# Risk assessment in the next Injector Complex

ANDREA APOLLONIO
TE-MPE-PE

MPP-MEETING 31/08/2012

# Outline

- Motivation
- Theoretical Approach
- Failure Catalogue
- Website
- Montecarlo Simulations for Availability, MTBF, MTTR, MDT
- Future Developments

# Motivation

1. The idea of realizing a Failure Catalogue for the LHC is very challenging: testing the adopted methodology to derive the failure catalogue on a smaller machine seems a good way to verify if this approach can be easily extended to bigger ones.

2. Having a complete Failure Catalogue helps in designing Machine Protection Systems (BIS, SIS) and possibly discover its ‘weak points’.

# Definitions (1/2)

**Accident**: An undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss.

**Incident**: An event that involves no loss (or only minor loss) but with the potential for loss under different circumstances.

**Hazard**: A state or set of conditions that, together with other (worst case) conditions in the environment, will lead to an accident (loss event).

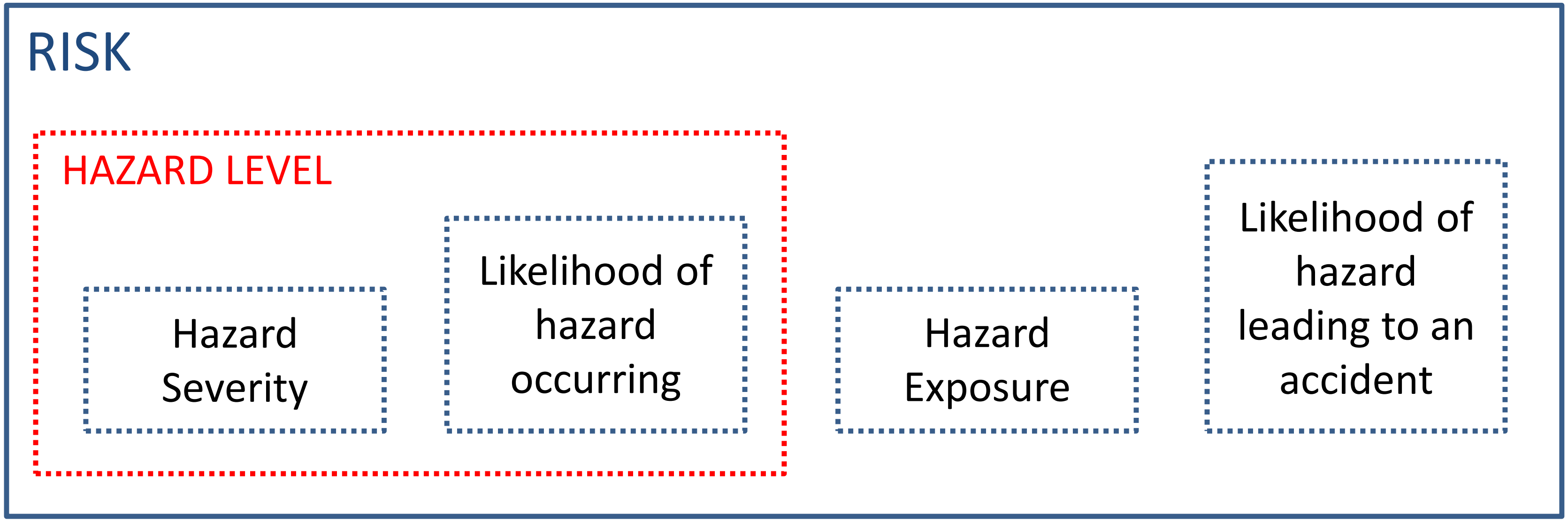
**Safety**: Freedom from accidents or losses.

Examples of so considered '*losses*': human injury, property damage, environmental pollution (damage), mission loss, etc.

# Definitions (2/2)

**Hazard Level**: A combination of severity (worst potential damage in case of an accident) and likelihood of occurrence of the hazard.

**Risk**: The hazard level combined with the likelihood of the hazard leading to an accident plus exposure (or duration) of the hazard.



# STPA: What is it?

**S**ystem – **T**heoretic **P**rocess **A**nalysis (Hazard Analysis):

- Investigating an accident before it occurs.

- Goal:

– Identify potential causes of accidents (scenarios that can lead to losses)
– So can be eliminated or controlled in design or operations before losses occur.

- Used for:

– Developing requirements and design constraints
– Validating requirements and design for safety
– Preparing operational procedures and instructions
– Test planning and evaluation
– Management planning

# Steps in STPA

1. Define accidents

2. Define system hazards associated with accidents

3. Translate system hazards into high-level safety requirements (constraints)

4. Construct high-level control structure including
   – Responsibilities of components
   – Preliminary process model

5. Refine high-level safety constraints into detailed safety requirements on components and scenarios for losses

6. Use results to create or improve system design

# STPA applied to Linac4 (1/4)

**ACCIDENTS**:

- Lack of beam for other accelerators (A1)
- Damage to equipment (A2)
- Release of radioactive material (A3)
- Injuries to staff members (A4)

Relevant Aspects for Machine Protection

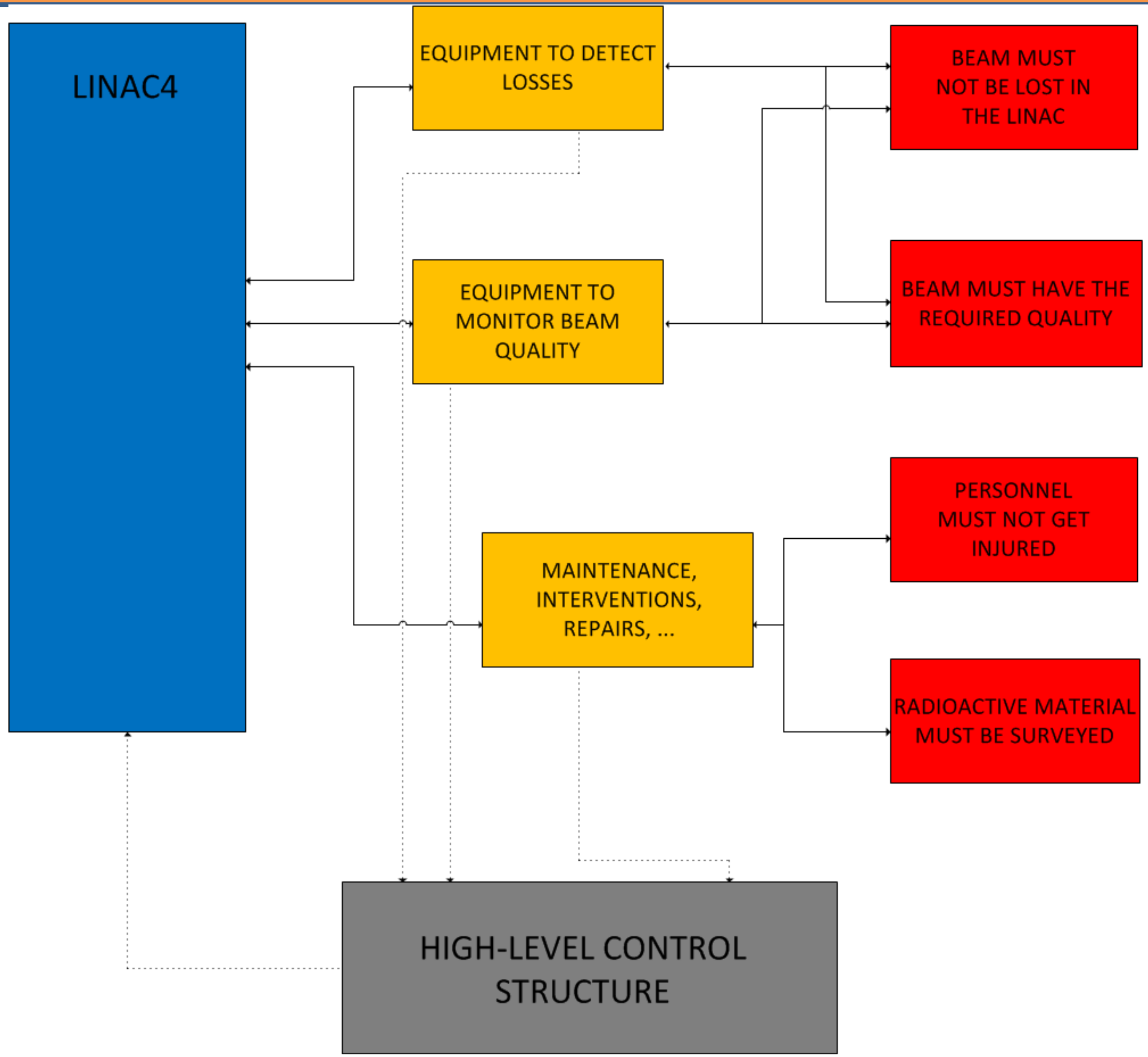
**HAZARDS**:

- The beam not sent to the TL (H1) [A1, A2]
- The beam lost before reaching the TL (H2) [A1, A2]
- The beam doesn't have the required quality for injection (H3) [A1]
- Radioactive contamination of staff members (H4) [A3, A4]
- Radioactive leaks in the environment (H5) [A3]

**HIGH-LEVEL REQUIREMENTS**:

- Beam must not be lost in the Linac (R1) [H1, H2]
- Beam must have the required quality (R2) [H3]
- Radioactive material must surveyed (R3) [H4, H5]
- Linac Availability must be as high as possible (R4) [H1, H2 , H3]

# STPA applied to Linac4 (2/4)



# STPA applied to Linac4 (3/4)

**1st ORDER REFINEMENT**:

- Beam must have the correct structure for injection (FO1) [R1, R2]
- All components must be ready for operation (FO2) [R1, R2 , R4]
- Losses must not be observed in the Linac (FO3) [R1, R2]
- Radiation levels must be monitored by specialized teams (FO7) [R3]

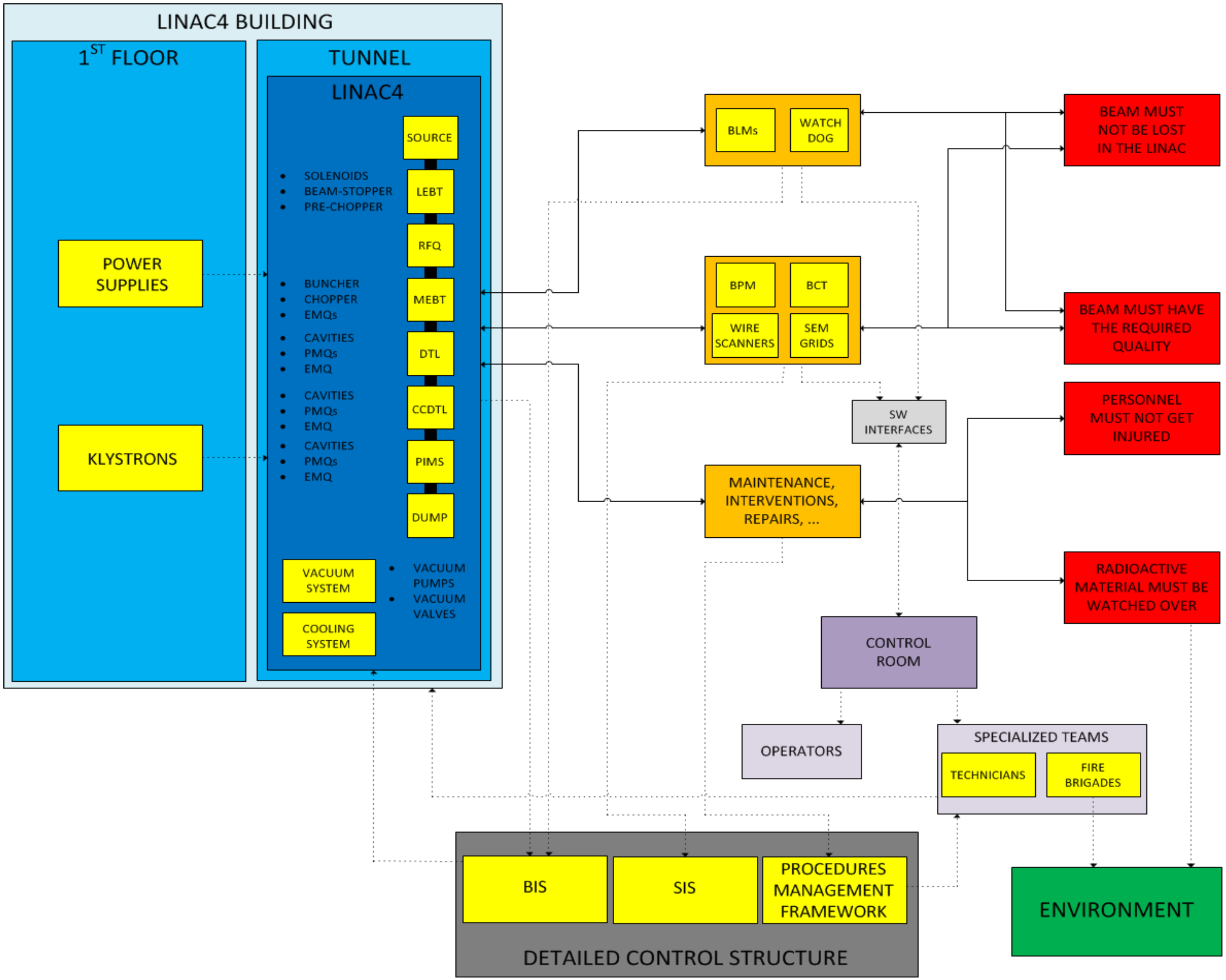
**2nd ORDER REFINEMENT**:

- Pre-Chopper, Buncher, Chopper, Debunching Cavity must work correctly (SO1) [FO1, FO2 , FO3]
- Power supplies and Machine Protection Systems must work correctly (SO2) [FO2, FO3]
- Losses must be detected and handled by dedicated systems (SO3) [FO3]
- The status of the components must be surveyed by operators (SO4) [FO2]
- Communication tools must be in place among different teams (SO5) [FO4, FO5, FO6]
- Records of components history and issues must be kept (SO7) [FO5]
- Fire brigades must be alerted in case of problems (SO8) [FO6, FO7]

**3rd ORDER REFINEMENT**:

…

# STPA applied to Linac4 (4/4)



# STPA applied to Linac4: Failure Catalogue

Going always in deeper detail for every requirement of the system leads to the definition of the *FAILURE MODES* of the system/components.

The *RISK* associated to every failure mode has to be evaluated, according to the definition, based on the *FREQUENCY* of the failure and its *IMPACT*.

A *FAILURE CATALOGUE* to collect this data has been realized.

A *WEBSITE* has been developed to hold the failure catalogue and all the related studies and is currently updated as the design of Linac4 components proceeds.

https://espace.cern.ch/linac4-and-machine-protection/SitePages/Home.aspx

NOTE: An ATS note on the Failure Studies related to Linac4 will be released in the coming weeks.

# STPA applied to Linac4: Failure Catalogue

The *Failure Catalogue* has been realized in collaboration with the experts from the different domains (Optics, Vacuum, Machine Protection, RF, …).

Other *Failure Modes* might come up or still need to be considered.

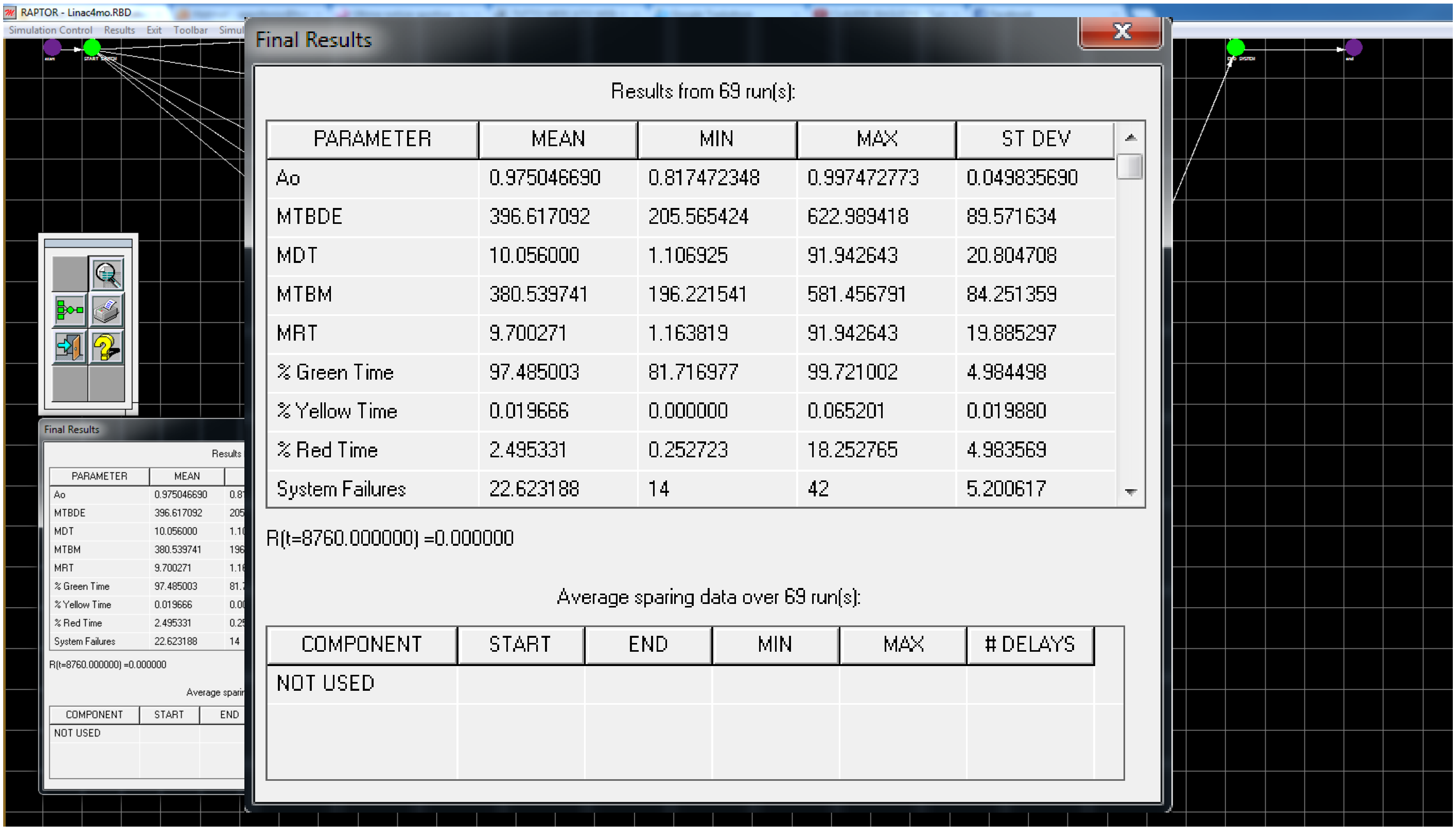
The *Frequency* of the different failures as well as the possible associated *Down-Time* and available *Spare Components* are parameters that only experts know or can derive.

A closer collaboration to cross-check the information contained in the *Website* and have estimates for these parameters is required and shouldn't be too time-consuming.

The *Risk Assessment* will be possible as the parameters will be available.

# Montecarlo Simulations: approach

One important application of the failure catalogue could be the study of the Machine Availability, MTBF, MDT through Montecarlo Simulations (RAPTOR4).



Final Results

Results from 69 run(s):

| PARAMETER | MEAN | MIN | MAX | ST DEV |
|---|---|---|---|---|
| Ao | 0.975046690 | 0.817472348 | 0.997472773 | 0.049835690 |
| MTBDE | 396.617092 | 205.565424 | 622.989418 | 89.571634 |
| MDT | 10.056000 | 1.106925 | 91.942643 | 20.804708 |
| MTBM | 380.539741 | 196.221541 | 581.456791 | 84.251359 |
| MRT | 9.700271 | 1.163819 | 91.942643 | 19.885297 |
| % Green Time | 97.485003 | 81.716977 | 99.721002 | 4.984498 |
| % Yellow Time | 0.019666 | 0.000000 | 0.065201 | 0.019880 |
| % Red Time | 2.495331 | 0.252723 | 18.252765 | 4.983569 |
| System Failures | 22.623188 | 14 | 42 | 5.200617 |

R(t=8760.000000) =0.000000

Average sparing data over 69 run(s):

| COMPONENT | START | END | MIN | MAX | # DELAYS |
|---|---|---|---|---|---|
| NOT USED | | | | | |

# CONCLUSIONS

Injector Complex Analysis:

- Components Analysis
- Failure Modes
- Optics Simulations + FLUKA Simulations for worst cases

Risk Assessment:

- The Failure Catalogue needs to be completed in order to assess the risk (SIL or equivalent)
- Knowledge and experience from the experts in different domains is needed for this
- Tentative document about Linac4 SIS

A website to collect and share knowledge on the project seems the most efficient way for this purpose.

# FUTURE DEVELOPMENTS

Can this approach be easily extended to other machines?

The next injector complex has been an ideal test bench for the developed approach:

- It is a relatively 'small' machine → failure cases can be handled more easily
- It's still under design for many aspects → collected information have to be continuously updated

Extend such studies to bigger machines is a challenge, considering all the possible failure cases. A very systematic approach is needed, as well as the collaboration of several experts for the different related studies.

Next steps:

- Conclude the studies related to Linac 4 – Risk Assessment
- CLIC study
- LHC study (already started, S. Wagner)
- Derive Availability and Reliability models based on the Failure Catalogue

# Risk assessment in the next Injector Complex

THANK YOU FOR YOUR ATTENTION

References:
[1] “A New Accident Model for Engineering Safer Systems”, Nancy Leveson, Aeronautics and Astronautics Dept. Massachusetts Institute of Technology, USA.
[2] “STPA: A New Hazard Analysis Technique” ”, Nancy Leveson, Aeronautics and Astronautics Dept. Massachusetts Institute of Technology, USA. http://csrl.scripts.mit.edu/home/stampstpa-workshop/materials
[3] “Beam Interlock Specifications for Linac4, Transfer Lines and PS Booster with Linac4”, B.Mikulec, J.L.S.Alvarez, B.Puccio, CERN, 2011.

# ADDITIONAL SLIDES

# RISK CLASSIFICATION

The specification of the LHC Machine Protection System gives the dependability requirement in the form of a Safety Integrity Level (SIL). Four possible levels exist, from 1 to 4. SIL 4 is the most strenuous. These are defined by the IEC-61508 standard.

| Frequency | per year | Catastrophic | Critical | Marginal | Negligible |
|---|---|---|---|---|---|
| Frequent | 1 | SIL4 | SIL3 | SIL3 | SIL2 |
| Probable | 0.1 | SIL3 | SIL3 | SIL3 | SIL2 |
| Occasional | 0.01 | SIL3 | SIL3 | SIL2 | SIL1 |
| Remote | 0.001 | SIL3 | SIL2 | SIL2 | SIL1 |
| Improbable | 0.0001 | SIL3 | SIL2 | SIL1 | SIL1 |
| Not Credible | 0.00001 | SIL2 | SIL1 | SIL1 | SIL1 |
| cost [Millions of CHF] | | >50 | 1-50 | 0.1-1 | 0-0.1 |
| downtime [days] | | >180 | 20-180 | 3-20 | 0-3 |

B. Todd

A single 10 hour operation of the LHC is referred to as a mission, some 400 missions per year are expected, a SIL 3 Machine Protection System has less than a 1% chance of failure in the 8000 missions that are expected in the 20 year lifetime of the LHC.

# LINAC4 PARAMETERS

| LINAC 4 MAIN PARAMETERS | |
|---|---|
| Ion species | H- |
| Output energy | 160 MeV |
| Bunch frequency | 352.2 MHz |
| Repetition Rate | 1.1 Hz |
| Beam pulse length | 400 µs |
| Source current | 80mA |
| RFQ output current | 70mA |
| Linac current | 40mA |

The beam coming from Linac 4 will join the existing Linac 2 Transfer Line through a new dedicated TL section (L4T) before injection in the PS Booster.

# RELIABILITY ANALYSIS

Approach:

- Study the system under investigation (every component!)
- Derive possible Failures and Failure Modes
- Identify Failure 'Categories' (e.g. cavities, quadrupoles, etc.)
- Consider several Test Cases for each category
- Identify the Worst Cases for each category
- Evaluate possible damage in these scenarios (FLUKA, particle physics MonteCarlo simulation package) in case of Protection Systems working or not

Difficulties:

1. Retrieve and collect informations (contact experts, components still under design,…)
2. Identify the Failure Categories and evaluate the impact of failures in circular accelerators
3. Cover all possible failure scenarios with 'adequate' accuracy

# FAILURES: TEST CASES

Test cases which have been studied:

- Quadrupoles
- Cavities
- Chopper – Quadrupole
- Bending magnets

Approach:

1. Simulate the failure of a component in a Tracking Code (*TraceWin*, CEA, *Travel*, CERN)

2. Quantify and localize the losses (percentage of particles and power)

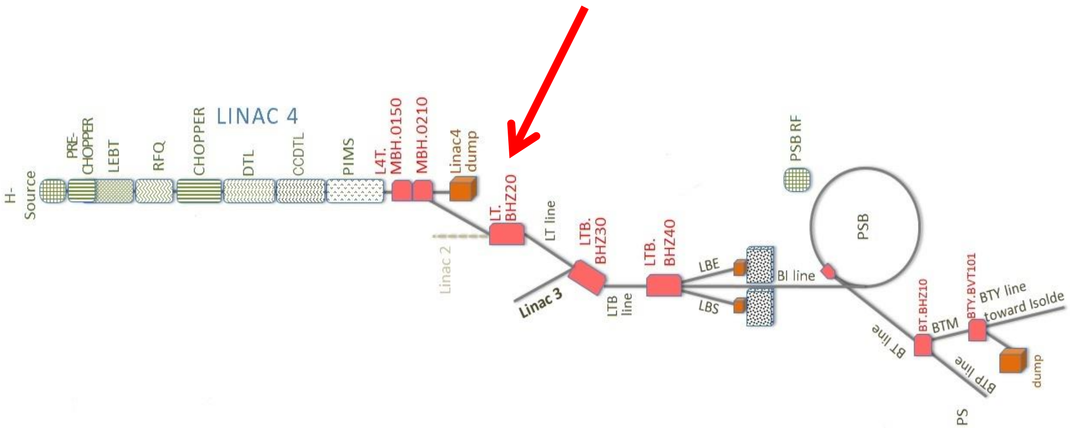
3. Run simulations (FLUKA) in the worst cases to verify the possibility of damage of the equipment

*Note 1*: Only single failures have been considered in these first studies

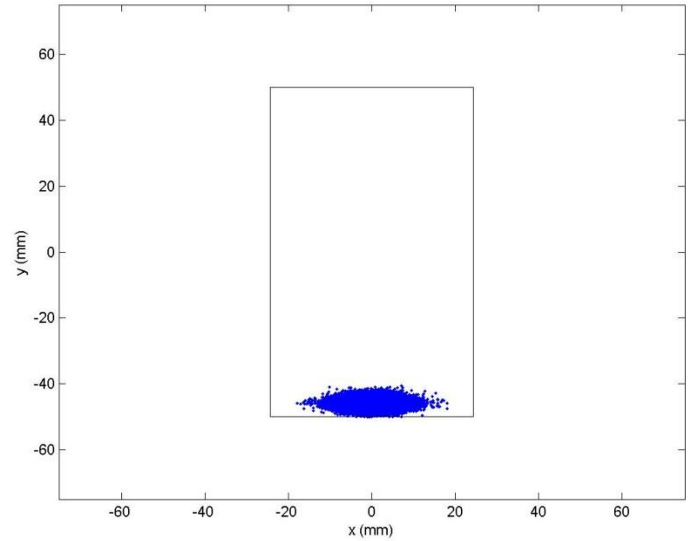
*Note 2*: tracking codes are not made to simulate failures therefore expedients are used. The results have then to be interpreted as estimates of the losses for the given failure cases.

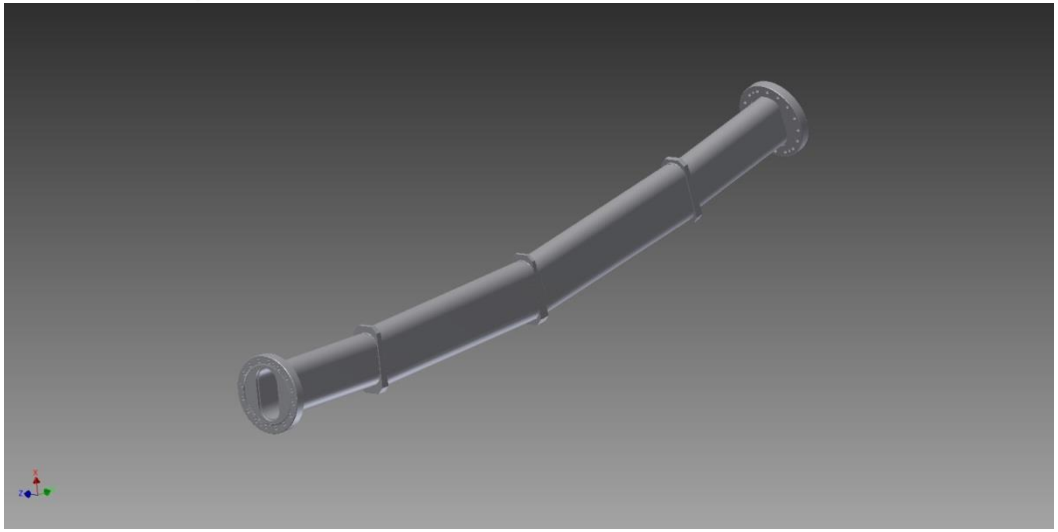
# WORST CASE: MBV FAILURE

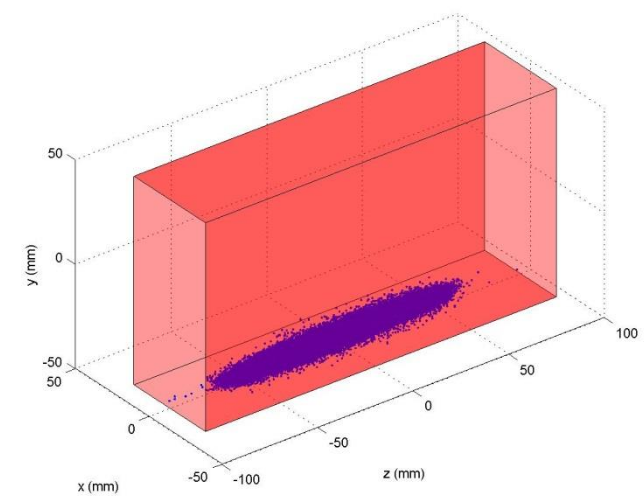
First Vertical Bending Magnet Failure in the TL



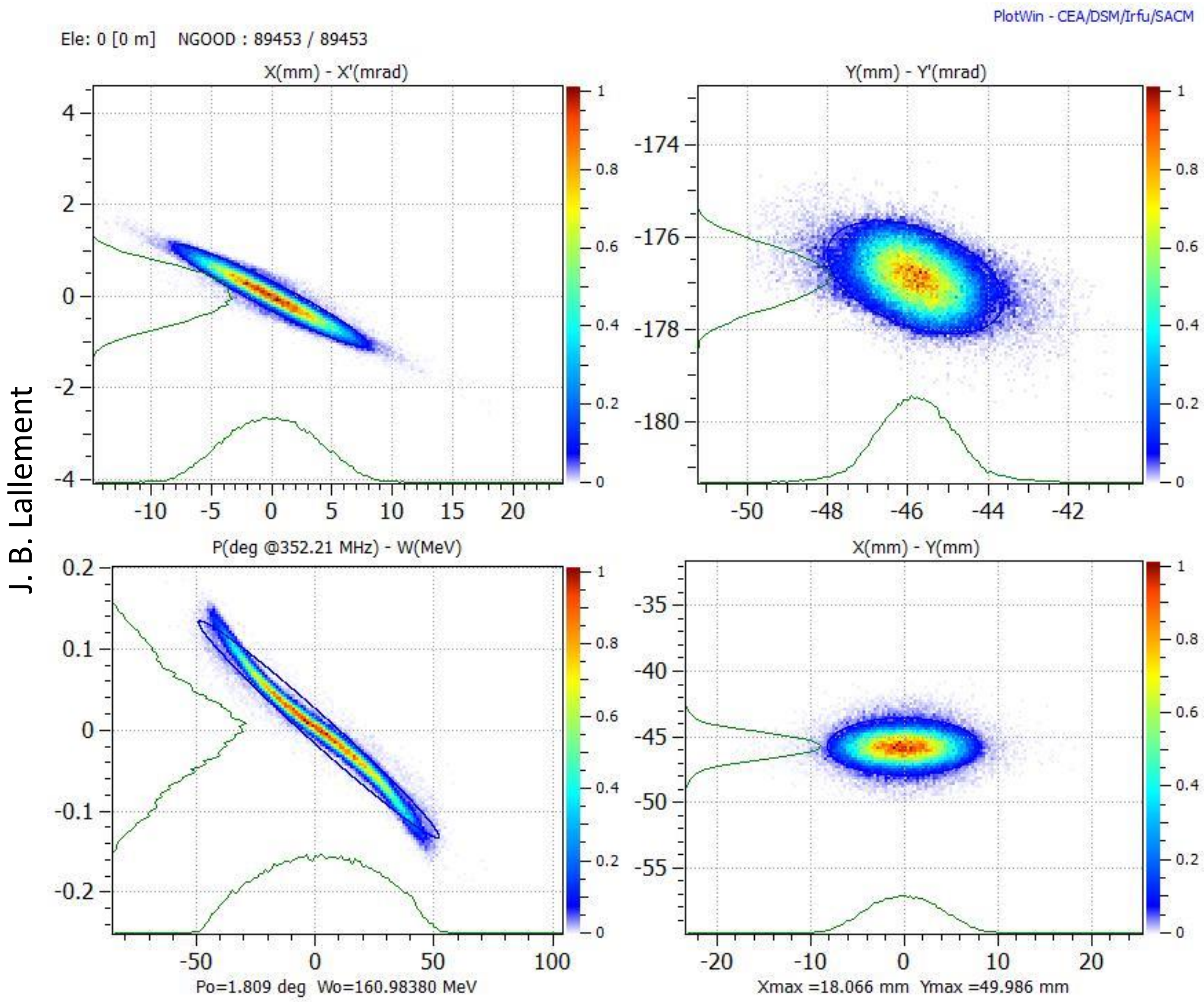

J. Humbert





# WORST CASE: BEAM FILE




BEAM DISTRIBUTION IN THE WORST CASE FROM THE BEAM FILE

ENERGY: 160 MeV

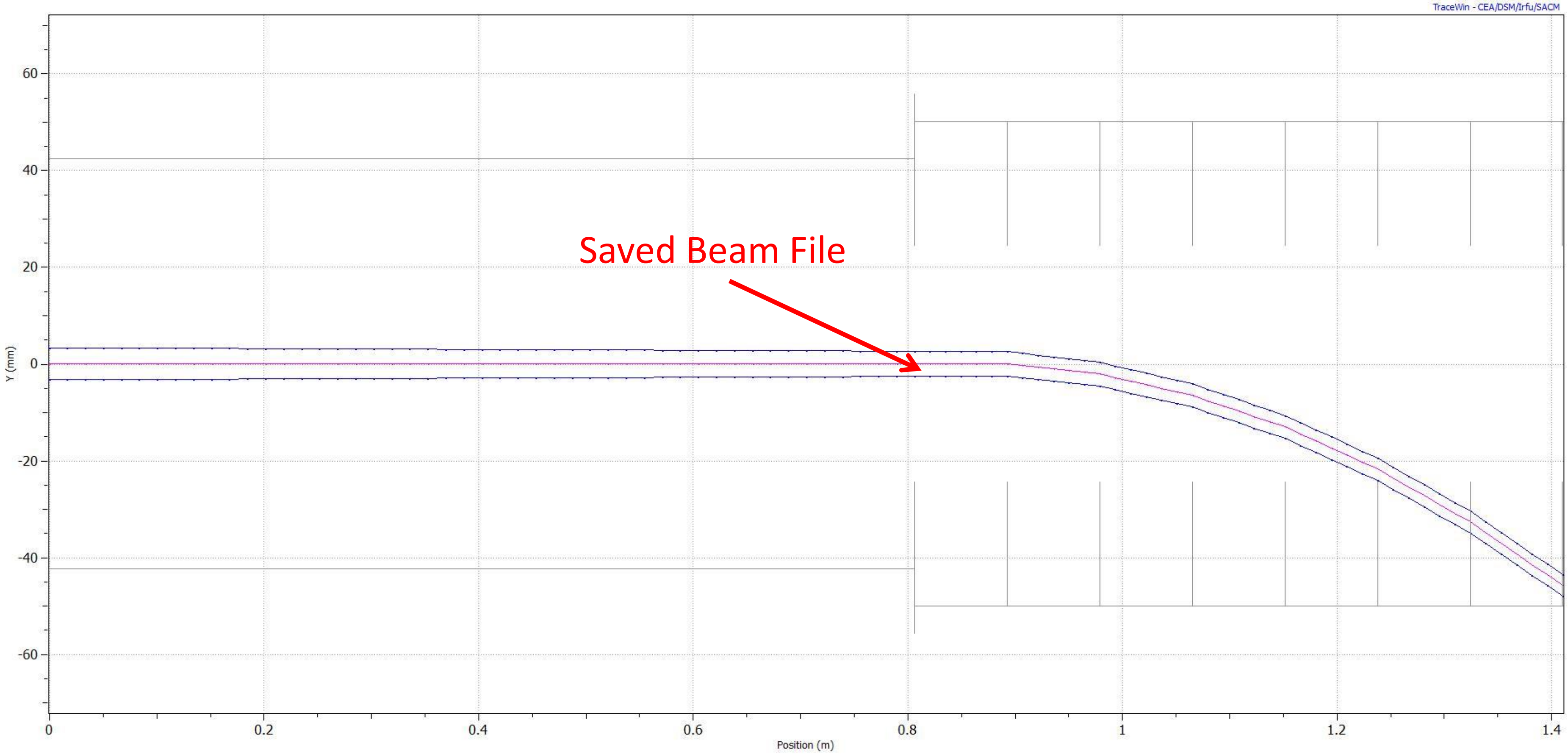
RMS SIZE (X*Y): 3.6194 mm * 0.9781 mm

POSITION: 120.8m

All beam lost after 60 cm in the MBV with a grazing angle of about 200 mrad

# WORST CASE: MBV FAILURE

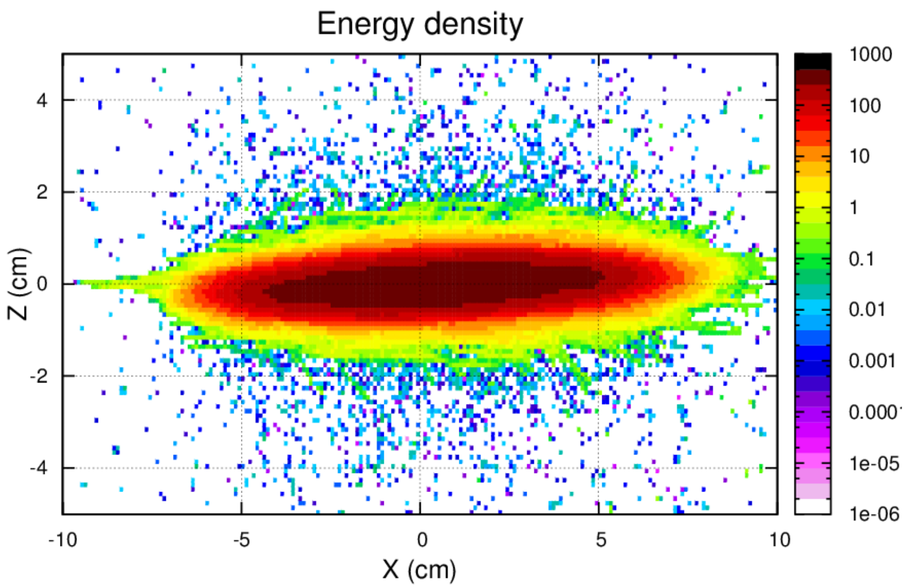
VERTICAL STEP OFF: Losses in MBV.1250 → Failure Simulation Expedient

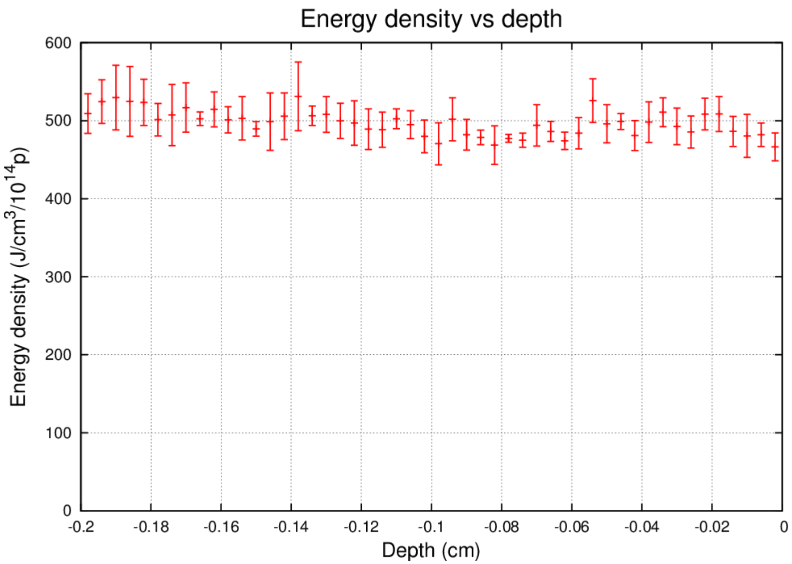



J. B. Lallement

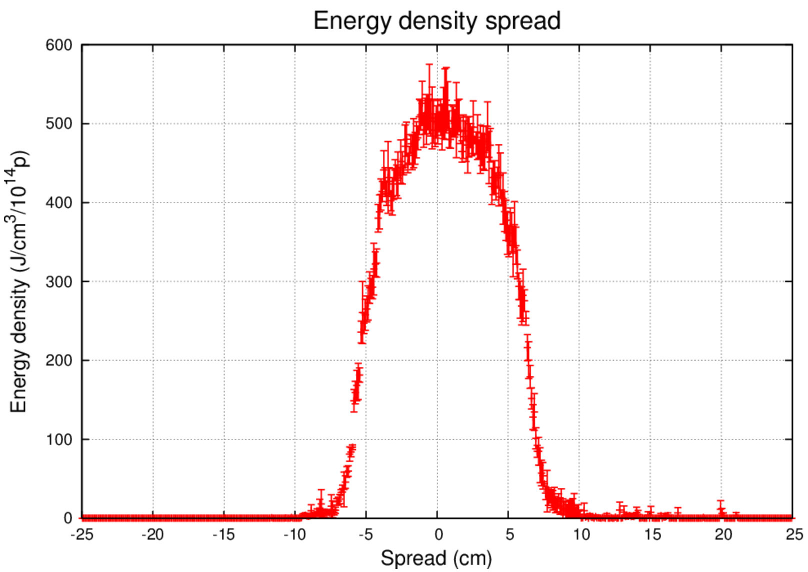
All beam lost after 60 cm from the beginning of the MBV with a grazing angle of 200 mrad (the code crashes!)

# WORST CASE: FLUKA ANALYSIS



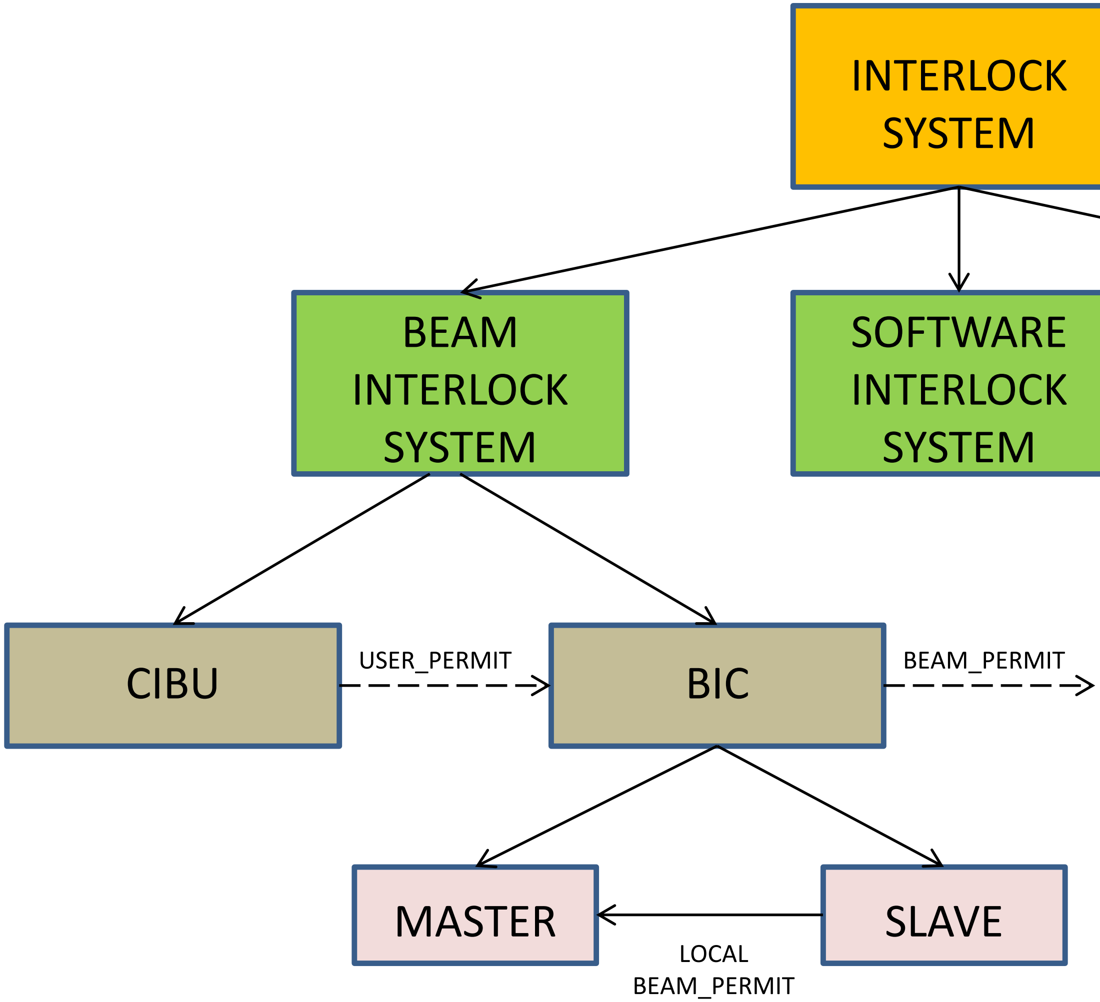




V. Vlachoudis



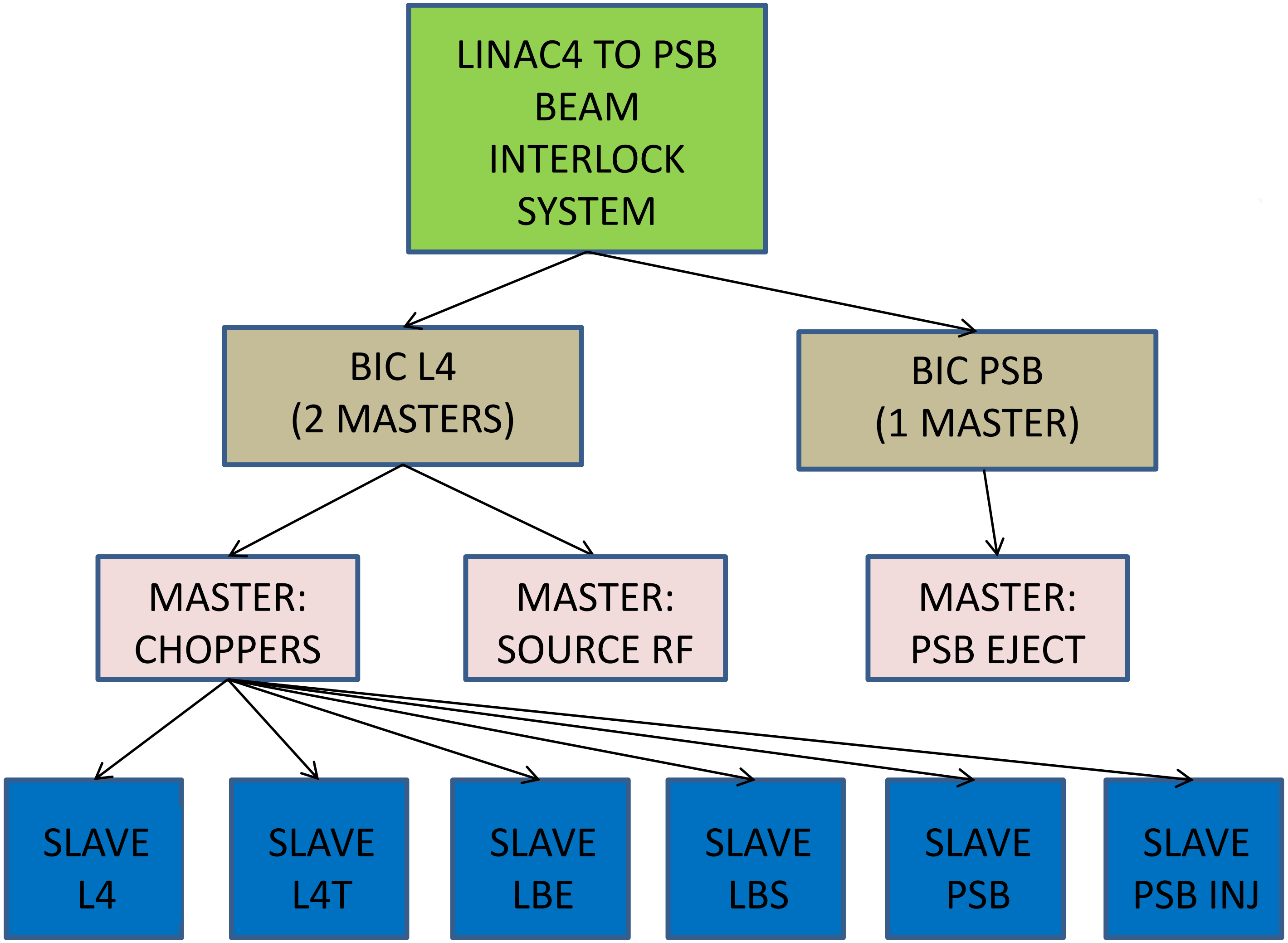

- Total energy: 160MeV *10^14p = 2.56 kJ 70% (~1.8 kJ) of the energy escapes the 2mm beam pipe downstream.
- Peak energy deposition ~530 J/cm3: adiabatic temperature rise of about 130 K.
- Critical temperature for 316LN SS: 833 °C
- Melting point for 316LN SS: 1390 °C
- Next step will be to verify the impact of the 70% of the energy on the magnet around the pipe

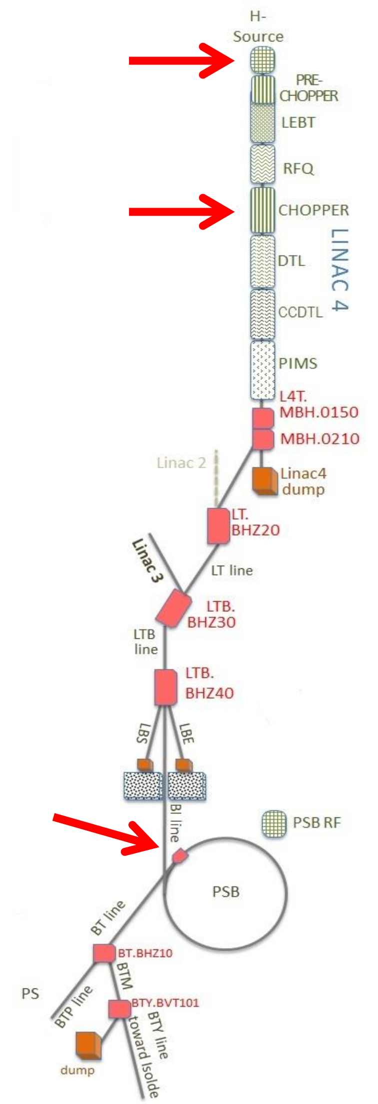
# INTERLOCK SYSTEM: GENERAL OVERVIEW




- BIS: fast reaction times or minimization of machine activation needed
- SIS: monitor slow-changing parameters or for complex logic implementation
- EC: Optimization (Users requests,…)

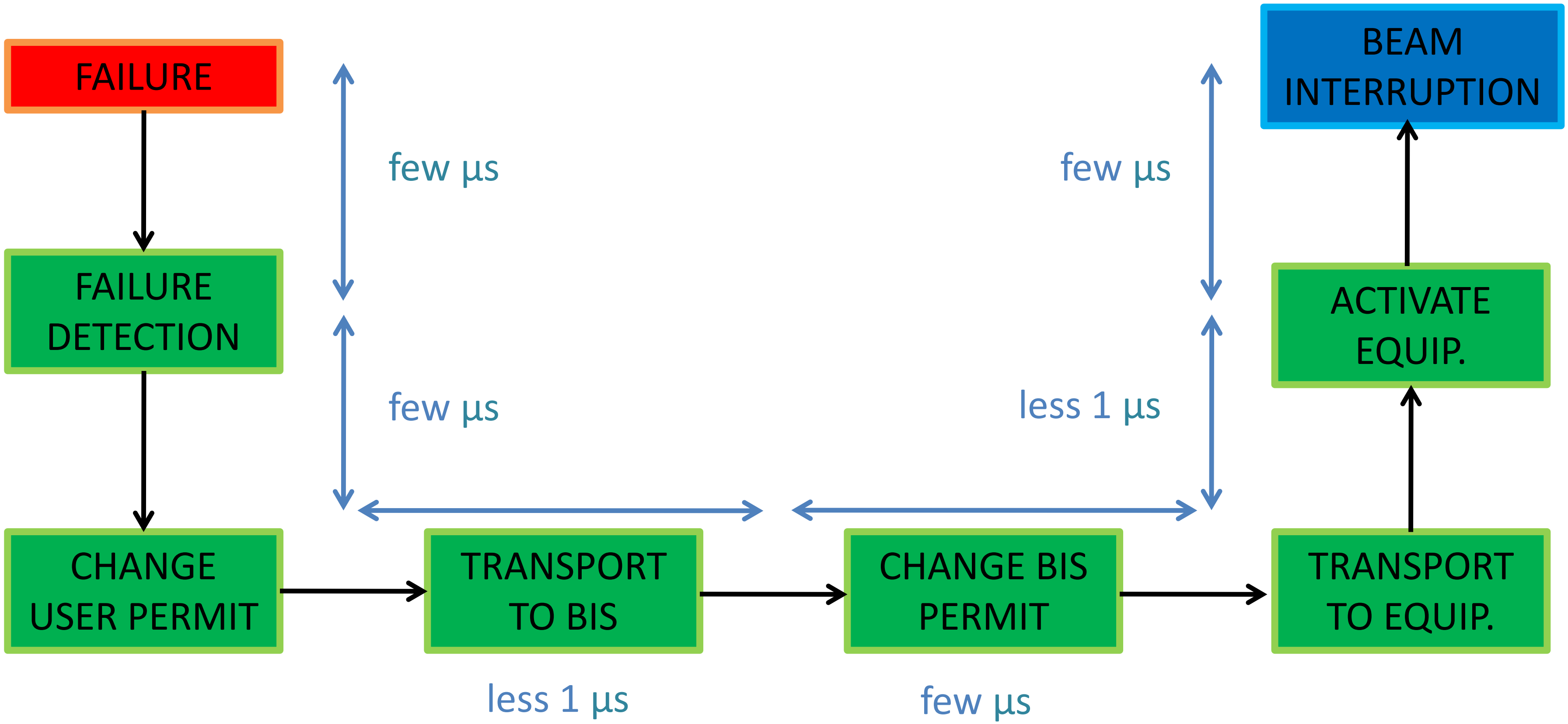
# LINAC4 TO PSB BEAM INTERLOCK SYSTEM [2]




The BIS is able to react within the same pulse as the failure is detected!

# MACHINE PROTECTION: TIMING




Total time: 10-20 µs Pulse length: 400 µs