STPA FOR LINAC4 AVAILABILITY REQUIREMENTS

A. **Apollonio,** R. Schmidt

4th European STAMP Workshop, Zurich, 2016


LHC colliding particle beams at very high energy
26.8 km Circumference
LHC Accelerator
(100 m down)
Switzerland
Lake Geneva
CMS
LHCb
ALICE
SPS Accelerator
ATLAS
France

CERN: Accelerators and Experiments

- CERN provides the world's largest and **most complex scientific instruments** to study the constituents of matter
- These instruments are **particle accelerators** and **experiments**
- **Accelerators** boost beams of elementary particles to high energies before they are made to **collide with each other**
- **Experiments observe** and record the results of these **collisions**

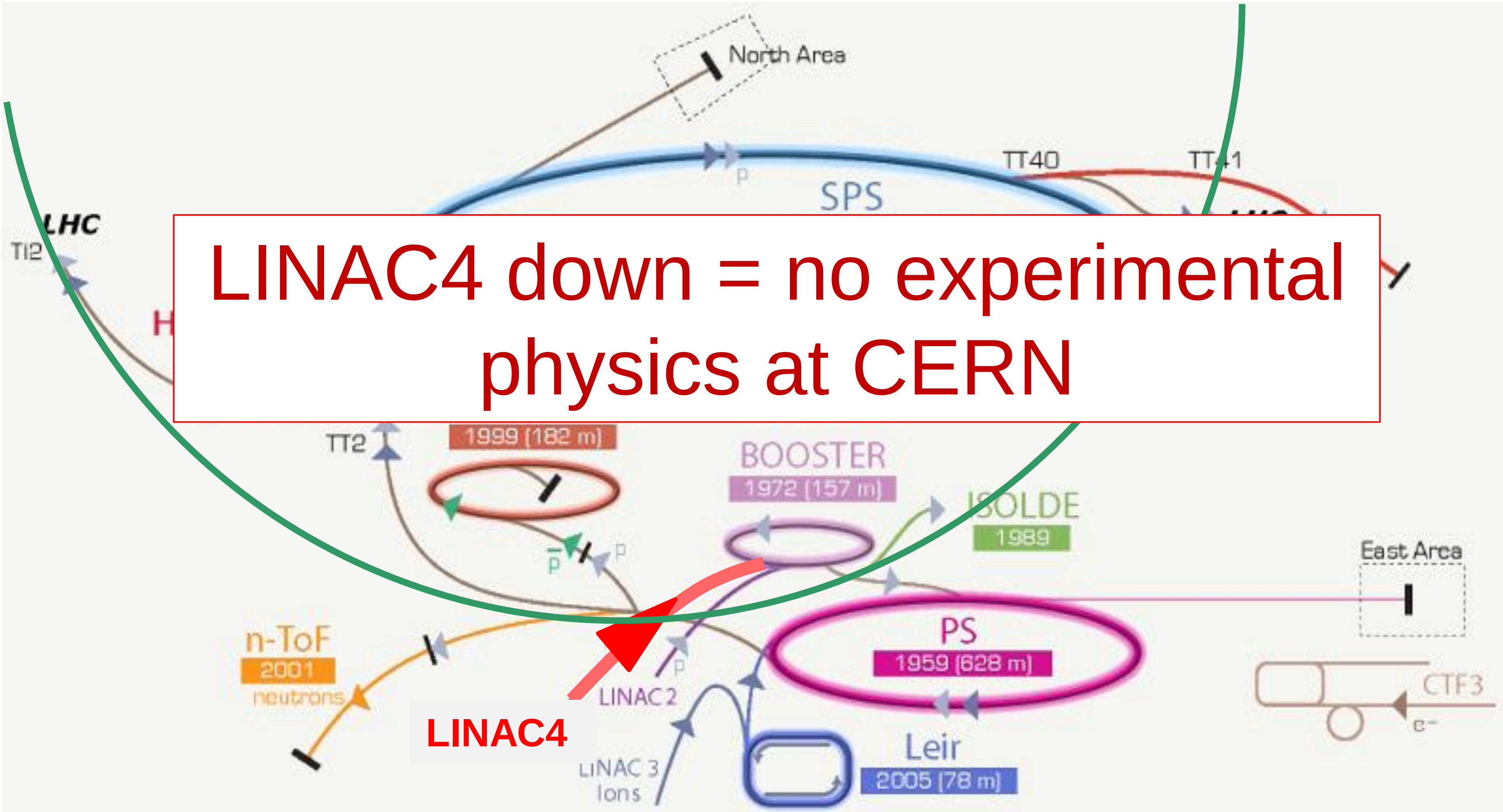
Our flag-ship project is the Large Hadron Collider…

- **LHC relies on** the **reliable operation** of the injectors, e.g. **LINAC4**

CERN is a research institute

All work at CERN can be openly published without limitations – interesting aspect for collaborations with University Groups

CERN: Particle Injector Chain



LINAC4 down = no experimental physics at CERN

LINAC4 provides beam for LHC and several other experiments

Risks for Particle Accelerators

- **Not to complete** the construction of the accelerator
  - Happened to other projects, the most expensive was the Superconducting Super Collider in Texas / USA with a length of ~80 km
  - Cost increase from 4.4 Billion US$ to 12 Billion US$, US congress stopped the project in 1993 after having invested more the 2 Billion US$

- **Not** to be able **to operate** the accelerator
- **Damage** to the accelerator **beyond repair** due to an accident

NO LHC: Future of Particle Physics compromised

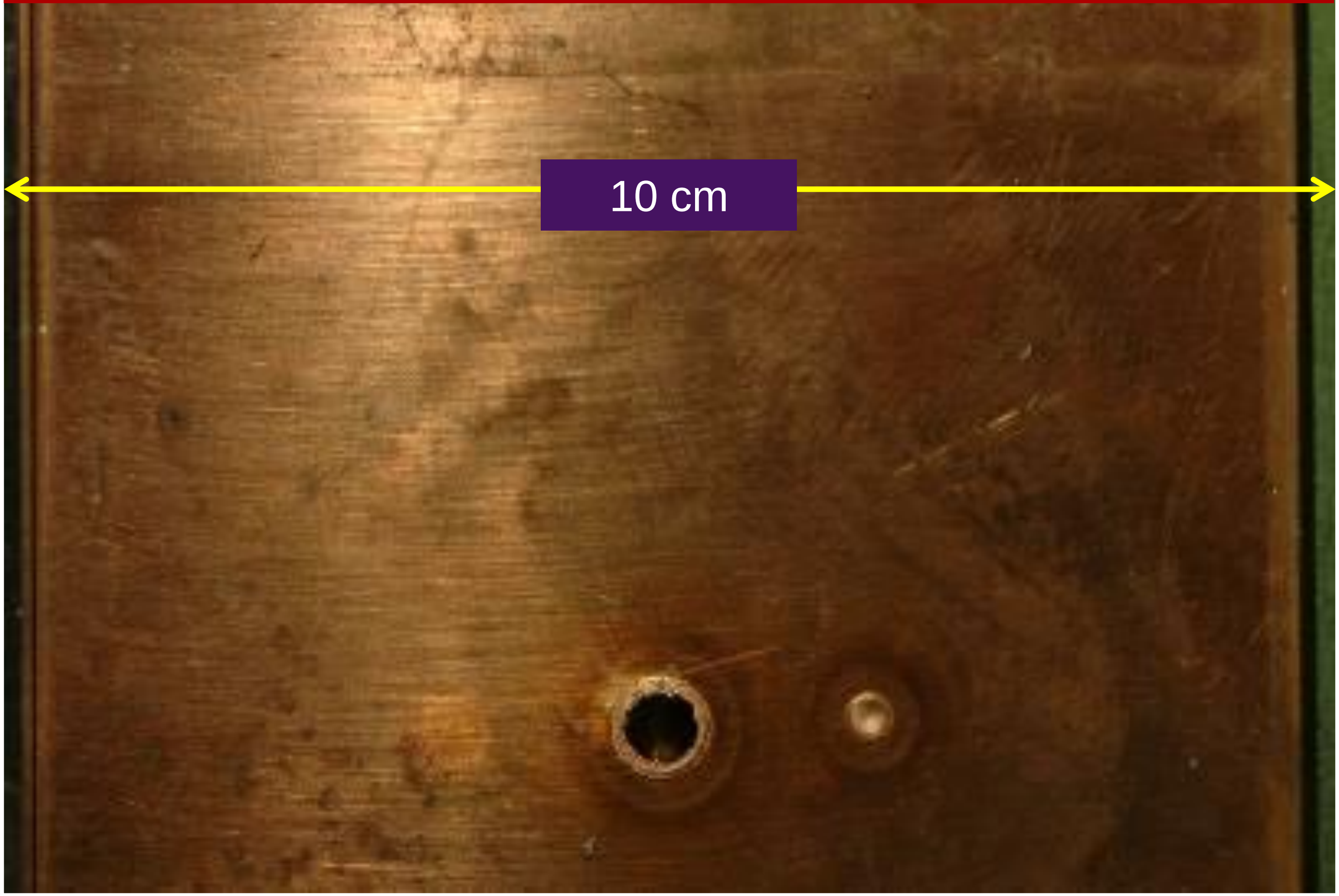
LHC: Hazards and Machine Protection

- Safety-critical:
  - 362 MJ stored beam energy
  - 9 GJ energy stored in the magnet powering system
- Complex:
  - Severa
  - Mix of … s,
    proced
- **LHC is the … protection is mission**
- Need for a
  requireme

- STPA was not used to develop the LHC MPS ….15 years ago

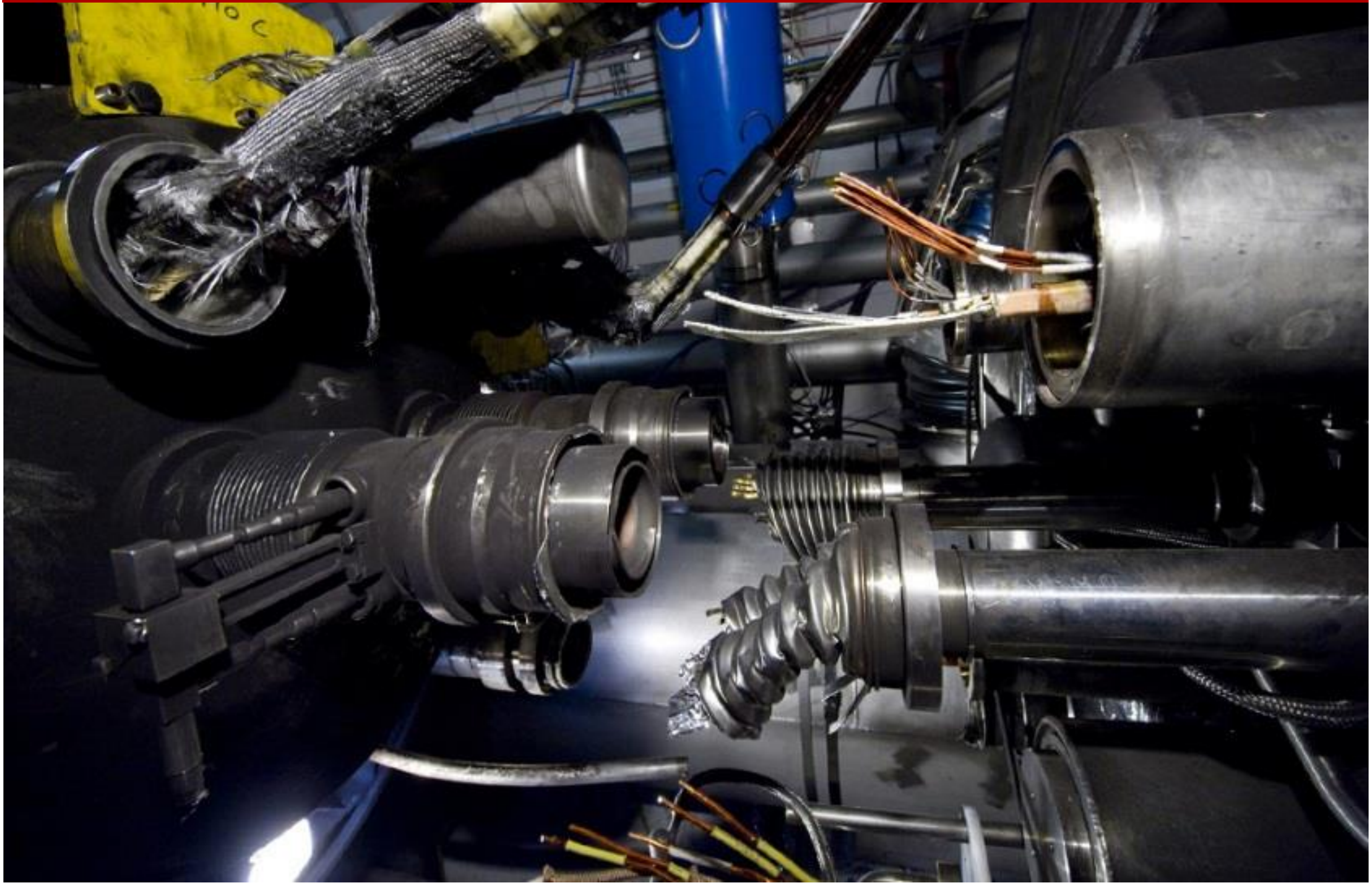
Addressing beam induced damage

Effect of 0.1% of the LHC beam energy on copper target (Experiment at SPS)

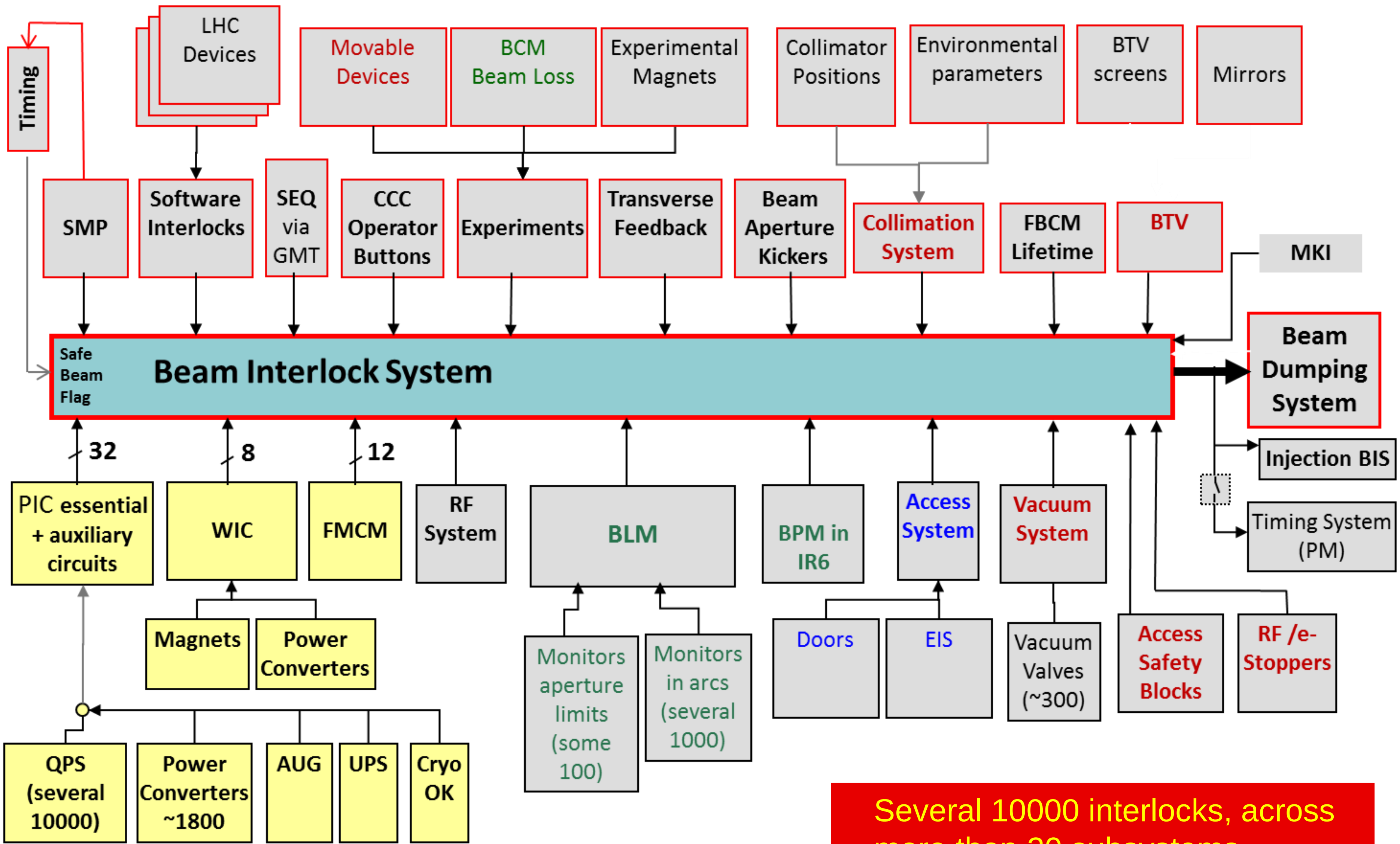


LHC: Real Accident without beam

Arcing in the interconnection in 2008 at LHC



LHC MPS to prevent beam accidents



Several 10000 interlocks, across more than 20 subsystems

Design principles for protection systems

- Efficient accelerator operation

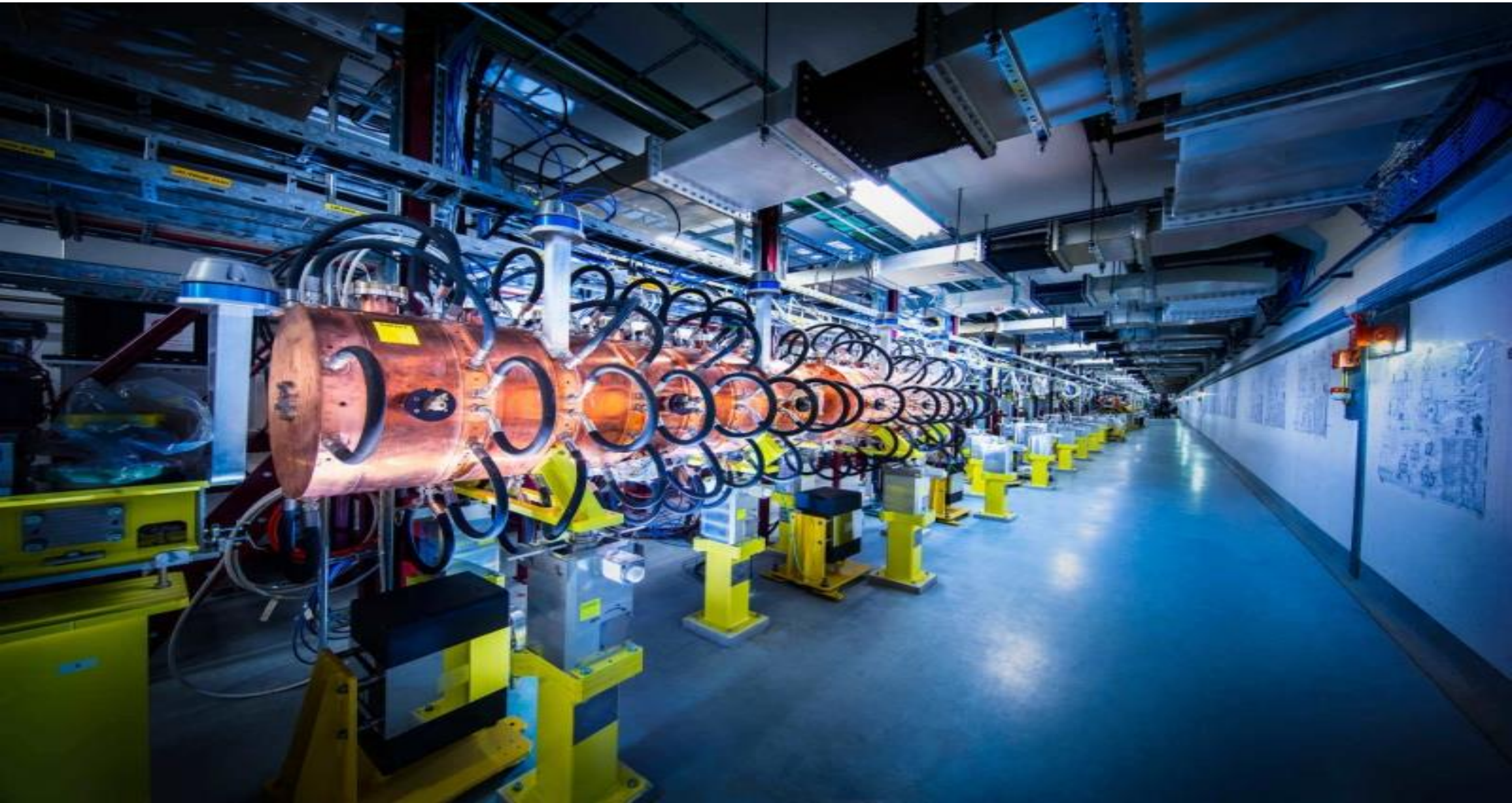
  Priority 1: Avoid accidents (reducing availability and introducing repair cost)

  Priority 2: Operate with high availability

- Failsafe design
  - detect internal faults
  - if the protection system does not work, better stop operation rather than damage equipment (affecting availability)
- Excellent diagnostics
  - recording all failures
- Flexibility: managing interlocks
  - disabling of interlocks is common practice **(keep track!)**
  - LHC: masking of some interlocks possible for low intensity / low energy beams

LINAC 4

- New injector for the CERN accelerator complex
- Being commissioned, regular operation starting in next years



Motivation for the use of STPA

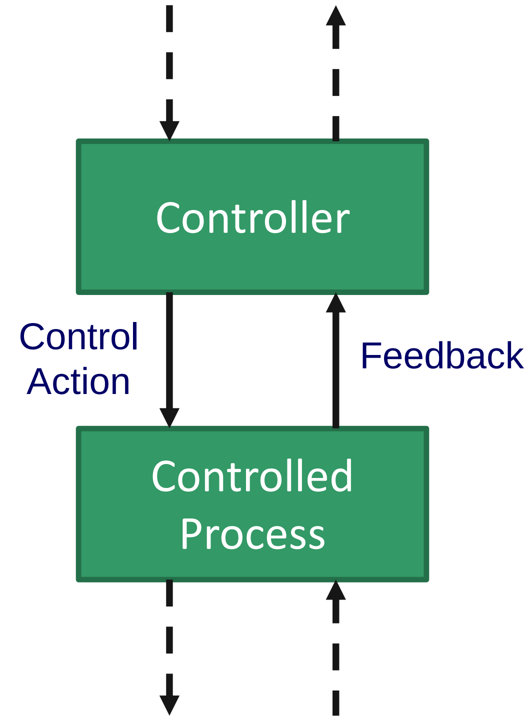
- Increasing **accelerator complexity** requires a systematic approach for identification of machine protection requirements
  - Address and optimize **contradictory requirements** (safety vs availability)
  - Applicable from **early design** stages (not applied to a given design)
  - Results should not regard only the **system architecture**, but also provide recommendations for correct **operation and management** of the accelerator

- Long-term goal
  - Identify suitable method for the design of machine protection systems for the **next generation** of particle accelerators

- As a start…
  - Apply method for the **first time to a small accelerator** to verify its suitability → LINAC4

STPA steps

- Step 1: Identify **accidents** and **hazards**
- Step 2: Draw the **control structure**
  - Controller + controlled process
  - Control actions + feedback
- Step 3: Identify **Unsafe Control Actions**
- Step 4: Identify **Causal Factors**
- (Step 5: Iterate 1 to 4 until suitable mitigation is found)



J. Thomas, RSRA2015

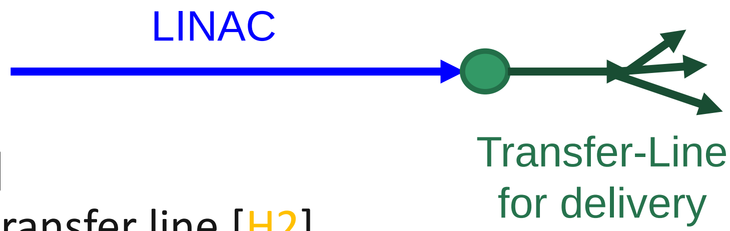
Step 1: LINAC4 Accidents and Hazards

ACCIDENTS:

- A1: Lack of beam for other accelerators
- A2: Damage to accelerator equipment
- A3: Injuries to staff members
- A4: Release of radioactive material in the environment

HAZARDS (only related to A1):

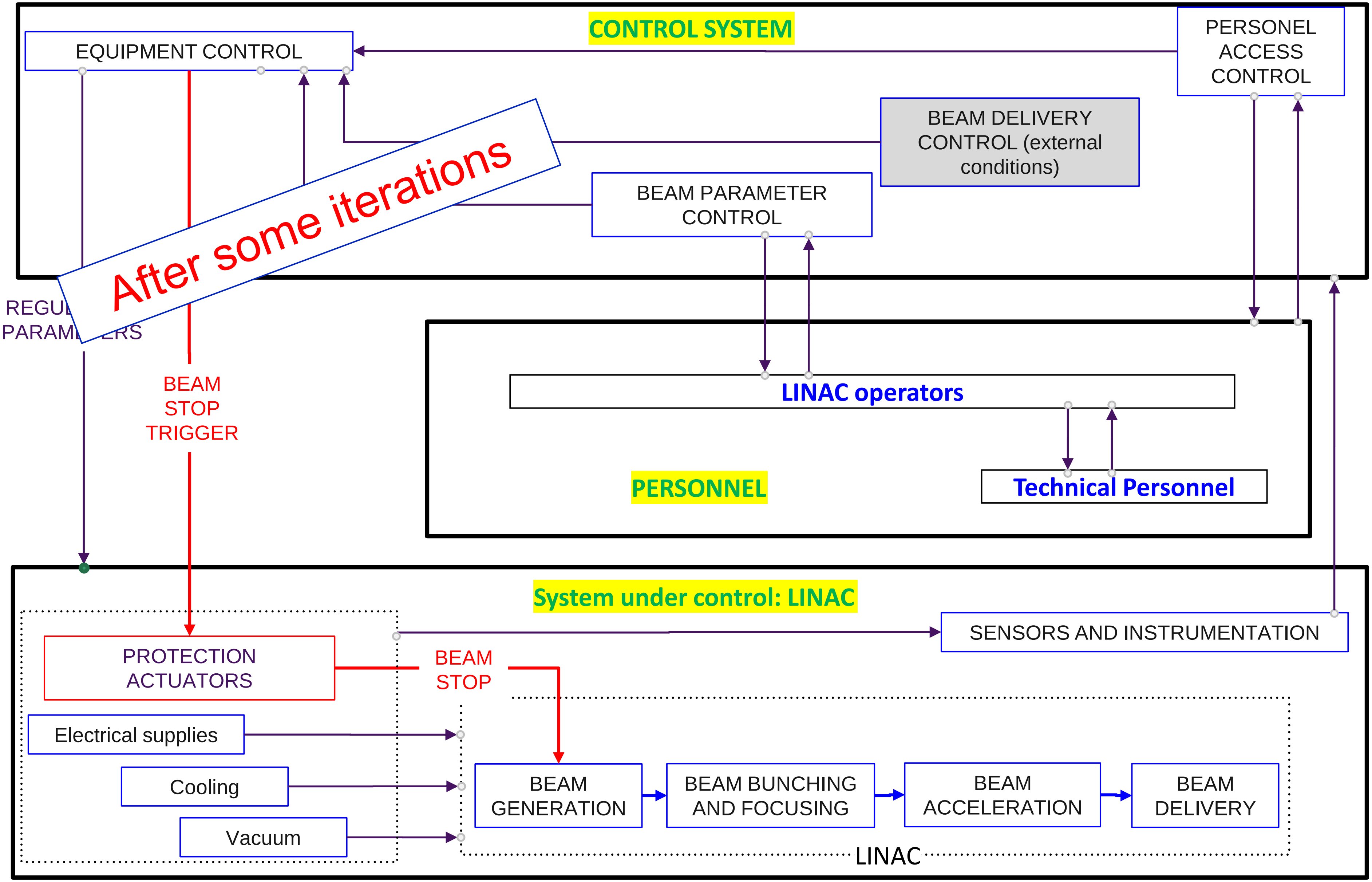
- H1: Accelerator equipment is not ready for operation [A1, A2]
- H2: Beam is lost before reaching the transfer line [A1, A2]
- H3: Beam is stopped before reaching the transfer line when it is not necessary [A1]
- H4: Beam doesn’t have the required quality for following accelerators [A1]



REQUIREMENTS:

- R1: Accelerator equipment must be operational [H1]
- R2: The beam must not be lost before reaching the transfer line [H2]
- R3: The beam must not be stopped when it is not necessary [H3]
- R4: The beam must have the required quality for following accelerators [H4]

Step 2: LINAC4 Control Structure



Step 3: "Unsafe" (unwanted) Control Actions

Control Action	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong order	Stopped too soon/applied too long
Beam stop	UCA2, UCA4, UCA5, UCA2	**UCA1**	UCA3	-

UCA1: The beam is stopped when it is not necessary (automatically or by an operator)

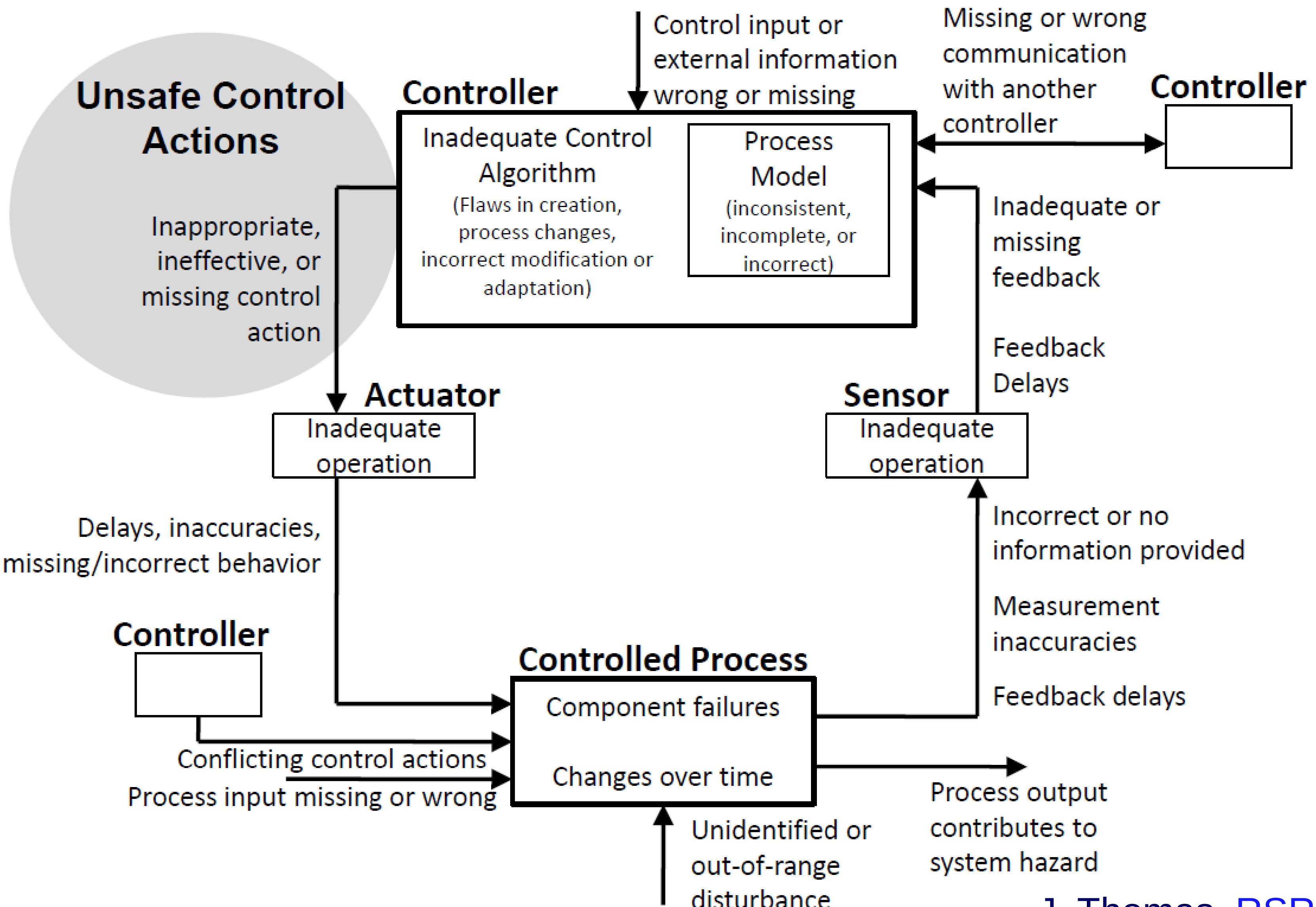
UCA2: The beam is not stopped in a detected emergency situation (automatically or by an operator) due to the unavailability of an actuator

UCA3: The beam is not stopped while personnel has access to the linac

UCA4: The beam is not stopped following the missed detection of an undesirable accelerator configuration

UCA5: The beam is not stopped when the beam quality is not sufficient for following accelerators

Identify Causal Factors



J. Thomas, [RSRA2015]

Step 4: Causal Factors

Scenario

Control input or external information wrong or missing: Operator triggers an unnecessary beam stop

Associated Causal Factors

Operator accidentally acts on the physical device connected to the controller

Notes

The emergency button in the control room is accidentally pushed

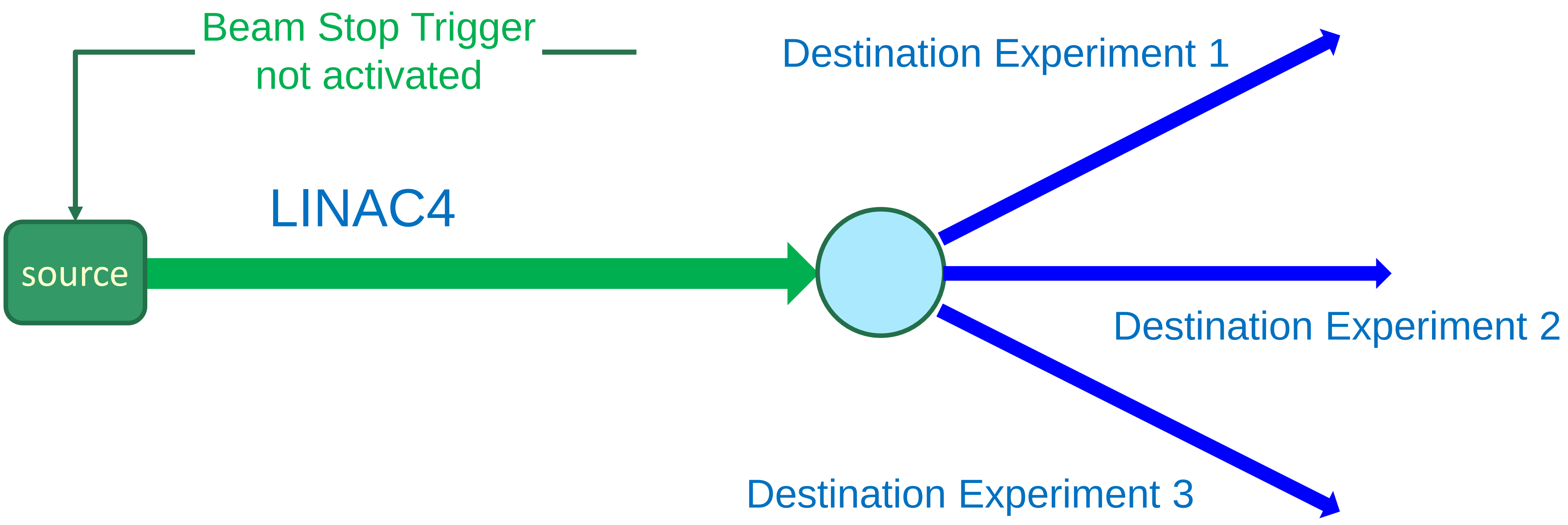
Requirements

Protect the physical device from accidental contact

	…ctors	Notes	Requirements
	…o is executed when it is not necessary		
	…y act …e	The emergency button in the control room is accidentally …	Protect the physical device …dental contact
	Operator misinte… feedback from instrumentation … trigger the beam		…rators to use …and processes …n the control room. …improving GUI.
	Operator execute… command that triggers a dangerous situation and thus a beam stop.	beam or hardware … this leads to a dang… that requires a bea…	…rators to use
	Technical personnel tries to access the linac while it is working, causing a beam stop.	Technical personne… that the machine is … tries to access it.	
Sensor - Inadequate or missing feedback: The sensor feedback is wrong and automatically triggers a beam stop.	Sensor is faulty and causes a beam stop.	A sensor gives wro… information and determines that a beam stopi s needed, even if no direct machine harm exists.	A ded… can as… senso… occur…
	Spurious trigger of a sensor causing a beam stop.	A sensor signals a hazardous operating condition due to a spurious failure (e.g. radiation-induced).	Consi… When… and in… radiat…

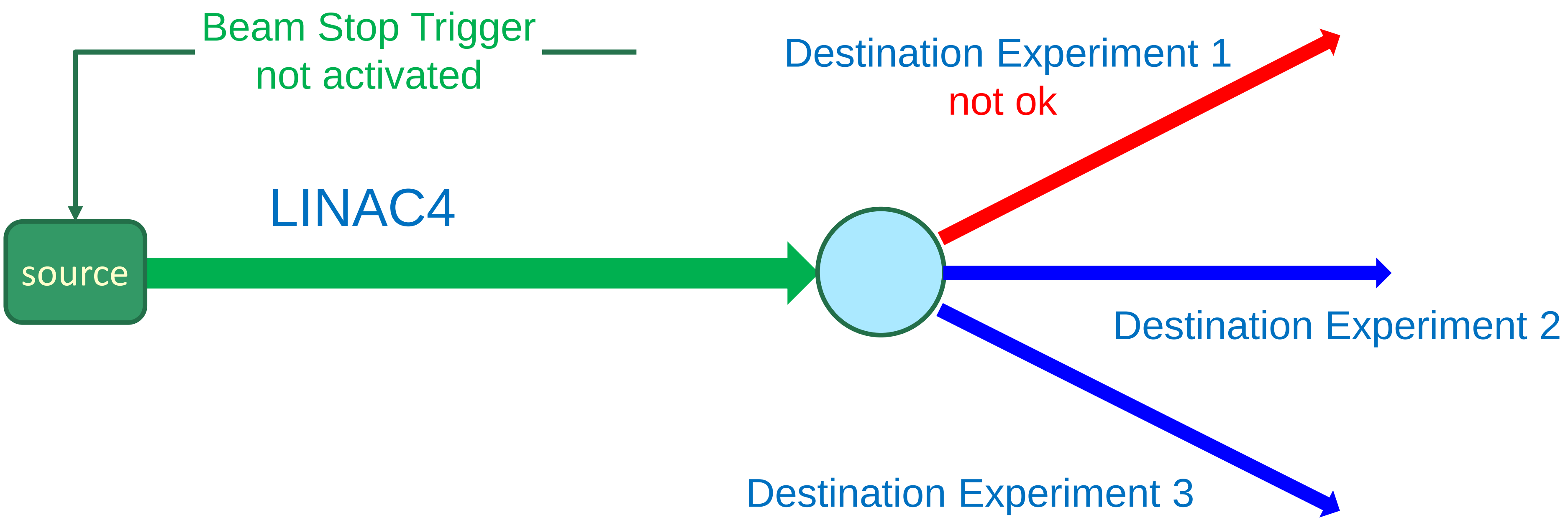
- **‘Practical’ measures**
- **Managerial and organizational measures**
- **…ral …es**

Machine Protection System for LINAC4



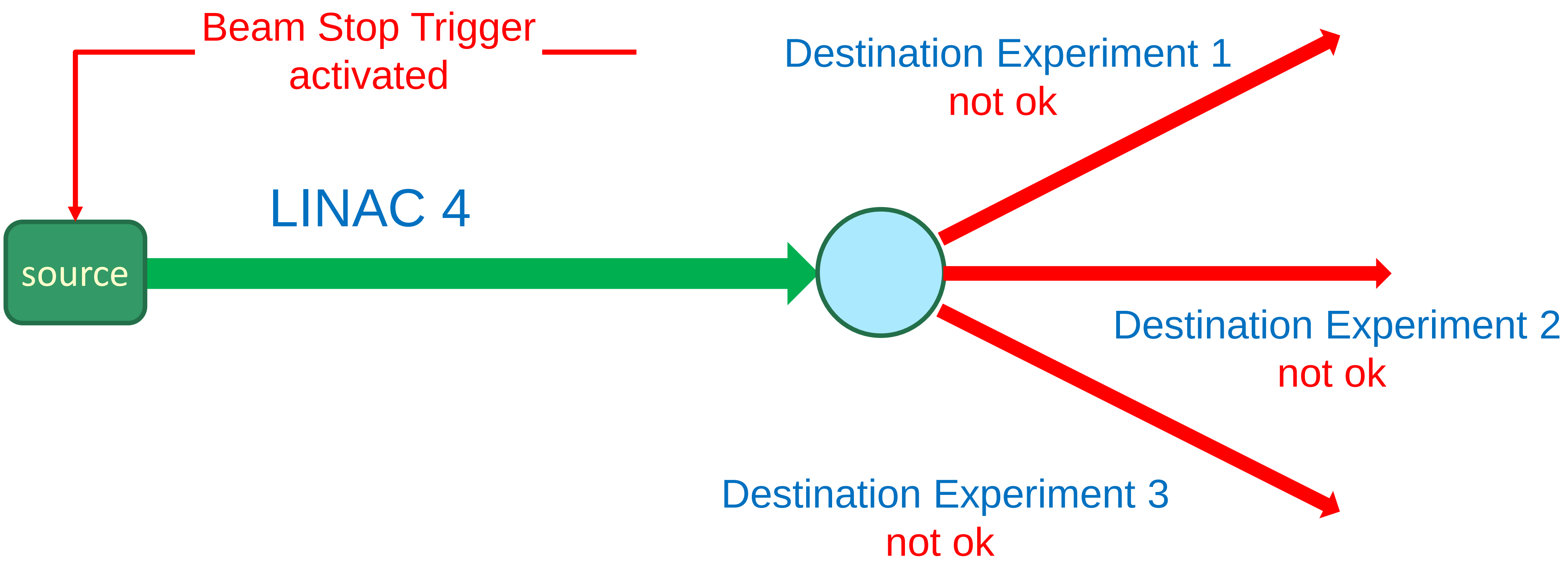
Beam can be send to all destinations

Machine Protection System for LINAC4



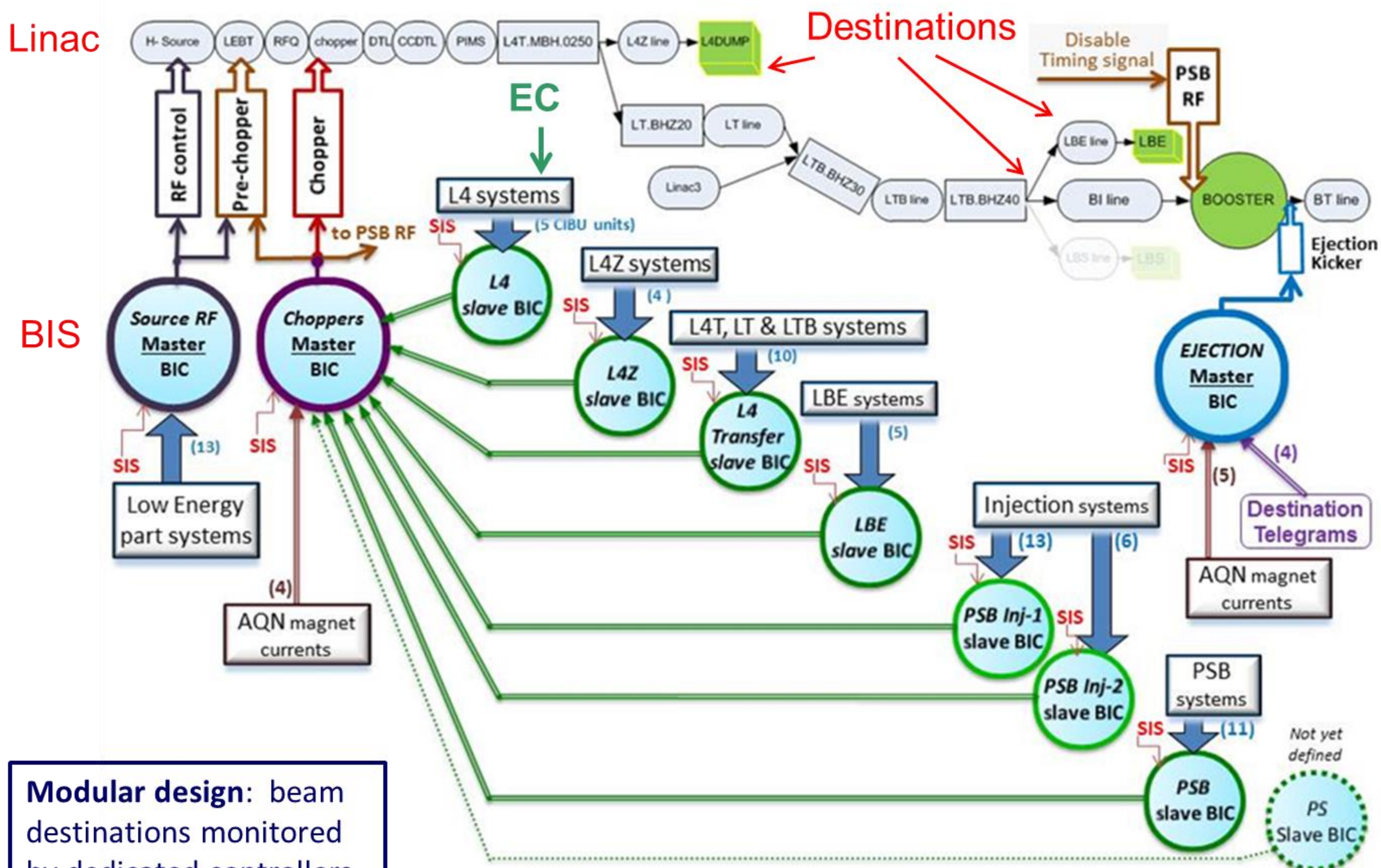
Beam can be send to destination 2 and 3

Machine Protection System for LINAC4



Beam stopped at the source

LINAC4 Machine Protection



Modular design: beam destinations monitored by dedicated controllers

BIS Linac4 & PSB layout

Main outcome of LINAC4 STPA

- Availability-oriented design of the Machine Protection System
  - Modular design of MPS → **Tree-like Architecture**
  - Management of beam destinations → **External conditions**
  - Flexibility of MPS → **Software Interlock System**

- Procedural/managerial measures
  - Definition of a **MPS responsible** for approval of changes/settings of the MPS
  - Document for **MPS requirements** during LINAC4 **commissioning**

Experience from LINAC4

- STPA: suitable tool for hazard analysis of safety-critical systems in accelerators
  - Allows dealing with increasing system complexity
  - Results go beyond requirements for hardware design

- Successful application to LINAC4 MPS
  - Set of availability requirements
  - Impact on LINAC4 MPS architecture design

- Needs to be complemented by other tools (e.g. fault trees etc.)
  - In particular for sub-systems / components
  - Numbers can still be very useful…

….. and from LHC

- LHC Machine Protection Global Design has been done in a somewhat similar way as STPA (starting with top-down approach), without using the formalism, complemented by traditional methods for subsystems
- General approach to Machine Protection
  - Protect the Equipment
  - Protect the Beam
  - Provide the Evidence
- Independently from the method: spread **Safety Culture** for particle accelerators (at CERN helped by the 2008 accident)

LHC produce excellent results

The Nobel Prize in Physics 2013

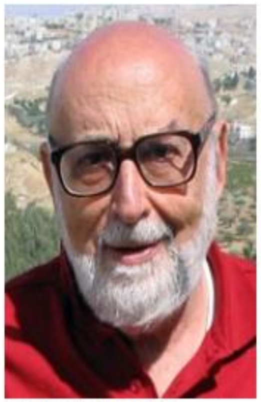


Photo: Pnicolet via Wikimedia Commons

François Englert

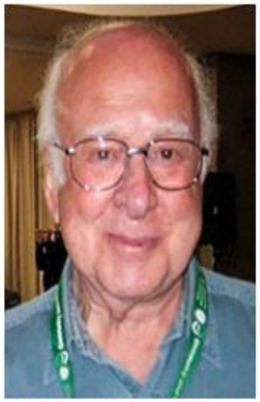


Photo: G-M Greuel via Wikimedia Commons

Peter W. Higgs

The Nobel Prize in Physics 2013 was awarded jointly to François Englert and Peter W. Higgs *"for the theoretical discovery of a mechanism that contributes to our understanding of the origin of mass of subatomic particles, and which recently was confirmed through the discovery of the predicted fundamental particle, by the ATLAS and CMS experiments at CERN's Large Hadron Collider"*

References:

- J. Thomas, “The Reliability and System Risk Analysis (RSRA) Workshop”, CERN, 2015 (link)
- N. Leveson, “An STPA primer” (link)
- A. Apollonio, “Machine Protection: Availability for Particle Accelerators” (link)
- A-STPA, University of Stuttgart (link)