Studies on Reliability

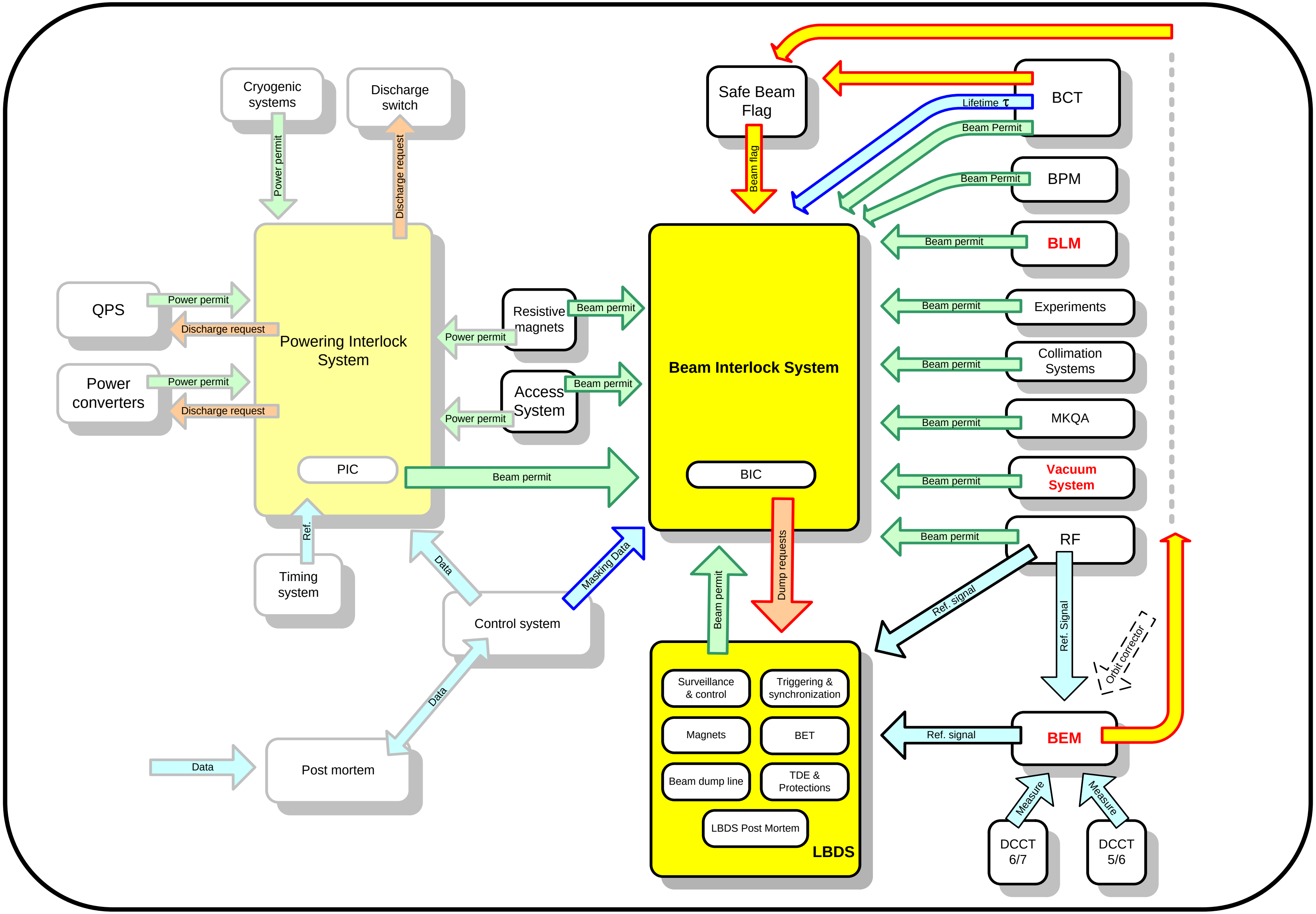
A General Approach

Topics of the Presentation

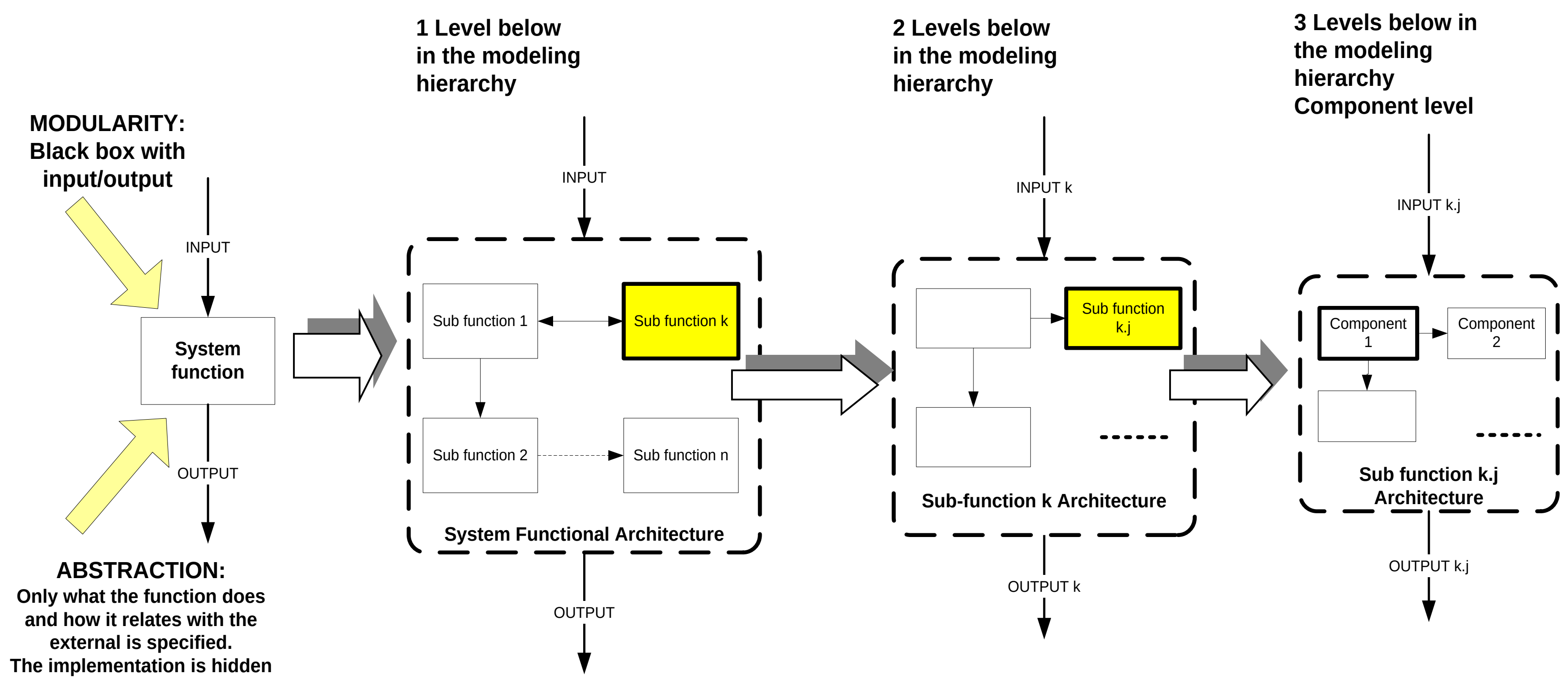
- Some guidelines to the **modeling of complex systems**.
- **Addressing dependability problems** of complex systems.
- **Application** to the LHC Machine Protection System and examples.

Introduction

- **The aim** is to manage complexity when addressing dependability issues for very large critical systems.
- **The proposal** is based on a **hierarchical functional modeling approach.**
  - Abstraction and modularity principles hold.
  - A top-down iterative procedure permits to build the hierarchy starting from the system functional specification. It can be detailed up to the desired level.
  - Dependability problems find a powerful support in the hierarchical functional structure.

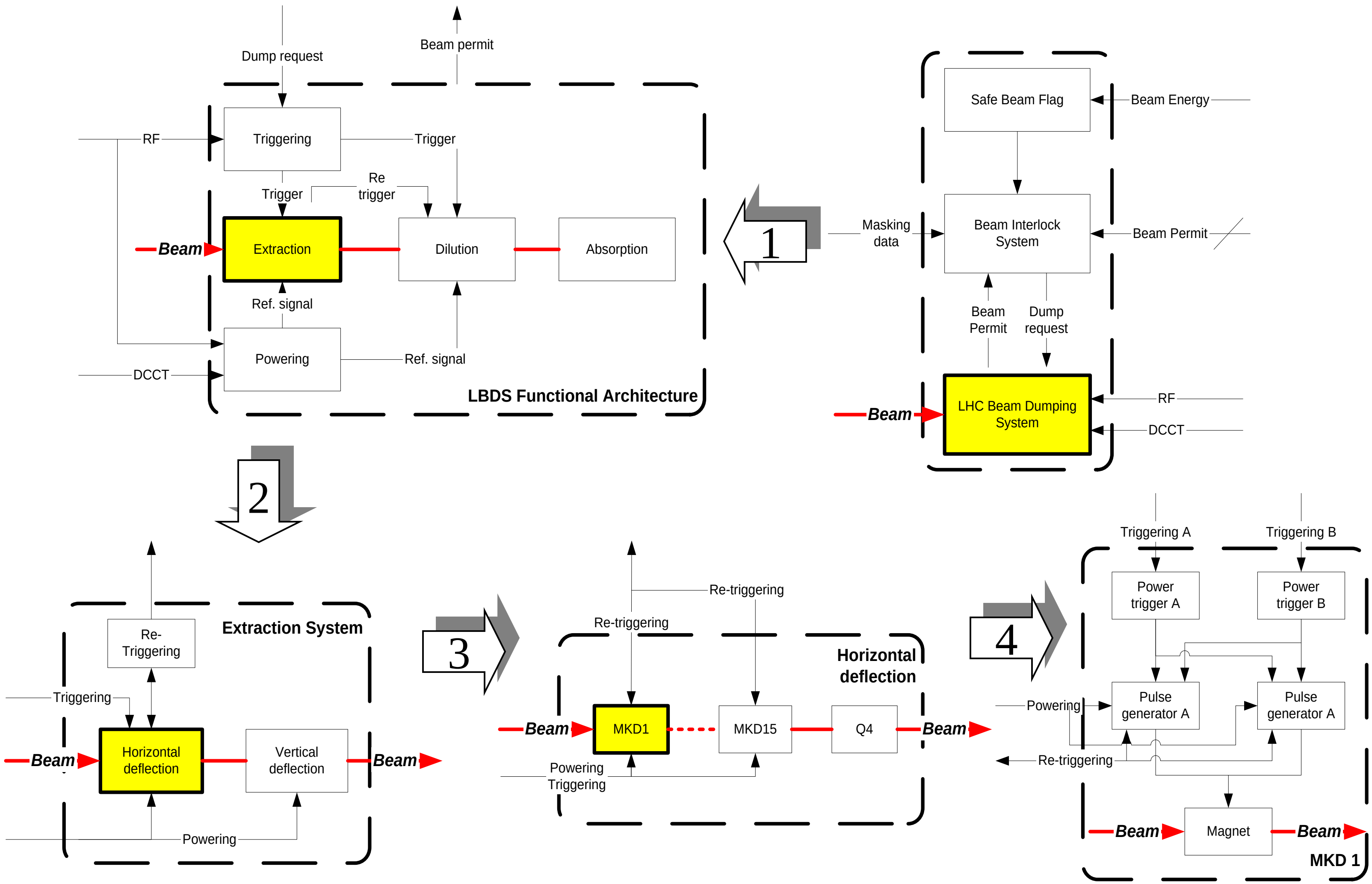

Cryogenic systems
Discharge switch
Power permit
Discharge request
Safe Beam Flag
Beam flag
BCT
Lifetime τ
Beam Permit
BPM
Beam Permit
BLM
Beam permit
QPS
Power permit
Discharge request
Powering Interlock System
Power converters
Power permit
Discharge request
PIC
Resistive magnets
Beam permit
Power permit
Access System
Beam permit
Power permit
Beam Interlock System
BIC
Beam permit
Experiments
Beam permit
Collimation Systems
Beam permit
MKQA
Beam permit
Vacuum System
Beam permit
RF
Beam permit
Timing system
Ref.
Data
Control system
Masking Data
Beam permit
Dump requests
Ref. signal
Ref. Signal
Orbit corrector
Data
Post mortem
Data
Surveillance & control
Triggering & synchronization
Magnets
BET
Beam dump line
TDE & Protections
LBDS Post Mortem
LBDS
Ref. signal
BEM
Measure
Measure
DCCT 6/7
DCCT 5/6

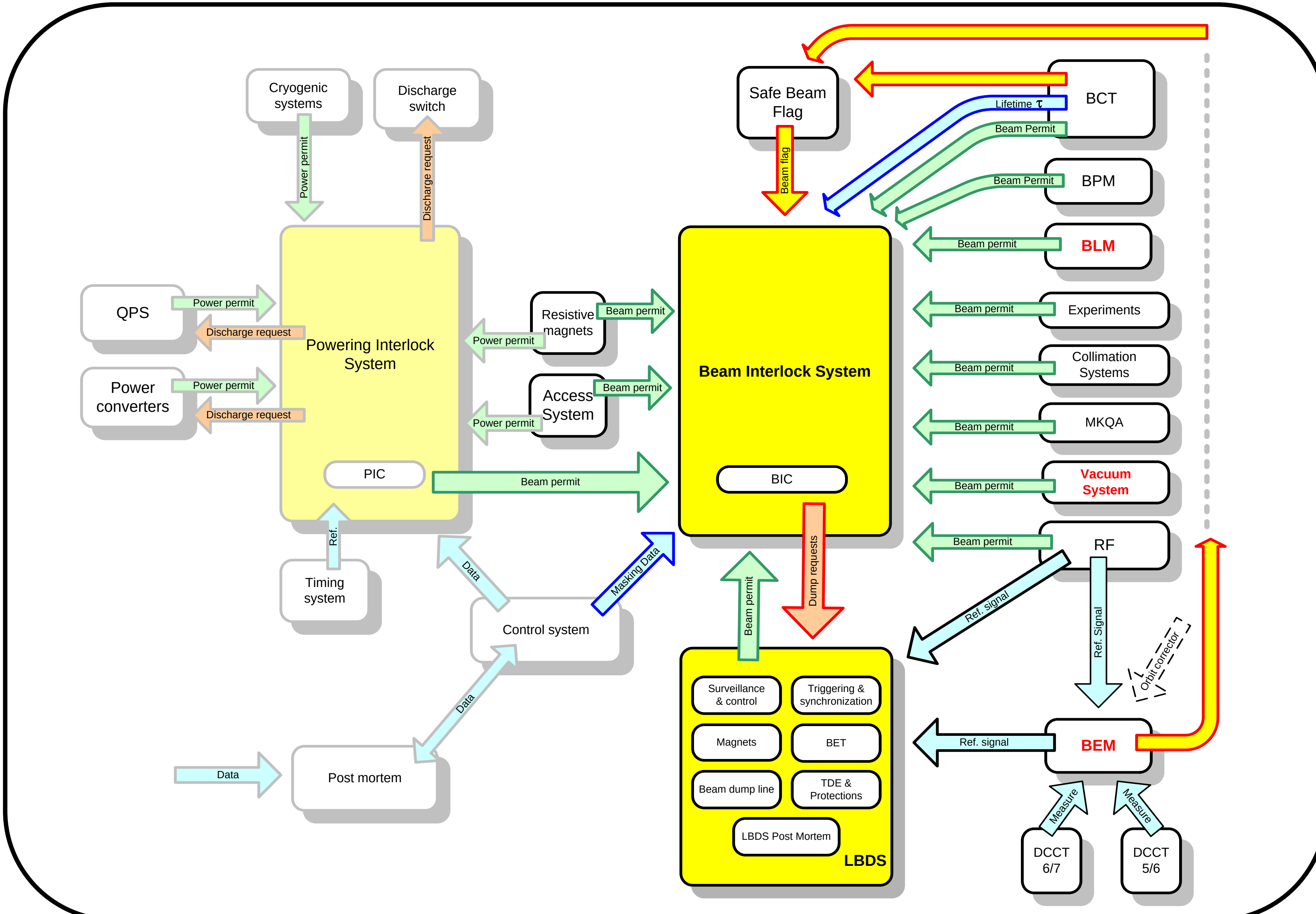
Hierarchical Modeling:
Managing complexity



Example of Hierarchical Modeling:

From the BIS to the MKD




Cryogenic systems
Discharge switch
Power permit
Discharge request
Safe Beam Flag
Beam flag
BCT
Lifetime τ
Beam Permit
BPM
Beam Permit
BLM
Beam permit
QPS
Power permit
Discharge request
Powering Interlock System
Resistive magnets
Beam permit
Power permit
Beam Interlock System
Experiments
Beam permit
Collimation Systems
Beam permit
Power converters
Power permit
Discharge request
Access System
Beam permit
Power permit
MKQA
Beam permit
PIC
Beam permit
BIC
Vacuum System
Beam permit
RF
Beam permit
Ref.
Timing system
Data
Masking Data
Control system
Beam permit
Dump requests
Ref. signal
Ref. Signal
Orbit corrector
Surveillance & control
Triggering & synchronization
Magnets
BET
Beam dump line
TDE & Protections
LBDS Post Mortem
LBDS
Data
Data
Post mortem
Ref. signal
BEM
Measure
Measure
DCCT 6/7
DCCT 5/6

Addressing Dependability

Formula Composition

Top

RELIABILIT Y OF LBDS

$$R_{LBDS}(t) = R_{Extr}(t) R_{Pow}(t) R_{Tri}(t) R_{Dil}(t) R_{Abs}(t)$$

1

2

......

RELIABILIT Y OF EXTRACTION

$$R_{Extr}(t) = R_{H-Extr}(t) R_{V-Extr}(t)$$

RELIABILIT Y OF HORIZONTAL DEFLECTION

$$R_{H-Extr}(t) = R_{Q_4}(t)\{R_{MKD}^{15}(t) + 15 R_{MKD}^{14}(t)[1 - R_{MKD}(t)]\}$$

......

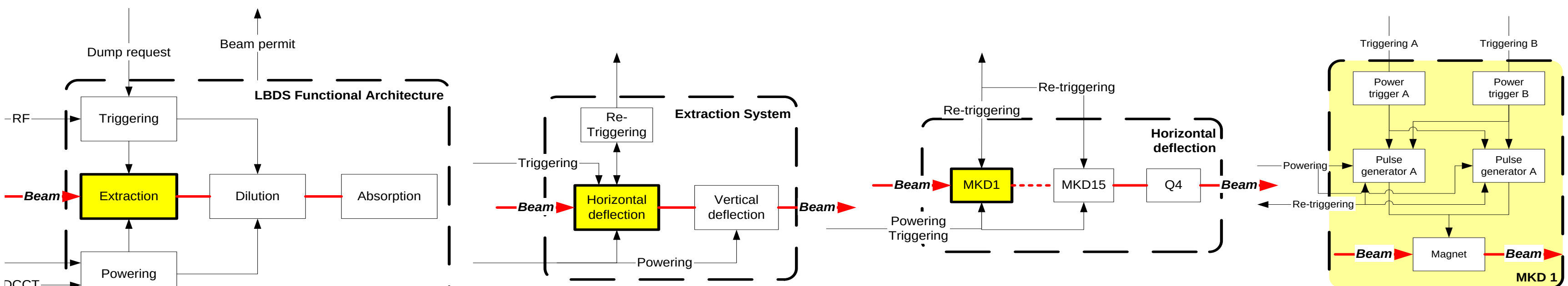
3

Down

......

RELIABILIT Y OF MKD1

$$R_{MKD1}(t) = \{1 - [1 - R_{TriggerA}(t)][1 - R_{TriggerB}(t)]\}\{1 - [1 - R_{PulseA}(t)][1 - R_{PulseB}(t)]\} R_{Magnet}(t)$$

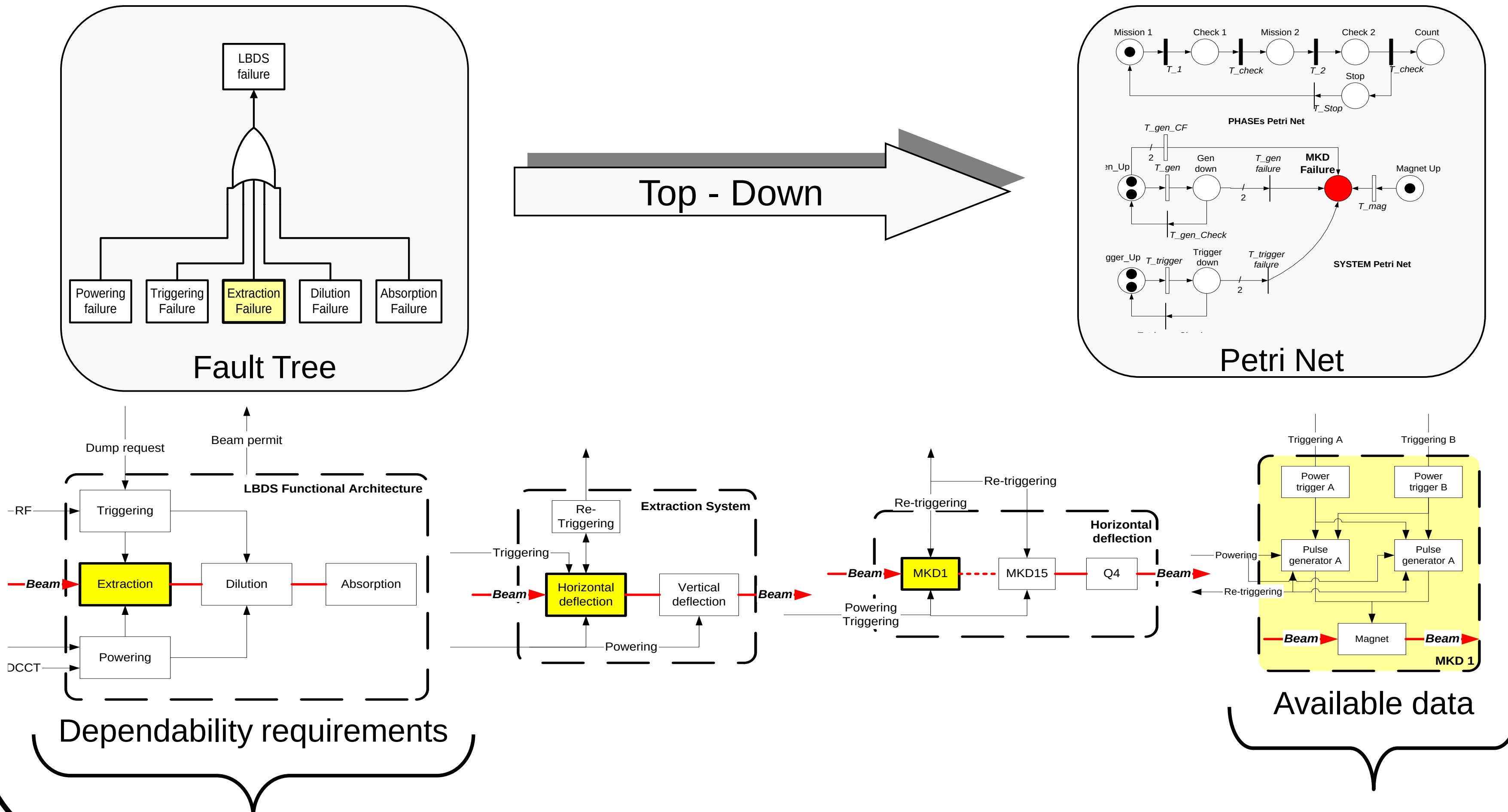


Dependability requirements

Data available

Addressing Dependability

Hierarchical Modeling of Failure Processes



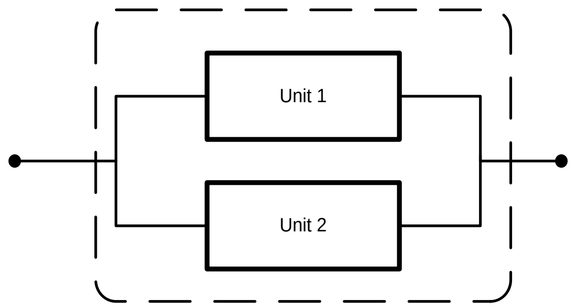
Comments on
Hierarchical Modeling

1. When **addressing reliability/availability issues**:
   - **Statistical independency** of failure processes must be checked.
   - <**?**> R(component j | component k is failed) = R(component j)
2. When **addressing safety issues**:
   - **Linearity of hazards** consequences must be checked.
   - <**?**> Risk {H1 U H2} = Risk {H1} + Risk {H2}.

- Whenever 1) or 2) are not true, the **modularity principle is violated** from a statistical point of view.
  - Reliability and availability will be overestimated.
  - Risk will be underestimated.
- Two **examples** following.

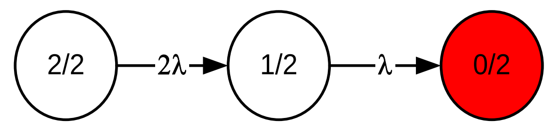
Example 1:
Overestimating Reliability

- **<u>The function</u>**: MKD pulse generator in the LBDS extraction function (horizontal deflection).
  - It consists of a parallel structure of two identical units.



- **<u>Reliability overestimate</u>**:
  - We ignore the common mode failure.

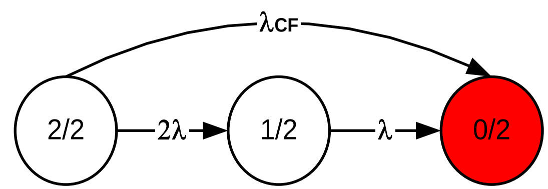
$R_{PG}(t) = 1-[1-R(t)]^2$; $R(t) = e^{-\lambda t}$



A: Statistical independent failure processes

- **<u>Reliability (true value):</u>**
  - We consider the common mode failure.

$\underline{R}_{PG}(t) = \{1-[1-R(t)]^2\}R_{CF}(t) < R_{PG}(t)$

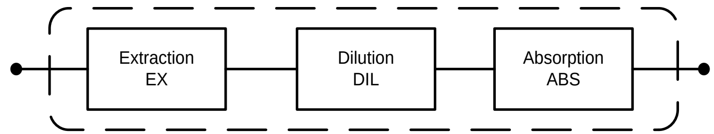


B: Statistically dependent failure processes

Example 2:

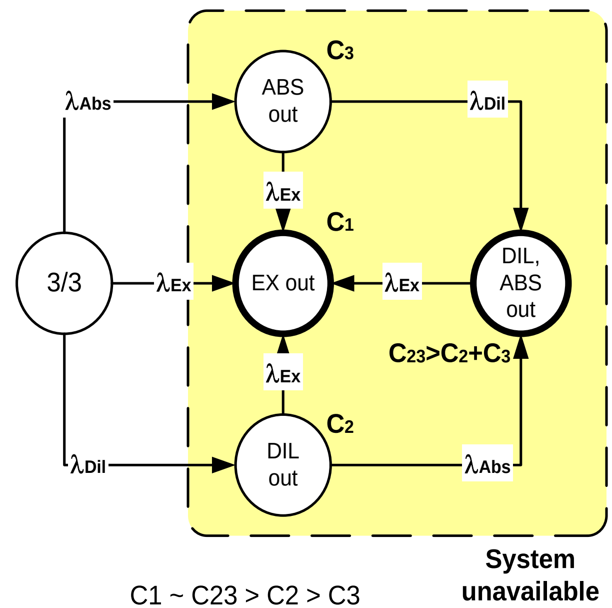
Underestimating risk

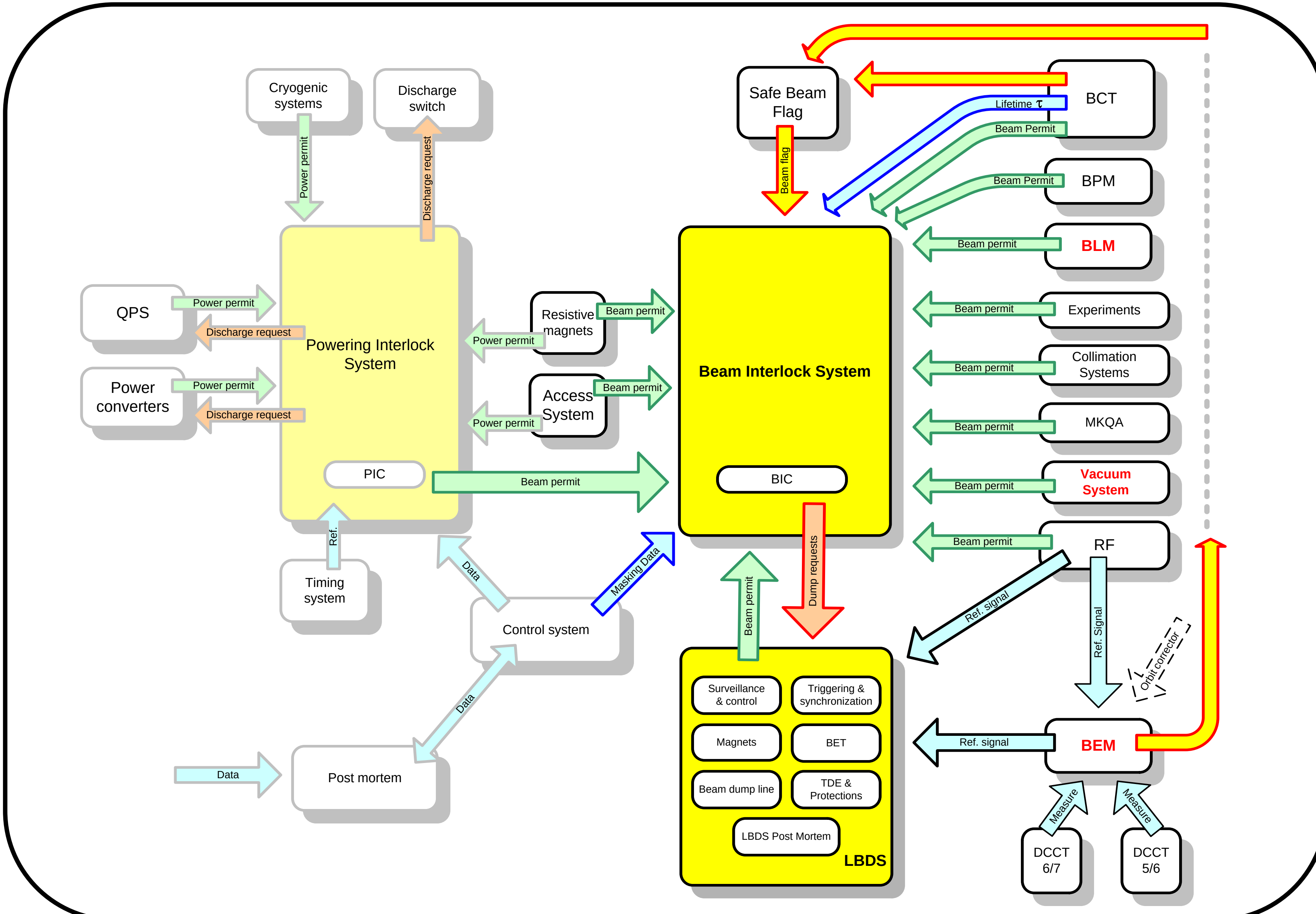
- **<u>The function</u>**: LBDS (simplified).
  - Three sub-functions in series: Extraction, Dilution and Absorption.



- **<u>The hazards</u>:**
  - H_1 {extraction failure} $[\lambda_{H1}(t), C_1]$
  - H_2 {dilution failure} $[\lambda_{H2}(t), C_2]$
  - H_3 {absorption failure} $[\lambda_{H3}(t), C_3]$
- **<u>Risk (underestimated)</u>**: we ignore hazards combinations.
  - $\text{Risk}(t) = \lambda_{H1}(t)C_1 + \lambda_{H2}(t)C_2 + \lambda_{H3}(t)C_3$
- **<u>Risk (true value):</u>** we consider hazards combinations
  - $\underline{\text{Risk}}(t) = \lambda_{H1}(t)C_1 + \underline{\lambda}_{H2}(t)C_2 + \underline{\lambda}_{H3}(t)C_3 + \lambda_{H2,3}(t)C_{23} > \text{Risk}(t)$

    $\underline{\lambda}_{H2}(t) < \lambda_{H2}(t)$; $\underline{\lambda}_{H3}(t) < \lambda_{H3}(t)$;



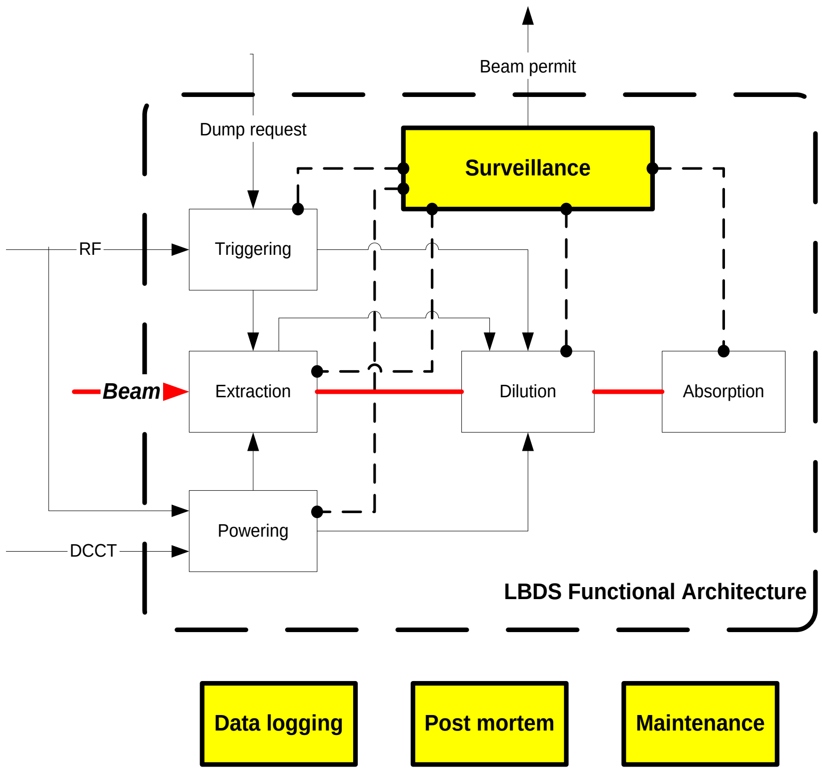


Cryogenic systems
Discharge switch
Power permit
Discharge request
QPS
Power permit
Discharge request
Power converters
Power permit
Discharge request
Powering Interlock System
PIC
Resistive magnets
Power permit
Beam permit
Access System
Power permit
Beam permit
Beam permit
Timing system
Ref.
Data
Control system
Masking Data
Data
Post mortem
Data
Safe Beam Flag
Beam flag
BCT
Lifetime τ
Beam Permit
BPM
Beam Permit
BLM
Beam permit
Experiments
Beam permit
Collimation Systems
Beam permit
MKQA
Beam permit
Vacuum System
Beam permit
RF
Beam permit
Beam Interlock System
BIC
Dump requests
Beam permit
Surveillance & control
Triggering & synchronization
Magnets
BET
Beam dump line
TDE & Protections
LBDS Post Mortem
LBDS
Ref. signal
Ref. Signal
Orbit corrector
BEM
Ref. signal
Measure
Measure
DCCT 6/7
DCCT 5/6

Auxiliary functions

- **Auxiliary functions** are functions that do not play a relevant role for the functional ability of the system but they **play a relevant role for the system dependability**.
- **Monitoring** prevents hazards (in mission).
- **Maintenance** prevents wearing and aging.
- **Diagnostics (Post mortem)**
  - checks for the healthy state of the system (out of mission).
  - gives the green light (beam permit).
- Two **examples** following.

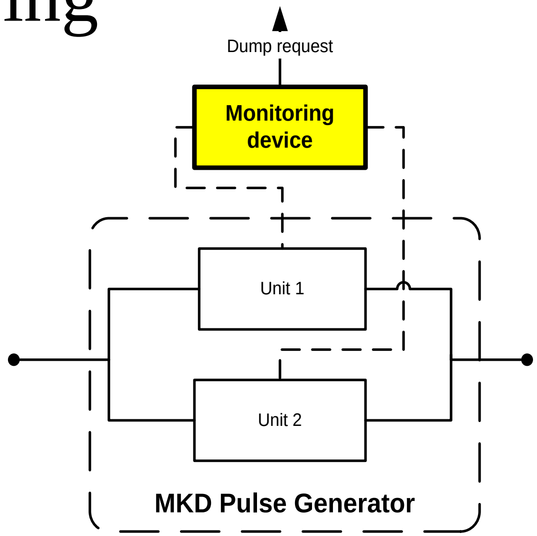
EXAMPLE: LBDS

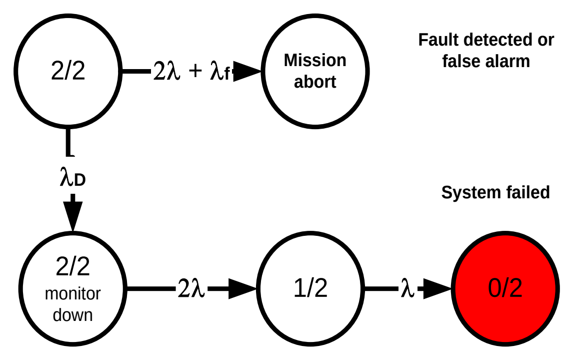


Example 3:

System Monitoring

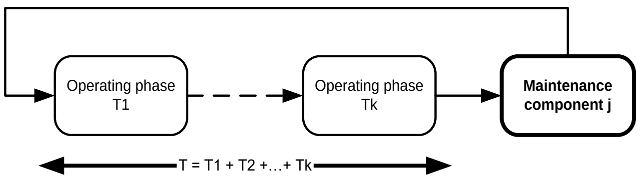
- **<u>Monitoring function</u>** for the MKD pulse generators generates a mission abort (before the mission time T) if at least one unit has failed.
- **<u>Monitoring parameters</u>:**
  - Failure rate: λ_D
  - Detection coverage = 1 (by simplicity).
  - False alarm λ_f
- **<u>Expected improvement</u>** (not for common mode failures).
  - $\underline{R}(t) = 1 - [1-R_D(t)][1-R(t)]^2 > 1 - [1-R(t)]^2$
  - $R(t) = e^{-\lambda t}$
- **<u>What we pay</u>**:
  - Mission abort rate: $2\lambda + \lambda_f$
  - Mission length = Min(T, $T_{\text{mission abort}}$) < T



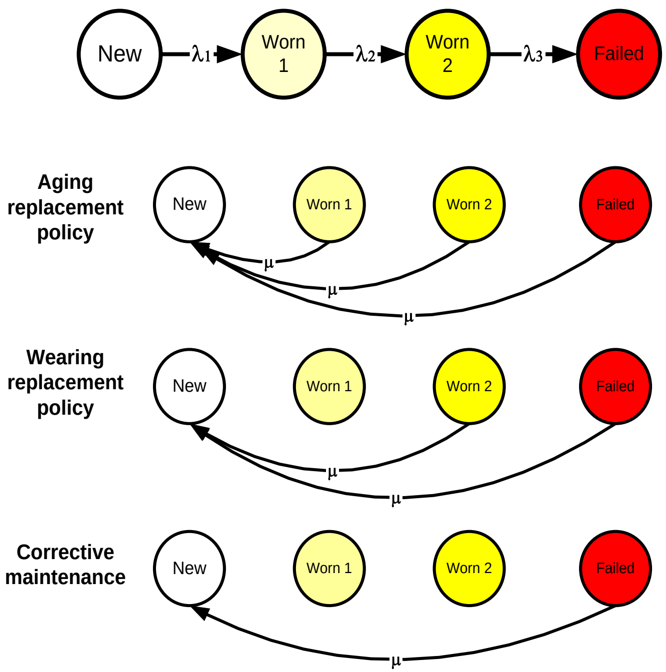


Example 4:
Maintenance Policies

- **<u>Maintenance policies</u>** prevent components from aging and wearing. Wearing and aging affect the failure rate.
- **<u>Three policies</u>**:
  - **Aging replacement**: the component is replaced after k operating phases (t = T).
  - **Wearing replacement**: the component is checked after k operating phases and is replaced only if it is worn above a threshold.
  - **Corrective maintenance**: the component is replaced only if it has failed.
- **<u>Expected improvement</u>:**
  - $R_A(t) = R(t\text{-}nT)R(T)^n > R_W(t) > R_C(t) = R(t)$
- **<u>What we pay</u>:**
  - Cost of replacement/maintenance.
  - $C_A(t) > C_W(t) > C_C(t)$

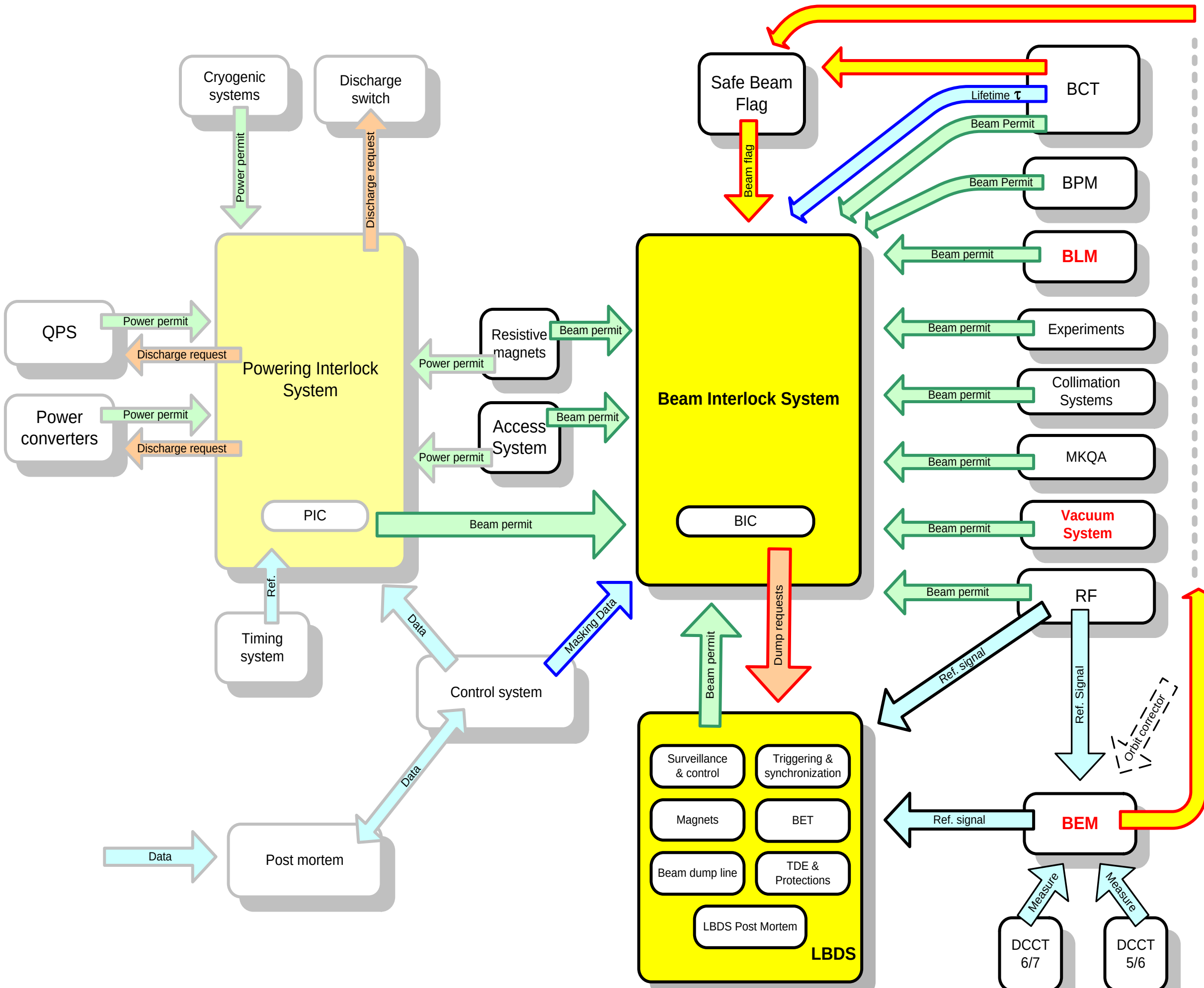


3 - Stages wearing process $\lambda_1 < \lambda_2 < \lambda_3$



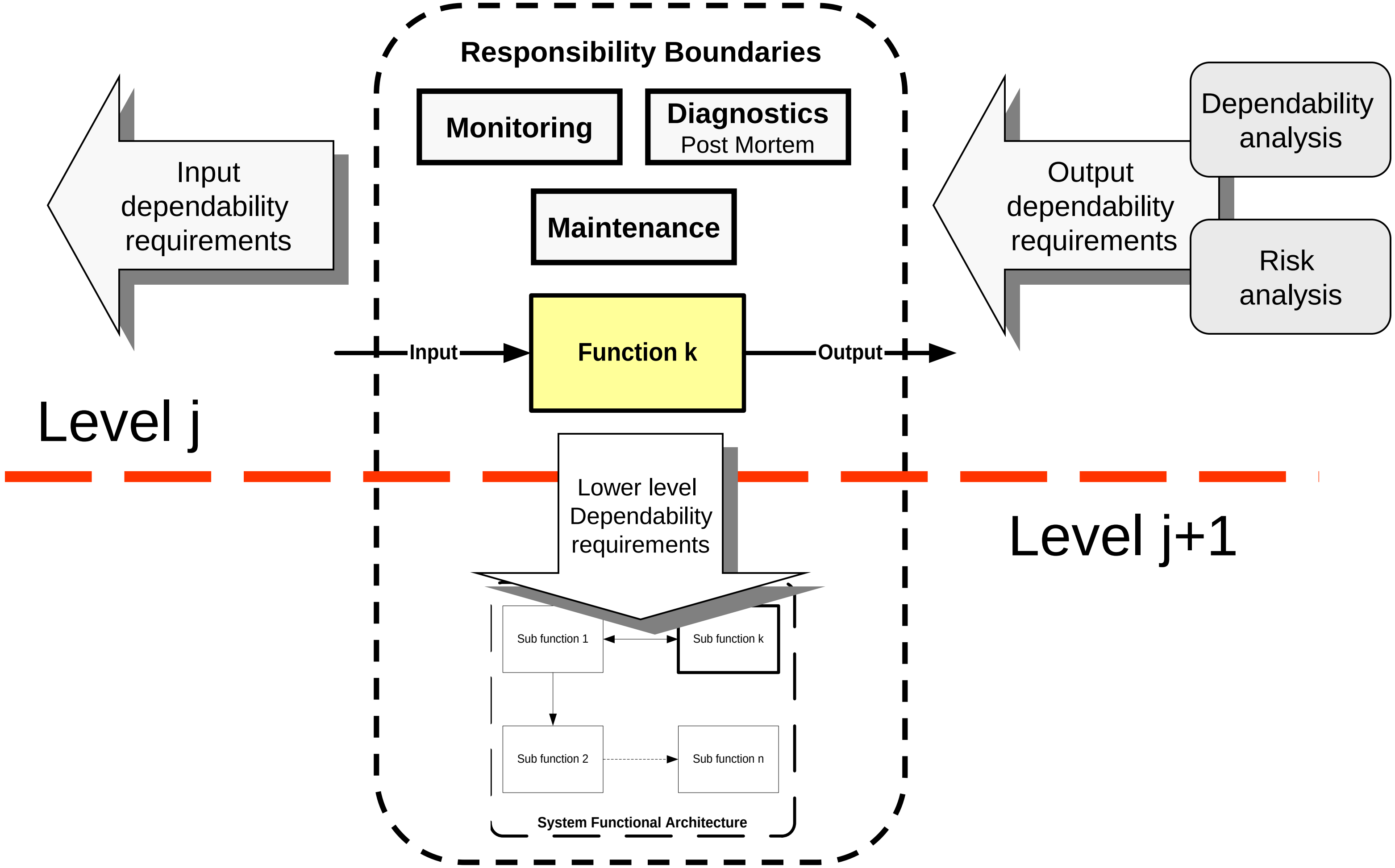
Some Questions to Be Asked by MPWG

- **BCT.**
  - Will lifetime generate a beam abort? Noise?
- **BLMs.**
  - Different families?
  - Redundancy.
- **BEM.**
  - RF frequency: energy changes allowed to 0.1% maybe to 0.3% ?
  - Orbit correctors.
- **Collimation system.**
  - Is the opening of collimators going into the BIC?



Dependability

Who Is Responsible of What



Conclusions

- **<u>Hierarchical modeling</u>** permits to manage complexity by:
  - Understanding interactions among different systems.
  - Defining relevant and not relevant modules/systems with respect to the analyzed function.
  - Addressing very complex dependability/performability problems in a hierarchical fashion.
  - Clarifying role and responsibility with respect to the global task.
  - Driving decisions top-down and vice versa.
- **<u>Responsibility of the MPWG</u>** is:
  - To built the structure of such a framework, similar to the one proposed in this presentation.
  - To fill each box with the information relevant for the dependability issues (including monitoring and maintenance).