Design process of the Interlock Systems

CLIC Workshop 2013
- Accelerator / Parameters & Design activities Session -

Patrice Nouvel - CERN / Institut National Polytechnique de Toulouse

Topics

Introduction

Principles

Requirements and Challenges

Specifications

- Interface
- Design, Functions and Architecture

Validations ongoing

- First Experience at CTF3
- Prototype

Wrap-up

Introduction

Basic Concepts

- As for LHC, CLIC Interlock Systems are defined at the machine design level
- Backbone of machine protection: ability to stop the operation
- Aim to increase the **Machine safety** and do not decrease the **Machine availability**

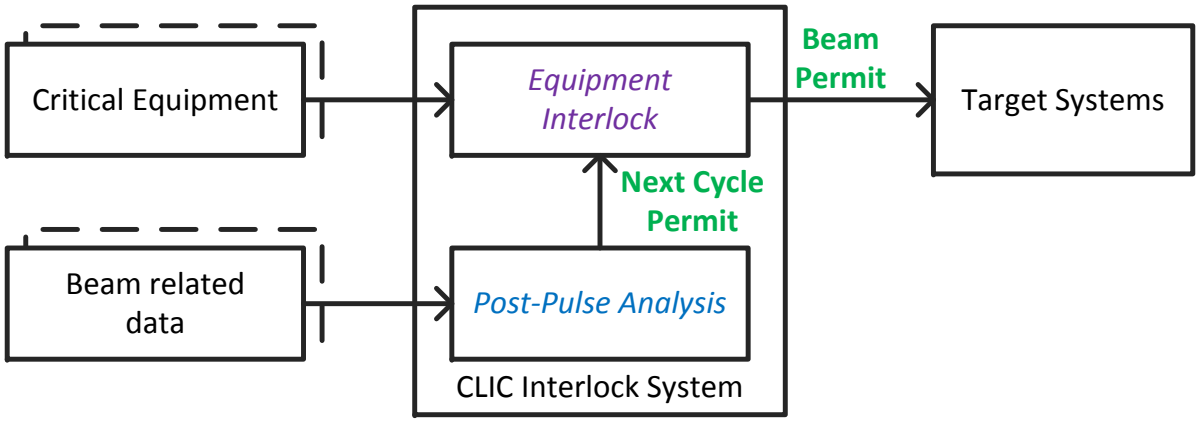
Linear Collider Challenge

- Cannot stop the beam in flight: the Beam Permit inhibits the next pulse

CLIC Interlock System Principles

- Critical Equipment:
  - Look for any equipment failures
  - Inhibit the next pulse => **Beam Permit**

- Post-Pulse Analysis:
  - Perform beam quality analysis: assert the next pulse quality
  - Inhibit the next pulse => **Next Cycle Permit**



Topics

Introduction

Principles

Requirements and Challenges

Specifications

- Interface
- Design, Functions and Architecture

Validations ongoing

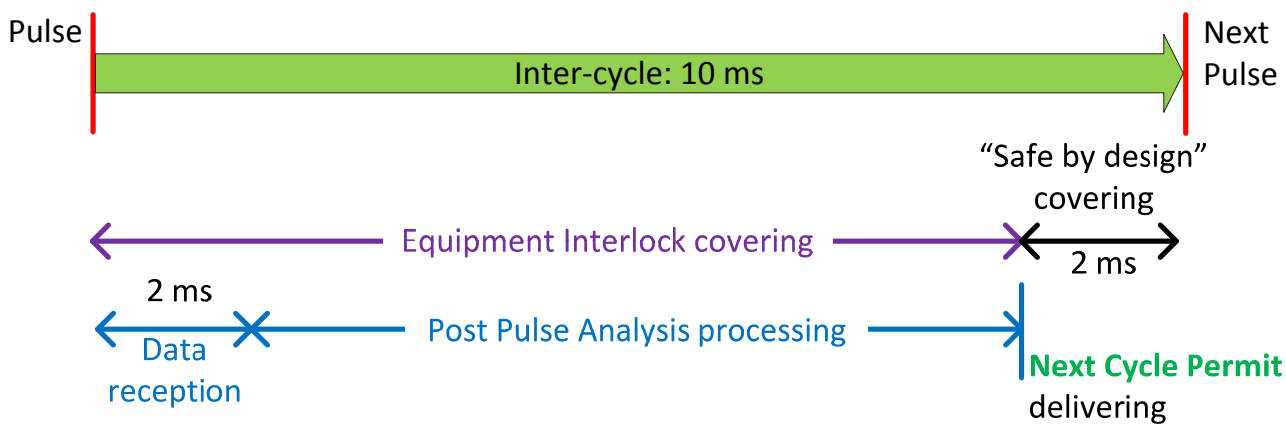
- First Experience at CTF3
- Prototype

Wrap-up

Requirements and Challenges

Response time

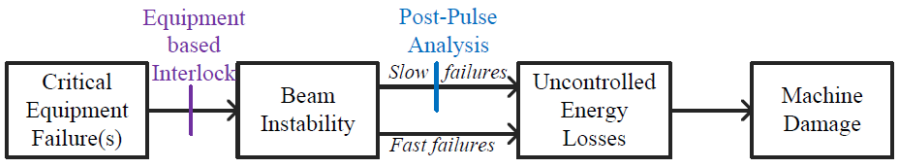
- **Equipment Interlock**: able to inhibit the next pulse in less than **2ms**
- **Post Pulse Analysis**: **6ms** to process data



Requirements and Challenges

Dependability study

- Risk identification
- Risk analysis, based on two methods:
  - Assumption on availability
  - Operational statistics
- Risk reduction: Failure mode
  - False PASS decision : **Machine safety**
  - False VETO decision: **Machine availability**
- Dependability attributes to be reached



Type of failure	Machine Failure Rate	impact
Critical Equipment	$2.65 * 10^{-7}$ pulse^{-1}	Catastrophic
	$4.78 * 10^{-1}$ mission^{-1}	
Slow Beam instability	$3.33 * 10^{-8}$ pulse^{-1}	
	$6 * 10^{-2}$ mission^{-1}	

Interlock System Failure Mode	Failure Rate	unavailability
False PASS decision	$5.23 * 10^{-7}$ pulse^{-1}	N/A (safety)
Transient false VETO decision	1 mission^{-1}	0.03 %
Permanent false VETO decision	2 year^{-1}	0.20 %

Attribute	Definition [3]	Value
Availability	readiness for correct service	99.75 %
Reliability (with transient)	number of failures over a period	$5.58 * 10^{-7}$ pulse^{-1}
	continuity of correct service	$1.8 * 10^{6}$ pulses
Reliability (without transient)	number of failures over a period	$2.79 * 10^{-9}$ pulse^{-1}
	continuity of correct service	$3.5 * 10^{8}$ pulses

Topics

Introduction

Principles

Requirements and Challenges

Specifications

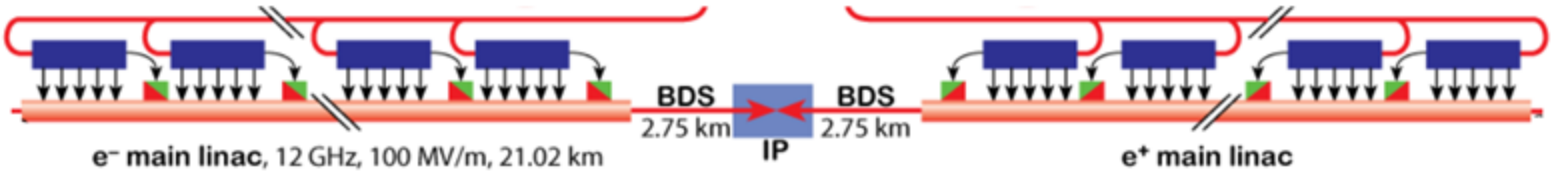
- Interface
- Design, Functions and Architecture

Validations ongoing

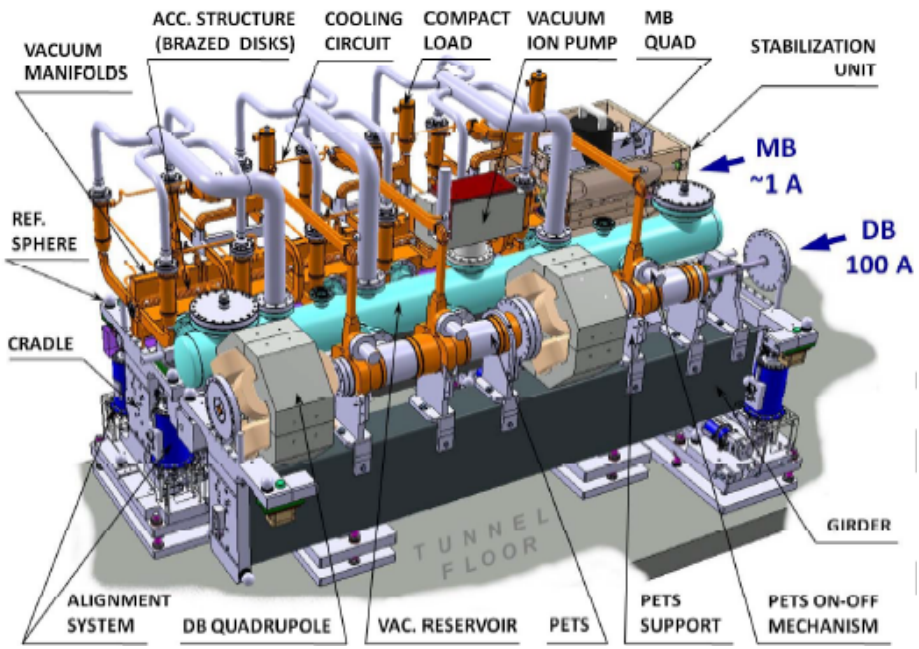
- First Experience at CTF3
- Prototype

Wrap-up

Interface with acquisition system



CLIC Main Linac



Acquisition and Control Module

X 22 000

CLIC Module (CLIC CDR chap 5.13 Control)

Interface with acquisition system

Example

Subsystem/Element	Description
BLM: 10-100m Fiber + PD	DB (2ch/fiber), 2 fibers
BLM: 10-100m Fiber + PD	MB (2ch/fiber), 2 fibers
Power Converter	2ch / Trimmer
RF Beam instrumentation	Module 0 (4xRF Unit)
RF: WakeField Monitor	All modules, config 0
RF: WakeField Monitor	Configuration 2
Stabilization: Positionning	Relative displacement
Vacuum Valve	status

Interface:

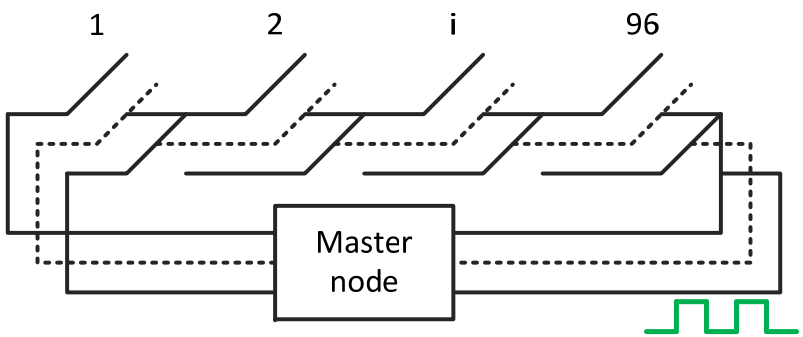
- 48 alcoves => 48 Machine Protection FECs
- Requirements from Machine protection to Acquisition system:
  - Redundancy on critical data
  - Low data corruption rate

*FEC: Front-End Computer
**ACM: Acquisition and Control Module

Design and Functions

Beam Permit Loop

- Master node: frequency generation
- Other nodes (FEC): switch
- Redundancy: defined regarding dependability study

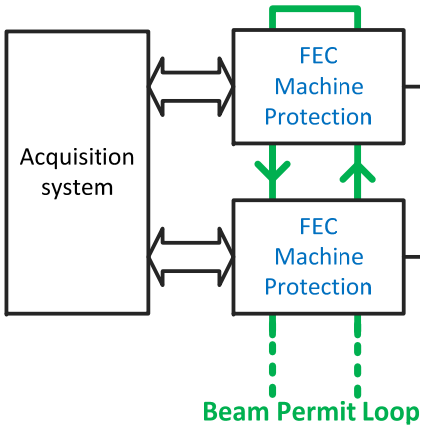


Thresholds comparison

- Standardized procedure for all data (equipment and beam quality related)
- Thresholds managed as Configuration Data

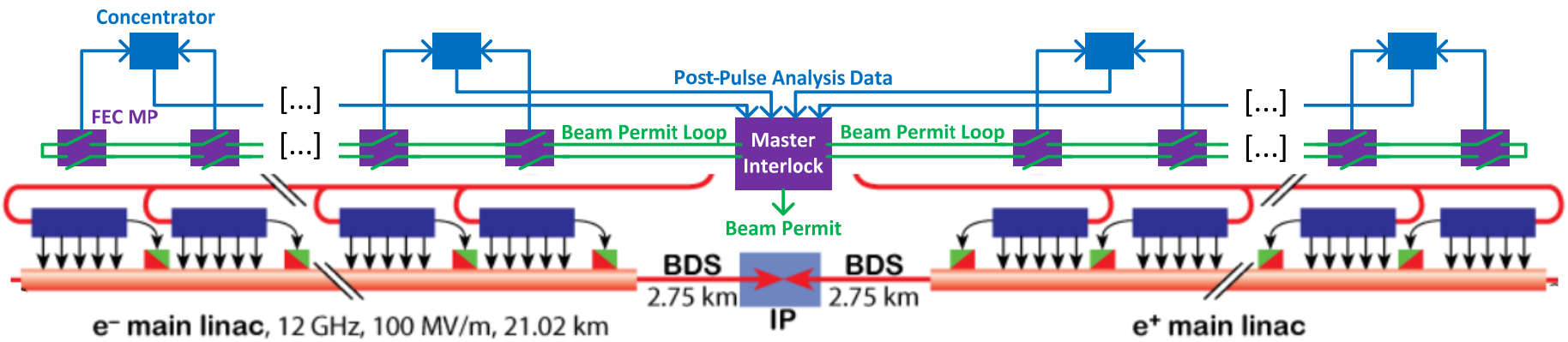
Global analysis

- Concentrator
- Glitch mitigation, local rules (masking)



Alcoves side

Architecture



Target Systems

- Drive Beam: Gun
- Main Beam: extraction kicker damping ring

Topics

Introduction

Principles

Requirements and Challenges

Specifications

- Interface
- Design, Functions and Architecture

Validations ongoing

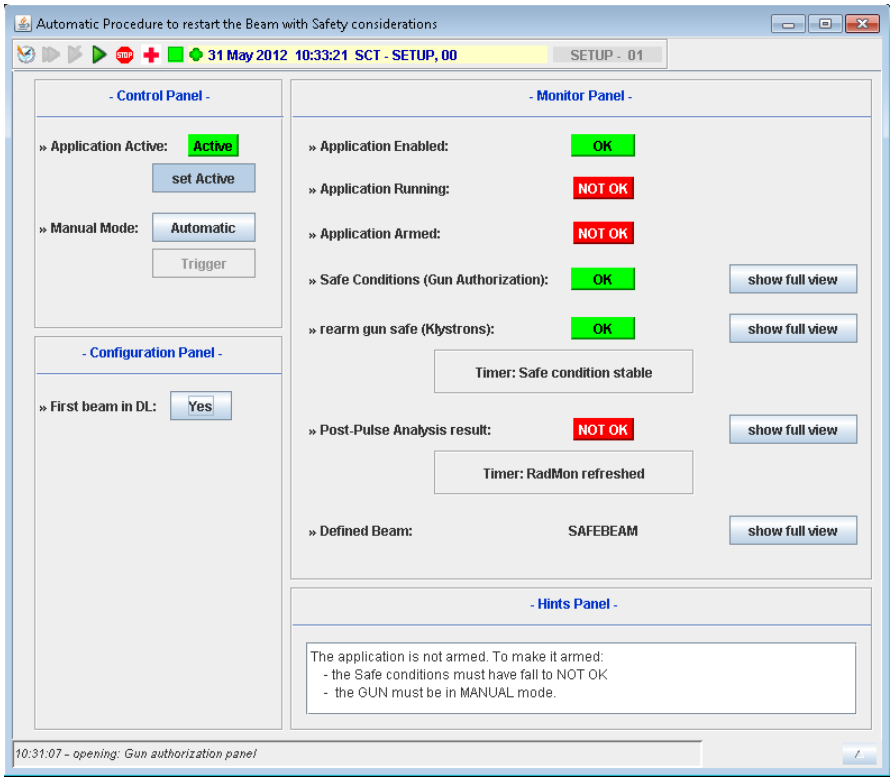
- First Experience at CTF3
- Prototype

Wrap-up

Post-Pulse Analysis at CTF3

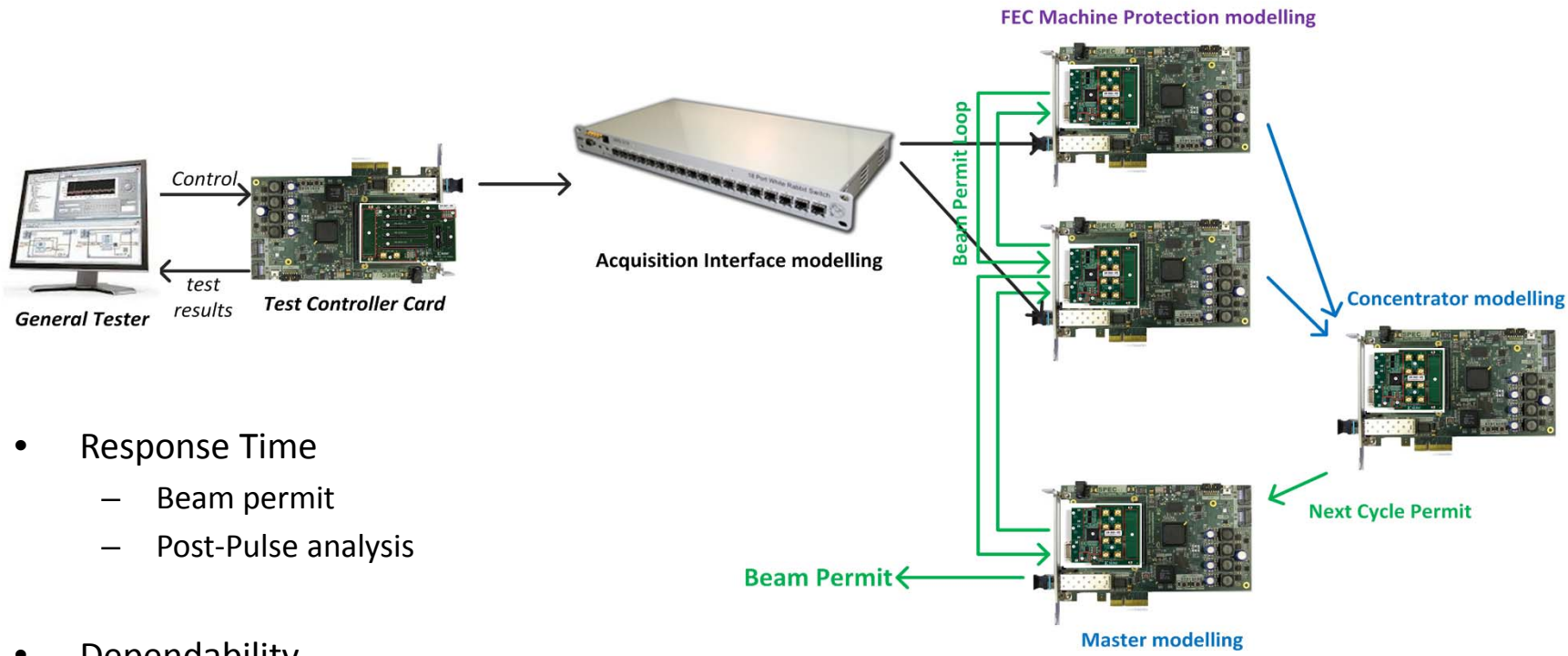
Beam sequencer based on post-pulse analysis

- Feasibility of Post-Pulse Analysis and first experience
- Software only (JAVA application)
- Applying the Post-Pulse Analysis Concept to ramp up the beam



Related Document=> EDMS 1182876

Interlock Systems Prototype



- Response Time
  - Beam permit
  - Post-Pulse analysis
- Dependability
  - Node characteristics (Failure rates)
  - Extrapolate to determine beam permit loop redundancy

Wrap up

System engineering process

- Concepts => requirements => specifications => validation
- Many iterations

Status

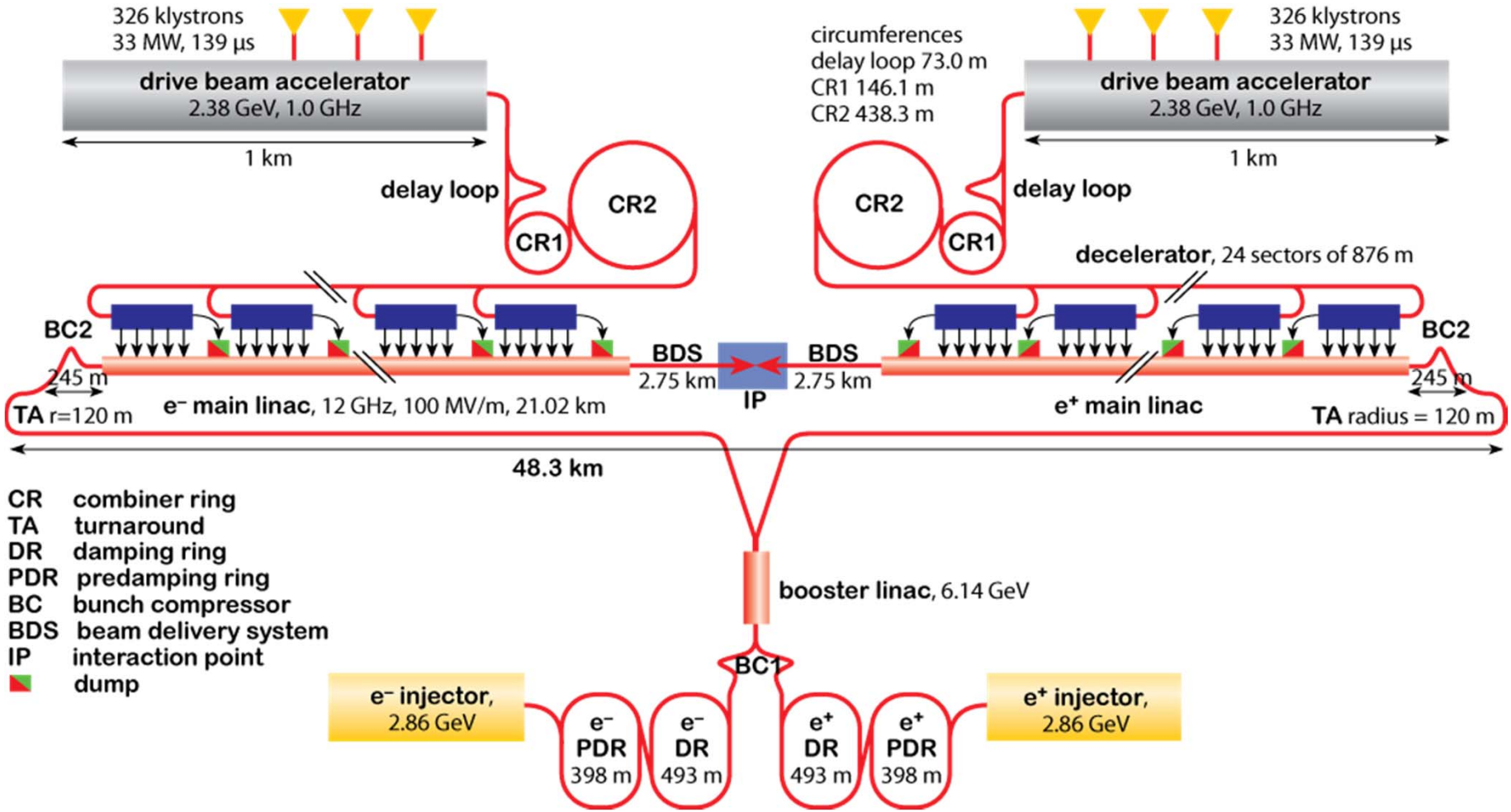
- Proof of concept at CTF3:
  - Test on going
- Prototype:
  - Response time reached: 320 µs to inhibit the next pulse

Thanks for your attention

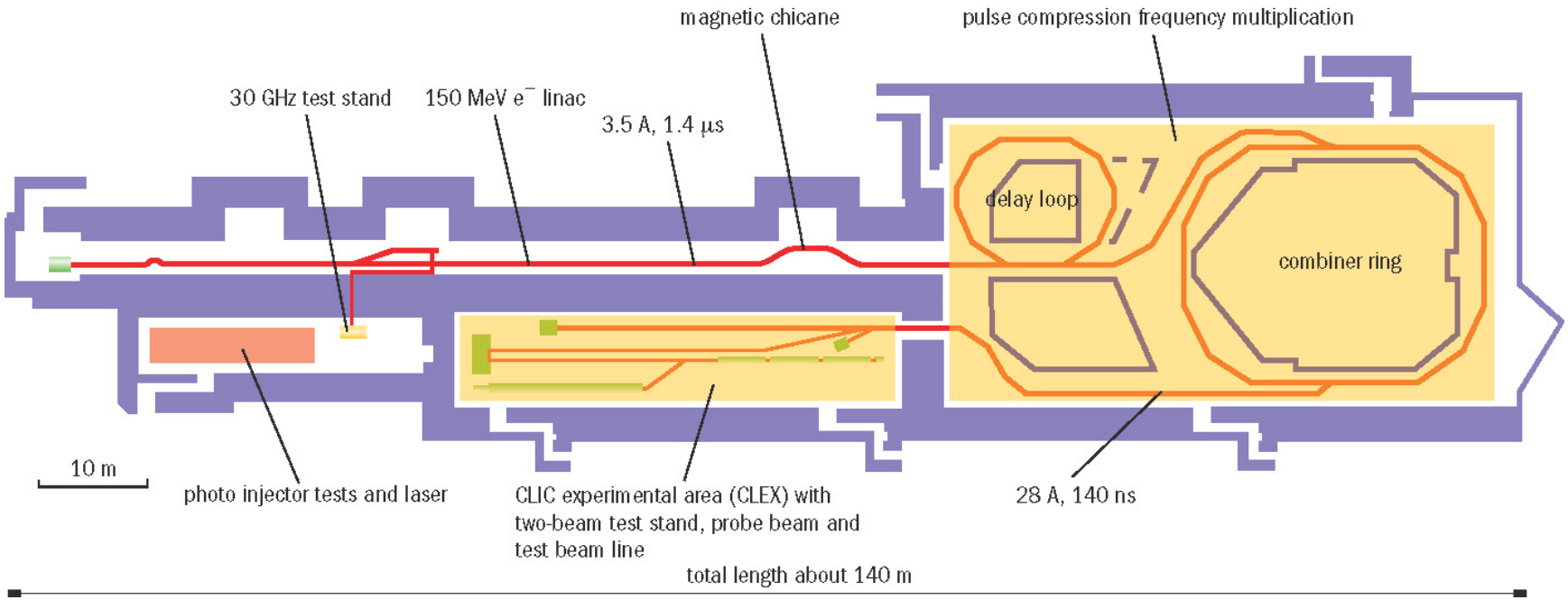
Questions and remarks are welcome

Spare slides

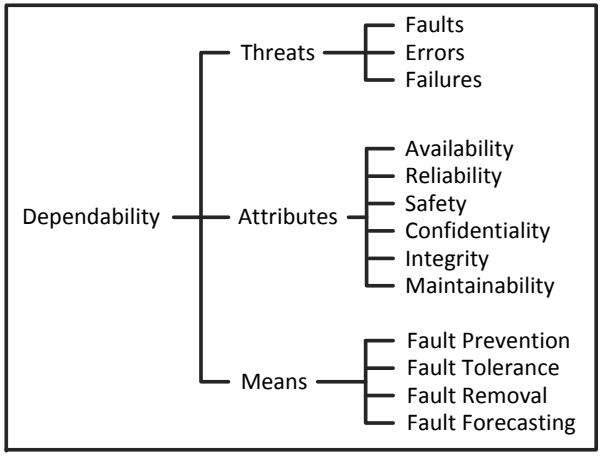
CLIC Layout


326 klystrons
33 MW, 139 μs
drive beam accelerator
2.38 GeV, 1.0 GHz
1 km
delay loop
CR1
CR2
circumferences
delay loop 73.0 m
CR1 146.1 m
CR2 438.3 m
326 klystrons
33 MW, 139 μs
drive beam accelerator
2.38 GeV, 1.0 GHz
1 km
CR2
CR1
delay loop
decelerator, 24 sectors of 876 m
BC2
245 m
TA r=120 m
e⁻ main linac, 12 GHz, 100 MV/m, 21.02 km
BDS
2.75 km
IP
BDS
2.75 km
e⁺ main linac
BC2
245 m
TA radius = 120 m
48.3 km
CR combiner ring
TA turnaround
DR damping ring
PDR predamping ring
BC bunch compressor
BDS beam delivery system
IP interaction point
dump
booster linac, 6.14 GeV
BC1
e⁻ injector,
2.86 GeV
e⁻
PDR
398 m
e⁻
DR
493 m
e⁺
DR
493 m
e⁺
PDR
398 m
e⁺ injector,
2.86 GeV

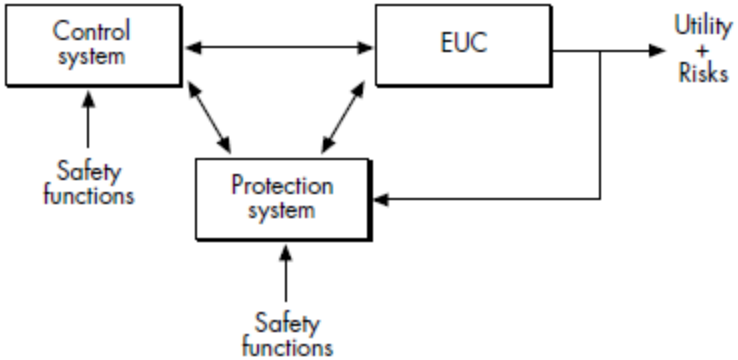
CTF3 Layout


magnetic chicane
pulse compression frequency multiplication
30 GHz test stand
150 MeV e⁻ linac
3.5 A, 1.4 μs
delay loop
combiner ring
10 m
photo injector tests and laser
CLIC experimental area (CLEX) with
two-beam test stand, probe beam and
test beam line
28 A, 140 ns
total length about 140 m

Dependability concept definition



Adapted from: "Functional Concepts of Dependability", A.Avizienis, J.C.Laprie, B.Randell



MTL Application Note: An introduction to Functional Safety and IEC 61508

Requirements for Control system: Machine Safety

- Failure mode: data corruption on critical interlock request
- **Tolerable risk** of 1 catastrophic event every 10^4 years (1.39×10^{-13}/pulse)

- Method 1 (based on operational year 2011)
  - 48.7% of missions (10h) aborted by critical equipment failures
  - 6% of missions (10h) aborted by beam instabilities
  - **Probability of Interlock request: 3×10^{-7}/pulse**

- Method 2 (based on assumptions on availability) – For comparison (don't include equipment failure)
  - 1 instable pulse leads to 10s downtime (interlock and ramp up)
  - Less 10% downtime is acceptable => 1 instable pulse every 100s
  - 1% of instable pulses are critical (leading to structure damage)
  - **Probability of Interlock request due to critical instable pulse: 2×10^{-6}/pulse**

- **Probability of Control system to *corrupt data* must be lower than**:
  - **4.6×10^{-7}/pulse** (method 1)
  - **7×10^{-8}/pulse** (method 2 – no equipment request)