ADDENDUM TO FUNCTIONAL AND TECHNICAL PERFORMANCE REQUIREMENTS FOR COLLISION PREVENTION SYSTEMS: FAIL TO SAFE WITHOUT HUMAN INTERVENTION

INDUSTRY ALIGNMENT ON TMM REGULATIONS; SPECIAL PROJECT OF THE MINERALS COUNCIL SOUTH AFRICA

REV 1

COMPILED BY:

Name	Organisation	Signature	Date
Kobus Blomerus	**SECDI**		**11 October 2025**

APPROVED BY:

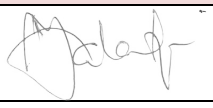
Name	Organisation	Signature	Date
Stanford Malatji	**Minerals Council**		20/10/2025

Table of Contents

1. Purpose

The purpose of this addendum to the CPS Functional and Technical Performance Requirements (F&TPR) specification, is to provide **additional information** to assist persons with the legal duty to specify their CPS products, as well as CPS product developers to ensure their products can fail to safe without human intervention (FTSWHI), according to regulation 8.10 of the Mine Health and Safety Act (Act 29 of 1996). FTSWHI is largely dependent on the design philosophies of the specific CPS products. **For this reason, a specific FTSWHI functional specification is not feasible. This document is not a design specification, and it does not absolve a product supplier of its engineering and design duty.** Since FTSWHI must be fully verified, the product supplier's FMECA is the **critical basis** of its product's FTSWHI. (Refer to the CPS Functional Readiness Criteria)

2. Scope

The scope of this document is limited to FTSWHI. This document must always be read in conjunction with the F&TPR Specification. The scope of the document is not to address all the detailed failures that a CPS must cater for.

3. Definitions and abbreviations

Definitions and abbreviations are listed in the F&TPR Specification and are not repeated here except for the addition of the following definitions:

NOP: Normal Operating

COC: Certificate of Conformance/Compliance

4. Context

The CPS F&TPR Specification defines all the functional and technical performance requirements that a Collision Prevention System must conform to. FTSWHI does not require any additional or different functionality, other than what is already specified in the CPS F&TPR Specification. Some CPS product suppliers have difficulty with the application of the FTSWHI requirement and therefore this addendum to the specification was developed to assist CPS product suppliers as well as legal appointees.

CPS product suppliers gave comments on and shared their understanding/interpretation of FTSWHI. Some of these are:

- A CPS can fail in an "unsafe area" of the mine and therefore the TMM cannot be automatically stopped and "safely" parked, the operator must stop the TMM in a "safe area" and "park" the TMM.
- A CPS FTSWHI is only required for some CPS element failures. Log keeping, self-diagnostics are examples that do not require FTSWHI.
- It is good enough to put the TMM in a "safe state", i.e. slow the TMM down to a limp speed so that the operator can park it.

These and other aspects of FTSWHI are addressed herein.

It is also important to note that a CPS failure will be a rare occurrence given the fact that the CPS reliability requirement is a MTBF > 2000 operating hours (more that 80 days of 24-hour operation and the CxD and TMM CPS availability of 98%, respectively. Naturally these requirements imply that CPS product suppliers have designed to these performance criteria and that:

- A CPS reliability model exists for every CxD/TMM CPS combination,
- A CxD reliability model exists for every CxD product/model,
- A TMM CPS reliability model exists for every TMM CPS supplied by TMM OEMs,
- A TMM CPS reliability model exists for 3rd Party TMM CPS products.

It is therefore important that CPS product suppliers do not focus on the potential place where a TMM might FTSWHI, but rather on the design of the product's reliability and the FTSWHI functions and requirements, to limit the occurrence of a FTSWHI as far as reasonably possible.

The fact that high risk areas do exist, and that unforeseen emergencies can arise requires CPS products to allow for these extremely rare cases.

PART 1: TECHNICAL CONTENT

5. Regulatory requirements

For ease of reference, the Mine Health and Safety Act (MHSA) Regulations 8.10.1 and 8.10.2 state:

Collisions between trackless mobile machines and pedestrians

"8.10.1.2 All underground diesel powered trackless mobile machines must be provided with means:

"(b…….. The prevent potential collision system on the diesel powered trackless mobile machine **must fail to safe without human intervention".**

Similarly, for opencast or open pit mines,

Collisions between diesel powered trackless mobile machines.

"8.10.2.1(b) ……. The prevent potential collision system on the diesel powered trackless mobile machine **must 'fail to safe without human intervention'".**

The MHSA further states 'Fail to Safe' means so designed as to **activate** and effectively perform its intended function without harm to persons and **without human intervention**.

A dictionary definition of **Fail to Safe**: may provide additional clarity to CPS product providers: 'causing a **piece of machinery** to revert to a "**safe condition"** in the event of a breakdown or **malfunction**, the purpose of which is, that, if this failure occurs, the operator or the equipment are not exposed to a higher level of danger'. Note that the definition emphasizes that the **machinery** must revert to a safe **condition** (not a safe position).

Applied to CPS, the question to be answered is: if a key functionality of the CPS (CxD or TMM CPS) malfunctions (is no longer available) due to some form of failure in the CPS, **will the operator or pedestrians** respectively be at higher levels of risk or harm, or not? The only credible answer is 'YES', because the operator(s) and the pedestrians have been trained to rely on the CPS, and now that functionality is missing. They are still relying on the system, but it is not working! Moreso, the CPS is intended to **only** function when a TMM operator is incapacitated, or a pedestrian (underground) is closer to an operating TMM than is safe. To allow a TMM with a failed CPS to continue to operate, will expose operators and pedestrians to a higher level of risk and danger respectively. A "slow" moving TMM can still cause a pedestrian a serious injury or even a fatal injury.

The **TMM** must therefore be put in a "**safe condition"** until the CPS is fully functional again, and it must be done **automatically**.

The FTSWHI relates to the **CPS** at a **system level** and **not** to the design of its elements, sub-elements or components. (This is the purpose of the design for reliability). FTSWHI is not at all related to the **prevention** of element or component failure, but the **detection** at an **element** level and the activation of the appropriate **system** (CPS) **response/action** when a CPS failure condition is detected.

Whilst other definitions related to equipment **failure** do exist, for the purpose of focus and clarity, those definitions are not discussed in this document.

6. High Level Requirements for FTSWHI

Although FTSWHI does not require **additional** functionality, it does **mandate** several CxD and TMM CPS requirements that product suppliers might not have considered **critical** before focusing on FTSWHI requirement.

TMM to be put in a "Safe Condition"

The safe condition for a TMM fitted with a CPS is **Safe Park**.

Safe Park is defined in the CPS F&TPR specification as: A way that a TMM is parked, namely: Machine static and prevented from any movement, whether through propulsion, articulation, or movement of any other controlled part (e.g. boom, fork, scoop, blade, etc.).

Without Human Intervention

The requirement is that the TMM reaches safe park without the operator doing anything.

CPS Fail to Safe without Human Intervention

When applying the fail-to-safe definition to regulations 8.10.1 and 8.10.2, it reads:

"*The **prevent potential collision system** on the diesel powered trackless mobile machine must be so **designed** as to **activate an FTS intervention** and effectively perform the FTS functions without harm to persons and **without human intervention** or*

"*The **prevent potential collision system** on the diesel powered trackless mobile machine must be so **designed to bring the TMM to a "safe condition" without** harm to persons and **without** human intervention.*"

The first aspect to consider is that the **CPS** must FTSWHI. This implies that when any of the elements of the CPS products can no longer fulfil its intended function, then the **CPS** must FTSWHI. It follows that the **CxD**, the **TMM CPS** or the **3rd Party TMM CPS** (where used) must all have **functions** (FTSWHI functions) to ensure that the CPS can FTSWHI. **(Note for underground TMMs' cap lamps form part of the CxD)**

When the CPS has failed before or at the time of **intended** use, it must not be possible to be used. Therefore, the CPS must **activate automatically when the operator starts the TMM**. The CPS must thus provide interlocks to prevent movement of the TMM before the CPS is operational.

It follows that the TMM CPS can only be started and put in motion once the CPS "handshake" is successfully concluded and full functionality confirmed.

A safe condition, i.e. safe park, also implies that, if the CPS failed, the TMM must be **prevented** from having any of its articulate elements (if fitted) moving so as not to put the person(s) that must attend to the failed CPS at higher risk than before the CPS failure. Whilst this is of particular importance for underground TMMs working in close proximity to pedestrians, it also applies to maintenance and repair personnel in both underground and surface operations.

A failed CPS therefore **must** result in the TMM being placed in safe park.

In the case of an operating TMM, it means the TMM must not be able to **continue** to operate and must be brought to **safe park as quickly as reasonably possible, without endangering the operator.**

The TMM must reach "safe park" **without** human intervention, i.e. **no reliance on the operator** to slow, stop, apply park brake or lock out articulation (where applicable) of the TMM. (This is the exact functionality employed for a collision prevention intervention)

The above can be summarized as:

A CxD, TMM CPS or 3rd Party TMM CPS (where applicable) must have FTSWHI functionality.

CPS must be automatically activated (CxD, TMM CPS or 3rd Party TMM CPS if applicable)

Successful full functionality handshake is required for the TMM to be put in motion/operation.

If the TMM is in safe park, the TMM must remain in safe park until the failure is resolved or authorized override is actioned (for recovering the TMM to effect repairs).

If the TMM is stationary with the engine running when failure is detected, the TMM must remain stationary, park brake to be applied automatically and shall not have any articulation, boom movement, etc. and the operator to follow the mine's procedure with regards to shutting down the TMM and disembarking from the TMM.

If the TMM is moving, the TMM must be brought to a **safe speed**, stopped and brought to safe park automatically.

7. FTSWHI States of the CPS

To facilitate alignment between mines and CPS product suppliers, it is useful to define specific **states** for a CPS FTSWHI event.

A **FTSWHI** event comprises the following four states:

7.1 The Fail to Safe initiator/trigger:

In the event of an element, subsystem or component failure, the **element** (CPS product) that identified the failure must trigger the FTSWHI intervention. That is:

In the case of a CxD failure, the CxD sends an FTS trigger via the interface to TMM CPS controller or detects communication timeout. **(Note: For underground TMMs a Cap Lamp low battery level or low bright LED must trigger a CxD FTS.)**

When the TMM CPS or 3rd Party TMM CPS receives a FTS trigger from the CxD or it detects communication timeout or if the failure is in a sub element of the TMM CPS, the FTSWHI intervention process must be **automatically** triggered by the TMM CPS / 3rd Party TMM CPS controller.

The importance of **self-diagnostic** functionality is evident from the abovementioned bullets. A CPS product must have the ability to continuously monitor its health and have the functionality to initiate a FTS trigger once it detects a failure that will jeopardize the **sub element** functionality.

7.2 The Fail to Safe Process:

If the FTS event is triggered while the TMM is moving, the TMM must automatically slow down to a **safe** or crawl speed and then **automatically** stop and **automatically** apply the park brake. **Note that this process is identical for the TMM CPS when a collision prevention intervention is triggered.**

Note: For FTSWHI the **rate** of slowing down a TMM that is above the **safe speed** can be **less** than that of a collision prevention deceleration, since there is no imminent collision, even the **safe speed** can be **lower**.

7.3 The Fail to Safe end state:

The end state is **safe park** and includes articulation and attachment lockout (where applicable).

This is the default end state for any FTSWHI.

Note: The machine must not be able to move until the technician has repaired the CPS and cleared the fault code with an authorized identification.

7.4 A Fail to Safe Motion Enabler (OVERRIDE)

If for whatever reason the **mine** procedures require/allow for the CPS-failed TMM to be moved, the CPS must have an FTS motion enabler.

For FTSWHI two movement enabler functions must be available as described below:

Authorised Override Standby mode (see ISO/TS 21815-2 2021)- If the TMM cannot be repaired in situ and must be moved back to the workshop/repair location for repair by an authorised person, the authorised person must be able to override the CPS. The standby mode is a configurable limited speed limp mode for a limited, configurable duration.

This functionality must be available on both the CxD and TMM. It is unreasonable to expect a CxD technician to have the necessary training, authorization and credentials to override a TMM CPS. In the same way, a TMM CPS technician should not have the authority to override a CxD. The CxD must use the appropriate command as specified in ISO/TS 21815-2:2021 to communicate an override to the TMM CPS. The TMM CPS shall use the appropriate message to indicate the Override Status as specified in ISO/TS 21815-2:2021.

Emergency Override – Standby mode. This mode is **operator** activated. Emergency override as per **mine procedures** can only be activated by a specially designed button that will ensure that the operator cannot use it other than for the emergencies as defined by the mine.

This functionality enables a mine to deal with any **“Emergency” and “High Risk”** scenarios based on its own risk assessment, operational rules and procedures.

Note: Emergency Override is primarily required for collision prevention interventions. The same functionality is used for FTSWHI.

Refer to Part 2 of this document for more information on emergency and high-risk scenarios. In these instances, the mine’s CPS emergency procedure shall define the conditions and requirements for such “Emergency” override as well as the procedures to be followed.

Emergency Override functionality resides on the TMM CPS. This is to ensure that the operator will be able to use the functionality even in the presence of a breakdown, fault or malfunction on the CxD. However, if redundancy is provided to ensure that the functionality remains available, even in the presence of reasonably foreseeable faults/breakdowns/malfunctions of the CxD, it will be deemed acceptable on the CxD.

Note: The speed limit and duration are to be configurable based on the outcome of a site-specific risk assessment. The default speed limit cannot be higher than 10km/h to ensure that the emergency override is not abused. Emergency override interventions must be specifically recorded and reported as per the mine's procedure.

Post Fail to Safe (After repair)

On completion of the repair of the failed product, the CPS must revert back to the state (settings and configuration) as before the FTS event, known as NOP – Normal Operation in ISO21815 terms. Refer to ISO21815-1 for specifics.

The mine must have a procedure to be followed before activating NOP, as the nature of the failure may require COC and functional testing of the equipment, e.g., brake tests, etc.

8. CPS Functional Breakdown

For ease of reference, paragraph 9 of the F&TPR Specification is repeated here:

The non-homogenous population of TMMs used in the SAMI necessitates a **single** set of CPS functions. For a fully functional CPS, **all** the performance requirements must be met. The extent to which a specific CPS product needs to be developed will be determined by the extent to which a specific TMM (Type, brand and model) is already intelligent.

The CPS Functional Breakdown is shown in Figure 1.

The CPS comprises two functional elements(products) namely:

- **TMM CPS Functions (TMMCPS).**
- **CxD Functions (CxD).**

Each of the functional elements have a number of subgroups of functions. These groups are **logically** structured and do not imply that a CPS element must have a similar product breakdown structure. Naturally the two elements are products.

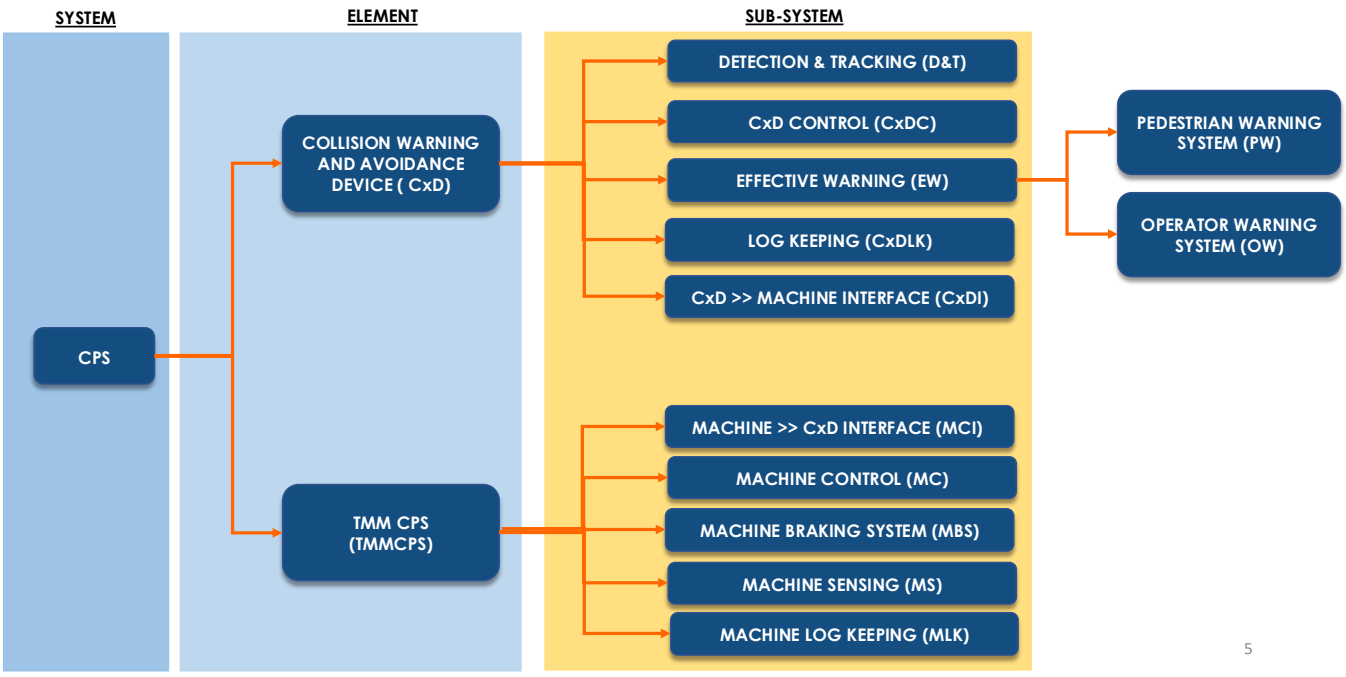


Figure 1: CPS functional breakdown structure.

The CxD Functions are broken down into 5 sub-groups namely:

- Detection and Tracking functions (D&T).
- CxD Controller functions (CxDC).
- Effective Warning functions (EW).
- CxD Log Keeping functions (CxDLK).
- CxD Machine Interface (CxDMI).

NOTE: For underground TMMs the cap-lamp is considered part of the CxD

The TMM CPS Functions are structured in 5 sub-groups namely:

- Machine CxD Interface functions (MCxDI).
- Machine Controller functions (MC).
- Machine Braking System functions (MBS).
- Machine Sensing functions (MS).
- Machine Log Keeping functions (MLK).

9. Implications for FTSWHI

Knowing what functional element failed (Self-Diagnostics)

For FTSWHI it is only necessary to know what **sub element** failed, i.e. CxD, TMM CPS or 3rd party TMM CPS (where applicable).

For the CxD

The Detection and Tracking functions (D&T): It is important that the self-diagnostics of the D&T element include off-board elements such as cap lamps pedestrian detection devices (underground), beacons (surface and underground) and repeaters (surface and underground) and any other component key to reliably detecting machines (surface) or pedestrians (underground).

CxD Controller functions (CxDC),

- Effective Warning functions (OWS & PWS for underground and OWS for surface),
- CxD Log Keeping functions (CxDLK),
- CxD Machine Interface functions (CxDMI).

Note: For underground TMM a failure of the cap lamp must also trigger a FTSWHI

For the TMM CPS / 3rd Party TMM CPS

- Machine CxD Interface functions (MCxDI),
- Machine Controller functions (MC),
- Machine Braking System functions (MBS),
- Machine Sensing functions (MS),
- Machine Log Keeping functions (MLK).

Acting on a CPS Failure

For the CxD

Upon detecting a CxD sub element failure, the CxD must:

- Trigger an FTS message to the TMM CPS,
- Notify the Operator of a CxD FTS event – Visual and audible notification,
- Notify the Operators of all other TMMs in the detection zone – status = broken down,
- Keep log of the sub element that failed,
- Keep on sending the FTS message until the failure has been resolved.

In order to notify other TMMs that a CPS failed, the TMM that FTSWHI must act as a beacon to prevent other TMMs from colliding with the failed TMM. This functionality must work irrespective of what CPS product failed. When the CxD to CxD communication fails, this function will not be possible.

Upon receiving a TMM CPS FTS notification the CxD must:

- Initiate the FTS process
- Send an FTS trigger – this is considered best-practice, although the CxD cannot reasonably expect a response from the TMM.
- Notify the Operator of a TMM CPS FTS event – Visual and audible notification
- Notify the Operators of all other TMMs in the detection zone – status = broken down.
- Keep log of the notification.

Power Supply/Battery Backup

To ensure that the CxD beacon functionality is active for a sufficient period, even if the TMM battery failed, or is isolated, a battery backup is required. (See F&TPR Specification).

For underground TMMs a cap lamp battery low level and/or a LED low bright must trigger a FTSWHI.

10. Testing FTSWHI Functionality

Since most of the functions required for FTSWHI are functions specified in the F&TPRS and are tested during a number of the TRL tests, there is not a FTSWHI **specific** test. To demonstrate verification of FTSWHI, once all the required functions have been verified, the stage gate report will include verification of the FTSWHI.

The Testing of FTSWHI is set out in the CPS Test specification.

PART 2: FREQUENTLY ASKED QUESTIONS

This part of the addendum addresses some of the frequently asked questions and issues raised around FTSWHI. This part is not an exhaustive list of scenarios or issues and is not to be construed as the only aspects to be addressed.

What about Emergency and High-Risk FTSWHI scenarios?

It is important for product suppliers to consider the context of FTSWHI specifically the probable frequency of such events. The CPS system reliability requirement is a MTBF > 2000 operating hours. Given this requirement, it is not necessary to design FTSWHI for extreme **peripheral** cases. With the very low probability of occurrence of a CPS FTSWHI event, the probability that a FTSWHI event will occur in a **high-risk scenario** is orders of magnitude smaller. The **CPS emergency override functionality** enables a mine to adequately provide for such very rare high-risk scenarios.

Since High-Risk CPS failure scenarios are frequently raised, a few such scenarios are specifically considered below:

A CPS that will FTSWHI next to a burning TMM.

The likelihood that a TMM operator will drive her/his TMM within 10m from another burning TMM is insignificantly low and for a TMM to start burning next to another FTSWHI TMM at exactly the time of FTSWHI is most likely improbable.

Pedestrian pinned or to be pinned against side wall.

A CPS failure at the exact instance of a collision prevention intervention and a pedestrian that was about to be pinned against the side wall or is actually pinned against the side wall or is trapped under a TMM is very unlikely and probably an incredible event. The purpose of the CPS is to prevent that a pedestrian will ever find herself/himself in such a situation. The CPS F&TPR further requires a **Pedestrian Activated Emergency Stop** function that can be used to prevent such a highly unlikely event. Additionally, based on the mine's specific risk assessment, the Emergency Override can be used by the TMM operator if such a highly unlikely event does occur.

CPS Failure on Blind Rise?

A CPS failure on a blind rise or a blind curve is another scenario often mentioned.

A CPS failure on a TMM that just passed a blind rise will bring the TMM to a **safe park.** Three CPS functionalities will be at play in this scenario. A TMM with a failed CPS will act as a beacon for other TMMs approaching. Where the rise is such that loss of communication is possible, a repeater will be required to ensure communication. The following distance functionality of the approaching TMM will ensure that the approaching TMM will not collide with the CPS-failed TMM. The emergency override functionality enables the operator of the CPS failed TMM to move the TMM as per mine specific procedure for the **specific** blind rise.

CPS Failure Next to a High Wall.

Most, if not all mines have **exclusion zones** from high walls and those exclusions are bounded by physical berms on crests and often also on the high wall side of loading areas or identified by cones.

The person in charge of the loading has the legal duty to ensure conformance to the exclusion zones. By implication, it is highly unlikely that a TMM will ever be inside a highwall danger zone. Such areas can also be enforced with CPS as an additional layer of control.

CPS Failure in Intersection

This is another frequently mentioned scenario. The question is what about a FTSWHI inside an intersection. The first aspect to consider is that intersections will either have stops on both sides of one of the roads or it will have stops at every entrance of the intersection. In the case of a CPS FTSWHI of one TMM approaching the intersection, all other TMMs approaching should be able to pass. A collision in this case is therefore not possible. If a CPS failure occurs when a TMM is just taking off at an intersection, the TMM will come to a stop and the operator can use the emergency override to move the TMM. If at that exact time another TMM is approaching the failed TMM, it should be stopped as per the mine procedure for any broken down TMM. If the operator is incapacitated, the approaching TMM's CPS will auto slow and stop the TMM.

CPS Failure on an Up ramp when Hauling

A CPS failure in this scenario will be handled exactly the same as any TMM brake failure, engine or fire warning except that in the case of a CPS failure the TMM will be automatically slowed and stopped.

The F&TPR specification and this addendum must be viewed in light of the context above and therefore "high risk scenarios" are not addressed in terms of specific FTSWHI processes; however, provision is made in the general FTSWHI process for mines to adequately deal with it from a CPS functionality point of view.

11. Other Frequently Asked Questions

Do both the CxD and TMM CPS products need to be Fail-to-Safe?

Yes, for the CPS as a system to be FTS both the CxD and TMM CPS must be FTS.

Can one rely on the operator to intervene when a critical failure is present?

No, Clauses 8.10.1.2(b) and 8.10.2.1(b), as well as the definition of fail to safe in the preamble of 8.10, specifically states that the system must fail to safe automatically without human intervention.

Which failure modes are considered critical, that require fail-to-safe intervention?

This is entirely dependent on the design of the CPS, i.e., CxD, cap lamp, TMM CPS / 3rd Party TMM CPS.

A CPS product provider is responsible to conduct a failure modes, effects and criticality analysis (FMECA) to identify reasonably foreseeable failure modes of its product and the criticality of the specific failure mode, in order to determine appropriate responses (fault tolerance).

Typically:

- Critical CPS functionality cannot be met (e.g., all sensors to detect pedestrians fail).
- Criticality of the failure mode to determine appropriate response (fault tolerance).

- Some redundancy may be included in the design (e.g., multiple sensors to detect pedestrians), brief failure of one sensor (e.g., loss of signal) not critical.
- Other failures may be CAN-bus unplugged.

How can we achieve improved reliability to minimize FTS interventions?

Being a safety system where system (CPS) reliability is a key performance criterion i.e. 2000 hours MTBF it is critical that a proper CPS reliability model be established at the beginning of the system design. The model must allocate reliability requirements to each of the products based on their individual design. A normal design for reliability process must be followed, including component selection based on reliability values, and/or redundancy may be included in the design (e.g., multiple sensors to detect pedestrians), such that brief failure of one sensor (e.g., brief loss of signal) is not critical. Another example is the use of multiple independent power sources.

How is a TMM recovered back to a workshop or other safe area to effect repairs once it is in safe park?

An authorized person may override the CPS to recover the TMM to the workshop (known as authorized override with stand-by/limp mode).

Activation of stand-by/limp mode triggers the mine's CPS maintenance override process.

Conditional release results in limited functionality (e.g., crawl speed only).

Besides all the functionalities required to ensure the above, the CPS must naturally have a very robust self-diagnostic capability as well as a log keeping capability that will enable unambiguous traceability of the detail parameters, requests, triggers, and instructions.

12. Conclusion

This addendum addresses concerns raised by CPS product suppliers and mines, clarifies the regulatory requirement, emphasizes the importance of a number of functional requirements, explains the level of self-diagnostics required for FTSWHI and documents context and content as applied to CPS.

13. References

The following documents are referenced in this document:

[1] Mine Health and Safety Act No. 29 of 1996 and Regulations

[2] ISO/PRF TS 21815-2:2021 Earth-moving machinery — Collision warning and avoidance — Part 2: On-board J1939 communication interface

[3] ISO/IEC/IEEE 15288:2015, Systems and software engineering — System life cycle processes

[4] MIL-STD-490B:1992 Draft Military Standard Program-Unique Specifications.

[5] ISO/FDIS 16290:2013. Space systems — Definition of the Technology Readiness Levels (TRLs) and their criteria of assessment