Reliability Study of the Beam Loss Monitor System for the LHC

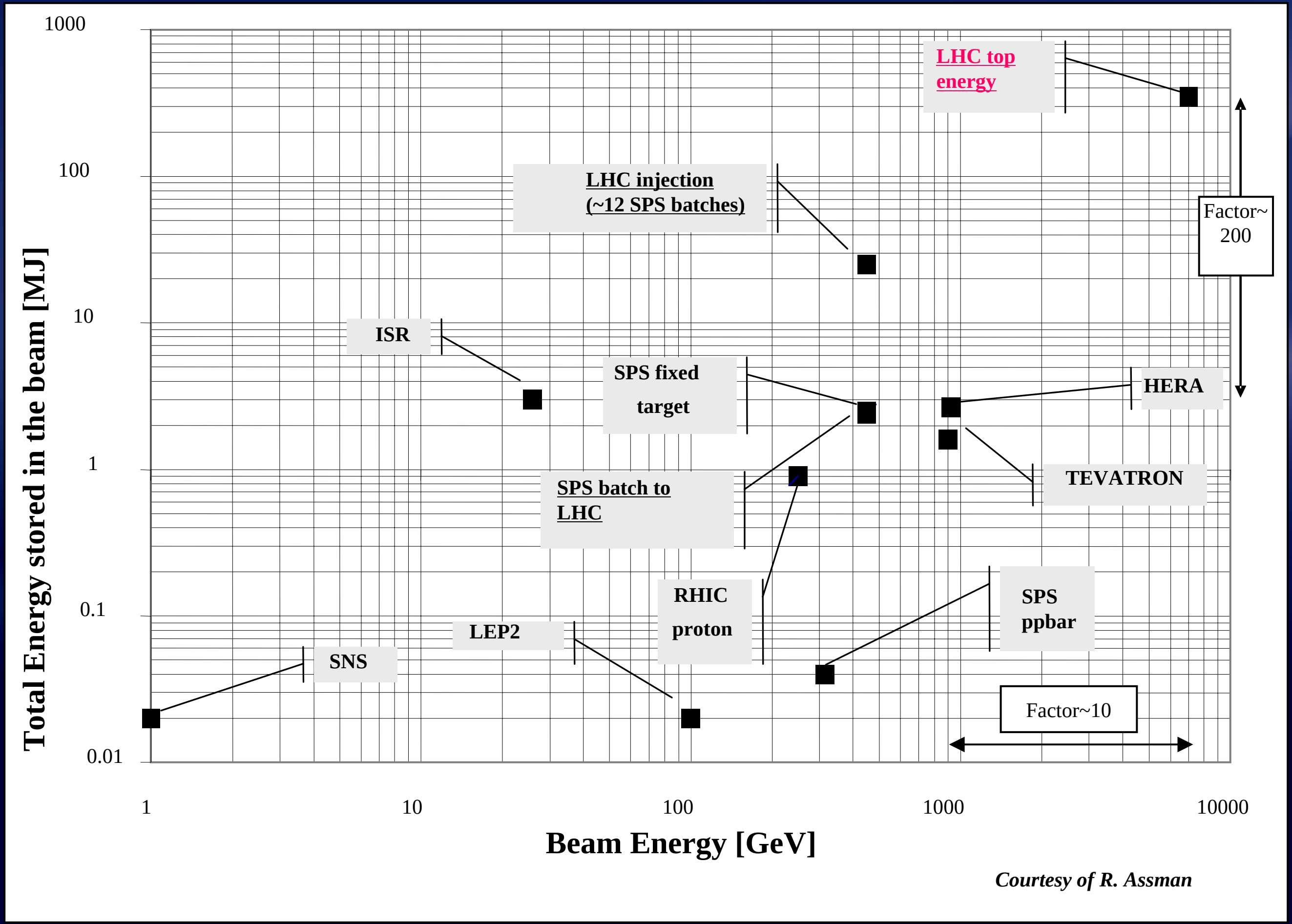
G. Guaglio

Outline

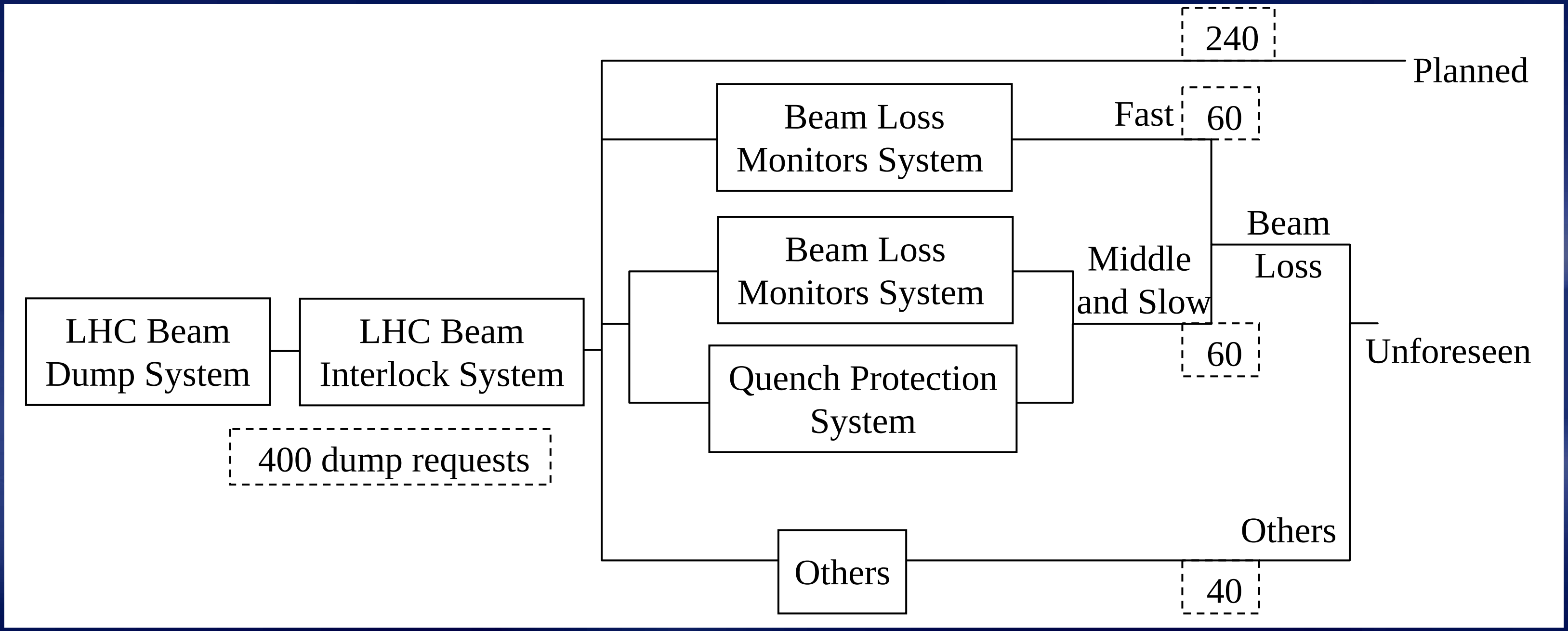
- Introduction.
- System Layout.
- Dependability.
- Dependable Design.
- Dependability Analysis.
- Conclusions.

LHC Challenges

1. 7 TeV protons (10 times higher than existing accelerators).
2. 724 MJ of energy in the two beams (200 times higher).
3. 10 GJ of energy in the electric circuits.
4. Superconductive magnets: 502 main quadrupoles, 1232 main dipoles.



LHC Protection System



In the frame of the Reliability Sub-Working Group, the <u>LHC systems</u> have been <u>globally investigated</u> from the dependability point of view.

BLMS Aims

Protection against damages caused by beam losses.

1. Measure the lost protons.
2. Compare the shower signal with thresholds.
3. Trigger the extraction of the beam to stop the beam losses.

The BLMS must be :

1. SAFE: in case of dangerous loss, it has to inhibit the beam permit. If it fails, there will be ~30 days of downtime.
2. FUNCTIONAL: in case of NO dangerous loss, it has NOT to inhibit the beam. If it fails, it generates a false alarm and 3 h will be lost to recover the previous situation. Such an event will decrease the LHC efficiency.

Outline

- Introduction.
- System Layout.
- Dependability.
- Dependable Design.
- Dependability Analysis.
- Conclusions.

System Layout

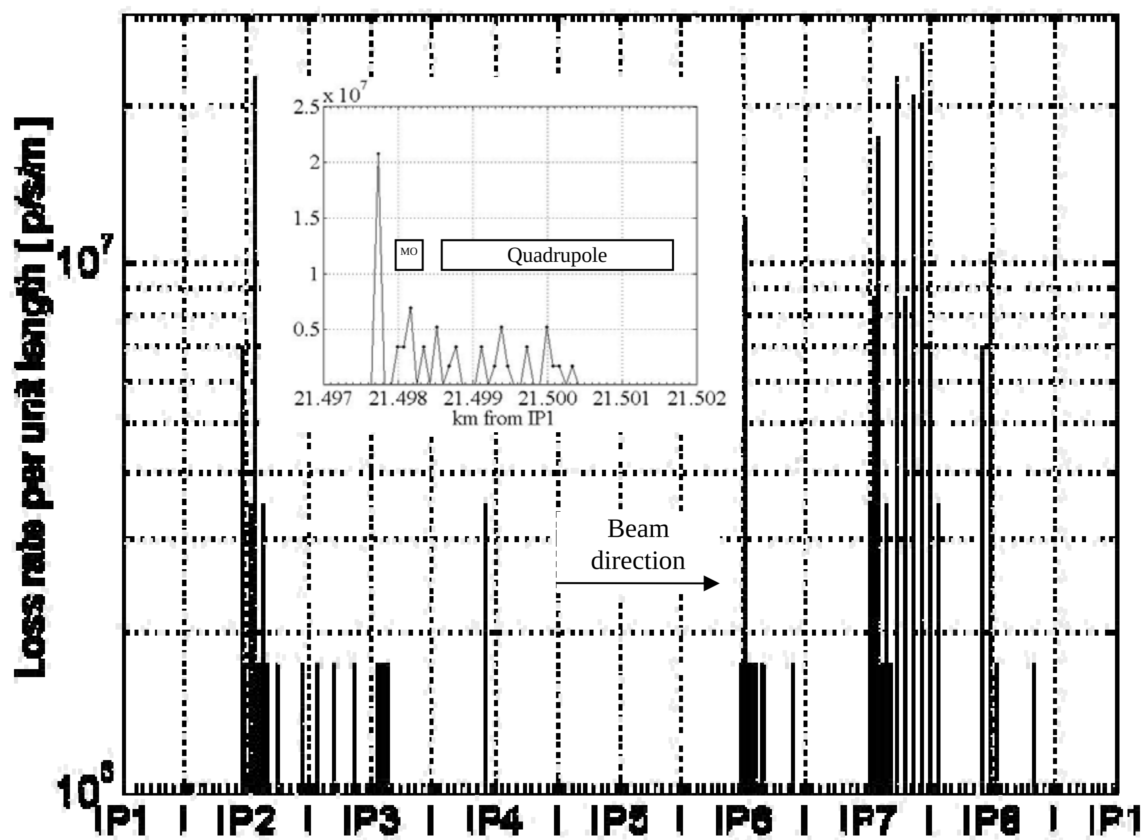
1. Detector Locations.
2. Secondary Particles Heating.
3. Front End Electronics.
4. Back End Electronics.
5. Combiner.
6. VME Crate and Rack.
7. Power Supplies.

Detector Location

Simulation of the loss locations along the LHC ring.

Concentration of losses at the quadrupole regions.

Conservative hypothesis: the simultaneous presence of high losses in different locations is neglected. Every dangerous loss could be seen just by one detector.



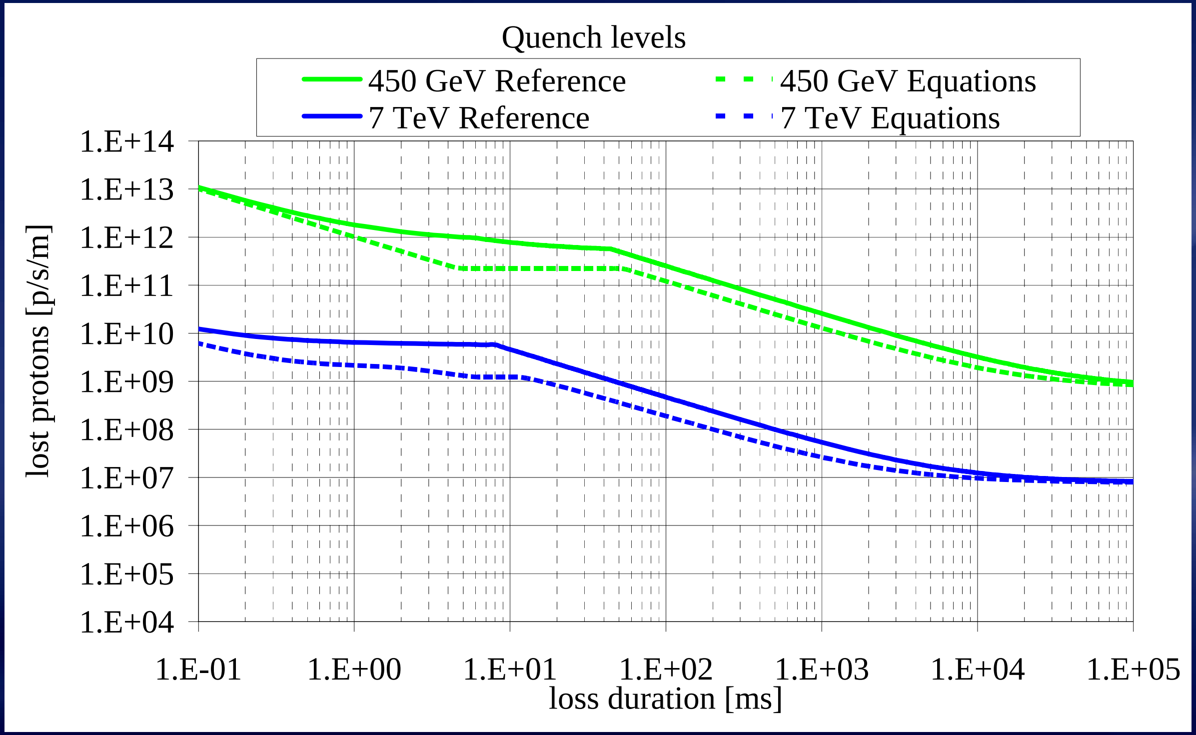
Courtesy of S. Redaelli

Secondary Particles Heating

Estimation of the <u>proton rate density necessary to perform a transition</u> from the superconductive state to the normal conductive state.

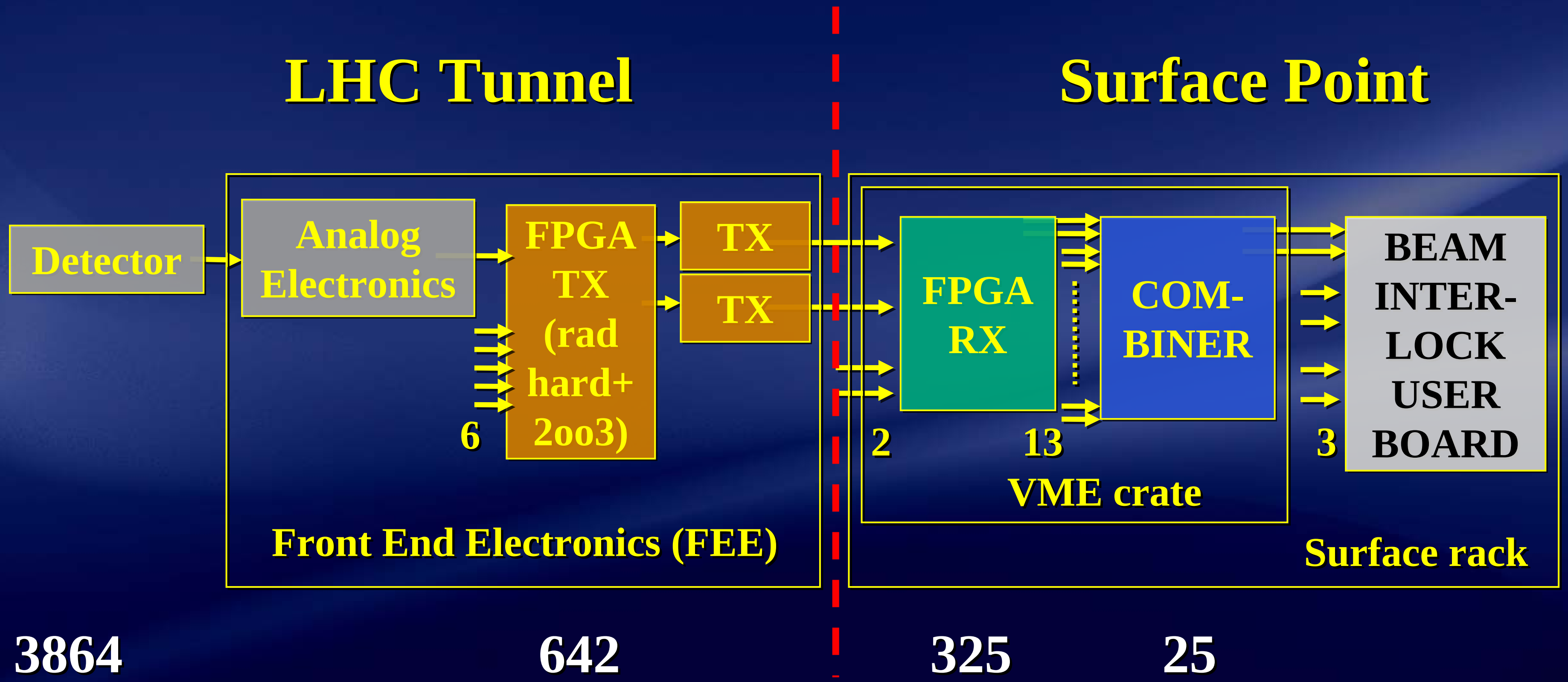
Different estimation performed with non-linear differential equations (film boiling effect, …).

***Big uncertainty**. Further studies motivated.*



$$
\begin{cases}
C_w(T_w)\cdot\Delta\dot{T}_w = \overbrace{p_{rate}(t)\cdot E_p}^{beam} - \overbrace{\Delta T_w/\tau_w}^{cable} - \overbrace{\varphi_{He}(\Delta T_w - \Delta T_{He})}^{helium} \\
C_{He}(T_{He})\cdot\Delta\dot{T}_{He} = \overbrace{\varphi_{He}(\Delta T_w - \Delta T_{He})}^{helium} - Cryogenics
\end{cases}
$$

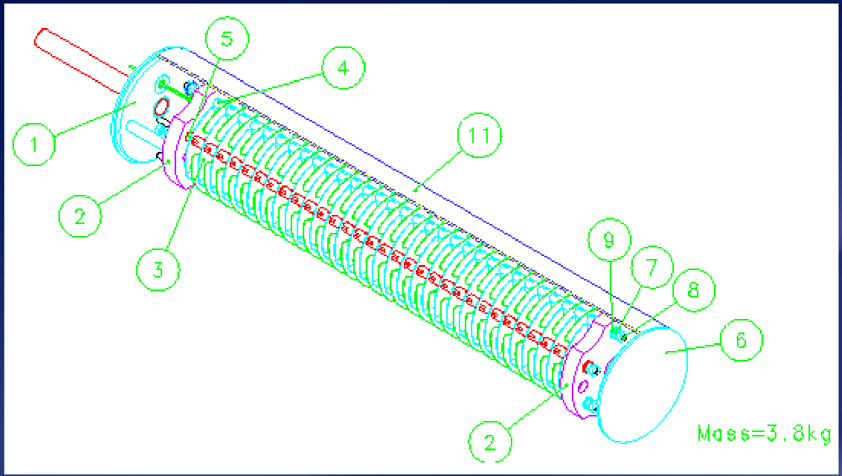
BLMS Signal Chain

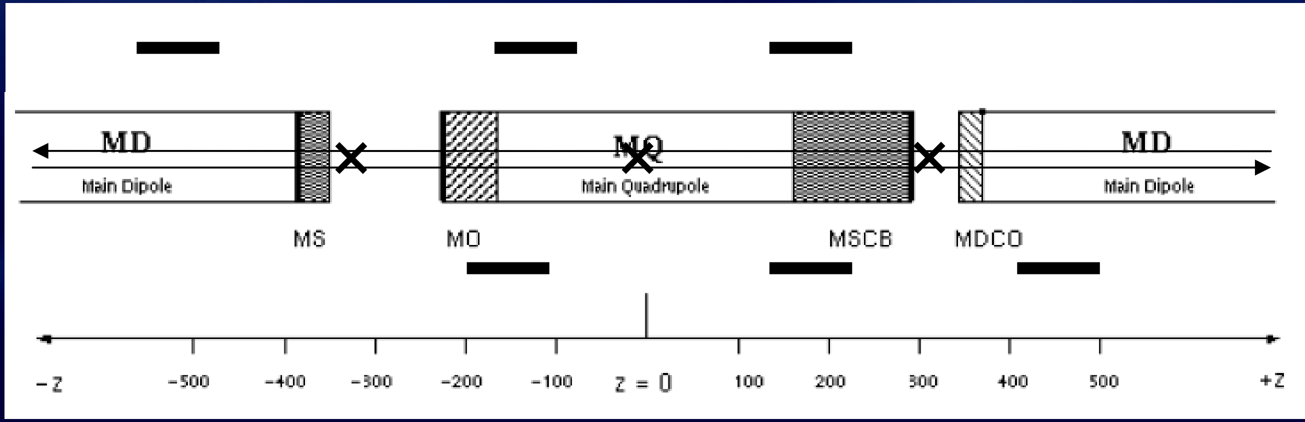


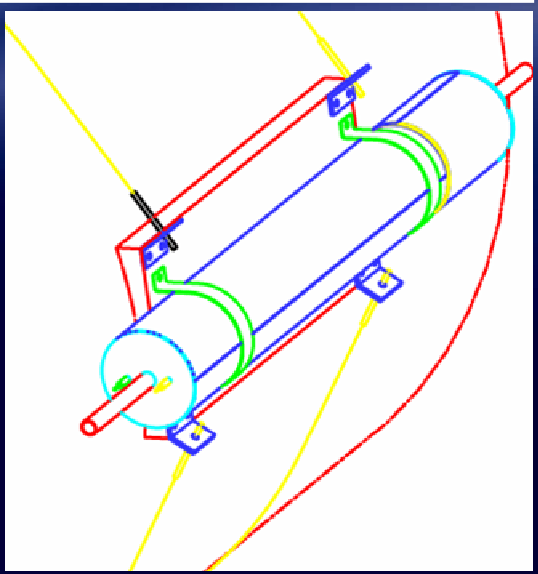
Total quantities in LHC

Detector

- Detection of the particles' shower.
- Current signal proportional to the particles' loss.
- Ionization chambers placed around the quadrupole region.

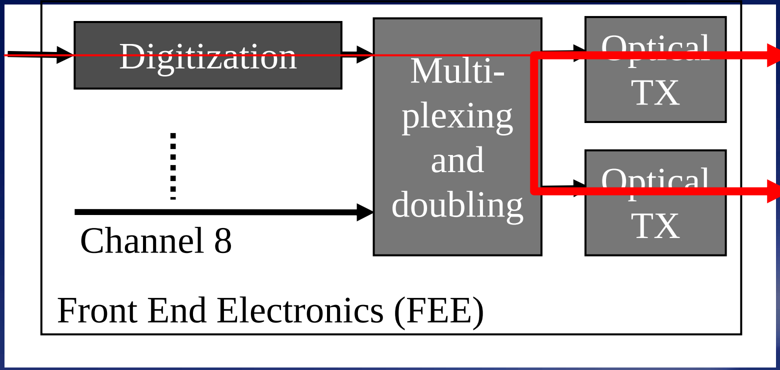


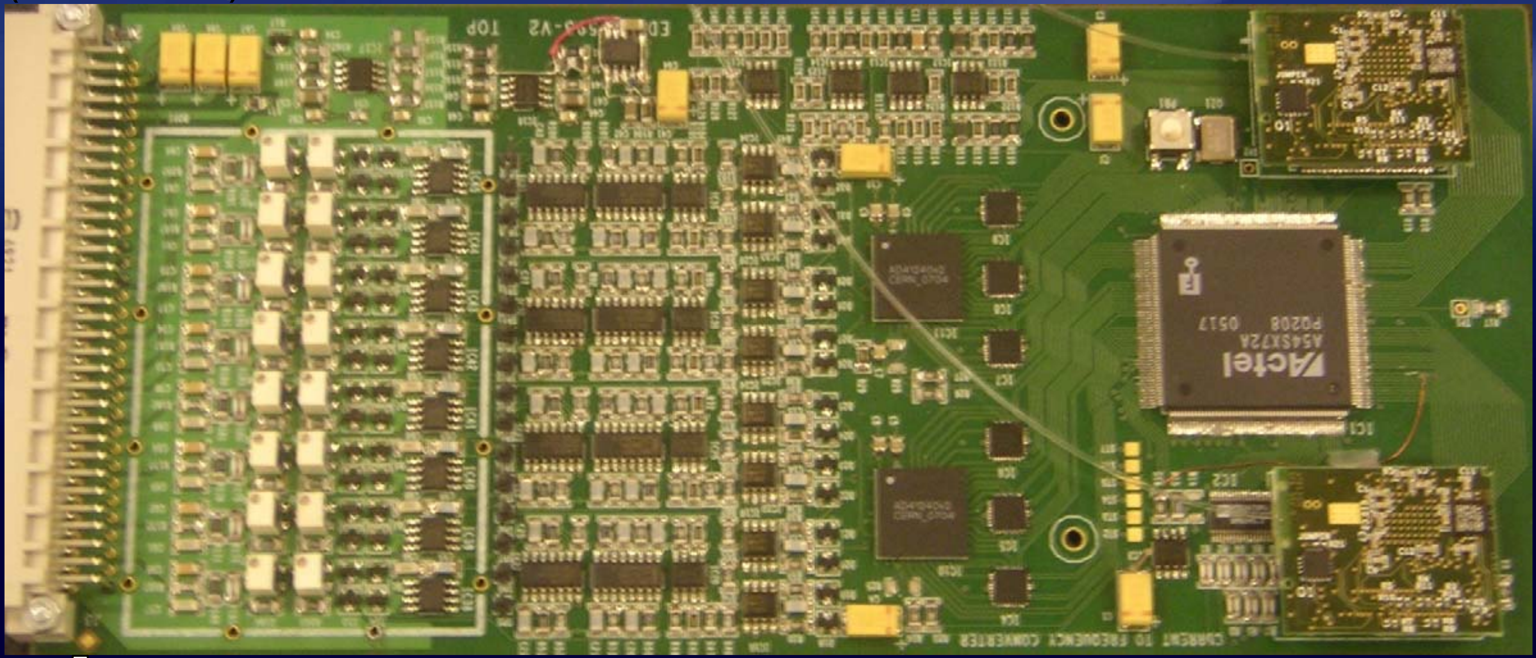




Front End Electronics

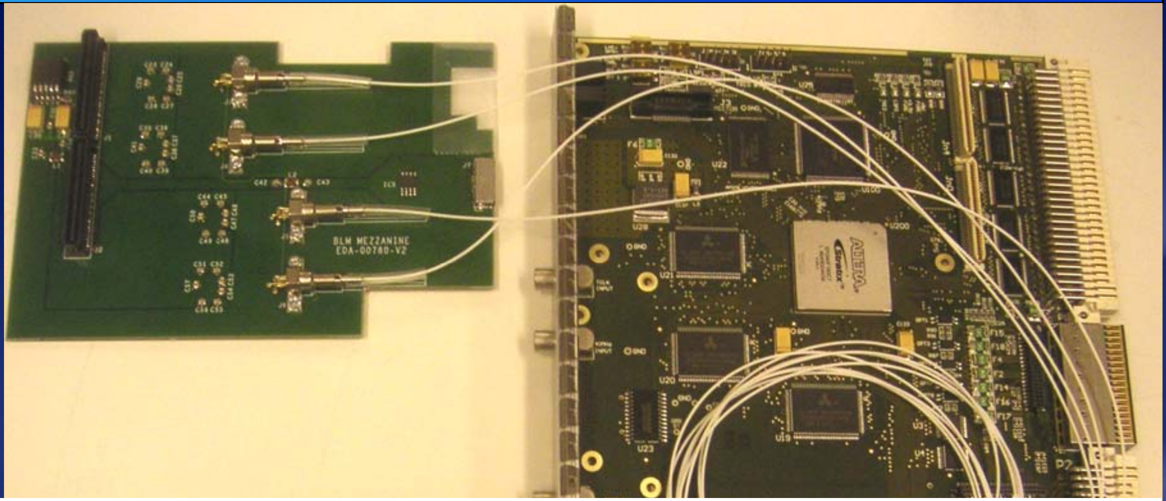
- Transformation of the current signal in a digital data.
- Multiplexing of 8 channels with redundant optical transmission.
- Electronics in an harsh environment (radiations).

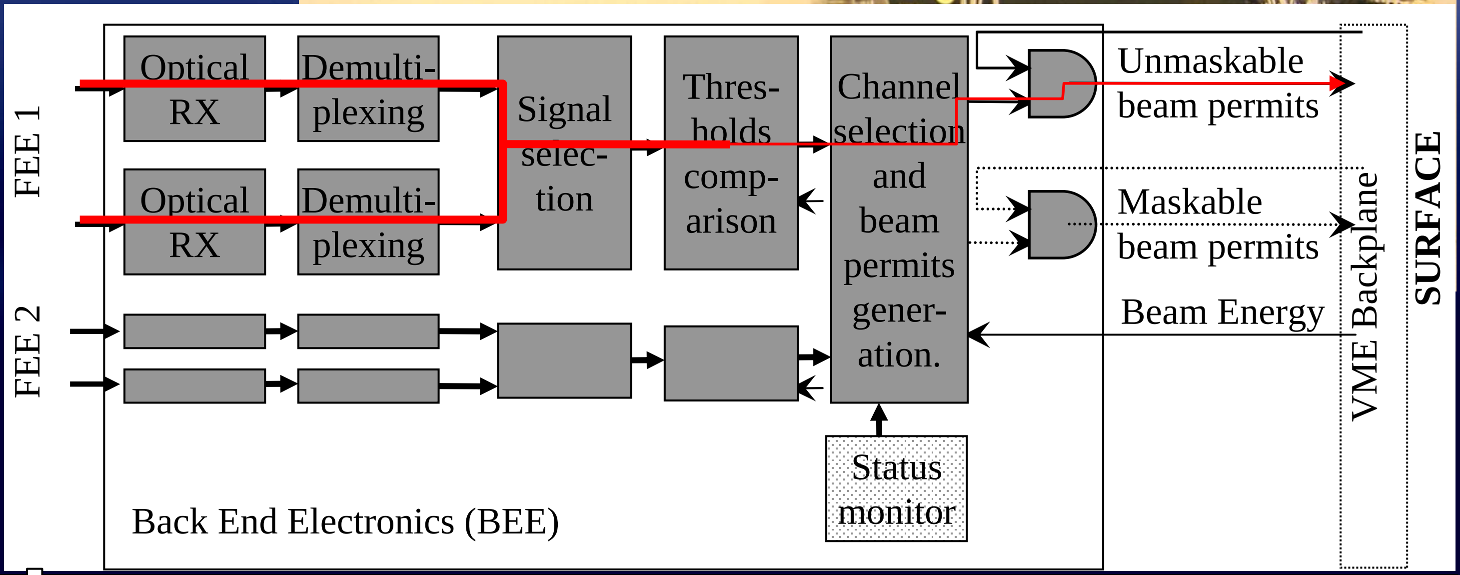




Back End Electronics

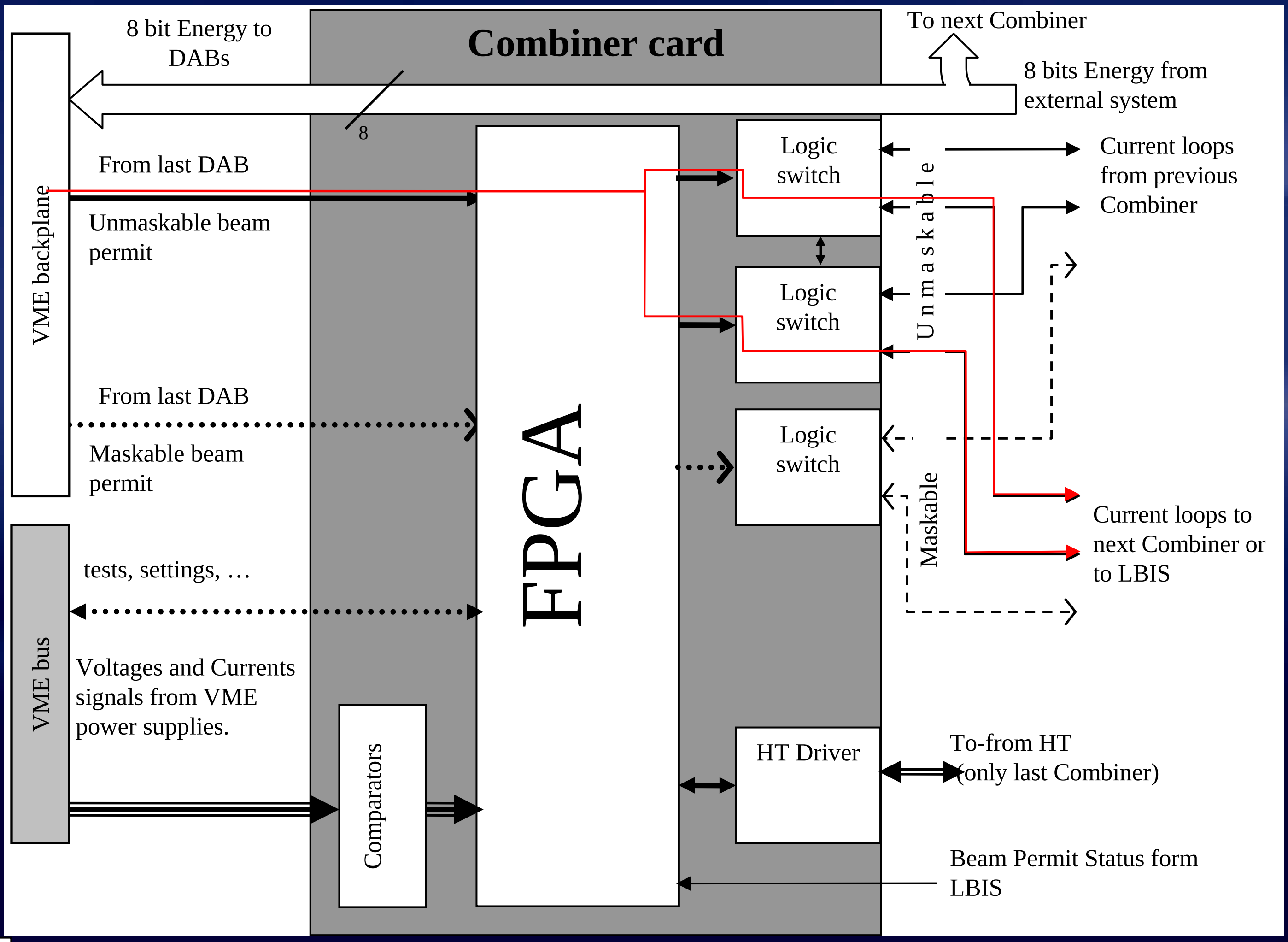
- Optical receivers in a mezzanine board.
- Data treatment in a Digital Acquisition Board. Energy input for the selection of the threshold levels.
- Beam permits connected to the backplane.





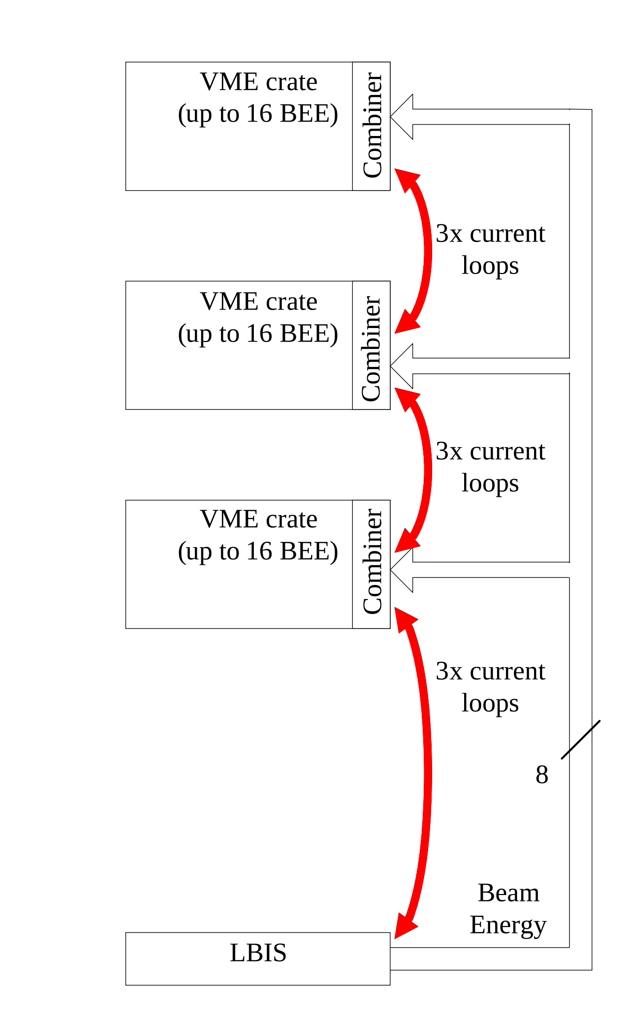
Combiner

- Reception of the beam permits and forwarding them to the LHC Beam Interlock System.
- Reception and distribution of the energy signal to the BEE cards.
- Surveillance: several testing process for the BLMS.



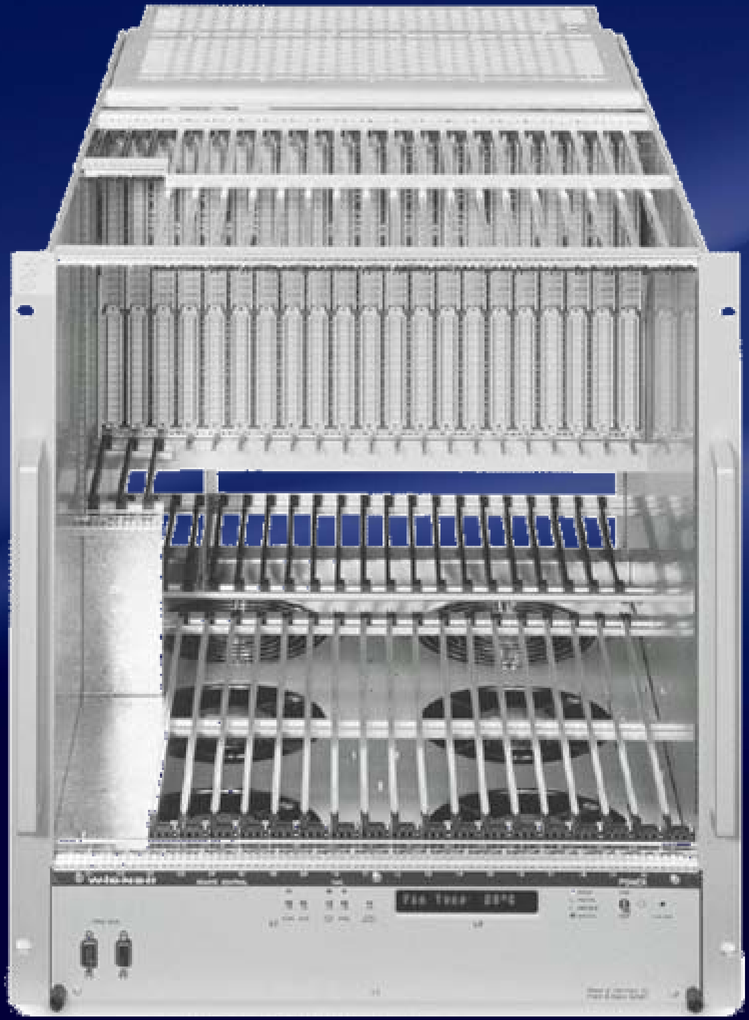
VME Crate and Rack

- Up to 16 BEE cards and a Combiner card are located in a VME crate.
- The beam permit lines of the BEE cards in a crate are daisy chained up to the Combiner card.
- 25 VME Crates in 8 racks. In each rack there will be a LHC Beam Interlock System user interface.
- The beam permit lines of the Combiner cards in a rack are daisy chained up to the LBIS user interface.
- The energy signal is provided in parallel to each combiner card.



Power Supplies

- 1926 power supplies in the tunnel.
- 25 VME power supplies at the surfaces.
- 16 High Tension (HT) power supplies at the surface for the detectors.



Outline

- Introduction.
- System Layout.
- Dependability.
- Dependable Design.
- Dependability Analysis.
- Conclusions.

Definitions 1

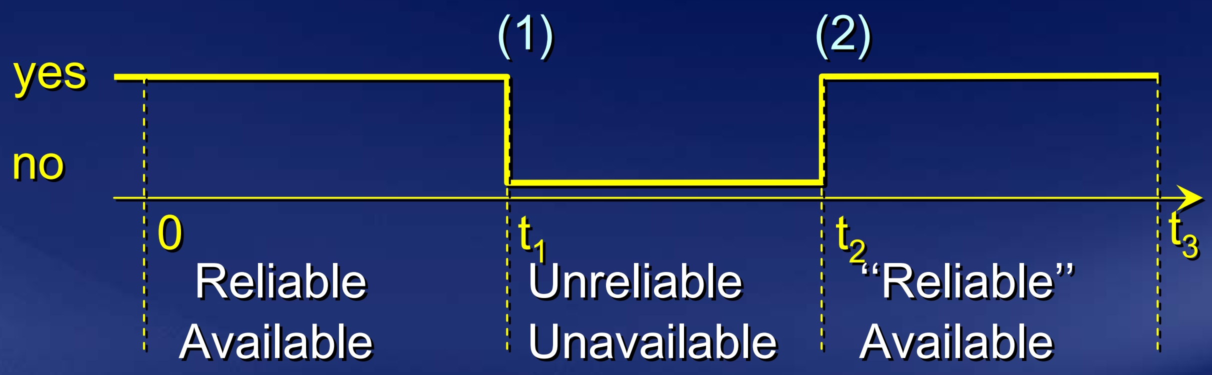
Reliability: probability of an element to operate under designated operating conditions up to a designated period of time.
Usually indicated by R(t), where t is an interval!

Maintainability: probability that a given active maintenance action, for an item under given conditions of use, can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources.
Usually indicated by G(t), where t is an interval!

Availability: is the probability of an element to operate under designated operating conditions at a designated time or cycle.
Usually indicated by A(t), where t is an instant!

Definitions 1: example

Function: run with two legs.



(1) Failure: broken leg.

(2) Reparation: recovered leg.

Notes

- If there is no reparation, reliability = availability.
- Person not reliable in the period 0 - t_3 but reliable between t_2 - t_3.

This is one case. To define the reliability, the maintainability and the availability several cases are needed.

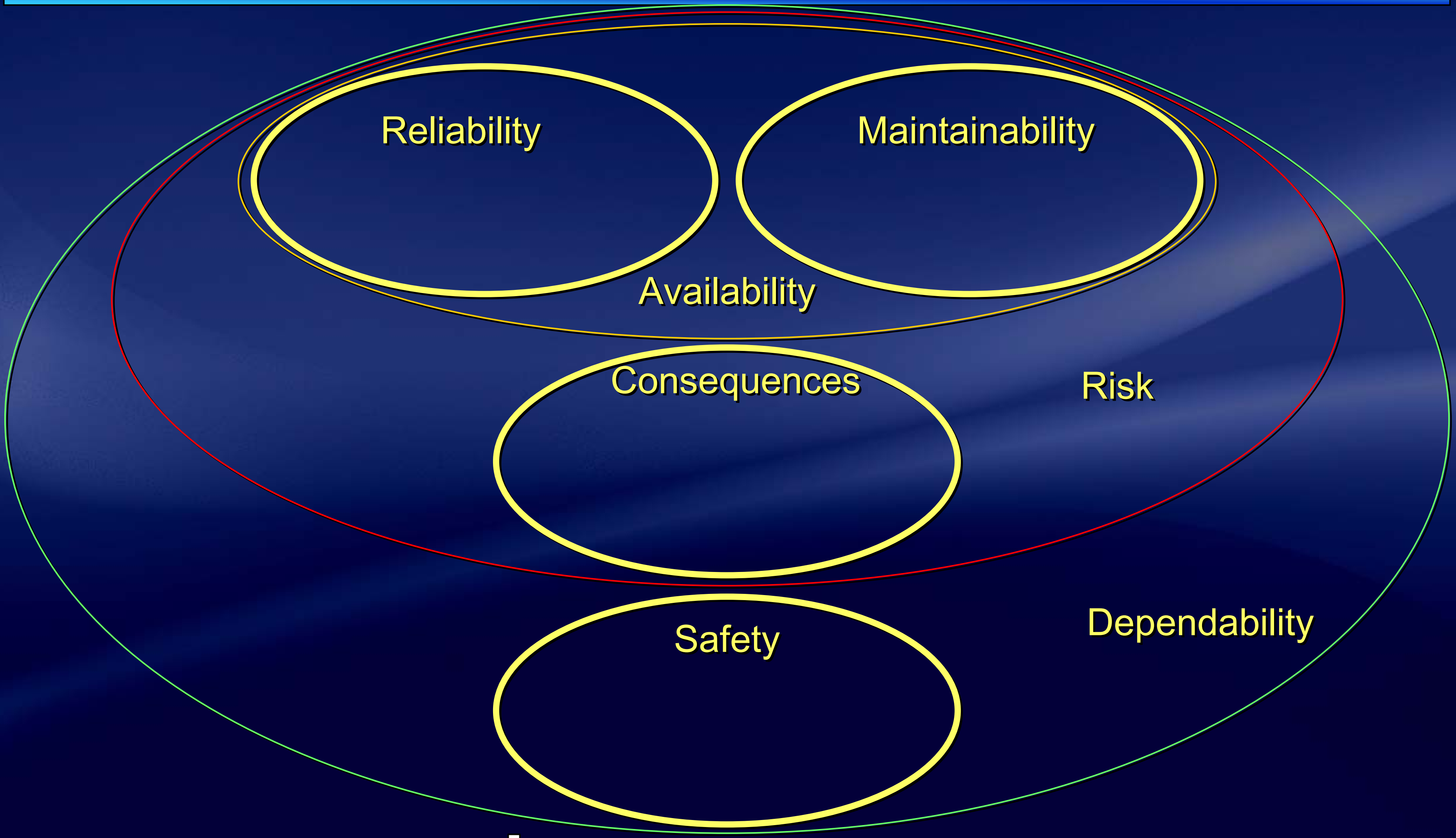
Definitions 2

Risk: Product of the probability to have a damage times the « cost » of the damage.
The availability analysis gives the damage probability, the risk analysis gives the cost of the damage.

Safety: the likelihood of an element to maintain throughout its life cycle an acceptable level of risk that may cause a major damage to the product or its environment.
Definition very vague!

Dependability: ensemble of reliability, availability, maintainability and safety.
Also called RAMS (Reliability, Availability, Mainteinabillity, Safety). It is a purist term. Reliability is the term improperly used to indicate “dependability”.

Dependability



Mathematics: reliability

$$\begin{cases} R(t) + F(t) = 1 \\ 0 \le R(t) \le 1 \end{cases}$$

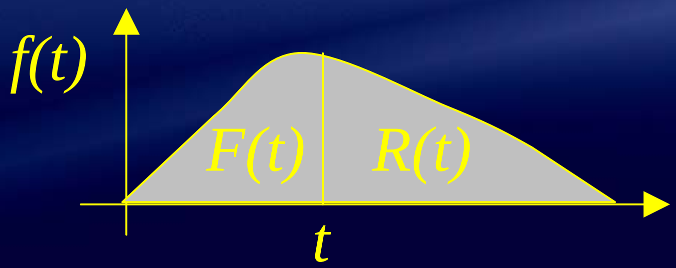
Reliability R(t) and Unreliability F(t) are probabilities.

$$\begin{cases} F(0) = 0 \\ F(\infty) = 1 \end{cases}$$

The element works at the beginning and it will fail.

$$f(t) \equiv \frac{dF(t)}{dt}$$

Failure density f(t): f(t)dt is the probability that an element fails in the period between t and t+dt given that the component was working at time zero.



$$r(t) \equiv \frac{f(t)}{R(t)} = \frac{f(t)}{1 - F(t)}$$

Hazard rate r(t): r(t)dt is the probability that an element fails in the period between t and t+dt given that it survived up to time t and it was working at time zero.

Mathematics: example F

r(t)

$$r(t) = \frac{f(t)}{1 - \int_0^t f(u)\,du}$$

$$r(t) = \frac{dF(t)}{dt} \cdot \frac{1}{1 - F(t)}$$

$$f(t) = r(t)\, e^{-\int_0^t r(u)\,du}$$

$$F(t) = 1 - e^{-\int_0^t r(u)\,du}$$

f(t)

F(t)

$$f(t) = \frac{dF(t)}{dt}$$

$$F(t) = \int_0^t f(u)\,du$$

Example 1: Exponential

$$r(t) = const = \lambda$$

$$F(t) = 1\text{-}e^{-\lambda t}$$

$$f(t) = \lambda e^{-\lambda t}$$

Example 2: Weibull

$$F(t) = 1 - e^{-\left(\frac{t-\gamma}{\sigma}\right)^{\beta}}$$

$$f(t) = \frac{\beta}{\sigma}\left(\frac{t-\gamma}{\sigma}\right)^{\beta-1} e^{-\left(\frac{t-\gamma}{\sigma}\right)^{\beta}}$$

$$r(t) = \frac{\beta}{\sigma}\left(\frac{t-\gamma}{\sigma}\right)^{\beta-1}$$

Mathematics: maintainability

$$\begin{cases} G(t) + (1 - G(t)) = 1 \\ 0 \le G(t) \le 1 \end{cases}$$

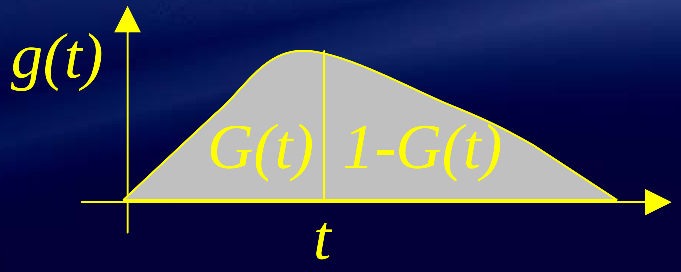
Maintainability G(t) is a probability.
"Unmaintainability" does not exist.

$$\begin{cases} G(0) = 0 \\ G(\infty) = 1 \end{cases}$$

The element does not work at time 0 and it will be repaired in the indefinite future.

$$g(t) \equiv \frac{dG(t)}{dt}$$

Repair density g(t): g(t)dt is the probability that a element repair is completed in the period between t and t+dt given that the component was failed at time zero.



$$m(t) \equiv \frac{g(t)}{1 - G(t)}$$

Repair rate m(t): m(t)dt is the probability that an element is repaired in the period between t and t+dt given that it has failed up to time t and it was failed at time zero.

Mathematics: availability

$$A(t)+Q(t)=1$$
$$0 \le A(t) \le 1$$

$$\begin{cases} Q(0)=0 \\ Q(\infty) \le 1 \end{cases}$$

Availability A(t) and Unavailability Q(t) are probabilities. The element works at time 0 and it has, in the long period, a steady probability to work.

$$\begin{cases} w(t) \equiv f(t) + \int_0^t f(t-u)v(u)du \\ v(t) \equiv \int_0^t g(t-u)w(u)du \end{cases}$$

Unconditional failure [repair] intensity w(t) [v(t)]: the probability that a component fails [is repaired] per unit time at time t, given that it was as good as new at time zero.

$$Q(t) \equiv \int_0^t [w(u)-v(u)]du$$

Unavailability at time 0 is the difference between the expected number of failures and the expected number of reparations in the interval 0-t.

$$\begin{cases} \lambda(t) \equiv \dfrac{w(t)}{A(t)} \\ \mu(t) \equiv \dfrac{v(t)}{Q(t)} \end{cases}$$

Conditional failure [repair] intensity λ(t) [μ(t)]: defined as the probability that a component fails [is repaired] per unit time at time t, given that it was as good as new at time zero and it is working [is failed] at time t.

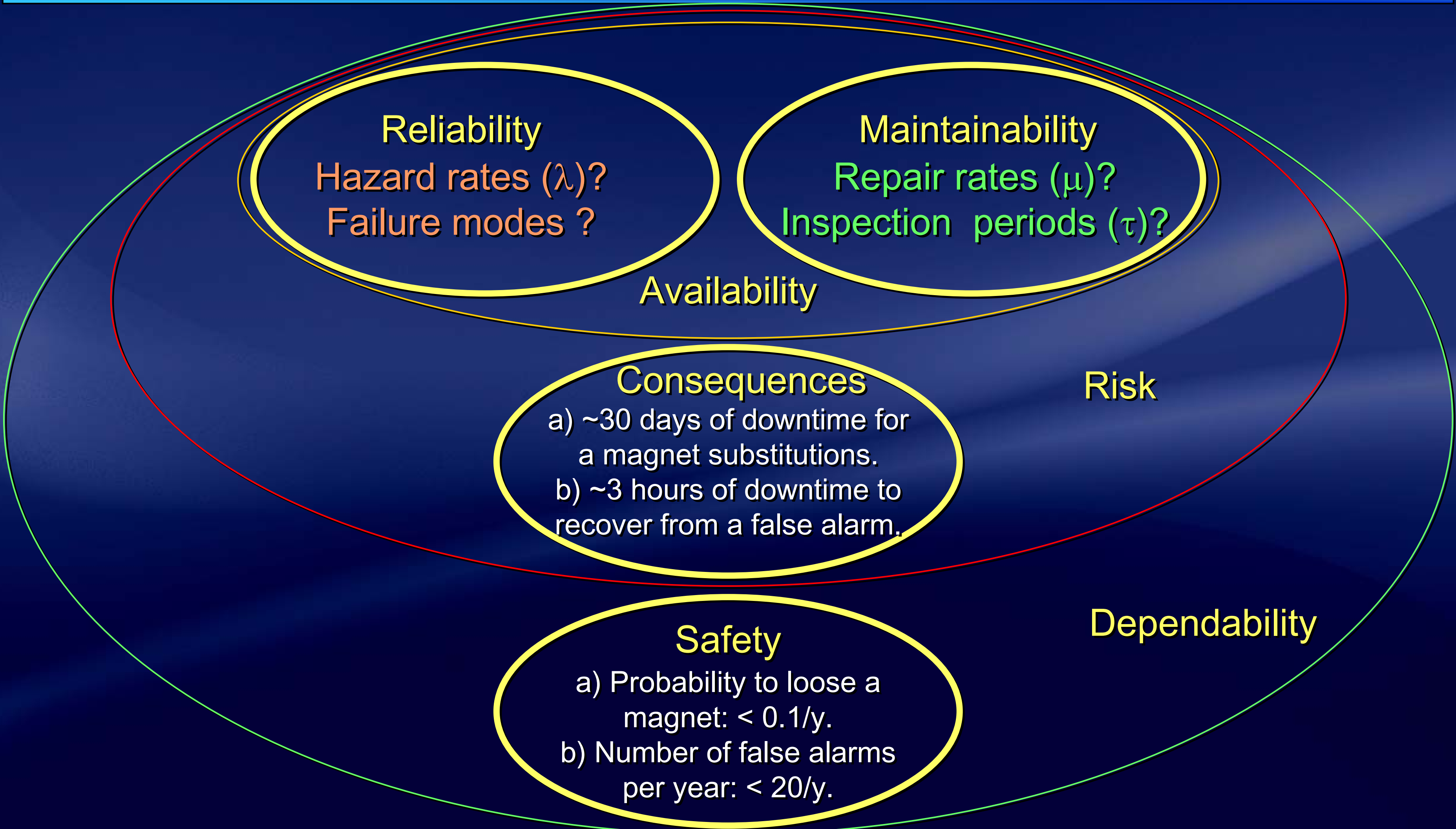
Mathematics: summary

Reliability	Maintainability	Availability
Reliability and Unreliability $R(t)+F(t)=1$		Availability and Unavailability $A(t)+Q(t)=1$
$\begin{cases}F(0)=0\\F(\infty)=1\end{cases}$	$\begin{cases}G(0)=0\\G(\infty)=1\end{cases}$	$\begin{cases}Q(0)=0\\Q(\infty)\le 1\end{cases}$
Failure density $f(t)\equiv\frac{dF(t)}{dt}$	Repair density $g(t)\equiv\frac{dG(t)}{dt}$	Unconditional failure and repair intensities $\begin{cases}w(t)\equiv f(t)+\int_0^t f(t-u)v(u)du\\v(t)\equiv\int_0^t g(t-u)w(u)du\end{cases}$
$F(t)=\int_0^t f(u)du$	$G(t)=\int_0^t g(u)du$	$Q(t)=\int_0^t [w(u)-v(u)]du$
Hazard rate $r(t)\equiv\frac{f(t)}{1-F(t)}$	Repair rate $m(t)\equiv\frac{g(t)}{1-G(t)}$	Conditional failure and repair intensities $\begin{cases}\lambda(t)\equiv\frac{w(t)}{1-Q(t)}\\\mu(t)\equiv\frac{v(t)}{1-A(t)}\end{cases}$
Mean Time To Failure $MTTF\equiv\int_0^\infty t\cdot f(t)dt$	Mean Time To Repair $MTTR\equiv\int_0^\infty t\cdot g(t)dt$	Mean Time Between Failures $MTBF\equiv\int_0^\infty t\cdot[f(t)+g(t)]dt$

Outline

- Introduction.
- System Layout.
- Dependability.
- Dependable Design.
- Dependability Analysis.
- Conclusions.

Dependability



BLMS Dependability

General Features:

- Hazard rates of the components:

  "How often does a component fail?"

- Failure modes of the components:

  "How does a component fail?"

- Fail safe design.

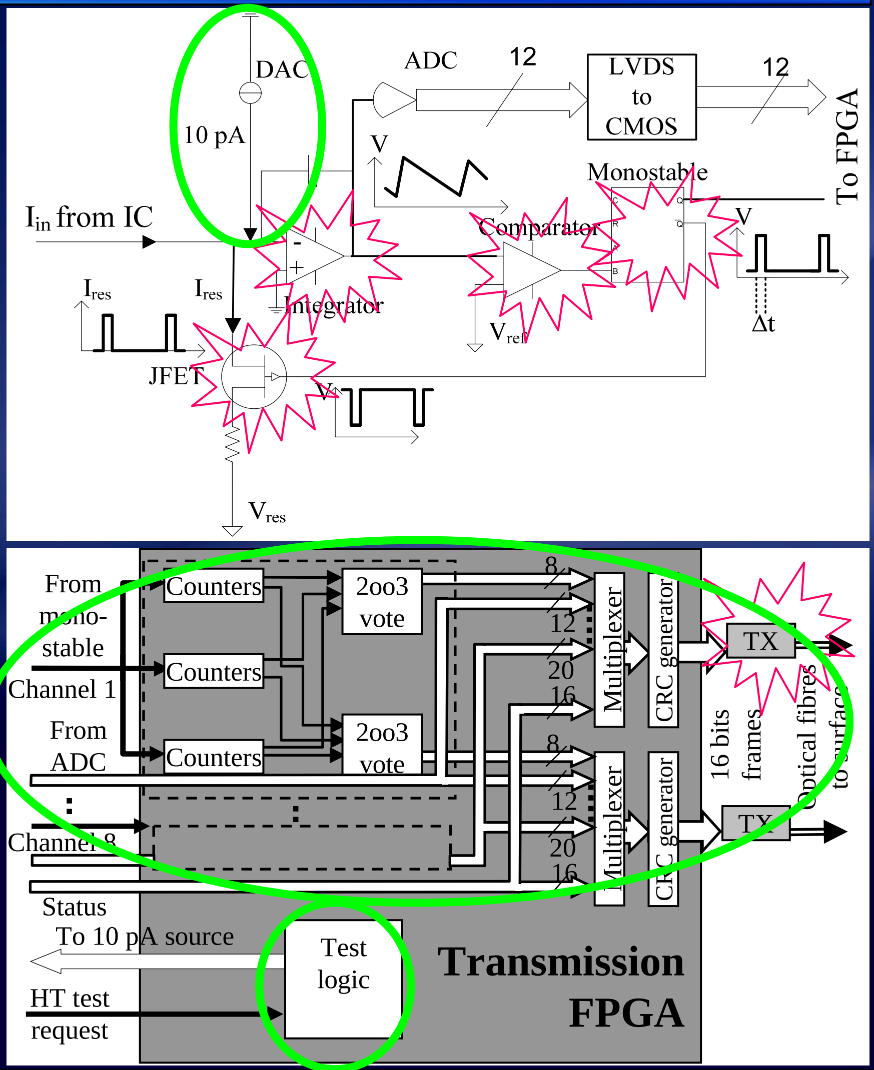
  The most probable failure of the component does not generate the worst consequence (= risk to damage a magnet).

FEE Dependability

- Irradiation tests on the analogue components and LASERs to investigate hazard rate variation. Induced error negligible.

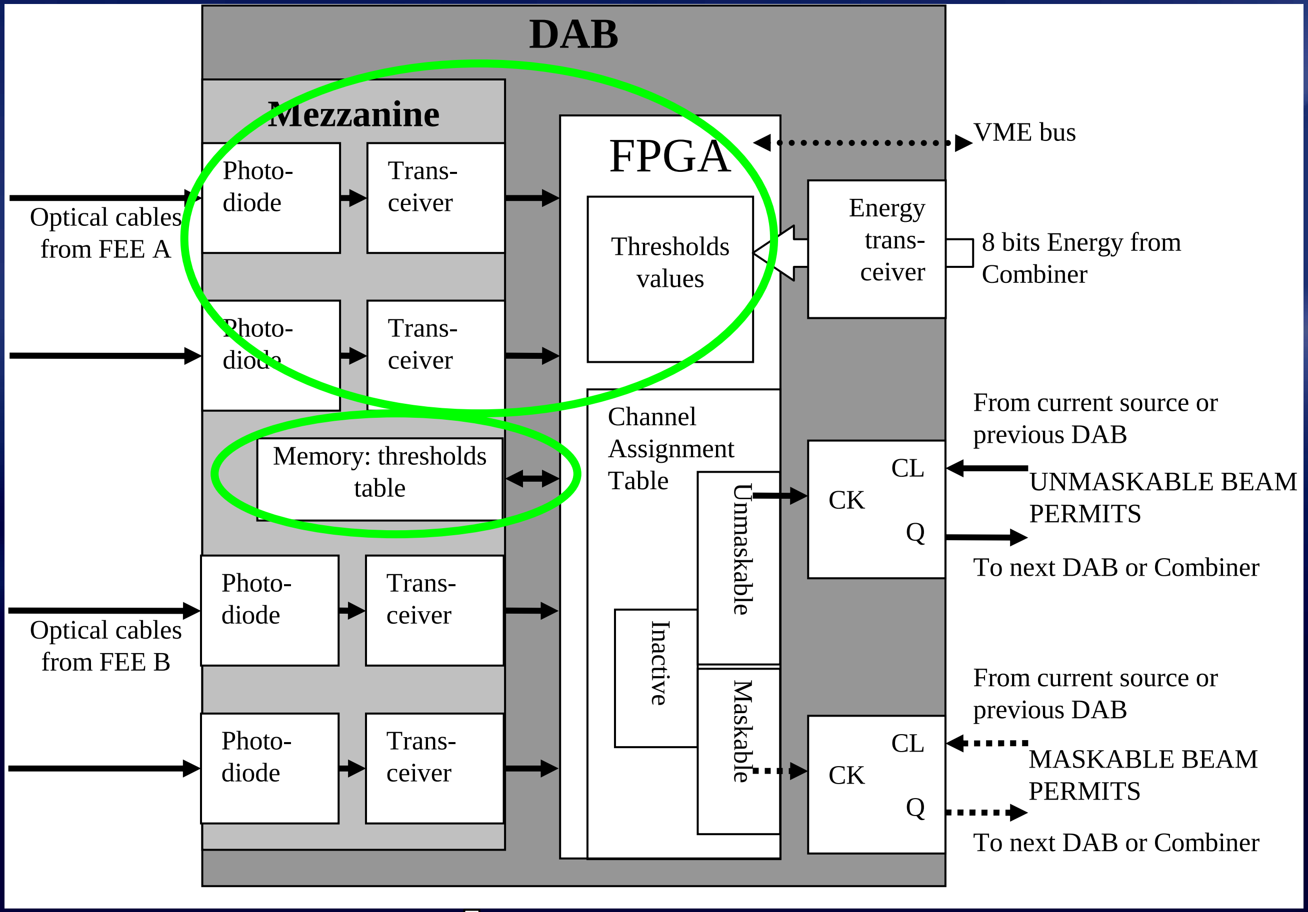
- Definition of the 10pA test and of the HT test to check the channel functionalities.

- Doubling of the optical lines and two-out-of-three (2oo3) redundancy in the FPGA.



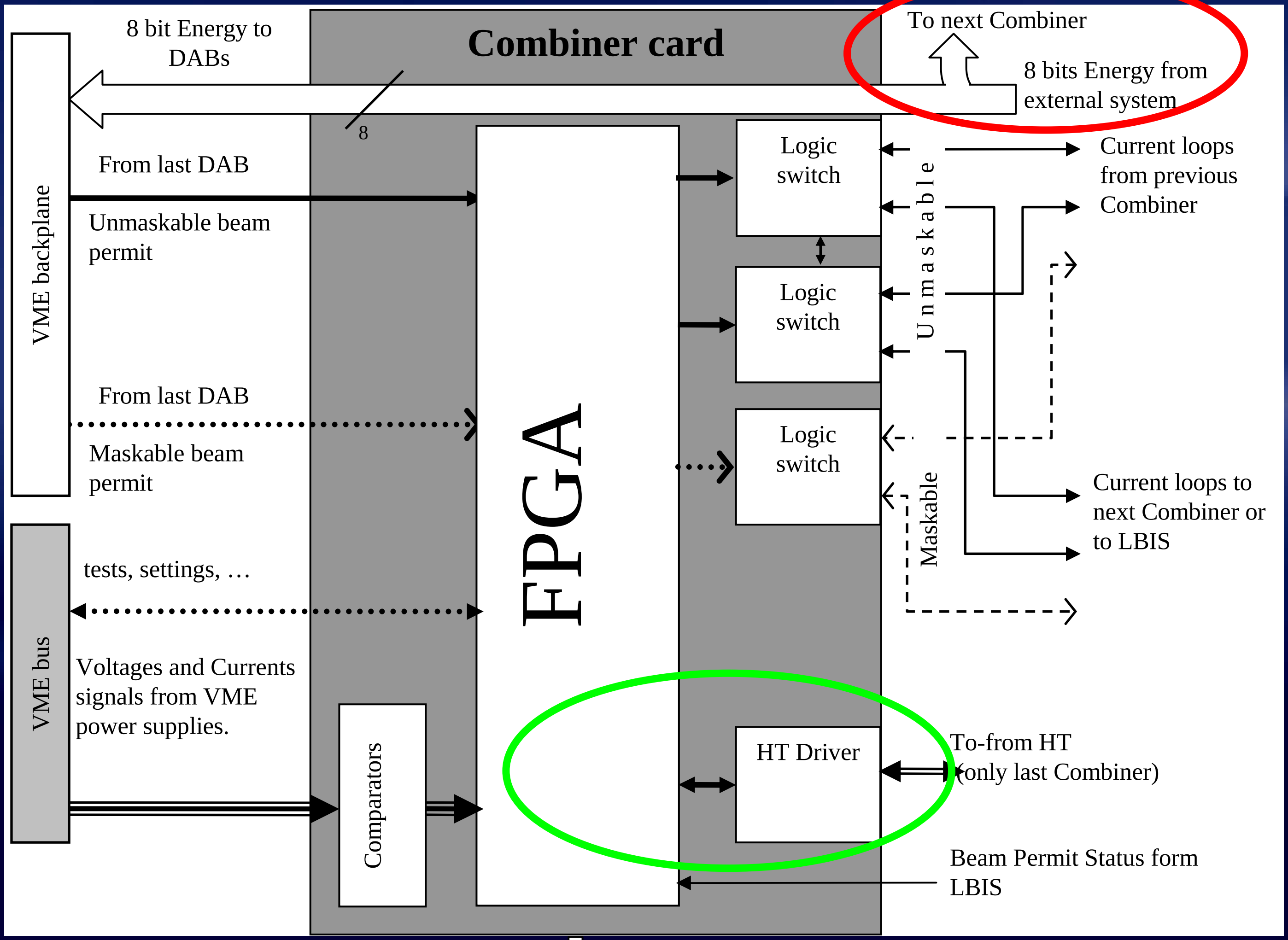
BEE Dependability

- Definition of the tests to check the integrity of the data.
- Definition of the thresholds windows to minimize the evaluation error.



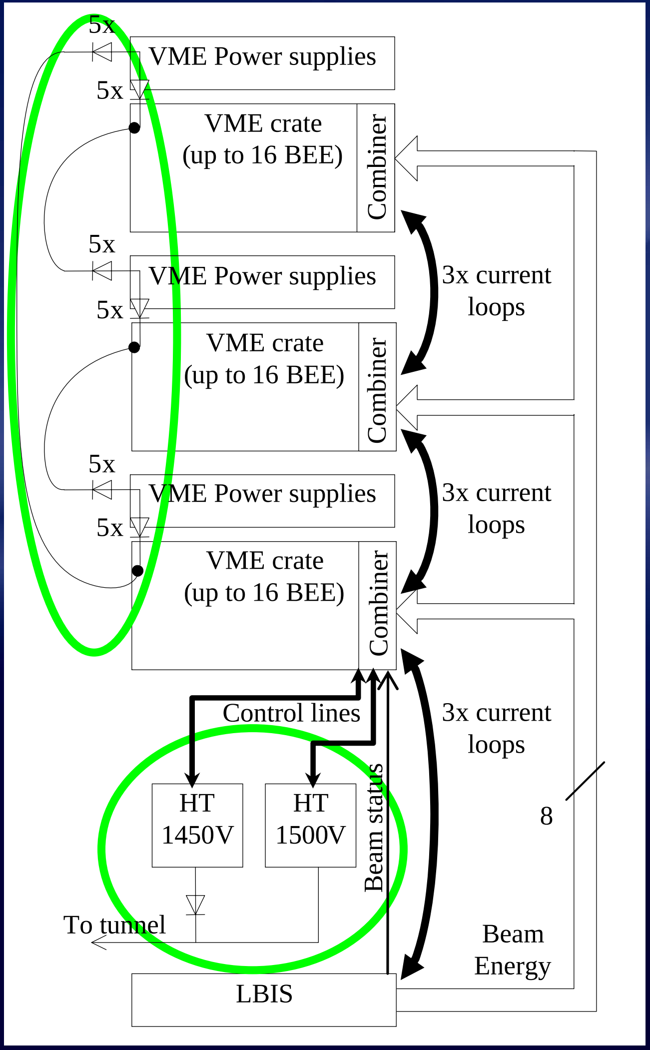
Combiner Dependability

- Definition of the tests to check the whole signal chain.
- Definition of the criticalities of the energy signal.



Power Supplies Dependability

- 2oo3 redundancy of the VME power supplies.
- Redundant High Tension power supplies.



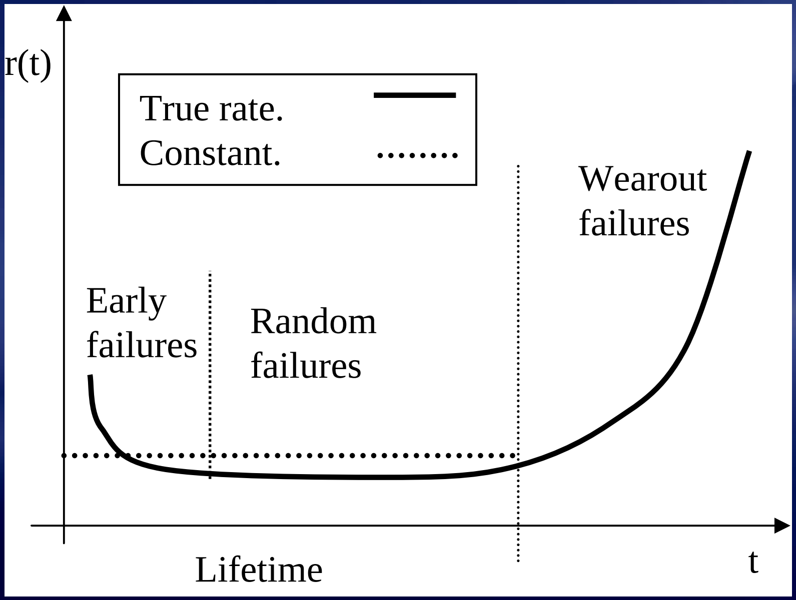
Outline

- Introduction.
- System Layout.
- Dependability.
- Dependable Design.
- Dependability Analysis.
- Conclusions.

BLMS Predictions

The Prediction is the estimation of the hazard rate of the components.

Hazard rates λ are assumed to be constant. After a short initial period, this assumption overestimates the failure rates.



Rates collected mainly from the suppliers, then from historical data, and finally from the MIL-HDBK 217F.

Predictions Uncertainties

Supplier	λ of the power supply in the arc: $2\cdot10^{-9}$/h.	λ of similar power supply in the tunnel: $2\cdot10^{-6}$/h.	Uncertainty is given by the unknown supplier test procedures.
Historical	216 detectors had no failure over 20 years (of 4800 hours).	Assumption: λ is constant. $\lambda < 4\cdot10^{-8}$/h (60% of CL) $1\cdot10^{-8}/h < \lambda < 8\cdot10^{-8}$/h (95%)	Uncertainty is given by the lack of failures.
Military handbook	λ has been evaluated by tests of electronics 20 years ago.	New electronics evaluation (IEC standard) lower λ.	MIL to be comparable with other LHC studies and to be conservative.

The Dependability Analysis will be performed on the central values.

The effect of the λ uncertainties on the dependability results will be estimated by the Sensitivity Analysis.

BLMS FMECA

The Failure Modes, Effects and Criticalities Analysis enumerates the failure modes of the components and studies the propagation of the failure effects to the system level.

Apportionment from FMECA

Failure Mode's hazard rate of the component → $\lambda_i^{FM} = \alpha_i^{FM} \cdot \lambda_i$ ← Component's Hazard rate from prediction

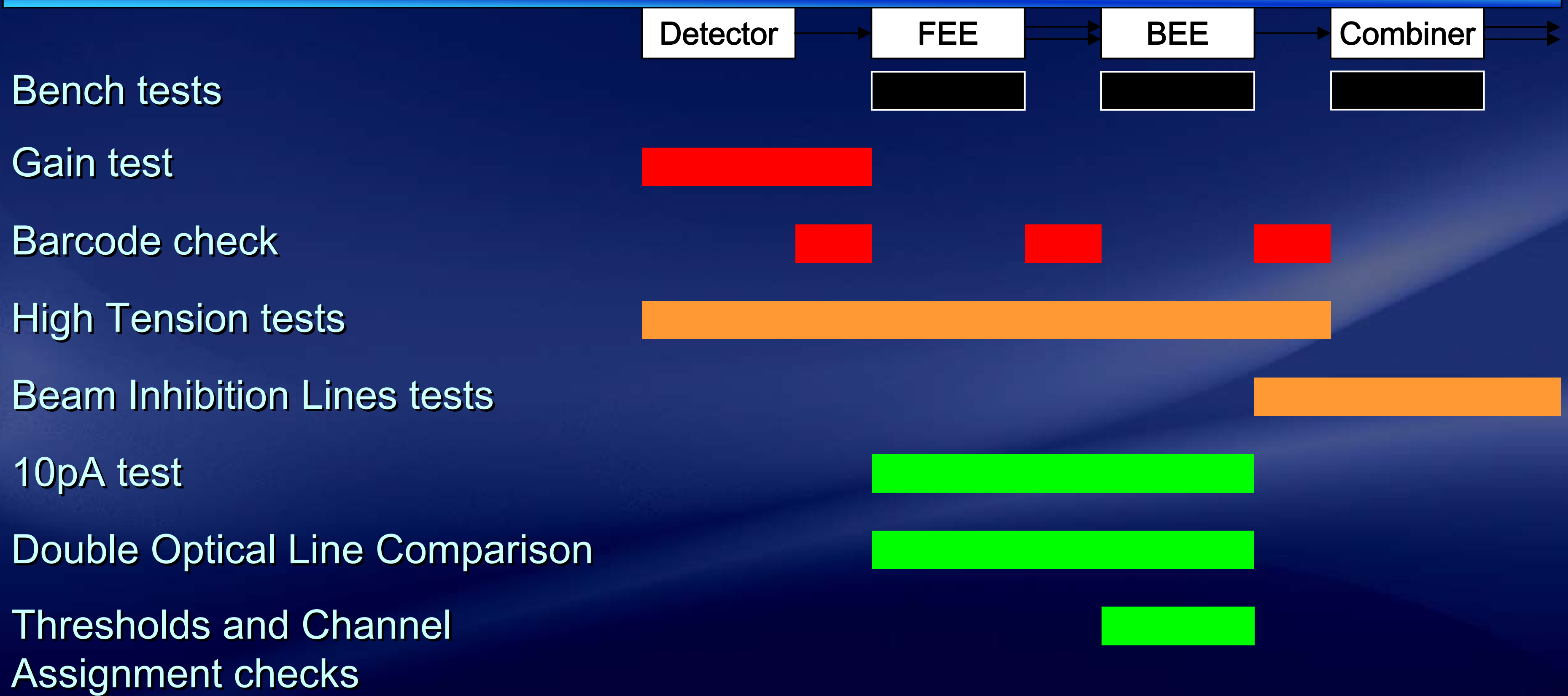
Almost 160 Failure Modes have been defined for the BLMS using the FMD-97 standard.

Conservative hypothesis: bench tests do not eliminate the construction failure modes.

Three Ends Effects:

1. Damage Risk: probability not to be ready in case of dangerous loss.
2. False Alarm: probability to generate a false alarm.
3. Warning: probability to generate a maintenance request following a failure of a redundant component.

BLMS Testing Processes



Inspection phases: ■ Check-in, ■ Maintenance, ■ Before every fill, ■ With the beam

The failure probability decrease with the decrease of the inspection period.

Fault Tree Analysis

The probability to have an Failure Mode A, Pr{A}, is calculated per each Failure Modes of the FMECA, given the hazard rate, the repair rate and the inspection period .

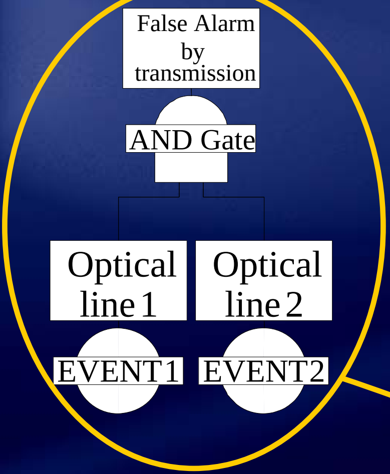
The Fault Tree Analysis is based on the combinatorial statistics. Some Basic Gates (= combination laws) are:

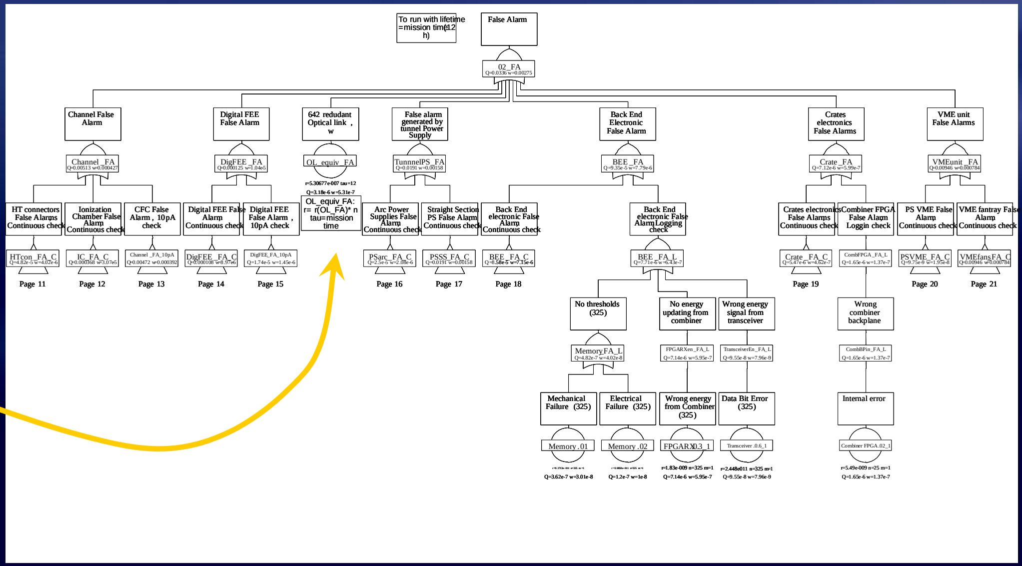
1. Two events, A & B, are statistically independent if and only if:

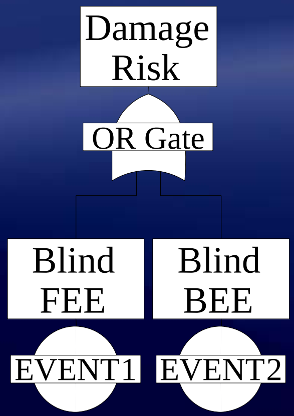
$Pr\{AB\} = Pr\{A\} \times Pr\{B\}$

2. The probability that at least one of two events A and B occurs is:

$Pr\{A + B\} = Pr\{A\} + Pr\{B\} – Pr\{AB\}$







Several other combination are available: XOR, Voting, NOT,…

Fault Trees Results

The probabilities to fail (unavailability) for the BLMS have been calculated.

Per each End Effects, the major contributors to such probabilities have been pointed out too.

	Consequences per year	Weakest components	Notes
Damage Risk	$5 \cdot 10^{-4}$ (100 dangerous losses)	Detector (88%) Analogue electronics (11%)	Detector λ likely overestimated (60% CL of no failure after 1.5 10^6 h).
False Alarm	13 ± 4	Tunnel power supplies (57%) VME fans (28%)	Hazard rate of the tunnel power supplies likely underestimated (see sensitivity example).
Warning	35 ± 6	Optical line (98%) VME PS (1%)	LASER hazard rate likely overestimated by MIL.

Sensitivity Analysis

The Sensitivity Analysis provides the impact of the variation of either a parameter or a system configuration on the unavailabilities of the system.

The rare event approach provides a good numeric approximation and highlights the dependencies of the variation.

Quantity of the component

End Effect's hazard rate of the component checked by the test t

End Effect's unavailability →

$$Q^{EE} = \sum_{i,t}^{OR} N_i \cdot {}^t\lambda_i^{EE} \cdot {}^t t$$

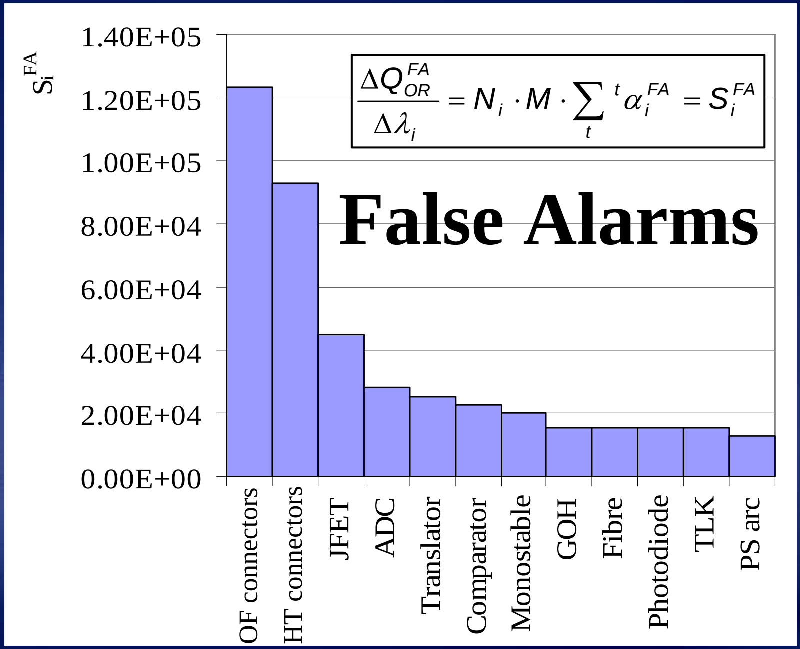
$${}^t\lambda_i^{EE} = {}^t\alpha_i^{EE} \cdot \lambda_i$$

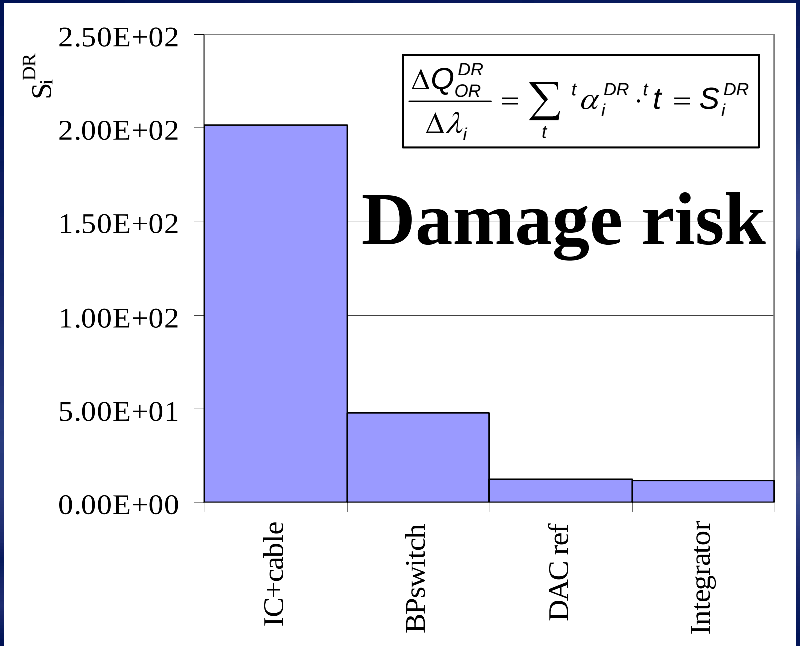
Inspection period of the test t

⇓

$$\Delta Q^{EE} = \sum_{i,t} \Delta N_i \cdot {}^t\lambda_i^{EE} \cdot {}^t t + \sum_{i,t} N_i \cdot \Delta {}^t\lambda_i^{EE} \cdot {}^t t + \sum_{i,t} N_i \cdot {}^t\lambda_i^{EE} \cdot \Delta {}^t t$$

Most Sensible Component





Example 1: Effect of the variation of the λ of the Power Supplies in the arc (PSarc).

λ PS in the arc $2 \cdot 10^{-9}$/h. If similar to the PS in the straight section ($2 \cdot 10^{-6}$/h),

$\Delta\lambda = \sim 2 \cdot 10^{-6}$/h.

$\Delta\lambda$ multiplied by the sensitivity factor ($1.3 \cdot 10^4$ h) reads:

$\Delta Q = 2.5\ 10^{-2}$ (from $Q = 3.4\ 10^{-2}$).

For the 400 missions, 10 extra False Alarms per year: number of False Alarms would be 23 ± 5.

Sensitivity: Considerations

Redefinition of the hazard rates after one year of LHC operation.

Estimated λ for comparator: $2 \cdot 10^{-7}$/h

For 1932 comparators, after one LHC year: 1932 x 4800h = $9 \cdot 10^6$ equivalent working hours.

Number of failures	λ 60% CL
0	1·10-7/h
1	2·10-7/h
2	3·10-7/h

The Sensitivity Analysis allows an estimation of the variation of the system dependability given by the re-evaluations of the component parameters.

Outline

- Introduction.
- System Layout.
- Dependability.
- Dependable Design.
- Dependability Analysis.
- Conclusions.

Conclusions

The average probability that in an year a channel will miss a dangerous loss is $5 \cdot 10^{-4}$ (less than the tolerated 0.1), assuming 100 dangerous losses per year.

The maximum number of expected false alarms is 13 ± 4 per year (less than the tolerated 20).

The expected maintenance actions (false alarms plus warnings) are 49 ± 7 per year, ~ 1 every 4 days.

Due to the conservative hypothesis, all the figures are expected to be overestimated.

Estimation of the actual hazard rates and possible corrective actions during the first years of commissioning are significant.

Questions?

Thank you for the attention.