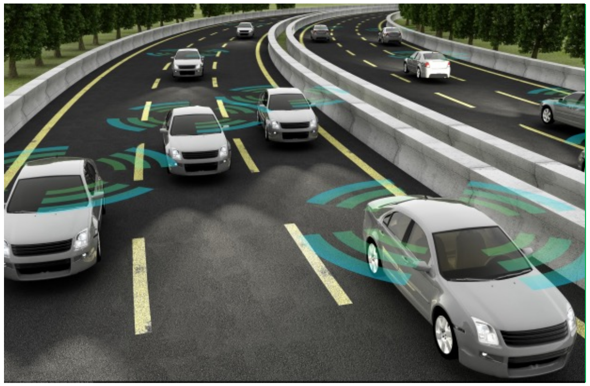
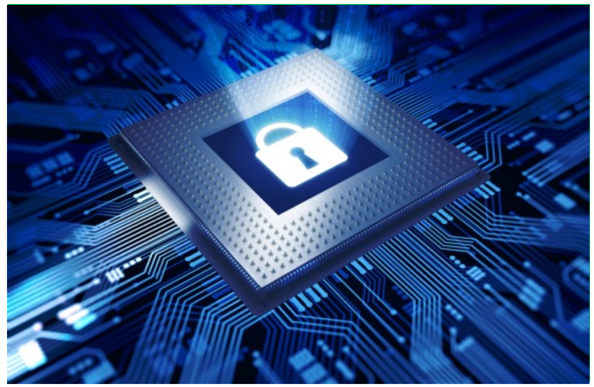
Critical Systems Labs
Strategic Insight for Safety

CERN LHC Machine Protection Assurance Case Argument – Assurance grounded in technical understanding rather than process compliance

Jeff Joyce, Laure Millet, Chris Reese, and Simon Diemert

LM

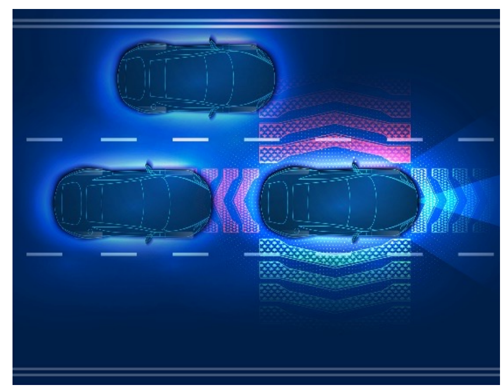
Critical Systems Labs Inc.









Critical Systems Labs
Strategic Insight for Safety

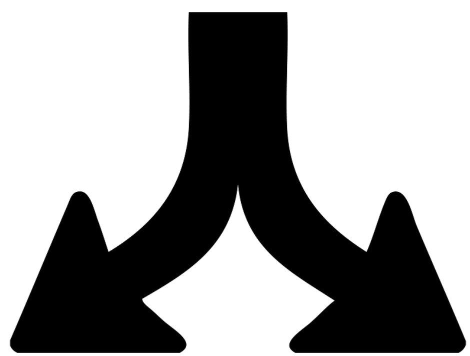
Abstract

A fundamental question regarding assuring safety of complex critical system is the extent to which the structure of an assurance case argument should be shaped around a technical understanding of how risk is controlled by the design, in contrast to an argument focused on compliance with requirements specified in a standard or other form of published guidance. This difference is sometimes referred to as a "product" versus a "process" argument. Through collaboration with researchers and technical staff at the University of Toronto, McMaster University and the European Organization for Nuclear Research (CERN), Critical Systems Labs (CSL) has developed a large assurance case argument for the CERN Large Hadron Collider (LHC) Machine Protection System (MPS). This 500+ node argument, which is publicly available on the CERN website, is meant to reflect the systematic thinking of the CERN technical staff during the development of this system that underlies their trust in this complex system. This argument relies on a dialectical approach, Eliminative Argumentation, to probe deeply into technical details to expose potential doubts and questions that would have surfaced during development.

LM

A Fundamental Question …

To what extent should the structure of an assurance case argument be shaped around a technical understanding of how risk is controlled by the design?



Process Argument | Product Argument

Process vs. Product

Process Argument

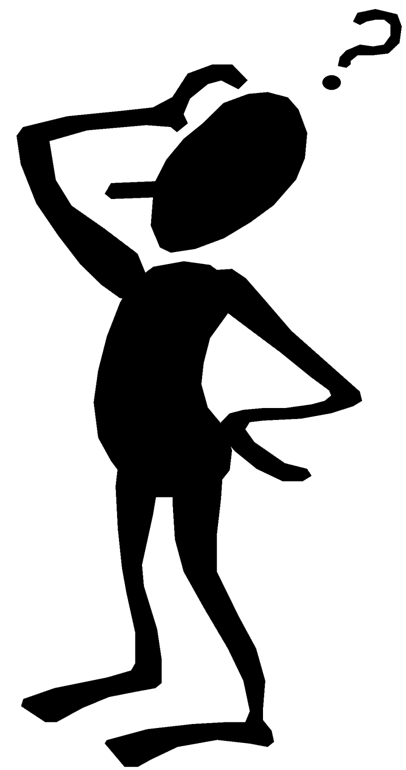
- Driven by compliance with requirements of a standard, or other guidance
- Primary inputs are typically organizations process definitions
- Principal contributors are often assurance experts

Product Argument

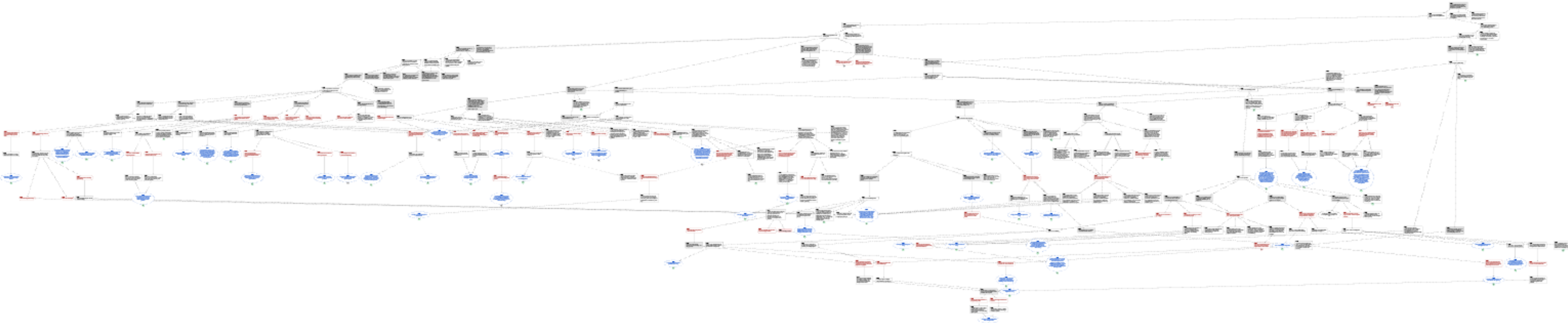
- Driven by a technical understanding of how risk is controlled by the design
- Primary inputs are typically engineering artifacts, e.g., functional requirements
- Principal contributors are Subject Matter Experts (SME)

Unlike a product argument, a process argument can be developed with little or no understanding of the technical design

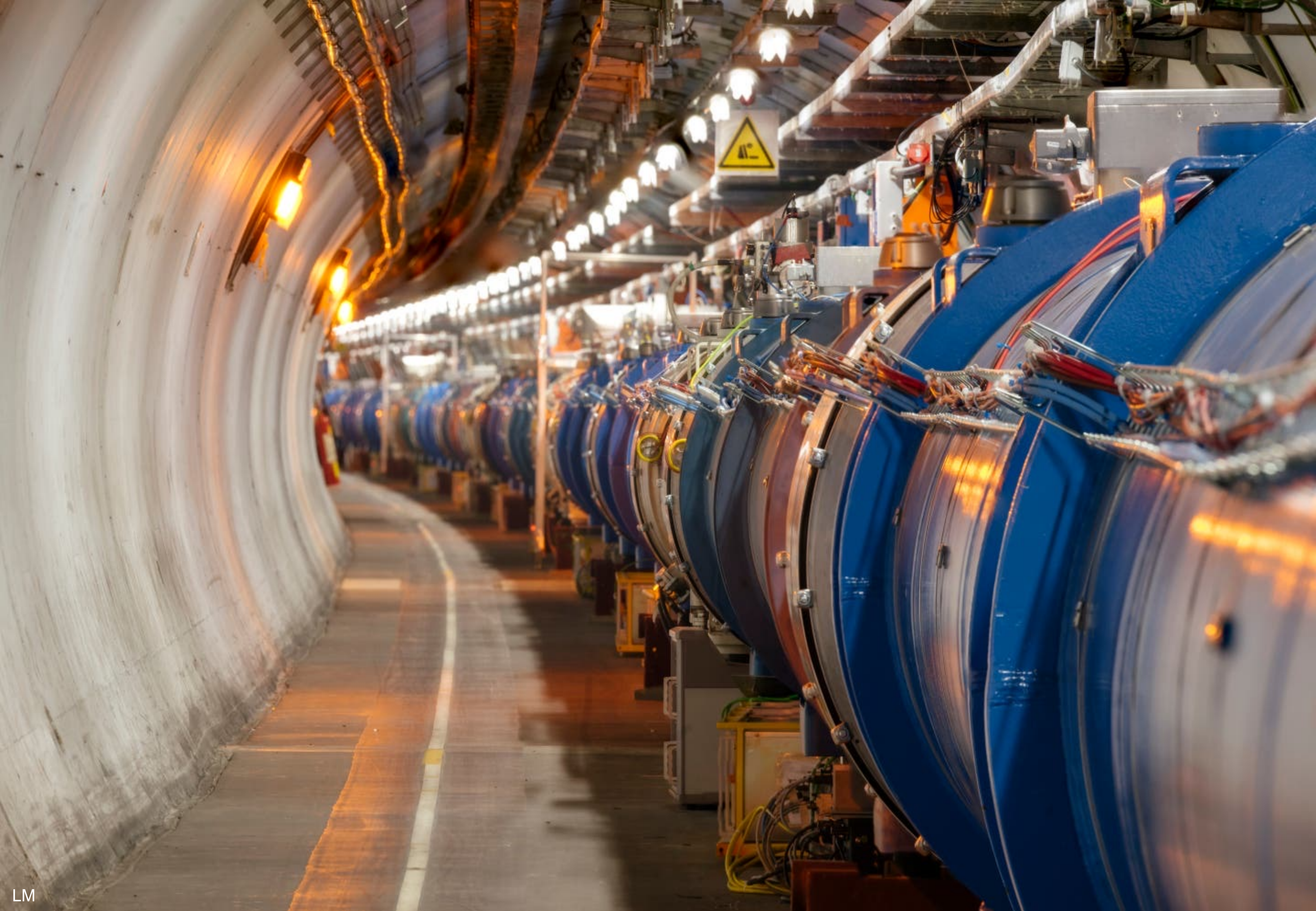
What does a Product Argument Look Like?



CERN Large Hadron Collider (LHC)



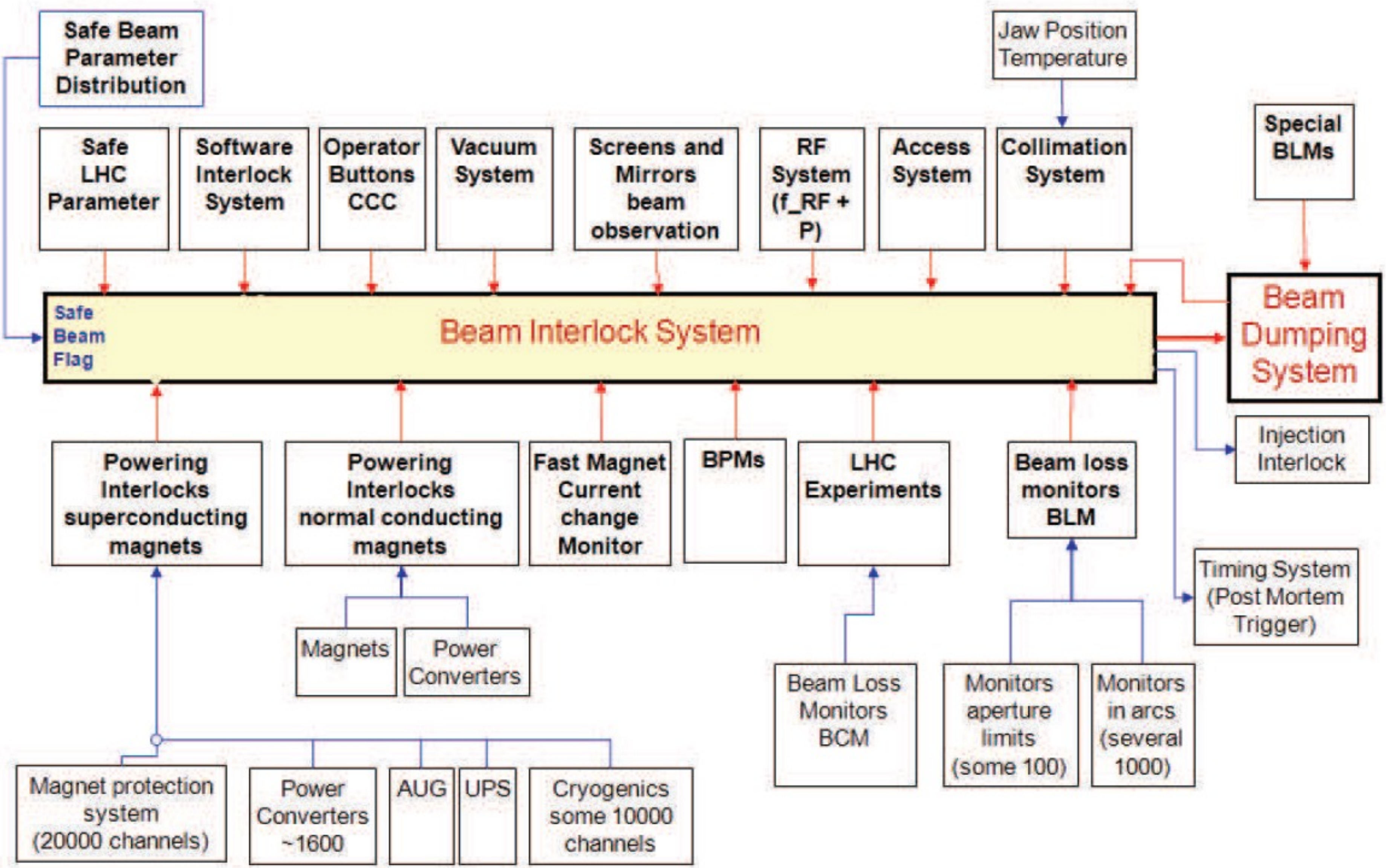
LM


LM

“The beam focuses the energy of an aircraft carrier in motion down to a width of less than a millimeter.”

LHC Machine Protection System (MPS)

1. Beam Loss Monitoring System
2. Beam Interlock System
3. Beam Dump System
4. Safe Machine Parameters System


Safe Beam Parameter Distribution
Jaw Position Temperature
Special BLMs
Safe LHC Parameter
Software Interlock System
Operator Buttons CCC
Vacuum System
Screens and Mirrors beam observation
RF System (f_RF + P)
Access System
Collimation System
Safe Beam Flag
Beam Interlock System
Beam Dumping System
Injection Interlock
Powering Interlocks superconducting magnets
Powering Interlocks normal conducting magnets
Fast Magnet Current change Monitor
BPMs
LHC Experiments
Beam loss monitors BLM
Timing System (Post Mortem Trigger)
Magnets
Power Converters
Beam Loss Monitors BCM
Monitors aperture limits (some 100)
Monitors in arcs (several 1000)
Magnet protection system (20000 channels)
Power Converters ~1600
AUG
UPS
Cryogenics some 10000 channels

JJ

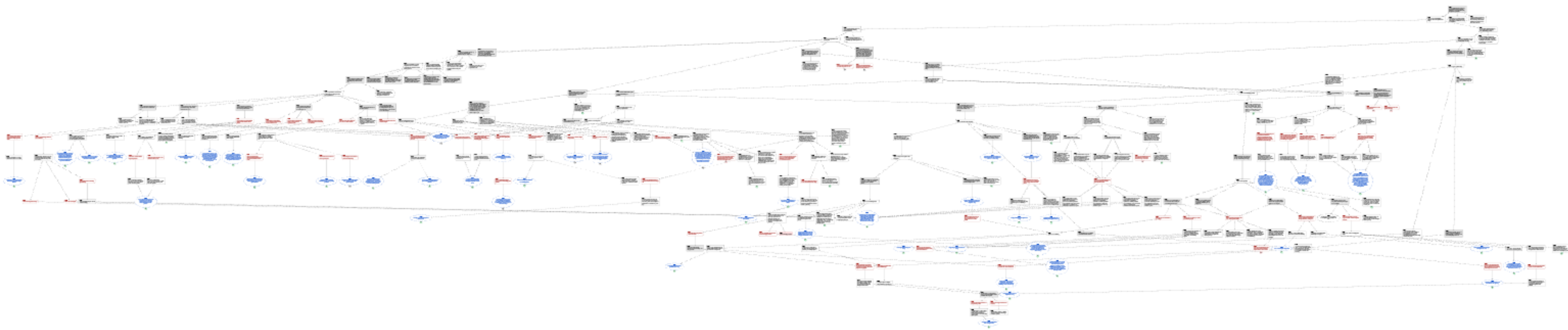
CERN LHC MPS Background

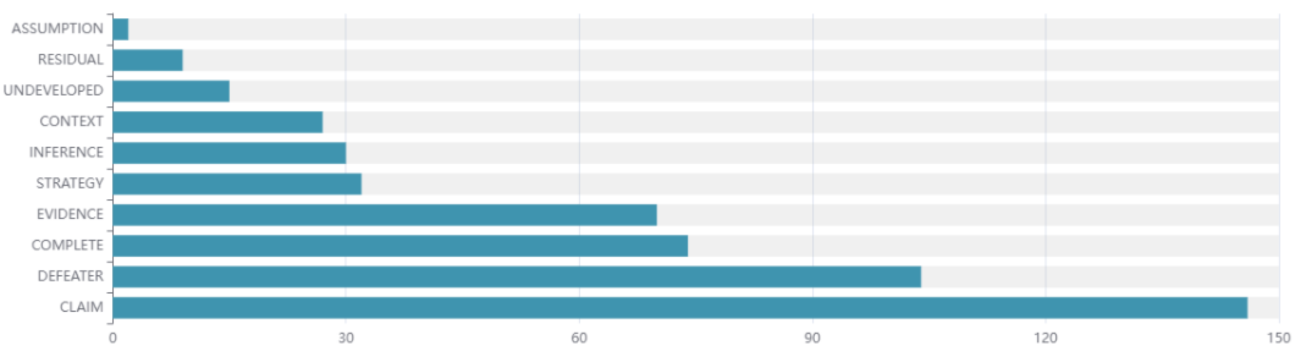
- Developed over 10 years beginning mid-1990s at estimated cost of $200M USD to protect $4.75B USD investment
- Depends on many instances of emergent technology ranging from high-speed micro-electronics to superconducting magnets
- Key elements were products of R&D collaborations between CERN experts and doctoral students
- Lack of non-generic published guidance as a basis for assurance
- Anxious not to rely only on past experience with machine protection for smaller, substantially less powerful accelerators

CSL @ CERN

- 2009-2011 – performed series of technical reviews for critical MPS components
- 2022-2023 – created an assurance case argument for the LHC MPS in collaboration with researchers at U of Toronto and McMaster, in consultation with CERN subject matter experts

LHC MPS Assurance Argument

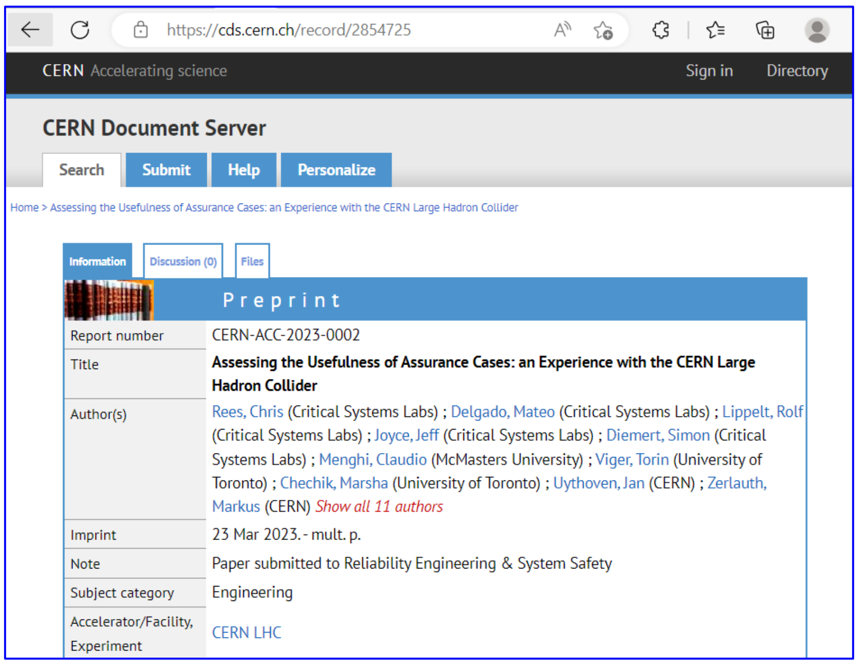




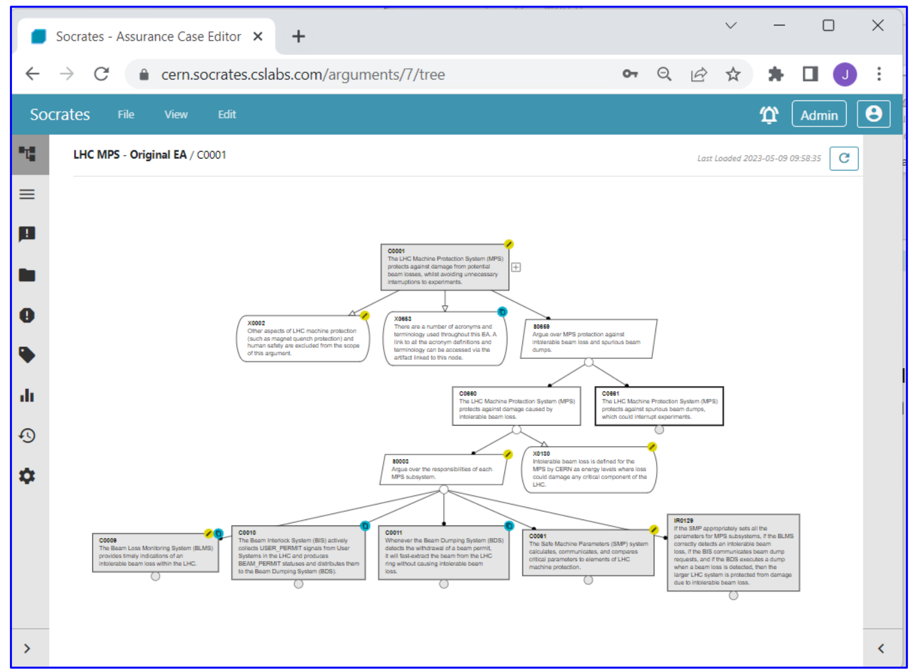
Node Type	Count	Percentage
ASSUMPTION	2	0.4 %
RESIDUAL	9	1.8 %
UNDEVELOPED	15	2.9 %
CONTEXT	27	5.3 %
INFERENCE	30	5.9 %
STRATEGY	32	6.3 %
EVIDENCE	70	13.8 %
COMPLETE	74	14.5 %
DEFEATER	104	20.4 %
CLAIM	146	28.7 %
Total	**509**	**100 %**

LHC MPS Assurance Argument

Two different ways to view a public version of the argument - see cslabs.com/cern.pdf for details

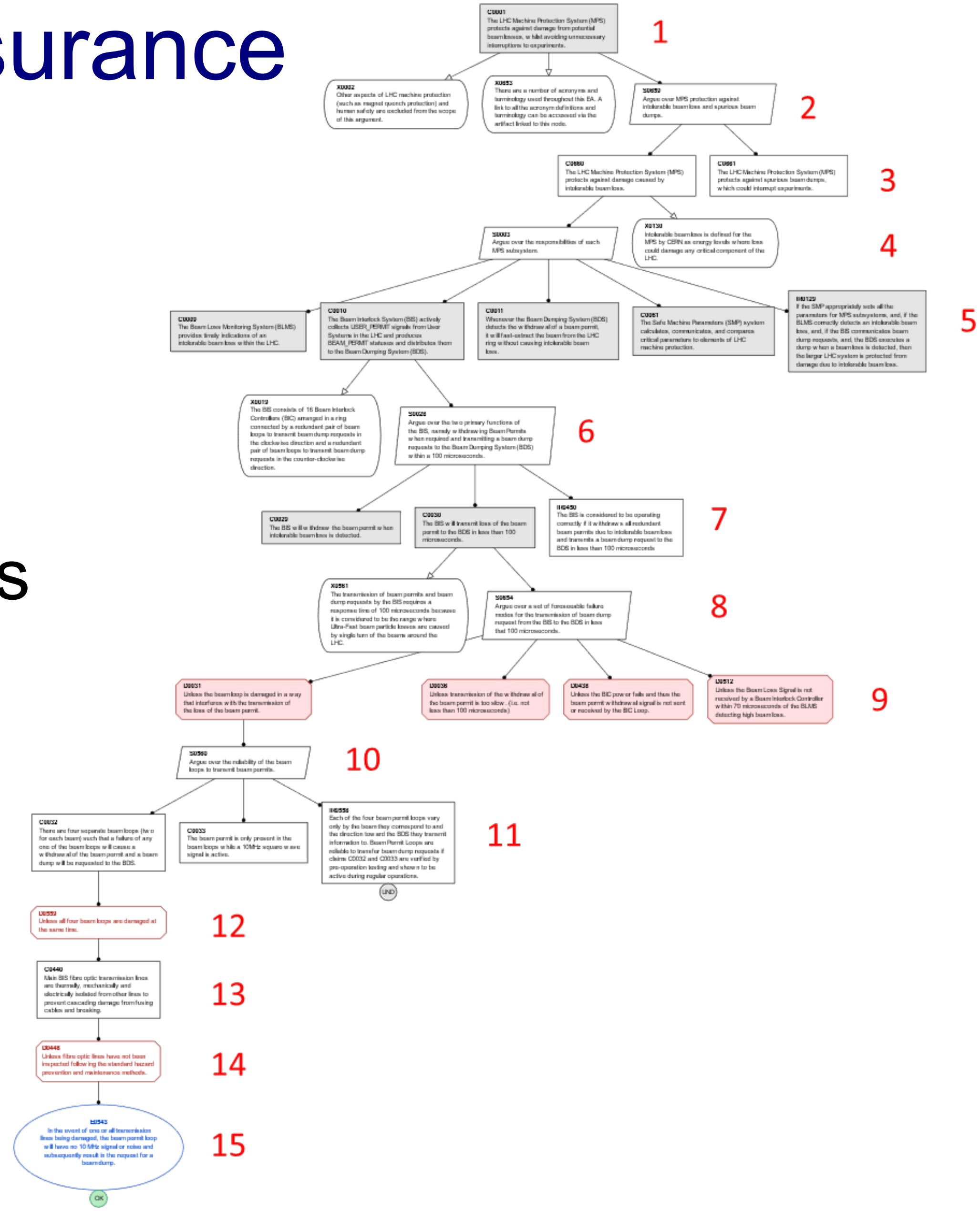


CERN website report (PDF, CSV)



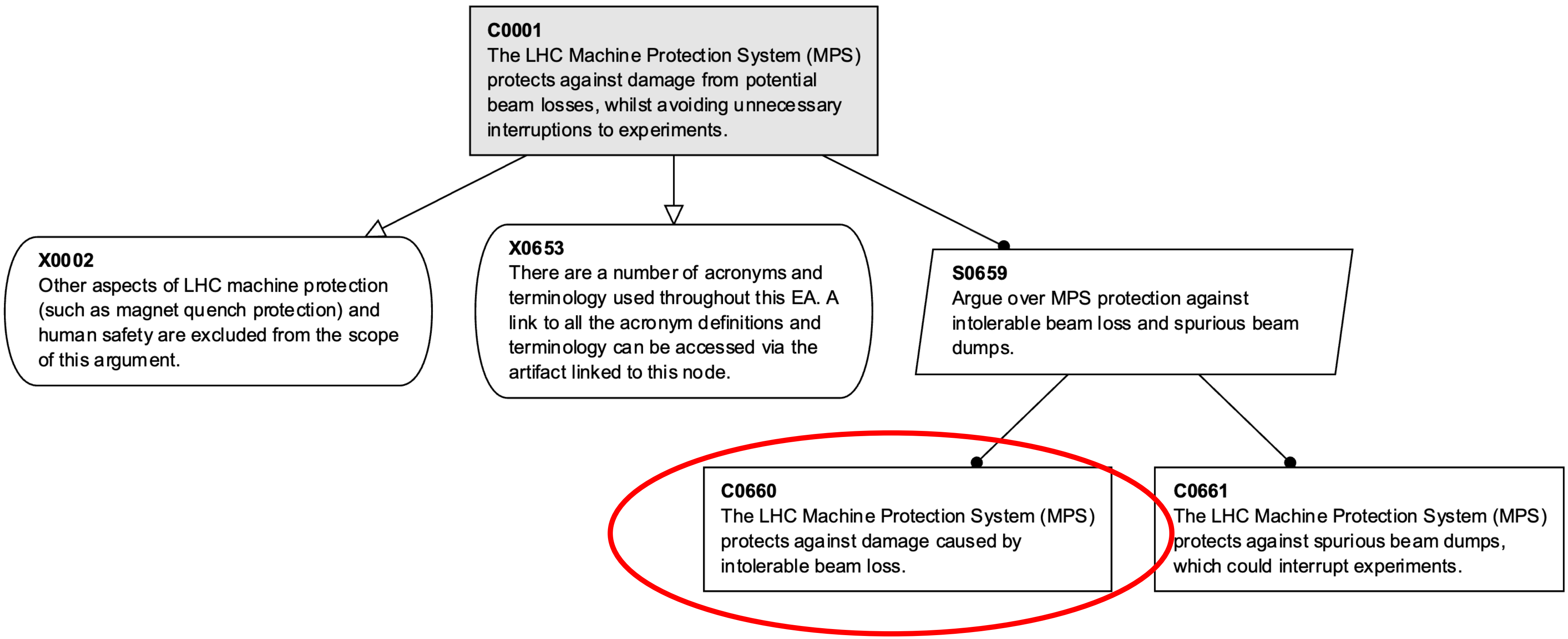
Browsable on-line access (only until May 12)

LHC MPS Assurance Argument

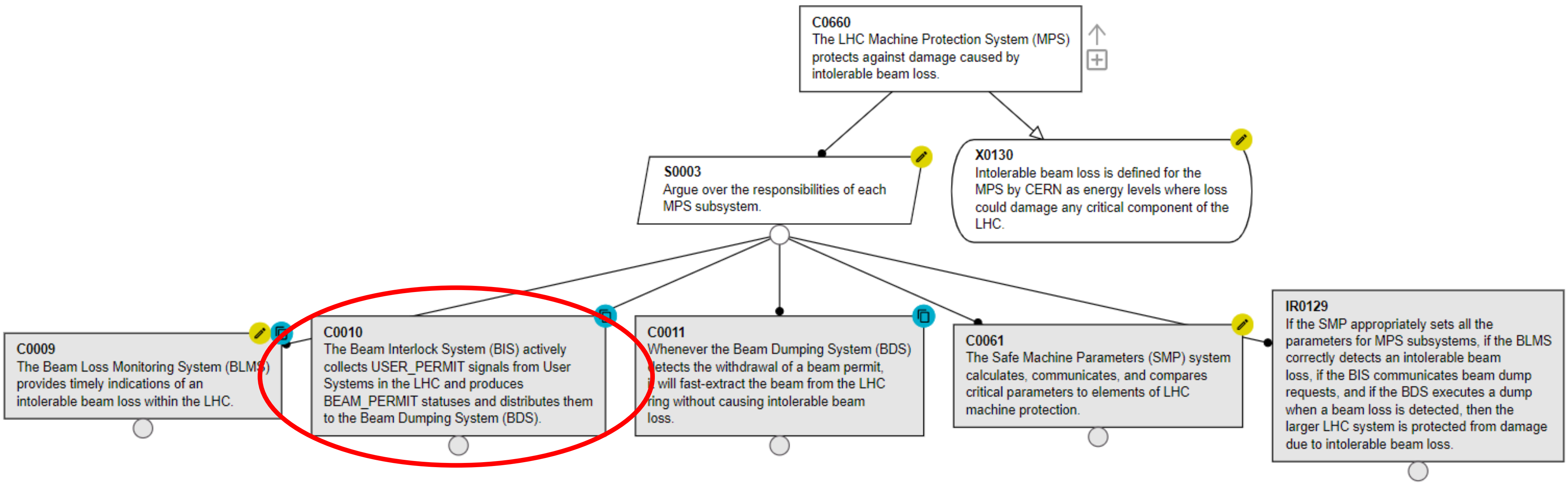


One of ~100 argument branches

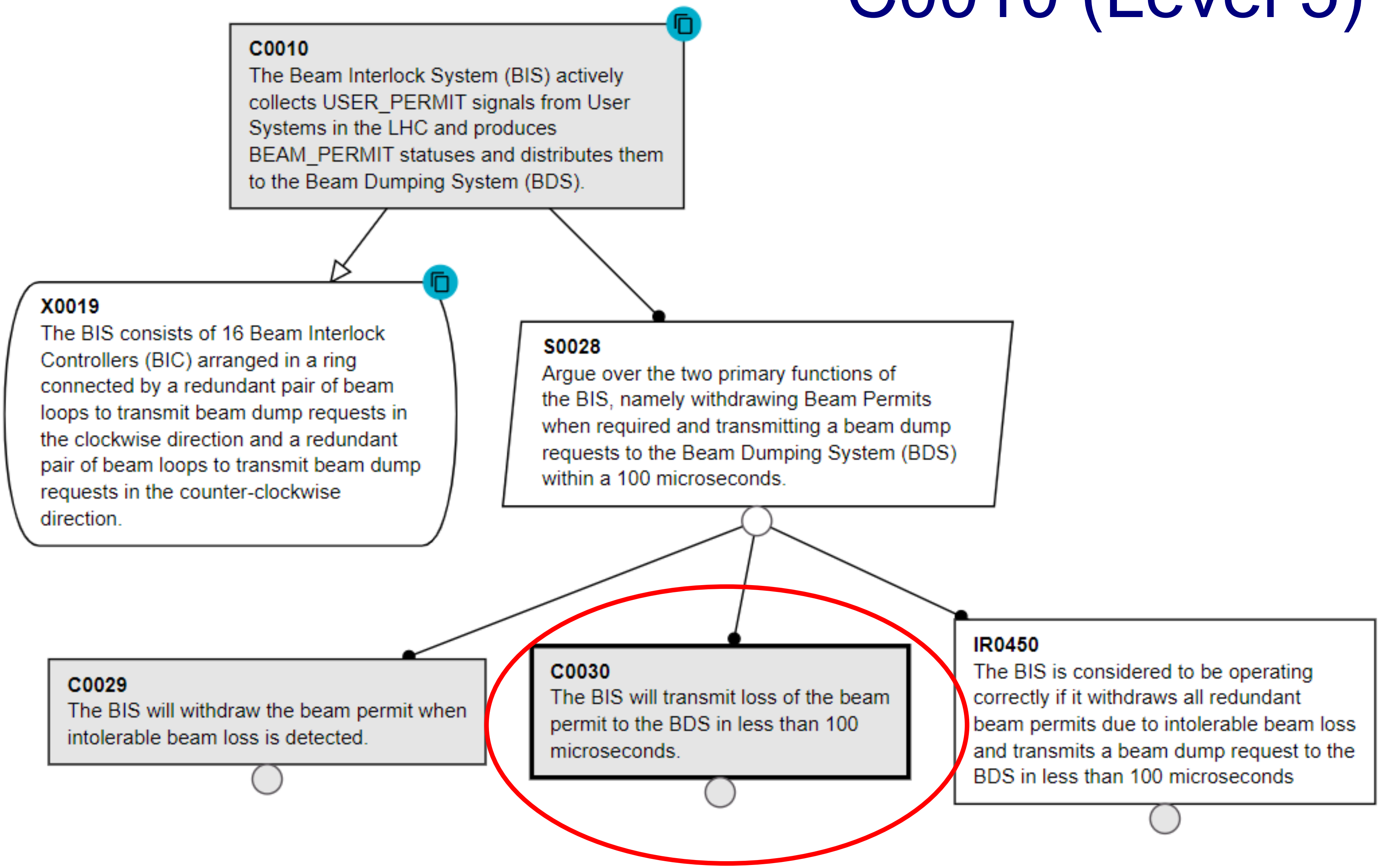
C0001 – Level 1



C0660 – Level 3



C0010 (Level 5)



Beam Permit Loops

4 fibre-optic channels from Point 6
1 clockwise &
1 anticlockwise for **each** Beam

Square wave generated at IP6
-Signal can be cut by any Controller
-Signal can be monitored by any Controller

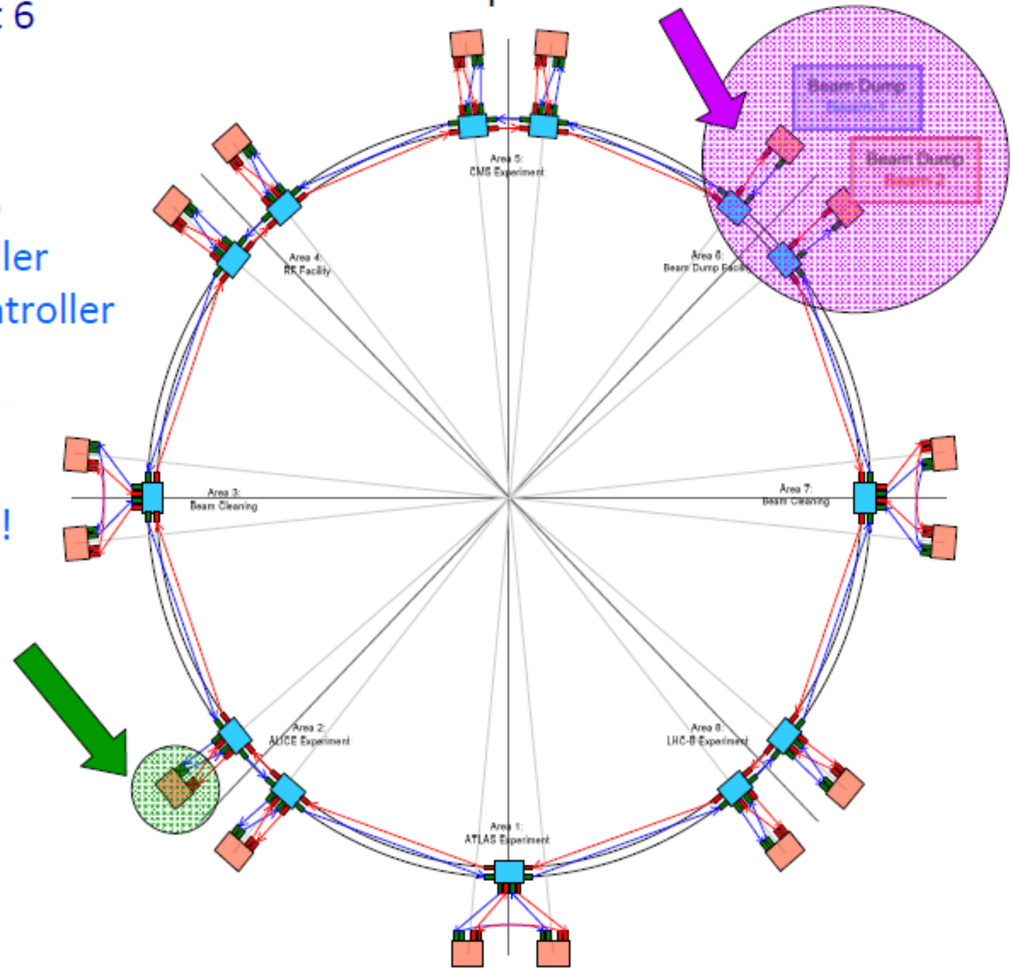
When any of the four signals are absent at IP6, BEAM DUMP!

Beam-1 / Beam-2 are Independent!
Beam Interlock Controllers (BIC)

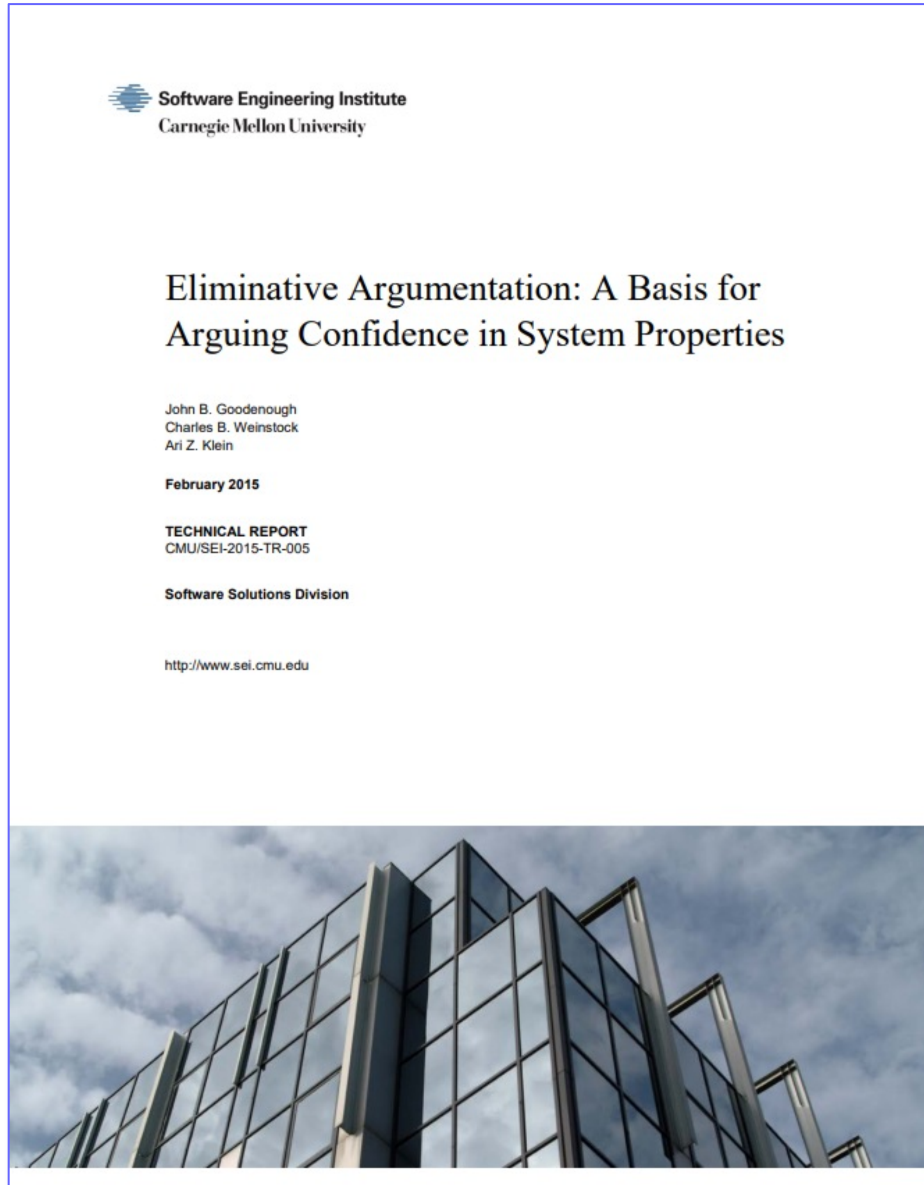
16 BICs per beam
- Two at each Insertion Point

Up to 20 User Systems per BIC
6 x Beam-1
8 x Both-Beam
6 x Beam-2

Beam Dump Beam-1 and Beam-2



Eliminative Argumentation



Software Engineering Institute
Carnegie Mellon University

Eliminative Argumentation: A Basis for Arguing Confidence in System Properties

John B. Goodenough
Charles B. Weinstock
Ari Z. Klein

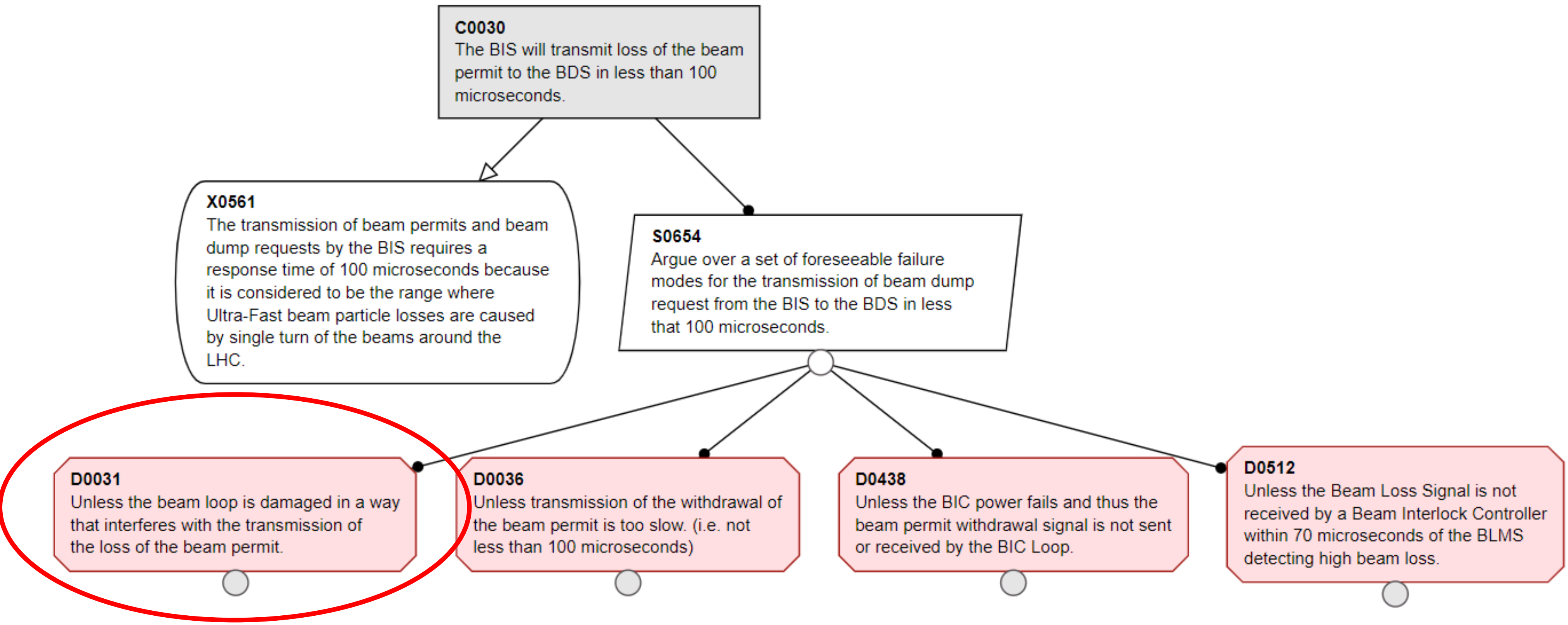
February 2015

TECHNICAL REPORT
CMU/SEI-2015-TR-005

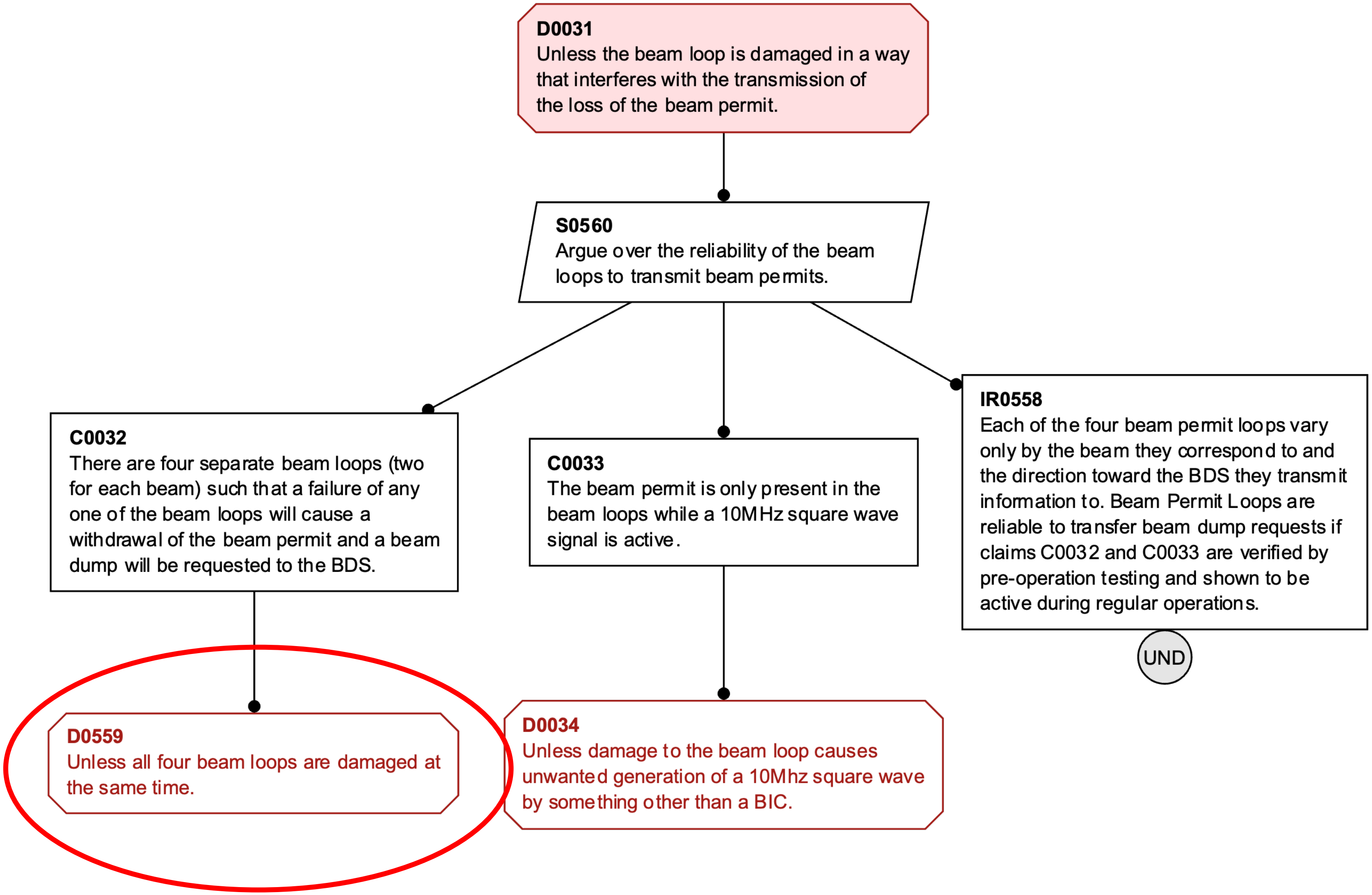
Software Solutions Division

http://www.sei.cmu.edu

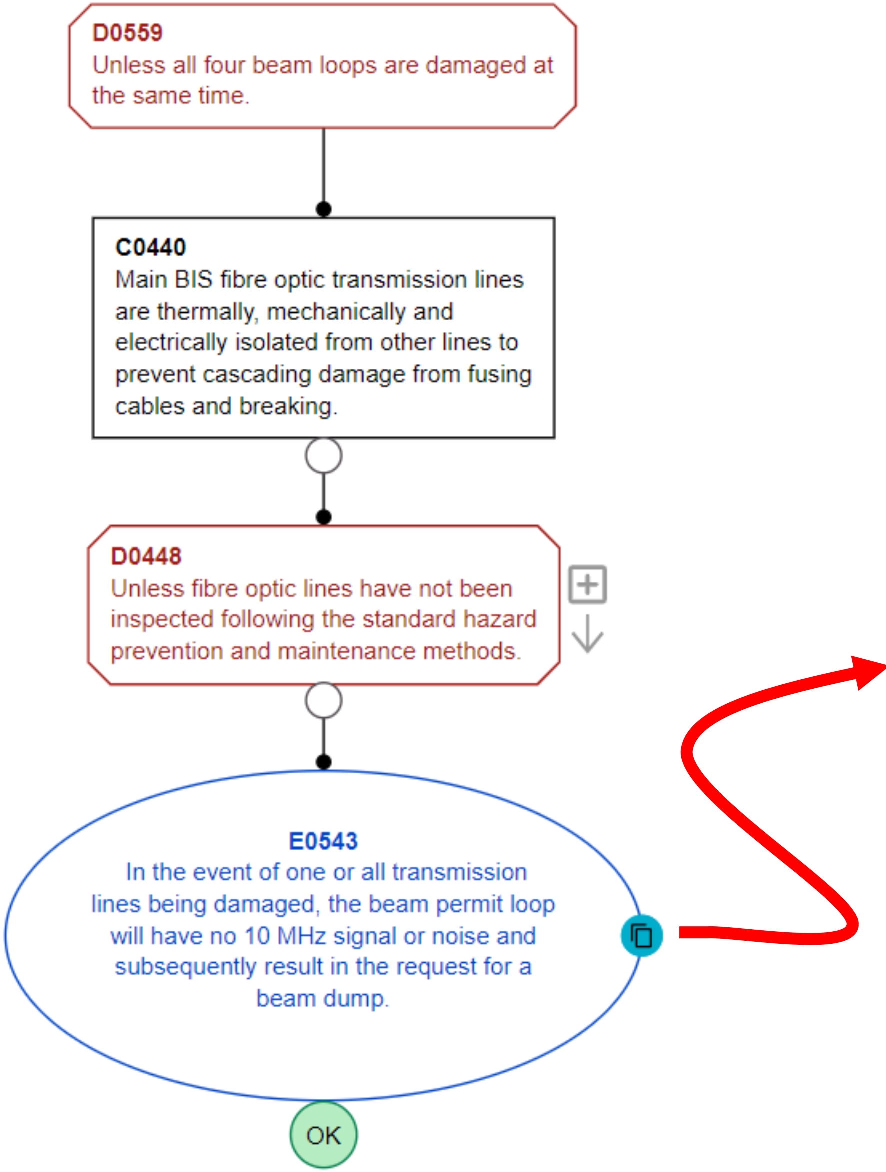
C0030 (Level 7)

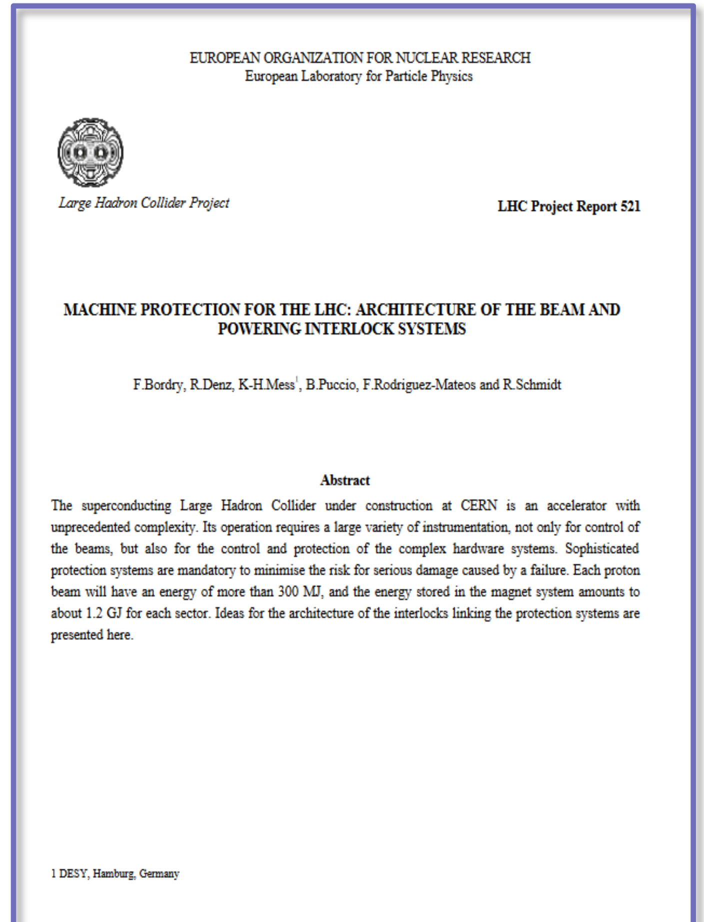


D0031 (Level 9)



D0559 (Level 12)





EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH
European Laboratory for Particle Physics

Large Hadron Collider Project

LHC Project Report 521

MACHINE PROTECTION FOR THE LHC: ARCHITECTURE OF THE BEAM AND POWERING INTERLOCK SYSTEMS

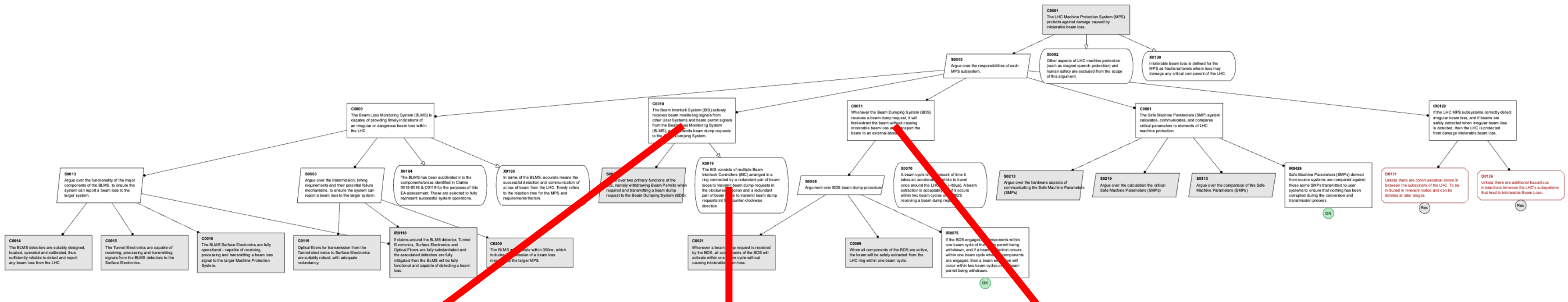
F.Bordry, R.Denz, K-H.Mess[1], B.Puccio, F.Rodriguez-Mateos and R.Schmidt

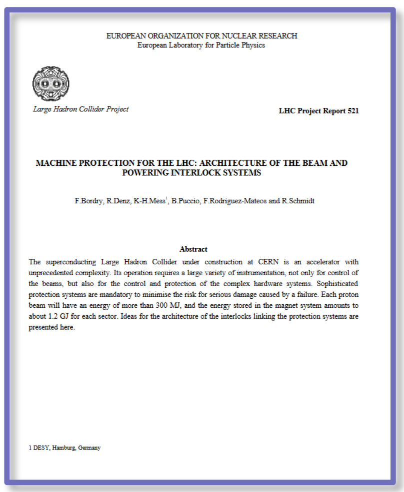
Abstract

The superconducting Large Hadron Collider under construction at CERN is an accelerator with unprecedented complexity. Its operation requires a large variety of instrumentation, not only for control of the beams, but also for the control and protection of the complex hardware systems. Sophisticated protection systems are mandatory to minimise the risk for serious damage caused by a failure. Each proton beam will have an energy of more than 300 MJ, and the energy stored in the magnet system amounts to about 1.2 GJ for each sector. Ideas for the architecture of the interlocks linking the protection systems are presented here.

1 DESY, Hamburg, Germany

Links from Argument Details to Artifacts




EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH
European Laboratory for Particle Physics

Large Hadron Collider Project

LHC Project Report 521

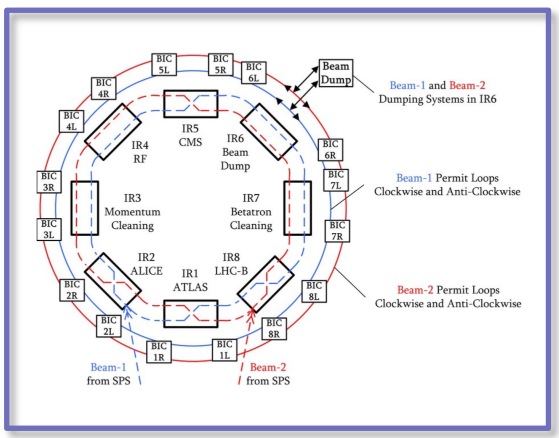
MACHINE PROTECTION FOR THE LHC: ARCHITECTURE OF THE BEAM AND POWERING INTERLOCK SYSTEMS

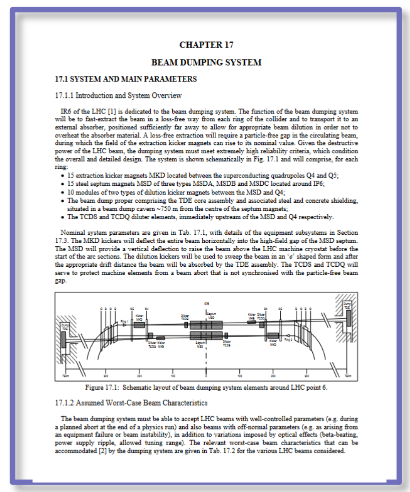
F.Bordry, R.Denz, K-H.Mess[1], B.Puccio, F.Rodriguez-Mateos and R.Schmidt

Abstract

The superconducting Large Hadron Collider under construction at CERN is an accelerator with unprecedented complexity. Its operation requires a large variety of instrumentation, not only for control of the beams, but also for the control and protection of the complex hardware systems. Sophisticated protection systems are mandatory to minimise the risk for serious damage caused by a failure. Each proton beam will have an energy of more than 300 MJ, and the energy stored in the magnet system amounts to about 1.2 GJ for each sector. Ideas for the architecture of the interlocks linking the protection systems are presented here.

1 DESY, Hamburg, Germany




CHAPTER 17

BEAM DUMPING SYSTEM

17.1 SYSTEM AND MAIN PARAMETERS

17.1.1 Introduction and System Overview

IR6 of the LHC [1] is dedicated to the beam dumping system. The function of the beam dumping system will be to fast-extract the beam in a loss-free way from each ring of the collider and to transport it to an external absorber, positioned sufficiently far away to allow for appropriate beam dilution in order not to overheat the absorber material. A loss-free extraction will require a particle-free gap in the circulating beam, during which the field of the extraction kicker magnets can rise to its nominal value. Given the destructive power of the LHC beam, the dumping system must meet extremely high reliability criteria, which condition the overall and detailed design. The system is shown schematically in Fig. 17.1 and will comprise, for each ring:

- 15 extraction kicker magnets MKD located between the superconducting quadrupoles Q4 and Q5;
- 15 steel septum magnets MSD of three types MSDA, MSDB and MSDC located around IP6;
- 10 modules of two types of dilution kicker magnets between the MSD and Q4;
- The beam dump proper comprising the TDE core assembly and associated steel and concrete shielding, situated in a beam dump cavern ~750 m from the centre of the septum magnets;
- The TCDS and TCDQ diluter elements, immediately upstream of the MSD and Q4 respectively.

Nominal system parameters are given in Tab. 17.1, with details of the equipment subsystems in Section 17.3. The MKD kickers will deflect the entire beam horizontally into the high-field gap of the MSD septum. The MSD will provide a vertical deflection to raise the beam above the LHC machine cryostat before the start of the arc sections. The dilution kickers will be used to sweep the beam in an 'e' shaped form and after the appropriate drift distance the beam will be absorbed by the TDE assembly. The TCDS and TCDQ will serve to protect machine elements from a beam abort that is not synchronised with the particle-free beam gap.

Figure 17.1: Schematic layout of beam dumping system elements around LHC point 6.

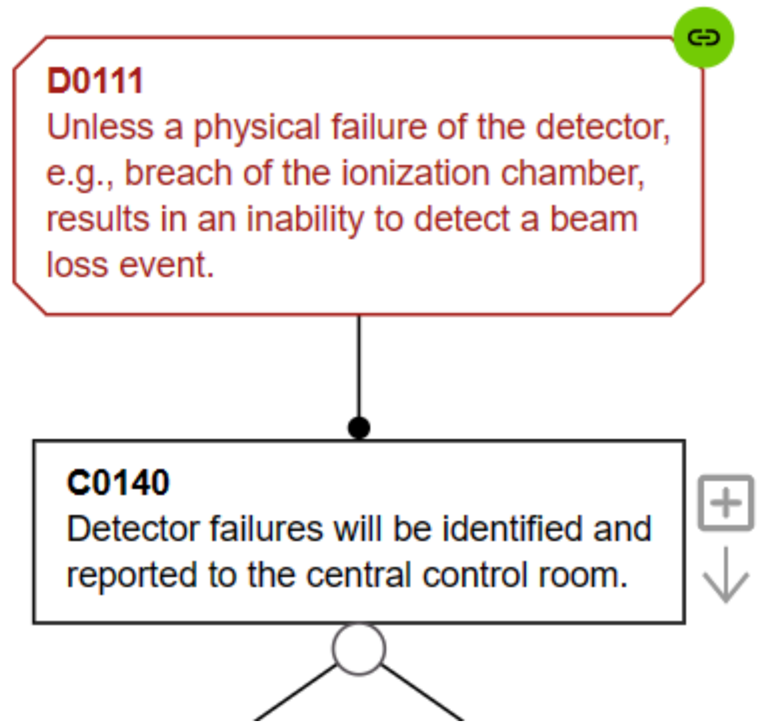
17.1.2 Assumed Worst-Case Beam Characteristics

The beam dumping system must be able to accept LHC beams with well-controlled parameters (e.g. during a planned abort at the end of a physics run) and also beams with off-normal parameters (e.g. as arising from an equipment failure or beam instability), in addition to variations imposed by optical effects (beta-beating, power supply ripple, allowed tuning range). The relevant worst-case beam characteristics that can be accommodated [2] by the dumping system are given in Tab. 17.2 for the various LHC beams considered.

■ ■ ■

Key Performance Indicators (KPIs)

- Review of EA defeaters and mitigating claims & evidence lead to identification of KPIs.
- 21 KPIs identified total:
  - 15 lagging
  - 6 leading
- Using as a case study to validate SPI/KPI functions in Socrates.



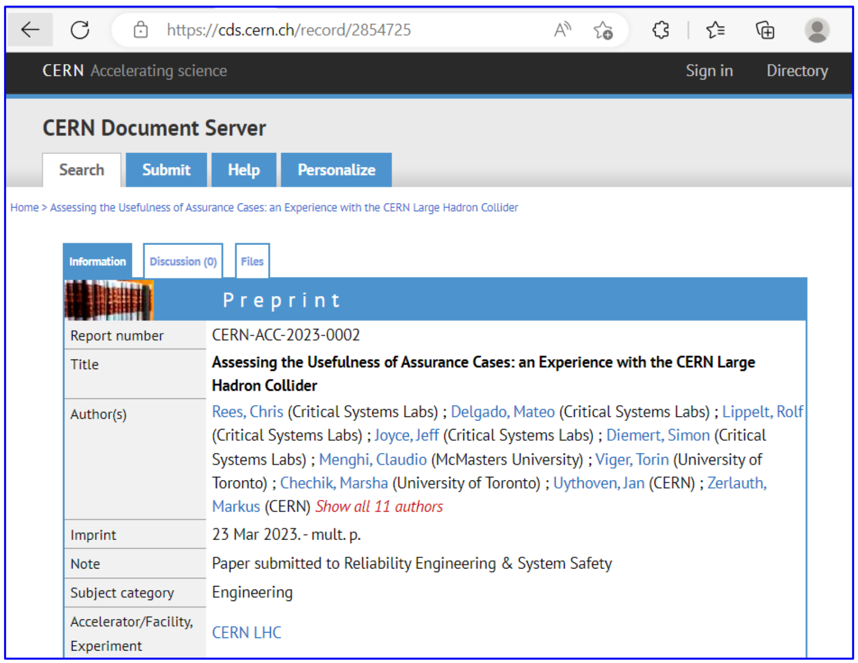
Leading Indicator: *frequency of detector failures as reported in control room.*

Result and Conclusions

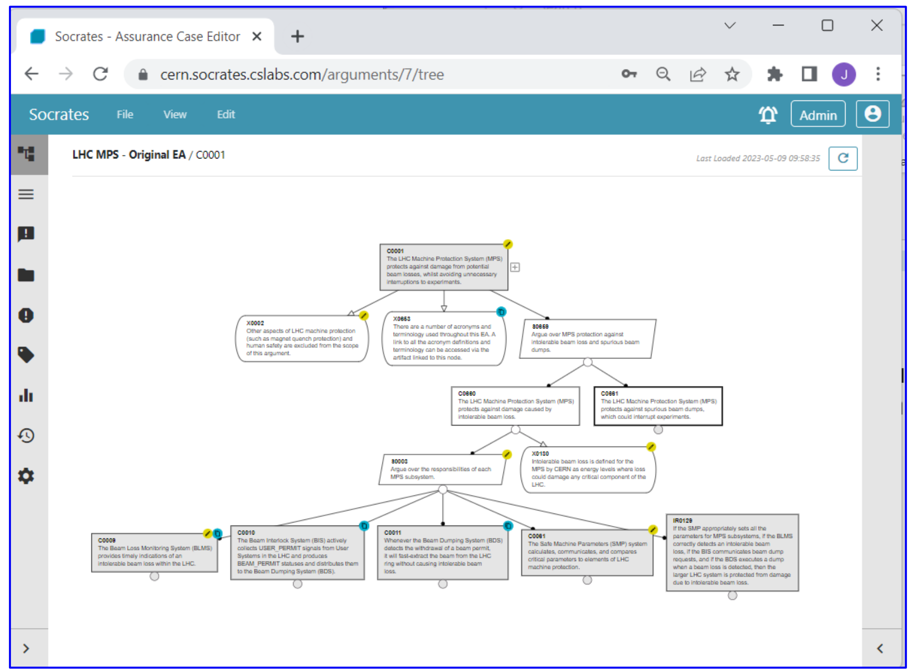
- Captures why the CERN subject matter experts have trusted the MPS for nearly 15 years of operational use
- While Eliminative Argumentation didn't reveal any previously unknown vulnerabilities, development of the assurance case identified gaps in the existing public documentation
- CERN experts were particularly interested in "cross cutting" inter-dependencies between sub-systems identified by the assurance case argument
- Associated specific elements of the assurance case with Key Performance Indicators (KPI)

More Information

Two different ways to view a public version of the argument - see cslabs.com/cern.pdf for details



CERN website report (PDF, CSV)



Browsable on-line access (only until May 12)