System of Systems Hazard Analysis Using HAZOP and FTA for Advanced Quarry Production

Faiz Ul Muram, Muhammad Atif Javed and Sasikumar Punnekkat
School of Innovation, Design and Engineering, Mälardalen University, Västerås, Sweden
Email: faiz.ul.muram|muhammad.atif.javed|sasikumar.punnekkat|@mdh.se

***Abstract*—The advanced production systems are composed of separate and distinct systems that operate in both isolation and conjunction, and therefore forms the System-of-Systems (SoS). However, a lot of production systems are classified as safety-critical, for example, due to the interactions between machines and involved materials. From the safety perspective, besides the behaviour of an individual system in SoS, the emergent behaviour of systems that comes from their individual actions and interactions must be considered. An unplanned event or sequence of events in safety-critical production systems may results in human injury or death, damage to machines or the environment. This paper focuses on the construction equipment domain, particularly the quarry site, which solely produce dimension stone and/or gravel products. The principal contribution of this paper is SoS hazard identification and mitigation/elimination for the electric quarry site for which the combination of guide words based collaborative method Hazard and Operability (HAZOP) and Fault Tree Analysis (FTA) are used. The published studies on HAZOP and FTA techniques have not considered the emergent behaviours of different machines. The applicability of particular techniques is demonstrated for individual and emergent behaviours of machines used in the quarry operations, such as autonomous hauler, wheel loader, excavator and crusher.**

***Index Terms*—hazard analysis and risk assessment, emergent behaviours, system-of-systems, safety and autonomous machines.**

I. Introduction

The production systems are typically composed of separate and distinct systems that may not be designed for integration. However, to support the smart production, the characteristics of System-of-Systems (SoS), in particular, operational and managerial independence, evolutionary development, emergent behaviour and geographic distribution are taken into consideration [1], [2]. Compared to an individual system, the system boundary is not clearly defined in SoS and a set of constituent systems might vary over time either as part of normal operation such as another automated vehicle enters in a traffic management system, or otherwise as part of evolutionary development such as traffic management system receives a new version of control system [3]. The SoS hazard identification and mitigation is therefore challenging for which besides the behaviour of an individual system, the emergent behaviour of systems that comes from their individual actions and interactions needs to be considered.

The safety assurance is a regulatory requirement for safety-critical production systems in which an unplanned event or sequence of events may results in human injury or death, damage to machines or the environment. The principal objective of system safety analysis and risks assessment is the identification, elimination or mitigation, and documentation of system hazards, in order to make the system acceptably safe. It has been recognized that the safety analysis is much more cost effective during system design and development than trying to inject safety after the occurrence of an accident or mishap [4]. The functional safety standards, such as ISO 26262 [5], ISO 25119 [6] and IEC 61508 [7] prescribe the adaptation of hazard analysis techniques.

The Hazard and Operability (HAZOP) [4], [8] analysis is widely used to identify possible deviations in systems and subsystems, their possible fault root causes and consequences. It is applicable to all types of systems and equipment [4]. Afterwards, for in-depth analysis, the Fault Tree Analysis (FTA) [9] would be used to develop the fault propagation pathways and to provide a probability for ranking of fault causes before the failures actually occur. The HAZOP and FTA techniques have been combined for risk analysis in fuel storage [10], oil refinery unit [11], and hydrogen refuelling station [12], [13]. Besides the chemical industry, the combination of HAZOP and FTA techniques is used for security vulnerability of web application and infrastructure [14], autonomous service robot [15] and flight conflict at airport [16]. To date, however, the published studies have not considered the HAZOP and FTA techniques for the emergent behaviours of different machines.

This paper focuses on the SoS hazard analysis for the electric quarry site [17], which solely produce dimension stone and/or gravel products. The heavy machines used in the quarry operations such as autonomous hauler, wheel loader, excavator and crusher represent the separate and distinct systems that have not been designed for integration. Due to the autonomous machines, heavy materials and human involvement, the quarry site is regarded as safety-critical. The SoS hazard analysis is performed for which the HAZOP and FTA techniques are used for the identification and elimination of potential hazards in the advanced quarry production. The results obtained from HAZOP and FTA techniques are utilized for elimination or control of identified hazards to demonstrate ultimate, acceptable safety of the quarry site.

The rest of this paper is organized as follows: Section II provides background information on electric quarry site and two hazard analysis techniques, in particular, HAZOP and

FTA. Section III describes the quarry production in a smart manner and also performs the SoS hazard analysis. Section IV presents the related work. Section V concludes the paper and discusses future research directions.

II. Baseline and Concepts

A. Electric Quarry Site

This subsection describes an operational quarry site [17]. It falls under the construction equipment domain. The quarry site solely produce dimension stone and/or gravel products of different granularity, which are used for the construction of buildings, roads and railway track beds. The quarry operation is carried out with different kind of machines such as autonomous hauler, wheel loader, excavator, primary/mobile crusher and secondary crusher. In particular, they collaborate together to realize the targeted production goals [18]. The quarry site is subdivided into different production zones.

- Feeding Primary Crusher: The primary crusher breaks the hard and bigger rocks into the smaller rocks. This is done to facilitate the transportation to the secondary crusher. The excavator feeds the raw material to primary crusher, i.e., the rocks that are broken out of the mountain with explosives. The ripper is attached to the excavator or otherwise the dozer to break down the rocks, which may create difficulties for the excavator and/or crusher.
- Direct Loading or Truck Loading: The conveyor belt is attached to the primary crusher. It is therefore possible to directly load the autonomous hauler from the primary crusher or otherwise the rock piles will be formed. The wheel loader is used for making changes in rock piles. The autonomous hauler might also be loaded with the wheel loader.
- Transporting and Dumping: The autonomous haulers travel in the defined path and dumps the loaded rocks in the feeding spot of the secondary crusher. The site management system is responsible for commanding the autonomous haulers. It is composed of three subsystems: (i) user interface visualizes the corresponding information; (ii) fleet management sets missions or tasks for individual autonomous haulers; and (iii) traffic control maintains sufficient distances to avoid collisions.
- Feeding Secondary Crusher: The secondary crusher is a fixed crusher and might be located bit far away. It further crushes the rocks into smaller granularity or fractions to meet the customer demands.
- Charging: The battery-powered autonomous haulers are used in the quarry site. After the completion of mission(s), there is a need to recharge the battery. To be able to recharge the battery, the charging spots have been defined.
- Parking: After the completion of assigned tasks, the machines can be moved to the parking station. If the parking station is not defined, the machines can be parked beside the transportation routes.

B. Hazard Analysis Techniques

The SoS hazard analysis performed in this paper is based on the HAZOP and FTA techniques. This subsection provides an overview of the particular techniques.

1) Hazard and Operability Analysis: The Hazard and Operability (HAZOP) analysis is an inductive technique for identifying and analysing the potential hazards and operational concerns of a system [4]. HAZOP was initially developed to analyse chemical process systems, but later extended for other types of complex systems, for instance, nuclear power plants, rail systems and air traffic management systems [8], [10]. HAZOP analysis is preferably carried out early in the design phase taking different parts into consideration such as software, hardware, procedures and human interactions. The HAZOP analysis sessions are reported in the HAZOP worksheets containing matrix or columns, in which the different items and proceedings are recorded.

The HAZOP analysis process starts with a full description of a system (or a process), which is broken down into system parameters (or steps). Afterwards, all possible deviations are systematically identified by comparing a set of guide words (e.g., more, less and part of etc.) against a list of system parameters or characteristics (e.g., flow of data, pressure and temperature etc.). It might be noted that not all combinations of guide words and parameters are expected to yield sensible or plausible deviations and these combinations can be omitted in the HAZOP worksheets. After the identification of deviations, an assessment is carried out to determine whether particular deviations and their consequences can have negative effects on the system's operation. Finally, the appropriate recommendations are identified that can help to prevent accidents or reduce the associated risk. These steps are repeated for each characteristic and then each node of the system until all hazards are identified.

2) Fault Tree Analysis: The Fault Tree Analysis (FTA) is one of most commonly used deductive analysis approach for modelling, analysing and evaluating failure paths in a large complex dynamic systems such as nuclear power stations, aircraft and chemical processes [9], [19]. Moreover, it can be conducted at different levels of abstraction, such as requirement phase to find out weaknesses in the specification and their impact on the system quality; and the detailed design phase to find weaknesses in design and to identify a direct effect on software safety [4]. The FTA process starts with a top undesired event or mishap and attempts to find out what nodes of a system, combination of events, or component behaviour lead to the occurrence of this top event. It uses a graphical model (i.e. fault tree), which is composed of a top undesired event (outcome), intermediate events, and bottom (basic) events; they are used to describe the internal functional logical (cause–effect) relationship between events. The cause–effect relationships between the components of a system and their events are achieved based on the operating principle and fault mechanisms of the system by using logic gates (e.g., AND-gate, OR-gate, etc.).

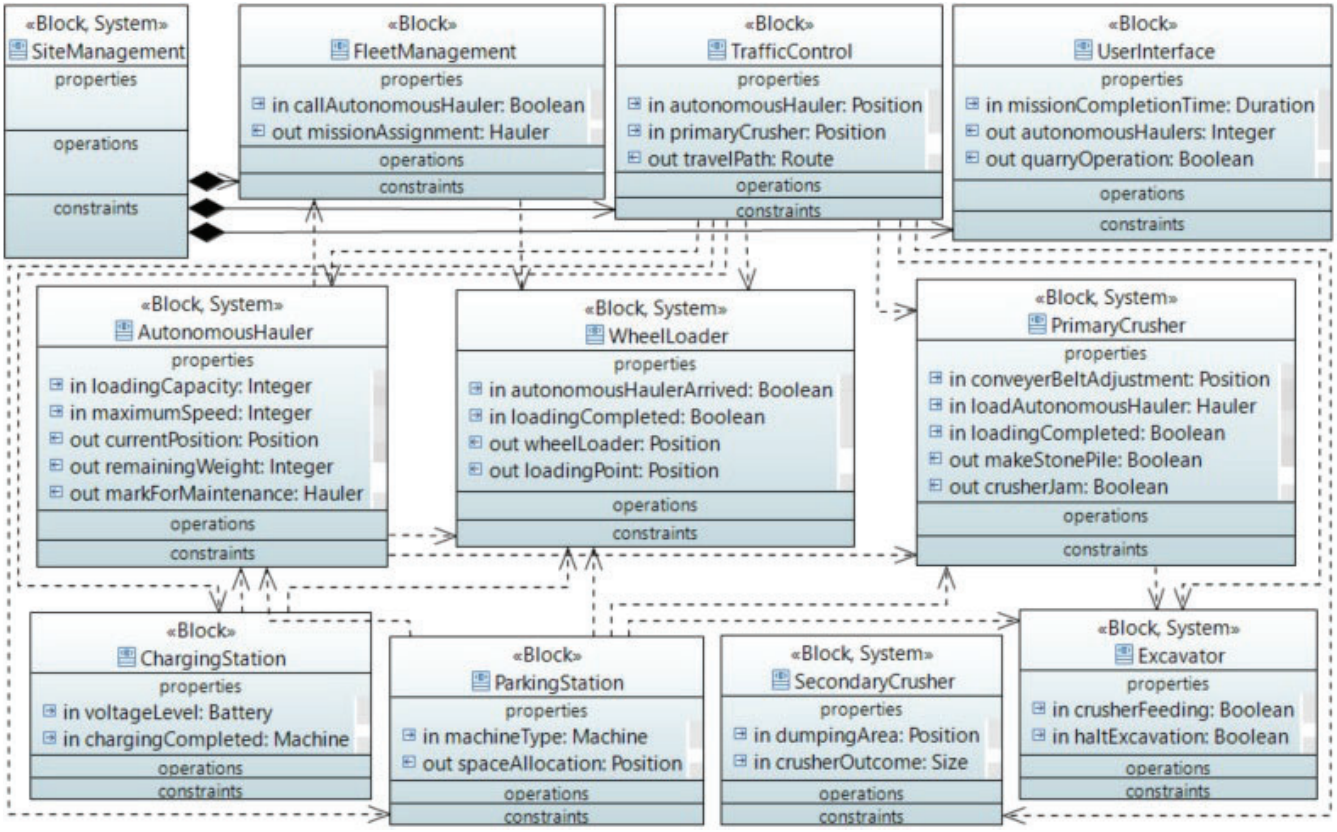

Fig. 1. System-of-Systems Architecture – Advanced Quarry Site

Fault tree development is an iterative analysis process, where the initial structure is continually updated to correspond with design development. During the analysis, those elements which are not contributing in the occurrence of a top undesired event can be eliminated. However, the elements not involved with the occurrence of one undesired event may be involved in the occurrence of another undesired event. A quantitative evaluation can be performed in addition to a qualitative evaluation to measure the probability of the occurrence of a top undesired event and the major faults contributing to this event.

III. Application of Hazard Analysis Techniques to the Advanced Quarry Production

The construction equipment manufacturers aims to provide innovative technological solutions. In the past year, the first emission free quarry site has been made operational [17]. The rocks transportation in quarry site is carried out with the autonomous haulers. The operation of autonomous haulers is similar to the Automated Guided Vehicles (AGVs). After the hauler, the automation of wheel loader could be considered [17], [20]. To support the smart or advanced quarry production, besides the behaviour of individual machines, the emergent behaviour of machines needs to be considered. For example, the automated loading requires emergent interactions of autonomous hauler with crusher or otherwise wheel loader. This section focuses on the SoS hazards analysis. At first, the SoS architecture for the advanced quarry production is described (Section III-A). The PolarSys CHESS[1] Toolset is utilized for the development of system models. After that, two hazard analysis techniques are applied: HAZOP (Section III-B) and FTA (Section III-C). The former establishes the worksheets, while the latter produces the fault trees.

A. System-of-Systems Architecture

The *site management* system serves as a primary controller. From the *traffic control* perspective, the positions of machines are tracked with the Global Positioning Systems (GPS), which are displayed on the site map. The travel paths need to be defined for moving towards the loading, dumping, charging and parking places. The *fleet management* subsystem commands the specific machines to perform their intended operations. For transportation, the missions are assigned to the autonomous haulers. To perform the mission efficiently, the required battery level needs to be determined. This is done before going to the loading place. To adapt the increased transportation demands, besides the direct loading from primary crusher, the parallel loading from wheel loader is considered. The *user interface* subsystem visualizes the status information. The autonomous haulers are moved to the *parking station* after the termination of transportation operation. If the *primary crusher* is building

[1]https://www.polarsys.org/chess/index.html

the rock piles, the direct loading is disabled. It is also possible to turn off the entire quarry operation, in particular, all the machines at the quarry site.

The autonomous vehicles contain the cameras, GPS and LIDAR (Light Detection and Ranging). These sensors are responsible for gathering surrounding information, such as positions, obstacles, and lane or boundaries. This information is processed for controlling the mechanical parts, for example, the drive unit for motion and operation, the steering system for manoeuvring, and the braking system for slowing down the vehicle to avoid collisions and accidents. The interaction platform and other attachments such as batteries for power supply are integrated in the *autonomous hauler*.

Together with the individual behaviour, the emergent behaviour of machines/systems is considered, as shown in Figure 1. The *wheel loader* is able to call the *autonomous hauler*, which informs back the *wheel loader* upon reaching the specified position. To be able to perform the direct loading, the adjustment of conveyor belt or otherwise *autonomous hauler* is desired. The remaining weight is conveyed to the *wheel loader* and *primary crusher*. There is also a need to pause the *primary crusher* for a while so that the next *autonomous hauler* is adjusted under the conveyor belt. If the crusher is jammed or the wait time for a next *autonomous hauler* is increased, the *excavator* is instructed to halt excavation. In the advanced *charging* and *parking* stations, for the assignment of specific places, the kind of machines needs to be determined. Besides that, the remaining battery and machine status might be conveyed.

B. Applying HAZOP Technique

In the context of SoS, a failure may not just lead to a hazard and accident of a system itself. But it can propagate to other systems, which lead to a mishap. This is because different systems have emergent interactions between them. In an SoS quarry production, the critical incidents can occur if correctly and timely communication is not established, for instance, a message is received too late, an incorrect message is transferred, or wrongly interpreted by the receiver. From the loading perspective, the delay of messages can result in severe damages to the machines. The collision of autonomous hauler is possible consequence, especially with the machines not equipped with obstacle detection and collision/avoidance mechanisms. Due to the incorrect mission or travel path assignment, the autonomous hauler may unintendedly enter into the restricted area in which humans are working or hazardous materials are stored. The failure of speed sensors may result in the wrong decisions which, in turn, may leads to the human injury or even life lose or damage to the environment.

We have performed a detailed HAZOP analysis for the advanced quarry production. For the hazard analysis, eight systems are taken into consideration; they are further divided into subsystems. The quarry production is carried out in different phases. In the context of an advanced quarry site, there is a need to address both individual and emergent behaviours of particular systems to realize the targeted production goals, as described in Sections II-A and III-A. To perform the HAZOP analysis, a set of guide words, parameters (e.g., speed, position, etc.), system inputs and outputs, a list of messages, and paths are identified. Table I shows a set of guide words and their interpretation. They are used for SoS hazard analysis. Each guide word is applied to all reasonable pairs of parameters, operations or components for determining the deviations. During the HAZOP analysis, the evaluation is carried out to determine whether the combinations makes

TABLE I
A SET OF GUIDE WORDS AND THEIR MEANINGS FOR SOS

Guide Word	Interpretation
Late	A message/data is transferred too late to be used.
Early	A message/data is transferred too early to be used.
No/Not/None /Omission	A message is not transferred. Interaction does not occur at all. None of the design intention is achieved.
More	The message is sent to more objects than intended. Too much or repeated information is transferred.
Less/Part Of	The message is sent to fewer objects (receivers) than intended. Too little information is transferred. Some of the design intention is achieved.
Incorrect/ Other Than	Incorrect message is transferred. Another activity takes place, opposite of what is intended.
Before/After	A message is transferred in a wrong sequence. Something happens before/after the intended order.
Slower/Faster	Activity is (not) done with the right timing.
Reverse	Source and destination objects are reversed.

TABLE II
CONSEQUENCES OF DEVIATIONS

ID	Consequences
C01	Human injuries or life lose
C02	Autonomous Hauler (AH) does not maintain a safe distance from other (autonomous or human operated) machines
C03	AH is unable to complete the mission
C04	AH enters in the restricted areas/region where human are working
C05	Major environmental damage
C06	Machine damage, loss of critical hardware
C07	AH rate of manoeuvre is insufficient to avoid the other obstacles
C08	AH fails to detect the obstacles at sufficient range
C09	AH unable to reduce/manage the speed or apply brake
C10	AH slips and falls during loading and unloading
C11	AH/other machines do not maintain a safe distance from human

TABLE III
EXTRACT OF RECOMMENDATIONS FOR HAZARDS

ID	HAZOP Recommendations
R01	Install roadside Dedicated Short Range Communications (DSRC) devices for better communication
R02	Introduce communication prioritization between machine to server communication, and machine-to-machine
R03	Use efficient networking protocol
R04	Increase number of wireless access point and retransmit the message
R05	Get the information from LIDAR as back up
R06	Take the values from camera
R07	Install additional sensors as back up
R08	Site manager takes the control
R09	Slow down speed motor
R10	Delete the connection with speed evaluator and switching to GPS
R11	Use dynamic filtering and inertial sensors

TABLE IV
EXTRACT OF THE HAZOP ANALYSIS REPORT FOR COMMUNICATION

Item	Guide Word	Parameter	Deviation	Cause	Consequence [Table II]	Recommendation [Table III]
H01	Late	Communication	Position of wheel loader or primary crusher is sent and/or received late than expected	Communication link between site server and wheel loader/primary crusher, or between site server and autonomous hauler is manipulated, downtime, loss of GPS signal	C02	R01
H02	No	Communication	Position of wheel loader or primary crusher is not transferred to autonomous hauler	Network unavailability, signal transmitter failure, reflection of signals, out of range	C01, C02, C03	R02
H03	More	Communication	Message received twice than expected to site management system	Autonomous hauler repeatedly sends the same message to site management over a determined amount of time	C02, C11	R02
H04	Other Than/ Incorrect	Communication	Incorrect mission or travel path is transferred to autonomous hauler	Wrong command is given by wheel loader and/or site server manager, site management system failed to detect human command	C01, C03, C04, C11	R03
H05	Less/Part of	Communication	Less information about mission is provided to autonomous hauler	Loose communication, intermittent communication	C03, C04	R04
H06	Other Than	Communication	Mission is transferred to the other autonomous hauler	Wrong command given by human, site management system failed to detect human command	C01, C04, C06, C11	R03

TABLE V
EXTRACT OF THE HAZOP ANALYSIS REPORT FOR SYSTEMS AND SUBSYSTEMS

Item	Guide Word	Parameter	Deviation	Cause	Consequence [Table II]	Recommendation [Table III]
H07a	Not	GPS system locate wheel loader position	GPS system fails to locate the wheel loader position, send and receive the location	GPS sensor fails, position estimator fails, communication failure	C02, C03	R05, R11
H07b	Less/Part of	GPS system locate wheel loader position	Send and receive less information of location. Route optimization failure	Wrong reading of GPS sensor, position estimator failure, biased position is calculated and forward	C03, C04	R06, R11
H08a	Not	GPS system locate Autonomous Hauler (AH) position	GPS system fails to locate the AH position, send and receive the location	GPS sensor fails, position estimator fails, GPS receiver fails, network unavailability	C02, C03, C07	R05, R11
H08b	Incorrect	GPS system locate AH position	GPS incorrectly estimates the location and direction. Send incorrect location	GPS sensor failure, wheel speed sensor failure, system controller failure, communication failure	C02, C07	R05, R11
H09a	Other Than/ Incorrect	LIDAR Position Encoder (AH)	Fails to detect obstacles and identify the location. Sends a wrong message	Mirror motor malfunction, position encoder failure, object to far to be detected, light emitter and receiver failure	C05, C06, C02, C08, C11	R07
H09b	More, Less, Other Than	LIDAR locate correct position	Misalignment. Data passed to the state estimator is either corrupted or less	Laser malfunction, light emitter and receiver failure	C01, C05, C06, C08	R07
H10a	No	Camera, Detect object (AH)	Could not detect the obstacles, difficult to localize	Improper lighting, blind spot, object is too far	C01, C02, C05	R07, R08
H10b	Other Than, Part of	Camera, Detect object	Detect object parts, cannot take the whole picture of object	Object is too close or too big. Improper lighting, misalignment, dirty or damaged lens	C05, C06, C01, C08, C11	R07
H10c	Late, Before After	Camera, Detect object	Detect the object late, difficult to localize	Object moves past, high speed, improper lighting, misalignment	C05, C06, C01, C11	R07, R09
H10d	No	Camera, Detect surface	Not able to detect unevenness of the surface	Adverse weather conditions, improper lighting, dirty lens	C10	R07, R08
H10e	No	Camera, Detect lane	Not able to detect lane	Improper lighting, blind spot	C04	R07, R08
H11a	Incorrect	Wheel speed sensor	Speed sensor emits wrong value, encoder feedback unable to be transferred	Speed sensor failure, wheel encoder failure	C09, C02, C01, C08, C11	R07, R10

sense. Afterwards, for the relevant hazards, all possible causes and potential consequences are identified. Table II shows the consequences of deviation. The proposed corrective measures to mitigate the hazards are shown in Table III. This process is repeated deviation by deviation and attribute by attribute until the analysis for SoS quarry production is completed.

The performed analysis not just focuses on the communication failures in SoS, but also external malfunctions and internal systems failures. Table IV shows the reduced hazard analysis results related to transmitting a message, in which the loading point, current position of machines and mission assignment are taken into consideration. Their listed failures concern the site management system, wheel loader/primary crusher, autonomous haulers and communication links. Note that the combinations without plausible deviations are omitted. It can be seen from the HAZOP results that the transformation of incorrect mission or travel path to autonomous hauler that can be caused by the command detection failure leads to the incomplete mission, machine damage or human injuries. This can be prevented by using efficient networking protocol. Table V summarizes the hazards caused because of the environmental influences and internal failures of autonomous hauler and wheel loader systems, or subsystems (e.g., LIDAR, GPS etc.) that are propagated to one or more systems, and in-turn lead to a mishap. The results from the HAZOP analysis have been used for prevention or mitigation of identified SoS hazards.

C. Applying FTA Technique

By focusing on a rigorous and structured methodology, FTA supports system analysts in modelling the unique combinations of fault events, which may cause an undesired event to occur. The comprehensive fault trees are developed based on the hazards and their potential effects understood from the HAZOP analysis, in which the identified hazards can serve as the top undesired events. To develop the fault trees, human injury, machine damage and mission failure are selected as the top undesired events or mishaps. After establishing a top event, sub-undesired events are identified and structured that is referred to the top fault tree layer. The logic between every event is investigated, in particular, the type of gates and their specific inputs are formulated. All possible reasons including human errors, and environmental influences are evaluated level-by-level until all relevant events are found.

Human injuries might occur at different phases of quarrying process, for example, upon the entry of machines or humans in the restricted areas. On the one hand, if an autonomous hauler enters in the restricted area, there is a possibility of collision with the working humans or explosive materials. On the other hand, if a human enters in the dangerous areas such as loading and dumping, there is a possibility of collision with an autonomous hauler or wheel loader. Figure 2 shows how the top mishap human injury is associated with the vulnerability of autonomous hauler at transporting phase. The autonomous hauler may unintendedly enter in the restricted areas due to the communication failures (i.e., emergent

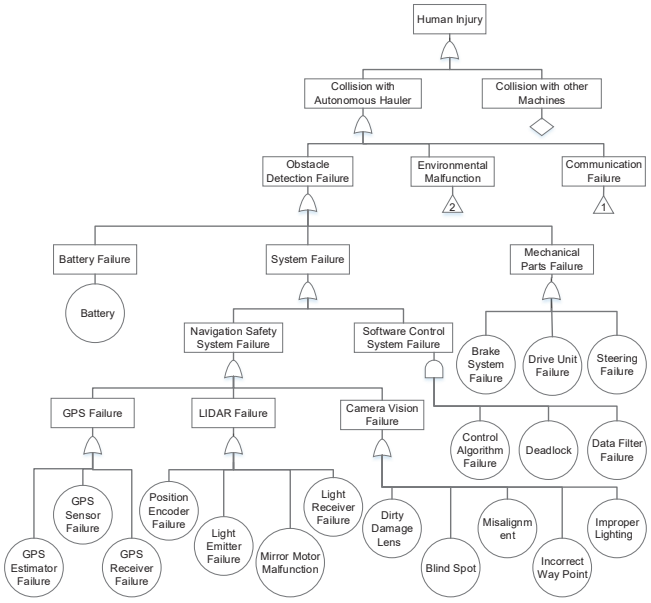

Fig. 2. Top level fault tree of human injury mishap

interactions), environment influences or obstacles detection failures. If an autonomous hauler or human is entered in the specific areas, besides the detection of obstacles, sufficient distance from human needs to be maintained. But, the failures caused by the battery power, system and mechanical parts may potentially lead to the collisions. The system failure is caused by two intermediate events: software control system failure and navigation safety system failure. In the context of mechanical parts failure, for example, drive unit, steering and brake systems, the autonomous hauler cannot be able to move, turn and apply brakes, respectively. The navigation safety system performance may also be affected for which the reasons include the degradation of GPS, LIDAR, or cameras. The fault tree shows that the resulting behaviour of particular failures will always reach a top mishap scenario.

As we see in Figure 3, the fault tree is further constructed with respect to the communication failure and environmental malfunction. The incorrect mission transfer to autonomous hauler and timing failures are related to the communication failures. If the site manager sent the wrong travel path, or mission and position, system fails to detect or autonomous hauler is out of range to receive commands. Besides the messages sent from site management system to autonomous hauler, the messages from wheel loader/primary crusher to site management system may cause the communication failures. Another reason of communication failure is the link failure (i.e. network unavailability). Therefore, these events are further developed into basic events. The environmental malfunction might be caused by the adverse weather conditions, drivable surface conditions and human behaviours.

In the fault trees, we have removed multiple occurring events and branches for the purpose of avoiding errors and obtaining accurate results. The presence of humans in the

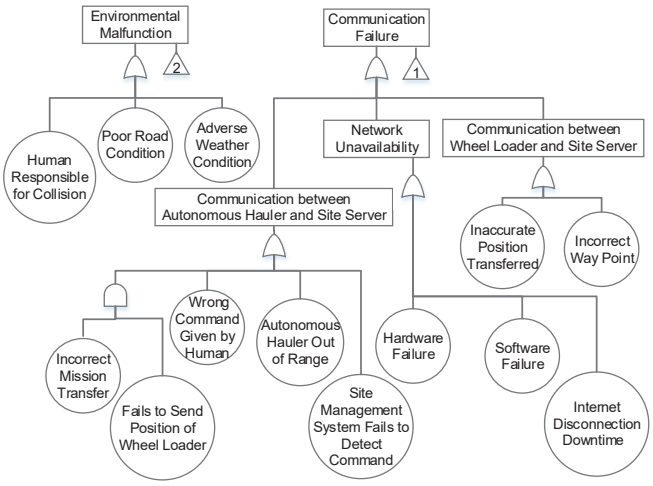

Fig. 3. Fault trees of communication failure and environmental malfunction

quarry site is one of the most crucial links. The communication failure is perceived as most vulnerable event among all events. The failure of sensors (e.g., camera, GPS and LIDAR) is the second most common problem for the failure of autonomous vehicles [21]. The results obtained from the FTA demonstrate that human injury, machine damage and mission failure are either caused by a communication failure, or otherwise one or more subsystem components.

IV. Related Work

Two of the studies consider the safety and reliability issues of the AGVs components and their probability of success in completing a prescribed mission. Yan et al. [22] merged Failure Modes and Effects Criticality Analysis (FMECA) and FTA to assess the safety of AGVs. Duran and Zalewski [23] applied the FTA on autonomous ground vehicles to identify hazards related to LIDAR and cameras.

Martin-Guillerez et al. [15] analysed risks for autonomous service robot. At first, the Preliminary Hazard Analysis (PHA) technique is used to identify hazards in the preliminary design. After that, the deviations in UML use cases and sequence diagrams are analysed by applying the HAZOP technique. However, the fault trees based on the PHA and HAZOP-UML hazards are not presented. Wu et al. [16] combined the HAZOP and FTA techniques for analysing the flight conflict at airport. The HAZOP technique is applied for acquiring the deviation and hazards list. For in-depth accident analysis, the fault trees are constructed based on the hazards list, in which the worst result is taken as the top event. Snamchaiskul and Phanrattanachai [14] used the HAZOP and FTA techniques to investigate the security vulnerability of web application and infrastructure. The guide words are proposed to cover the vulnerabilities, such as cross site scripting, SQL injection and script injection. The authors found that the fault tree of vulnerabilities in web applications did not yield much contribution than web infrastructure. Wu et al. [16] and Snamchaiskul and Phanrattanachai [14] have not considered the preventive measures. The aforementioned studies focus on the safety analysis of a single system.

There are few attempts to perform HAZOP analysis on an SoS. Redmond et al. [24] propose an SoS hazard analysis technique, which is a mixture of HAZOP and network analysis. The technique focuses on just one type of hazards, particularly interface hazards, in which one system causes a mishap in another system by transferring a failure over specified interface. Michael et al. [25] introduce a validation framework by combining Goal Question Metric (GQM), HAZOP and network analysis for measuring the sufficiency of software safety requirements with a set of metrics for an SoS missile defense. Stephenson et al. [26] present hazard assessment and safety-case production for Integrated Aircrew Training (IAT). To do that, they adapt product line techniques (feature model) to manage variation between staff training scenarios. The initial data for each system is derived from a differential analysis. The high-level hazard assessment is performed using HAZOP and HAZAN (Hazard Analysis) on training scenario. Then, a low-level exemplars assessment is performed.

Baumgart et al. [18] apply System-Theoretic Process Analysis (STPA) on the quarry site, in which just the control structure diagram is taken into consideration. In comparison to our work, the causes of communication failures, influences of environment and internal failure of the system, as well as the advancements in quarry site have not been investigated. For the SoS hazard and safety analysis, the simulation-based approaches are also proposed. In particular, they are designed to give quantitative assessments of the overall risk present in the system. For example, Blom et al. [27] in airspace system safety, and Mohaghegh et al. [28] in socio-technical systems use Monte Carlo techniques to acquire quantitative statistical measures of the overall safety of a system under specified conditions. Alexander and Kelly [29] present an analysis technique (SimHAZAN) that uses multi-agent modelling and simulation to explore the effects of deviant node behaviour within an SoS. However, the output results of simulation-based approaches contain thousands or millions of run logs, each containing tens of thousands of entries. It is very difficult for a human analyst to read such logs and understand them.

The principal contribution of this paper is SoS hazard analysis, which is performed as a first step towards advanced quarry production. For this reason we applied HAZOP and FTA techniques for the identification of hazards occurred due to the interactions between heavy machines/systems used in the quarry operations. Besides the identification of hazards, their prevention and mitigation had been considered.

V. Conclusion and Future Work

To be able to support the advanced quarry production, besides the individual behaviour of machines used in the quarry operations, such as autonomous hauler, wheel loader, excavator, primary crusher and secondary crusher, their emergent behaviour needs to be considered. Accordingly, this paper focuses on the SoS hazard identification and mitigation/elimination for the quarry production. Two hazard anal-

ysis techniques, particularly HAZOP and FTA are applied. The former is applied to identify possible deviations in SoS quarry production, their possible fault root causes and consequences. The latter supports in-depth analysis; the fault trees are constructed based on the hazards and their potential effects understood from the HAZOP analysis. The preventive measures drawn from the hazard analysis are used to eliminate or control the identified hazards for the demonstration of ultimate, acceptable safety of the quarry site.

The simulation environment of machines used in the quarry site is available in the university lab. A site sever is used for the specification of different machines in a site. As future work, we plan to support the dynamic safety assurance. The safety cases will be developed in the PolarSys OpenCert[2] platform. The safety contracts derived from the HAZOP and FTA techniques will be associated with the safety cases. The simulation data is used for the runtime monitoring of safety contracts. The results will be processed for updating the assurance (safety) cases and evidence models developed in the OpenCert platform.

ACKNOWLEDGMENT

This work is supported by SUCCESS (Safety assUrance of Cooperating Construction Equipment in Semi-automated Sites) project via the AAIP (Assuring Autonomy International Programme) and FiC (Future factories in the Cloud) project funded by SSF (Swedish Foundation for Strategic Research).

REFERENCES

[1] J. T. Boardman and B. J. Sauser, "System of systems - the meaning of of," in *1st IEEE/SMC International Conference on System of Systems Engineering (SoSE), Los Angeles, CA, USA, April 24-26*, 2006, pp. 1–6.

[2] C. B. Nielsen, P. G. Larsen, J. S. Fitzgerald, J. Woodcock, and J. Peleska, "Systems of systems engineering: Basic concepts, model-based techniques, and research directions," *ACM Comput. Surv.*, vol. 48, no. 2, pp. 18:1–18:41, 2015.

[3] R. Alexander, M. Hall-May, G. Despotou, and T. Kelly, "Towards using simulation to evaluate safety policy for systems of systems," in *Safety and Security in Multiagent Systems (SASEMAS) - Research Results from 2004-2006*, vol. 4324, 2009, pp. 49–66.

[4] C. A. Ericson, *Hazard Analysis Techniques for System Safety, 2 edition*. John Wiley & Sons, 2015.

[5] International Organization for Standardization (ISO), "ISO 26262–3:2011-Road vehicles-Functional safety. International Standard, November," 2011.

[6] ——, "ISO 25119–4:2018 tractors and machinery for agriculture and forestry – safety-related parts of control systems–part 4: Production, operation, modification and supporting processes," 2018.

[7] International Electrotechnical Commission (IEC), "IEC 61508-1:2010-Functional safety of electrical/electronic/programmable electronic safety-related systems," 2010.

[8] J. Dunjó, V. Fthenakis, J. A. Vílchez, and J. Arnaldos, "Hazard and operability (HAZOP) analysis. a literature review," *Journal of Hazardous Materials*, vol. 173, no. 1, pp. 19 – 32, 2010.

[9] L. Xing and S. V. Amari, "Fault tree analysis," in *Handbook of Performability Engineering*, K. B. Misra, Ed. London: Springer London, 2008, ch. 38, pp. 595–620.

[10] J. Fuentes-Bargues, M. González-Cruz, C. González-Gaya, and M. Piedad Baixauli-Pérez, "Risk analysis of a fuel storage terminal using HAZOP and FTA," *International Journal of Environmental Research and Public Health*, vol. 14, p. 705, 06 2017.

[2]See https://www.polarsys.org/proposals/opencert

[11] S. Dacosta, I. Al-Asýari, A. Musyafa, and A. Soeprijanto, "HAZOP study and fault tree analysis for calculation safety integrity level on reactor-c.5-01, oil refinery unit at balikpapan-indonesia," *Asian Journal of Applied Sciences*, vol. 5, 05 2017.

[12] M. Casamirra, F. Castiglia, M. Giardina, and C. Lombardo, "Safety studies of a hydrogen refuelling station: Determination of the occurrence frequency of the accidental scenarios," *International Journal of Hydrogen Energy*, vol. 34, no. 14, pp. 5846–5854, 2009.

[13] E. Kim, K. Lee, J. Kim, Y. Lee, J. Park, and I. Moon, "Development of korean hydrogen fueling station codes through risk analysis," *International Journal of Hydrogen Energy*, vol. 36, no. 20, pp. 13 122 – 13 131, 2011.

[14] S. Pumisake and P. Thitinan, "Using HAZOP and FTA to analyse security vulnerability of web application and infrastructure," in *3rd International Conference on Informatics, Environment, Energy and Applications (IEEA 2014), Shanghai, China*, 2014.

[15] D. Martin-Guillerez, J. Guiochet, and D. Powell, "Experience with a model-based safety analysis process for autonomous service robot," in *7th International Workshop on Technical Challenges for Dependable Robots in Human Environments (DRHE 2010), Toulouse, France*, 2010.

[16] Q. Wu, X. Gan, D. Yao, and Q. Sun, "Fault tree establishment of flight conflict based on the HAZOP method," in *4th International Conference on Machinery, Materials and Computing Technology, ICMMCT 2016, January 23-24, Hangzhou, China*, 01 2016.

[17] Volvo Construction Equipment, "Emission-free quarry," Available at https://www.volvoce.com/global/en/news-and-events/press-releases/2018/testing-begins-at-worlds-first-emission-free-quarry/.

[18] S. Baumgart, J. Fröberg, and S. Punnekkat, "Can STPA be used for a system-of-systems? experiences from an automated quarry site," in *2018 IEEE International Symposium on Systems Engineering (ISSE), Rome, Italy*, no. 4, October 2018, pp. 1–8.

[19] P. Liu, L. Yang, Z. Gao, S. Li, and Y. Gao, "Fault tree analysis combined with quantitative analysis for high-speed railway accidents," *Safety Science*, vol. 79, pp. 344–357, 2015.

[20] R. Lilja, "A localisation and navigation system for an autonomous wheel loader," Master's thesis, Mälardalen University, Västerås, Sweden, 2011.

[21] P. Bhavsar, P. Das, M. Paugh, K. Dey, and M. Chowdhury, "Risk analysis of autonomous vehicles in mixed traffic streams," *Transportation Research Record: Journal of the Transportation Research Board*, vol. 2625, pp. 51–61, 01 2017.

[22] R. Yan, S. J. Dunnett, and L. M. Jackson, "Reliability modelling of automated guided vehicles by the use of failure modes effects and criticality analysis, and fault tree analysis," in *5th Student Conference on Operational Research (SCOR), Nottingham, UK, April 8-10*, 2016, pp. 2:1–2:11.

[23] D. Reyes-Duran, E. Robinson, A. J. Kornecki, and J. Zalewski, "Safety analysis of autonomous ground vehicle optical systems: Bayesian belief networks approach," in *Proceedings of the 2013 Federated Conference on Computer Science and Information Systems (FedCSIS), Kraków, Poland, September 8-11*, 2013, pp. 1407–1413.

[24] P. J. Redmond, J. B. Michael, and P. V. Shebalin, "Interface hazard analysis for system of systems," in *3rd IEEE International Conference on System of Systems Engineering (SoSE), Singapore, June 2-4*, 2008, pp. 1–8.

[25] J. B. Michael, M. Shing, K. J. Cruickshank, and P. J. Redmond, "Hazard analysis and validation metrics framework for system of systems software safety," *IEEE Systems Journal*, vol. 4, no. 2, pp. 186–197, 2010.

[26] Z. Stephenson, C. Fairburn, G. Despotou, T. P. Kelly, N. Herbert, and B. Daughtrey, "Distinguishing fact from fiction in a system of systems safety case," in *Advances in Systems Safety–Proceedings of the Nineteenth Safety-Critical Systems Symposium, Southampton, UK, February 8-10*, 2011, pp. 55–72.

[27] H. A. P. Blom, S. H. Stroeve, and H. H. de Jong, "Safety risk assessment by monte carlo simulation of complex safety critical operations," in *Developments in Risk-based Approaches to Safety–Proceedings of the Fourteenth Safety-critical Systems Symposium (SCSC-6), Bristol, UK, February 7-9*, 2006, pp. 47–67.

[28] Z. Mohaghegh, R. Kazemi, and A. Mosleh, "Incorporating organizational factors into probabilistic risk assessment (PRA) of complex socio-technical systems: A hybrid technique formalization," *Rel. Eng. & Sys. Safety*, vol. 94, no. 5, pp. 1000–1018, 2009.

[29] R. Alexander and T. Kelly, "Supporting systems of systems hazard analysis using multi-agent simulation," *Safety Science*, vol. 51, no. 1, pp. 302–318, 2013.