White Paper and Guiding Principles

Functional Safety for Earthmoving Machinery

REVISION HISTORY

Version	Date	Comments
0.0	12/12/2019	Initial release
0.1	13/12/2019	Minor editorial changes
0.2	07/01/2020	Revised ICMM perspective
0.3	12/02/2020	Draft for review. Revised following GMG comments
0.4	17/02/2020	Minor editorial changes
0.5	05/03/2020	Changes made to address stakeholder feedback

Executive Summary

The intention of this white paper is to guide the approach to functional safety for mobile earthmoving machinery. It also provides guidance for the interim approach to non-deterministic systems whilst standards for these are being developed.

- Functional safety is only one aspect of system safety and should be viewed in the broader context of a safety management system, in order to meet societal expectations of workplace safety.

- Higher performance/integrity level systems require commensurate increases in cost and complexity of maintenance and deployment practices. However, note that this may still be an appropriate approach for some systems.

- The ISO 19014 series, when published, will be the most applicable and appropriate standard for functional safety requirements for deterministic aspects of earthmoving machines and systems. However, note that there may be some retrospectivity considerations as OEMs transition from existing standards such as ISO 13849.

- The following is jointly recommended to address end user requests for functional safety assurance documentation, and is aligned with ISO/DIS 19014-2 which states:

  "…This information could be included in manuals or in other documentation given to the end user
  - *A listing of the safety functions on the machine*
  - *A listing of the safety-related parts of the control systems; particularly if changes to those parts could void the functional safety conformance of the machine*
  - *Any maintenance, tests or inspection tasks that are necessary to maintain the integrity of the SCS's over the lifecycle of the machine"*

  Further clarification is provided within the white paper.

- The increase in the level of automation of earthmoving machinery (e.g. autonomous haul trucks, collision avoidance systems) has led to the introduction of non-deterministic systems which cannot be analysed using traditional (or established) functional safety methodologies. There are standards under development to address this, however in the interim, a risk-based approach is recommended.

Introduction

This paper has been written as a result of recognition of need from earthmoving machinery end users, suppliers and manufacturers and represents the joint position of the Construction and Mining Equipment Industry Group (CMEIG), the Earthmoving Equipment Safety Round Table (EMESRT), and the International Council on Mining and Metals (ICMM).

The intention of this white paper is to guide the approach to functional safety for mobile earthmoving machinery. It also provides guidance for the interim approach to non-deterministic systems whilst standards for these are being developed.

CMEIG Perspective

CMEIG members have identified significant industry confusion in terms of understanding functional safety, as it applies it to earthmoving machinery and aspects of automation of earthmoving machinery. CMEIG member companies have been active in the development of related international standards such as ISO 13849 and ISO 19014 and consider this paper as an opportunity to educate and harmonise the industry on what is a very complex topic, for the net benefit of industry.

EMESRT Perspective

The Earth Moving Equipment Safety Round Table (EMESRT) is a global initiative involving major mining companies. EMESRT engages with key mining industry Original Equipment Manufacturers (OEM's) to advance the design of equipment to improve safe operability and maintainability beyond Standards. EMESRT recognises the need for clarity, and for a unified approach to functional safety.

EMESRT commenced working on vehicle interaction in 2013, with the first project being development of an interface protocol between Proximity Detection Systems and machines. The role of functional safety within the protocol and with vehicle interaction in general was raised as a concern to be dealt with.

ICMM Perspective

In 2018 the International Council on Mining & Minerals (ICMM) launched the Innovation for Cleaner Safer Vehicles (ICSV) initiative which includes a workstream on vehicle interaction. The requirements for these systems to comply with functional safety principles and comply with functional safety standards was identified as one of the roadblocks in continuing development of this technology. The number of standards, limited applicability to earthmoving machinery, and emphasis on different standards in different jurisdictions all work towards delaying introduction of new technology. The development of a common approach across both surface and underground mining will overcome these issues and allow more rapid development and uptake of new technology. ICMM intends the applicability of this white paper to extend beyond earthmoving machinery to include other mobile machines used on mine sites.

Explaining Functional Safety in the Earthmoving Machinery Context

Functional safety is defined as part of the overall safety relating to the equipment under control and its control system, that depends on the correct functioning of the safety control system and other risk reduction measures. It determines the level of risk posed by the failure of a control system and establishes what measures would be reasonably practicable to ensure that the probability of failure of the system is commensurate with the hazard posed by a failure.

Functional safety is a complex subject that requires deep expertise in system design, application and functional safety analysis, to apply appropriately. Incorrect application can lead to unnecessarily complex systems and machines that are not sufficiently reliable or safe, and too costly or difficult to maintain.

As explained in Figure 1, it is important to understand that functional safety is only one part of the earthmoving machinery risk management process.

In the earthmoving machinery context, a 'functionally safe' machine may only address a small proportion of the root causes of earthmoving machinery incidents. This highlights that a focus on 'SIL conformance' can detract from the potential for technology to significantly improve overall health and safety outcomes – this aspect is discussed in more detail later this document.

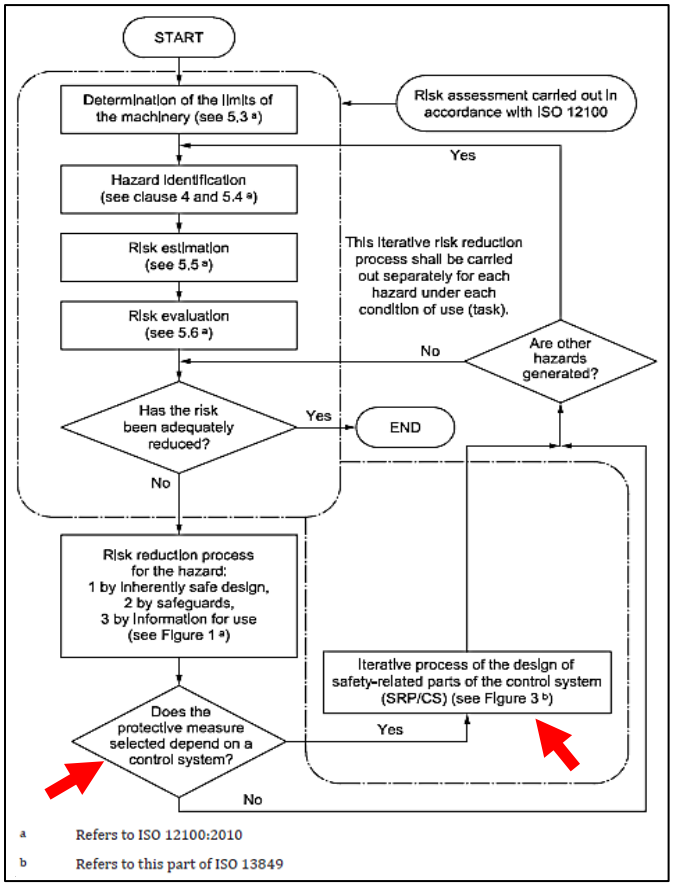


Figure 1 - Visual representation of where functional safety sits relative to a holistic risk assessment or risk reduction process (Source: ISO 13849 -1:2015)

The functional safety approach is to ensure that the integrity of a control system is commensurate with the level of risk posed should that control system fail. It deals with machine controls that work in conjunction with administrative controls to reduce the overall risk to a tolerable level.

Functional safety is only one aspect of system safety and should be viewed in the broader context of a safety management system, in order to meet societal expectations of workplace safety.

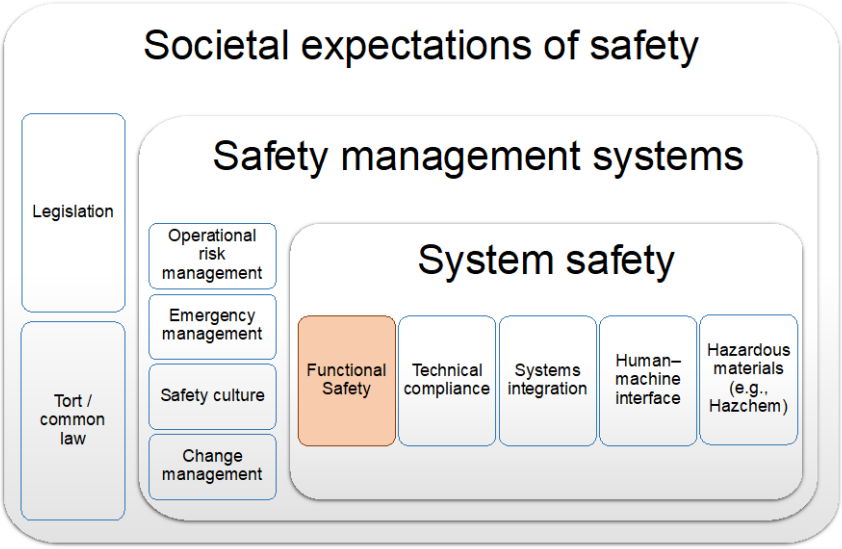


Figure 2 – Functional safety viewed from the broader context of workplace safety (source: Global Mining Guidelines Group)

Managing risk occurs over the entire product lifecycle. Irrespective of lifecycle management criteria in high-level functional safety standards, the earthmoving machinery industry successfully manages lifecycle safety considerations through processes such as new product introduction processes, information for use, service and warranty processes, and incident reporting and resolution.

Lifecycle Considerations and Functional Safety

Earthmoving machines are predominantly serially produced, which means that safety lifecycle activities are planned and carried out in a way that the product will be able to be used and maintained safely throughout the product's life-cycle phases across a series of product, rather than on a case by case basis. A suitable quality management system is typically implemented by the OEM to ensure that serially produced machines continue to meet specified criteria.

In assessing the integrity level of each safety function, the OEM will determine testing and maintenance requirements. These are then communicated through several means, including, but not limited to commissioning literature, operation and maintenance manuals, service literature, recalls etc. End user risk assessments may drive the need for additional testing and validation specific to that site.

The end user will also need to implement appropriate procedures to ensure that machines are operated and maintained in accordance with OEM specifications.

Application of Functional Safety to Earthmoving Machinery

In 1998 the International Electrotechnical Commission (IEC) published the IEC 61508 series, Functional safety of electrical/electronic/programmable electronic safety-related systems. This series of standards has been progressively making its way into the safety-critical and safety-related digital systems' mainstream. From IEC 61508, several industry specific standards were developed for different applications. Functional safety was first introduced to the earthmoving industry in the mid 2000's. The topic's introduction to earthmoving machines was not to address a specific problem, rather to support the increasing use of complex electronic, and programmable electronic systems.

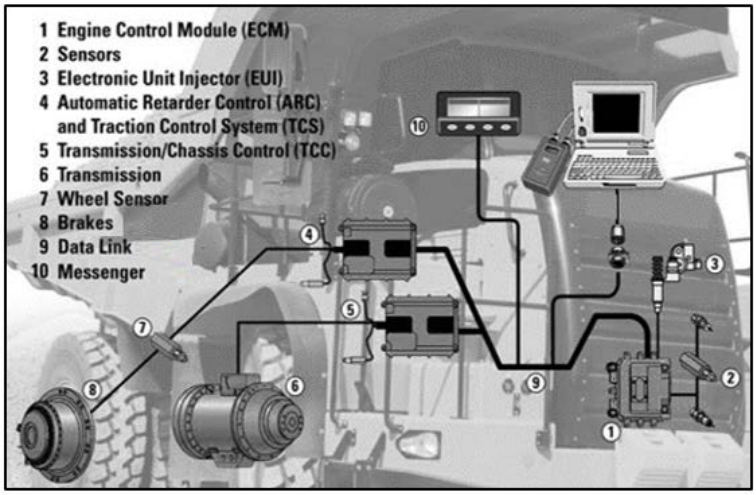


Figure 3 - A powertrain control system on a modern dump truck. A modern dump truck has a multitude of complex systems and software to manage its powertrain and vehicle dynamics. Likewise, there are complex systems for other functions such as hydraulics, engine and emission management etc.

Due to the lack of directly applicable standards, earthmoving machinery OEM's have faced many challenges since that time in applying functional safety. As a result, a new series of functional safety standards dealing specifically with earthmoving machinery (the ISO 19014 series), is progressively reaching publication stage and is expected to present a clear path forward for industry in applying functional safety to earthmoving machinery.

Detailed information about the different functional safety standards and their applicability is provided in Appendix A.

Application of Functional Safety to Automation of Earthmoving Machinery

The earthmoving machinery industry is moving from traditional manned machines, to machine level automation (e.g. automatic implement movement, adaptive cruise control, auto-dig etc.), system level automation (e.g. collision awareness and avoidance systems etc.) through to complex site automation systems (e.g. autonomous haul trucks).

Automation of earthmoving machinery creates opportunities to achieve significant health and safety benefits. However, the perception that automation solutions move risk mitigation measures up the hierarchy of controls is not completely accurate and can lead to a false sense of security. Due to the inherent complexity of these systems, it's important to note that the fundamental safety capability of the machine/system is based on the user having a thorough understanding of the system limits, and through adherence to prescribed administrative controls. For example, where autonomous operations are geofenced, this relies on accurate assignment and monitoring of those zones to prevent interactions between machines inside and outside the zone.

The conversation around functional safety also becomes more complex.

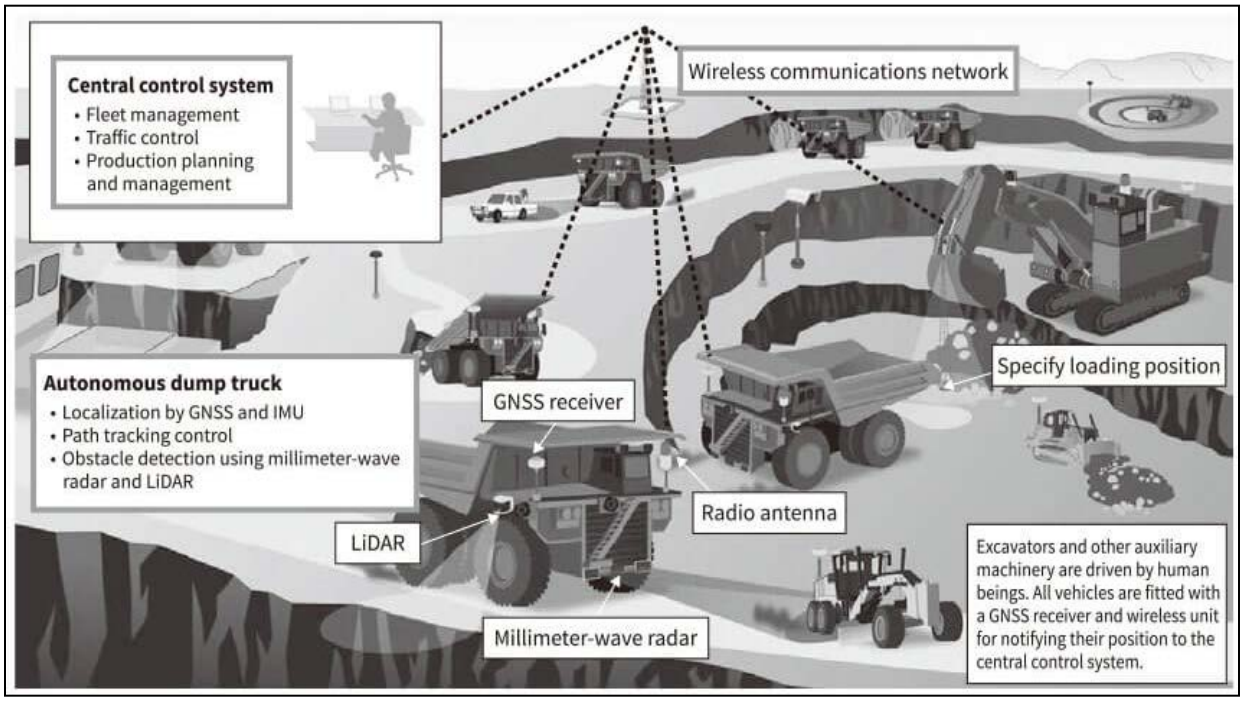
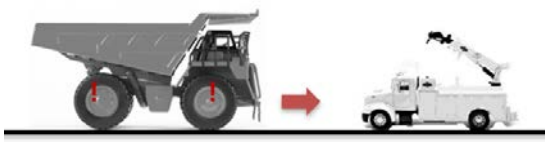


Figure 4 - An autonomous haulage solution (Source: https://www.hitachi.com/rev/archive/2018/r2018_01/10a07/index.html)

Limitations, Degradations and Failures

When applying functional safety principles to earthmoving machinery automation, it's important to understand the concepts of limitations, degradations and failures of systems.

A failure describes the scenario where a problem has occurred within the system that does not allow the system to perform as intended e.g. a system function such as brakes are actuated, but a hardware/software fault prevents brake application.



A limitation describes the scenario where the system is performing as intended, however the system is not capable of performing beyond certain parameters e.g. radar object detection sensors alone cannot detect a objects over the crest of a rise.

A degradation describes the scenario where the system performance is eroded e.g. reducing braking performance in low-traction conditions.

Deterministic and Non-deterministic Aspects of Systems

Deploying earthmoving machinery automation technologies requires a sound understanding of deterministic and non-deterministic systems, and of system limitations and degradations.

For deterministic systems, failure modes are known and understood. They are relatively easily detectable, and systems can therefore determine the presence of a fault and react to it. System software can be comprehensively validated. Current functional safety standards suit such systems well in that they enable accurate assigning of failure rates, diagnostic coverage, safe failure fraction and hardware fault tolerance.

However, automation systems will generally involve artificial intelligence and machine learning systems. They typically include algorithms that make complex judgments and predictions of the future (e.g. positioning estimation, trajectory prediction etc). They will likely also involve a myriad of limitations and degradations associated with their sensory inputs (e.g. GPS, Lidar, Vision, Infrared, Personal RFID tags etc.) or environmental conditions. The ability to differentiate between a failure, limitation and degradation, as well as determine the decision to be made is probabilistic, and thus, not all systems or aspects of systems can be analysed using existing functional safety standards . A functional safety performance level claim may not be possible for these aspects, or for the system as a whole which incorporates such aspects. A proposed approach for such scenarios is discussed later in this document.

Other Industries Approach

Other industries have also discovered the challenges of applying traditional functional safety analysis techniques to non-deterministic aspects of safety related control systems i.e. there are a multitude of safety hazards that may appear to be system failures, but are actually limitations and degradations of the system or environment. These safety hazards occur even though the system hasn't failed, in contrast to traditional functional safety which is concerned with mitigating risk due to system failures.

The automotive industry has invested significantly in this space. Much discussion has been had in industry forums and standards committees on how to handle this challenge. The automotive ISO functional safety committee[1] published ISO/PAS 21448 – *Safety of the Intended Function (SOTIF),* as a methodology for evaluating whether non-deterministic aspects of safety related control systems will function with an acceptable level of safety.

The intent of the SOTIF process is to demonstrate that system behaviour and performance is suitable and reliable for use, through extensive validation over a range of reasonably foreseeable use/misuse cases. The outcome is a better understanding of the system behaviours in known unsafe, known safe, unknown unsafe and unknown safe scenarios. This SOTIF process is intended to be used in parallel with established functional safety processes for the deterministic aspects of systems.

[1] ISO/TC 22/SC 32 Road Vehicles - *Electrical and electronic components and general system aspects*

Proposed Approach for the Evaluation of Systems with Non-Deterministic Aspects

The earthmoving machinery ISO committee[2] has recognised this issue and initiated the following work-items:

- A method to evaluate the net benefit of implementing collision avoidance systems in the absence of an applicable functional safety approach[3]
- An earthmoving machinery adaptation of the automotive SOTIF approach[4]

In the interim, CMEIG, EMESRT and ICMM submit that a risk-based evaluation is an appropriate approach to enable the use of technologies such as autonomous haulage and collision avoidance, that have potential to significantly improve health and safety outcomes, rather than to attempt to apply inappropriate functional safety standards. This risk-based evaluation may include, but is not limited to:

- Risk assessment techniques such as is outlined in ISO 12100, or equivalent risk assessment techniques, which may include:
    - Systems Theoretic Process Analysis (STPA)
    - Fault Tree Analysis (FTA) / Event Tree Analysis (ETA)
    - Failure Mode and Effects Analysis (FMEA)
    - Bowtie analysis
- Robust system development/project management processes
- Extensive system testing and validation
- EMESRT Control Framework (CfW)
- EMESRT Levels 1-6 – Incident preventative control levels[5]
- Engagement and collaboration between the various parties to address
    - Site specific aspects via risk assessment e.g. isolation and administrative processes to maintain restricted access to machine operating areas where appropriate
    - Change management
    - Configuration management
    - Operation and maintenance information

[2] ISO/TC 127 Earth-moving Machinery

[3] ISO/TC 127/SC 2/JWG 28, which is responsible for the development of ISO 21815 - *Earth-moving machinery — Collision warning and avoidance*, has determined to develop a methodology to assess the net benefit of deployment of collision awareness and avoidance systems.

[4] ISO/TC 127/SC 2/WG 24, which is responsible for the development of ISO 19014 - *Earth-moving machinery — Functional safety*, has determined to develop an earth-moving application of ISO/PAS 21448 to be used in conjunction with the ISO 19014 series. This work is expected to begin in the second quarter of 2020.

[5] EMESRT PR-5A Vehicle Interaction Systems (https://emesrt.org/2019/09/emesrt-publishes-pr-5a-version-2/)

Sharing of Functional Safety Information

There is much discussion on what level of functional safety information should be shared. These discussions include requests for OEM's to share detailed functional safety-related design information with end users and/or obtain independent third-party assessment of control system safety. A thorough analysis of such information requires detailed knowledge about the machine's design.

Sharing detailed information also poses significant risk to both the end user (e.g. anti-trust, transfer of design liability) and the OEM (e.g. risk of loss of technological advantage).

For deterministic systems, ISO/DIS 19014-2 states:

> *"…the following information may be shared relative to the functional safety of EMM that meet this standard. This information could be included in manuals or in other documentation given to the end user*
>
> - *A listing of the safety functions on the machine*
> - *A listing of the safety-related parts of the control systems; particularly if changes to those parts could void the functional safety conformance of the machine*
> - *Any maintenance, tests or inspection tasks that are necessary to maintain the integrity of the SCS's over the lifecycle of the machine"*

To further clarify, the following are examples of what this information may entail:

- A statement of what functional safety standard the machine safety functions meet
- A list of what the safety functions are on the machine, and what they do.
- End users may additionally request Machine Performance Levels Required (MPLr) and Machine Performance Levels Achieved (MPLa). ISO 19014 provides two methods to determine performance levels required:
    - ISO/TS 19014-5 provides a normative list of standardised safety functions, the MPLr, assumptions that formed the basis of the assessment, and the associated reasoning. Where the OEM provides assurance of conformance to ISO/TS 19014-5, this confirms that the MPLr has been met.
    - Where ISO/TS 19014-5 is not used, ISO 19014-1 provides a method to determine safety functions and/or scenarios not covered by ISO/TS 19014-5. If ISO 19014-1 is used, the MPLr should be provided along with confirmation that this MPLr has been met.
- Information necessary to maintain the safety integrity of the safety-related control system, including:
    - Operation and maintenance manuals, and service-related literature – maintenance frequencies, component change-out intervals etc
    - Commissioning testing and requirements documents
    - Testing requirements necessary to validate that the safety function is meeting performance requirements

For autonomy, specific to the system, application and site, further information-sharing and collaboration on the system and the process followed may be required commensurate to the complexity of the system such that the end user is able to manage functional safety risks on site e.g. change management of software updates.

For non-deterministic systems, refer to the proposed approach stated previously.

Appendix A - Background on Commonly Referenced Functional Safety Standards

ISO 13849 - *Safety of Machinery - Safety-Related Parts of Control Systems*, was originally intended to cover stationary machinery and associated energy types and is harmonized to the EU machinery directive. Its reference in **ISO 15998 - *Earth-moving machinery - Machine-control systems (MCS) using electronic components - Performance criteria and tests for functional safety*** has resulted in most mobile machine manufacturers electing to apply it to their product in the absence of a more applicable standard. However, the application of ISO 13849 to mobile earthmoving machines requires adaptation, principally because the machinery use-cases and content covered within the standard is specific to stationary machines, electronic systems and discrete safety functions (e.g. light curtain or interlock system that stops the machine when interrupted). ISO 13849 lacks application guidance on how to apply its principles to mobile machines and how its principles can appropriately be applied to complex non-electronic control systems, although such systems are included in the standards scope.

Some examples of the current challenges in applying ISO 13849 and other stationary machine standards to earthmoving machines include:

- The safe state for a mobile machine is at times dependent on the part of the operating cycle the machine is in, and may be different or even contradictory between parts of the cycle e.g. for a high speed vehicle travelling at full speed the safe state may be to slow at a pre-determined rate, but at lower speeds would be to stop with full braking. Another example is when travelling, steering should be maintained following failure of a component in the system until the machine is stationary, at which time the function should be disabled. ISO 13849 doesn't provide guidance for these situations.

- ISO 13849 assumes that base machine operations are not safety related, only the systems added to the machine specifically to address a hazard are safety related. This is not the case for mobile machines. Unlike stationary machines, dangerous control systems failures are not limited to interlocks around the machine – mobile machinery system failures to be considered also include control system that control machine movement, control systems that fail in a way that affects machine movement, as well as any control systems that were added to mitigate hazards. In the earthmoving machine industry typically these safety functions are embedded and integral to the

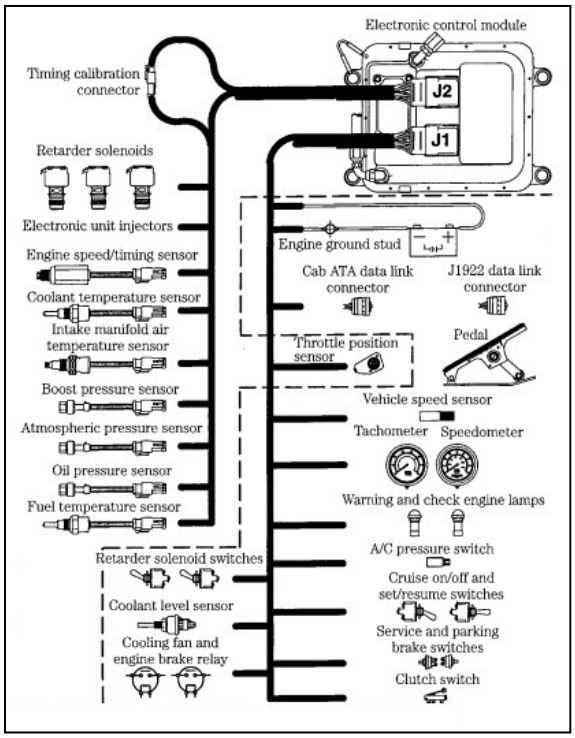


Figure 5 – I/O into an earthmoving machine diesel engine control module (a modern earthmoving machine may have 5 or more other similar electronic control modules). Note that I/O includes machine features that perform both operational and safety related functions

base machine functionality, rather than overlaid on top of the base machine function with separate control systems.

- Lack of guidance when two safety functions have conflicting outputs, for example: on high speed mobile machines 'applying brake without demand' and 'failing to apply brake on demand' may both be dangerous. However, the safe state of a system to prevent brakes applying without demand would be to not brake, and the safe state for a system that prevents a failure on demand of a brake system is to have the brakes apply. The two safe states for these hazards associated with the same system are contradictory to each other.

- While ISO 13849 considers control systems of all energy types, it lacks guidance for complex non-electronic systems. Many safety systems on earthmoving machines are complex hydraulic or mechanical systems.

The Earthmoving machine industry ISO standards committee (ISO/TC 127) attempted to rectify some of the aforementioned challenges by developing ***ISO/TS 15998 - Earth-moving machinery -- Machine-control systems (MCS) using electronic components*** --Other industries have taken a similar approach (agricultural industry with ISO 25119, and the automotive industry with ISO 26262).

As the industry's understanding of functional safety evolved, ISO 15998 needed updating to reflect current practices. As such, an ISO working group was formed to develop a replacement C-type standard, the ***ISO 19014 - Earth-Moving Machinery - Functional Safety*** series.

There are several other functional safety standards that have been proposed for use on earthmoving equipment. Some commentary is provided below:

- ***IEC 61508 series - Functional safety of electrical/electronic/programmable electronic safety-related systems***

  IEC 61508 is often colloquially referred to as 'the mother of functional safety standards'. It was written primarily with the intent of providing a set of methods, techniques and measures to be used in industry-specific functional safety standards development over the entire life cycle. The most common use of IEC 61508 is to design and certify safety related components, although it has also been used for system design. Because of the original intent, it is written to cover anything from the simplest system through to systems intended to prevent catastrophic events resulting from the failure of electronic / electronic programable systems. There are certain aspects and parts of this standard that can be helpful in the development of earthmoving machine systems and the design of their components. However, the experience of machine designers has been that something more specific and applicable to the earthmoving machinery application is required.

- ***IEC 62061 series - Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems***

  This standard is an adaptation of IEC 61508 to the stationary machine industry. It has a lot of overlap in scope with ISO 13849 and is often treated as an alternative to ISO 13849. Given the extent to which ISO 13849 is used already in the industry, IEC 62061 presents many of the same

issues related to inherent assumptions that the machine does not move. Additionally, IEC 62061 does not cover non-electronic control systems which are a prevalent control system type on earthmoving machinery.

- ***ISO 25119 series - Tractors and machinery for agriculture and forestry -- Safety-related parts of control systems***

  Early in the development of ISO 19014, the relevant ISO working group extensively discussed potential use of ISO 25119. It was noted by the committee that the risk graph in this standard was more suitable to earthmoving machines than those used in ISO 13849 and IEC 62061. However, due to the extensive use of hydraulic systems on earthmoving machines in comparison to agricultural machines (ISO 25119 does not cover this aspect), and the desire to be more closely aligned with the principles of ISO 13849 resulted in ISO 25119 not being adopted by the earthmoving industry.

- ***ISO 26262 series - Road vehicles -- Functional safety***

  There is some similarity between the earthmoving machinery component supply base and the automotive supply base. This lent itself well to the utilization of ISO 26262 as a reference standard during the development of the ISO 19014 series (particularly in the determination of performance levels and software requirements). However, ISO 26262 is written assuming high volume production and thus would have introduced significant complexity in the lower-volume production environment prevalent in the earthmoving industry. .

- ***ISO/PAS 21448 series - Road vehicles – Safety of the intended functionality***

  ISO/PAS 21448 applies to intended functionality that requires proper situational awareness in order to be safe, and where that situational awareness is derived from complex sensors and processing algorithms. The standard is concerned with guaranteeing safety of the intended functionality - SOTIF – in the absence of a fault i.e. it covers safety hazards that occur even though the system hasn't failed. Reasonably foreseeable misuse e.g. operator confusion or overload is also addressed. This is in contrast with traditional functional safety, which is concerned with mitigating risk due to system failure. SOTIF provides guidance on design e.g. requirement for sensor performance, verification e.g. test cases with high coverage of scenarios, and validation e.g. simulations. Functional safety (addressed by the ISO 26262 series) and SOTIF are distinct and complementary aspects of safety.

ISO 19014 Series

The intent of the ISO 19014 working group is to provide more specific guidance for the earth-moving industry by filling in the gaps in guidance that exist in ISO 13849 and ISO 15998 with material from other credible functional safety standards. Accordingly, the basic principles and processes of ISO 13849 are followed; however greater guidance on adaptation to the earthmoving machinery application is provided.

Development of the ISO 19014 series of standards is ongoing, with various parts gradually reaching publication stage. A summary of the series of standards is provided below:

- ***ISO 19014-1 – Earthmoving Machinery – Functional Safety - Performance level determination***
    - Contains an earthmoving specific risk graph with parameters defined specific to the application and characteristics.
    - The risk graph is adapted from ISO 25119 and ISO 26262.

- ***ISO 19014-2 – Earthmoving Machinery – Functional Safety – Hardware and system integration requirements***
    - An adaptation of ISO 13849 to mobile machines.
    - Explains what parts of ISO 13849 should and should not be used, with new content where needed.
    - New content taken from IEC 61508-2 and other best practices in the earthmoving industry.
    - Identifies the information related to functional safety that may be helpful to end users

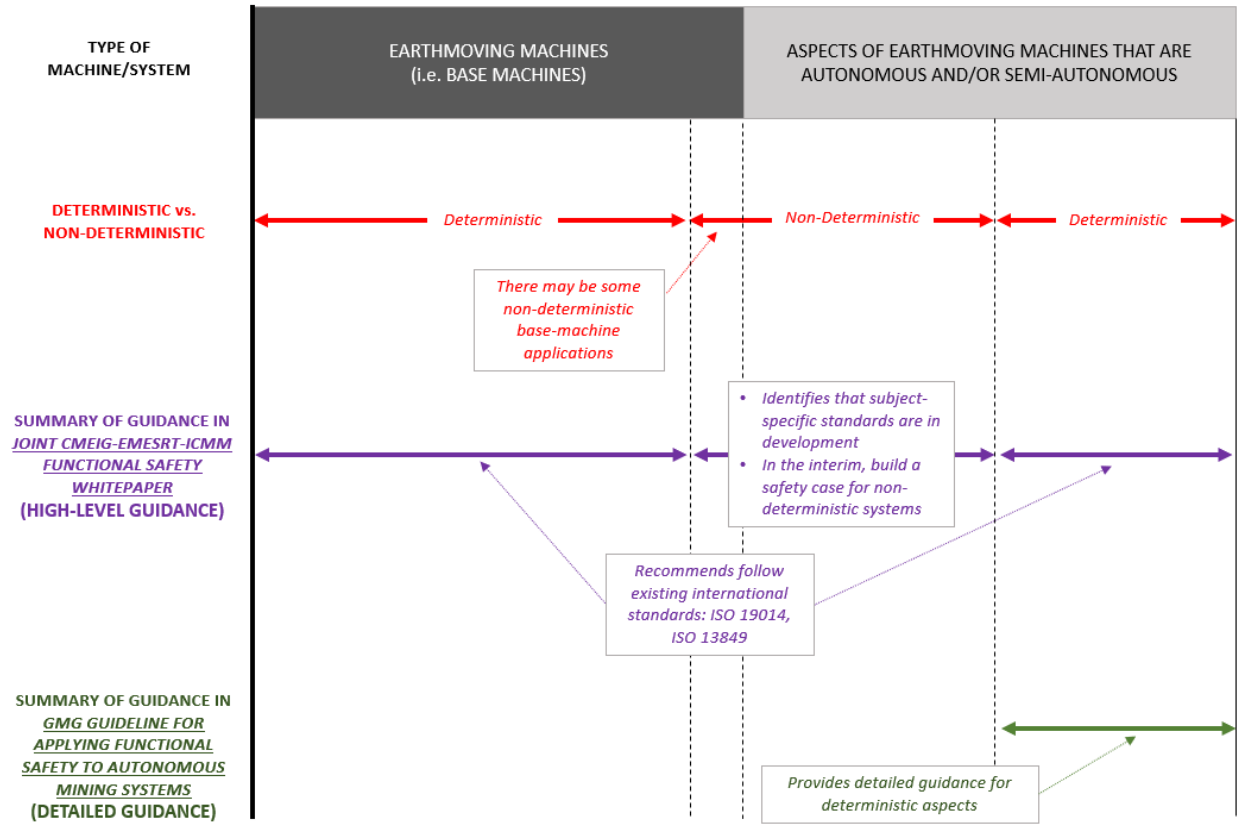
- ***ISO 19014-3 – Earthmoving Machinery – Functional Safety - Environmental testing requirements***
    - Due to the harsh operating conditions relatively unique to earthmoving machines, this part sets testing requirements to ensure safety related parts of control system components are suitable for the operating environment.

- ***ISO 19014-4 – Earthmoving Machinery – Functional Safety – Software development requirements***
    - Adaptation of software requirements within IEC 61508-3, ISO 25119 and ISO 26262, to the earthmoving machine application.

- ***ISO/TS 19014-5 – Earthmoving Machinery – Functional Safety - Table of performance levels***
    - Developed by an international team with broad experience of earthmoving machine use cases and applications.
    - Contains normative tables of performance levels required by machine and function.
    - Manufacturers have the choice of using part 1 or part 5. If the required performance levels determined in part 1 are different to those in part 5, then justification is needed as to why.

Appendix B – Relationship between this white paper and the GMG guideline

The illustration below explains the relationship between this white paper and the Global Mining Guidelines Group (GMG) *Guideline for Applying Functional Safety to Autonomous Mining Systems*[6].



[6] GMG Functional Safety Project - https://gmggroup.org/projects/functional-safety/