Safety requirements for an automatic mining truck without onboard operator

Joseph-Jean Paques, Philippe Villeneuve de Janti, Réal Bourbonniere, Jean-Luc Durka

▶ **To cite this version:**

Joseph-Jean Paques, Philippe Villeneuve de Janti, Réal Bourbonniere, Jean-Luc Durka. Safety requirements for an automatic mining truck without onboard operator. International Conference and Advances in Vehicle Control and Safety, Jul 1998, Amiens, France. pp.195-200. ineris-00972134

HAL Id: ineris-00972134
https://ineris.hal.science/ineris-00972134

Submitted on 3 Apr 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Safety requirements for an automatic mining truck without onboard operator

Joseph-Jean Paques[1] & Philippe Villeneuve de Janti[2] - Authors

Réal Bourbonniere[1] & Jean-Luc Durka[2] - Coauthors

[1] Institut de Recherche en Santé et en Sécurité du Travail du Québec - 505, boulevard de Maisonneuve Ouest - Montréal H3A 3C2 - CANADA
[2] Institut National de l'Environnement Industriel et des Risques - B.P. n° 2 - 60550 Verneuil-en-Halatte - FRANCE

Abstract

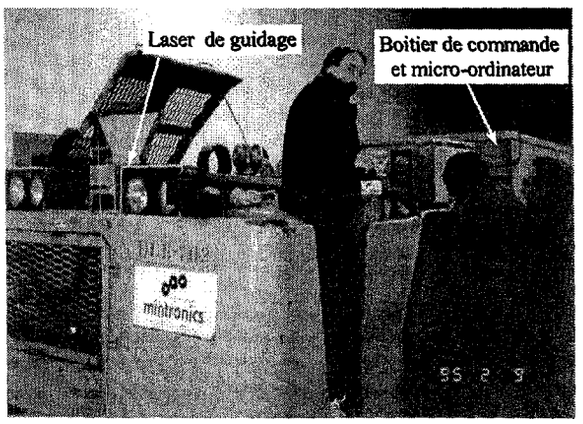
A prototype of an automatic truck has been developed for ore haulage in underground gold mines in Quebec (Canada). The control system is a computerized guidance system that is designed to give standard underground mining haulage vehicles the ability to operate fully automatically without an onboard operator. It combines scanning lasers with the most successful elements of radio remote controls on the leading edge of mine automation. It uses also a collision avoidance system to detect specific transponders equipping all people and vehicles in the mine by using microwave signals. The presentation will deal with the development of the safety program and with what has been done in the real life-cycle of the project.

1. INTRODUCTION

A mining company in Quebec is planning to install a system of automatic trucks in its mine at Abitibi. This will be the first time such a system has been used in Canada, and the trucks will transport ore between the cutting face and the treatment plant with no human intervention.

These automatic trucks are expected to operate in certain areas where there are also operator-driven vehicles and workers on foot.

As part of a safety assurance programme, the IRSST in co-operation with INERIS has been asked to develop and apply a safety programme to ensure that the automatically guided vehicle system is safe enough with respect to workers in the mine.



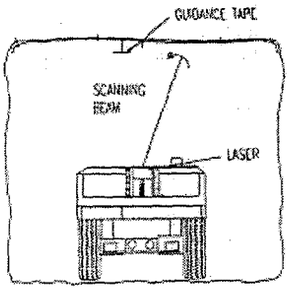
Locations of the guidance system and the onboard computer

System operation is based upon three major components:

- A system to guide and operate the automatic trucks employing fixed markers (overhead reflecting strips and bar codes of the same type).
- An onboard device to detect people carrying passive transducers.
- A traffic control system employing command and communication facilities operating throughout the site.

To ensure the safety of such a system, special efforts must be made in its design and operation.

A particularly serious problem in obtaining an adequate level of safety is that workers and automatic machines are present in the same areas.



Principle of the guidance system

2. PARTICULARS OF THE SYSTEM

The system is made up of four parts:

- Control of the automatic truck.
- Control of traffic.
- The truck protection systems (against fire, overspeed, and so on).
- The collision avoidance system consisting of a transceiver and passive transducers attached to the helmets of the personnel (3 transducers) and vehicles (6 transducers) which receive the signal from the truck and transmit a signal at twice the frequency.

When the collision avoidance system receives this double frequency, it issues the order to stop the truck.

At the unloading point at each cycle, the system carries out a self-test to verify the integrity of its safety function (checking the performance of the detection system at the front and rear of the truck).

3. SAFETY ASSURANCE PROGRAMME

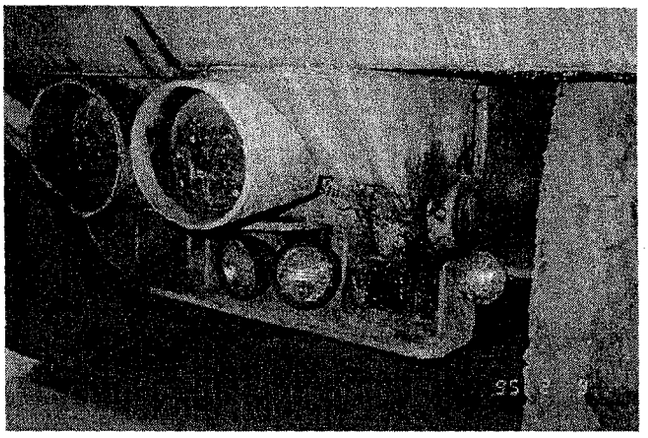
A programme of safety assurance was developed and applied in order to ensure that the self-guided vehicle system showed an adequate level of safety with regard to workers.

Evaluation of the system provided data about the level of safety resulting from the principles applied and, secondly, provided users with further information for optimising its use. It is based upon European standards, notably standard EN 954 "Safety of machinery and safety-related system components", and on the draft international standard IEC 61508 "Functional safety of electrical/electronic/programmable electronic systems relative to safety".

The safety file was prepared in four main phases:

1. Analysis of system risks.
2. Definition of objectives and technical safety requirements for the system.
3. Validation of the design and construction of the system.
4. Evaluation of the operating safety of the system.

The safety file sets out all the analysis done together with the tests carried out on an experimental site, together with a summary of the necessary improvements to meet the safety objectives. There are also certain recommendations concerning maintenance and the operating requirements for the machine: self-tests, periodic tests, and so on.



Rear view of a mining truck fitted with the receiving antenna of the collision avoidance system

4. SAFETY FILE

4.1 Analysis of system risks

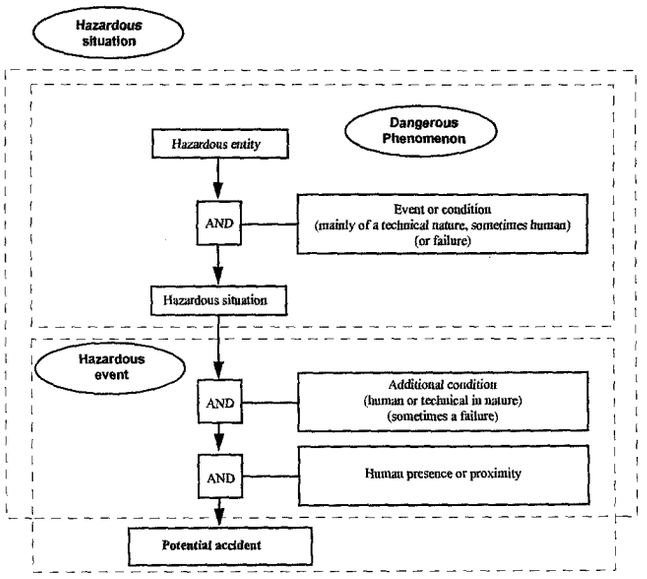
The aim of this phase is to identify any hazards of the system in each operating mode: loading the truck, transfer from the loading point to the unloading point, truck unloading and maintenance.
The analysis was in four phases:

- Identification of hazards.
- Preliminary analysis of hazards to determine safety-related events.
- Preliminary analysis of risks.
- Deductive analysis using causal trees.

The analysis was applied to the entire installation, i.e., the automatic truck in its mine environment and its control system (excluding the protective devices). The analysis leads either to certain functions of the control system being identified as requiring handling with a high level of safety (guidance, braking) or, usually, to a protection system (such as collision avoidance, overspeed) being introduced.

4.1.1 Identification of hazards

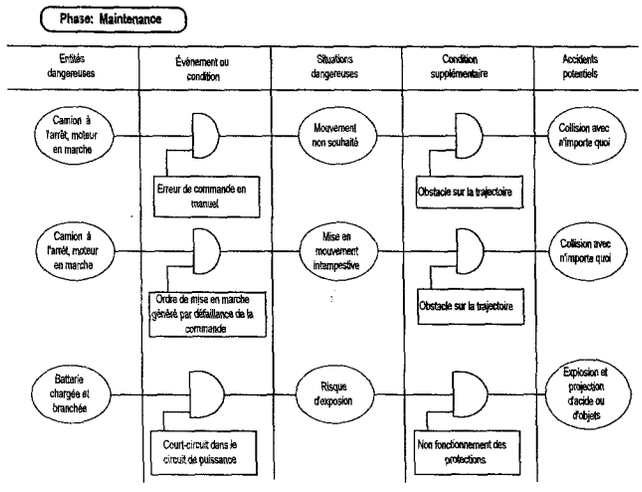
The following figure shows how hazardous situations leading to a potential accident can be broken down:



Breakdown of potential accidents

- *Dangerous entities*, i.e., the parts of the installation that can be associated with an intrinsic or potential hazard, or an external attack. The hazardous entity has to be exposed to an event or condition (failure of the command system) to lead to a hazardous situation.
- *Hazardous situations* that result from the interaction of a hazardous entity or an external attack with the context of or the entire installation. This hazardous situation has to be associated with an additional condition if it is to be converted into a potential accident.
- *Potential accidents* related to the interactions between the hazardous entities and the events causing a hazardous situation and their consequences.

The following table gives an example of an analysis using this model for three hazardous entities:



Analysis of hazardous entities

4.1.2 Preliminary analysis of hazards

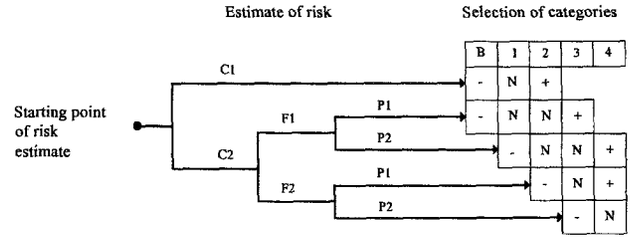
The hazards were identified and risks analysed for the five operating modes of the system. Three of these modes are related directly to production (loading – transit – unloading). One mode is associated with the maintenance of the vehicle and the last mode corresponds to a test run carried out at the beginning of each shift:

- Loading the truck – low speed (collision avoidance system not in service).
- Transit of truck from loading point to unloading point – high speed (collision avoidance system in service).
- Unloading truck – low speed (collision avoidance system not in service). This situation is similar to the loading station (layout of the unloading station to be taken into account).
- Maintenance (collision avoidance system not in service). This situation is regarded as similar to the loading station except as concerns the commands by guide rail and bar codes.
- First test circuit in automatic mode with driver on board (at the beginning of each shift).

4.1.3 Preliminary risk analysis according to EN 954

The risk analysis must also specify the level of safety with which the control and protection functions must be executed. According to a model proposed in standard EN 954-1, estimation of the risk takes into account the following three parameters:

- Seriousness of damage: **C**
- Time spent in the hazardous zone: **F**
- Possibility of containing the hazard: **P**



- N: Category having preference
- +: Measures excessive for the risk in question
- -: Possible category requiring additional measures

The synthesis of the risk analysis was presented in the following form:

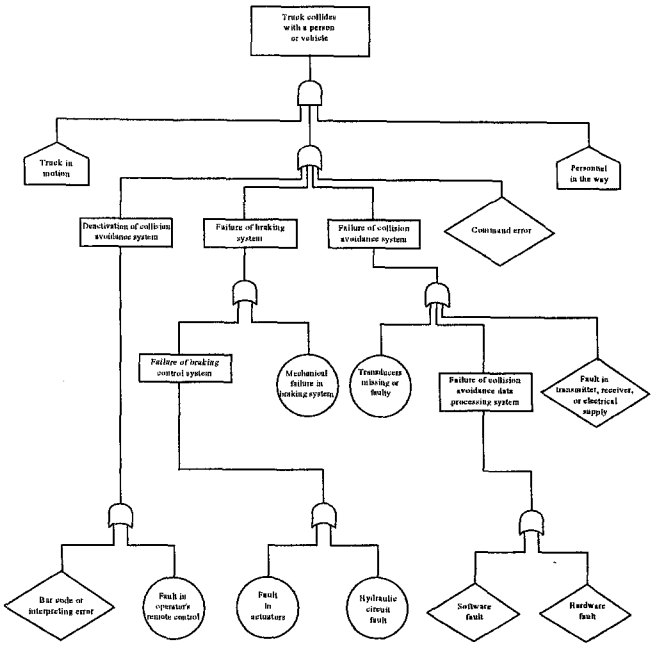
Function	Hazardous event	Existing preventive measures	Cat.
Test of the efficiency of the truck braking system.	Mechanical breakage or failure of the brake operating system ⇒ loss of control.	Braking test carried at the mine entrance on flat ground at each loading cycle. Shut down engine and apply brakes in the event of malfunction. Preventive maintenance procedure.	2
Collision avoidance.	System failure ⇒ Collision with another vehicle. ⇒ Collision with a person on foot.	Test of system integrity during each unloading cycle. Shut down engine and apply brakes in the event of malfunction. Several transducers per person or vehicle.	2

The risk analysis may be qualitative and/or quantitative. Each of these approaches has advantages and drawbacks; for this reason a combination of the two is recommended for critical installations.

4.1.4 Fault trees

General fault trees were plotted for the main undesirable events.

They determine the various possible combinations of events that result in an undesirable top event and allow any common causes to be determined.



Fault tree concerning collision with a person or a vehicle

4.2 Objective and technical safety requirements

This phase involves defining the safety objectives at system level based upon the analysis of hazards and risks. As an example, the technical requirements in category 2 applicable to the equipment are:

1. For the collision avoidance function:
    - The system should be designed in such a way that its functions self-test at appropriate intervals (at least every second during operation).
    - The system should be capable of stopping the truck (shutting down the engine and applying the brakes) if a fault occurs (weak on-line coverage of faults: 60%).
    - Malfunctions affecting safety (truck accidentally starting, bar codes wrongly read) and not tested on-line should be detected by off-line tests at appropriate intervals to maintain a level of safety better than 10^{-1}/year.
2. For the overspeed and braking functions:
    - Malfunctions affecting the safety (failure of the truck transmission system, failure of the braking system) should be detected by off-line tests at appropriate intervals to maintain a level of safety better than 10^{-1}/year.

4.3 Validation of the phases of design and construction

Based upon the technical specifications laid down, this phase covers:

- Validation of the system with regard to the environmental constraints it is likely to encounter.
- Validation of the methodology used for developing the software to highlight the methods and facilities employed to ensure safety.

4.3.1 Qualification tests

- Climatic testing: Ability to withstand cold, dry heat, and temperature changes.
- Mechanical tests: Vibration and impacts.

4.3.2 Electrical tests

- Electrostatic discharges.
- Radiated EM fields.
- Interruptions to power supplies.
- Fluctuation in supply voltage.

4.4 Analysis of the methodology used for developing software

As a rule, the process of software development is broken down into activities that constitute the life cycle of a program. This entire breakdown is translated into "quality requirements" and is used to define the basic way of looking at the tasks of developing, testing and evaluating the software. Thus the aim of this analysis is to provide a qualitative view of the functional safety level of the program by means of an evaluation questionnaire adapted to the application for the following phases:

- Specifications of the software.
- Preliminary design of the software.
- Detailed design.
- Writing code.
- Unit tests on the software.
- Integration tests on the software.
- Utilisation procedures.
- Development and modification of the software.

4.5 Evaluation of the functional safety of the system

Functional safety is evaluated in 3 stages:

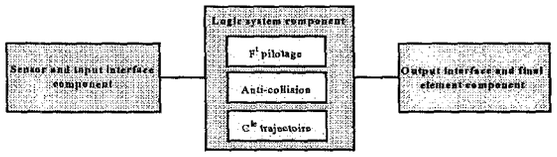
1. Structural analysis of the system as a whole (functional structure, common modes).

2. Evaluation of the hardware structure.

3. Evaluation of the integrity of the software.

4.5.1 Overall analysis of the system

The system must be capable of stopping the truck (shutting down the engine and applying the brakes) when a fault occurs. Moreover it must be designed in such a way that its functions are self-tested every second during operation. The safety architecture concept adopted by the manufacturer is of the 1oo1 type:



Architecture structure adopted

Overall analysis of the system shows that, in its present state, it does not present an adequate level of confidence for utilisation in a mine.

However, in view of the test procedures devised for detecting faults affecting:

- the collision avoidance system,
- the brakes,
- mistakes in reading or interpreting critical data from bar codes,

consideration may be given to its use on an experimental site on condition that appropriate safety instructions and training arrangements are drawn up. The experimental site investigated is located at the Val d'Or (Quebec) mining research centre.

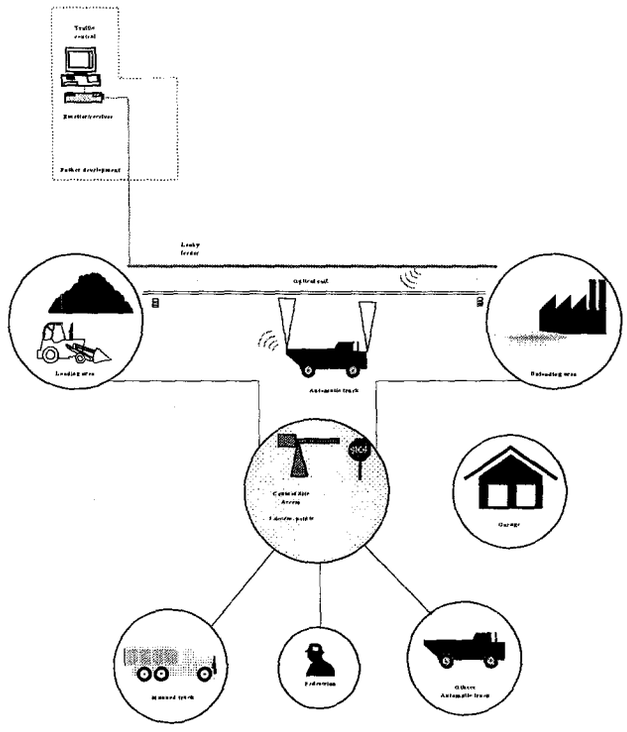


Diagram showing a mining vehicle integrated in the experimental environment investigated

4.5.2 Evaluation of the hardware structure

The hardware and its structure were evaluated on the basis of the data – occasionally preliminary – available.

4.5.3 Functional analysis

The functional analysis was done with the system broken down to level –4. It contains structural diagrams that explain the technical composition of systems providing the identified functions.

The following table gives an example of how the control-command function for the truck's path is broken down:

Level -1	Level -2	Level -3	Level –4
Control-command of the truck's path and of the driving functions.	Monitoring the truck's path.	Measuring the position of the truck centre line with respect to the guide rail.	• Guide rail • Laser 1 (front) • Laser 2 (rear) • Angular sensor.
		Calculate the deviation of the truck centre line from the guide rail.	• Computer.

The following structural diagram supplements the description of the path control-command function:

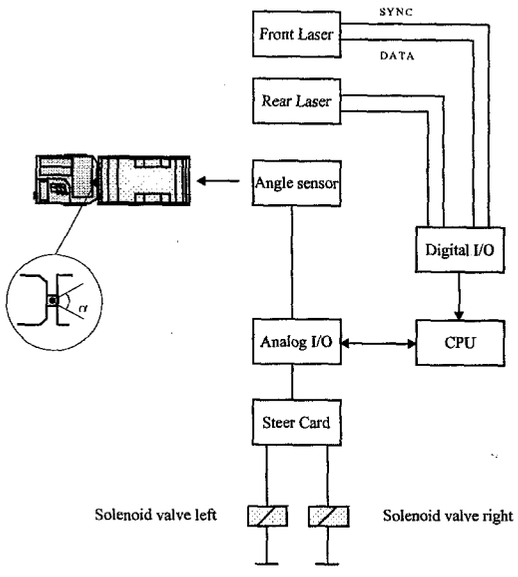


Diagram showing the principle of the path control system

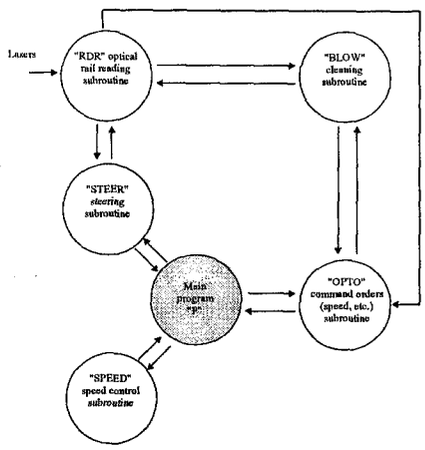
4.5.4 Analysis of failure modes and their effects

The main thread running through this analysis is the level of detail of the functional analysis, and links the disclosure of malfunctions to the safety objectives.

Function	Failure mode	Cause of failure	Effect on the function	Detection	Disposition
To detect the presence of a vehicle or of a person in the path of the truck.	Spurious detection.	Faulty transmissio n relay.	Truck stops even though no vehicle or person is present.	None.	Maintenance.

4.6 Evaluation of the software structure

The software structure was also analysed. The program operates in multi-task mode. It is loaded into the "RAM" memory. A CRC16 is performed only during loading. The system has no independent hardware watchdog.



5. CONCLUSION

The results of this study were used to prepare a safety file that will serve as a basis for the design and evaluation of these safety-related electronic systems.

The conclusions reached in the safety file resulted in recommendations being made to the designer and will serve as a basis for future experiments.

6. REFERENCES

[1] IEC project 61508 – parts 1 to 7: [Functional safety of safety-related E/E/PE systems].

[2] Standard EN 954-1 – safety of machinery – safety-related parts of control systems – general design principles.

[3] Méthodologie de développement du Logiciel [software development methodology] – technical document INERIS/LSSE/93.09.

[4] Evolution historique de la sécurité des machines – Revue générale de sécurité n° 86 [history of the development of the safety of machinery – general safety review n° 86] J. J. Paques.

[5] Health and safety guideline: Operator-less automated haulage – ministry of Labour of Ontario, June 1994.

[6] Etude des systèmes de détection d'humains et d'anticollision pour les véhicules opérant en milieu minier [investigation of human detection and collision avoidance systems for vehicles operating in mines] – Montreal Polytechnic, Hurteau, Côté, St. Armand.

[7] "The Opti-Track system, a system for automating today's LHDs and trucks", CIM Bulletin, Vol. 87, N° 984, October 1994, G. Brophey, D. W. Euler.

[8] Manual of operation of automated truck, Mintronics, 45 pages, 1997.