Critical Systems Labs
Innovating Safely

Assurance Case Arguments in the Large: the CERN LHC Machine Protection System

SafeComp 2023 – Toulouse

Critical Systems Labs Inc.

L. Millet, S. Diemert, C. Rees, T. Viger, M. Chechik, C. Menghi, and J. Joyce

Presenter

Laure Millet is a Software and Systems Engineer at Critical Systems Labs Inc. She has extensive experience in safety assurance across a wide range of technical domains including aerospace, automotive, defense, medical and rail. She is often involved in client projects that involve unique challenges in managing safety risk associated with emergent technology such as the use of Machine Learning in autonomous vehicles. Laure has received a doctorate in Computer Science from Pierre and Marie Curie University (Paris, France).

The Problem

- Public assurance case
  - Available arguments are lacking
    - In term of size
    - In term of details
  - No public industrial arguments
    - For the evaluation of new methods and techniques
    - For showcasing best practices

CERN Large Hadron Collider (LHC)

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

CERN LHC MPS Background

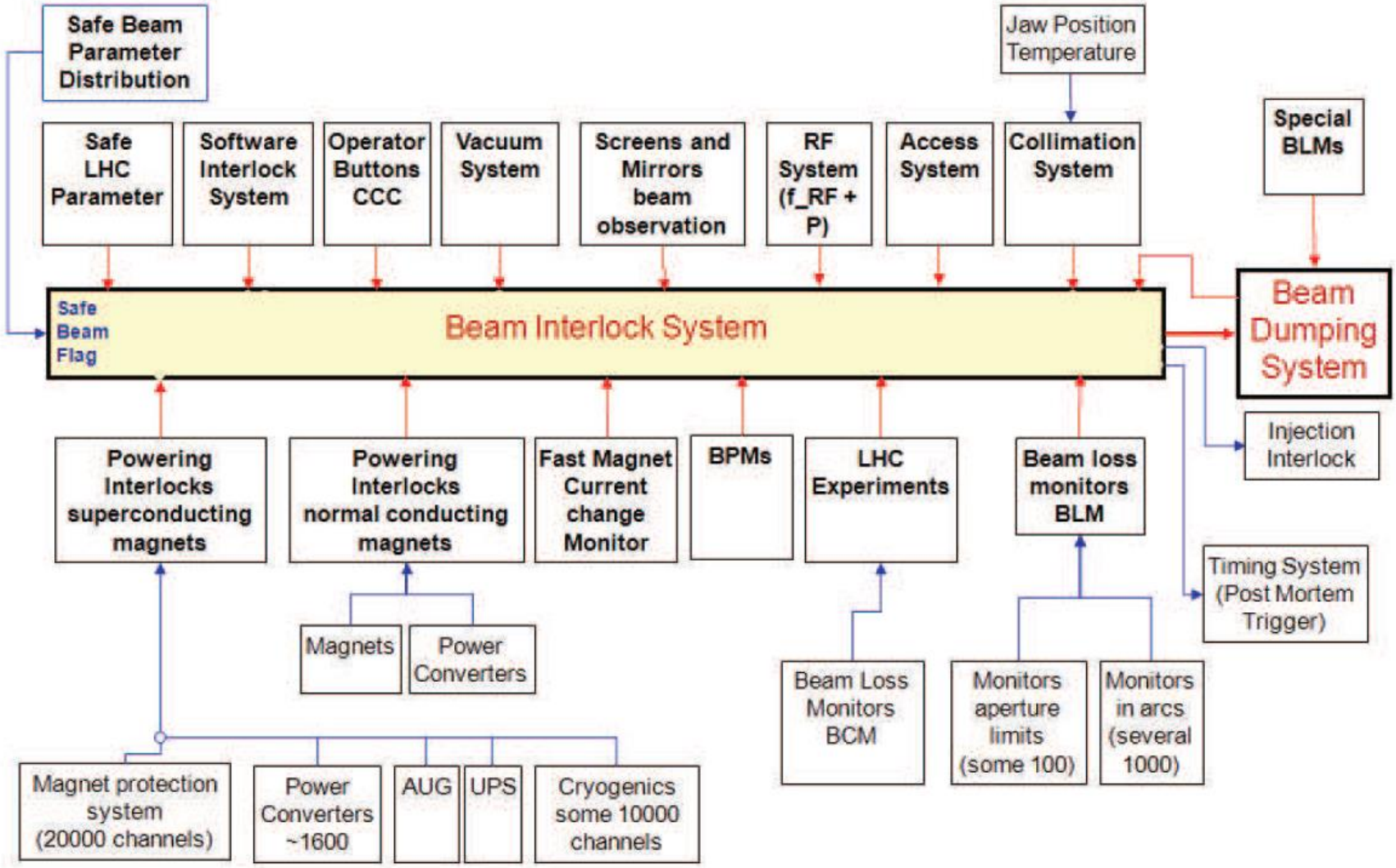
- Developed over 10 years beginning mid-1990s at estimated cost of $200M USD to protect $4.75B USD investment
- Depends on many instances of emergent technology ranging from high-speed micro-electronics to superconducting magnets
- Key elements were products of R&D collaborations between CERN experts and doctoral students
- Lack of non-generic published guidance as a basis for assurance
- 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 Machine Protection System (MPS)

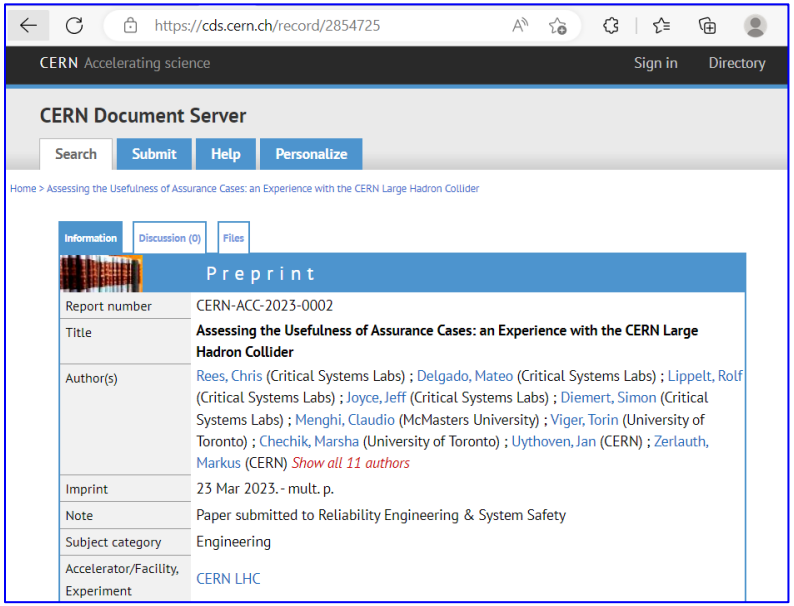
1. Beam Loss Monitoring System
2. Beam Interlock System
3. Beam Dump System
4. Safe Machine Parameters System



LHC MPS Assurance Argument

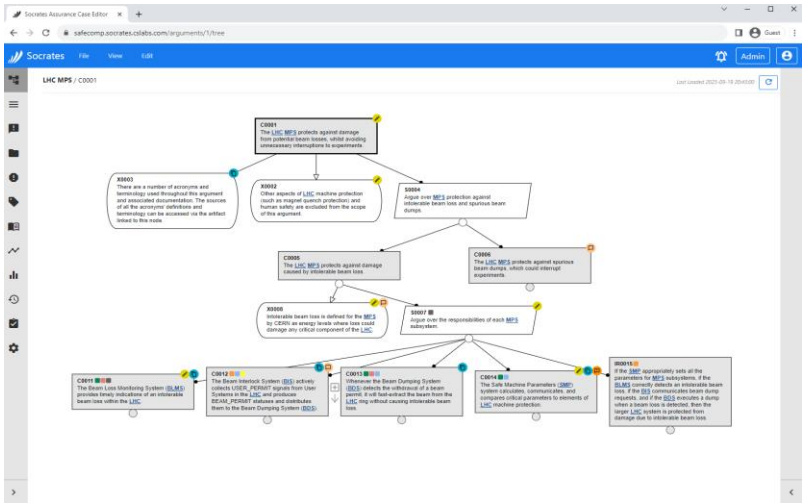
Two different ways to view a public version of the argument.

https://tinyurl.com/CERN-ACC-2023



CERN website report (PDF, CSV)

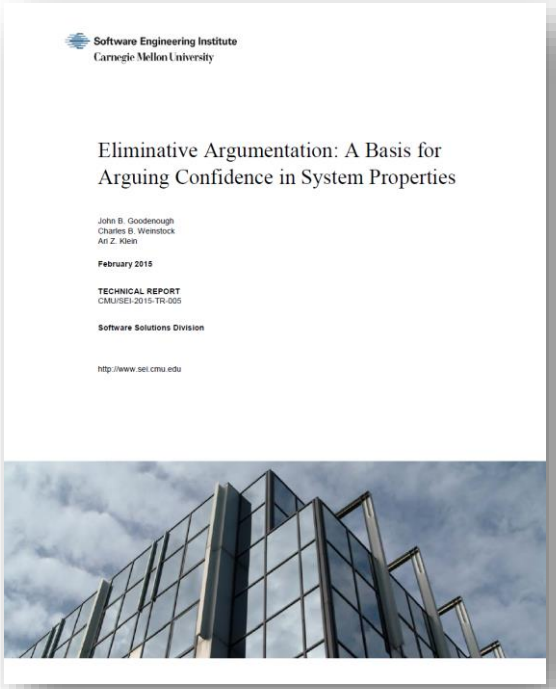
https://safecomp.socrates.cslabs.com/
Login: guest
Password: SafeComp2023@Toulouse



Full on-line access

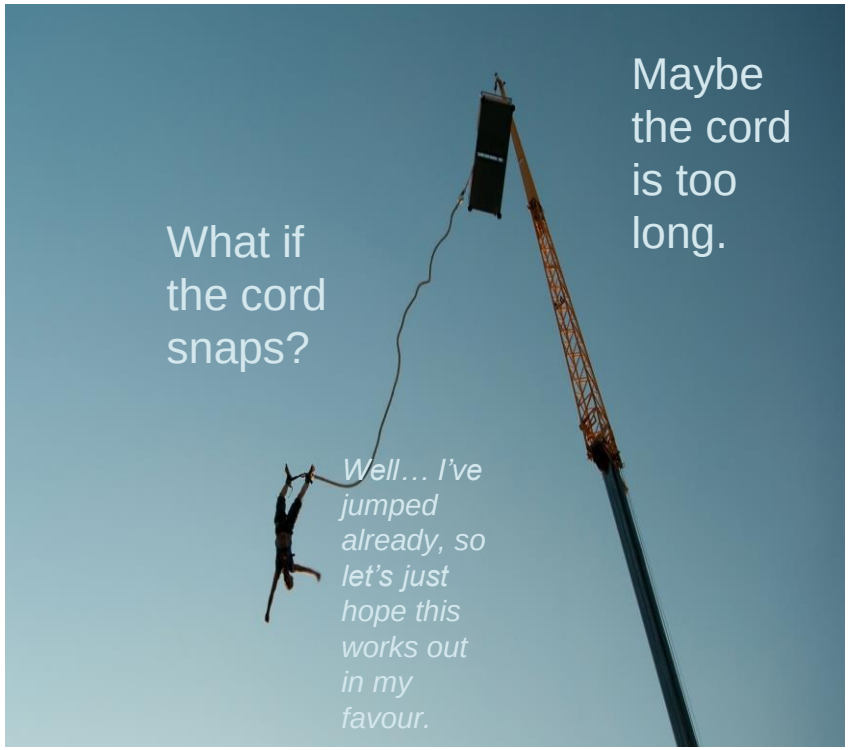
Eliminative Argumentation

- An extension (flavour) of GSN created by researchers at the SEI.
- Incorporates the notion of “doubt” as defeaters.
- Defeaters that are not resolved by additional claims/evidence are “residual”.
- Also referred to as a “dialectic argument”.



A teaspoon of doubt

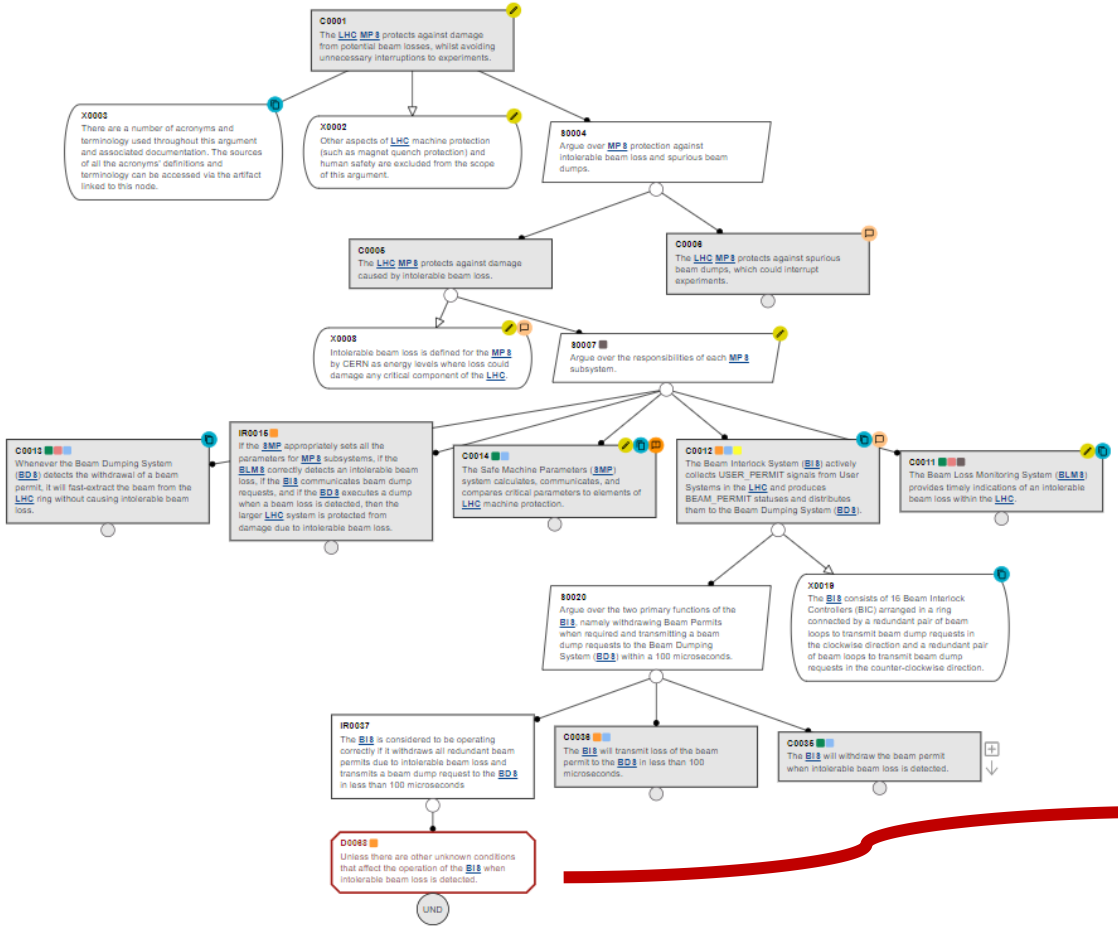
- Engineers naturally have doubts about the systems they design
  - “defect free software is impossible”
- Our assurance case methods should take advantage of this doubt rather than try to hide it



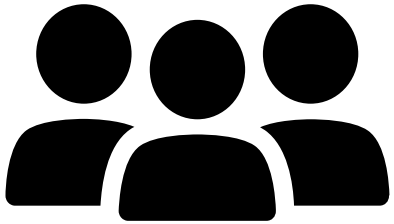
What to do about defeaters?

- What do we do with “residual” (uneliminated) defeaters in our argument?
- Depends on who you ask:
  - You *must* resolve all doubts/defeaters.
  - It’s not possible to eliminate all risk, so enumerating residual doubts can be a helpful communication too.

Communicating Doubt to Stakeholders

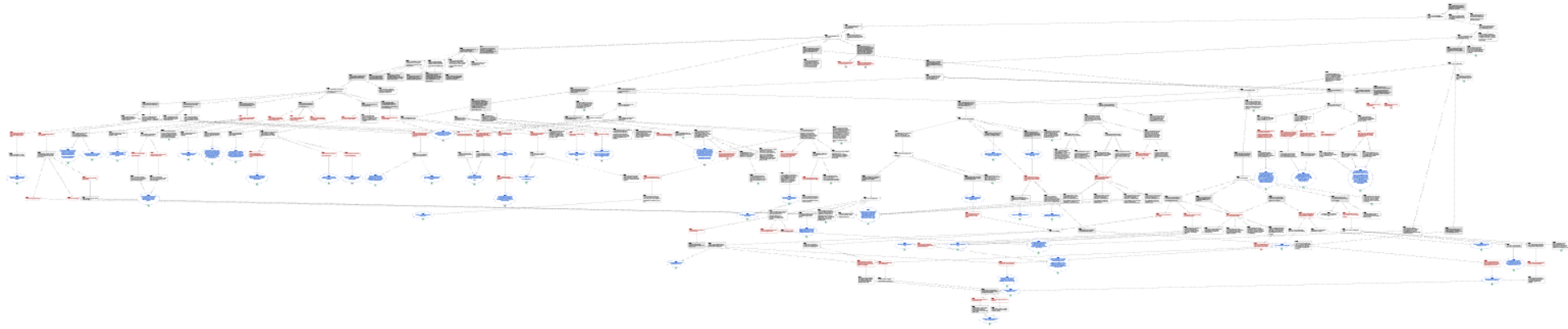


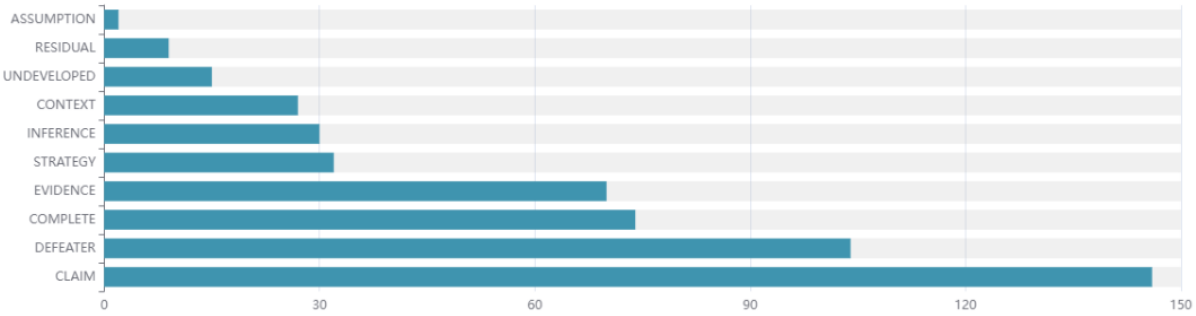
Expressing residual doubt in an assurance case is an effective means of communicating with top-level decision makers in your organization.



The Argument

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 %**

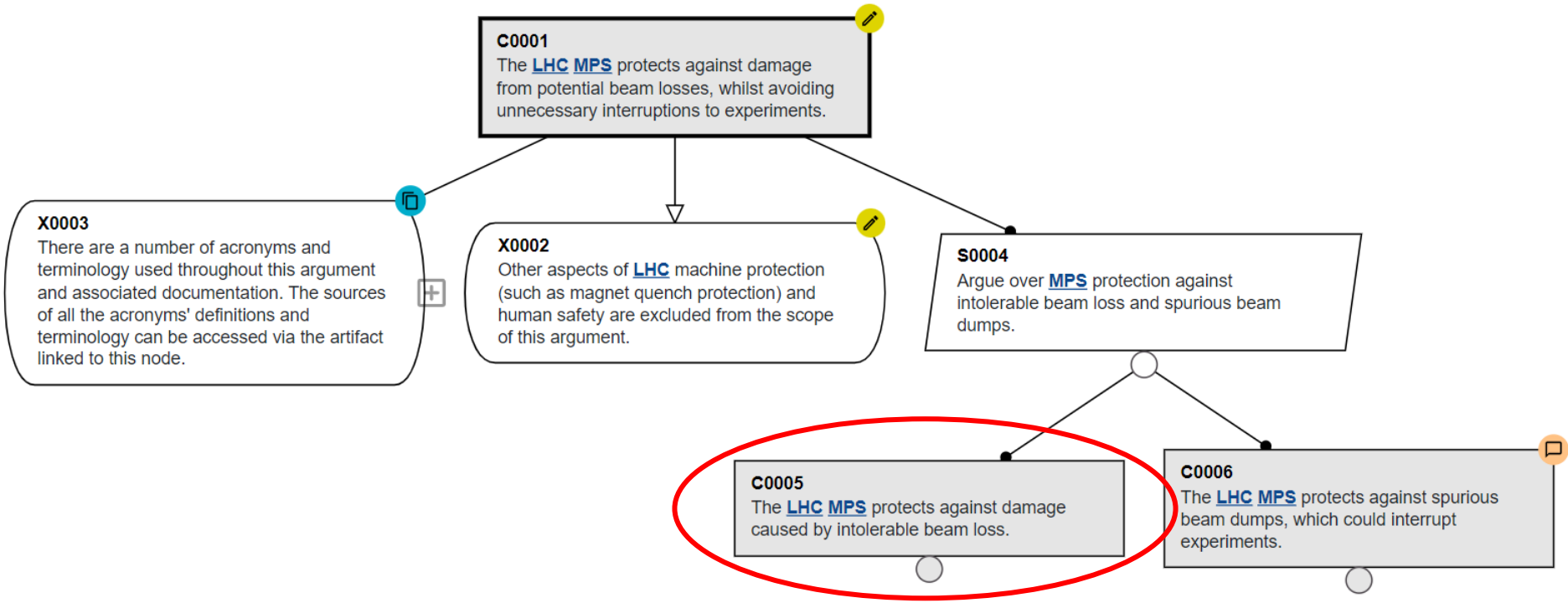
Product Argument

- Based on system engineering understanding

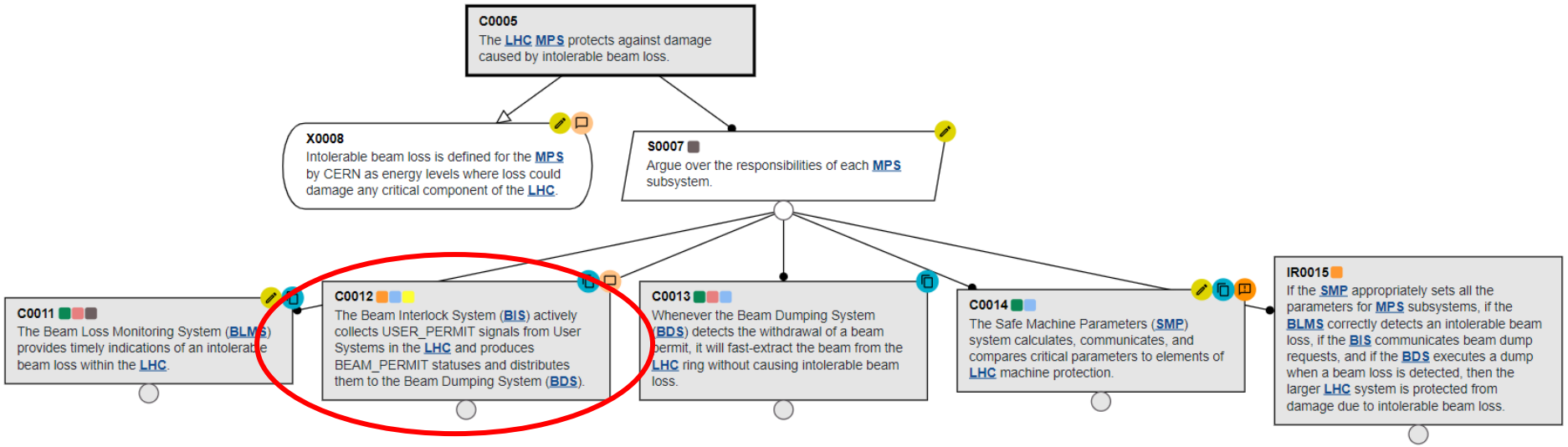
  - Capture reasoning for trust
  - Intuitive for internal stakeholders
  - Design-focused
  - Not reusable
  - Does not address system lifecycle

A Collaborative Effort

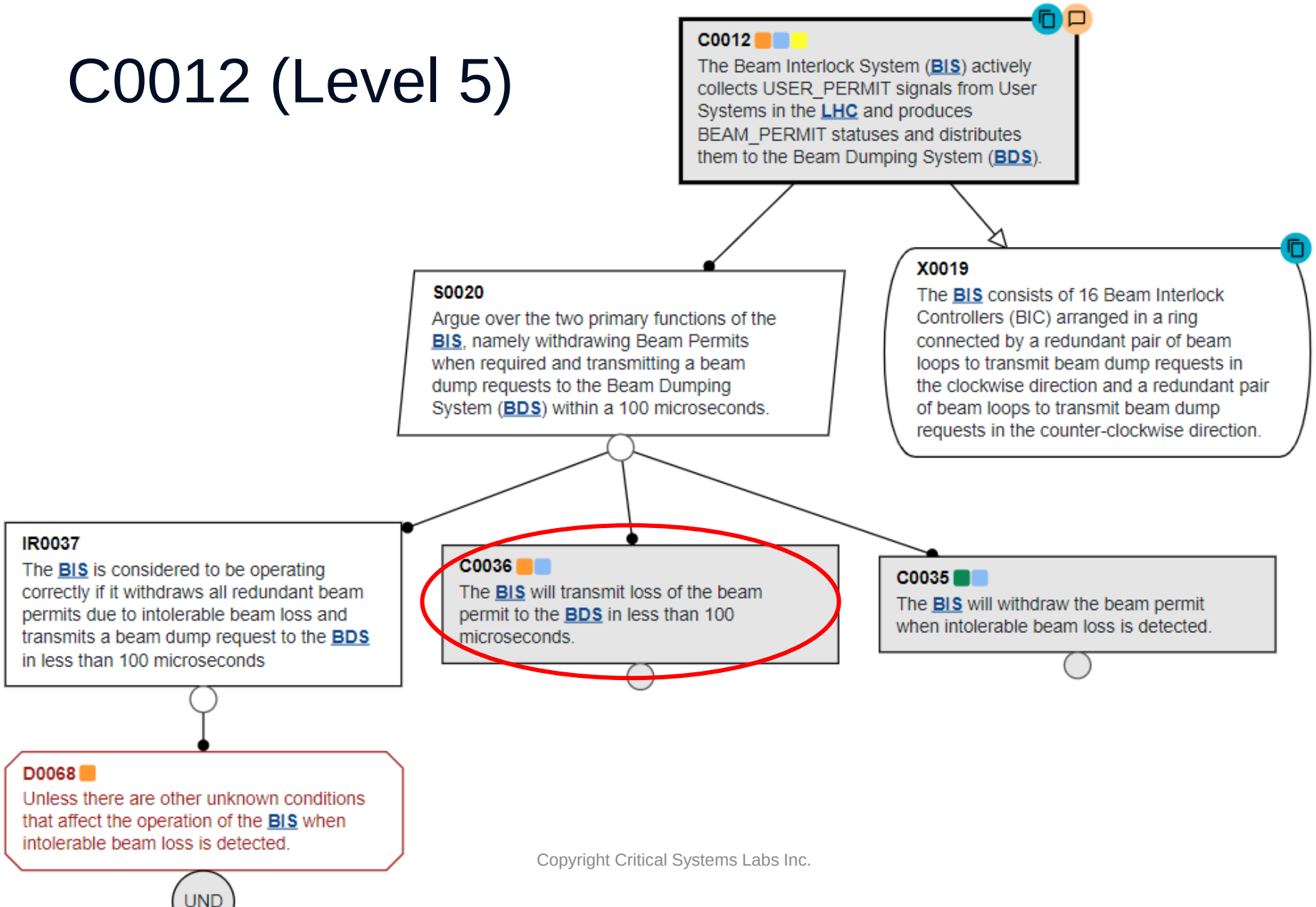
C0001 – Level 1



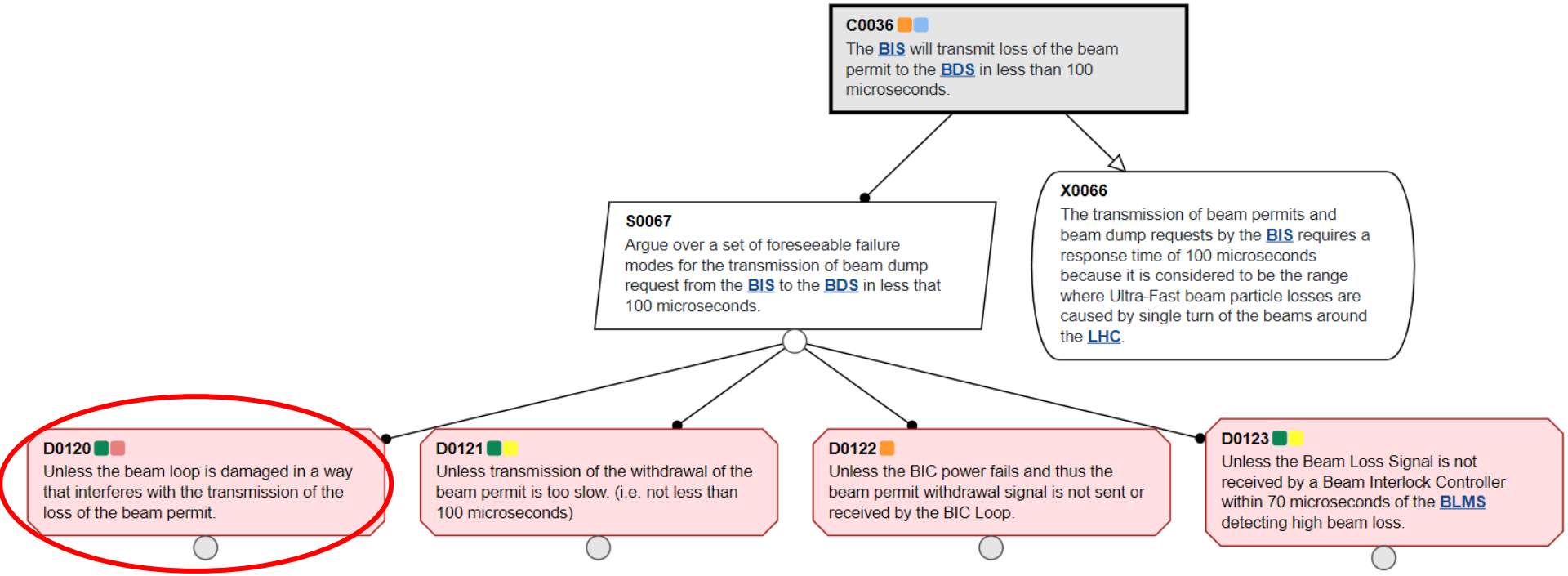
C0005 – Level 3



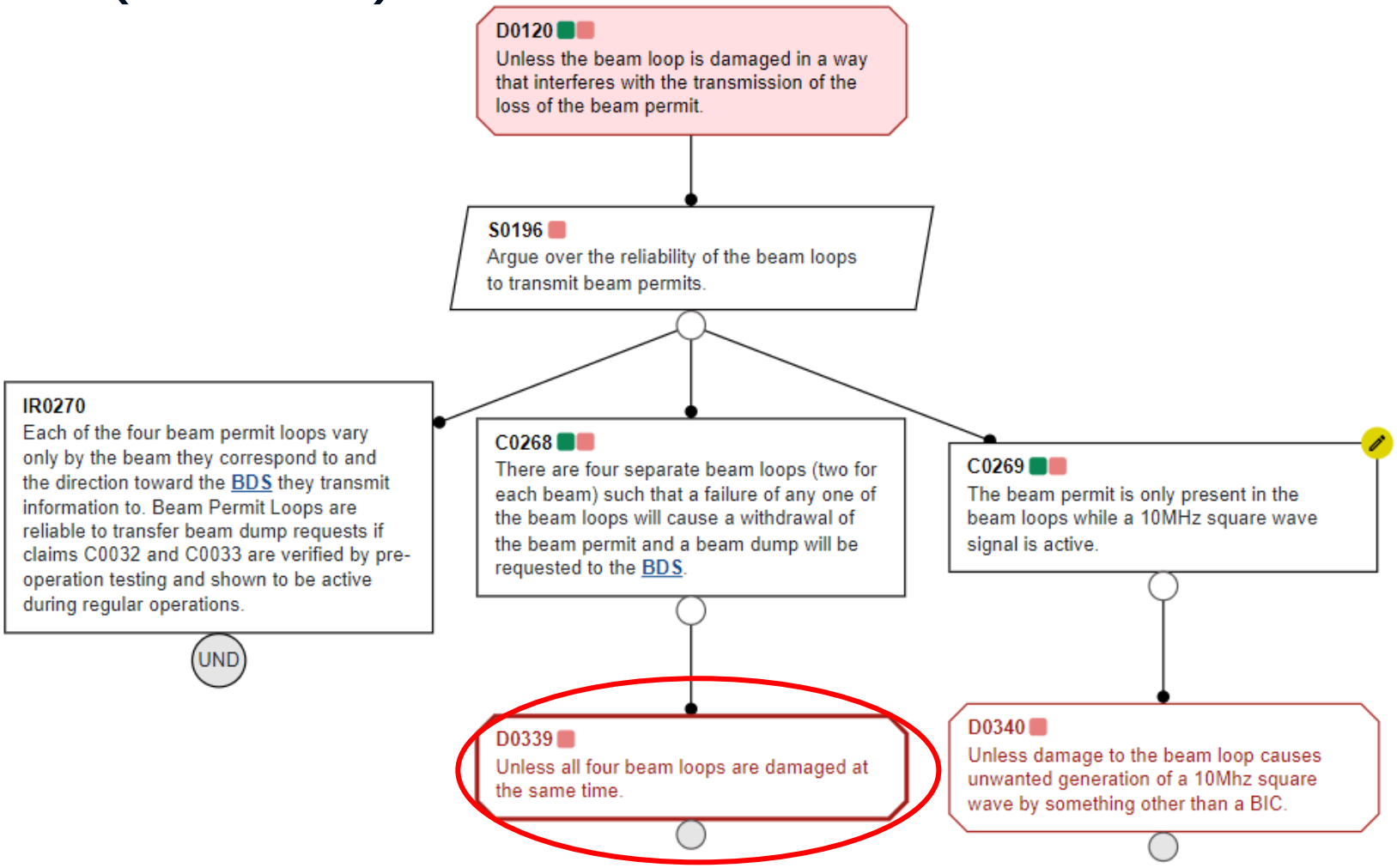
C0012 (Level 5)



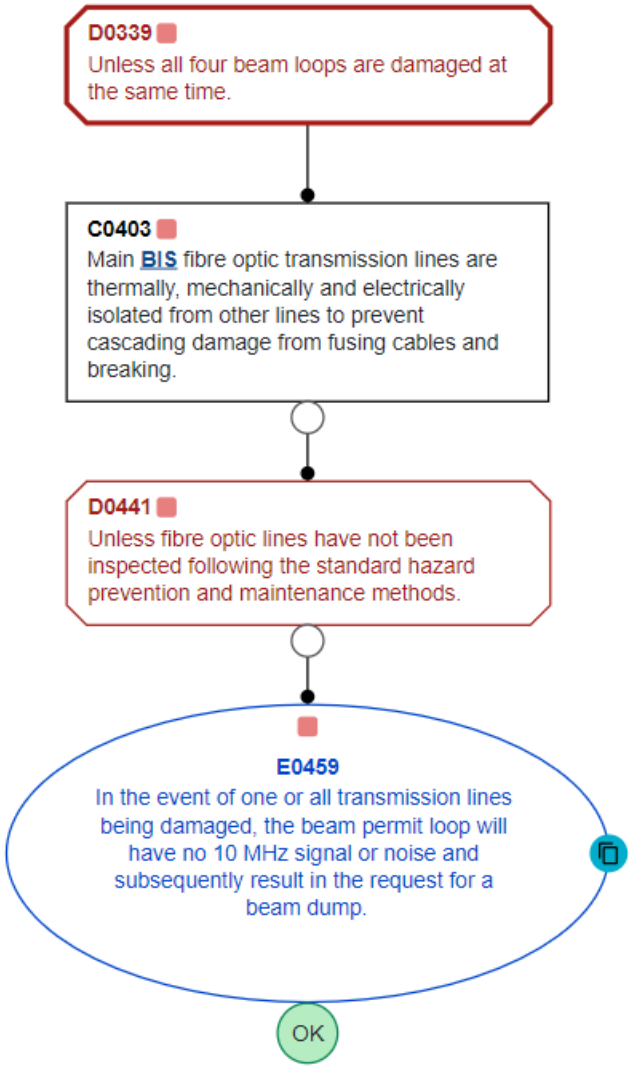
C0036 (Level 7)

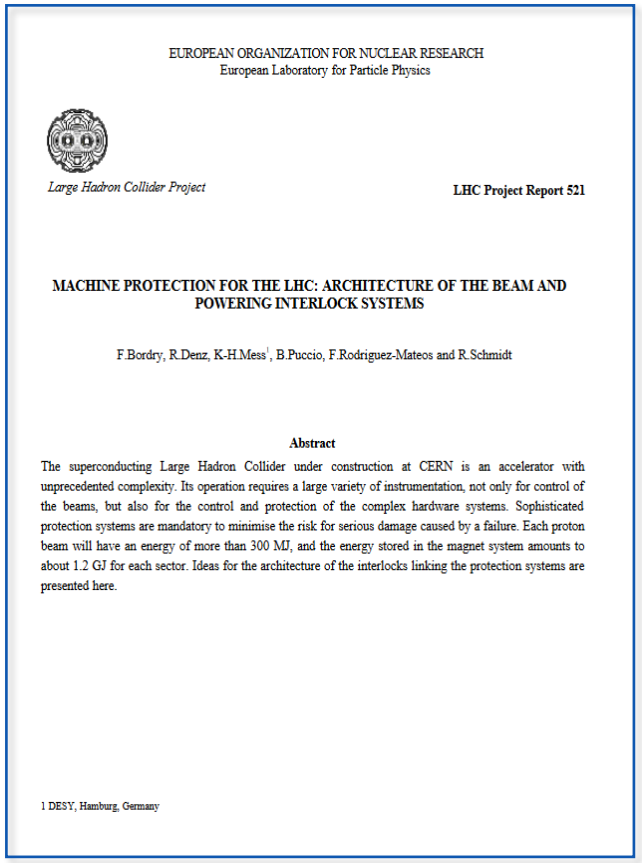


D0120 (Level 9)



D0339 (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

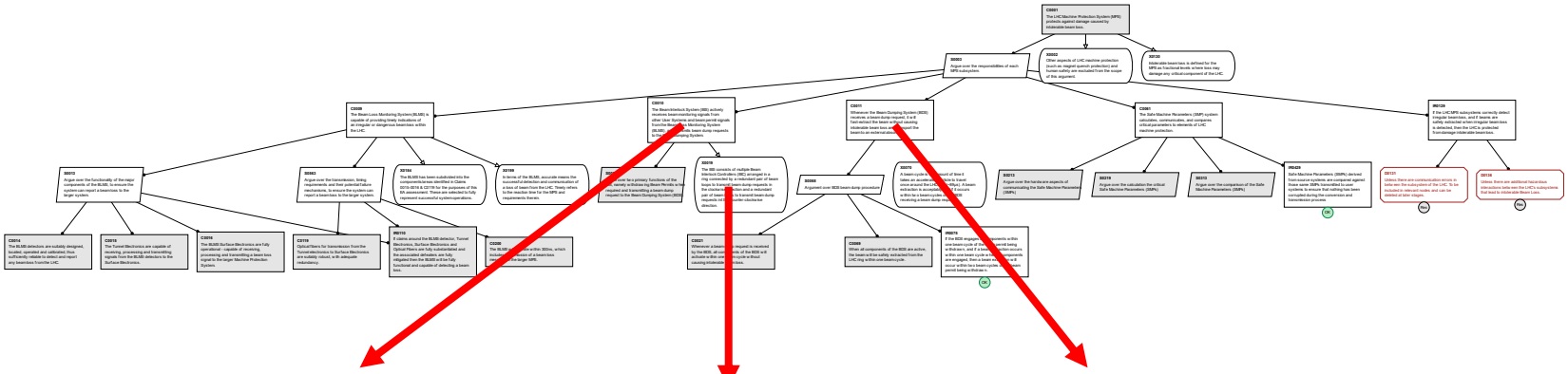
F.Bordry, R.Denz, K-H.Mess[1], B.Puccio, F.Rodriguez-Mateos and R.Schmidt

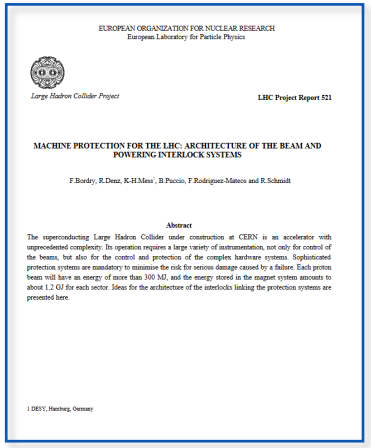
Abstract

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

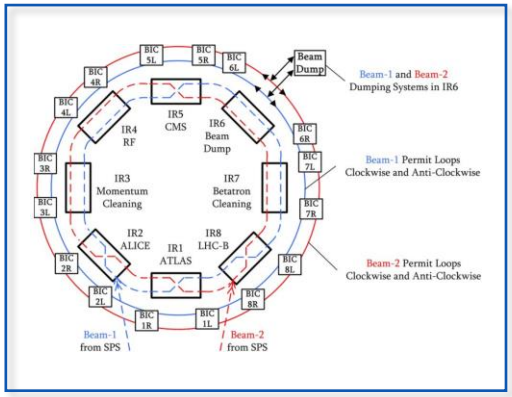
MACHINE PROTECTION FOR THE LHC: ARCHITECTURE OF THE BEAM AND POWERING INTERLOCK SYSTEMS

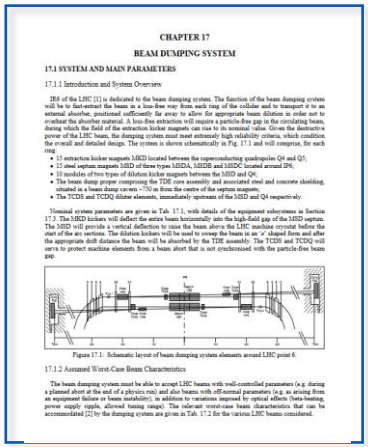
F.Bordry, R.Denz, K-H.Mess[1], B.Puccio, F.Rodriguez-Mateos and R.Schmidt

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 MSD 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 'x' 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.

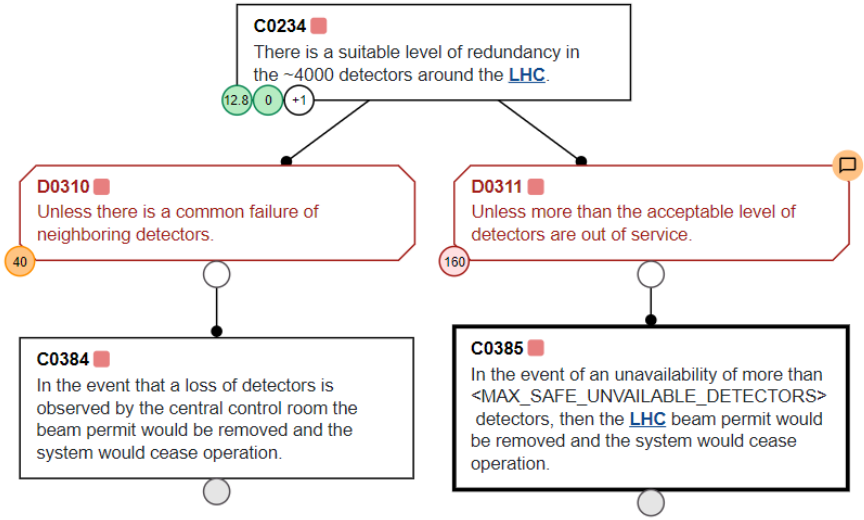
Figure 17.1: Schematic layout of beam dumping system elements around LHC point 6.

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.

“Live” Assurance Case with KPIs

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



Leading Indicator: *distance between damage dectectors*

AC Tools Capabilities

- Necessary Capabilities
  - Navigation Features
  - Collaborative Environment
  - Linking Artifacts
  - Version Control
  - Impact Analysis
- Good to have Capabilities
  - Natural Language Processing
  - Static Analysis
  - Conformance Traceability
  - Metrics / Dashboard

Socrates
Assurance Case Editor

https://criticalsystemslabs.com/socrates/

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
  - Assurance Case identified some interesting "cross cutting" inter-dependencies between sub-systems.
- A middle size public Argument available to academia and the industry
- Assurance Case Tools support retrospective

Laure Millet, Ph.D.
VP Research
laure.millet@cslabs.com