CPS Fail to safe

Herman Hamersma

26 January 2023

Make today matter

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Faculty of Engineering, Built Environment and Information Technology

Fakulteit Ingenieurswese, Bou-omgewing en Inligtingtegnologie / Lefapha la Boetšenere, Tikologo ya Kago le Theknolotši ya Tshedimošo

Fail to safe

What do the Regulations say?

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.

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

Dictionary: causing a piece of machinery to revert to a safe condition in the event of a breakdown or malfunction.

Fail-safe

What does it mean?

- Fail-safe means:
  - 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.
  - Fail-safe does not mean failure is impossible or improbable (not inherent safety)
  - When a fail-safe system fails, it remains at least as safe as it was before the failure
    - Will failure of the CPS place the operator or pedestrians at more risk of harm?
    - Probably. The operator and pedestrians have been trained to rely on the CPS to ensure safety.
    - CPS failure thus requires more than just fail-safe

Fail to safe

What does it mean?

- What about fail-to-safe, as required in the Regulations?
  - 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 without human intervention
    - The CPS must activate automatically, e.g.
      - Activate CPS (boots-up) when the machine starts
      - Without operator action
      - TMM may not move until CPS is ready
    - If the CPS cannot effectively perform its intended function, it must prevent the TMM from performing anything that may lead to harm to persons (operators and pedestrians), e.g.
      - When CPS fails, TMM may not move
      - Articulation and attachment movement locked out

Key questions

- **When can the CPS not effectively perform its intended function?** (some examples)
  - 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), e.g.
    - 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
    - FMECA to determine criticality of failure mode

- **How is a failure detected?** (some examples)
  - Following proper fail-safe design principles, e.g. SAHR brakes, etc. (mechanical system)
  - Self-diagnostics to detect presence of failure modes (electronic detection)

Key questions

What happens when a failure occurs? (some examples)

- Depends on the current state of the TMM. Is it moving or stationary? Is it safe parked?
  - Safe parked: TMM remains in safe park
  - Stationary with engine running: TMM remains stationary
  - TMM moving: TMM brought to a gradual, safe stop and kept stationary
- Once a critical failure occurs, TMM must be brought to a safe stop, or kept stationary, until the failure is resolved.
  - Fail-to-safe functionality needed on both the CxD and the TMM
  - A clearly defined separation of the responsibility of each
  - If failure occurs on TMM, irrational to expect CxD to trigger fail-to-safe functionality. What about accountability?
  - Section 21 responsibility on all suppliers of equipment, unassigned/ambiguous responsibility will be assigned to the 2.13.1

Fail to safe

What happens once the TMM is in a safe state?

- 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 mode).
  - Activation of stand-by mode triggers maintenance override process
- If TMM needs to be moved, conditional release (override) may be granted, e.g.
  - In case of a medical emergency.
  - Override triggers reportable incident process
- Conditional release results in limited functionality (e.g. crawl speed only)

Key points

- Fail-to-safe functionality is required by the Regulations.
    - If your supplier does not have fail-to-safe functionality (CxD & TMM), you need to apply for exemption
- The CPS safe state is a stationary TMM that is prevented from moving (including no articulation/boom extension, etc.) before the issue is resolved by a competent person
- The TMM must reach the safe state without human intervention, i.e. no reliance on the operator to slow and stop the TMM.
    - This implies fail-to-safe functionality on both the CxD and the TMM
    - Responsibility on both suppliers (Section 21) to provide fail-to-safe functionality
- Once the TMM is safely parked, a conditional release (override or stand-by mode) may be granted
    - Depends on the situation, but there are consequences
    - Conditional release results in limited functionality (e.g. crawl speed only)

Discussion

Thank You