Requirements for "Fail to Safe" (FTS)
for
Collision Prevention Systems (CPS)

1. Context

1.1 Regulations

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:

(a) to automatically detect the presence of any pedestrian within its vicinity. Upon detecting the presence of a pedestrian, the operator of the diesel powered trackless mobile machine and the pedestrian shall be warned of each other's presence by means of an effective warning; and

(b) in the event where no action is taken to prevent potential collision, further means shall be provided to retard the diesel powered trackless mobile machine to a safe speed whereafter the brakes of the diesel powered trackless mobile machine are automatically applied. ***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 The employer must take reasonably practicable measures to ensure that persons are prevented from being injured as a result of collisions between diesel powered trackless mobile machines. At any opencast or open pit mine where there is a significant risk of such collisions, such measures must include:
8.10.2.1 Every diesel powered trackless mobile machine must be provided with means to automatically detect the presence of any other diesel powered trackless mobile machine within its vicinity; and
8.10.2.1(a) upon detecting the presence of another diesel powered trackless mobile machine, the operators of both diesel powered trackless mobile machines shall be warned of each other's presence by means of an effective warning; and
8.10.2.1(b) in the event where no action is taken to prevent potential collision, further means shall be provided to retard the diesel powered trackless mobile machine to a safe speed where after the brakes of the diesel powered trackless mobile machine are automatically applied. ***The prevent potential collision system on the diesel powered trackless mobile machine must 'fail to safe 'without human intervention."***

8.10 Definitions: *'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 is: "causing a piece of machinery to revert to a safe condition in the event of a breakdown or malfunction".

2. Requirements

2.1 Fail-safe

The **first** aspect to clarify is "Fail-safe". Fail-safe is the requirement that, in the case of a failure, the system will respond in a way that will cause minimal to no harm to other equipment, the environment or to people. When a fail-safe system fails, it remains at least as safe as it was before the failure. Fail-safe does not mean failure is impossible or improbable (not inherent safety).

2.2 Fail to Safe

The **second** aspect to clarify is "fail-to-safe", as required in the TMM Regulations. 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 and effectively perform its intended function without harm to persons and without human intervention.*"

- Firstly, this means the collision prevention system (CPS) must **activate automatically,** when necessary, i.e. when the TMM is started up, or attempted to be used. An operator-switch to activate the CPS does not therefore conform to this requirement.
- The requirement further implies that, if the CPS cannot effectively perform its intended function, it **must prevent** the machinery from performing anything that may lead to harm to persons. In the case of a TMM, it means the TMM must not be able to continue to operate and must be brought to a **safe state.**
- The TMM must reach the safe state **without** human intervention, i.e., no reliance on the operator to slow and stop the TMM.

This reality has a major impact on the design and legal accountability of:

1) The CPS provider.
2) The CxD (Collision avoidance and warning Device) provider (including cap lamps).
3) The TMM CPS provider.
4) The interface supplier, if applicable.

Implications of Fail to Safe

As defined in the CPS technical documentation (Part 1: Functional Readiness Criteria for Collision Prevention Systems Development) for every CPS, meaning, every single CxD and TMM combination (brand, type, model, and even serial no.) a CPS provider must be agreed between the CxD and TMM CPS providers. The CPS

provider is responsible to ensure "fail to safe" of the CPS, i.e., fail-to-safe of that integrated system.

The implication is that the CxD and the TMM CPS must each be "fail to safe", (including clearly defined separation of the responsibility of each), and the integrated system (CPS) must also be "fail to safe."

Why not only have the CxD to Fail to Safe?

It is unreasonable and irrational to expect a CxD to auto slow and stop the TMM if the TMM CPS fails. Such intervention into a product from another manufacturer/supplier will have serious implications for liability. Section 21 of the MHSA places responsibility on all persons (suppliers) of items (products)each for its own product.

Self -diagnostics

The CPS and its elements therefore must be provided with a robust self-diagnostic functionality, again, implying that the CxD, the interface (where a separate product) and the CPS TMM must have its own self-diagnostics, such that failure on any one of the products will result in a CPS failure being detected and actively controlled/managed.

Requirements of the interface between the products, such as the "heartbeat" are also key aspects of the fail to safe functionality and thus must be part of the self-diagnostics.

Cap Lamps

For underground TMM CPS CxDs, the pedestrian cap lamp is a key element of the CxD product that requires special focus in terms of its requirements and self-diagnostics.

Safe State.

A safe state is the state of the TMM, such that it cannot perform anything that may lead to harm to persons. A safe state is when the TMM cannot move and any of its movable elements (articulation, boom, bucket etc.) are de-energized.

- A safe state therefore depends on the state of the TMM when the failure occurred. Is it moving, stationary or safe parked?
  - If safe parked: TMM remains in safe park.
  - If stationary with engine running: TMM to remain stationery, park brake applied and no articulation, boom movement, etc.
  - TMM moving: TMM brought to a safe speed, brakes park brake applied and no articulation, boom movement, etc.

Post Fail to Safe

On completion of the repair of the failed product, the CPS must revert back to the state (settings and configuration) as before the fail to safe event.

3. Frequently Asked Questions

Does my CxD and TMM CPS product need to be Fail-to-Safe?

Yes, this is required in Clause 8.10.1.2(b) for underground TMMs and 8.10.2.1(b) for surface TMMs. The CPS as a system must also be FTS.

What if bringing the TMM to a safe stop further endangers the operator or other persons?

A CPS failure will be a very rare event if the CPS is correctly designed and qualified. In the unlikely event that a CPS failure occur in a high hazard area or to remove the TMM from inflicting further harm to persons an Emergency override (conditional release) may be granted to authorized, competent persons, e.g., in case of a medical emergency, but the override must trigger a reportable incident process and the conditional release must result in limited functionality (e.g., crawl speed only and for a limited time eg. 3 minutes).

Can I 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 state 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 and the interface.

A 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 more critical, e.g., 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, as an example: some 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.
- Failures such as CAN-bus unplugged may be more critical.

How do I recover a machine once it is in a safe condition back to a workshop or other safe area to effect repairs?

- Authorized, competent person to effect repairs if it is safe to do so. If necessary, authorized person may override the CPS to recover TMM to workshop (known as stand-by/limp mode).
  - Activation of stand-by/limp mode triggers maintenance override process
  - Conditional release results in limited functionality (e.g., crawl speed only)