Arguing Operational Safety for Mixed Traffic in Underground Mining

Julieth Patricia Castellanos Ardila, Sasikumar Punekkat, Hans Hansson and Christian Grante
IDT, Mälardalen University and Combitech AB, Sweden
Email: (julieth.castellanos, sasikumar.punnekkat and hans.hansson)@mdu.se and christian.grante@combitech.com

***Abstract*—Practitioners report improved productivity as one of the main benefits of using autonomous dump trucks in underground mining. However, manned vehicles are still needed to transport materials and personnel in the tunnels, which requires practices that may diminish autonomy benefits. Thus, both fleets shall be efficiently mixed to maximize the autonomy potential. In addition, sufficient safety shall be demonstrated for operations approval. This paper proposes a strategy to populate a GSN (Goal Structuring Notation) structure to argue for the sufficient safety of mixed traffic operations in underground mining. Our strategy considers SoS (System of Systems) concepts to describe the operations baseline and the initial argumentation line, i.e., risk reduction mitigation strategies for existing SoS components. Such a strategy is further detailed with risk reduction mitigation arguments for control systems. Mitigation strategies at both levels are derived from safety analysis supported by STPA (System-Theoretic Process Analysis), a safety analysis technique that aligns well with the SoS perspective. We also incorporate regulatory frameworks addressing machinery to align the arguments with mandatory statements of the machinery directive. Our strategy combines SoS concepts with analysis techniques and regulatory frameworks to facilitate safety case argumentation for operations approval in the European mining context.**

***Index Terms*—Mixed Traffic, Machinery Directive, Harmonized Standards, Safety Case Arguments, SoS, GSN, STPA.**

I. Introduction

Assigning repetitive tasks to autonomous dump trucks in underground mining has reported increased productivity and safety (e.g., Rio Tinto [1], Ferrexpo [2] and Boliden [3]). However, manned vehicles are still needed to transport materials and personnel in the tunnels. In such cases, priority must be granted to manned transportation, an operation that may diminish autonomy benefits. Thus, both fleets shall be efficiently mixed to maximize the autonomy potential [4].

Manned vehicles' operation ultimately relies on human control, e.g., a human can stop the car if needed [5]. Conversely, autonomous machines are equipped with assistance systems to decide their next move. In addition, underground mines are operational sites that rely on control systems to ensure productivity and safety [6]. However, most risks still arise from collisions in which heavy machinery is involved [7]. Such collisions, including manned vehicles, may result in catastrophic consequences, e.g., harming or even killing human operators.

This research has been supported by Vinnova via the project ESCAPE-CD (Efficient Safety for Complex Autonomous Production Environments - Concept Design) Reference: 2021-03662. We thank our industrial partner - Boliden Mineral AB- for the preliminary review of the proposed approach.

Collisions can be prevented with a Safety Control System (SCS), which halts autonomous machines by issuing an Automated Safety Stop Command (ASSC) upon risk discovery, i.e., manned machines in their proximity. The SCS shall provide a fail-safe strategy that shall be trusted. Thus, it is a safety-related control system that must have a robust design to ensure its reliable performance. As such, the SCS requires high levels of integrity and conformance to the Machinery Directive [8].

Sufficient safety shall be demonstrated for operations approval in the context of machinery. For this reason, this paper proposes a strategy to populate a GSN (Goal Structuring Notation) [9] structure to argue for the sufficient safety of mixed traffic operations in underground mining. As a starting point, we assume mixed traffic operations as an SoS (System of Systems) problem, i.e., constituent systems interacting to provide a unique capability [10]. The SoS perspective helps us to describe the operations baseline and the initial argumentation line, i.e., risk reduction mitigation strategies for existing SoS constituent systems and supporting systems. Such a structure is further detailed with risk reduction mitigation arguments for control systems. Mitigation strategies at both levels are derived from safety analysis supported by STPA (System-Theoretic Process Analysis) [11], a methodology that aligns well with the SoS perspective since it provides analysis means for high-level interactions between different systems that include control actions [12]. Finally, we incorporate the best practices included in harmonized standards [13] (i.e., standards that provide a presumption of conformance with the machinery directive). In particular, we use the standard EN ISO 12100:2010 [14] to support the argumentation related to the risk management process for the general operation. Then, we use the standard EN ISO 13849-1:2015 [15] to support the control system level argumentation. We illustrate the applicability of our strategy by considering a case study from a European mining company. Our strategy combines SoS concepts with safety analysis techniques and regulatory frameworks to consolidate safety case arguments for operations approval in the European mining context.

This paper is organized as follows. Section II presents essential background information. Section III presents our proposed argumentation strategy. Section IV presents a case study. Section V presents the discussion of the findings. Section VI presents related work. Finally, Section VII presents the conclusions and future remarks.

II. Background

A. Safety Case and the Goal Structuring Notation

An assurance case, according to the standard ISO/IEC/IEEE 15026-1:2019 [16], is *a reasoned, auditable artifact created to support the contention that its top-level claim (i.e., a true-false statement about the limitations on the values of an unambiguously defined property) is satisfied*. When the assurance case is related to safety, it is called a safety assurance case (for short, a safety case). A safety case can be defined as a reasoned and compelling argument supported by a body of evidence demonstrating that a given system (or, as in our case, an SoS) is acceptably safe in a given context and under given assumptions. To document safety cases, several approaches exist. This paper focuses on the Goal Structuring Notation (GSN) [9], which is notation based on graphical elements (see Fig. 1).

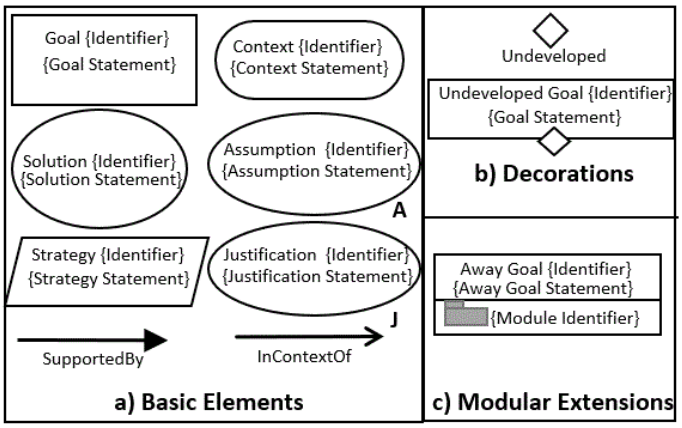

Fig. 1: GSN Elements.

In particular, GSN starts with a top-level goal supported by a reasoning step called strategy that connects the goal with subgoals and solutions (evidence). Goals and strategies can be derived under specific assumptions and justifications in a particular context which explain why the claim is acceptable. Those elements (see Fig. 1a) are connected with two types of relationships: SupportedBy (link claims with strategies/evidence) and InContextOf (link claims/strategies with contextual information). GSN provides decorators (see Fig. 1b). For example, the hollow diamond, added to a goal, represents an undeveloped goal, i.e., a goal to which the line of argument still needs to be developed. GSN structures can also be partitioned into separate packages (see Fig. 1c), e.g., an away goal represents a claim presented in another module.

B. System of Systems (SoS)

A system of Systems (SoS) is a *set of systems or system elements that interact to provide a unique capability that none of the constituent systems can accomplish on its own* [10]. According to Maier [17], these constituent systems have operational and managerial independence (i.e., they meet an individual valid purpose and are managed independently). However, component interactions also produce emergent behaviors that are more complex than the component's original behavior [18]. As such, the SoS requirements cannot be limited to the core functional performance of such components. In particular, an SoS has a hazards space, which combines the hazards resulting from individual components that affect the SoS-specific purpose and the hazards that result from components interactions [19]. Those hazards, called emergent hazards, shall also be considered during the safety assurance process.

C. The Machinery Directive and Harmonized Standards

The Machinery Directive [8] is a European regulation that establishes safety requirements for the design and construction of machinery. In particular, Annex I mandates a risk management strategy guided by the standard EN ISO 12100:2010 [14]. This standard prescribes a risk management process composed of three activities. First, the identification of the machinery limits. Second, the risk analysis and assessment, where hazards are identified and their risk is estimated. Finally, the risk reduction strategy where safe design measures, complementary safeguarding, and information for use shall be implemented.

Clause 1.4.3. considers the design of control systems as a protective measurement for different hazards. Guidance for this aspect is provided in the standard EN ISO 13849:2015 [15], which assumes performance levels (PL) for the design and integration of safety-related parts of control systems. A PL is a level between a to e, with e being the most stringent, which is used to specify the ability to perform a safety function. One specific protective measurement is the emergency stop (see clause 1.2.4.3), guided by the standard EN ISO 13850:2015 [20]. Additional safeguarding measures, e.g., halting the operation automatically (Clause 3.3.3), could also be included if the risk assessment results require it.

D. System-Theoretic Process Analysis (STPA)

STPA [11], [12] is a hazard analysis technique that comprises four steps. First, the system of interest is defined, and potential accidents and hazards related to the application scenarios are identified. Second, a control structure is modeled by considering the feedback control loops between their functional components. Third, unsafe control actions (UCAs), i.e., actions that could lead to losses, are identified. Control actions can be unsafe in different ways. We focus on two cases, i.e., when the control action is not provided and when it is provided too late. Fourth, the loss scenarios must be considered for each UCA. In particular, there may be unsafe controller behavior due to failures in the controller, inadequate control algorithm, unsafe control inputs, and inadequate process model or feedback.

III. Argumentation Strategy for Mixed Traffic

As presented in the introductory part of this paper, sufficient safety shall be demonstrated for operations approval in the mining context (especially in the European context). A way to do this is by creating a safety assurance case (as recalled in Section II-A), which shall show not only acceptable levels of safety but also the required degree of conformance to

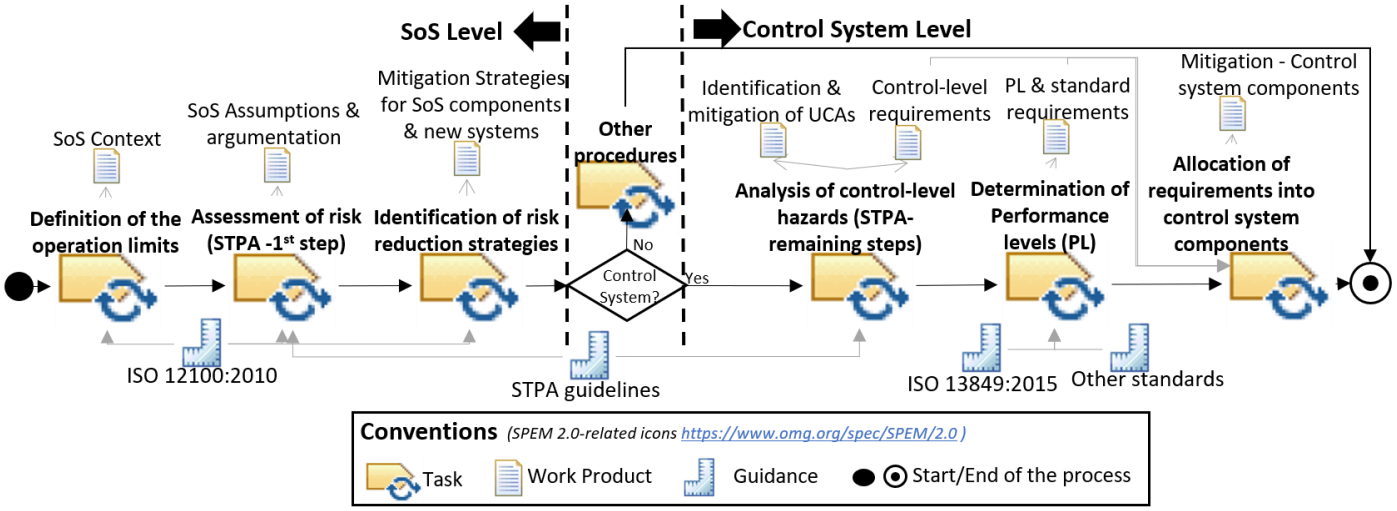

Fig. 2: Argumentation Strategy for Mixed traffic.

the machinery directive. In particular, the safety of mixed-traffic operations can be seen as an SoS problem (recalled in Section II-B) where different constituent components are part of such operation, i.e., autonomous machines, manned vehicles, and human operators. Constituent components of such an operation interact independently to reach a goal. In addition, it is possible to change them from one mine to another to do the same job. Thus, addressing safety in this context will require the mitigation of emergent hazards by improving existing SoS components and designing new supporting systems to take care of the loss scenarios. The safety case shall show that those mitigation strategies are adequate and follow mandatory statements from the machinery directive (recalled in Section II-C).

This paper proposes a strategy for populating the safety case in GSN (recalled in Section II-A). Such a strategy (depicted in Fig. 2) produces SoS and control-related arguments. On the SoS side, we have three tasks extracted from the standard ISO 12100:2010. First, the **definition of the operation limits**, which produces the context of the initial argument. Then, the **assessment of risk**, which is supported by the first step of the STPA (recalled in Section II-D), produces the SoS assumptions and first argumentation line. Finally, the **identification of the risk reduction strategies**, which produces the mitigation strategies for SoS components and eventual new systems.

If risk reduction strategies target control systems, we continue at the control system level. First is the **analysis of control-level hazards**, a task supported by the remaining STPA steps. Its results define the argumentation strategy based on identifying and mitigating unsafe control actions. Second, we **determine performance levels (PL)**, which is a step based on the standard EN ISO 13849:2015. The PL defines standard-related requirements, which, combined with the ones acquired from the hazard analysis, are **allocated into different control system components**. Strategies beyond control systems require other procedures not addressed in this paper. We may use other standards when allocating requirements to make further use of best practices, enforcing the claims of the safety case.

IV. Case Study

The use case consists of a tunnel where a fleet of autonomous machines is mixed with a fleet of manned vehicles. In this section, we follow the strategy defined in Section III to create safety case arguments for such an operation.

A. Definition of the Operation Limits

The tunnel has an Autonomous Operating Zone (AOZ) used only for traffic operations (areas in blue color in Fig. 3) with a principal entrance/exit for autonomous machines (shown in yellow). The AOZ shall also permit the transit of manned vehicles (shown in orange), which have specific access/exit points (orange areas). Both autonomous and manned vehicles have buffer areas (displayed in gray) for waiting their turn to enter the AOZ. Meeting areas (depicted in red) and prospected drilling areas (shown by one side tunnel ending in a dead-end room) are alongside the tunnel. This information is part of the context C1 in Fig. 4.

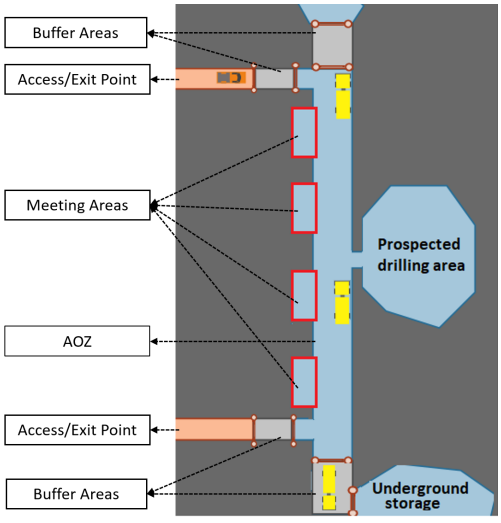

Fig. 3: Tunnel AOZ.

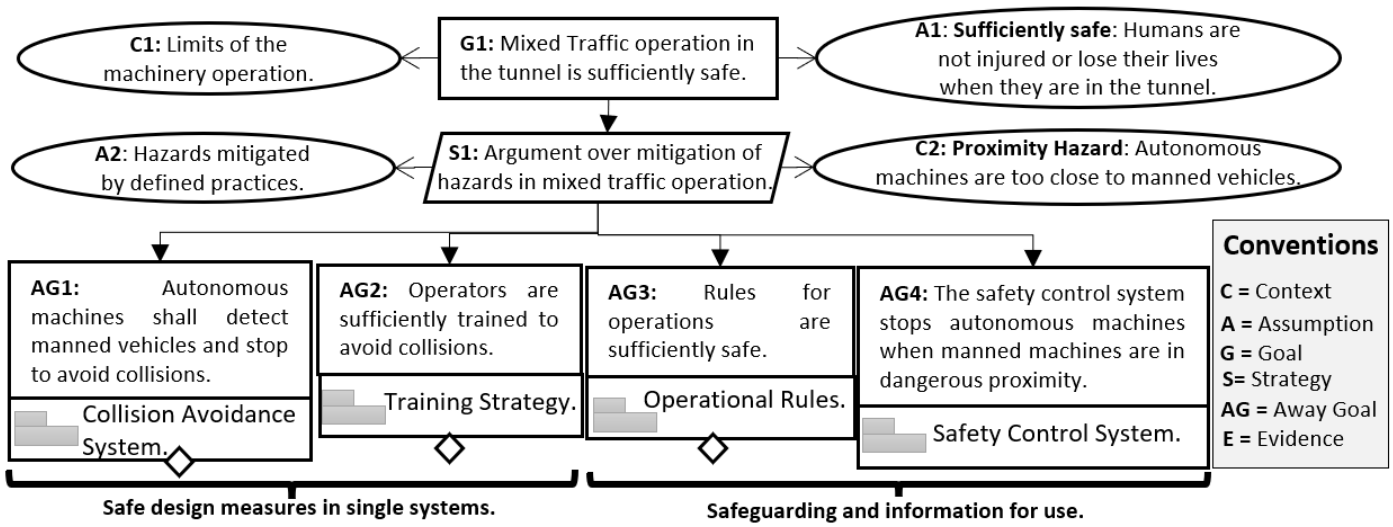

Fig. 4: GSN Argument for Machinery Operations.

B. Assessment of Risk (STPA - First step)

Mixed Traffic operations are a novelty in the mining industry. It considers rules for the operation aimed at mitigating some hazards (A2 in Fig. 4). First, manned machines shall check in at their gate and wait for approval to pass. Second, zones near the manned vehicles shall not be occupied by autonomous machines. Third, autonomous machines shall be located in parking areas, their gates, or outside the tunnel when manned vehicles enter the AOZ. The traffic flow of the mixed operations is managed through the traffic management system, which offers traffic monitoring, route planning, and optimization based on operational needs. It also helps the human supervisor to solve potential conflicts. However, unsafe situations could arise from the unpredictable behavior of autonomous machines in harsh environments and the misbehavior of the humans involved in the operation. These situations could result in the risk of having autonomous machines in dangerous proximity to manned vehicles, which could lead to the loss we are trying to avoid, i.e., humans are injured or lose their lives when they are in the tunnel (A1 in Fig. 4). In this case, the system-level hazard is that autonomous machines are too close to manned vehicles (C2 in Fig. 4).

C. Identification of Risk Reduction Strategies

The analysis with domain experts resulted in four mitigation strategies. First, a safe design is required for the autonomous machines, i.e., they shall stop upon detecting manned vehicles. One way to fulfill this aspect is by considering stringent requirements for the collision avoidance system of the autonomous machines (AG1 in Fig. 4). Second, sufficient training for the operators, who are also constituent systems of the SoS, is also required (AG2 in Fig. 4). The following two strategies correspond to information for use in the form of rules for mixed operation (AG3 in Fig. 4) and a safeguarding strategy, which corresponds to a safety control system (SCS) (AG4 in Fig. 4). In particular, the SCS shall halt autonomous machines when they are too close to manned machines.

D. Analysis of Control-level Hazard (STPA remaining steps)

We perform a hazard analysis in a small representation of the SCS control structure (see Fig. 5), which was fully developed in our previous work [4].

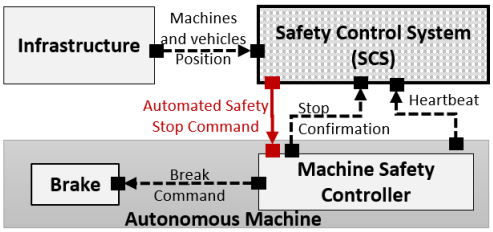

Fig. 5: Control Structure for the SCS.

As Fig. 5 depicts, the infrastructure sends the position of the manned vehicles and autonomous machines from sensors. The SCS processes this information and provides the automated safety stop command (ASSC) to the autonomous machines if needed. Machine brakes actuate the ASSC received via their machine safety controller. Once the machine stops, a notification is sent to the SCS. In addition, the safety controller of the autonomous machines (also for the manned machines, which are not depicted in the figure) sends a heartbeat to the SCS to guarantee their connection to the system.

There is a red arrow from the SCS to the machine safety controller (see Fig. 5), which represents the control action (CA) of interest in this analysis, i.e., the ASSC is provided when an autonomous machine is too close to a manned vehicle. This CA becomes unsafe in several ways (Table I).

TABLE I: UCAs and System Safety Requirements

UCA	Safety Requirement
UCA1: The ASSC is not provided when an autonomous machines is too close to a manned machine.	**SR1:** The ASSC shall be always available and operational.
UCA2: The ASSC is provided too late when an autonomous machines is too close to a manned machine.	**SR2:** The ASSC command shall be provided withing t milliseconds after the detection of dangerous conditions .

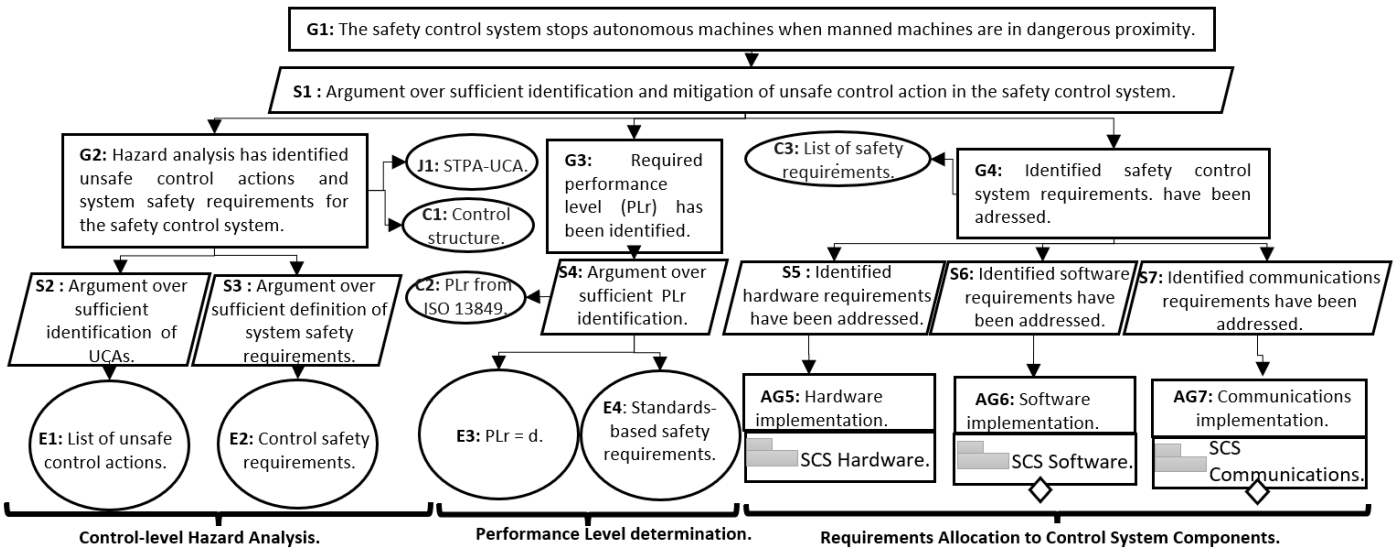

Fig. 6: Argument over Away Goal AG4.

We focus on cases when the CA is not provided and when it is too late (first column of Table I). Safety constraints for addressing the UCAs are defined by considering the requirements of a closely related control system, i.e., the emergency stop function, developed in the standard EN ISO 13850:2015 (second column in Table I). UCAs and requirements are the evidence required to argue sufficient control-level hazard analysis as presented in Fig. 6 on the left side.

E. Determination of Performance Level

According to EN ISO-13849:2015 [15], the performance level required (PLr) is calculated by combining three risk parameters. First, the severity of injury (S), which can be S1 (slight, normally reversible injury) or S2 (serious, normally irreversible injury or death). Second, the frequency and/or exposure to hazard (F), which can be F1 (seldom-to-less-often and/or exposure time is short) or F2 (frequent-to-continuous and/or exposure time is long). Third, the possibility of avoiding hazard or limiting harm (P), which can be P1 (possible under specific conditions) or P2 (scarcely possible).

The injury's severity could be serious if a collision between an autonomous and a manned vehicle occurs (S2). Instead, the exposure is short since manned transportation occurs only a few times during operation (F1). However, if a collision occurs, it is not easy to limit the harm (P2). Thus, the PLr of the ASSC shall be d. This result is compatible with the determination of the PLr suggested by the standard ISO 13850:2015, clause 4.1.5.1. which considers a minimum PLr of c. The definition of PLr and its corresponding evaluation is the evidence required to argue sufficient performance level identification as presented in the middle part of Fig. 6.

F. Requirements Allocation into Control System Components

UCAs can lead to a loss when the safety requirements defined in Table I are not fulfilled due to specific causal factors. In particular, there may be flaws in the creation of the safety control algorithm, inadequate coding of the software, or inconsistent, incomplete, or incorrect determination of machines and manned vehicle localization (SCS - software). In addition, there may be a failure in the processor, the sensors used in the infrastructure or the machines, and the brake in the autonomous machine (SCS - hardware). Finally, there may be delayed information from the sensors, missing feedback or feedback delays from the autonomous machines and the manned vehicles, and failure in the communications between the infrastructure, the SCS, the autonomous machines, and the manned vehicles (SCS - communications).

In addition, the standard EN ISO-13849:2015 prescribe requirements according to PLr d. In particular, there are requirements regarding the type of architecture (e.g., double channel architecture) and the evaluation of the PL achieved with such architecture. Moreover, there is a specific requirement on the software construction, such as the provision of particular work products related to mandatory activities of the software life cycle, e.g., code documentation and test cases. This means that we need to allocate and fulfill safety requirements into software, hardware, and communications components of the SCS, as presented on the right side of Fig. 6.

We develop AG5 further in Fig. 7. As mentioned, hardware causal factors exist for UCAs failures. We also noted that PLr d requires specific measurements from the standard. This information could be translated into requirements as follows. First, the architecture shall be designed following PLr d (e.g., designated architecture category 3). In addition, the architecture shall also be evaluated under PLr d. Second, the sensors shall provide the required properties corresponding to PLr d. Third, similarly, the processor shall not fail in the safety control system and shall correspond to PLr d. And finally, the actuators (i.e., the brakes) used to stop autonomous machines shall also provide the properties corresponding to PLr d. Fulfilling those requirements can be used as evidence to provide sufficient confidence in the hardware implementation.

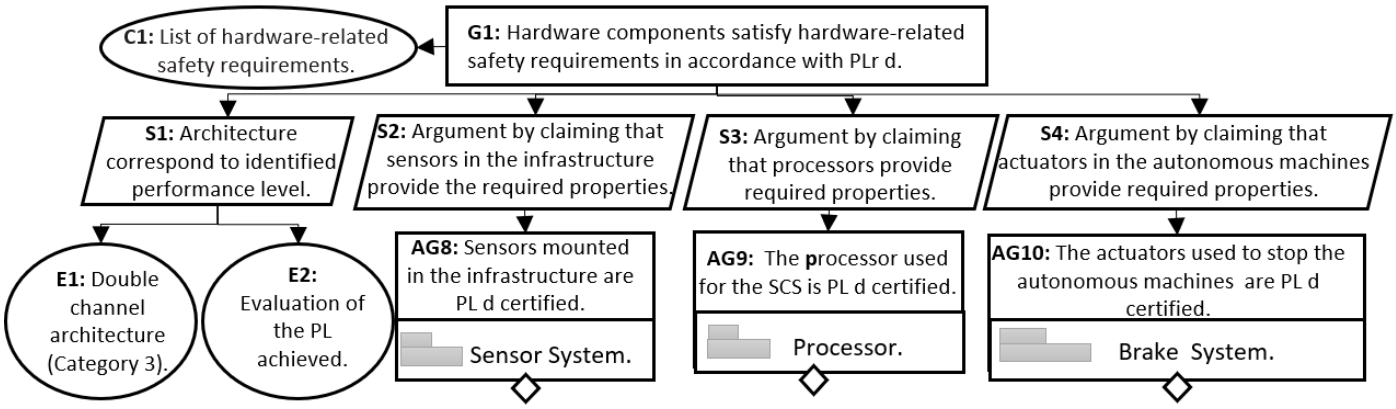

Fig. 7: Argument over Away Goal AG5.

V. Discussion

There are some aspects related to our argumentation strategy presented and illustrated in this paper that we consider worth highlighting and discussing. First, designing a safety case and collecting the evidence to populate it during project execution can be a complex task, especially when there are only a few examples in the domain. In this sense, our argumentation strategy (see Section III) could be of value for practitioners since it proposes a step-by-step reasoning strategy grounded on state-of-the-art methods and techniques (i.e., SoS concepts and STPA) as well as standards harmonized with the machinery directive which guides the regulatory facets that are mandatory (at least in Europe) for commercializing and operating machinery. Such a strategy can also be seen as a planning methodology since it describes the minimal set of tasks that should be done to reach the evidence required to show the presumptions of conformance with the machinery directive.

As seen in Section IV, the argumentation resulting from the case study is modular, allowing us to split the responsibilities regarding the safety case description into different packages that can be allocated to different stakeholders, i.e., the original equipment manufacturers (OEMs) and service providers. For example, in Fig. 4, we present four modules. One of such modules, e.g., AG1 can be defined as a contract argument for the machine's manufacturer, who shall develop and provide machines according to defined requirements, e.g., the collision avoidance system shall be able to brake automatically and independently at least when they detect a potential forward collision with a stationary or moving object. If done properly, the machine providers' safety case can be seamlessly attached to our general argumentation, strengthening it. Similarly, the modules AG8, AG9, and AG10, in Fig. 7 can also be allocated to hardware providers. A similar module type will be generated from the software and communications reasoning structure.

The mining company shall also provide evidence for other modules. In particular, AG2, AG3, and AG4 in Fig. 4 are the company's responsibility, but they can be distributed in different areas. For example, operators' training may be a process that the human resources department shall perform. In addition, if the operation grows, further mitigation strategies could be added to the basic GSN structure. Consider, for example, that the mining company needs to include operators on foot in the same areas where the two types of vehicles are already operating. Thus, a new analysis may comprise additional controls that must be assured. As controls are separated, their argumentation can be added separately to the original safety case, making it reusable and extendable.

In the current analysis, we assumed that the components of the control structure (see Fig. 5) communicate with each other through a separate protected network. With this assumption, the networks and components may not be the target of an attacker. However, security requirements are also essential to consider in a different configuration. In such a scenario, security arguments may also be relevant and should be analized.

Finally, we consider the generalization of our argumentation strategy. In particular, such a strategy considers SoS concepts as a starting point. On top of such concepts, we add safety analysis techniques (such as STPA) and regulatory frameworks (in this case, targeting the machinery sector) to demonstrate sufficient safety for mining operations. Such a strategy is developed systematically (see Section III). Thus, with some adjustments, especially related to regulations, which are usually context-specific, the strategy can be adapted to other domains and operations with similar characteristics, i.e., safety as emergent behavior and mandatory regulatory frameworks addressing risk management techniques and control systems.

VI. Related Work

Safety mechanisms to control autonomous operations have been proposed in [21], where the authors present a safety supervisor in charge of triggering a stop upon detecting malfunctions in a car. However, there is no argumentation strategy for the safety case. In [22], the authors proposed an approach for the safety analysis of an automatic emergency brake by considering the standards ISO 26262:2018 and ISO 21448:2022. They also mentioned that their method's possible outcomes could support the safety case argumentation proposed by ISO 21448. In [23], the authors present an approach for safety requirements elicitation of a pedestrian detection component system that also considers ISO 26262:2018 and ISO 21448:2022. Their main difference from the previous work is that they include STPA for supporting the hazard analysis and the derivation of the

top-level safety argument, as we also do. Similarly, the authors in [24] use STPA for the safety analysis during the design and runtime phases. However, they do not explicitly propose safety case argumentation.

We have provided an operational design domain in [25], which was used in [4] to define safety requirements for mixed traffic operations in underground mining. However, we did not present safety case arguments in those works. The work presented in [26] also offers a safety concept for mining operations, which can be used in safety argumentation. In [27] and [28], the importance of a safety case for the mining industry is outlined but not developed in detail. A more detailed description of the safety case argumentation is presented in [29]. However, as we are doing in the present paper, this paper does not present the level of detail required to show alignment with the standards and regulations addressing the machinery directive.

VII. Conclusions and Future Work

This paper proposes a strategy for populating a GSN structure to argue for the sufficient safety of mixed traffic operations. Such a strategy takes as inputs the SoS concepts and combines them with safety analysis methodologies (in our case, STPA) and regulatory frameworks targeting the machinery sector (mainly, EN ISO 12100:2010, EN ISO 13849-1:2015). The argumentation strategy described and illustrated in this paper shows a general operations argument for mixed traffic operations, which is then broken down into the levels of control systems. Such an argumentation strategy, which facilitates safety case argumentation for operations approval in the European mining context, is done systematically. Therefore, it can be considered for other domains and operations with similar characteristics, i.e., safety as emergent behavior and mandatory regulatory frameworks to comply with.

We are currently working on the algorithm included in the SCS, which is the core of the safety work in our project. In the future, we plan to add arguments contracts to replace the undeveloped away goals that have to be done by third parties. In addition, we plan to develop and collect the evidence suggested as solutions for the company-specific arguments. (Cyber) security arguments will be also considered after a proper analysis of threats. Finally, we plan to test the appropriateness of the available tools for supporting STPA analysis and GSN argumentation to investigate their potential for being part of a tool-chain supporting our argumentation strategy.

References

[1] Global Mining Guidelines Group, "Case studty: Rio tinto's experience with automation improving safety for employees and creating value," 2021. [Online]. Available: https://gmggroup.org/wp-content/uploads/2021/03/2021-01-11-Rio-Tintos-Experience-with-Automation-and-People.pdf

[2] Ferreexpo. (2020) Yeristovo Mining. [Online]. Available: https://www.ferrexpo.com/what-we-do/operations/yeristovo/

[3] Boliden. (2021) Autonomous Hauling System for increased productivity in Boliden Aitik. [Online]. Available: https://news.cision.com/boliden/r/autonomous-hauling-system-for-increased-productivity-in-boliden-aitik,c3437805

[4] J. P. Castellanos-Ardila, H. Hansson, and S. Punnekkat, "Safe integration of autonomous machines in underground mining environments," in *8th IEEE International Symposium on Systems Engineering*. IEEE, 2022, pp. 1–8.

[5] T. Heath, "Autonomous industrial machines and the effect of autonomy on machine safety," Master's thesis, Tampere University, 2018.

[6] T. Hamada and S. Saito, "Autonomous haulage system for mining rationalization," *Hitachi Rev*, vol. 67, no. 1, pp. 87–92, 2018.

[7] Department of Natural Resources, Mines and energy , "Collision Prevention. Mining and Quarrying Safety and Health. Act 1999," 2017.

[8] The Council of the European Parliament, *Machinery - Directive 2006/42/EC*, Std., 2006.

[9] The Assurance Case Working Group (ACWG), *GSN Community Standard. Version 3*, Std., 2021.

[10] ISO/IEC JTC 1/SC 7, *ISO/IEC/IEEE 21839:2019. Systems and software engineering — System of systems (SoS) considerations in life cycle stages of a system*, Std., 2019.

[11] N. G. Leveson and J. P. Thomas, *STPA Handbook*, 2018.

[12] N. G. Leveson, *Engineering a safer world: Systems thinking applied to safety*. The MIT Press, 2016.

[13] European Commision, *Summary of references of harmonized standards published in the Official Journal – Directive 2006/42/EC*, Std., 2022.

[14] ISO/TC 199, *ISO 12100:2010. Safety of machinery – General Principles for design – Risk Assessment and Risk Reduction*, Std., 2010.

[15] ——, *EN ISO 13849-1:2015. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*, Std., 2015.

[16] ISO/IEC JTC 1/SC 7, *ISO/IEC/IEEE 15026-1:2019. Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*, Std., 2019.

[17] M. W. Maier, "Architecting principles for systems-of-systems," *The Journal of the International Council on Systems Engineering*, vol. 1, no. 4, pp. 267–284, 1998.

[18] H. Van Dyke Parunak and R. S. VanderBok, "Managing emergent behavior in distributed control systems," Defense Technical Information Center, Tech. Rep., 1997.

[19] P. Redmond, "A system of systems interface hazard analysis technique," Naval Postgraduate School Monterrey CA, Tech. Rep., 2007.

[20] ISO/TC 199, *EN ISO 13850:2015. Safety of machinery — Emergency stop function — Principles for design*, Std., 2015.

[21] R. Adler, P. Feth, and D. Schneider, "Safety engineering for autonomous vehicles," in *International Conference on Dependable Systems and Networks Workshop*. IEEE, 2016, pp. 200–205.

[22] V. J. Expósito Jiménez, H. Martin, C. Schwarzl, G. Macher, and E. Brenner, "Triggering conditions analysis and use case for validation of ADAS/ADS functions," in *Computer Safety, Reliability, and Security*. Springer, 2022, pp. 11–22.

[23] E. Acar Celik, C. Cârlan, A. Abdulkhaleq, F. Bauer, M. Schels, and H. J. Putzer, "Application of stpa for the elicitation of safety requirements for a machine learning-based perception component in automotive," in *Computer Safety, Reliability, and Security: 41st International Conference, SAFECOMP 2022, Munich, Germany, September 6–9, 2022, Proceedings*. Springer, 2022, pp. 319–332.

[24] L. Buysse, D. Vanoost, J. Vankeirsbilck, J. Boydens, and D. Pissoort, "Case study analysis of STPA as basis for dynamic safety assurance of autonomous systems," in *Dependable Computing*, 2022, pp. 37–45.

[25] J. P. Castellanos-Ardila, S. Punnekkat, A. Fattouh, and H. Hansson, "A Context-Specific Operational Design Domain for Underground Mining (ODD-UM)," in *European Conference on Software Process Improvement*. Springer, 2022, pp. 161–176.

[26] H. Ishimoto and T. Hamada, "Safety concept and architecture for autonomous haulage system in mining," in *International Symposium on Automation and Robotics in Construction*, vol. 37, 2020, pp. 377–384.

[27] Global Mining Guidelines Group, "*Systems Safety for Autonomous Mining*," 2021. [Online]. Available: https://gmggroup.org/wp-content/uploads/2021/09/GMG_System-Safety-for-Autonomous-Mining-2021-09-29.pdf

[28] Volvo Technology AB. (2015) Automated Safe and Efficient Trasnport System. [Online]. Available: https://www.vinnova.se/en/p/automated-safe-and-efficient-transport-system2/

[29] M. A. Javed, F. U. Muram, H. Hansson, S. Punnekkat, and H. Thane, "Towards dynamic safety assurance for industry 4.0," *Journal of Systems Architecture*, vol. 114, p. 101914, 2021.