Reliability Engineering and Availability of a Large Collider Complex

CAS on Beam Dynamics and Technologies for Future Colliders

www.cern.ch

M. Zerlauth, A.Apollonio, R. Giacchino, B.Todd, R. Schmidt, J. Wenninger, L. Ponce, J. Uythoven, A. Nordt, and many more…

Outline

Last slide

- Occasionally I go into the LHC tunnel
- and ask myself how do we manage to get this to work…?
- You tell me!

To the entire LHC team

Congratulations and all our thanks for this splendid achievement !

6

M.Lamont

Outline

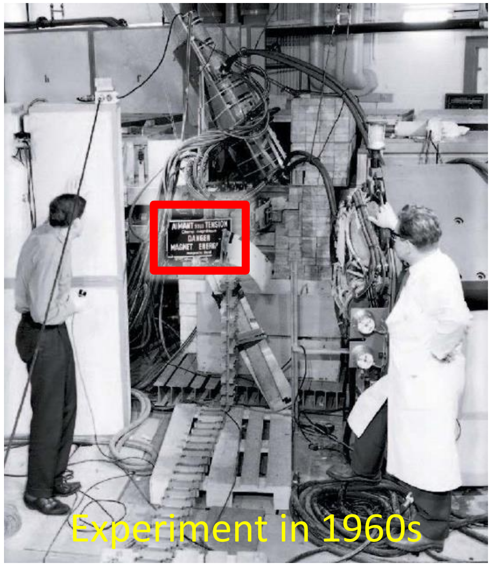
- Why is dependability increasingly important for accelerators?
- Dependability Engineering in a nutshell
  - Dependability definitions, RAMS
- How to design reliable systems and operate them as such?
  - Understanding and mitigating the risks
  - Failure frequency
  - Failure impact – damage and downtime
  - Maintenance and operability
- Conclusions

Outline

- Why is dependability increasingly important for accelerators?
- Dependability Engineering in a nutshell
  - Dependability definitions, RAMS
- How to design reliable systems and operate them as such?
  - Understanding and mitigating the risks
  - Failure frequency
  - Failure impact – damage and downtime
  - Maintenance and operability
- Conclusions

Dependability for todays accelerator's

- Today's (and tomorrows) accelerator projects are unprecedented in terms of size, complexity, damage potential and process requirements



- Modern equipment mostly has to be remotely controlled, are exposed to harsh environments, are not accessible for years and are assemblies of complex and highly sensitive systems

What is dependability?

- In systems engineering, **dependability** is a measure of a system's **availability**, **reliability**, and its **maintainability**, and **maintenance support performance**, and, in some cases, other characteristics such as **durability**, **safety** and **security**.

- In software engineering, **dependability** is the ability to provide services that can defensibly be trusted within a time-period. This may also encompass mechanisms designed to increase and maintain the dependability of a system or software.

Wikipedia

What is dependability?

Reliability

Availability

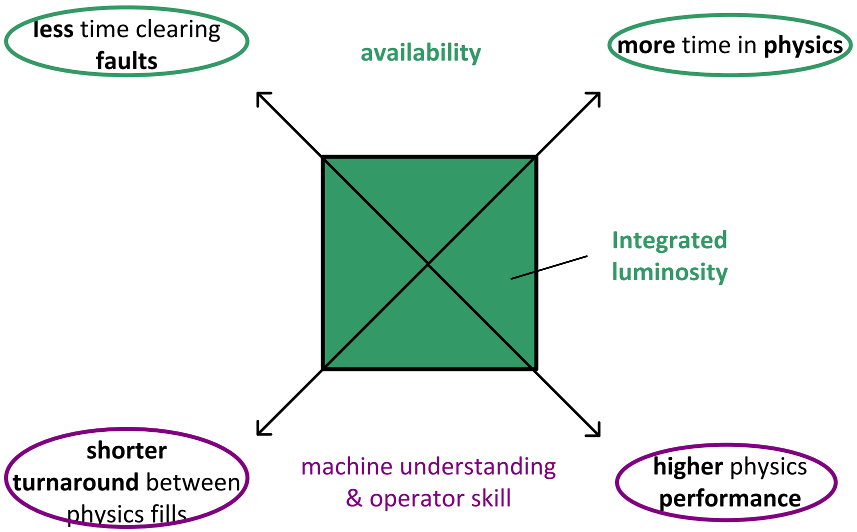
Maintainability

Productivity

Operability / Safety

Optimisation of all aspects required to achieve optimimum output
The parameters are partially dependent on each other!

What defines the productivity / physics output?



Physics output is a function of…

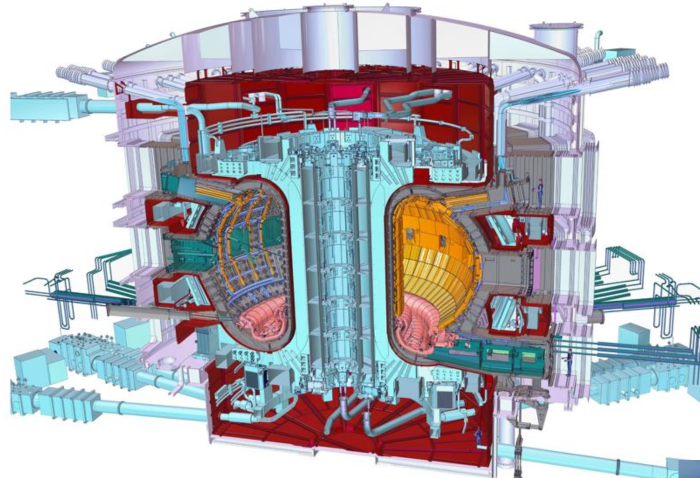
machine understanding & operator skill

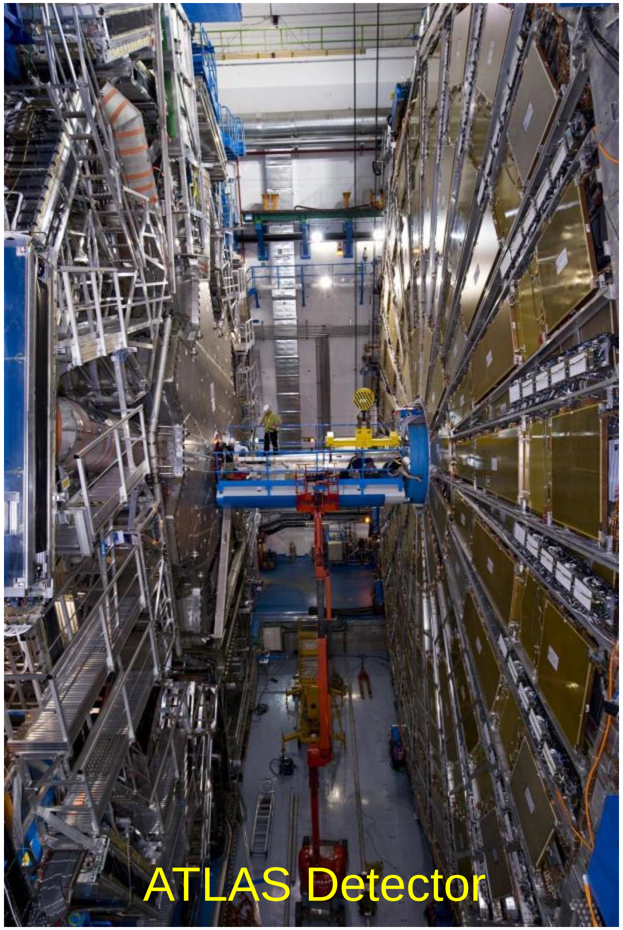
1. time producing physics beams
2. turnaround between successive experiments
3. time to clear faults
4. physics performance during experiments

Availability
Maintainability
Scheduling

Reliability challenges

ITER Tokamak





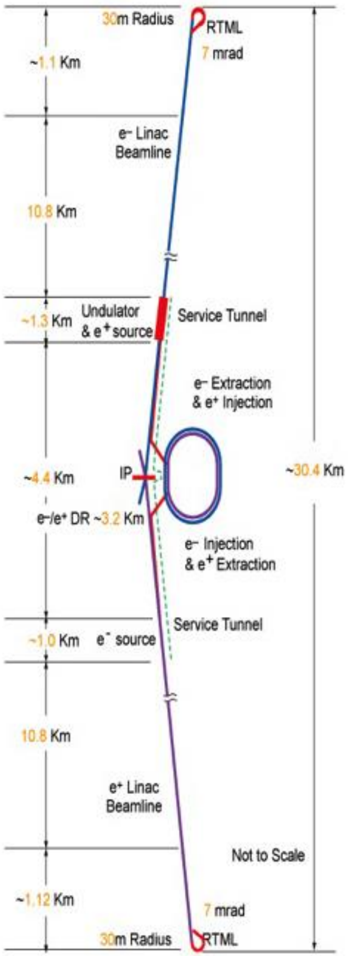
ATLAS Detector

Opportunity has been active for 55 times its designed lifespan.

Space shuttle Discovery

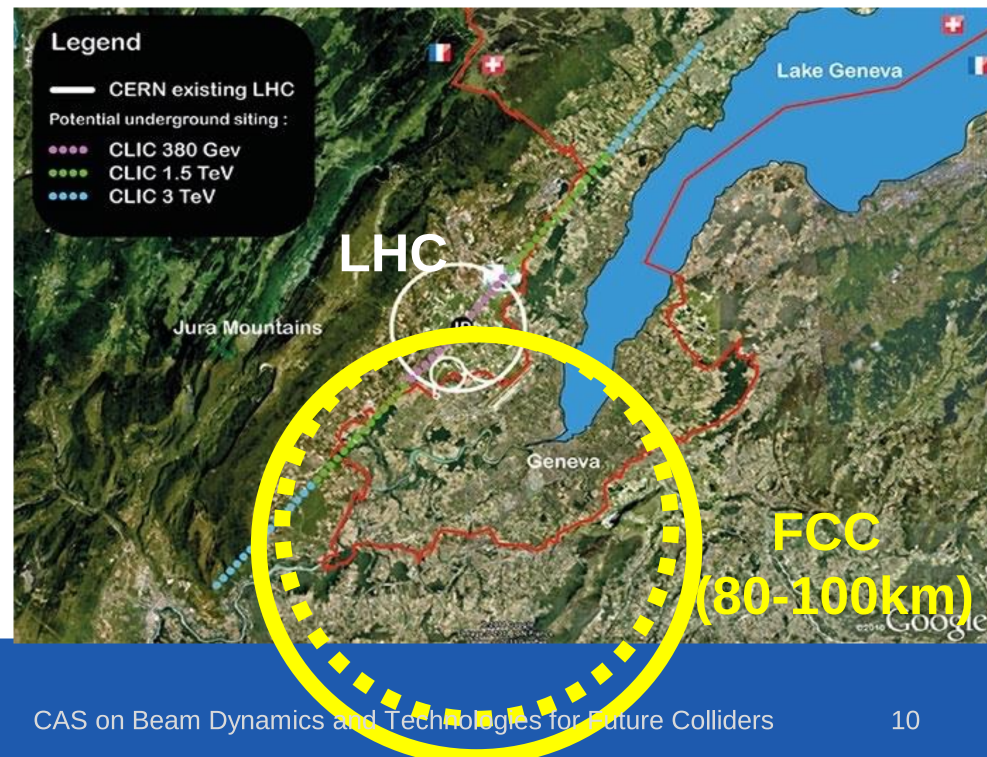
No accessibility for maintenance, radiation/EMC environments, limited possibilities or very costly redundancy…

Maintainability challenges

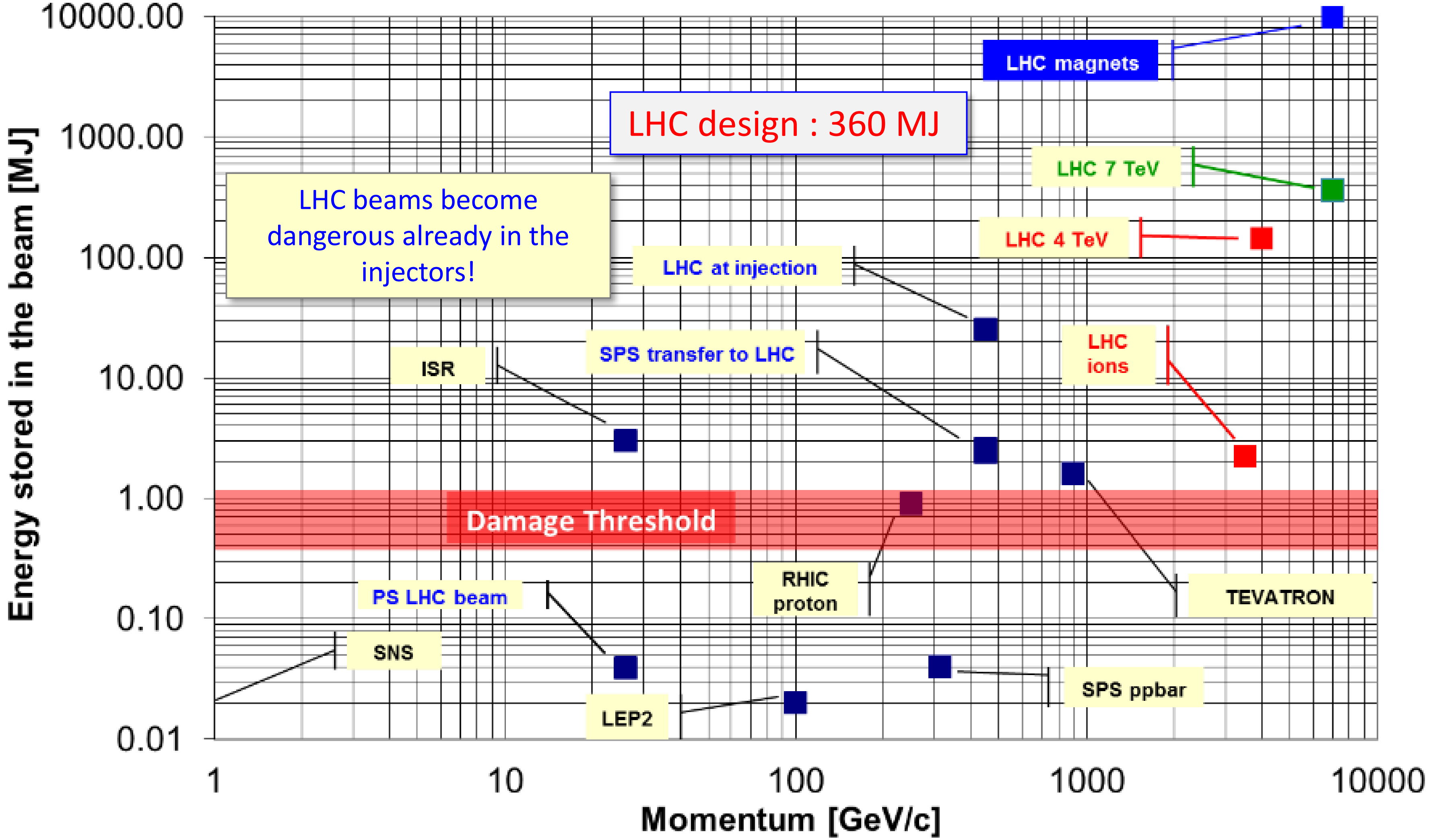


Interational Linear Collider

Geographical extent of machines, complexity and environmental conditions impact fault duration …

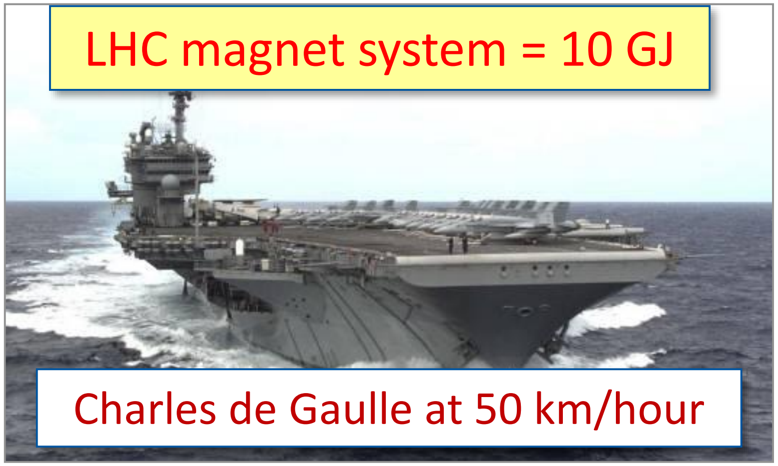


Protection (operability) challenges



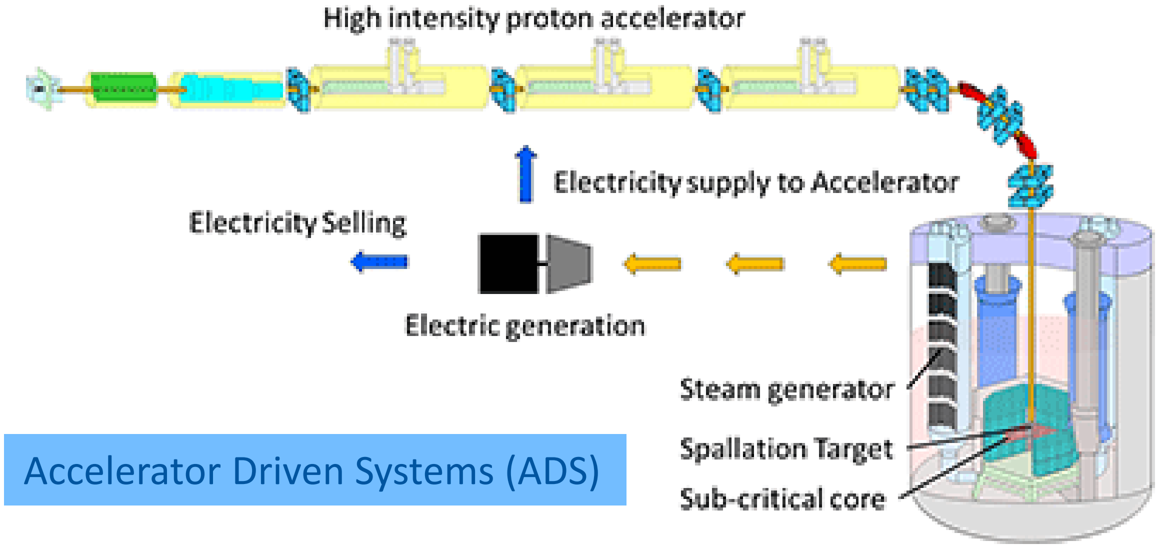
Relevant parameters for protection

- Momentum of the particle
- Particle type
  - Activation of material is mainly an issue for hadron accelerators.
- Energy stored in the beam
  - 360MJ per beam in the LHC
    when fully filled with 2808 bunches
- Beam power, Beam size, Time structure of beam
- Stored energy in (superconducting) powering systems (magnets, RF…)



Availability challenges – Example of ADS

- Accelerator Driven Systems (ADS) can reduce toxicity of radioactive waste and shorten the length of their half-life
- Operational concepts in machines until now: a fault is detected, then stop the beam(s) as fast as possible
- Consensus on ADS requirements
  - Unlimited number of short interruptions < ~ 1s
  - Few beam stops a year > ~1s -> All hardware failures !!
- ADS concepts require entirely new concepts for beam diagnostics and fault handling
  - case also exists for future HEP machines (e.g. 33 km Linear Collider)



Accelerator Driven Systems (ADS)

Availability challenges – Light sources

- Physics experiments @ todays light sources have stringent requirements for beam availability

Integrated-flux experiments
90% beam availability and 80% average beam power for duration of experiments
Beam unavailable: power less than 50% for more than one minute

Kinetic experiments
90% reliability for the duration of the measurement
Failure: Beam trip with a duration of more than 1/10th of the measurement length

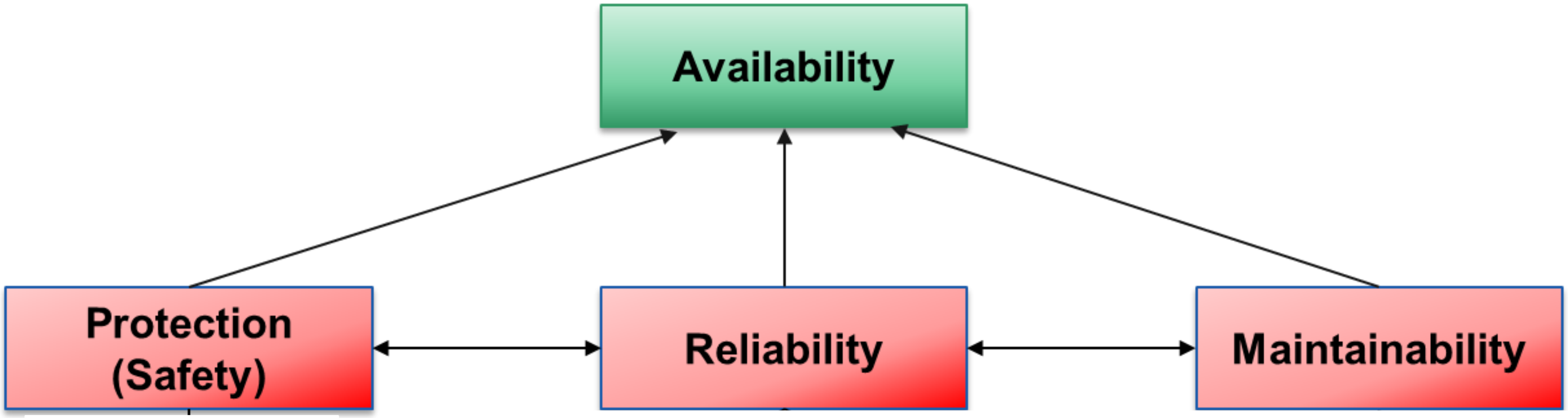
Swiss Light Source at PSI

ESS in Lund

Outline

- Why is dependability increasingly important for accelerators?
- Dependability Engineering in a nutshell
  - Dependability definitions, RAMS
- How to design reliable systems and operate them as such?
  - Understanding and mitigating the risks
  - Failure frequency
  - Failure impact – damage and downtime
  - Maintenance and operability
- Conclusions

Reliability Availability Maintainability Safety

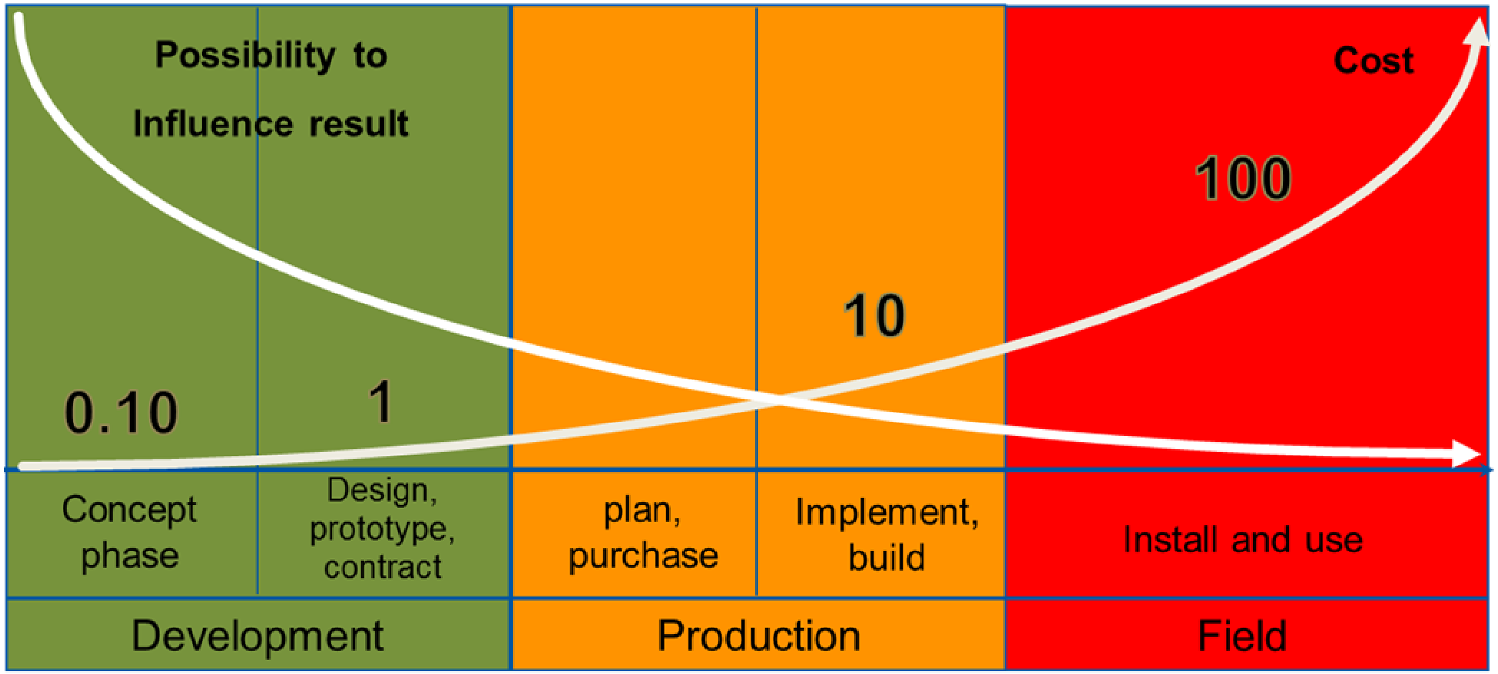


- Reliability analyses that are conducted early on in the life-cycle of a project allow us to determine (estimate) and influence (adjust) the dependability figures
  - Requires detailed understanding of underlying mechanisms

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

Importance of Reliability Analyses

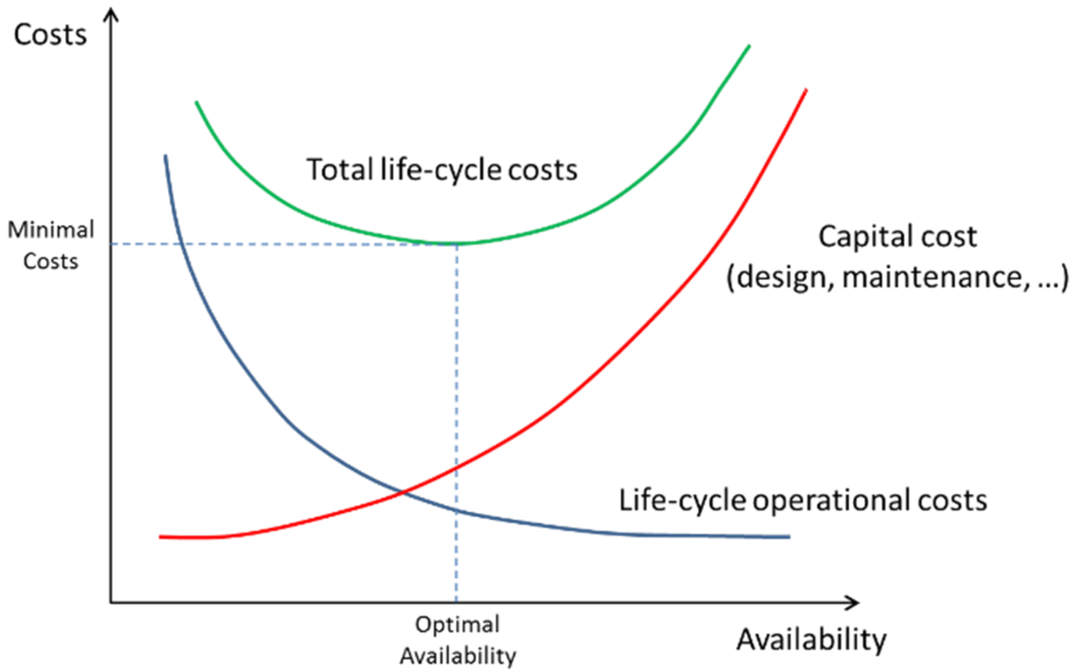
- Product/Accelerator Lifecycle



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

Prof. Dr. B. Bertsche, Dr. P. Zeiler, T. Herzig, IMA, Universität Stuttgart

Importance of Reliability Analyses



- Given a target performance reach (luminosity production, neutron fluence, number of patients treated, …), an optimal balance between capital costs and operational costs must be found
- Even more extensively applied in e.g. automotive or consumer electronics industry (link to TTZ 2017 in Appendix)

Basic Definitions 1/2

- **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 is 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 → :

What are the factors that limit their reliability and availability?

How can these be quantified systematically?

Basic Definitions 2/2

- **Maintainability (0-1)** is the probability of performing a successful repair action within a given time and restore the system to an operational status after a failure occurs.
  - Example of reliability specification: ”A particular component has a 90% maintainability for one hour if there is a 90% probability that the component will be repaired within an hour. ”

- **Safety (0-1)** is the probability that no catastrophic accidents will occur during system operation, over a specified period of time
  - Safety looks at the consequences and possible (impact of) accidents. Safety requirements are therefore concerned with making a system accident-free.

Outline

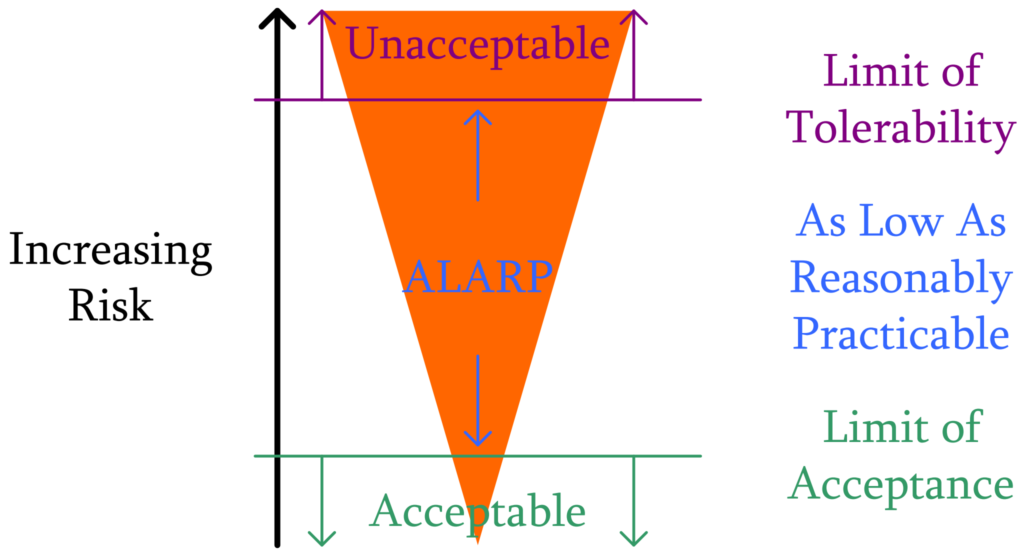
- Why is dependability increasingly important for accelerators?
- Dependability Engineering in a nutshell
  - Dependability definitions, RAMS
- How to design reliable systems and operate them as such?
  - Understanding and mitigating the risks
  - Failure frequency
  - Failure impact – damage and downtime
  - Maintenance and operability
- Conclusions

Risks for Particle Accelerators

- **Not to complete** the construction of the accelerator
  - Happened to other projects, the most expensive was the Superconducting Super Collider (SSC) in Texas / USA with a length of ~80 km
  - Cost increase from 4.4 Billion US$ to 12 Billion US$, US congress stopped the project in 1993 after having invested more than 2 Billion US$
- **Not** to be able **to operate** the accelerator
  - Insufficiently available machine / too many interlocks or false triggers
- **Damage** to the accelerator
  - **beyond repair** due to a major accident
  - Less serious but frequent accidents (damage to reputation of organisation)

Risk Assessment

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



- Risk is the product of the probability (frequency) of occurrence of an undesired event • 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

IMPACT

FREQUENCY

Risk Assessment: Example

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

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

Risk Assessment: Example

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

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				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

		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

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

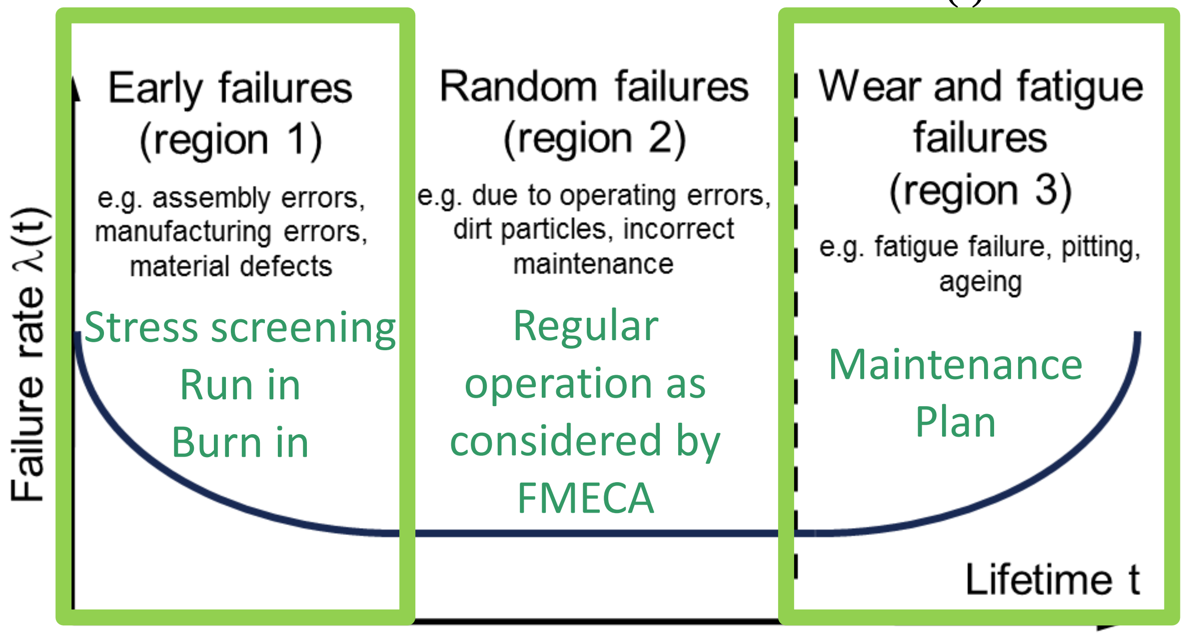
- Assessment of the required level of risk reduction (1-4) for different failure scenarios

Outline

- Why is dependability increasingly important for accelerators?
- Dependability Engineering in a nutshell
  - Dependability definitions, RAMS
- How to design reliable systems and operate them as such?
  - Understanding and mitigating the risks
  - Failure frequency
  - Failure impact – damage and downtime
  - Maintenance and operability
- Conclusions

Failure Rate and Bathtub Curve

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



Software?
Programmable Logic?

- 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…

How to estimate Component Failure Rates?

- 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 (or supplier if available)
  - Big uncertainties on boundary conditions
  - Good approximation for known technologies
  - Good for preliminary estimates

- Using Standards (Mil. Handbooks)
  - Very systematic approach, providing as well probability of possible failure modes
  - 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

Failure Mode Effect and Criticality Analysis

Failure Modes, Effects and Criticality Analysis

In what way can the system fail?…

…and what happens because of that?…

…and just how much of a problem does this cause?

34

Failure Mode Effect and Criticality Analysis

MIL-STD-1629

FMECA starts at the Component Level of a system

Break a large system into blocks, defining smaller, manageable sub-systems

⇩

get subsystem schematics, component list, and understand what it does

MIL-HDBK-338 ⇩ MIL-HDBK-217

get MTBF of each component on the list, derive P_{FAIL}(mission)

MIL-HDBK-338 ⇩ FMD-97

derive failure modes and failure mode ratios for each component

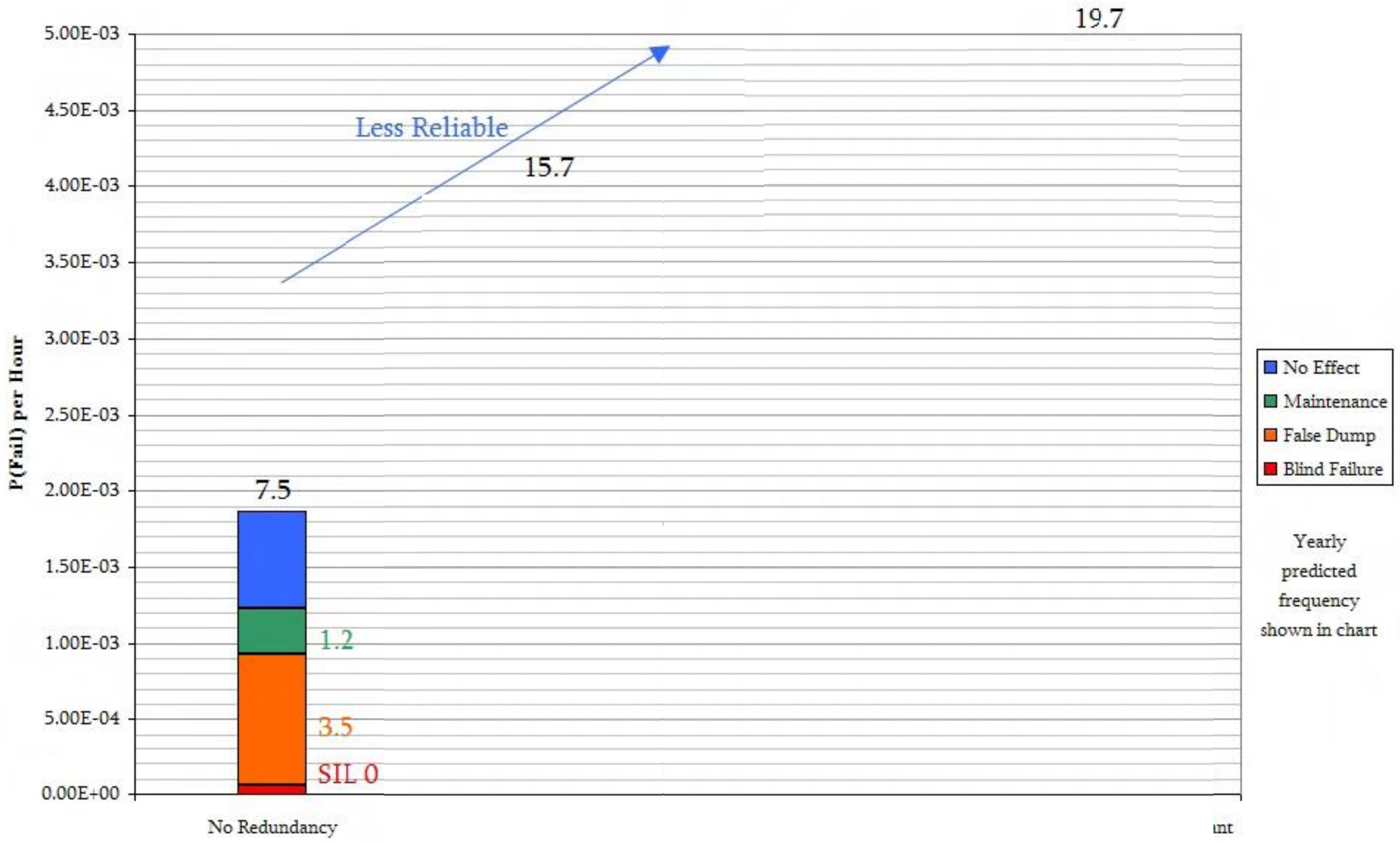
⇩

explain the effect of each failure mode on both the subsystem and system

⇩

determine the probability of each failure mode happening. Draw conclusions.

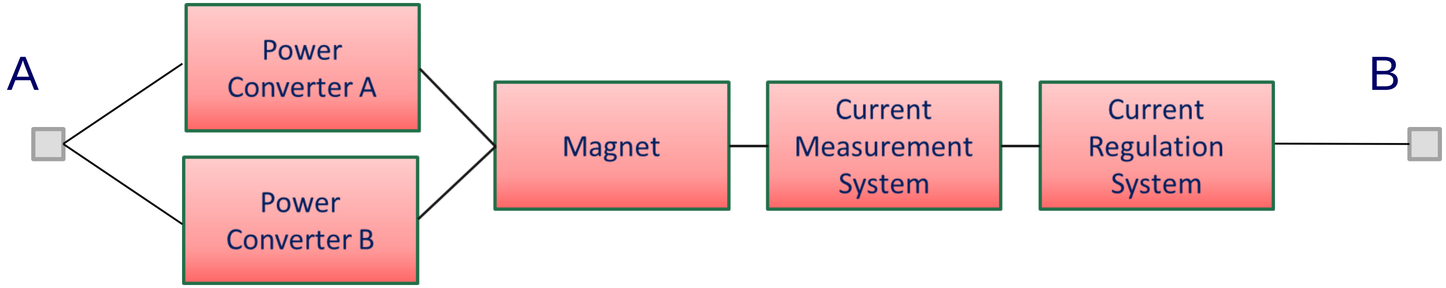
Dependability vs system configuration



Alternative methods to describe system failure behaviour

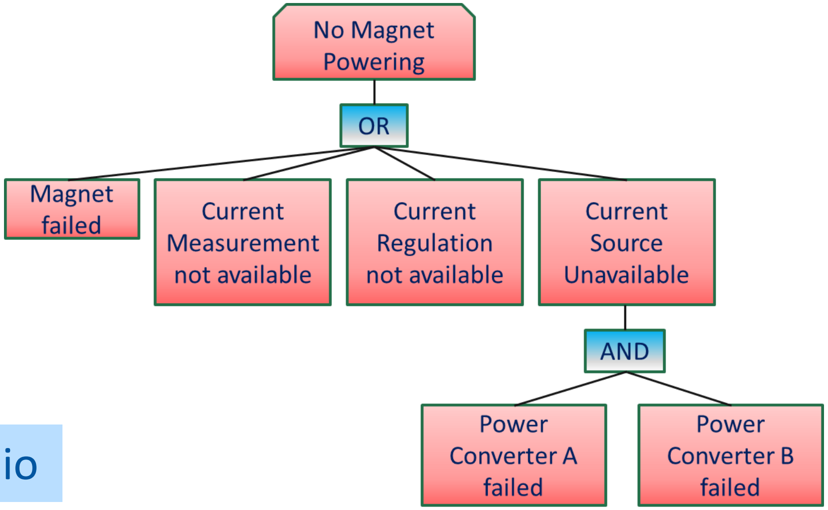
- Reliability Block Diagram:

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



- Fault Tree:

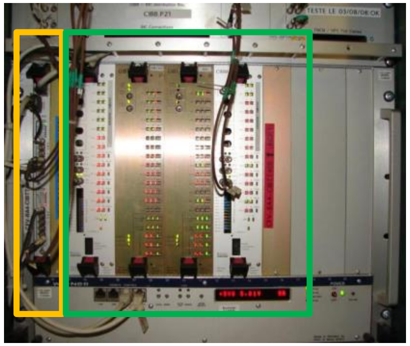
Question: what are the combinations of failures that lead to a system failure?



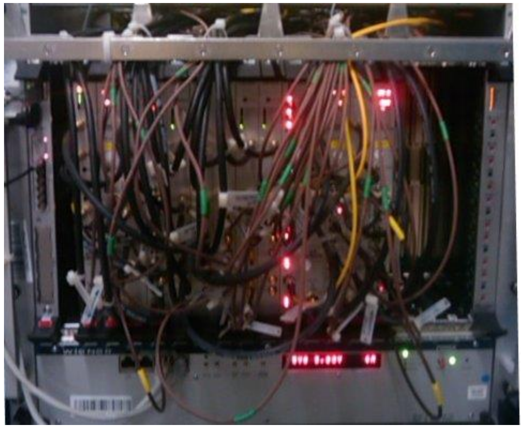
Boolean Algebra allows calculating system reliability from component reliability

Courtesy: A.Apollonio

Things outside the scope of a reliability analysis



- Services
- Infrastructure
- Controls



Redundancy is more effective when it goes beyond the system boundary

- Reliability during installation

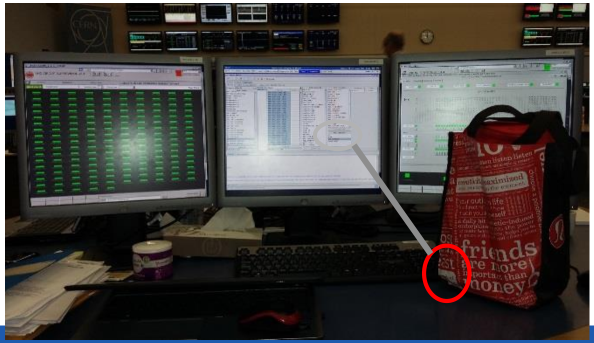
- Interconnections between systems

- Maintenance and spares

- Human Errors

100kg of batteries in front of the spares cupboard… and no pallet lifter in sight…

If you have open racks… expect things like this

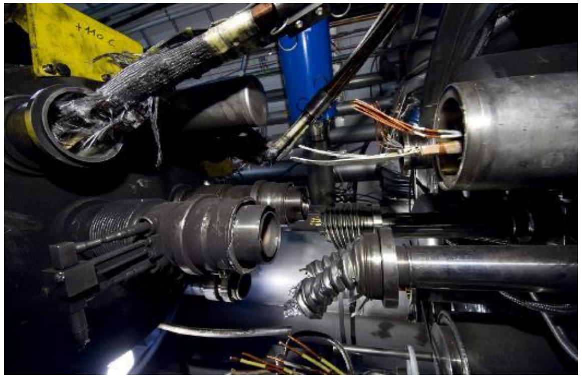


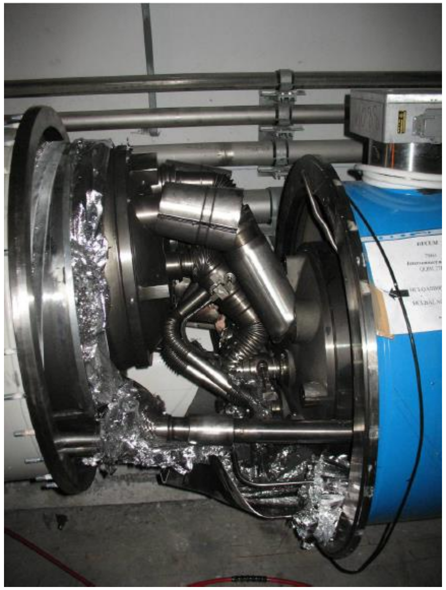
“mystery of the missing 220V cable”

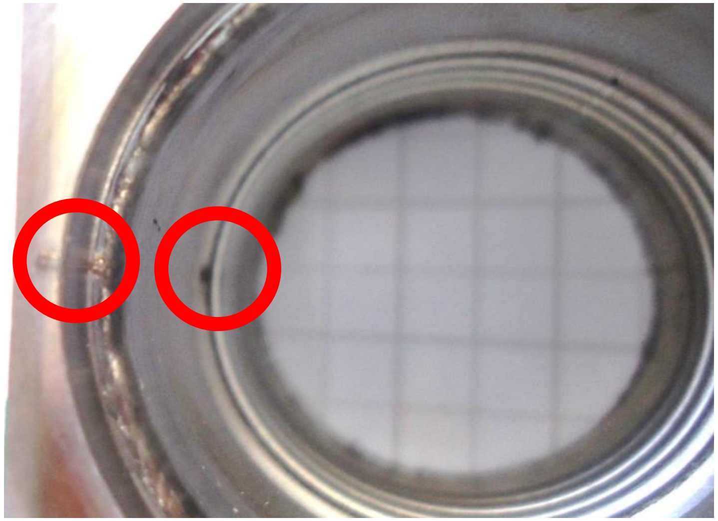
Outline

- Why is dependability increasingly important for accelerators?
- Dependability Engineering in a nutshell
  - Dependability definitions, RAMS
- How to design reliable systems and operate them as such?
  - Understanding and mitigating the risks
  - Failure frequency
  - Failure impact – damage and downtime
  - Maintenance and operability
- Conclusions

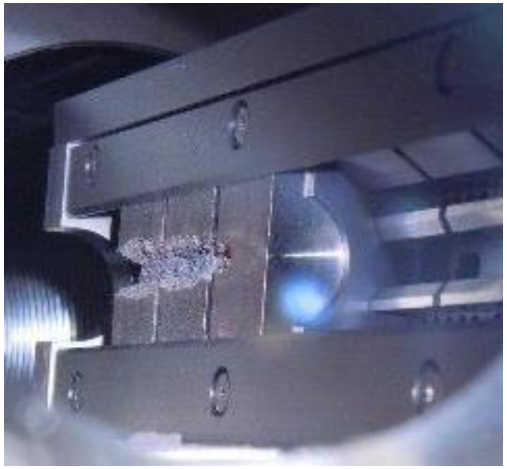
Failure Impact: Damage (learn from experience)

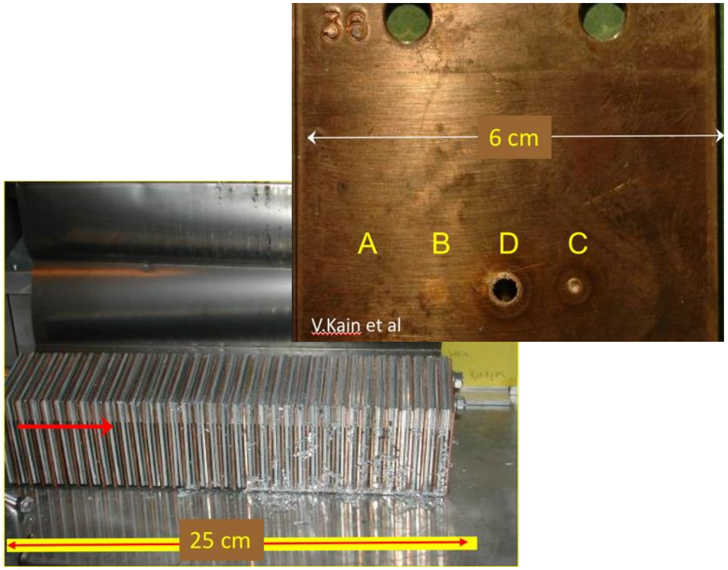


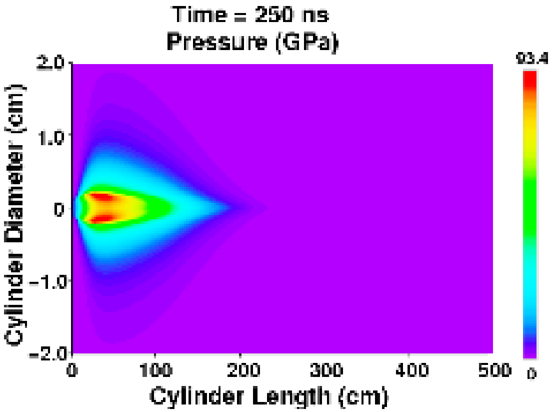


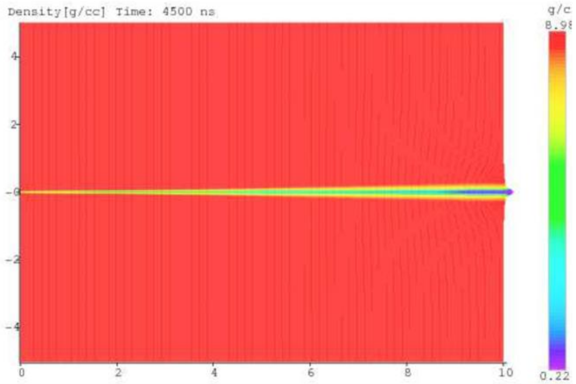


Failure Impact: Damage (tests and simulations)

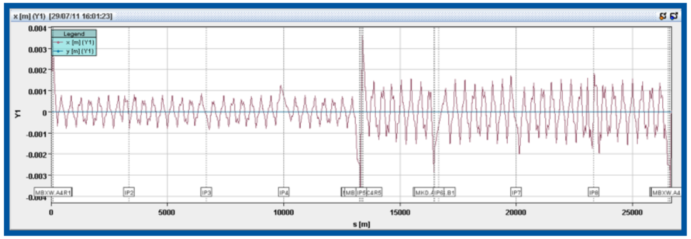








(c) Density (g/cm^3).



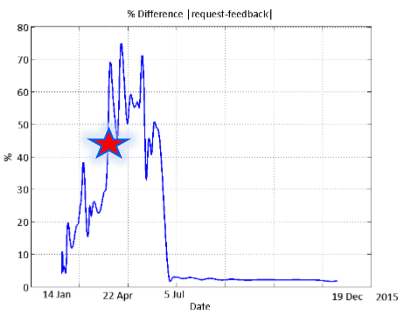
Failure Impact: Downtime

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

For a large complex, include technical infrastructure and eventual injectors!

Failure Impact: 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,…)

Outline

- Why is dependability increasingly important for accelerators?
- Dependability Engineering in a nutshell
  - Dependability definitions, RAMS
- How to design reliable systems and operate them as such?
  - Understanding and mitigating the risks
  - Failure frequency
  - Failure impact – damage and downtime
  - Maintenance and operability
- Conclusions

Failure Impact: Maintenance strategies

- Breakdown/reactive Maintenance:
  - Waiting until equipment fails before repairing or servicing it
- Preventive Maintenance (PM):
  - (Time-based or run-based) Periodically inspecting, servicing, cleaning, or replacing parts to prevent sudden failure (Cryogenics, Cooling & Ventilation..)
  - (Predictive) On-line monitoring of equipment in order to use important/expensive parts to the limit of their serviceable life (RF components, klystrons,…)
- Corrective Maintenance:
  - Improving equipment and its components so that preventive maintenance can be carried out reliably
    -> Long-term feed forward from fault tracking into consolidation

Low initial cost
Faults piling up

High initial cost
Fault rates kept ~ constant

Failure Impact: Maintenance strategies

- "...the (long-term) cost of breakdown maintenance is usually much greater than preventive maintenance."

- Preventive maintenance...
  - Keeps equipment in good condition to prevent large problems
  - Extends the useful life of equipment
  - Finds small problems before they become big ones
  - Helps eliminate rework/scrap and reduces process variability
  - Keeps equipment safer and greatly reduces unplanned downtime

- In a 24x7 manufacturing operation, it is typically better to perform the hours of activities in several smaller periods of time
- Performing PMs inconsistently is functionally equivalent to consistently having much longer downtime durations

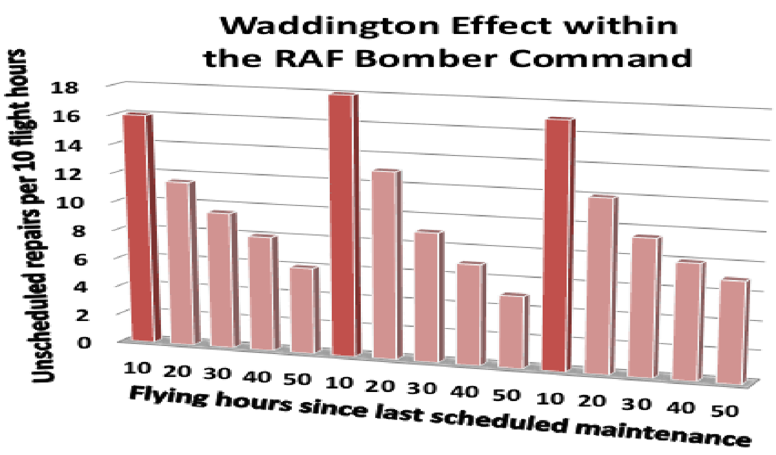
http://www.prenhall.com/divisions/bp/app/russellcd/PROTECT/CHAPTERS/CHAP15/HEAD01.HTM

Waddington Effect

- First observed by C.H. Waddington during the 2nd world war studying British aircraft maintenance
  - RAF had major reliability issues with their B24 planes
- Background theory: unscheduled downtime should be a random phenomenon
- If all unscheduled downtime events are plotted with respect to the last preventive maintenance action, there should not be any pattern evident

Conrad Hal (C.H.) Waddington - (1905-1975)
Developmental biologist, paleontologist, geneticist, embryologist and philosopher

Waddington Effect



A pattern of increased un-scheduled downtime immediately following PM's is a "Waddington Effect"

- Increase the time interval between scheduled maintenance cycles, and eliminate all preventive maintenance tasks that couldn't be demonstrably proven to be beneficial. -> effective flying hours of fleet increased by 60 percent!
- Maintenance isn't an inherently good thing, but it's a necessary evil (like surgery). We have to do it from time to time, but we sure don't want to do more than absolutely necessary to keep our aircraft safe and reliable. Doing more maintenance than necessary actually degrades safety and reliability
- Maintenance actions and plans have to be adapted to the system at hand to make them effective! There is not one that fits them all (electronics, mechanical, …)!

Outline

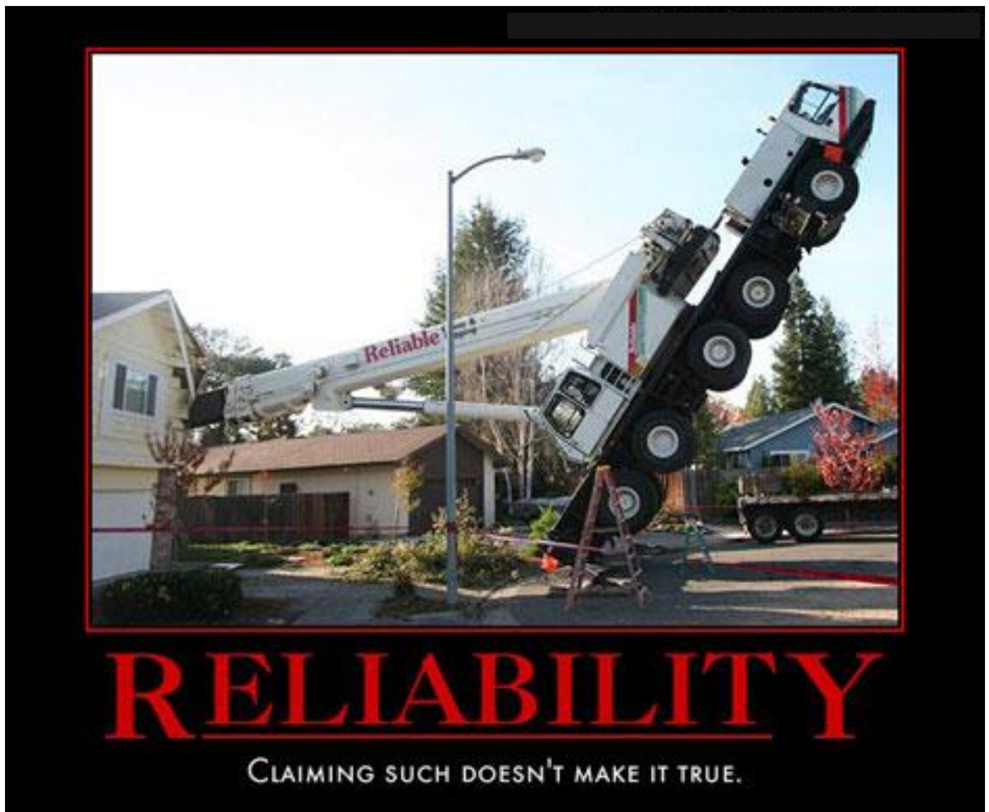
- Why is dependability increasingly important for accelerators?
- Dependability Engineering in a nutshell
  - Dependability definitions, RAMS
- How to design reliable systems and operate them as such?
  - Understanding and mitigating the risks
  - Failure frequency
  - Failure impact – damage and downtime
  - Maintenance and operability
- Conclusions

Conclusions

- Reliability engineering is the art and challenge to determine and find the optimal working point of a given installation
- Large set of tools and methodologies exists today, optimized for respective domains and problems
- Always remains a trade-off, but needs to be considered from early design phases as it will be a key ingredient to the success of our future projects

Many thanks for your attention!

Questions?

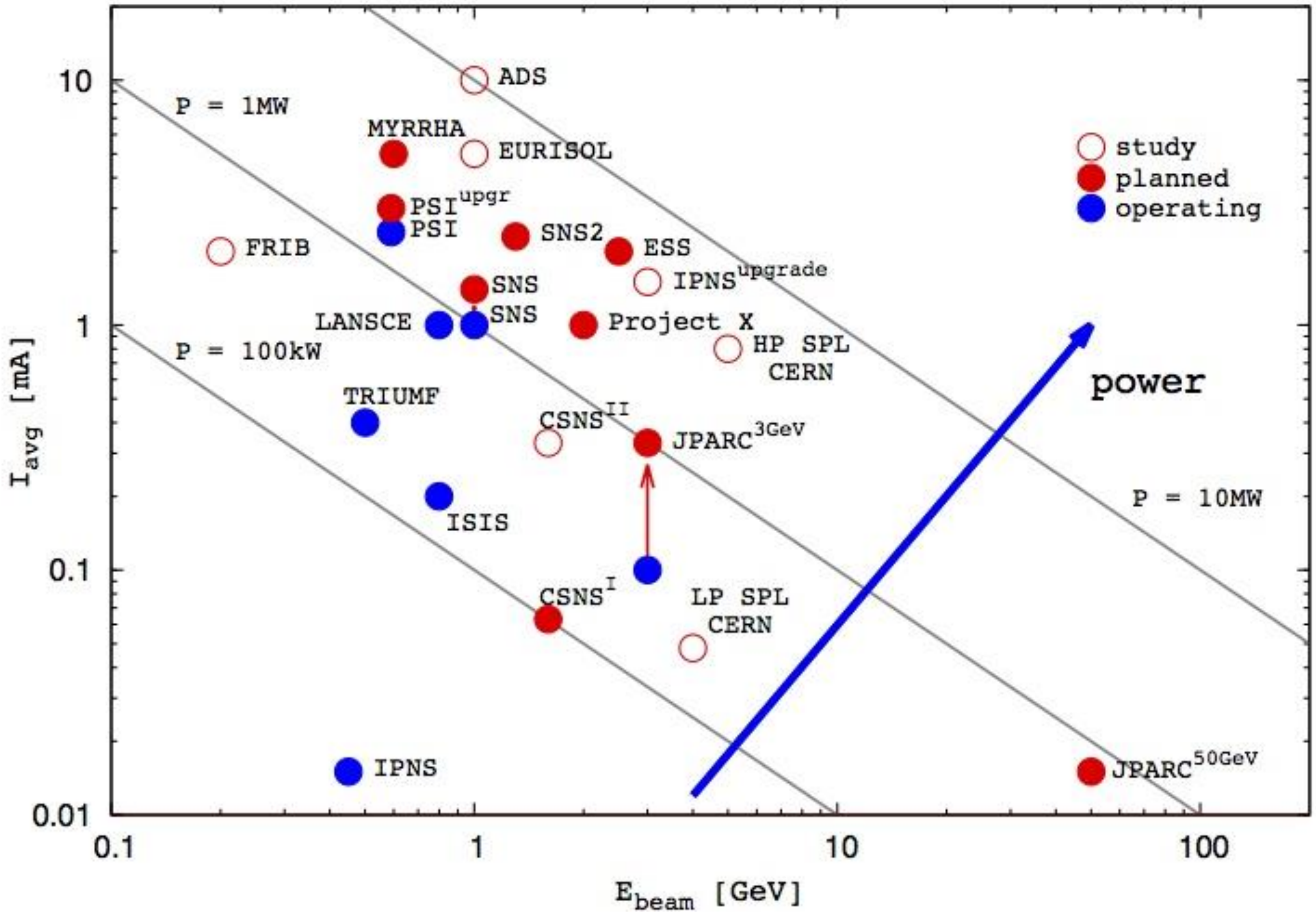


Additional reading

Accelerator Reliability Workshops
https://www.synchrotron-soleil.fr/fr/evenements/arw-2017-accelerator-reliability-workshop

TTZ 2017
https://www.vdi-wissensforum.de/weiterbildung-maschinenbau/technische-zuverlaessigkeit/

Spallation Sources + High Intensity Accelerators



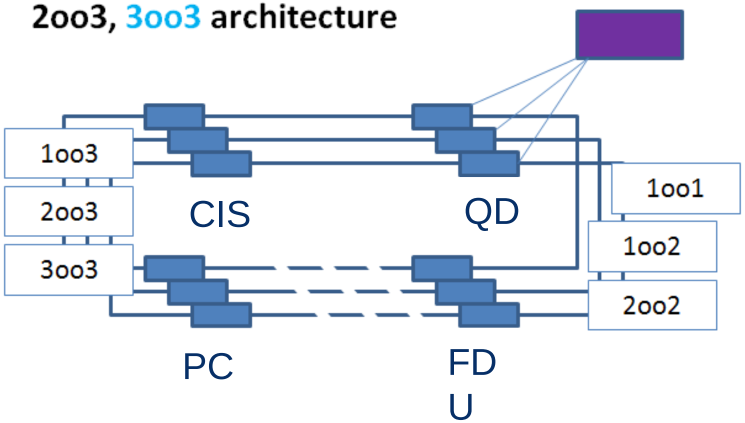
Use of COTS in Highly Dependable systems

Collaboration with ITER for development of magnet protection system

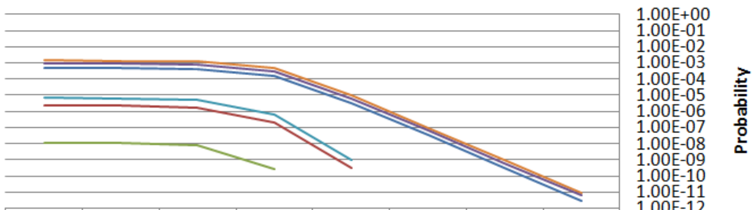
Dependability requirements of ITER for **high safety AND availability** + desire to use COTS components are huge challenge for machine protection systems

Extensive dependability studies done, confirming 2oo3 architecture as the sole suited candidate to meet dependability requirements

Comparison between 1oo1, 1oo2, 1oo3 , 2oo2 2oo3, 3oo3 architecture



n:250, Demand missed B6A



	1.00E-08	1.00E-07	1.00E-06	1.00E-05	1.00E-04	1.00E-03	1.00E-02	1.00E-01
3oo3	1.40E-03	1.39E-03	1.25E-03	4.77E-04	9.49E-06	9.62E-08	9.63E-10	9.00E-12
2oo2	9.37E-04	9.27E-04	8.35E-04	3.18E-04	6.33E-06	6.42E-08	6.42E-10	6.00E-12
2oo3	6.63E-06	6.47E-06	5.10E-06	6.19E-07	9.54E-10	0.00E+00	0.00E+00	0.00E+00
1oo1	4.70E-04	[illegible]	4.18E-04	1.59E-04	3.16E-06	3.21E-08	3.21E-10	3.00E-12
1oo2	2.22E-06	2.16E-06	1.71E-06	2.06E-07	3.18E-10	0.00E+00	0.00E+00	0.00E+00
1oo3	1.18E-08	1.14E-08	7.78E-09	2.76E-10	0.00E+00	0.00E+00	0.00E+00	0.00E+00

λf

Safety

Courtesy of S.Wagner

Use of COTS in Highly Dependable systems

Architecture problem was analytically solved, allowing for extensive sensitivity studies of variants as function of input parameters

Analytical approach was confirmed by Monte-Carlo like simulation

Default, x=2E-4	Number of clients=2			Number of clients=4		
Scenario	1oo1 (k=1)	1oo3 (k=3)	2oo3 (k=3, voting)	1oo1 (k=1)	1oo3 (k=3)	2oo3 (k=3, voting)
Completed mission (1)	75%	25%↓	10% ↑	65%	44%↓	12%↑
False triggered (2)	12.5%	Factor 2.6↑	Factor 2.8↓	23.3%	Factor 2.3↑	Factor 1.6 ↓
Demand success (3)	12.5%	12.2%↓	6%↑	11.7%	22.1%↓	9%↑
Demand missed (4)	4E-4	Factor 47'600 ↓	Factor 77 ↓	4E-4	Factor 60'700↓	Factor 87↓

Sigrid Wagner et al: "Architecture for Interlock Systems: Reliability Analysis with Regard to Safety and Availability", ICALEPCS 2011, Grenoble, WEPMU006

Use of COTS in Highly Dependable systems

Prototype to be delivered these days to ITER

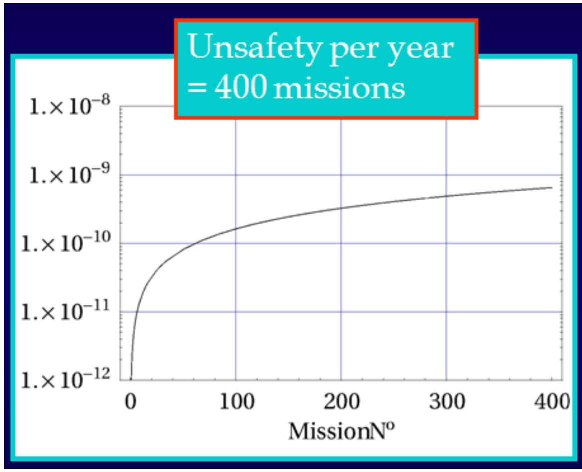
Based on redundant safety PLCs + 2oo3 I/O module configuration (down to and including client connections)

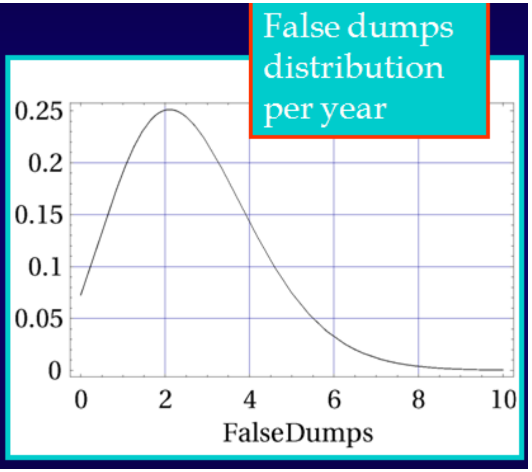
Fault tolerant to single component failure

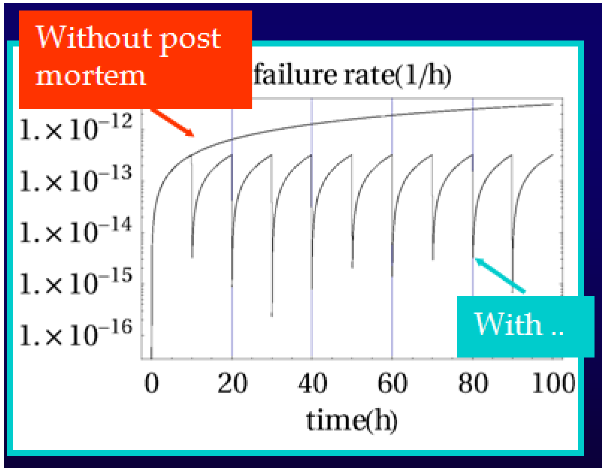
Redundancy of programming through safety matrix + standard logic

Standard user interface for client connections and diagnostics

Commissioning and repetitive testing







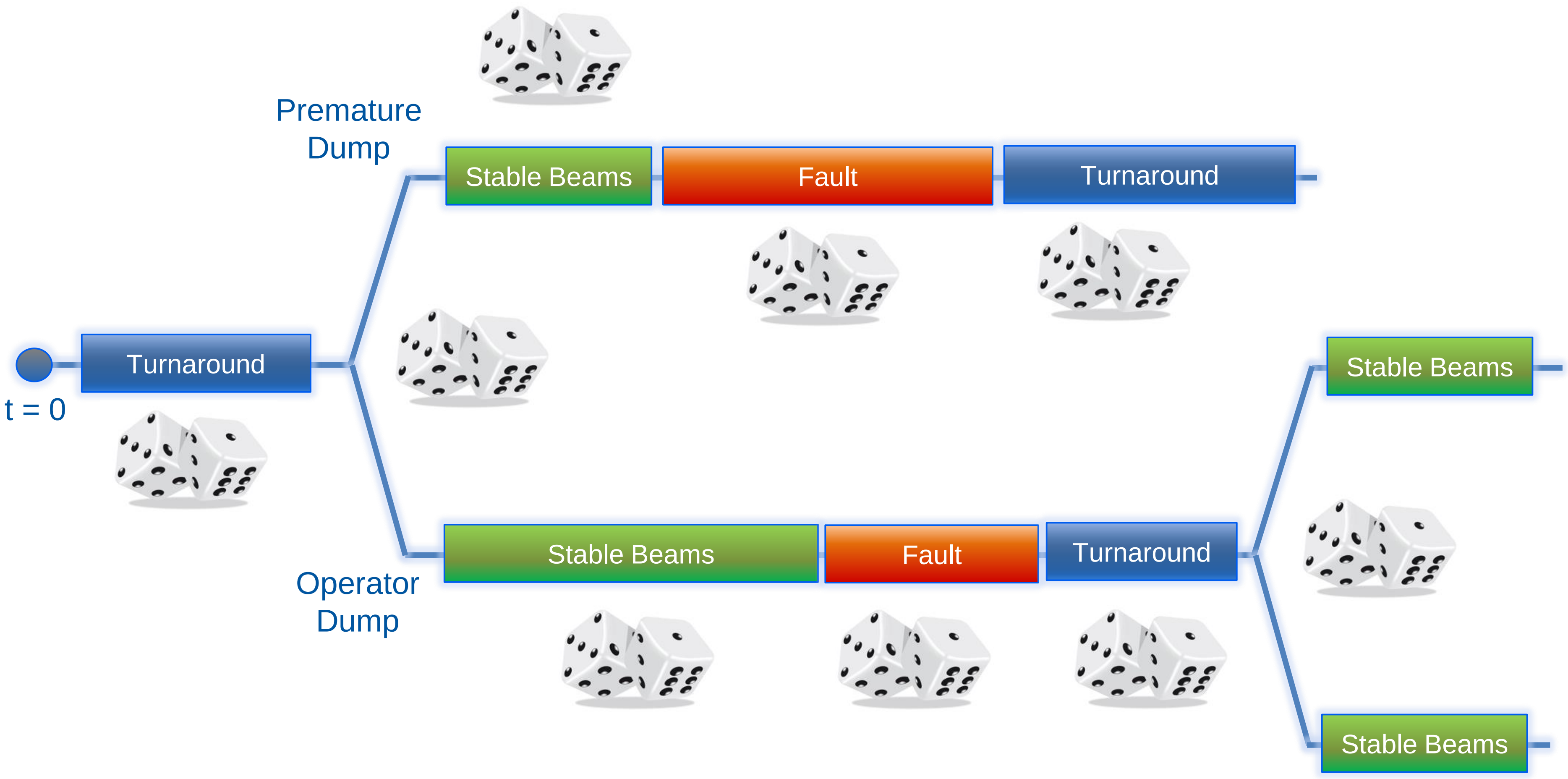
- To maintain desired reliability, big investment into commissioning procedures, sequencing, automated regular testing (pre-/post-operational checks),…
- Assuring for every mission (~10hours) an as good as new system through analysis of ‘Post mortem’ data (automated + manual by machine protection expert)

ADS and light source specifities

- Very efficient failure detection means
- Extensive diagnostics capabilities
- Beam diagnostics needs to be **non-interceptive (**high beam Power)
- Redundancy in the signals to **avoid accidental start of corrective actions**
- Strategies to maintain accelerator operation within nominal parameters when a fault is detected, before intervention of safety or MPS (Machine Protection System) interlocks
- Need a new concept of control system, with respect to existing machines, *unprecedented in accelerator operation*, handling redundant components and fault tolerance

Trip duration	Max. number of trips
1 second - 6 seconds	758 trips per day
6 seconds - 1 minute	136 trips per day
1 minute - 6 minutes	12 trips per day
6 minutes - 20 minutes	350 trips per year
20 minutes - 1 hour	99 trips per year
1 hour - 3 hours	33 trips per year
3 hours - 8 hours	17 trips per year
8 hours - 1 day	6.7 trips per year
More than 1 day	3.25 trips per year

Monte Carlo simulations



Monte Carlo simulations