10th Mini lecture:
Reliability and Availability

T. Cartier-Michaud

Acknowledgments: A. Apollonio, M. Blumenschein, L. Felsberg, B. Todd, J. Uythoven
Main source: A. Apollonio, ADS School 2016

Outline

- Definitions: Reliability and Availability
- Motivational !
- Risk Assessment
- Prediction of Reliability and Availability
- Case study: HL Inner Triplet

Outline

- **Definitions: Reliability and Availability**
- Motivational !
- Risk Assessment
- Prediction of Reliability and Availability
- Case study: HL Inner Triplet

Reliability and Availability

- **Reliability** (in [0-1]) is the probability that a system does not fail during a defined period of time (or number of cycles, amount of work) under given functional and environmental conditions.
  - 99% reliability of a magnet after X thermal cycles in the tunnel
  - 99% reliability of a source after X hours of production at Y mA
  - 99% reliability of a target after X MJ absorbed below Y MW

- **Availability** (in [0-1]) is the probability that a system is functioning according to its specification at any point in time.
  - 70% availability of LHC
  - 99% availability of LINAC2

Reliability and Availability

- **Reliability:** idea of time integration, with:
  - f(t), the time dependent failure density (exponential, Weibull, …)
    == distribution of how long should we wait before a failure occurs
  - F(t), the cumulative distribution function
    == probability that the system is still running after a given time
  - Lambda(t), the failure rate or hazard function
    == ratio between item which have failed and total number of units

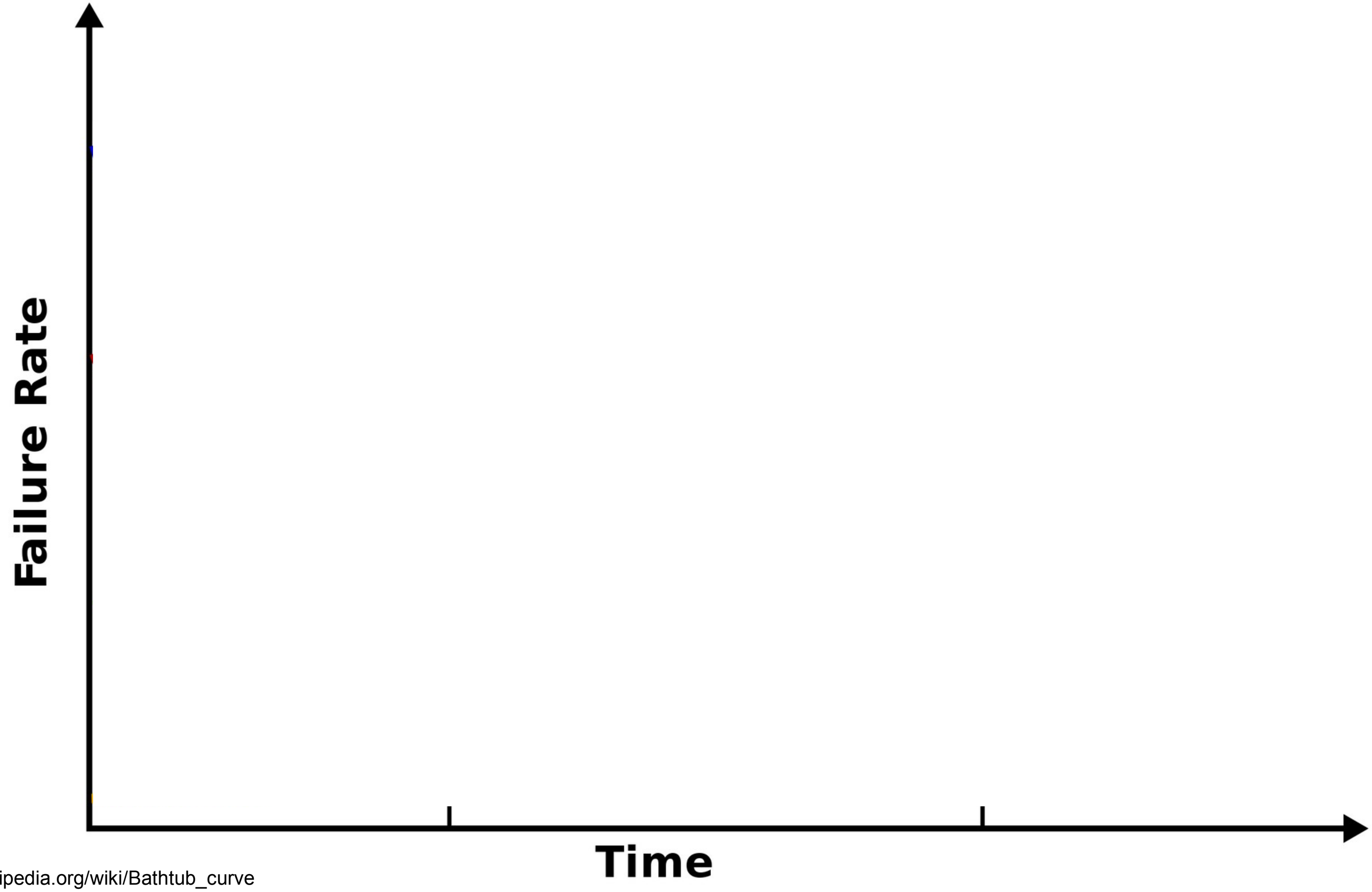
$$f(t) = \lambda exp(-\lambda t)$$

$$F(t) = \int_0^t f(s)ds = 1 - exp(-\lambda t)$$

$$\Lambda(t) = \lambda$$

➡ The failure rate of an exponential distribution does not depend on the time = no memory = no aging

Reliability and Availability



https://en.wikipedia.org/wiki/Bathtub_curve

Reliability and Availability

- **Availability:** idea of operation, with:
  - t: a duration of observation,
  - t_UP: the time the system spent functioning and
  - t – t_UP = t_DOWN: the time the system spent not functioning
  - then Availability = t_UP / t
- for an exponential distribution with a failure rate λ

  => mean time to fail = MTTF = $1/\lambda$

  => mean time to repair = MTTR
  (mean time before failures = MTBF = MTTF + MTTR)

  => availability = MTTF / (MTTR + MTTF)

Reliability in the **Machine Protection** context, and Availability

- **Reliability:** computed with respect to major events / features:
  - Being able to protect a magnet during a quench
  - Being able to dump the beam

  => if systems are not protected, up to months of repairs / high cost

- **Availability:** computed with respect to every event
  - Glitch of power converter
  - Cryo failure

  => repair can be almost instantaneous to a few hours

  => the failures considered for the reliability are also taken into account but their probability of occurrence is so low that their impact is low

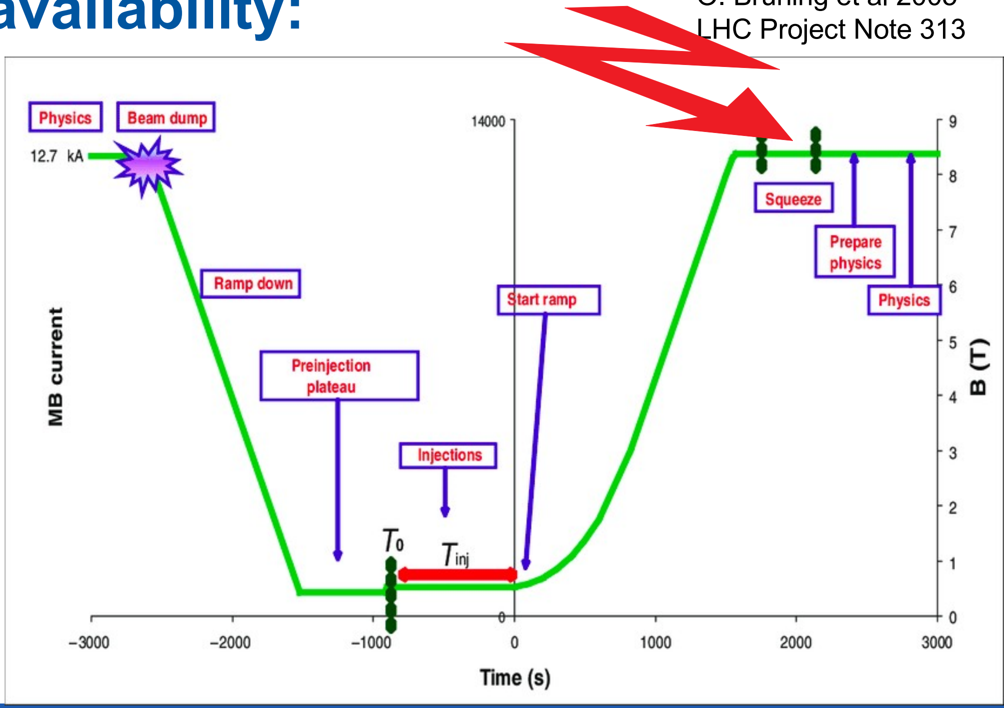
- High reliability and high availability might sometimes conflict:

  => unnecessary beam dump

Reliability and Availability of LHC

- **LHC = circular accelerator + last accelerator of a chain**
- **True reliability of LHC = Product of the reliability of the chain:** if LINAC4 is down, LHC cannot be fed
- **Production of physics != availability:** LHC operation is based on phases in a specific order.
- Systematic failures of 1s during squeeze phase = ~100% availability but no time spent in stable beam!

O. Brüning et al 2005
LHC Project Note 313



Outline

- Definitions: Reliability and Availability
- **Motivational !**
- Risk Assessment
- Prediction of Reliability and Availability
- Case study: HL Inner Triplet

Risk Assessment: risk examples

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 (@ 7 TeV)

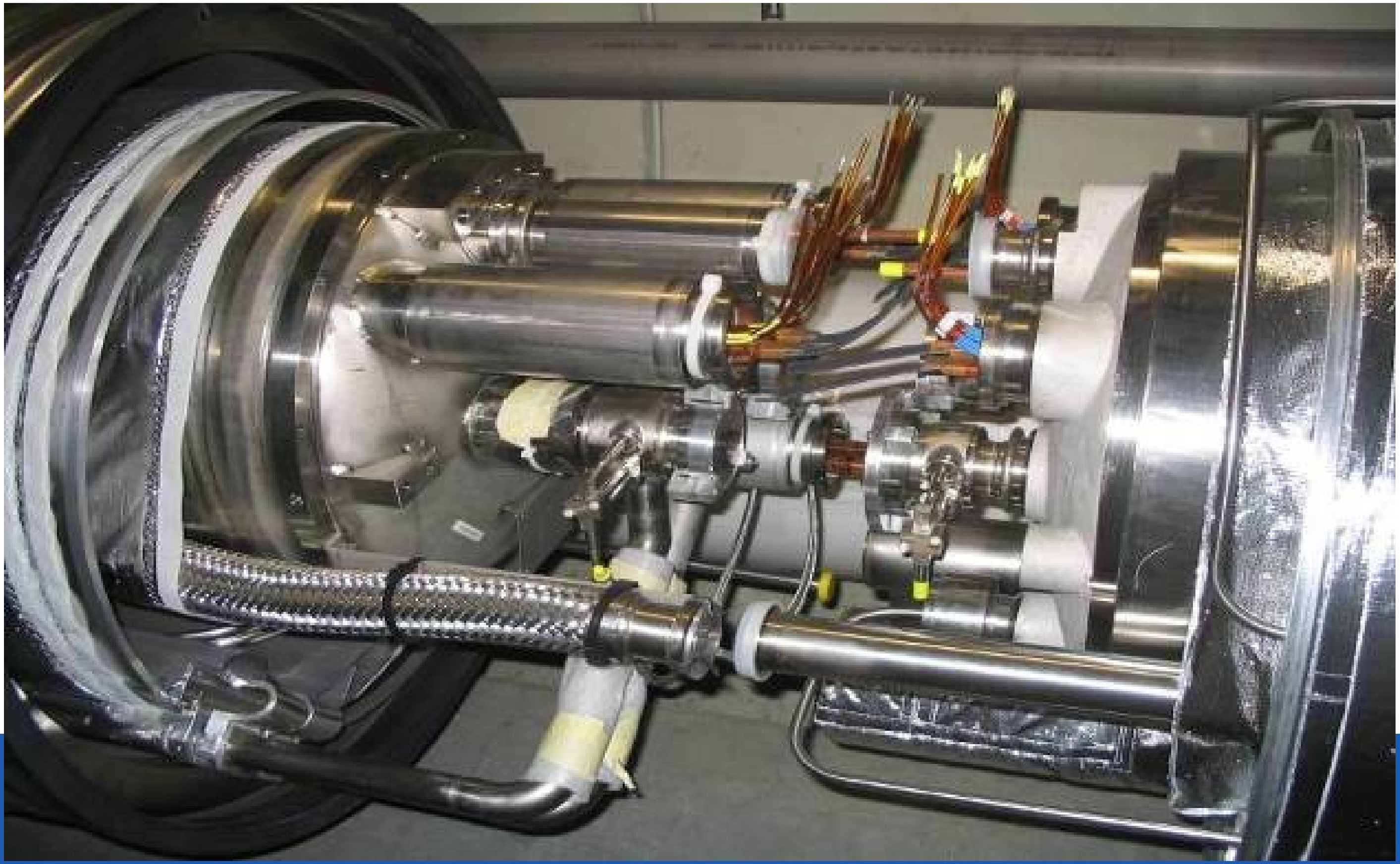
Kinetic Energy of 200 m Train at 155 km/h ≈ 360 MJ

Stored energy per beam is 360 MJ

Risk Assessment: risk examples

10 000 high current superconducting **cable joints**

~ 600 MJ stored in each magnet

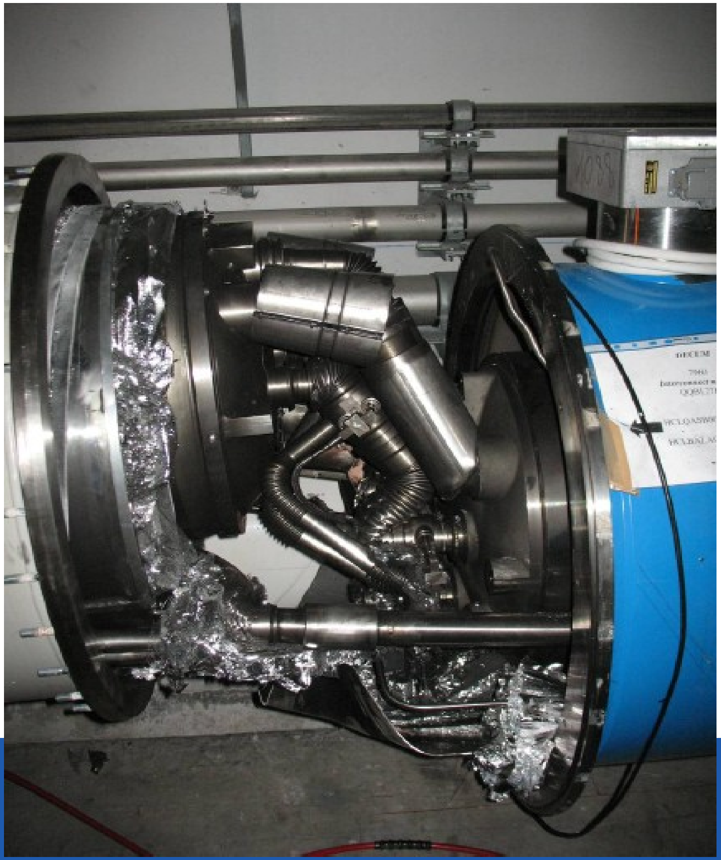


Risk Assessment: risk examples

1 / 10 000 joints failed in 2008

~ 420 MJ dissipated in the tunnel

(electric arc + vaporizing material + moving magnets)



Reliability and Availability in the life cycle

<table>
<tr><td>Concept phase</td><td>Design, prototype, contract</td><td>plan, purchase</td><td>Implement, build</td><td>Install and use</td></tr>
<tr><td colspan="2">Development</td><td colspan="2">Production</td><td>Field</td></tr>
</table>

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

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

Outline

- Definitions: Reliability and Availability
- Motivational !
- **Risk Assessment**
- Prediction of Reliability and Availability
- Case study: HL Inner Triplet

Risk Assessment

- 1) Identification of the failure modes

  ==> Failure Mode Analysis and Effects

  IEC 60812, Analysis techniques for system reliability -
  Procedure for failure mode and effects analysis (FMEA),edition 2.0, 2006

- 2) Allocation of a consequence and/or tolerance

  ==> Risk Matrix

  ISO/TR 14121-2:2012, Safety of machinery -
  Risk assessment - Part 2: Practical guidance and examples of methods, 2013

- 1+2=3) Reliability Requirements and Initial Risk Evaluation

  ==> RIRE, M. Blumenschein and al.:
  https://cds.cern.ch/record/2666957/files/73.an%20approach%20to%20reliability%20assessment%20at%20CERN_20181011.pdf

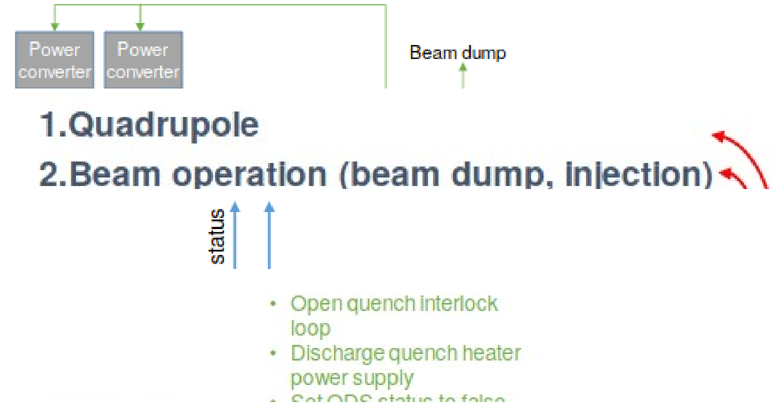
FMEA: study of the system

(Illustrations from the quench detection system of LHC, M. Blumenschein)

Failure Modes and Effects Analysis is a quite flexible tool adapted / customized to different contexts

1) Block diagram of the system environment: neighboring systems, interfaces, common cause failure, …
2) Structure of the system itself
3) Function of each sub part of the system
4) Context dependent function / Easter eggs
5) Failure Modes and End Effects

==> lots of discussion with experts
==> lots of "naive" questions asked



1)
2)
3)
4)
5)

Table 1: Excerpt of the FMEA table

FMEA black box level: quench detection system			
Context	Normal operation of QPS (~4800 h/a)	Asymmetric quench (~0.5 s)	Post quench 1 (~5-10 min)
Function	Keep quench interlock loop closed	Open quench interlock loop	Keep quench interlock loop opened
ID failure mode	OP.1	AQ.1	PQ1.1
Failure mode	Quench interlock loop opened 1oo2 or 2oo2	Quench interlock loop not opened 1oo2	QIL is closed locally 1oo2 or 2oo2
Immediate effect	False energy extraction, no firing of the quench heaters, false circuit quench interlock	Energy is extracted, both quench heater series are fired, circuit quench interlock is sent	No effect in this state, if undetected, higher probability of missing interlock in case of quench
End effect	False beam dump	Injection delayed (3 h)	Injection delayed (3 h)
Severity of EE	2	2	2
Detection Method	Quench interlock loop monitoring indicates loop status	Detector post mortem, (no final detection if only loop relay is broken	Post mortem (loop falgs, loop open or closed)
Notes	after upgrade additional loop voltage monitors (eases fault localization)	Quench interlock loop is opened by second, redundant quench detector	
Recommendations		put secondary relay contact in detector	

Risk Matrix: allocation of tolerance

- Risk = consequence * probability
- Acceptable risk are defined by experts with respect to availability targets and reliability targets

LHC risk matrix		Recovery						
		∞	year	month	week	day	hours	minutes
		S7	S6	S5	S4	S3	S2	S1
Frequency	1 / hour							
	1 / day							
	1 / week							
	1 / month							
	1 / year							
	1 / 10 years							
	1 / 100 years			**EE2**				
	1 / 1000 years							

Protection

Availability

Data driven Risk Matrix

- The overall availability – reliability are defined
- The distribution of allowed / not allowed couples of (recovery time, frequency) could follow different distribution
- Definition of data driven risk matrices (using AFT inputs)

Recovery time

Failure frequency

	[1m - 20m)	[20m - 1h)	[1h - 3h)	[3h - 6h)	[6h - 12h)	[12h - 24h)	[24h - 2d)	[2d - 1w)	[1w - 1M)	[1M - 1Y)	[1Y - 10Y)
1/H	U	U	U	U	U	U	U	U	U	U	U
1/Shift	~	U	U	U	U	U	U	U	U	U	U
1/Day	A	~	~	~	U	U	U	U	U	U	U
1/Week	A	A	A	A	~	~	U	U	U	U	U
1/Month	A	A	A	A	A	A	~	U	U	U	U
1/Year	A	A	A	A	A	A	A	A	U	U	U
1/10Years	A	A	A	A	A	A	A	A	A	U	U
1/100Years	A	A	A	A	A	A	A	A	A	A	U
1/1000Years	A	A	A	A	A	A	A	A	A	A	A

Outline

- Definitions: Reliability and Availability
- Motivational !
- Risk Assessment ==> schematics + targets
- **Prediction of Reliability and Availability**
  Failure rate figures + computational methods
- Case study: HL Inner Triplet

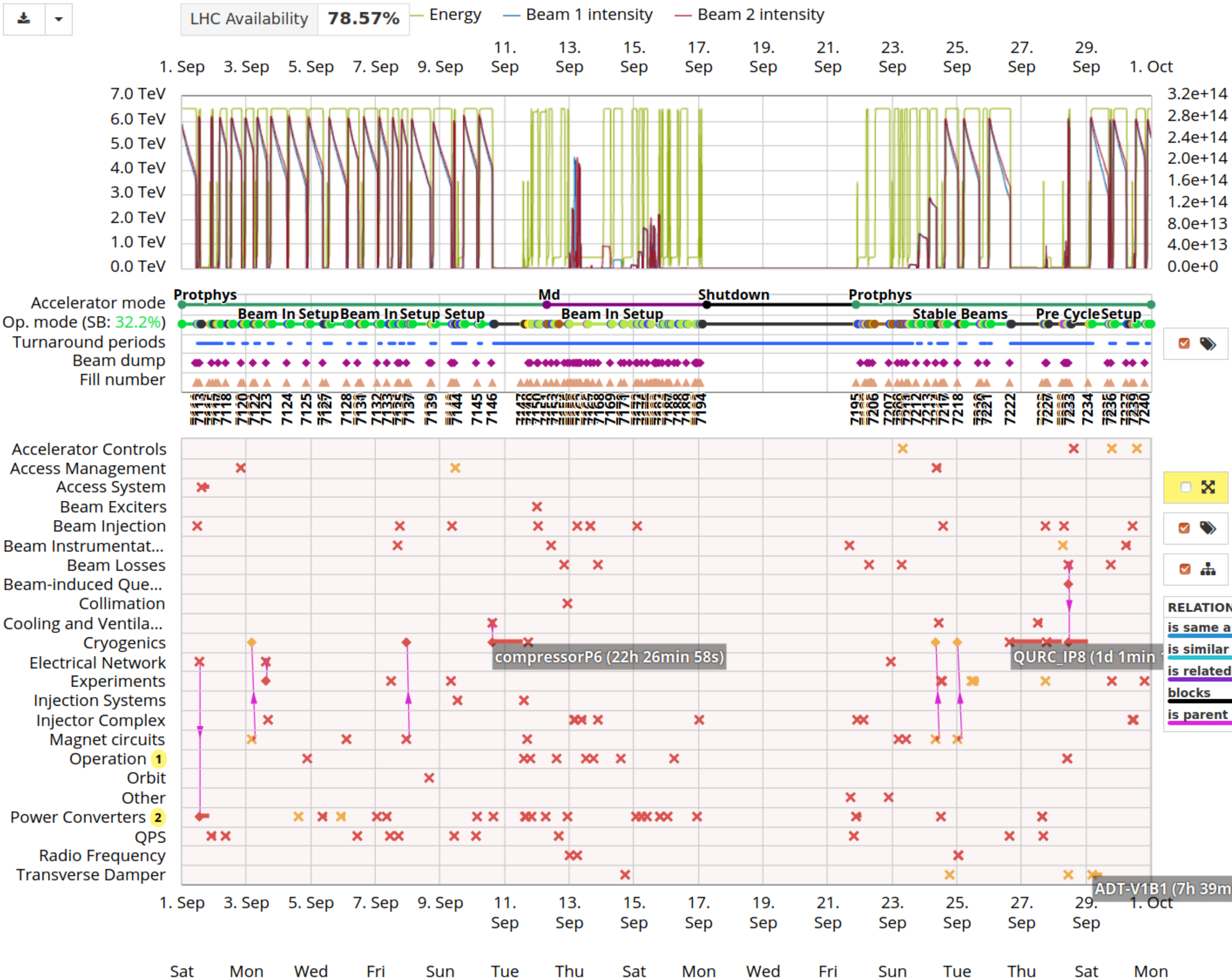
Failure rate estimation

1) Failure rates measure on comparable devices
   - Test campaign (accelerated lifetime, ...)
   - AFT, PM, nxcals, LASER, … => logging is important !
2) Experts' estimate
   - Large uncertainties
3) According to manufacturer / Military Handbook
   - Very pessimistic approach

The lower the reliability of the input, the more important the sensitivity analysis over that parameter

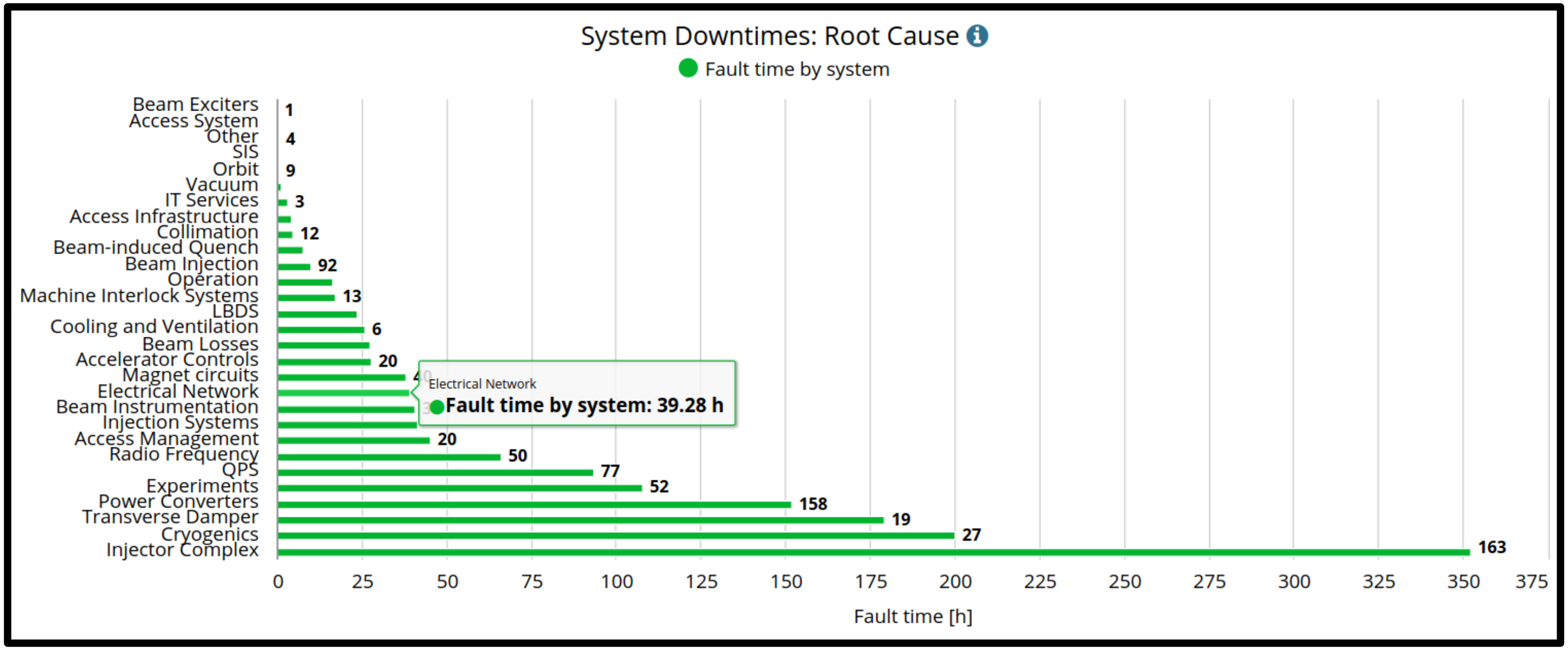
Accelerator Fault Tracking

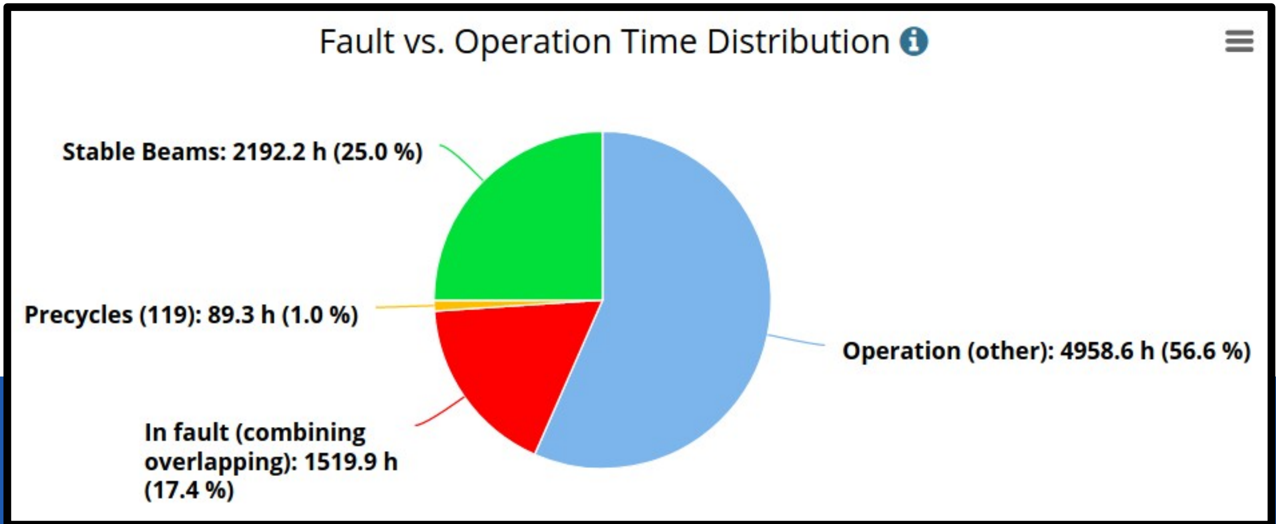
https://aft.cern.ch/



Accelerator Fault Tracking

https://aft.cern.ch/

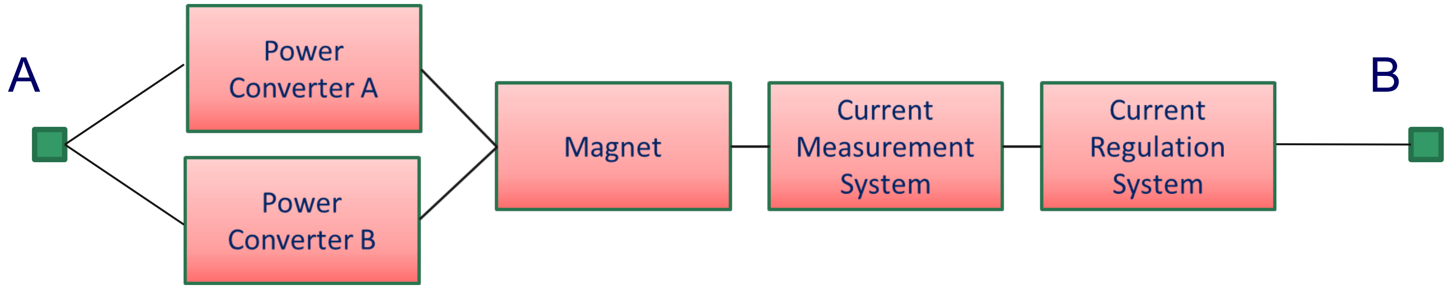




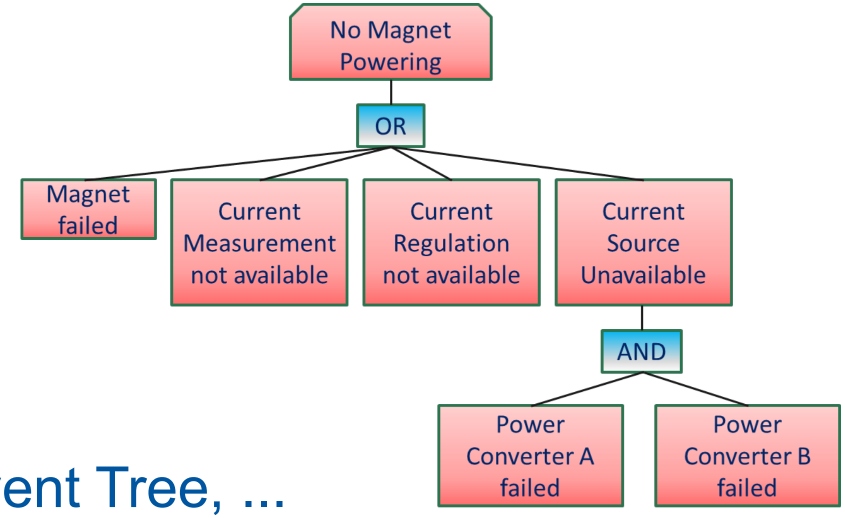
CERN

Model and computational methods

- Reliability Block Diagram: what is the minimum set of components that allows fulfilling the system functionality?



- Fault Tree:
  what are the combinations of failures that lead to a system failure?



- Functional Block Diagram, Event Tree, ...

Model and computational methods

- Functional Block Diagram, Reliability Block Diagram, Fault Tree, Event Tree, ...

- Computations:
  - “Analytical”: possible when the structure/logic is simple
  - “Numerical”: possible even for complex structure/logic but higher computational cost (simulation budget for Inner Triplet study ~= 30 000 core.hours with AvailSim4)

- AvailSim4 (developed at CERN):
  - Discrete Event Simulation: first principle +complex logic ready
  - Monte Carlo ~= random exploration of possible scenarios

Use of the Predictions

- Do we meet the reliability / Availability target?

- If no, trying to refine the reliability / availability study :-D
  What are the sensitive elements?
  - are the inputs on the failure rates accurate enough?
  - could a test campaign better estimate some failure rates and relax/dismiss a weak point?

- What is the more cost efficient way to improve the system ?
  - more monitoring
  - more periodic inspection / predictive maintenance
  - more reliable (/expensive) components (if any)
  - more (/diverse) redundancy

Predictive maintenance

- Predicting a failure before it happens = increasing availability and reliability by early repair

- Explainable Deep Learning for Fault Prognostics in Complex Systems: A Particle Accelerator Use-Case
  https://doi.org/10.1007/978-3-030-57321-8_8

  ~= Training a Neural Network on the LASER database to predict faults / detect non trivial dependencies between systems

- Prediction of break down in an RF cavity to better protect the machine and increase availability
  (WIP) CLIC team talk: https://indico.cern.ch/event/957293/

Case study: HL Inner Triplet

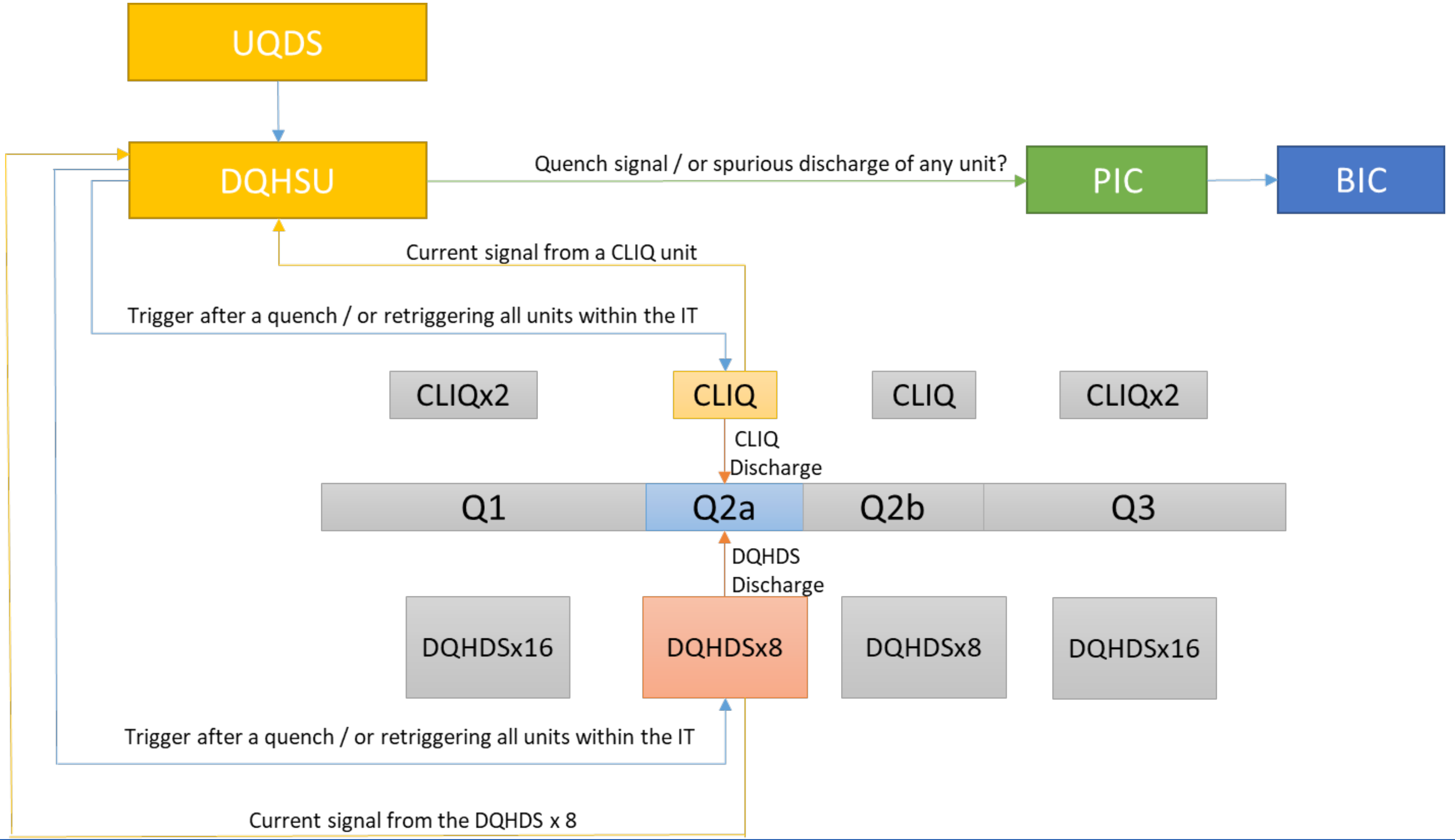
- Magnets for final focusing before collision points
  HL requires an update with a new technology

- FMEA:
  1) unprotected quench is the worst failure for the system
  2) too slow protection of a quench is the worst failure for the close by experiment
  3) electrical arcs in the power rack is the worst failure for personal safety (not machine protection)

- Risk matrix: case 1 has an acceptable probability of occurrence of 2.1% in 20 years

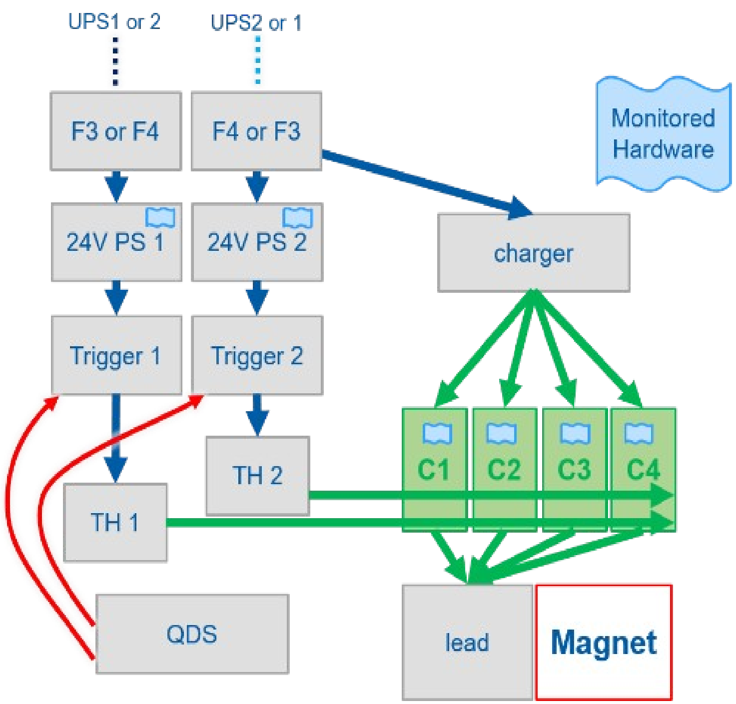
Case study: HL Inner Triplet

- (some) Functional Block Diagrams

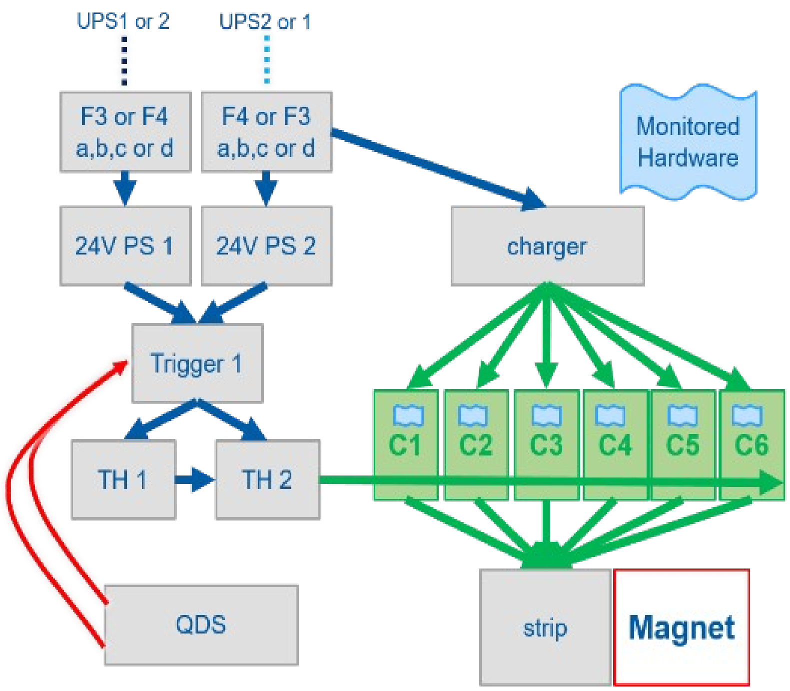


Case study: HL Inner Triplet

- (some) Functional Block Diagrams



CLIQ power unit



QH power unit

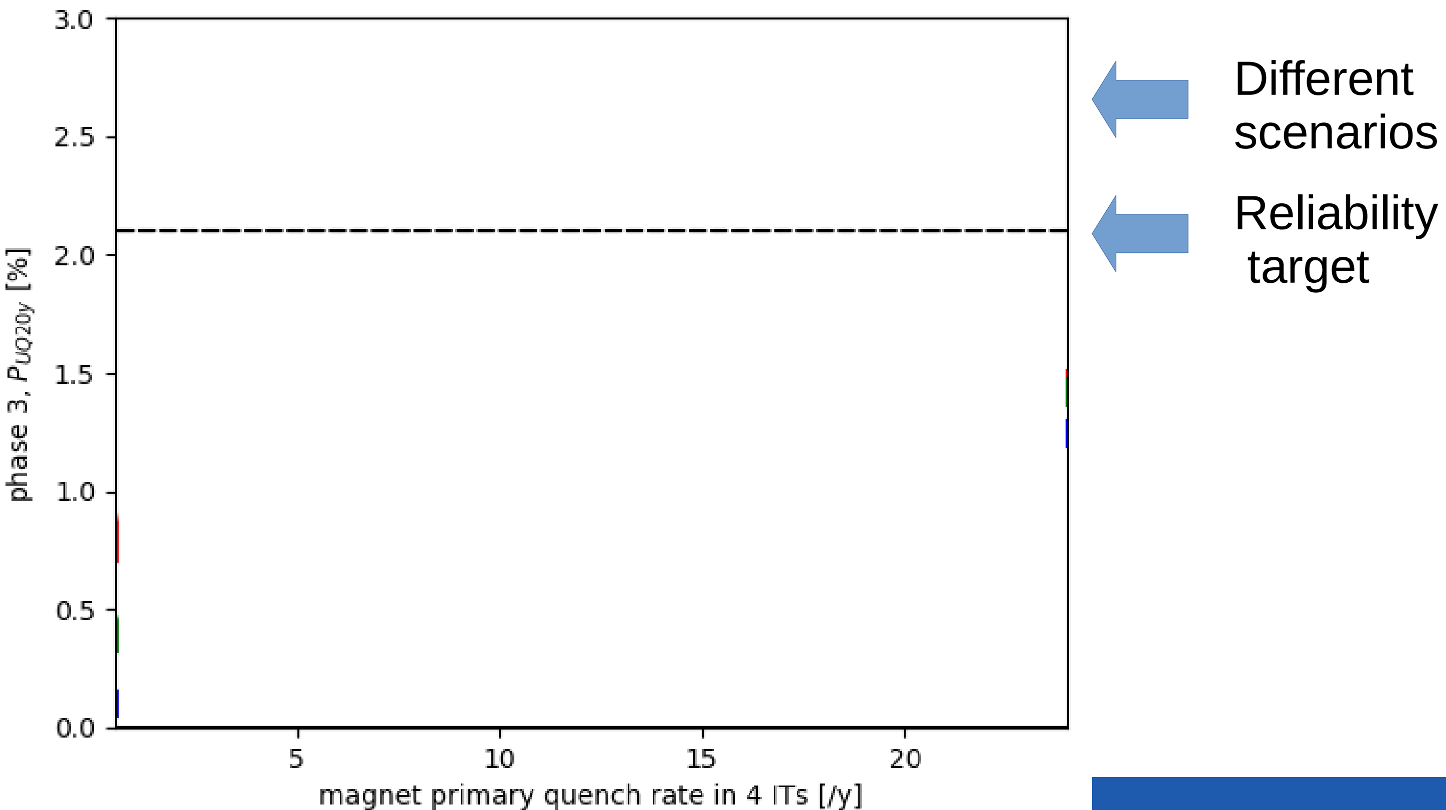
Case study: HL Inner Triplet

- Failure rates inputs

	PS24V	trigger	TH	charger	capacitor	strip	c. breaker
# of element	6 000	6 000	12 000	6 000	36 000	5 000	6 000
Number of faults	2	0 **-> 1**	0 **-> 1**	0 **-> 1**	0 **-> 1**	10	6
Operation time [y]	7 (+2 of LS)	7 (+2 of LS)	7 (+2 of LS)	7 (+2 of LS)	7 (+2 of LS)	7 (+2 of LS)	7 (+2 of LS)
measured MTTF [y]	21 000	42 000	84 000	42 000	252 000	3 500	7 000
MTTR [h]	5	5	5	5	5	change magnet	5
Type of faults	blind	blind	blind	blind	monitored	blind	blind
# in IT	384	384	384	192	1152	192	192

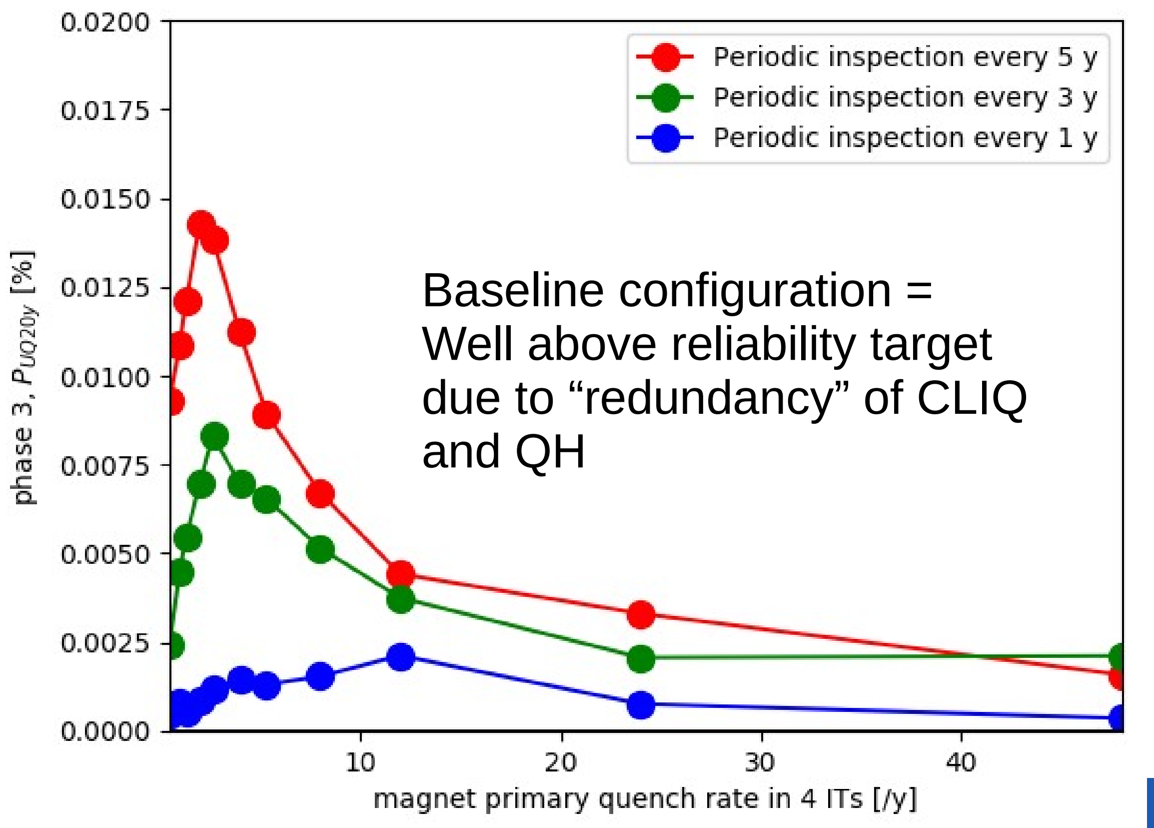
Case study: HL Inner Triplet

- Probability of not protecting a magnet in 20 years using CLIC only (no QH):



Case study: HL Inner Triplet

- Probability of not protecting a magnet in 20 years using CLIQ and QH



Conclusion

- Wide rage of methods and tools to **estimate** and **adjust** reliability and availability of systems
- **Predictions are as good as the hypothesis**
  Estimation of failure rate of components is difficult, especially on very rare failure events ==> sensitivity analysis
- … but **reliability and availability studies are more and more important** as systems become more and more complex / have more severe failures
- **Unknown unknowns** are most likely what will be the problem in the end. To compensate, one of the main drivers when designing a system is experience gained on similar/previous designs

Thank you for your attention