*Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)*
*Edited by* Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P152-cd

# A discussion on the use of Eliminative Argumentation (EA) to identify Key Performance Indicators (KPIs) for the CERN LHC Machine Protection System.

Chris Rees, Adam Casey, Jeff Joyce

*Critical Systems Labs, Vancouver, Canada.*

*E-mail: chris.rees@cslabs.com, adam.casey@cslabs.com, jeff.joyce@cslabs.com*

Jan Uythoven, Markus Zerlauth, Lukas Felsberger

*European Organization for Nuclear Research (CERN).*

*E-mail: jan.uythoven@cern.ch, markus.zerlauth@cern.ch, lukas.felsberger@cern.ch*

Torin Viger

*University of Toronto*

*Email: torin.viger@mail.utoronto.ca*

## Abstract

Key Performance Indicators (KPIs) and Safety Performance Indicators (SPIs) form an integral part of the Safety Management System (SMS) for a selected system. They provide a key insight into the system's safety performance and risk management, and enable data-driven decision-making.

A KPI for a system is defined as "a quantifiable measure used to evaluate the success of an organization, employee, etc. in meeting objectives for performance". The KPIs discussed within this paper denote a measure of success/performance of the relevant identified sub-systems. Integration of KPIs and SPIs serves as a method of performance and safety evaluation of the systems they are associated with. KPIs can be used to estimate the safety performance of a system, as well as to support the safety case and ensure that it remains "fit for purpose" and "live".

The paper also discusses how KPIs can be grouped into "leading" and "lagging" indicators. A leading indicator is one that tracks the occurrence of events that, while not themselves harmful, are expected to precede, or indicate the potential for, more harmful events. A lagging indicator is one that tracks the occurrence rate of hazards and/or loss events, such as crashes, injuries and fatalities. Leading and lagging indicators have limitations, advantages and disadvantages, which will be discussed further in the paper. Further we also discuss the challenges of accurate data collection to support KPIs.

KPIs have a variety of potential uses, such as tracking safety trends over time, measuring system compliance to regulations/legislation, and providing evidence for the system's safety case. This paper will focus on how KPIs can be defined from the safety (assurance) case assessment process. Specifically, this paper demonstrates the use of Eliminative Argumentation (EA) to define the potential hazards associated with the machine protection system at the nuclear research facility CERN. We discuss the evaluation and identification of the KPIs for each of these systems. Further, we show how performance indicators are identified with the EA assessment and the corresponding nodes, whilst demonstrating how the content of this assessment is linked via a "golden thread". We show how they can be analysed post-mortem to ensure that the safety case remains valid and "live" as the system changes. Finally, we discuss how the use of KPIs can benefit the safety case and why ensuring that it remains "live" (fit for purpose) is critical to the continued safe operation of a system.

In summary, KPIs play a critical role in keeping a safety case live by providing ongoing monitoring, driving continuous improvement, providing documentation, and establishing accountability for safety performance. By using them effectively, organizations can ensure that safety goals are being met over time.

*Keywords*: *Safety Case, CERN, Nuclear Research, Machine Protection System, LHC, Risk Assessment, HAZOP, FMEA, SWIFT, EA, Performance Indicators, SPIs, KPIs.*

## 1. Introduction

Safety Performance Indicators (SPIs) and Key Performance Indicators (KPIs) form an integral part of the Safety Management System (SMS) for a system. They provide a valuable insight into the system's safety performance, risk management and enable data-driven decision making.

Thus, the safety case can benefit from KPIs/SPIs by remaining "live" ("current") and having a "golden thread" back to the requirements of key (safety) performance indicators.

KPIs/SPIs have historically been identified from hazard assessment techniques such as Hazard Operability (HAZOP), Failure Modes Effects Analysis (FMEA), etc. studies. However, there are very limited public examples of KPIs/SPIs being defined from Eliminative Argumentation (EA). This paper looks to demonstrate how EA can be successfully used to identify KPIs for a complex safety case. Note: the subsequent research questions are defined in Section 4: Methodology.

## 2. Background

### 2.1 *Safety Cases*

Safety Cases, also sometimes referred to as Safety Assurance Cases, have a long history that can be traced back to the early 20th century. The primary purpose of these assessments is to ensure that the public and workers are protected from potential harm caused by accident or failure scenarios. The concept of a safety case assessment was first introduced in the UK in the 1970s in response to the need for a systematic approach to assessing the safety of high hazard industries (*R. Shaw, 1995)*.

Since then, the use of safety cases has expanded worldwide to other industries and sectors, including nuclear, oil and gas, aerospace, transportation, and pharmaceuticals. The main goal of these assessments is to identify and evaluate potential hazards, as well as to demonstrate that appropriate measures have been taken to minimize the risk of harm to the public and workers. Ultimately the safety case aims to demonstrate that identified risks are 'As Low As Reasonably Practicable (ALARP) or 'As Low As Reasonably Achievable (ALARA)'.

In order for safety cases to remain valid for a selected system, the hazard assessment and associated claims need to remain "live". Hence, there is a requirement to ensure that safety cases remain live, accurate and highlight key performance (safety) claims on a system to end users and stakeholders.

### 2.2 *Performance Indicators*

Within this paper we discuss two types of performance indicators for the selected systems safety case, namely:

**Key Performance Indicators (KPIs)**

KPIs are quantifiable and detectable measurements of events whose rate of occurrence can be used to gauge the performance of a system. Identifying KPIs helps develop and manage a system, as they give concrete measurements that can be analysed to determine whether a system or its subsystems are functioning correctly.

The works discussed in this paper assessed the performance indicators associated with the Machine Protection System (MPS) of CERNs Large Hadron Collider (LHC). From this, two types of measurements for KPIs were identified as leading and lagging indicators:

- Leading indicators measure the occurrence of events that, while not themselves harmful, are expected to precede or indicate the potential for future failures.

- Lagging indicators track the occurrence rates of hazards, loss events and violations of "safety barriers", such as crashes, breach of operating rules, injuries, and fatalities.

Lagging indicators are heavily dependent on collecting data after a loss event and leading indicators precede a potential failure. Thus, the use of leading and lagging indicators alone to measure a system's performance is not ideal. The two indicators are complementary: lagging indicators detect the occurrence of hazards and loss events when they occur, whereas leading indicators can process larger amounts of data and pre-emptively detect problems in performance.

**Safety Performance Indicators (SPIs)**

It should be noted that KPIs are distinct from SPIs. SPIs are metrics that are used to measure and evaluate the safety performance of a system or process. SPIs can be quantitative or qualitative and are typically developed based on specific safety goals and requirements.

Note: the focus of this paper and the work with CERN on the LHC MPS concentrated on the identification and substantiation of KPIs only. SPIs are noted here for information only.

### *2.3 Eliminative Argumentation*

Eliminative Argumentation (EA) *(J. Goodenough, et al. 2015)* is a graphical notation for AC development that extends the Goal Structuring Notation (GSN) *(GSN Working Group, 2011)*. EA enables us to express reasons to doubt safety case claims using defeater nodes. EA has been shown to be easy to learn, facilitates independent review and emphasises the importance of doubt *(S. Diemert, et al, 2020)*. EA utilises nodes of different types for assessment of a system, namely:

- *Claim nodes* express affirmative statements asserting that a system satisfies one or more properties.

- *Defeater nodes* express doubts about the validity of an assurance argument. Defeaters are unique to EA, whereas the other node types presented in this section are also included in other notations such as GSN. A defeater can be decomposed into nodes showing how it has been mitigated, or it may be left as residual risk that threatens the argument's validity.

- *Strategy nodes* express reasoning steps used to decompose a claim into more refined subclaims.

- *Context nodes* are used to provide background information or missing details that may be necessary to understand the argument.

- *Inference rule nodes* are attached to strategy nodes and are used to explain the rationale for why a strategy's child claims are sufficient to show that the parent claim holds. Inference rules may also be referred to as justification nodes (e.g., in GSN).

- *Assumption nodes* may be used to list conditions related to the system or its operational environment that are assumed to be true in the argument.

EA was used as the basis for the assessment of the safety case for the LHC MPS, which included the identification of KPIs.

## 3. CERN Large Hadron Collider

The CERN Large Hadron Collider (LHC) is a particle accelerator and collider built by the European Organization for Nuclear Research (CERN). Building the LHC required approximately 10 years and a material cost of approximately 4.6 billion SFr, ≈ 4.4 billion USD (*Wikipedia, 2023*). The LHC was selected as our case study because (a) it is a large and representative complex system; (b) it is carefully documented; (c) the documentation is publicly available; and (d) we had contact with CERN engineers that could help us to answer our research questions around the defining of KPIs.

The LHC enables testing of theories and investigating unanswered questions in particle physics by observing collisions between accelerated particles. The LHC consists of two 27-kilometer-long rings that accelerate particles to nearly the speed of light in opposite directions (see Figure 1). Particle beams travel around each ring in clusters (with particle-free gaps between them), and over 10,000 superconducting magnets are used to bend and focus two counter rotating beams around the ring. During collisions the trajectories of these beams are diverted so that they intersect and collide, and phenomena related to the collision are then detected and analysed by a range of sensitive scientific detectors.

Figure 1 – CERN Large Hadron Collider ring and tunnel containing superconducting magnets for the guidance of the particle beams *(CERN Website, 2022)*.

The accelerated particle beams used in experiments have very high energy and pose a significant risk of damage to the system if their trajectories become unstable (one proton beam within the LHC has the stored energy of an aircraft carrier moving at 12 knots).

The protection of the LHC is provided in part via the Machine Protection System (MPS). The MPS is composed of inter-dependent systems designed to ensure that the LHC does not become damaged during operation. It proactively protects the system by monitoring all conditions that could lead to damage, and issuing a beam dump (i.e., extracting all particles from the LHC rings) before hazardous scenarios occur.

The MPS consists of four main components: the Beam Loss Monitoring System (BLMS), the Beam Interlock System (BIS), the Beam Dumping System (BDS) and the Safe Machine Parameters (SMP). All of these subsystems need to operate and intercommunicate correctly to ensure the functionality of the MPS and protection of the LHC.

The MPS has a postmortem system designed to analyze and diagnose the causes of equipment failures or accidents that occur in the LHC. This system uses a combination of hardware and software tools to monitor and record data from various sensors and detectors installed throughout the machine, including electrical and thermal sensors, beam position monitors, and radiation detectors. If an event occurs, the system can quickly identify the source of the problem and provide engineers with a detailed report that includes information on the sequence of events leading up to the incident, potential causes, and recommended corrective actions.

## 4. Methodology

The safety case and defining of suitable performance indicators for this case study of the LHC MPS involved a team of four people. Three of them were industry safety experts, working for a consultancy specializing in safety case development. These engineers have a combined experience in safety case development of over 25 years. The final member of the team was a PhD student with four years research experience in safety case development.

The questions posed for the study of performance indicators for the MPS, and to be answered within this paper, are as follows:

- **Research Question (RQ1**) - How can EA be successfully used to identify KPIs for a system's safety case?
- **Research Question (RQ2)** - How can it be demonstrated that KPIs can directly assist in keeping a safety case live?

The project completed an EA for the safety case for the LHC MPS in late 2022. This was presented, and agreed with CERN experts, as being an accurate representation of the case for the operation and claims on the MPS.

Post this submission, members of the project team have defined a number of KPIs for the MPS. The KPIs are based on the identification of systems/functions/events whose performance can be monitored to ensure the successful operation of the MPS. These have been identified in addition to the parameters measured by the LHC Post-Mortem System. Note: the KPIs were assessed against the relevant subsystems of the MPS, namely, the BLMS, the BIS, the BDS and SMPs.

## 5. Performance Indicator Analysis

### *5.1 LHC MPS*

Through our wider work on the safety case for the LHC MPS we have concluded that development of a case using EA is useful to accurately identify doubts about a system *(S. Diemert, et al, 2020)*. As part of this work, we had numerous interactions with CERN experts, which included a discussion and definition of KPIs.

These discussions, and project team assessment work led to the identification of 19 KPIs (12 lagging and 7 leading indicators) for the LHC MPS. These were identified by analysing claims and defeaters related to measurable aspects of the system's performance, and events which can be monitored by the LHC MPS. The KPIs were mainly derived from key Claim, Residual and Undeveloped nodes, where monitoring the system could provide data to help measure and mitigate potential residual risks. As an example, the KPI BLMS-KP2 (a lagging indicator) states that "A failure of a single, or multiple, BLMS detector(s) would be reported to the control room, and thus a user permit not granted for operations" is derived from Claim C0140 - "Detector failures will be identified and reported to the central control room", within the case.

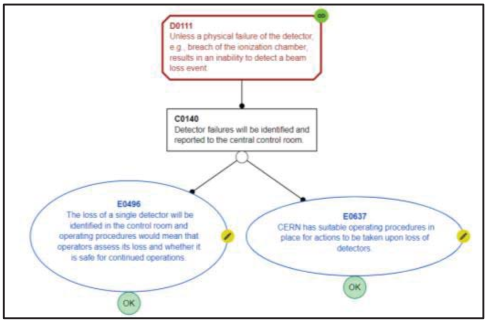
D0111
Unless a physical failure of the detector, e.g., breach of the ionization chamber, results in an inability to detect a beam loss event
C0140
Detector failures will be identified and reported to the central control room.
E0496
The loss of a single detector will be identified in the control room and operating procedures would mean that operators assess its loss and whether it is safe for continued operations.
E0637
CERN has suitable operating procedures in place for actions to be taken upon loss of detectors.
OK
OK

Figure 2 – Snapshot of argument, including Claim C0140, where BLMS-KP2 originates from.

Our experience shows that the EA has enabled these KPIs to be easily identified from the wider argument (approximately 500 nodes), due to the structure of the argument and the ease of identifying residual risks, claims and defeaters.

These KPIs were shared, reviewed, and discussed with CERN experts, who confirmed that these KPIs are reasonable and largely addressed by their existing postmortem system. The CERN postmortem system will identify items such as missing redundancy between systems or within a system. Operations can only continue after redundancy and fully nominal conditions have been re-established. The fact that the identified KPIs have been considered by the postmortem system of the LHC confirms that they are reasonable, demonstrating that safety case development and the use of EA can help identify KPIs that mitigate residual risks in a system. KPIs are noted to benefit the postmortem analysis, namely performance tracking, root cause analysis, communication, and reporting. In addition, the discussion related to some KPIs aided in identification of potentially unrealized loss events.

### *5.2 List of Identified KPIs*

The following presents some key examples of identified KPIs along with their area of operation:

**Beam Loss Monitoring System (BLMS)**

- BLMS-KP1 (Leading Indicator): The tolerability for number of potential failures for the BLMS detectors during a single run is greater than **>99% (MIN_DETECTOR_KPI_THRESHOLD).**

- BLMS-KP2 (Lagging Indicator): The number of unreported critical failures of the BLMS detector is less than **one** per run **(MIN_CRITICAL_FAILURES**).

- BLMS-KP3 (Lagging indicator): This KPI notes the number of times the tunnel electronics initiate a beam dump due to energy levels outside the specified range **(OUTSIDE_BEAMDUMP_RANGE**).

**Beam Interlock System (BIS)**

- BIS-KP1: Interlock Response Time (Leading Indicator) – KPI notes the number of times, during a run, the BIS fails to react to events within the specified response times. **(MIN_BISRESPONSE_KPI).**

**Beam Dump System (BDS)**

- BDS-KP1 (Leading indicator): The number of asynchronous beam dumps do not exceed 1 in a 365-day period, e.g. number of times when the system loses track of the particle bunches in the ring **(MIN_ASYNC_BEAMDUMP).**

- BDS-KP2 (Lagging indicator): The frequency a failed MKD kicker magnets in a run: the tolerable threshold for this KPI is if 1 out of the MKD 15 magnets fails in a run **(MIN_KICKMAG_KPI).**

- BDS-KP3 (Lagging indicator): Number of failed MKB diluter magnets in a run: the tolerable threshold for this KPI is if 1 of 4 horizontal MKB diluter magnets to fail, as well as 1 of 6 vertical MKB diluter magnets **(MIN_MAGFAIL_KPI).**

## 6. Related Work

The oil and gas industry is a crucial sector of the global economy, and as such, there is a lot of research and industry interest in ways to measure and improve its performance *(R. M. Elhunia, et al, 2017) (A. Crivellari, et al. 2019) (N. C. Onyemeh, et al. 2015)*. One approach that has gained considerable attention is the use of KPIs. In the oil and gas industry, like nuclear, KPIs are commonly used to track progress, identify areas for improvement, and make data-driven decisions.

There are several types of KPIs that are relevant to the oil and gas industry. Environmental indicators, for example, might include measures of carbon emissions, water usage, and waste management practices. Operational indicators might focus on metrics such as production efficiency, downtime, and equipment reliability. Quality indicators could encompass factors like product yield, compliance with regulatory standards, and customer satisfaction. Finally, performance indicators might involve measures of profitability, return on investment, and other financial metrics.

While KPIs have been widely used across various industries, their application to the oil and gas sector is still relatively new. Many organizations in the industry are exploring ways to incorporate KPIs into their operations to improve their sustainability, efficiency, and profitability. However, much of the research and industry focus on KPIs in the oil and gas industry has been limited to small showcase examples. This means that there is still much work to be done to fully understand the potential benefits of KPIs in this sector and how they can be effectively implemented at scale. To benefit this, and the nuclear industry, the KPIs published in this paper and the associated argument have been made publicly available.

## 7. Conclusions

In this paper, we have evaluated the use of EA to identify KPIs for the LHC MPS. In this section we present our findings to the two RQs presented in this paper.

### RQ1

By analyzing the various claims, defeaters and residual risks in an EA it has been shown that you can easily identify KPIs for a safety case. Further, the use of EA allows a user to eliminate any arguments that are flawed, such as those based on incorrect assumptions or faulty data. Thus, further supporting the process to correctly identify the strongest and most valid arguments, which could then be used to inform the selection of KPIs.

Once KPIs have been identified via a review of the EA, there are several benefits to the safety case, namely:

- Improved safety: Selecting KPIs that are directly related to safety goals, you can improve the overall safety of the system or process. Further, by monitoring these KPIs, you can quickly identify any potential safety issues and take corrective action before they become major problems.

- Better decision-making: KPIs provide a clear and objective way to measure progress and performance. By regularly reviewing these metrics, you can make more informed decisions about how to optimize the system or process to achieve the safety goals.

- Increased accountability: By establishing KPIs and monitoring them regularly, you can create a culture of accountability and responsibility within the organization. Everyone involved in the system or process can see the progress being made towards the safety goals, and they can be held accountable for their contributions to that progress.

Overall, it is noted that the use of EA to identify KPIs for a safety case can help to improve the safety and performance of the system or process, while also promoting accountability and informed decision-making.

### RQ2

KPIs play a critical role in keeping a safety case live by providing ongoing monitoring and evaluation of safety performance. They enable the safety case to remain live via:

- Regular monitoring: monitoring KPIs regularly ensures that safety performance is being measured accurately and effectively. This ongoing monitoring helps to identify any potential safety issues before they become major problems and allows for corrective action to be taken as needed.

- Continuous improvement: KPIs can help to drive continuous improvement in safety performance by providing a clear and objective way to measure progress. By regularly reviewing these metrics, organizations can identify areas where safety performance could be improved and take action to make those improvements.

- Documentation: KPIs provide documentation of safety performance over time. This documentation helps to demonstrate that safety goals are being met and provides evidence of ongoing safety performance for regulatory agencies, stakeholders, and other interested parties.

- Accountability: By establishing KPIs, organizations can create a culture of accountability and responsibility for safety performance. Everyone involved in the system or process can see the progress being made towards safety goals and can be held accountable for their contributions to that progress.

In summary, KPIs play a critical role in keeping a safety case live by providing ongoing monitoring, driving continuous improvement, providing documentation, and establishing accountability for safety performance. KPIs form an integral part of keeping safety cases live, they are identified as part of the case construction process, namely hazard analysis, safety case construction, identification of KPIs, and monitoring and feedback (see Figure 3). By using KPIs effectively, organizations can ensure that safety remains a top priority and that safety goals are being met over time. Further, KPIs can be databased with the ability to be queried. Some KPIs could also lead to additional instrumentation being added to a system to monitor performance.

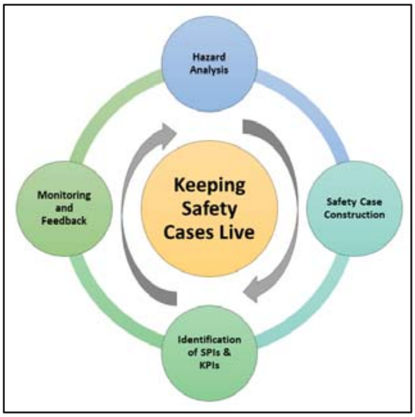

Figure 3 – Keeping safety cases live, assessment process and identification of SPIs/KPIs.

For example, if a safety engineer has identified a particular hazard associated with a safety-critical system, they may develop a KPI to monitor the system's performance in relation to that hazard. The KPI could be a measure of the frequency of the hazard occurring, or the severity of the consequences if the hazard were to occur. By monitoring the KPI, the safety engineer can ensure that the system remains safe and that any potential safety risks are identified and addressed.

In conclusion, EA is a powerful tool for identifying KPIs that are critical to ensuring system safety. By using KPIs to monitor system performance, safety engineers can ensure that safety cases remain live and fit for purpose and that the system continues to meet safety requirements. (Test n.d.)

## Acknowledgement

We acknowledge the support of the support of CERN employees with this work. Along with the support of McMasters University and the University of Toronto.

## Acronyms

| | |
|---|---|
| BLMS | Beam Loss Monitoring System |
| BIS | Beam Interlock System |
| BDS | Beam Dumping System |
| EA | Eliminative Argumentation |
| KPI | Key Performance Indicator |
| LHC | Large Hadron Collider |
| MPS | Machine Protection System |
| RQ | Research Question |
| SMP | Safe Machine Parameters |
| SPI | Safety Performance Indicator |

## Terminology

"Golden thread" - refers to a logical and coherent chain of evidence that links the various elements of a system or process, providing transparency, traceability, and assurance that the safety case requirements have been satisfied.

"Fit for purpose" – refers to safety cases/arguments that are tailored to the specific needs of a system or process, and are designed to provide confidence to stakeholders that the safety requirements have been met.

## References

1. *R. Shaw*, "Safety Cases — How Did We Get Here?," Safety and Reliability of Software Based Systems, Twelfth Annual CSR Workshop , Vols. DOI: 10.1007/978-1-4471-0921-1_2, Bruges, 12–15 September 1995.

2. *J. Goodenough, C. Weinstock, A. Klein,* Eliminative Argumentation: A Basis for Arguing Confidence in System Properties, Tech. Rep. CMU/SEI-2015-TR-005, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA (2015). URL http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=434805.

3. GSN Working Group, GSN Community Standard Version 2, http://www.goalstructuringnotation.info/ (2011).

4. *S. Diemert, J. Joyce*, Eliminative Argumentation for Arguing System Safety - A Practitioner's Experience, in: Proceedings of International Systems Conference, IEEE, 2020, pp. 1–7

5. Large Hadron Collider, https://en.wikipedia.org/wiki/Large Hadron Collider

6. CERN Website Images, https://home.web.cern.ch/about

7. *Redha M. Elhunia, M. Munir Ahmadb*, Key Performance Indicators for Sustainable Production Evaluation in Oil and Gas Sector, 27th International Conference on Flexible Automation and Intelligent Manufacturing, FAIM2017, 27-30 June 2017, Modena, Italy.

8. *Anna Crivellari; Alessandro Tugnoli; Sarah Bonvicini; Anna Laura Garbetti; Valerio Cozzani; Paolo Macini*, Key Performance Indicators for Environmental Protection from Oil Spills During Offshore Oil & Gas Operations, Paper presented at the Offshore Mediterranean Conference and Exhibition, Ravenna, Italy, March 2019. Paper Number: OMC-2019-1021 Published: March 27 2019.

9. *N. C. Onyemeh, C. W. Lee and M. A. Iqbal*, "Key performance indicators for operational quality in the oil and gas industry a case study approach," 2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Singapore, 2015, pp. 1417-1421, doi: 10.1109/IEEM.2015.7385881.