Safety Concept and Architecture for Autonomous Haulage System in Mining

H. Ishimoto and T. Hamada

Mining Solutions Div., Client Solutions Group, Hitachi Construction Machinery Co. Ltd, Japan
E-mail: h.ishimoto.gl@hitachi-kenki.com, t.hamada.at@hitachi-kenki.com

Abstract –

In recent years, automation of mining equipment has been required to improve productivity, predictability, and safety of mining operations. Some major mining companies have begun efforts to automate dump trucks that transport overburden and minerals, eliminating the need for human operators, aiming for reducing labor costs, increasing operating hours, and improving efficiency of vehicle assignment. It is called an autonomous haulage system.

The introduction of an autonomous haulage system requires significant changes in operations management. Particularly, safety needs to be carefully considered.

Conventionally, in manned mining operations, ensuring the safety while at work has largely been the responsibility of site managers, fleet controllers, machine operators, and field workers.

However, when making the machine unmanned, it is necessary that the system bears a part of the function for ensuring safety, which has been conventionally carried out by humans, and that the user appropriately understand and operates the system.

This paper describes the concept of ensuring safety when applying an autonomous haulage system using unmanned dump trucks to mining operations, and a system architecture based on it.

First, we proposed the basic structure of the autonomous haulage system, conducted a risk assessment assuming mine operation using the system, and identified possible protection measures.

Next, we examined the architecture of an autonomous haulage system with a safety function that enables more deterministic performance evaluation while considering the complexity of the system.

This system was installed in an actual mine site, tested and operated, and it was confirmed that the safety functions worked properly. When introducing the system, the safety concept and architecture of the system have been explained to the site safety manager and governmental regulators and have been validated.

Keywords –

Autonomous haulage; Dump truck; Unmanned Control; Safety; Mining

1 Introduction

1.1 Background

1.1.1 Industry Trends

Prices of resources such as coal, iron ore and copper have risen sharply since around 2005 due to economic growth in China and emerging countries. During this period, there was a shortage of workers due to the booming mining industry, and so the rise in personnel costs was a problem. In response, major Australian resource development companies have expanded their investment, especially for machine automation, with the aim of unmanned mining in the future.

Due to the subsequent slowdown of the Chinese economy, which caused the global economic downturn, resource prices peaked, and mining companies were required to improve the efficiency of mine operations and reduce operating costs. This change in circumstances, together with the recent development of IoT and AI technology, has become the driving force for accelerating the shift to unmanned mining and machine automation, rather than stopping it.

1.1.2 Demand for Autonomy

In the mining industry, ensuring the safety of workers has been an issue for a long time. Particularly, there is a need to improve the safety and comfort of the operators of machinery operating on the site. In addition, the ESG concept has spread as a method of corporate evaluation in investment activities, and the mining industry is in a situation where improvement of environmental impact and working environment is required.

1.2 Autonomous Haulage System (AHS)

One of the efforts for unmanned or automated mining equipment is the autonomous driving system (AHS: Autonomous Haulage System) of dump trucks. AHS is a system that allows the dump truck to be unmanned and to be centrally managed from the control system in the office to carry out hauling and dumping products. Unmanned dump trucks not only reduce labour costs for operators, but also increase economic benefits, such as extended operating hours by eliminating breaks and shift changes, reduced fuel consumption by an efficient and appropriate driving by computer-controlled operations, and an extended machine life by driving control with less damage to the vehicle body. In addition, safety is expected to be improved by reducing human error during dump truck operation. Furthermore, it is expected that the mine operation itself can be made more efficient by linking the hauling process with the production management system.

The introduction of AHS to actual operation began around 2008, and in recent years the number of deployment cases has gradually increased, especially in iron ore mines in Western Australia. [1][2]

1.3 Safety of AHS

AHS will change dump trucks in a conventional mining haulage operation to unattended. Therefore, many of the roles played by the dump truck operator, including ensuring safety, are replaced by the functions of various systems that are components of AHS.

The operator is not present in the driver's cab of an autonomous haulage truck (AHT) during AHS operation, but a mixed situation of AHT and other manned vehicles in the AHS operation area can occur at any time. In addition, operations involving human intervention such as AHT start/end operations, maintenance/conditioning work, and manual operation for moving inside parking areas and workshops will continue to be performed. Thus, given the actual mining operation and site environment, it is difficult to take intrinsically safe measures such as physically isolating AHT, which is a major hazard source, from humans and manned vehicles. Therefore, it is essential that the system functions play a certain role to ensure safety.

Based on the above, this paper aims to show the AHS safety concept and architecture for safe operation of the mine.

2 AHS architecture

2.1 Overview

Various architectures can be applied to the system configuration that realizes AHS. It is possible to have a completely centralized implementation in which even the actuator control of the dump truck is performed on the cloud server side, and conversely, there may be an autonomous decentralized configuration in which each vehicle determines its own target position and route.

A centralized system has the advantage of reducing the number of in-vehicle devices for dump trucks and facilitating software updates. On the other hand, since the responsiveness of each vehicle control strongly depends on the communication performance with the central control system, there is a problem that the system scale and operation are limited when the wireless communication infrastructure is not sufficient.

The autonomous decentralized system can reduce the dependency on wireless communication, but the dispersion of autonomous operation of each vehicle becomes large. As a result, multiple vehicles may not be properly controlled, and efficient operation may not be realized as the entire system.

As an alternative to these, an intermediate approach is applied to the AHS we have developed (hereinafter simply referred to as AHS). In other words, this is an approach that achieves overall efficiency while suppressing the dependence on wireless communication by giving each vehicle a certain degree of autonomy.

Figure 1 shows the architecture of AHS.

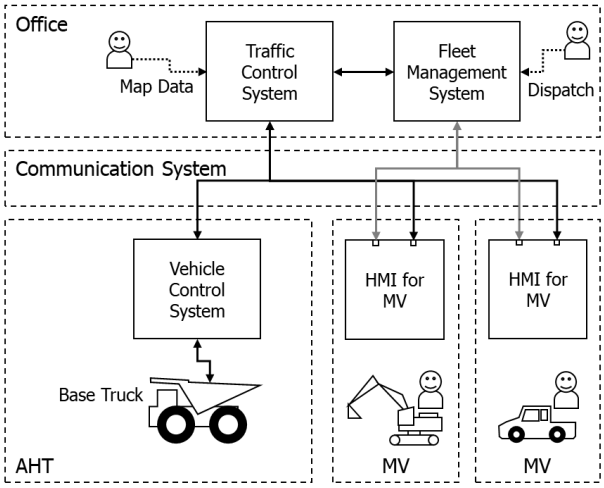


Figure 1. Architecture of AHS

The AHS consists of Fleet Management System and Traffic Control System located in Office, Vehicle Control System installed in AHT, and Communication

System that connects them. The manned vehicle (MV) used in the AHS operation site is equipped with a Human Machine Interface (HMI) that can monitor the operation status of the AHS and the status of AHTs.

The role of each subsystem that constitutes AHS is explained in the following sections.

2.2 Fleet Management System (FMS)

The role of the Fleet Management System (FMS) is to give a dispatch instruction to each AHT. That is, a destination such as a loading place or a dumping place to which the AHT should head is designated according to the current position of each AHT or the loading state. This dispatch instruction includes a method of directly setting a destination by an Office operator and a method of automatically issuing a repeat dispatch instruction based on a preset destination. The dispatch instruction is once passed to the Traffic Control System, converted into smaller driving instructions by the Traffic Control System, and sent to AHTs.

The FMS also displays the operating status of AHTs and the production volume estimated from them.

2.3 Traffic Control System (TCS)

In addition to multiple AHTs, MVs such as excavators, dozers, and light vehicles that are driven by humans also operate on the AHS operation site. The Traffic Control System (TCS) wirelessly communicates with AHTs and MVs, adjusts vehicle traffic throughout the site so that the interference between AHTs or between AHTs and MVs does not occur. The travel route of the AHT is divided into multiple sections, and by allowing the travel of each section exclusively to one AHT, interference between the AHTs is prevented. When the permitted section of AHT and the buffer area set in the traveling direction of MV overlap, the MV operator is guided by the HMI mounted on the MV so as not to enter the permitted section of AHT. At the same time, the TCS issues a deceleration/stop instruction to the AHT to avoid interference. [3]

2.4 Vehicle Control System (VCS)

The Vehicle Control System (VCS) controls the dump truck to move along the route to the destination specified by the FMS based on the TCS-controlled travel-permitted section. The AHT performs route-following traveling while comparing the route map information received from the TCS in advance with the self-position estimation results from the GNSS and IMU. In addition, the AHT detects obstacles with an environment recognition sensor and performs deceleration/stop behaviour as necessary.

2.5 Communication System (CMS)

Communication System (CMS) is responsible for information transmission between FMS, TCS, VCS, and HMI for MV. The CMS also has a function of monitoring the communication status including wireless communication.

3 Safety Concept

3.1 Principle

In the conventional hauling operation, the responsibility for ensuring safety during work has been delegated to appropriate actions and communication between people, such as operation managers, dispatchers, dump truck operators and other vehicle operators. On the other hand, in the AHS operation, it is necessary for the system to take over many of the roles for ensuring the safety, which was performed by the dump truck operator in the conventional operation.

However, it is hard to say that the concept of safety is established in the industry because AHS is still used only in some mines and is not widely used in many mines of the world. In addition, AHS is not a product with standardized structure and function like earthmoving machinery, and system configurations and functions are not common among manufacturers. Therefore, no common understanding has been established regarding the specific methodologies on which safety design is based or the performance target values for safety functions.

Therefore, we considered securing AHS safety based on the following basic policy:

- Compliance with safety requirements based on related international standards.
- Conduct risk assessments based on the operating environment and system architecture.
- Clarification of safety design requirements for protection measures derived from risk assessment.

3.2 International Standards

In 2017, ISO issued ISO 17757 “Earth-moving machinery and mining – Autonomous and semi-autonomous machine system safety”. The revised version was published in 2019. The standard covers systems in general that provide for autonomy in earth-moving machinery, primarily mining equipment and dump trucks in particular, and specifies the requirements that the system must have in its design, the information that the system integrator (which may be the same as the machine manufacturer) must disclose to the user, and the operating conditions that the user must control.

Regarding the safety of the system, it is required to carry out risk assessment according to the principles shown in ISO 12100. What constitutes a safety function in a specific system, and the required safety performance level thereof, cannot be uniformly determined because they largely depend on the operating conditions of the mine. Therefore, ISO 17757 does not provide a common target specification, and system integrators should make decisions based on the results of risk assessment. It is suggested to refer to ISO 13849, IEC 62061 or IEC 61508 for requirements in designing safety related control systems.

We have referred to this ISO 17757 as the basis for our AHS safety concept development and safety design.[4][5][6][7]

However, ISO 17757 does not mention specific procedures for risk analysis of autonomous systems and determination of required performance levels of safety functions. Therefore, we referred to the method proposed in the process industry that applies IEC 61508 or IEC 61511 to plant design.[8][9]

3.3 Layers of Protection

ISO 17757 describes risk management requirements for both AHS system integrators and users. Based on this, it was decided to secure safety based on the concept of hierarchical protection layers which combines system functions and operation management. The concept is shown in Table 1.

Table 1. Protection Layers of AHS

PL#	Protection Layer Category	Provided by
PL4	AHS Safety Functions	System Integrator (OEM)
PL3	AHS Control Functions	
PL2	Physical Barricades / Signage	User
PL1	Site Rules / Education	

At the first layer, user protection measures require AHS operation rules, provision of appropriate procedures, and education/training for workers involved in AHS operation [PL1 Rules/Education]. In the next layer, facilities to prevent human-AHT interference, such as signage and physical barriers that indicate the boundary between the AHT operation area and the manned area (parking area, workshop, etc.), are required. [PL2 Barricades/Signage].

As a protection measure by the system integrator (manufacturer), two layers of AHS control function [PL3 Control Functions] and safety function [PL4 Safety Functions] are provided.

PL3 is a layer for measures devised based on the AHS use cases assumed at present and the system architecture (shown in previous chapter) and comprises a variety of functionalities for realizing the main operation of the system. Each subsystem that constitutes the AHS has functions such as map management, traffic control, route tracking, and environment recognition, and these have the effect as protective measures in addition to realizing efficient operation.

PL4 is a layer of functions intended exclusively to ensure safety regardless of the action of the various functions of PL3 or the occurrence of a failure of the PL3 layer functions. In other words, it is a more universal and primitive protection measure that is less dependent on the functional specification of the system.

In ISO 12100 and ISO 13849, “safety function” is defined as “function of a machine whose failure can result in an immediate increase of the risk(s)”. PL4 is based on this definition. On the other hand, PL3 is regarded as a control function rather than a safety function. This means that a single failure of the PL3 function does not immediately increase the risk. In other words, even if one function of PL3 fails, as long as the function classified in PL4 is effective, the risk is still reduced to an acceptable level and it does not result in an immediate increase in risk.

The protection measures for PL4 or PL3 provided as AHS are designed on the assumption that the protection measures for PL2 and PL1 by the user are functioning properly. Safety cannot be ensured only by the protection measures by the function of AHS.

3.4 Risk Assessment

To extract the requirements that the system and the user should support for ensuring AHS operation safety, a risk assessment has been conducted according to the following procedure based on ISO 12100.

1. Assumed hazardous events due to system malfunction or human error.
2. Devised protective measures that can reduce the probability of occurrence of harm or the severity of harm.
3. Categorized to which layer of the hierarchical protection layers the devised protective measures should be placed.

Table 2 shows examples of hazardous events extracted by the risk assessment. In the actual development process, the probability of occurrence of harm and the severity of harm are estimated for each dangerous event, but they are omitted here.

Table 2. Examples of hazardous events

Origin	Hazardous Scenario	Target of Harm
AHT fault	Unexpected movement of AHT causes a collision with personnel.	Bys
AHT/TCS /CMS fault	AHT deviates from its travel route due to any abnormality in VCS/TCS/CMS, which causes a collision with personnel/MV.	Bys /MV Op
MV Op human error	The MV operator inadvertently enters MV into the AHT travel route, which causes a collision with the AHT.	MV Op
Bys human error	Personnel accidentally approaches the AHT, which causes collides with the AHT.	Bys

MV Op: Manned Vehicle Operator
Bys: Bystander (Field Operator, Maintenance Personnel)

Table 3 shows examples of the major protective measures (PRM: Protective Measure) devised corresponding to hazardous events extracted in the risk assessment. Each PRM is classified into one of layers PL1 to PL4. By applying a combination of a plurality of these PRM to each of the previously assumed hazardous events, the probability of occurrence of harm or the severity of harm can be reduced. PL1 and PL2 are user-controlled measures, and PL3 and PL4 are measures provided by the system integrator.

Table 3. Examples of Protective Measures

PRM type	Description	PL#
Rules / Education	Restrict personnel and MVs from entering the AHS area and AHT traveling routes.	PL1
Rules / Education	AHT start/stop procedure.	PL1
Barricades	Install a protective barrier between the AHS area and the manned area.	PL2
Barricades / Signage	Install AHS area entrance/exit gates.	PL2
AHT mode switching device	Proper placement of AHT start and mode switching devices.	PL3
AHT anomaly detection	AHT stops when it detects a system malfunction.	PL3
AHT deviation detection	AHT stops when it detects a deviation from the given route.	PL3
AHT obstacle detection	AHT stops when it detects an obstacle with the onboard sensor.	PL3
AHT permission control	AHT will stop within the given permit section if the next permit is not obtained.	PL3
AHT indicator	Notify the surroundings of the operating status of the AHT using indicators etc.	PL3
AHT audible warning	External notification of AHT start/start via horn, etc.	PL3
Site info provision	Provision of AHS area map information to MV operator.	PL3
Approach notification	Notify MV operator when MV and AHT approach each other.	PL3
AHT status info provision	Notify MV operator of moving/stopping status of AHT.	PL3
AHT Remote Stop	MV operator or personnel on site remotely stops AHT.	PL4
AHT approach speed limit	Limit the speed of the AHT when the MV and the AHT are close to each other.	PL4
AHT control system shutdown	Shut off the AHT vehicle control system during non-AHS operation.	PL4

The procedure for selecting PL4 safety functions from PRMs provided by the system integrator is described in the next section.

3.5 Selection of Safety Functions and PLr Determination

Figure 2 shows the safety function selection procedure.

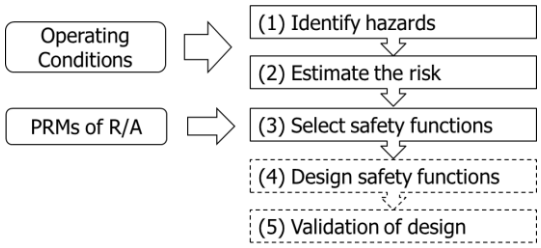


Figure 2. Safety functions selection process

3.5.1 Identify hazards

Accident scenarios due to AHT operation failure are identified as hazards. AHT operation failure means that the AHT does not operate as instructed, or that it operates unexpectedly. The cause of AHT operation failure is not necessarily limited to the failure of the hardware/software that controls the AHT base truck. AHS is a system that operates a dump truck by FMS, TCS, CMS and VCS triggered by human operation input. Therefore, the failure of any of the components that make up the AHS and the error of the person who operates the AHS can ultimately cause the operation

failure of the AHT. (For example, improper destination setting to FMS by a person, input error of map data, error of instruction to AHT due to TCS software bug, loss of operation instruction to AHT due to communication error, etc.)

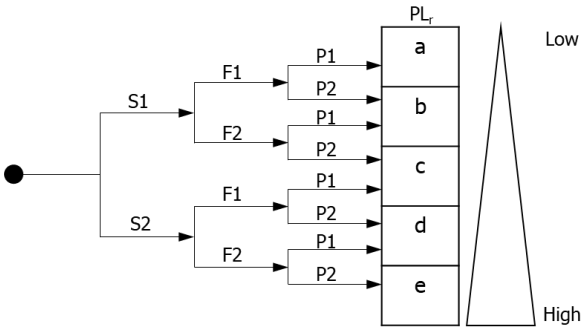
AHS has a large system scale, and the number of hardware and software that constitutes it is also large. There are also various combinations of operations between subsystems. Therefore, it is not practical to perform failure mode and effect analysis (FMEA) on all system components and consequently analyse all possible hazards in the entire system.

Therefore, we decided to conduct HAZOP for the behaviour of AHT, which finally becomes a hazard to humans, and identify the hazard. First, the movement of the dump truck was classified into acceleration, deceleration, steering, stop, and body lifting. Next, based on the HAZOP guide word for each movement, we assumed deviations such as "NO OR NOT", "MORE", "LESS", "REVERSE", and identified the resulting hazards.[8]

3.5.2 Estimate the risk

For all identified hazards, the risk estimation was performed and the required performance level (PLr) for the safety function to reduce the risk of hazard was determined.

For risk estimation, the analysis method using the risk graph (Figure 3) shown in ISO 13849-1, Annex A was applied.



S Severity of injury
S1 Slight
S2 Serious
F Frequency and/or exposure to hazard
F1 Seldom-to-less-often and/or exposure time is short
F2 Frequent-to-continuous and/or exposure time is long
P Possibility of avoiding hazard or limiting harm
P1 Possible under specific conditions
P2 Scarcely possible

Figure 3. Graph for determinating PLr for safety function

The procedure for determining the PLr based on the risk graph is described below.

1 Assume the situation before setting the intended safety function.
2 Estimate the risks caused by the failure of the safety function (in other words, the lack of the safety function). Consider the following parameters:
  2.1 Severity of injury
  2.2 Frequency and/or duration of exposure times to hazards
  2.3 Possibility of avoiding the hazard and probability of occurrence of a hazardous event
3 By selecting the above parameters, PLr to be assigned to the intended safety function is determined.

3.5.3 Select safety functions

Select a specific protective measure that can reduce the risk against the identified hazard from the results of the risk assessment. The selected protection measure is placed as the safety function of PL4, and PLr determined in the previous section is applied.

As a method of actual system design, safety functions are selected from the following viewpoints:

- To enable common risk reduction for more hazards with fewer safety functions.
- Safety functions can be placed independently of control functions.
- Safety-related part of the control system (SRP/CS) that performs the safety function can be downsized and the number of components can be reduced.

Table 4 shows examples of safety functions for each AHT operation scene selected in the above procedure.

Table 4 Examples of Safety Functions

AHT Operation Scene	Safety Function
Unmanned /Autonomous Mode	ASL: Approach Speed Limit
	R-Stop: Remote Stop
Manned /Manual Mode	AHT Control System Shutdown

During AHS operation is being conducted, AHT is in unmanned/autonomous mode. In this case, the situation where the AHT approaches a MV is a major hazard. As a protective measure, when the MV is close to the AHT within a certain range, the traveling speed of

the AHT is limited to reduce the kinetic energy of the AHT and lower the severity of harm. In addition, if the AHT is in low speed, the possibility that the MV operator can avoid the collision with the AHT increases, so that the risk can be reduced. Moreover, the possibility of avoiding a collision is further enhanced by equipping the MV with a device capable of remotely stopping the AHT.

During non-AHS operation, AHT may be used in manned/manual mode. In that case, there is a risk that the AHS function is activated unintentionally and obstruct human operations, resulting in a hazardous event. As a protection measure, the circuit is configured so that the AHT autonomous/manual mode switching device shuts off the power of the AHT control system during manual operation. This will prevent unexpected behaviour of the AHT in manual mode and reduce risk.

For each safety function, PLr based on the risk estimation under the assumption that the safety function is not provided is applied. This determines the target performance of the safety function and enables deterministic evaluation.

Note: The purpose of this chapter is to show the process of developing the AHS safety concept and determining the target performance of the safety function. It is out of scope to assert the need for a specific safety function and show a unified value of PLr for general automation systems for mining machinery. As described above, what kind of safety function is set and how the value of PLr should be are depending on the conditions under which the system is operated and the system architecture, and there is no general specification. Therefore, PLr value of each safety function is not described here.

3.6 AHS architecture with safety functions

Figure 4 shows the architecture in which the safety function components selected in the previous section are added to the AHS main function system shown in the previous chapter.

To provide the ASL function, the MV is equipped with means for measuring its own position and means for wirelessly transmitting the position. The AHT is equipped with means for measuring its own position and means for receiving position information from the MV. The received MV position and the AHT's own position are compared, and if it is determined that they are close to each other, the speed limit control of the base track is activated.

Similarly, to provide the R-Stop function, the MV comprises a wireless transmission means with a stop switch. When the AHT receives the stop signal from the MV, the control for activating the brake and stopping the base truck is activated. The MV transmitter and AHT receiver are shared by both ASL and R-Stop functions.

The communication system that transmits ASL/R-Stop signals is provided independently of the AHS main function communication system (CMS) and is used only for safety functions.

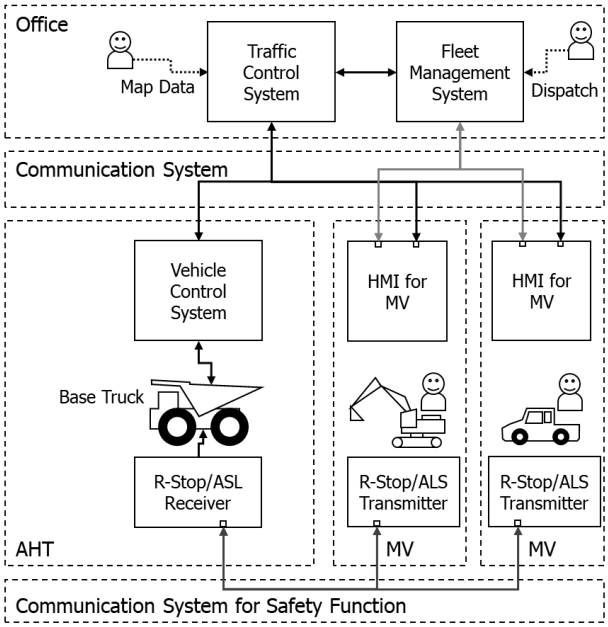


Figure 4. AHS architecture with safety functions

Implementing the system that provides the PL4 safety function independently of the system that provides the PL3 control function as described above has the following advantages:

- The safety function can always be activated as required without being affected by the operating status or malfunction of the main control function.
- The design of the separated SRP/CS becomes relatively easy and its performance can be evaluated deterministically.
- Since the safety function is not easily affected by the specification change of the main control function, it is possible to expand the functionality of the entire system without modifying the safety function.

4 Deployment and Evaluation

4.1 Deployment

With the cooperation of Stanwell Corp, an electric power company in Queensland, Australia, a trial of the AHS of the configuration introduced in this paper is being conducted within the Meandu coal mine owned by the company.[11]

As a result, commercial deployments of the AHS have commenced at the Maules Creek mine owned by Whitehaven Coal, a major coal producer in New South Wales, Australia. [12]

4.2 Evaluation

Mining companies that introduce and operate autonomous/unmanned systems are required to report their safety management plans and/or safety measures to the mining inspector in their state. In that case, the system integrator who provides AHS may also be required to submit the AHS system configuration, safety concept, and functional safety study report. If the information is insufficient, AHS operation in the mine may not be approved.

In preparation for the AHS operational test mentioned above, the safety of the AHS system and operation was reported based on the approach described in this paper and was validated by the mining companies' safety managers and state regulators.

5 Conclusions

We have developed a safety concept for introducing an autonomous haulage system (AHS) for dump trucks in mining operations. This concept is in line with the safety policy of earthmoving machinery and autonomous machine system, which is indicated by international standards.

Specifically, we conducted a risk assessment based on the AHS operating environment and system characteristics, and proposed protection measures for both the user side and the manufacturer side based on the concept of hierarchical protection layers. Hazard analysis was carried out to select the protection measures placed as safety functions, and the method to determine the required performance level of the safety function was established. An AHS architecture was formulated in which the selected safety function is provided independently of the main control function.

AHS based on this safety concept was introduced to an actual mining site. At that time, our approach to system safety was accepted by mining companies and officials, and the effectiveness of this approach was confirmed.

References

[1] Cecilia J. Rio Tinto autonomous trucks now hauling a quarter of Pilbara material. Online: https://www.mining.com/rio-tinto-autonomous-trucks-now-hauling-quarter-pilbara-material/, Accessed: 15/06/2020

[2] Daniel G. Why the Pilbara leads the way in haul truck automation. Online: https://im-mining.com/2019/08/06/pilbara-leads-way-haul-truck-automation/, Accessed: 15/06/2020

[3] Hamada T. and Saito S. "Autonomous Haulage System for Mining Rationalization". Hitachi Review, 67(1): 87-92, 2018.

[4] ISO 17757, "Earth-moving machinery and mining – Autonomous and semi-autonomous machine system safety". 2019.

[5] IEC 61508, "Functional safety of electric/electronic/programmable electronic safety related systems". 2010.

[6] IEC 62061, "Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems". 2005

[7] ISO 13849, "Safety of machinery – Safety-related parts of control systems"., 2015.

[8] IEC 61511, "Functional safety – safety instrumented systems for the process industry sector". 2003.

[9] Sakuma A. and Yoneki S. and Kushibiki T. "Risk Analysis and Safety Integrity Level Analysis Services for Plants, Machinery, and Equipment". Toshiba Review, 61(11):40-43, 2006.

[10] IEC 61882, "Hazard and operability studies (HAZOP studies) – Appication guide"., 2016

[11] PRESS RELEASE. Successful trial of Hitachi autonomous system. Online: https://www.miningmagazine.com/innovation/news/1331994/successful-trial-of-hitachi-autonomous-system, Accessed: 15/06/2020

[12] Daniel G, Whitehaven Coal hits automation milestone at Maules Creek mine. Online: https://im-mining.com/2020/04/16/whitehaven-coal-hits-automation-milestone-maules-creek-mine/, Accessed: 15/07/2020