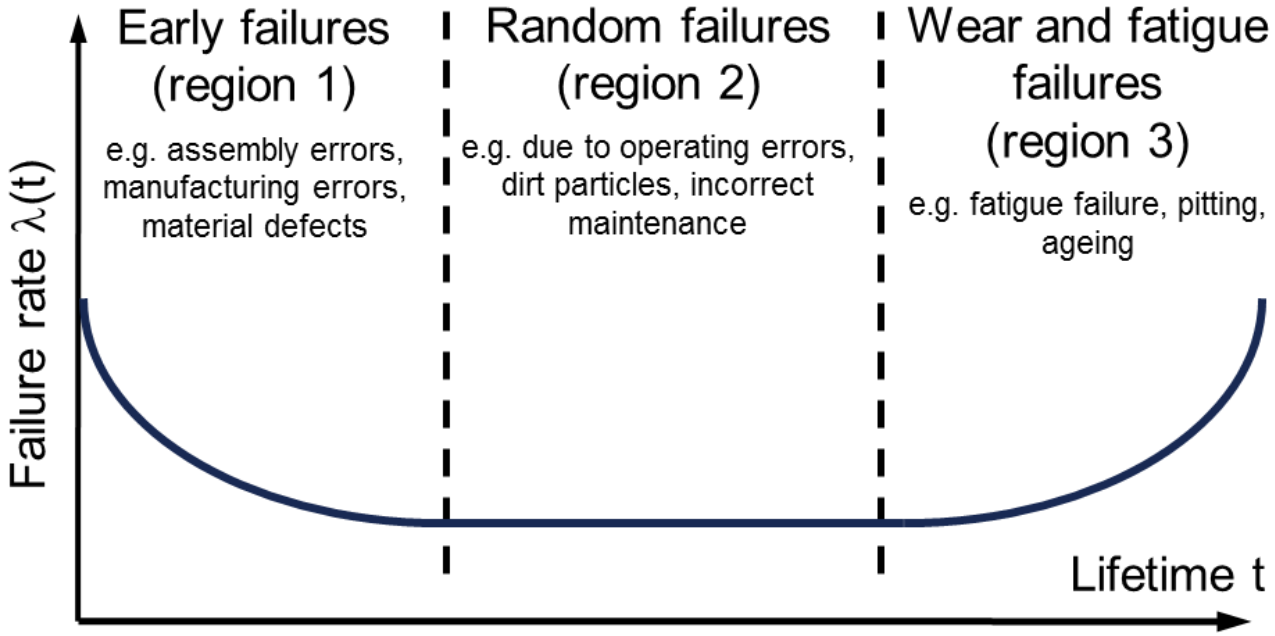
If *a design has to meet explicit reliability targets*, then a **quantitative reliability analysis** should be performed (e.g. *Fault-Tree analysis*)
Result: calculation of probability of failure and expected performance

Reliability Analyses: LHC was a Game Changer for CERN

First particle accelerator with damage potential beyond repair
Requirement 1: Must have active Machine Protection Systems (MPS) → Interlocks
Requirement 2: MPS must meet very strict reliability requirements
Requirement 3: MPS must not trigger unnecessary beam interruptions

Quantitative Analyses: Failure Rate λ

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



- 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

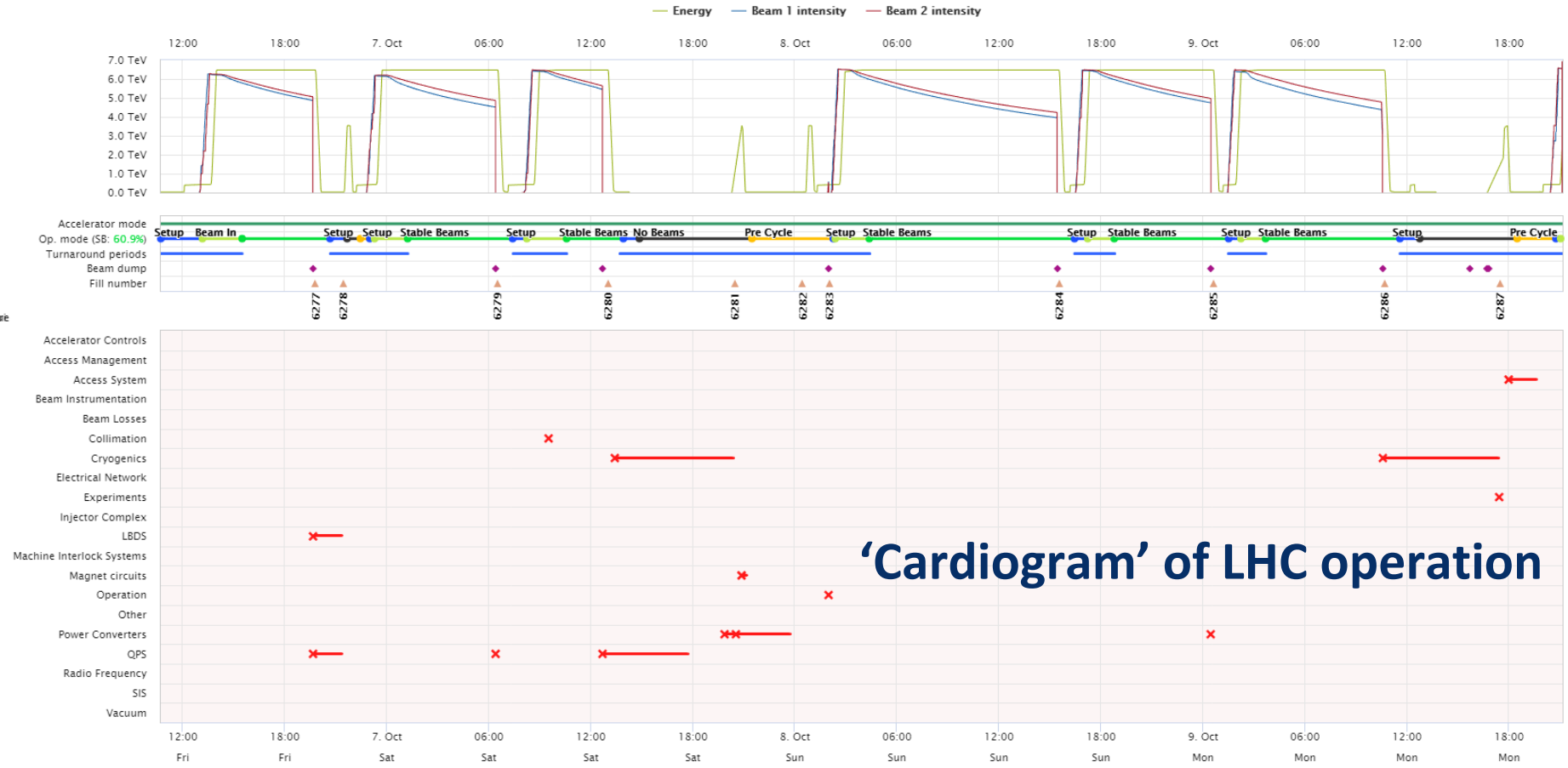
- Tests:
  - Accurate results
  - Large number of samples to be tested / long time for testing (impractical)
  - Accelerated lifetime tests (if applicable)
- Expert estimates
  - Big uncertainties on boundary conditions
  - Good approximation for known technologies
  - Good for preliminary estimates
- Using Standards (e.g. 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 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

Importance of Tracking Failure Data

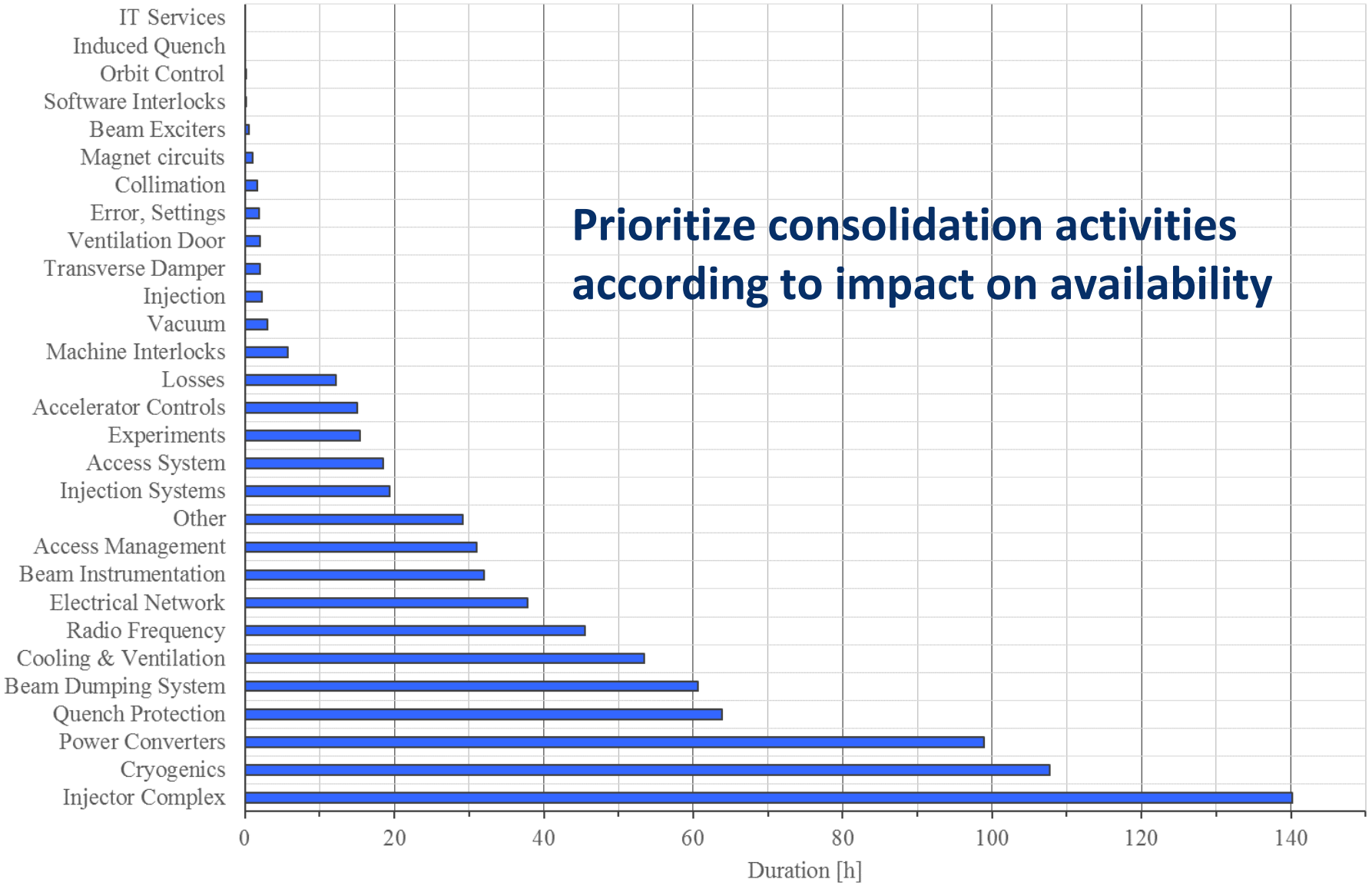
Systematic follow-up of failures → learn from experience → possible reduction of recovery times (faster diagnostics, faster repairs, better management of spare parts,…)

Since 2015 at CERN, Accelerator Fault Tracker in use to keep consistent records of accelerator system reliabilities during LHC lifetime



‘Cardiogram’ of LHC operation

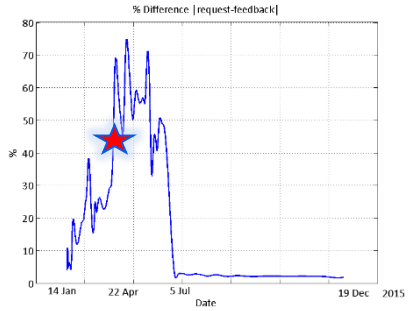
LHC Downtime Contributors in 2017



Failure Duration

Failure Duration

Identification



Diagnostics

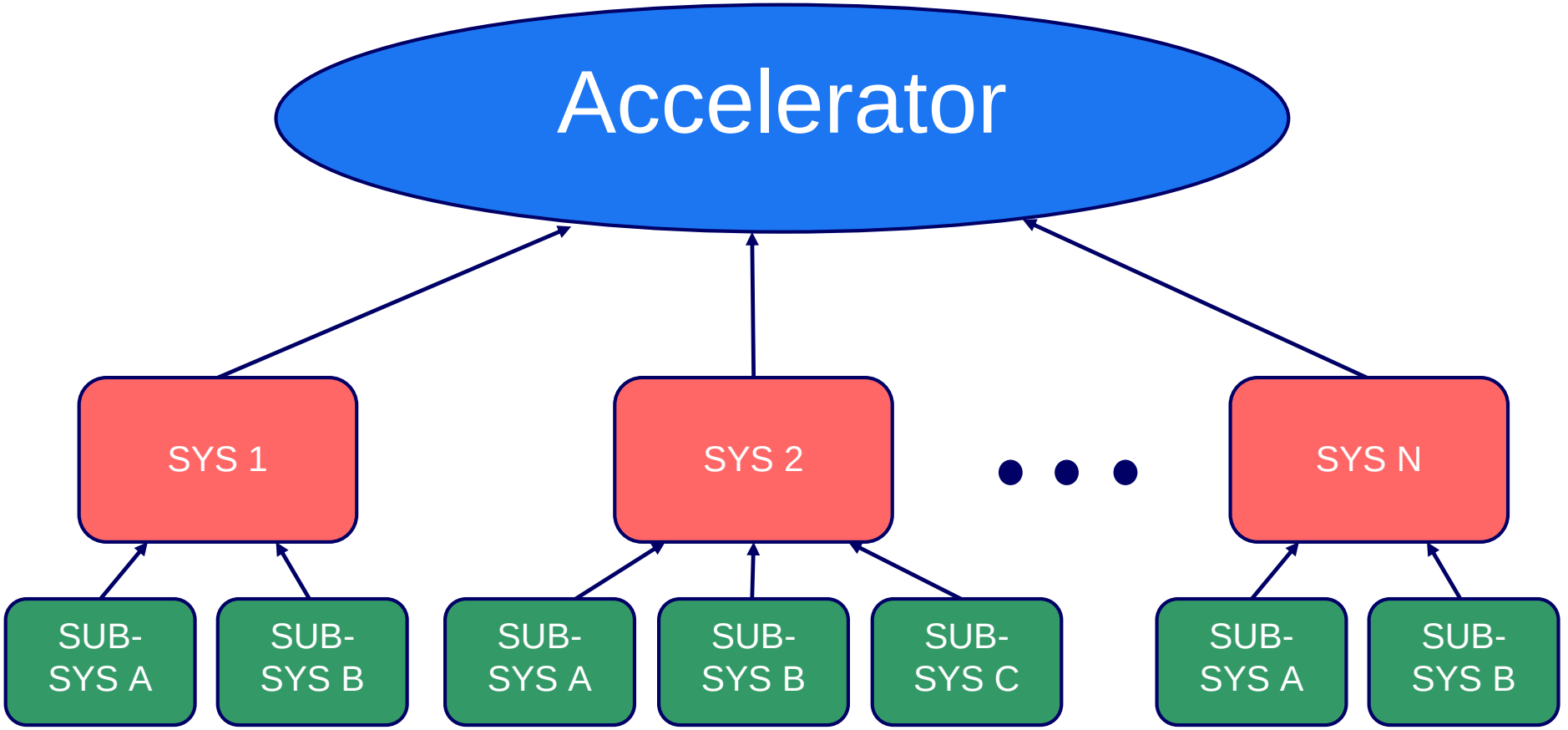
Logistics

Repair

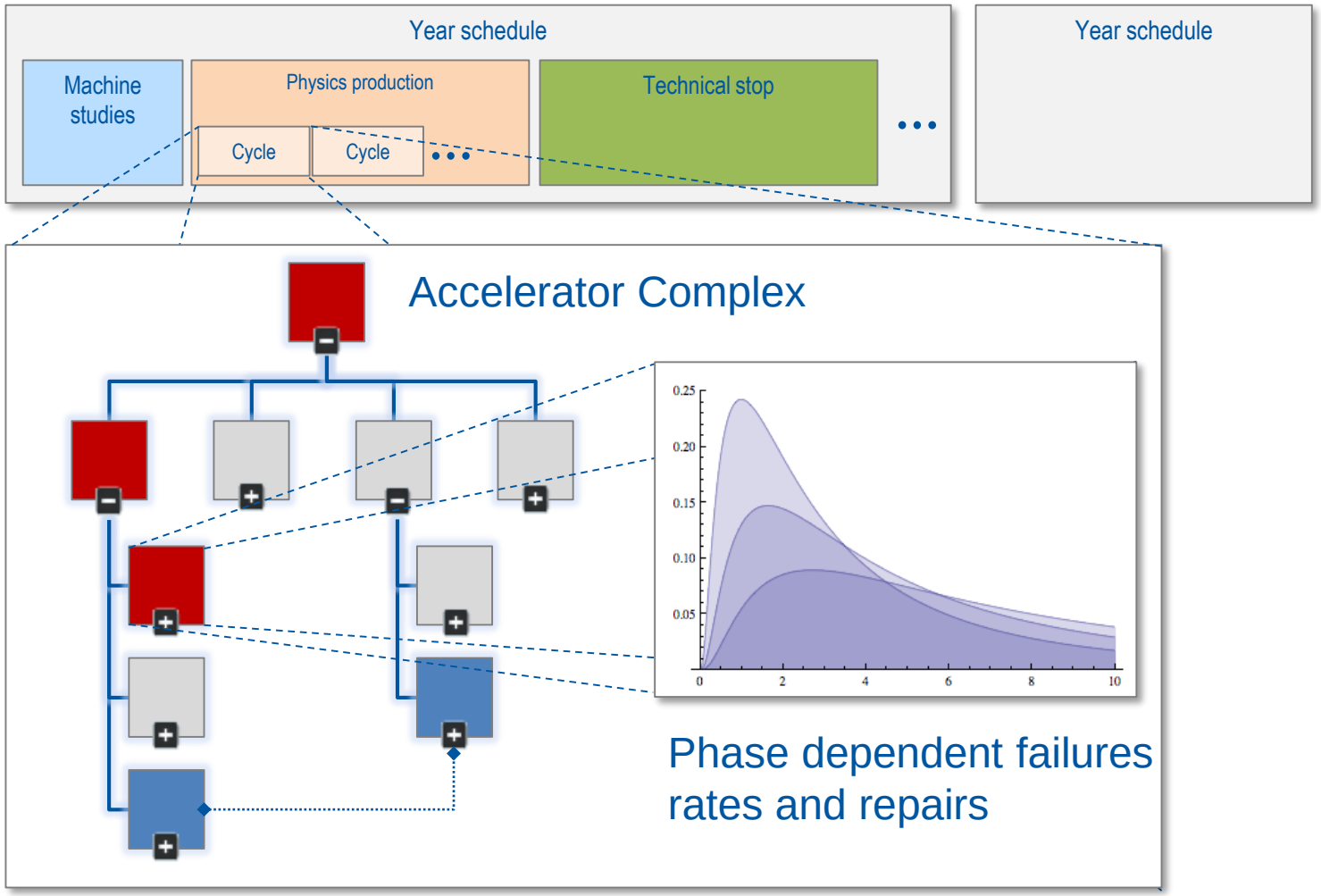
- **Mean Time to Repair (MTTR)**: the average time required to repair a failed component or device.
- In addition, some time might be required to recover nominal operating conditions (e.g. beam-recommissioning, source stabilization, magnetic pre-cycles,…)

Accelerator Modelling Concept

Prediction of future accelerator performance based on historic data



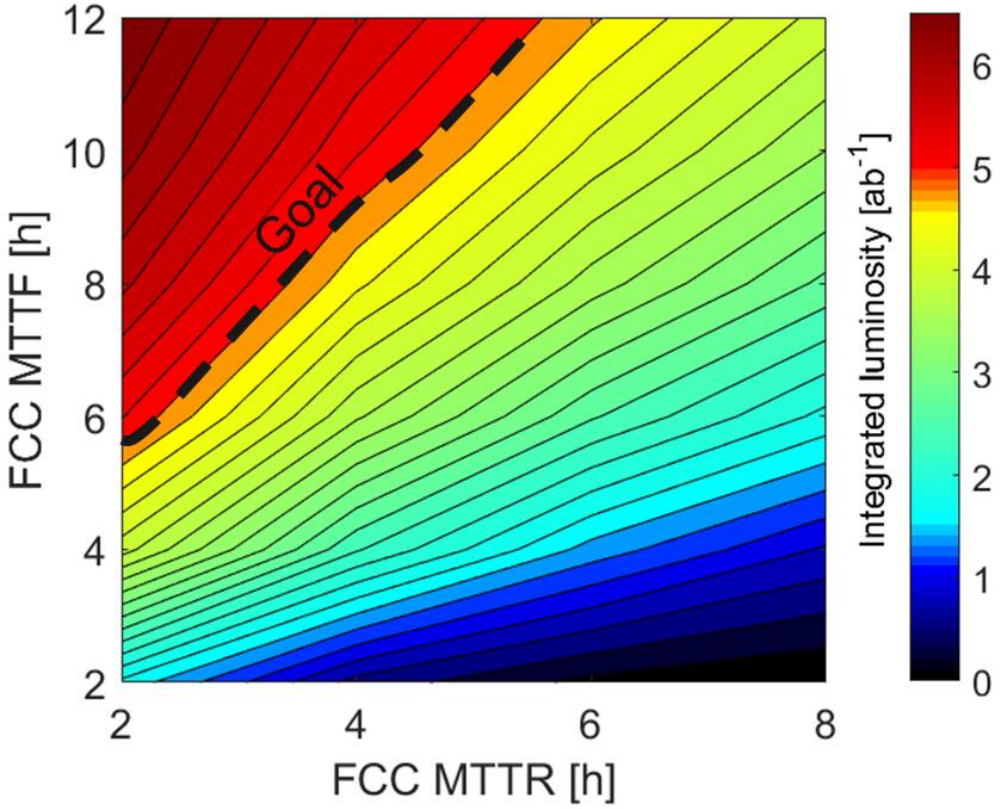
Modelling for Cycling Machines



Model Applications

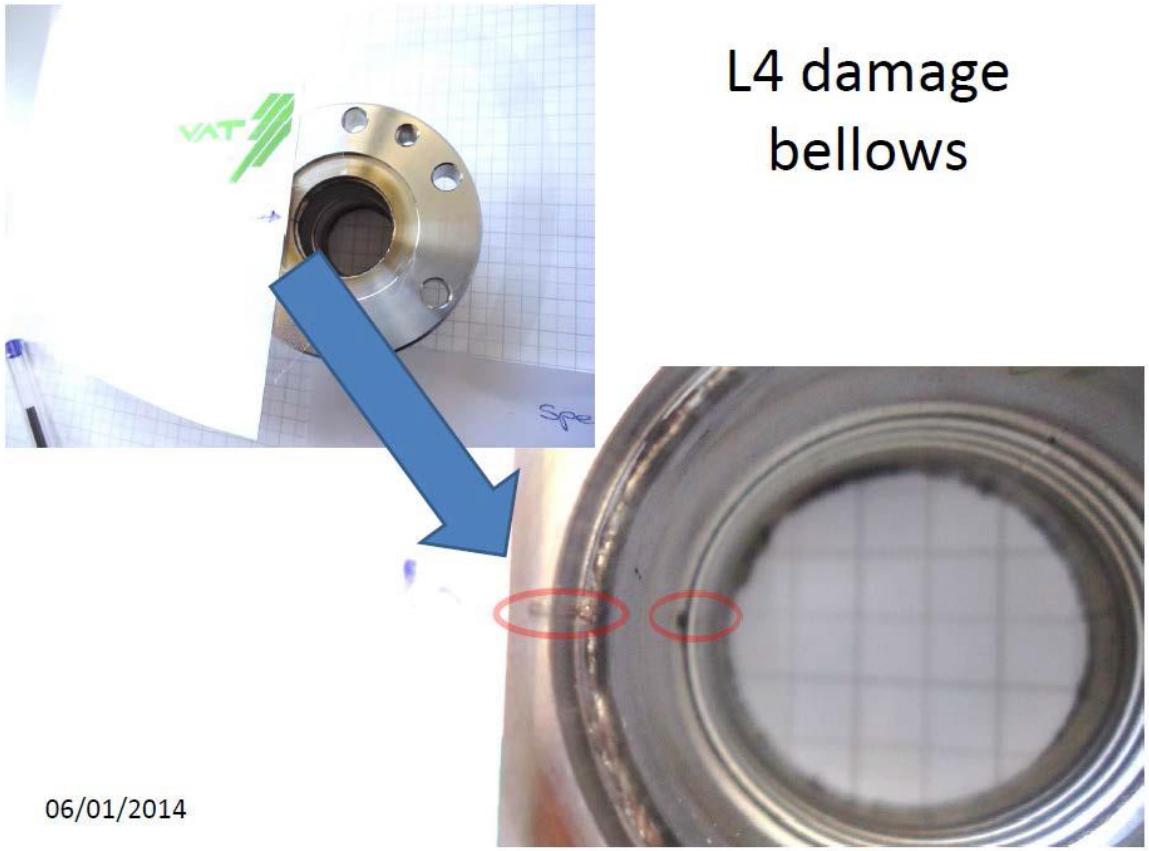
- **Monte Carlo simulations** of accelerator operation:
  - Accelerator cycles, faults and luminosity production
- Fault tree description of system availability/reliability:
  - Failure rates + repair times
- Requires **accurate data** for meaningful predictions, not always available to the desired level of detail
- **Fault Tracking** of operating accelerators is fundamental for accurate performance predictions of future machines

'Sensitivity Analysis' for integrated luminosity production of the Future Circular Collider



A. Niemi, A. Apollonio et al, "Availability modelling approach for future circular colliders based on the LHC operation experience", Phys. Rev. Accel. Beams 19, 2016.

Does It Always Work?



1) Severe misalignment in the low-energy section
2) Optics 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

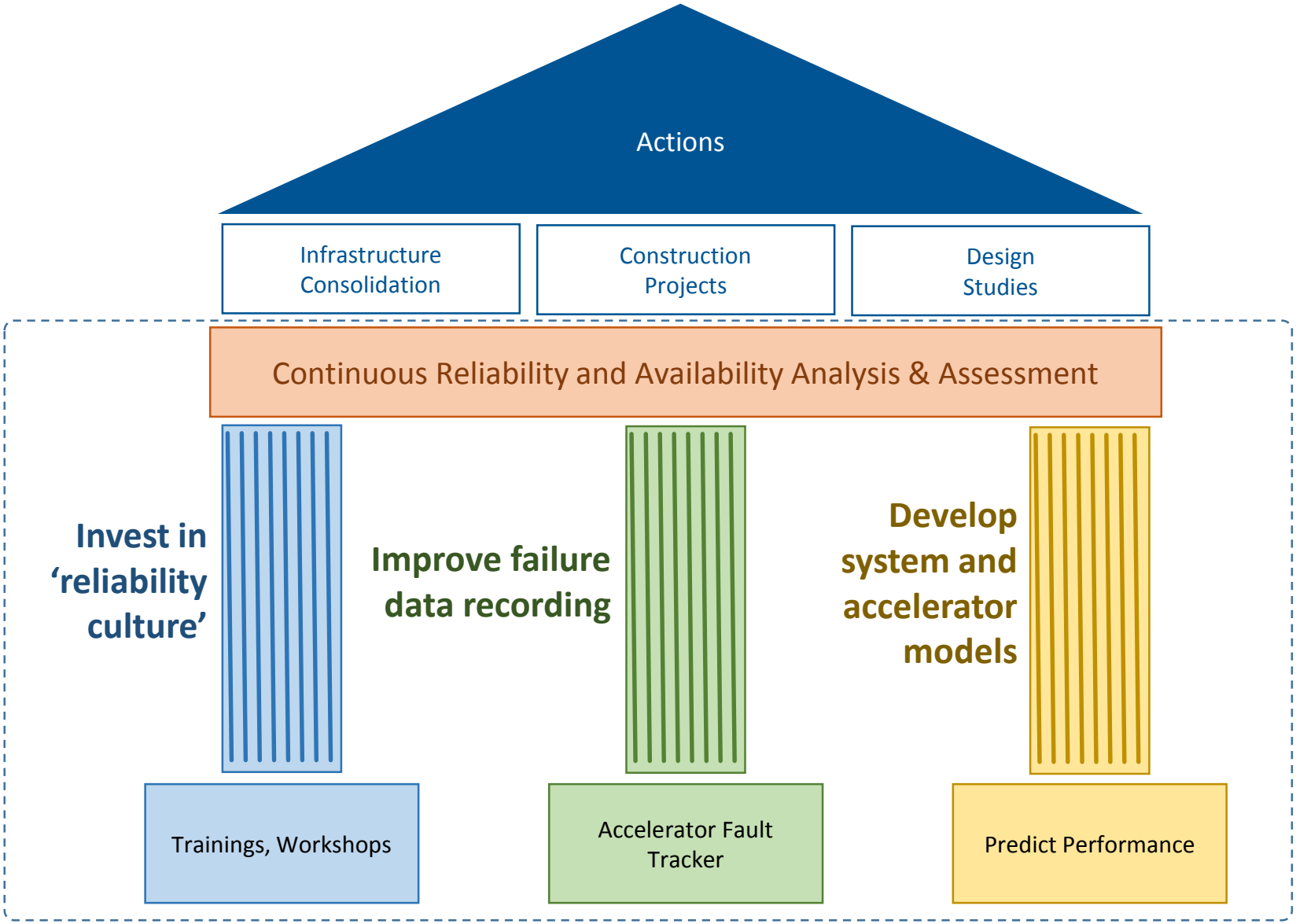
Accidents might occur due to a combination of different factors (change of boundary conditions, non-standard operation, design flaws, human errors, timing contraints…)

Outlook

- Achieving high **availability will be a key requirement** for the success of next-generation particle accelerators and needs to be pursued from early design phases

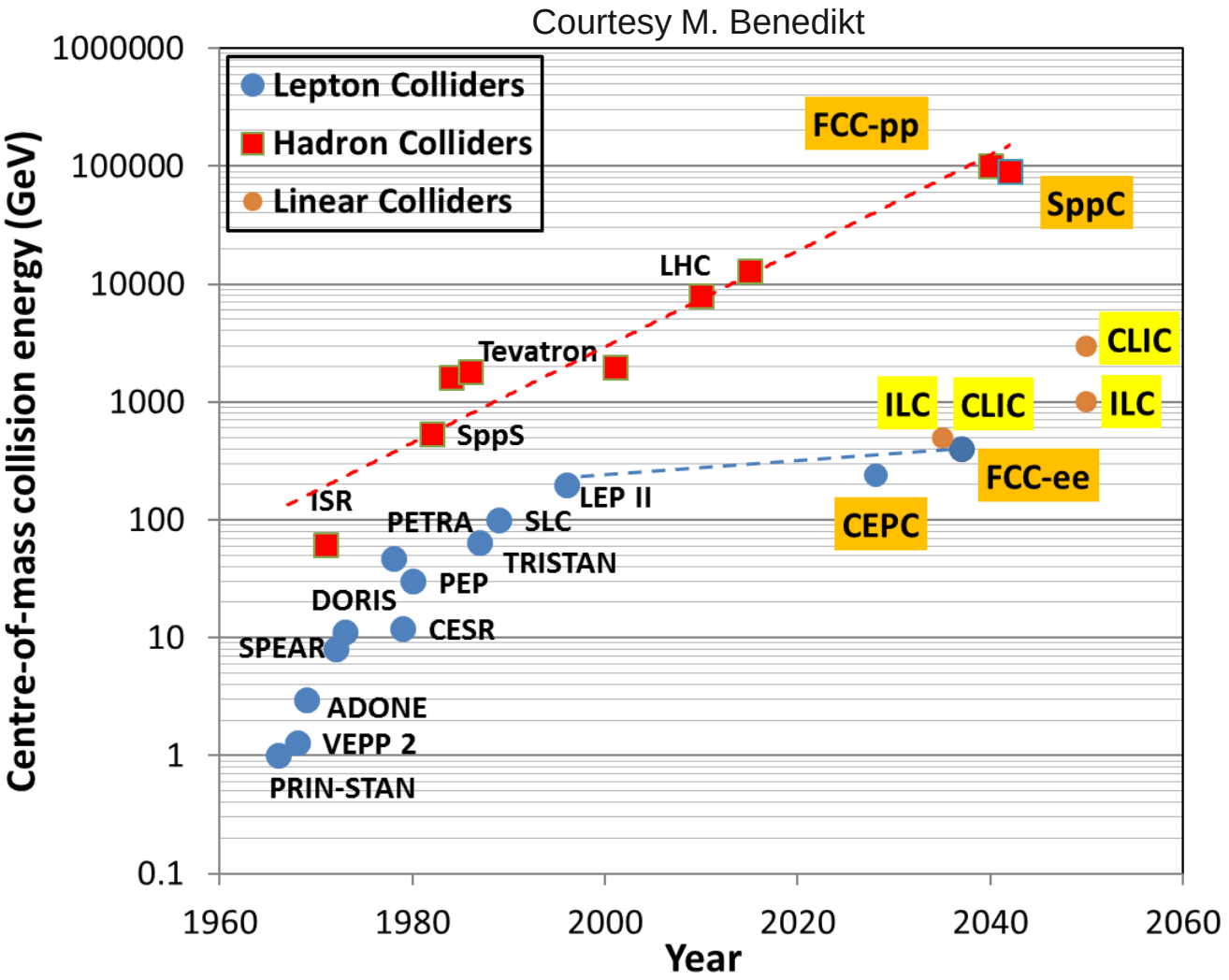
- Strategies to achieve the required availability for large-scale machines:
  - Design systems with a high degree of redundancy / fault tolerance → Target **maintenance-free operation → TOTAL AVAILABILITY** (B. Todd, R. Schmidt, L. Felsberger)
  - Reduce logistics time → Robotics for **remote maintenance**
  - Invest in **advanced diagnostics** techniques → Anticipate failure occurrence (failure prediction via pattern recognition,…)

Conclusions




Total
Availability
Source: https://www.mrusselphotography.com/blog/lynn-canyon-suspension-bridge/

Looking at the Future…



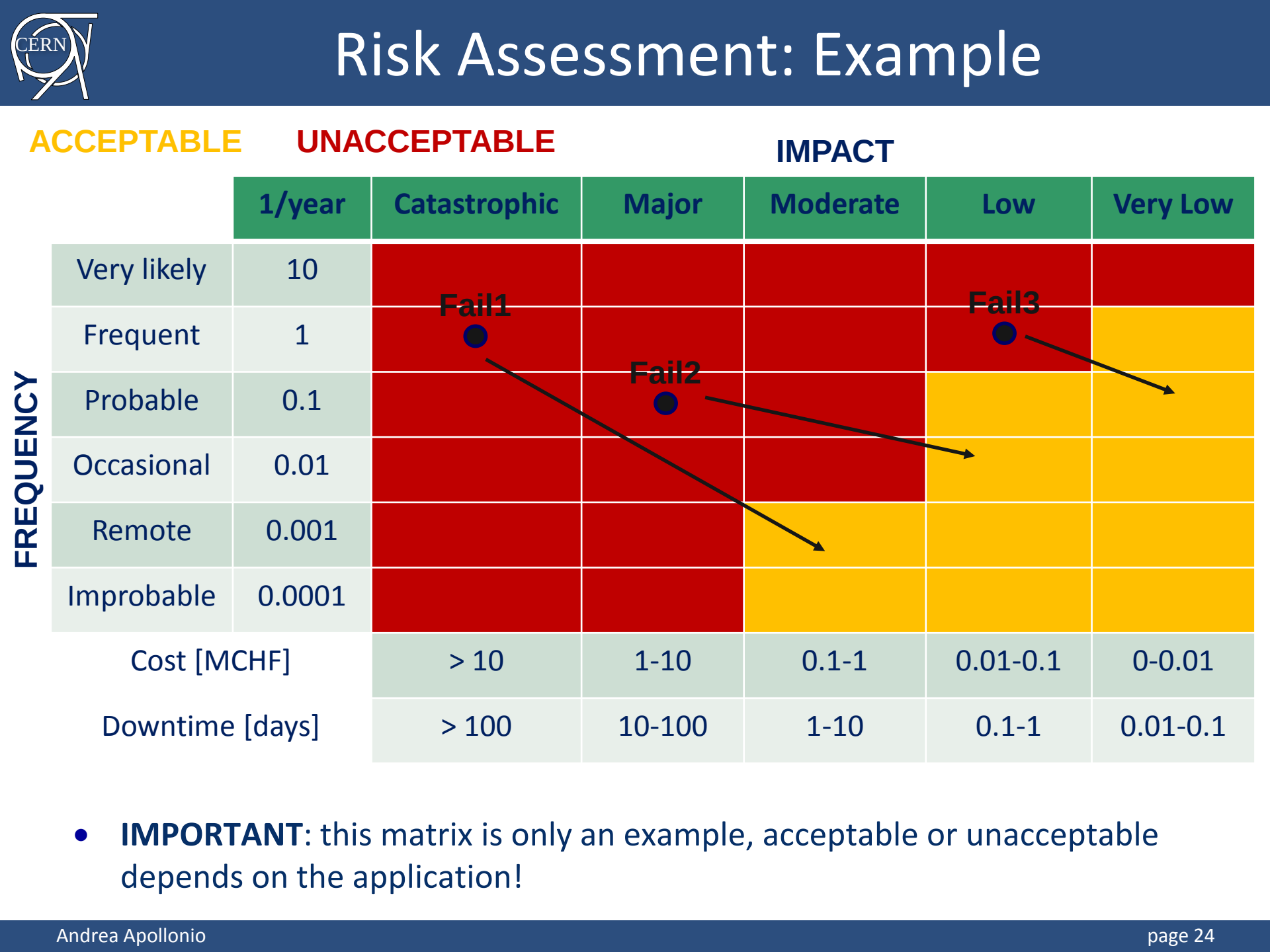
All future machines will push the energy/power frontiers beyond present limits
This is also true for accelerators other than colliders

Risk Assessment: Example

ACCEPTABLE **UNACCEPTABLE**

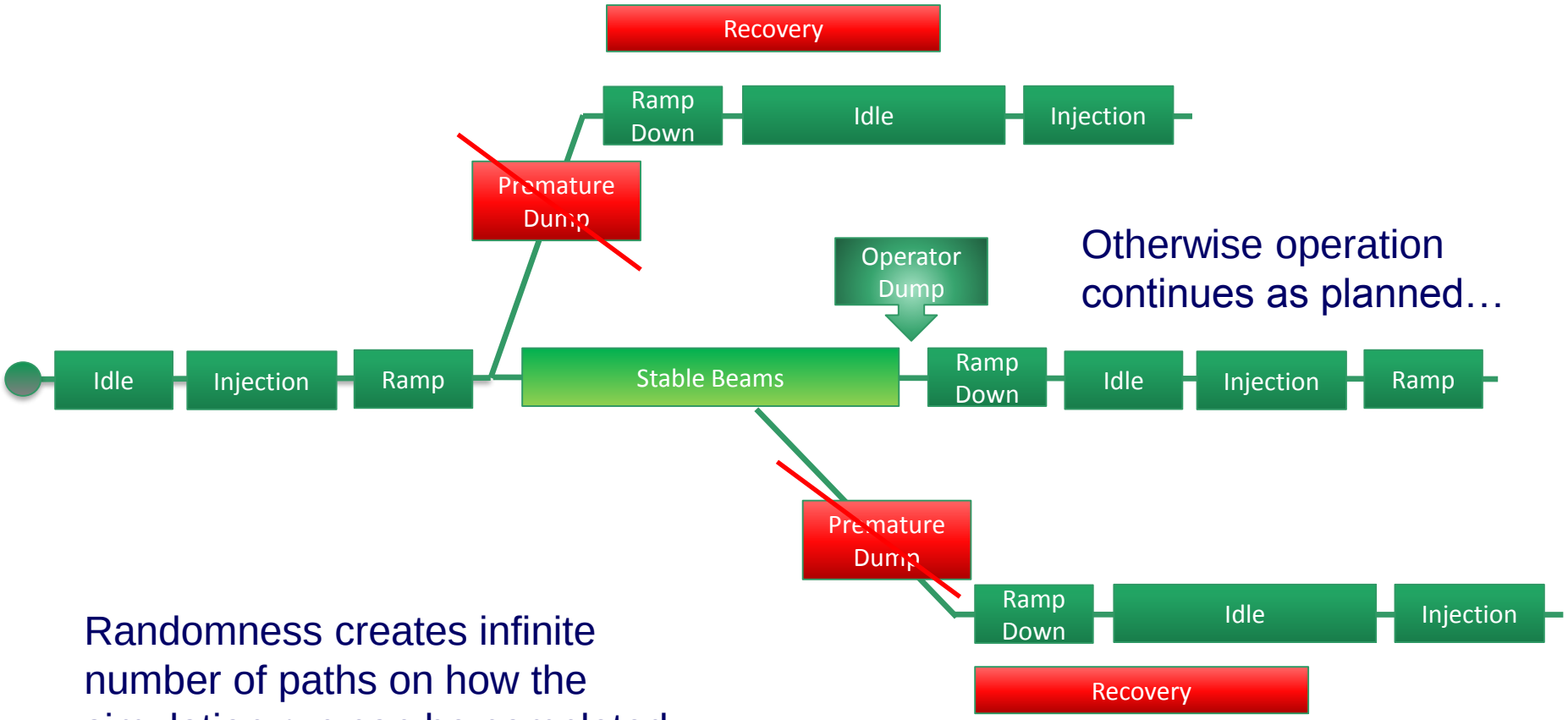
IMPACT

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]		> 10	1-10	0.1-1	0.01-0.1	0-0.01
Downtime [days]		> 100	10-100	1-10	0.1-1	0.01-0.1



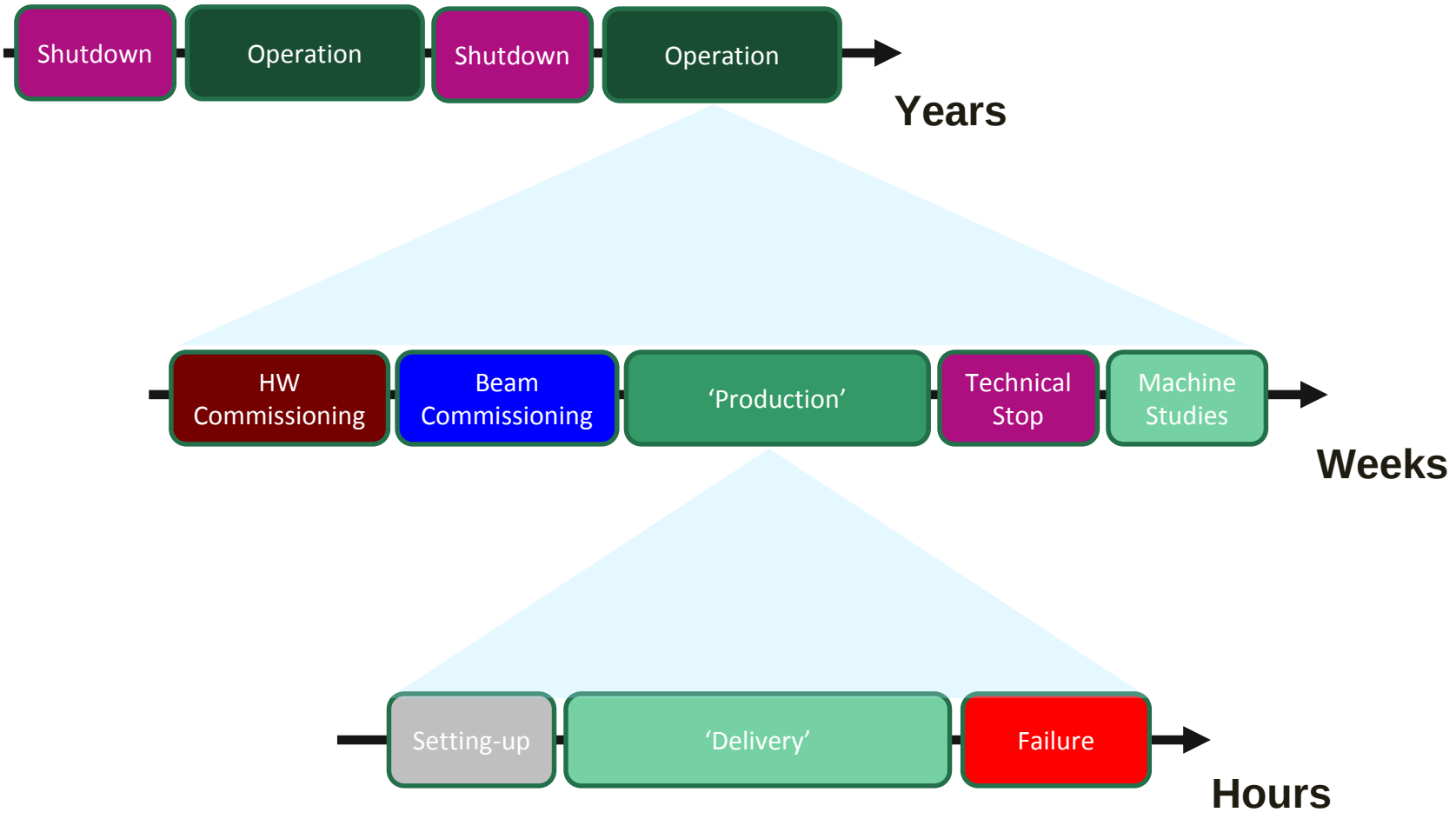
- **IMPORTANT**: this matrix is only an example, acceptable or unacceptable depends on the application!

Monte Carlo Simulation Concept

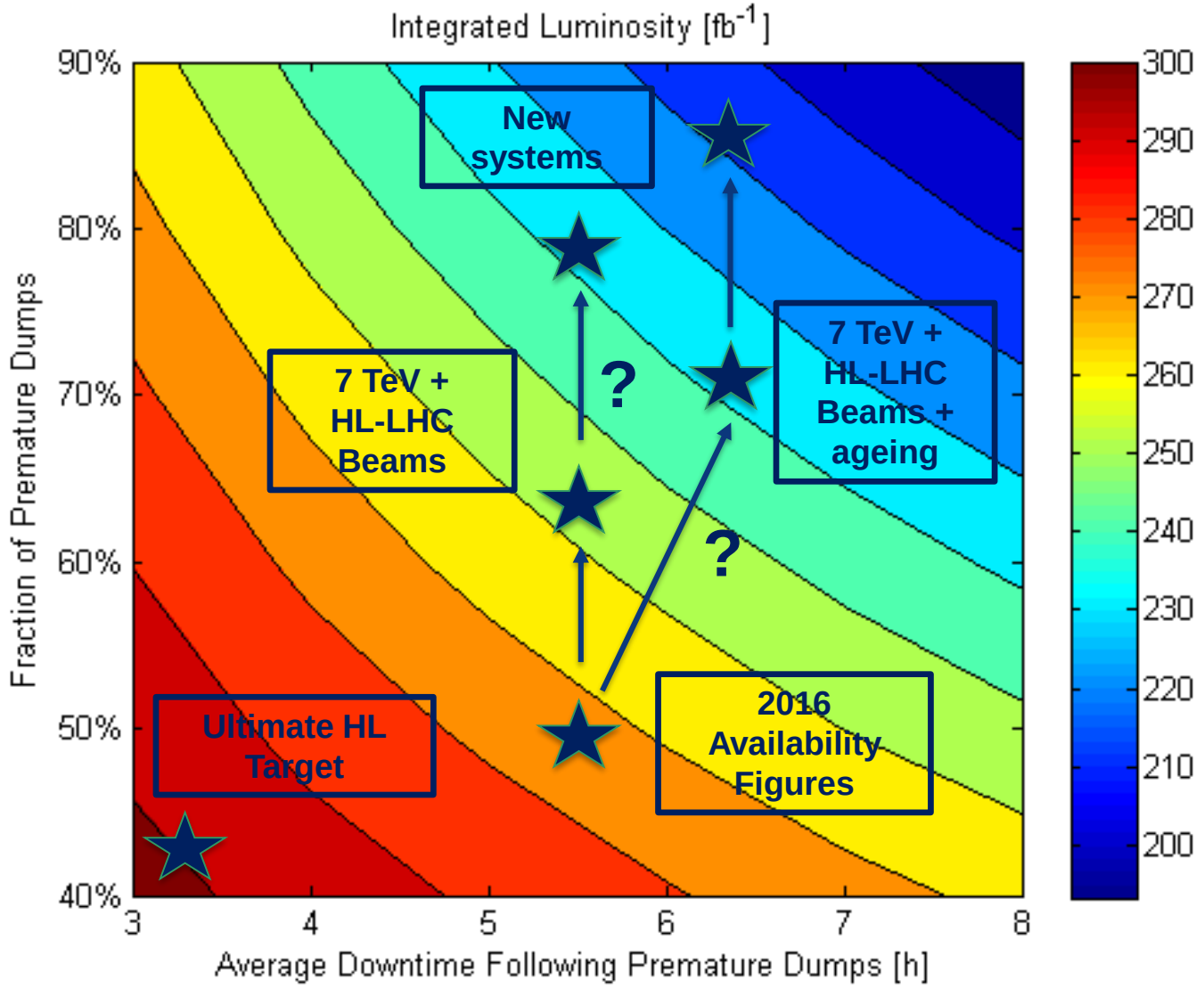


Randomness creates infinite number of paths on how the simulation run can be completed

Accelerator Exploitation

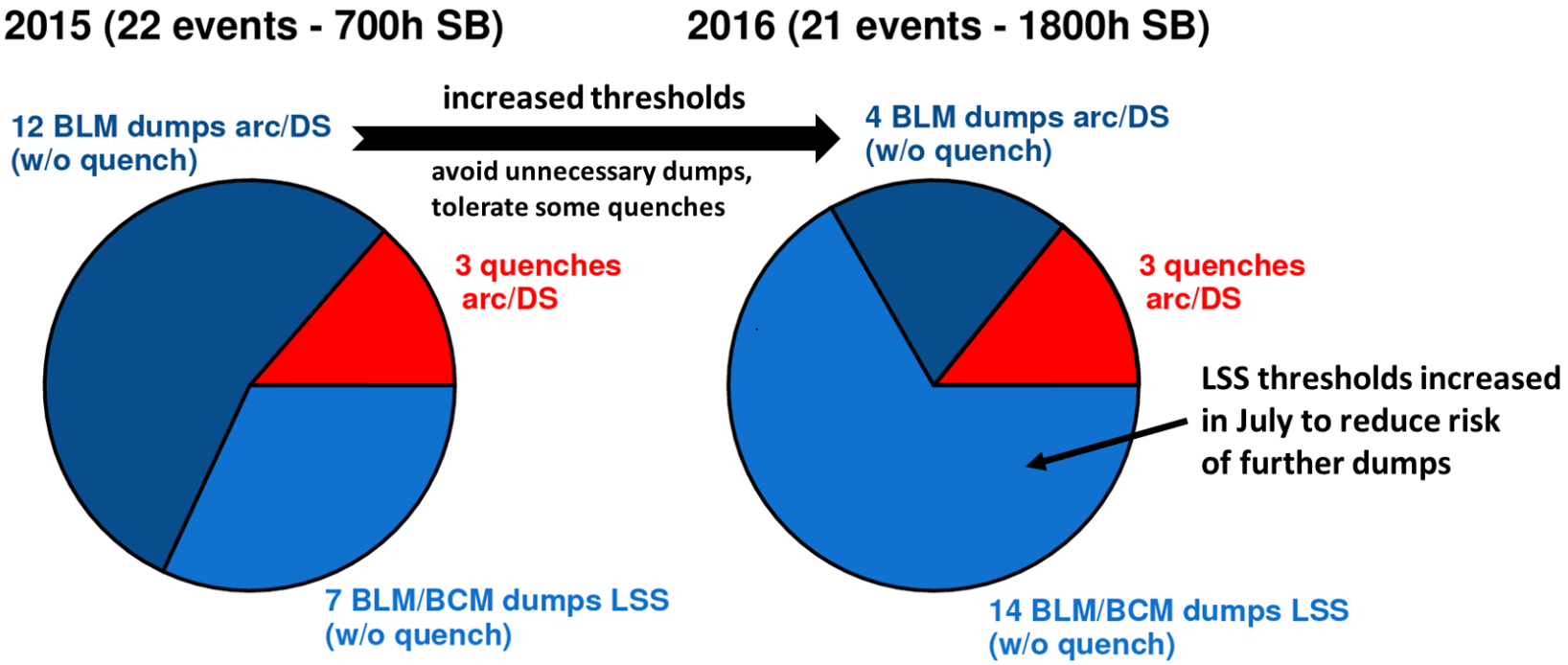


Sensitivity Analysis: HL-LHC



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)

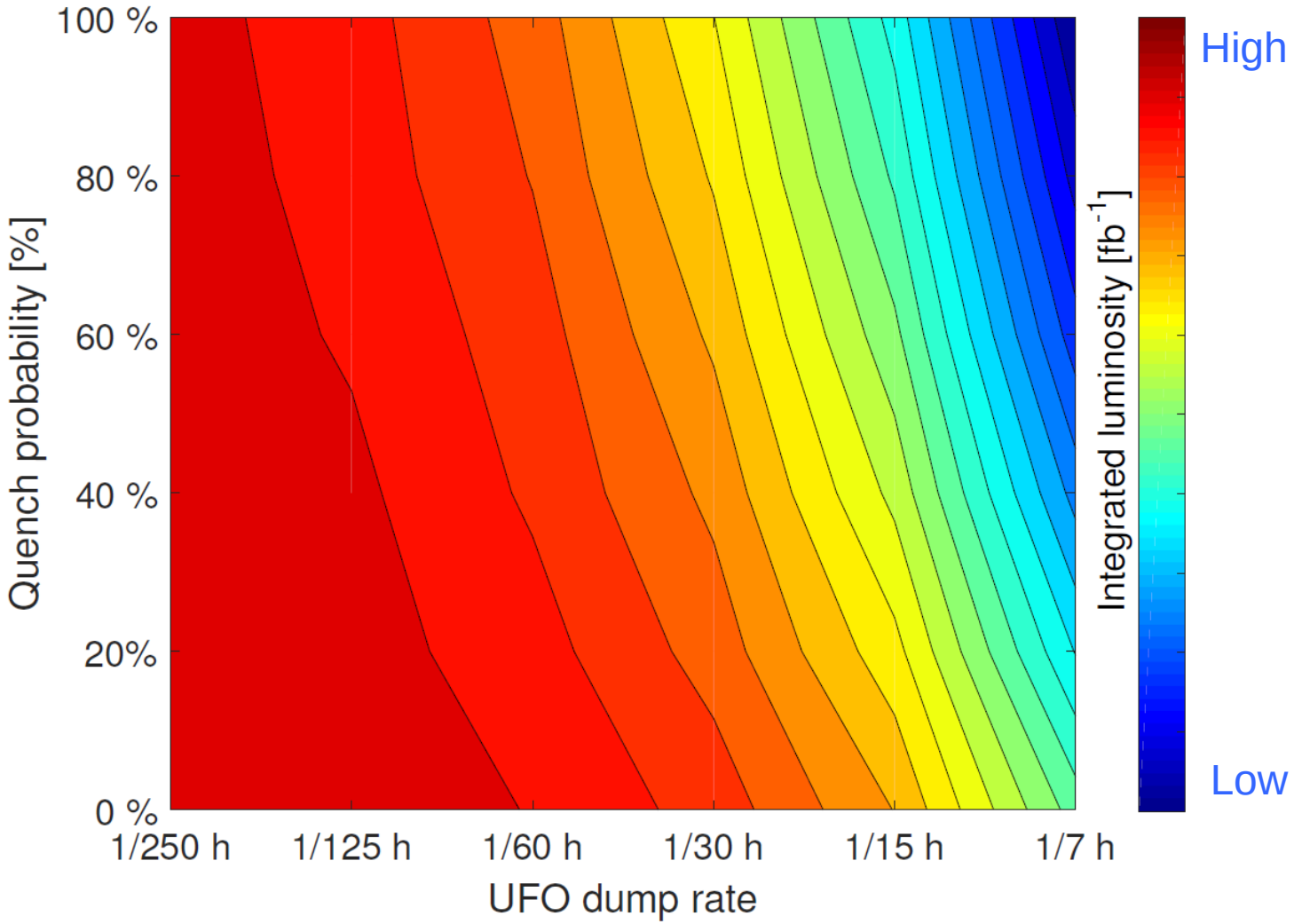
** Simple count of 2016 fills which would have been prematurely dumped if tenfold lower thresholds would have been applied in all sectors throughout the whole year. Multiple occurrences per fill are only counted once.

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)

Protection vs Availability

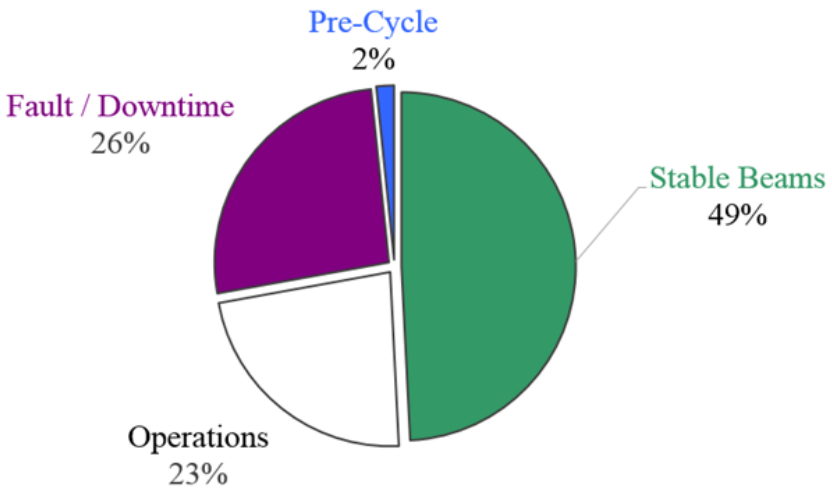


LHC Availability in 2016-2017

Proton run 2016

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

= 3738.7

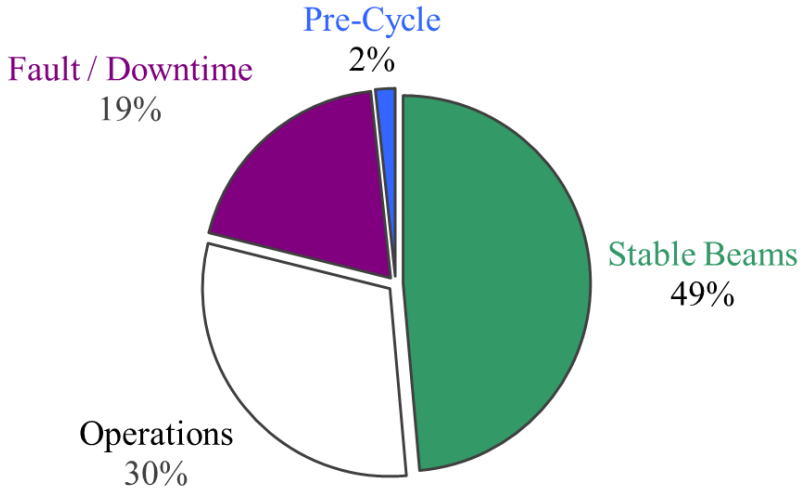


Dominated by few isolated, high impact faults

Proton run 2017

	Duration [h]
Stable Beams	1633.9
Fault / Downtime	652.9
Operations	1018.1
Pre-Cycle	57.2

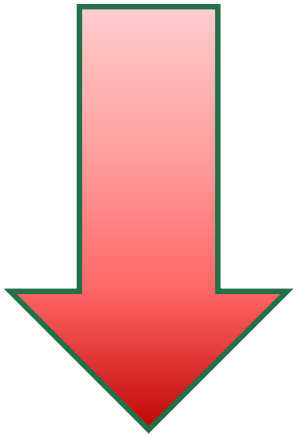
= 3362.1



Dominated by recurring faults with short duration (16L2)

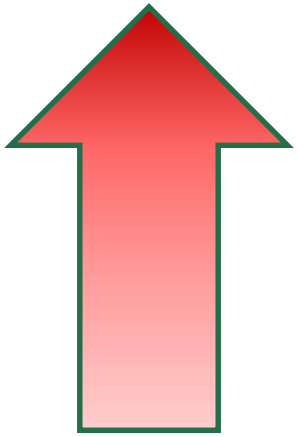
Reliability: Top-Down or Bottom-Up?

Definition of high level accidents / failure scenarios



Identification of causal factors leading to accidents

Consequences of component failure on system behaviour



Component Level

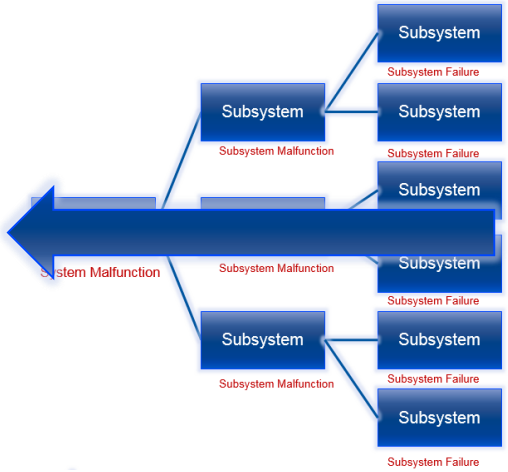
- **Example: System-Theoretic Process Analysis (STPA)**
- **Suitable for increasing complexity**
- **Extends further than 'component failures'**

- **Example: Failure Mode and Effects Analysis (FMEA)**
- **Maybe impractical for large projects**
- **Limited to 'component failures'**

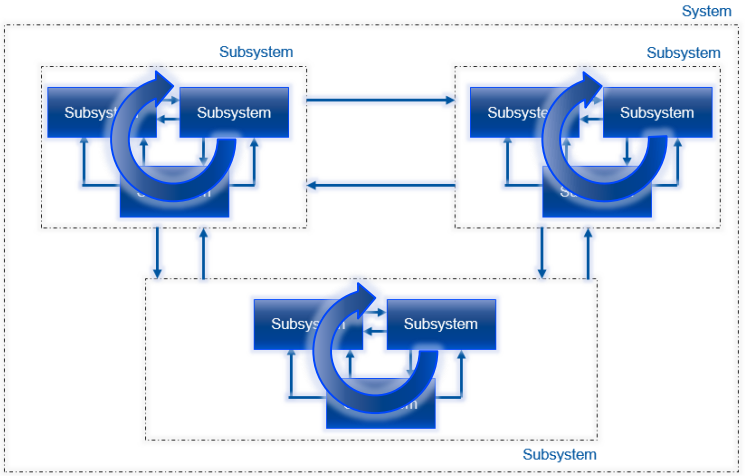
Comparison to Traditional Methods

D. Hugle, “System Theoretic Dependability Analysis of the LHC Superconducting Magnet Circuit Protection“, in preparation.

FMEA



STPA



System View

Strategy

Results

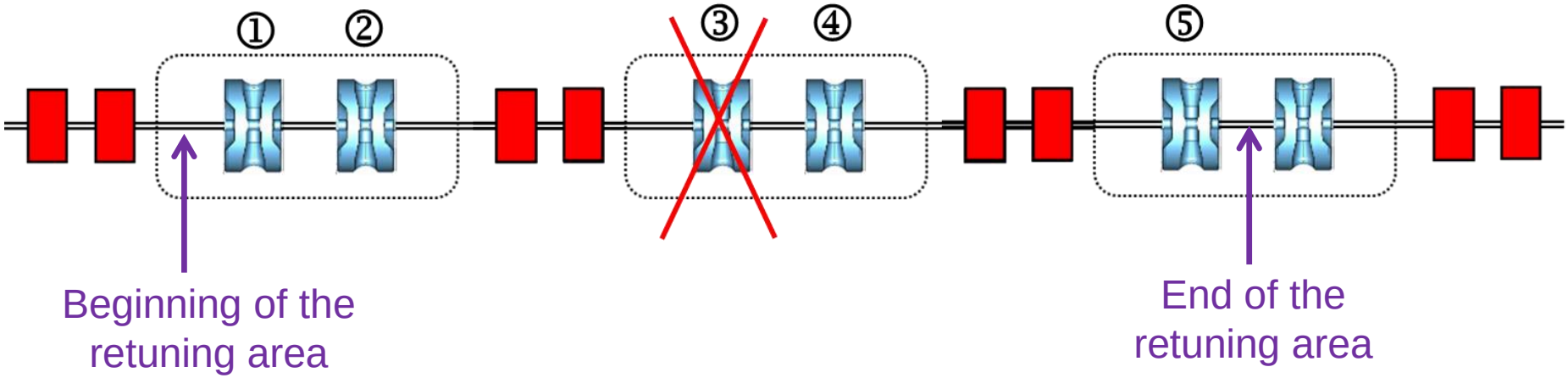
Focus: Component failures and effects
More rigid format
Spreadsheet results
Risk Priorization

Focus: System interaction
More flexible
No dedicated format
Includes IT & social factors
„Deal with every risk“

Accelerator-Driven Systems: The Exception

- 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

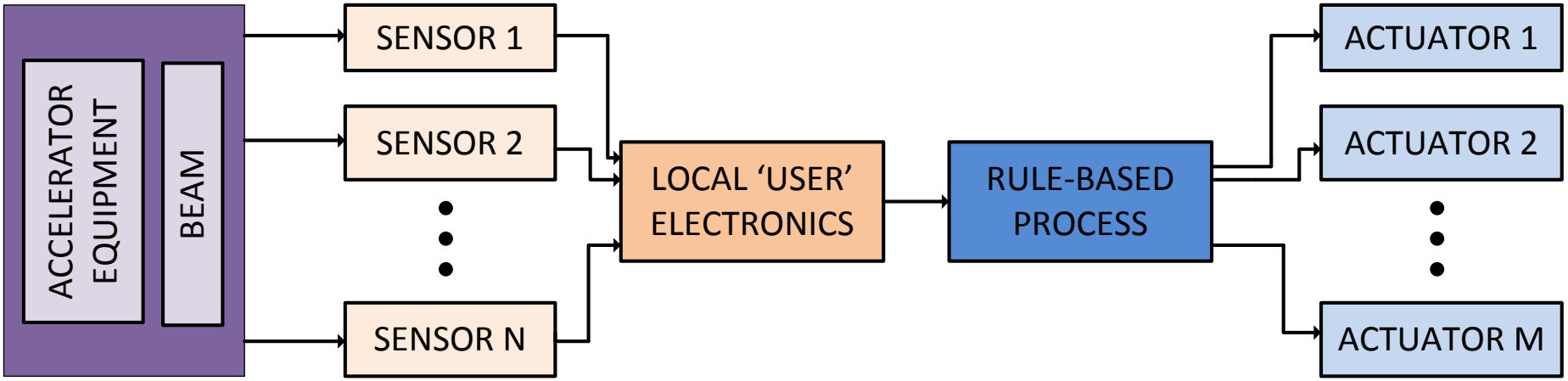


- **1st criterion**: recover the same transfer matrix of the retuned area than in nominal condition
- **2nd criterion**: the total Energy gain should remain the same than in the nominal case
- **3rd criterion**: the time of flight should remain the same than in the nominal case

To be done in less than 3 seconds for MYRRHA…

Courtesy F. Bouly, MYRTE WP2 Meeting, October 2016

Machine Protection: Interlocks



LHC: Several thousands → complex Several km → distributed

- Perform **controlled removal** of beams in case of failures:
  - Circular accelerators (e.g. LHC): Beam dump (100 µs – ms)
  - Linear accelerators (Linac4, ESS): Beam stop (1-10 µs)
- Improve availability by preventing consequences of severe failures
- Affect availability by triggering unnecessary ('false') beam aborts