भारतीय मानक

Indian Standard

IS 19092 (Part 5) : 2024
ISO 19014-5 : 2021

भू-संचलन मशीनरी — कार्यात्मक सुरक्षा

भाग 5 निष्पादन स्तरों की सारणियाँ

Earth-Moving Machinery — Functional Safety

Part 5 Tables of Performance Levels

ICS 53.100

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुर शाह ज़फर मार्ग, नई दिल्ली - 110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI - 110002
www.bis.gov.in www.standardsbis.in

December 2024 **₹ 2775**

Earth Moving Equipment and Material Handling Sectional Committee, MED 07

NATIONAL FOREWORD

This Indian Standard (Part 5) which is identical to ISO/TS 19014-5 : 2021 'Earth-moving machinery — Functional safety — Part 5: Tables of performance levels' issued by the International Organization for Standardization (ISO) was adopted by the Bureau of Indian Standards on recommendation of the Earth Moving Equipment and Material Handling Sectional Committee and approval of the Mechanical Engineering Division Council.

The text of ISO standard is proposed for publication as an Indian Standard without deviations. Certain terminologies and conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'; and

b) Comma (,) has been used as a decimal marker, while in Indian Standards, the current practice is to use a point (.) as the decimal marker.

Under the general title 'Earth-moving machinery — Functional safety', the other parts are as following:

Part 2	Design and evaluation of hardware and architecture requirements for safety-related parts of the control system
Part 4	Design and evaluation of software and data transmission for safety-related parts of the control system

In this adopted standard, reference appears to certain International Standards for which Indian Standards also exist. The corresponding Indian Standard, which are to be substituted in their respective place, are listed below along with their degree of equivalence for the editions indicated:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
ISO 6165 Earth-moving machinery — Basic types — Identification and terms and definitions	IS/ISO 6165 : 2012 Earth-moving machinery — Basic types — Identification and terms and definitions	Identical
ISO 12100 : 2010 Safety of machinery — General principles for design — Risk assessment and risk reduction	IS 16819 : 2018/ISO 12100 : 2010 Safety of machinery — General principles for design — Risk assessment and risk reduction	Identical
ISO 19014-1 Earth-moving machinery — Functional safety — Part 1: Methodology to determine safety-related parts of the control system and performance requirements	IS/ISO 19014-1 : 2018 Earth-moving machinery — Functional safety: Part 1 Methodology to determine safety related parts of the control system and performance requirements	Identical
ISO 19014-3 Earth-moving machinery — Functional safety — Part 3: Environmental performance and test requirements of electronic and electrical components used in safety-related parts of the control system	IS/ISO 19014-3 : 2018 Earth-moving machinery — Functional safety: Part 3 Environmental performance and test requirements of electronic and electrical components used in safety-related parts of the control system	Identical

(*Continued on third cover*)

Contents

Page

Introduction

This document addresses functional safety of all types of energy systems utilized by earth-moving machinery.

The structure of safety standards in the field of machinery is as follows:

Type-A standards (basis standards) give basic concepts, principles for design and general aspects that can be applied to machinery.

Type-B standards (generic safety standards) deal with one or more safety aspects, or one or more types of safeguards that can be used across a wide range of machinery:

— type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);

— type-B2 standards on safeguards (e.g. two-hands controls, interlocking devices, pressure sensitive devices, guards).

Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

This document is a type C standard as stated in ISO 12100.

This document contains a list of Machine Performance Level requirements (MPL_r) by function and earth-moving machinery type, determined through the process outlined in ISO 19014-1.

This document is of relevance, in particular, for the following stakeholder groups representing the market players with regard to machinery safety:

— machine manufacturers (small, medium and large enterprises);

— health and safety bodies (regulators, accident prevention organizations, market surveillance etc.).

Others can be affected by the level of machinery safety achieved with the means of the document by the above-mentioned stakeholder groups:

— machine users/employers (small, medium and large enterprises);

— machine users/employees (e.g. trade unions, organizations for people with special needs);

— service providers, e. g. for maintenance (small, medium and large enterprises);

— consumers (in case of machinery intended for use by consumers).

The above-mentioned stakeholder groups have been given the possibility to participate at the drafting process of this document.

The machinery concerned and the extent to which hazards, hazardous situations or hazardous events are covered are indicated in the Scope of this document.

When requirements of this type-C standard are different from those which are stated in type-A or type-B standards, the requirements of this type-C standard take precedence over the requirements of the other standards for machines that have been designed and built according to the requirements of this type-C standard.

Indian Standard

EARTH-MOVING MACHINERY — FUNCTIONAL SAFETY

PART 5 TABLES OF PERFORMANCE LEVELS

1 Scope

This document provides normative tables of machine performance levels required (MPL_r) by common function and type for earth-moving machinery (EMM) as defined in ISO 6165. These MPL_r can then be mapped or applied to safety control systems (SCS) used to control or that affect the functions defined in the table.

The MPL_r in this document are determined through the machine control system safety analysis (MCSSA) process outlined in ISO 19014-1. A brief explanation of how the levels were derived and the associated assumptions are contained herein.

This document is not applicable to EMM manufactured before the date of its publication.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 6165, *Earth-moving machinery — Basic types – Identification and terms and definitions*

ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 19014-1, *Earth-moving machinery — Functional safety — Part 1: Methodology to determine safety-related parts of the control system and performance requirements*

ISO 19014-2:2019, *Earth-moving machinery — Functional safety – Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system*

ISO 19014-3, *Earth-moving machinery — Functional safety — Part 3: Environmental performance and test requirements of electronic and electrical components used in safety-related parts of the control system*

ISO 19014-4, *Earth-moving machinery — Functional safety — Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 6165, ISO 12100, ISO 19014–1, ISO 19014-2, ISO 19014-3, ISO 19014-4 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
idle factor
factor applied as part of determining the H variable (hazard time) to account for maximum or minimum idle time (100 % - max / min idle %)

EXAMPLE 1 Minimum idle time would be applied to loading a machine waiting for hauling machines during the loading cycle (idle factor = 10 %).

EXAMPLE 2 Maximum idle time would be applied to hazards associated with a stationary machine [*hold still* (3.2) function – idle factor = 50 %].

3.2
hold still
function that keeps the wheels or crawler tracks stationary, preventing the machine from moving

EXAMPLE A SCS that would control the hold still function is a park brake.

3.3
slow/stop
function which reduces or brings to zero the *machine speed* (3.4)

EXAMPLE A SCS that would control the slow/stop function is a service brake.

3.4
machine speed
function which controls the rate of travel

EXAMPLE A SCS that would control the machine speed function is a throttle control, propel control or gear selection control.

3.5
engine speed
function which controls the rotational speed of the engine

EXAMPLE A SCS that would control the engine speed function is a throttle control.

3.6
machine direction
function which controls the longitudinal direction of the machine travel

EXAMPLE A SCS that would control the machine direction function is a forward/neutral/reverse selection control.

3.7
steering
function which controls the lateral direction of machine travel

EXAMPLE A SCS that would control the steering function is a steering wheel or joystick.

3.8
swing/slew
function which controls the clockwise or anti-clockwise rotation of the upper structure of an excavator or digging linkage

EXAMPLE A SCS that would control the swing/slew function is a joystick.

3.9
machine abuse
activities that are outside the intended use of the machine and are beyond the reasonably foreseeable usage as communicated in the machine operation and service literature

EXAMPLE 1 Standing under a suspended load.

EXAMPLE 2 Using an earth-moving machine as an elevating work platform.

EXAMPLE 3 Intentionally driving machines in a way that would harm oneself or others.

EXAMPLE 4 Performing activities that are illegal.

Note 1 to entry: It is considered abuse to perform some maintenance tasks with the engine running or systems de-energized unless otherwise stated in the operator's manual.

3.10
roading
machines moving on a *road* (3.14)

Note 1 to entry: A suitably designed machine and road homologation can be required.

3.11
traveling
machine moving from one point on a worksite to another without going on a *road* (3.14)

EXAMPLE On a haul road, unimproved road or other thoroughfare on a site.

3.12
high wall
mine, quarry or other similar type wall associated with the worksite that a machine may be working near

Note 1 to entry: It is considered *machine abuse* (3.9) to operate machines near high walls without *berms* (3.13) in place.

3.13
berm
pile of dirt, rocks or other material intended to prevent a machine from passing into an area it is not intended to be operated in

Note 1 to entry: Some regions use different terms, e.g. bund, windrow.

3.14
road
public traffic area for use by automotive vehicles for travel or transportation

Note 1 to entry: Public traffic area does not include the sites of temporary road works (e.g. for repairs, maintenance, alteration, improvement, installation, or any other works to, above or under the road, including work to road equipment, lighting, barriers, walls etc) or roads not open to the public (e.g. on new housing and industrial developments), or on which public traffic is not permitted.

[SOURCE: ISO 17253:2014, 3.2]

3.15
work cycle
repeated process or task a machine performs within a use case

Note 1 to entry: Work cycles can be broken down into segments and steps (examples can be found in 5.4).

3.16
operator presence system
system fitted to a machine that detects if an operator is positioned in an operator station and automatically takes a control system action based on that determination

4 General

4.1 General principles

4.1.1 Safety requirements

The MPL_r provided in this document may be used as an alternative to performing an MCSSA for like machinery per ISO 19014-1 and were derived using that process. The functions, applications and use cases used to determine these levels are based on generic limits of machine application for the machine type. If the MPL_r in this document are used, the MPL_r shall be in accordance with Annexes A - AA after following the review outlined in 4.1.2, 4.2, 4.3, 4.4, 4.5, and 4.6.

Machinery shall comply with the safety requirements and/or protective/risk reduction measures of ISO 19014-1, ISO 19014-2, and ISO 19014-4. In addition, the machine shall be designed according to the principles of ISO 12100:2010 for relevant but not significant hazards which are not dealt with by this document.

4.1.2 Information for use

Limits of machine use, notable assumptions or examples of machine abuse considered in this document shall be communicated in the information for use according to ISO 19014-2:2019, Clause 8 and ISO 12100:2010, 6.4 and 6.4.5.

4.2 Mapping of functions to a SCS

The MCSSA supporting these MPL_r were carried out by function rather than system. In practice, there can be several SCS that could fail in a way that is described by the failure type listed for any particular function. All SCS on a machine shall be reviewed to determine if any failure could cause a hazardous outcome associated with a failure type of the functions listed. For example, a brake system may be mapped from a slow/stop or hold still function, as could another system that interferes with the ability of the machine to brake at an appropriate rate to meet the ISO 3450 stopping distance.

Measures beyond SCS may be applied to mitigate hazardous failures (e.g. mechanical lock outs, guards, administrative controls). In such a case, a MCSSA shall be completed to assess the MPL requirements of any residual risk associated with the SCS.

4.3 Applicability of the listed MPL_r to machines

This document does not eliminate the need to do a risk assessment per ISO 12100 as defined in ISO 19014-1.

The MCSSA supporting these MPL_r were carried out considering the limits of the machine type usage across the industry. Unique or limited applications or use cases can result in a different MPL_r for the machine function. If a machine is specifically designed or modified for an application other than what is considered in the tables in this document, an MCSSA shall be performed to determine if any functions require a different MPL_r.

While every effort was made to perform the supporting MCSSA in a general sense, there can be times where the assessment does not match a specific machine design; this is particularly relevant to the selection of the controllability factors (AC, AR, AW). The supporting MCSSA assume a common operator control layout around the operator station and no common cause failures. If there is a common cause failure between the SCS mapped to the function being assessed and the MCS or SCS being used for controllability, the MPL_r in the table is not applicable (e.g. two systems sharing a control element or a control unit). Likewise, where the control used to activate the avoidance on a particular design does not align with the AR score in the table, the table is not applicable (e.g. a brake is assumed to be on the floor immediately next to a throttle/propel pedal, if the brake is controlled with a lever the AR score would change from an AR3 to an AR2, a size difference within a machine type that results in a change in severity). In this case, the designer shall perform a MCSSA according to ISO 19014-1 to consider these

facts. If the remaining data used in the assessment are applicable to the machine being assessed, the data can be used in that MCSSA and the non-applicable score changed. It is the responsibility of the machine designer to review and assess whether the scoring used in the MCSSA are applicable to their machine.

4.4 Truncation

Due to the large number of combinations of inputs, the MCSSA supporting these tables are focused on scenarios that would clearly dominate the MPL_r (scenario that drives the highest MPL_r for the same function). Where a dominant scenario was not clearly identifiable, multiple scenarios were assessed to find the scenario(s) that led to highest MPL_r. Non-dominant scenarios were truncated from MCSSA. Part of the truncation process included equating scenarios to be the same, no worse, or less than scenarios already assessed; where this is the case, detail is not provided in the tables for the sake of legibility.

Only the scenarios that led to the highest MPL_r are included in the tables in the annexes unless a different failure type with a different hazardous outcome existed, in which case the scenarios with the highest MPL_r for all those failure types are included in the tables. Additional explanation in this space can be found in the function dominant failure type matrices. When more than one scenario of the same failure type led to the highest MPL_r, all such scenarios have been included.

4.5 Effects of different technologies on MCSSA

In most cases, the MPL_r in this document apply regardless of the technology used in the SCS; however, there are times when this is not the case, e.g. mechanical drivetrains versus electric or hydrostatic drivetrains.

When considering an alternative SCS technology (e.g. electric or hydrostatic), the assessments in the tables in this document shall be reviewed. Any assumptions or assessments that are invalidated by the introduction of a different technology shall be reassessed according to 4.3. Additionally, the functionality of these systems can cause MPL_r to be mapped to different SCS.

NOTE Not all machines were assumed to have mechanical drivetrains; dozers, excavators, skid steer loaders and rollers were assumed to have a hydrostatic drivetrain.

The following are some situations where technology differences can affect MPL_r:

— there are changes in response to machine speed, propel, brake or direction commands (e.g. compared to mechanical drivetrains, some electric and hydrostatic drivetrains apply functions differently);

— retarders may not have been considered a safety function on a mechanical drive system but can possibly be the primary means of slowing the machine in an electric drive machine;

— controllability assessments may be different due to common components and other common cause failure considerations;

— there are additional safety functions associated with new hazards created by using a different energy type;

— engine speed can become decoupled from other systems (e.g. no longer has a direct effect on machine speed);

— there are changes in SCS performance due to system stored energy level (e.g. output performance varying due to battery charge).

4.6 Supporting diagrams and data for the tables of machine performance levels

Scenarios that dominated the MPL_r score in the MCSSA are listed in the tables and a brief explanation are contained in the annexes. Where more detail is deemed necessary additional diagrams and information are provided in Clause 5.

5 Additional MCSSA scenario information

5.1 Traffic rate on road

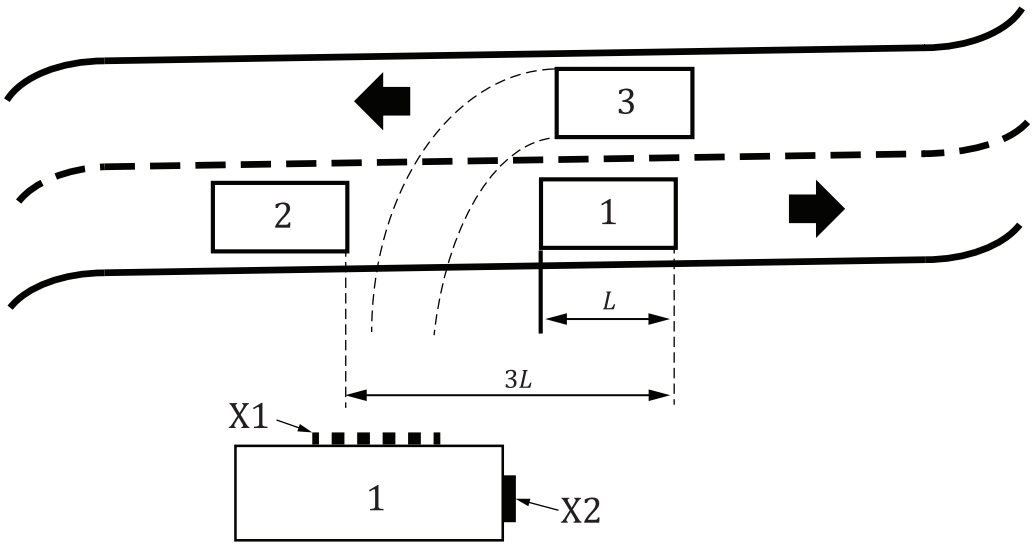
After reviewing the scenarios that earth-moving machines are used in, it was determined that the highest P value was bystanders in other vehicles when roading. The exposure of bystanders to an uncommanded steering event is largely dictated by the distance between vehicles. Machines cannot be designed to mitigate situations where illegal or unsafe actions are committed by other road users. The MCSSA considered traffic rates with 2 car lengths distance between cars as the norm (less distance between cars being commonly considered unsafe across the world).

While traffic can momentarily exceed this rate, the P value needs to account for the machine lifecycle. Traffic rates with less spacing would not occur continually over the entire machine lifecycle; this makes the traffic rate of 1 car every 3 car lengths conservative (see Figure 1).

NOTE This document refers to cars, light vehicles, and vehicles. Car is typically used in the context of a roading use case. Light vehicles is typically used in mining applications and weigh less than 3 500 kg. Vehicles is used generically.

5.2 Steering while roading

All failure types for steering create the same hazard, depending on whether the desired path is straight or curved (i.e. uncommanded steering on a straight road has the same hazardous outcome as failure to steer on a curved road) – the machine will leave the intended travel lane.



Key

1 vehicle 1
2 vehicle 2
3 machine
X1 zone 1
X2 zone 2
L length

Figure 1 — Steering hazard zone for on road travel

Earth-moving machines can cause an S3 injury if there is contact between the machine and a vehicle. The proportion of the vehicle that results in an S3 injury is quantified below.

— The passenger cabin of the vehicle (i.e. machine contacts the side of the vehicle); this equates to approximately ½ the car length (see dotted line on vehicle in Figure 1, X1).

— The front of the vehicle (i.e. the vehicle drove straight into the side of machine due to the machine steering in front of the vehicle); this equates to approximately ½ the width of the vehicle (see solid line on vehicle in Figure 1, X2). Contact on the corners of the vehicle would be less likely to cause an S3 Injury.

— The ratio of length to width varies by vehicle; however, an estimation of an average ratio of 1:3,5 has been used.

When roading there is a risk of contacting a vehicle, a bystander or an object on the other side of the machine; this is less than the traffic rate. A P variable of 10 % has been used.

Based on these limiting factors the H and P variables for machines roading can be shown to be no higher than:

$$H_R P_R + H_L P_L = H_R P_R + H_L \left(T_R \left(\frac{L}{2} + \frac{W}{2} \right) \right) = (50\ \% \times 10\ \%) + \left(50\ \% \left(\frac{1}{3} \left(\frac{1}{2} + \frac{1}{7} \right) \right) \right) = 16\ \%$$

where

L = 1 car length;

H_R = H variable for right hand uncommanded steering = 50 % (if the machine steers without command, half the failures would steer the machine to the left, the other half to the right);

P_R = P variable for the right-hand uncommanded steering = 10 %;

H_L = H variable for left hand uncommanded steering = 50 %;

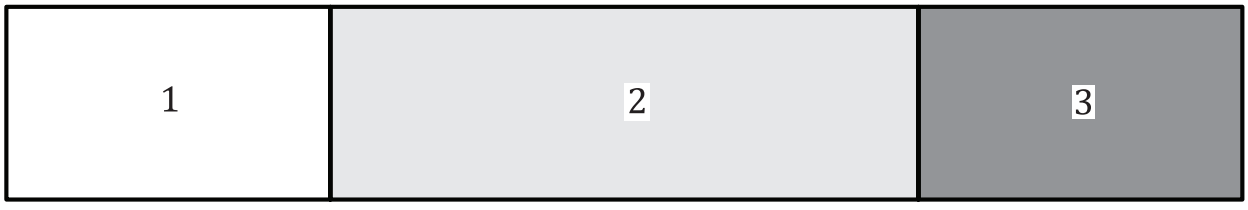
P_L = P variable for the left-hand uncommanded steering;

T_R = traffic rate per 5,1 = 1/3;

W = L/3,5.

5.3 Slow/stop and machine speed

The hazard zone for a brake failure is the area beyond the machine's normal stopping distance. An uncommanded increase in machine speed has a similar hazard zone (see Figure 2).



Key

1 machine
2 intended stopping distance
3 increased stopping distance

Figure 2 — Slow/stop and machine speed hazard zone

5.4 Work cycles

This section contains descriptions of common work cycles for the various machine types used in the MCSSA evaluations to determine MPL_r.

The values used in the percentage breakdown in Tables 1 through 6 represent the worst credible scenario for the failure type being assessed as determined in the MCSSA.

Figures 3 through 6 represent work cycles as considered in the MCSSA.

5.4.1 Dumpers

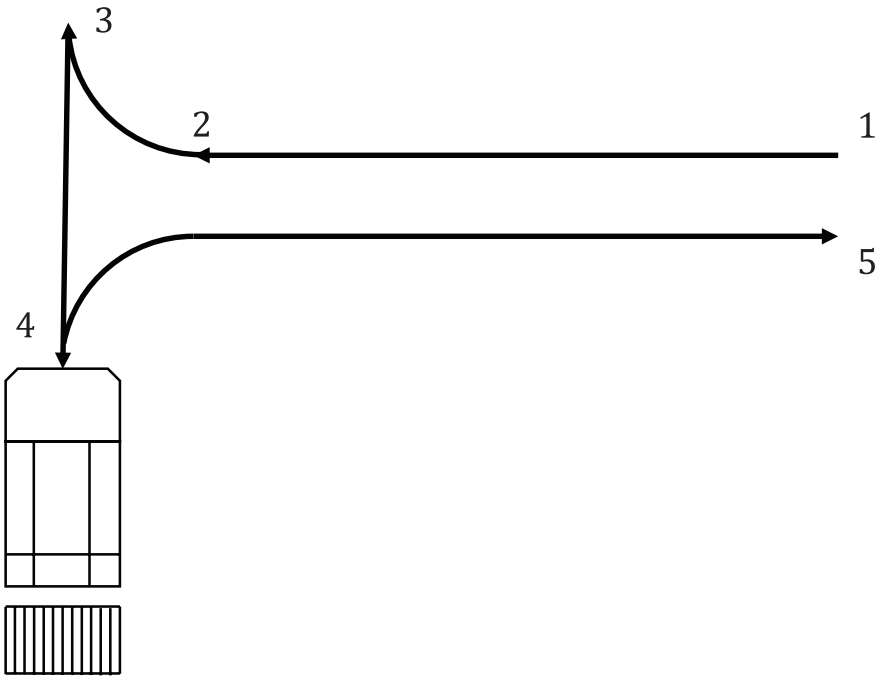


Figure 3 — Truck unloading and queuing cycle

Table 1 — Truck unloading and queuing cycle

Unloading and queuing – long cycle – see Figure 3	
1 – 2 (slow forward speed, high traffic)	50 %
2 – 3 (slow forward speed, low traffic)	8 %
3 – 4 (slow reverse speed, low traffic)	17 %
Dump	17 %
4 – 5 (medium forward speed, high traffic)	8 %

5.4.2 Excavators

Table 2 — Excavator object handling work cycle

Object handling cycle		
Step	Time [s]	% cycle
① lower/lash	45	21,3 %
② lift	30	14,2 %
③ swing	15	7,1 %
④ lower	60	28,4 %

Table 2 *(continued)*

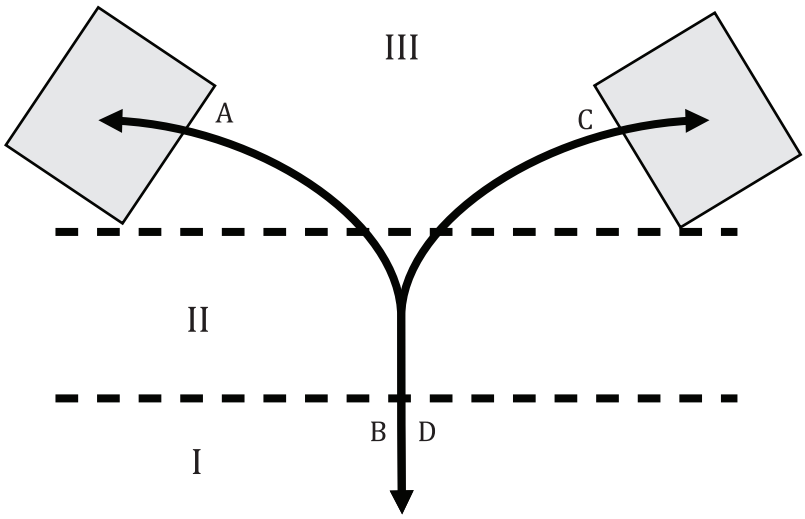
Object handling cycle		
Step	Time [s]	% cycle
⑤ unlash	45	21,3 %
⑥ lift	4	1,9 %
⑦ swing	2	0,9 %
⑧ travel	10	4,7 %
total cycle time	211	100,0 %

Table 3 — Excavator trenching work cycle

Trenching use case	
dig (includes some lift)	35 %
swing CCW	25 %
dump	10 %
swing CW	25 %
travel	5 %

5.4.3 Wheel loaders

5.4.3.1 Wheel loader bucket work



Key

A loading
C unloading
B/D travel during cycle
I zone with offsite traffic P = 50 %
II zone with site traffic P = 20 %
III zone where it is considered machine abuse, between machine and destination P = 0 %

Figure 4 — Wheel loader bucket work cycle

Table 4 — Wheel loader bucket work cycle

Wheel loader bucket work cycle – see Figure 4	
Segments A, C	30 %
Segments B, D	20 %

5.4.3.2 Wheel loader loading/unloading and lifting

Key

A unloading
C loading
B/D travel during cycle
I zone with more pedestrian traffic, less vehicular traffic P = 20 %
II zone with more vehicular traffic, less pedestrian traffic P = 20 %

Figure 5 — Wheel loader work lifting and loading/unloading cycle

Table 5 — Wheel loader lifting and loading/unloading cycle

Lifting and loading/unloading use case – see Figure 5	
A1	6,25 %
A2	6,25 %
A3	6,25 %
A-Positioning	6,25 %
B	25 %
C1	6,25 %
C2	6,25 %
C3	6,25 %
C-Positioning	6,25 %
D	25 %

5.4.4 Skid steer loaders

Lifting, material handling, low to the ground and bucket work cycles look similar to the wheel loaders, however, instead of doing a 3-point turn, the machine rotates by counter steer.

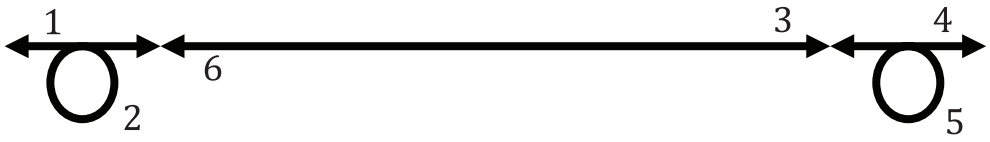


Figure 6 — Skid steer loader lifting, loading/unloading, low to ground cycle diagram

Table 6 — Skid steer loader lifting, loading/unloading, low to ground cycle

Lifting, loading/unloading, low to ground use case	
1	1 %
2	1 %
3	48 %
4	1 %
5	1 %
6	48 %

5.5 Swing/slew of backhoe loaders and excavators

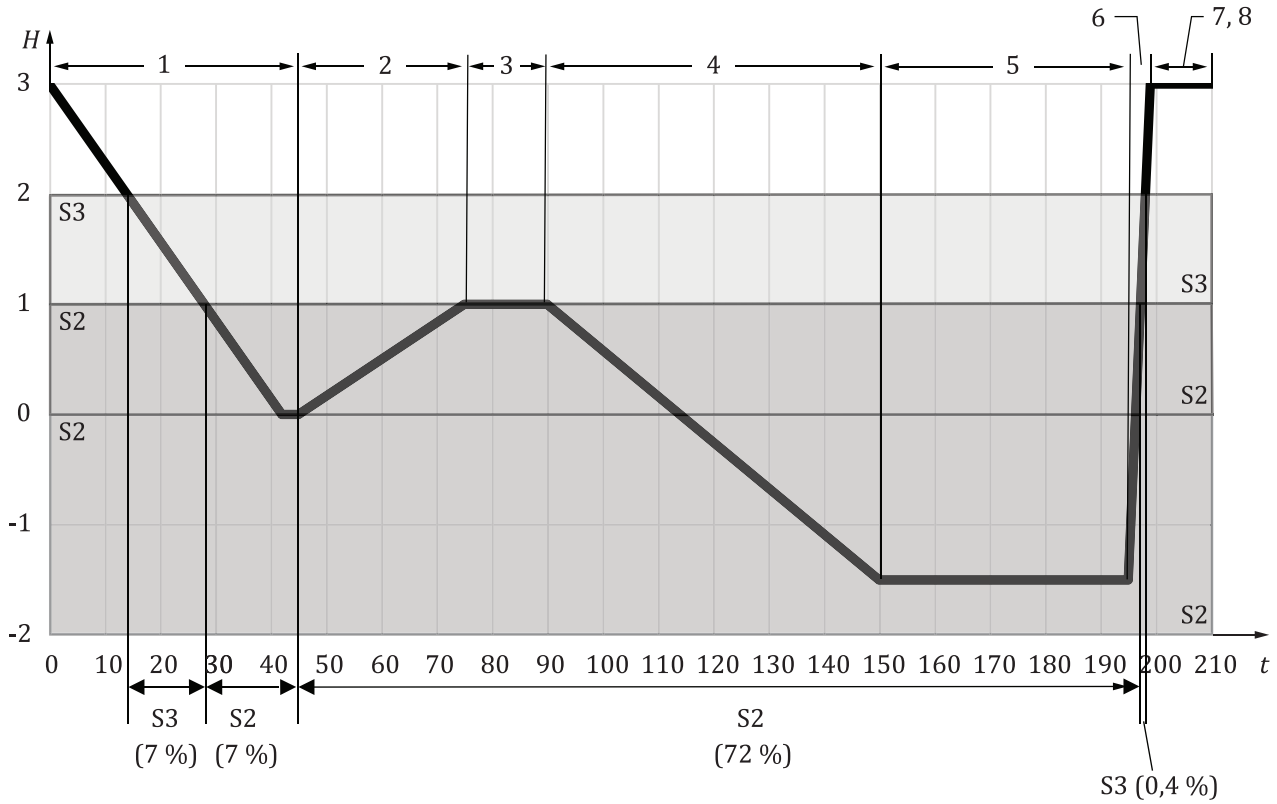
5.5.1 H variable for working beside traffic or co-workers

An excavator swing radius is a hazard zone and it is not intended for people, objects or traffic to be within the hazard zone. These MCSSA assume sufficient worksite hazard mitigations are in place (such as barriers and worksite rules).

Contact with an excavator tool during swing has three-dimensional zones in which the severity differs. Between the ground and 1 m from the ground, the worst credible injury is an S2. Between 1 m – 2 m from the ground, the worst credible injury is an S3. When the tool is within a trench, it is machine abuse to stand between the arm and the trench wall, however, a limb may momentarily be in this area and has been considered an S2. When the tool is on the ground or 2 m above, it is not considered a hazard.

When the motion of the lowest point of the tool is plotted over the object handling work cycle it can be determined which portions of the work cycle fall within the S2 and S3 zones. Both zones were analysed with the dominant score being shown in the scenarios contained in the tables in Annexes D, E, and F.

A representation of this is shown in Figure 7 and Table 2.



Key

t time in seconds

H height in meters

S2 zones in which an S2 severity could occur (0 m - 1 m above the ground or in the trench)

S3 zone in which an S3 severity could occur (1 m - 2 m above the ground)

Figure 7 — Different severity score zones of the swing cycle (see cycle in Table 2)

The result is the following H variables:

— H_{S2} = 79 %,

— H_{S3} = 7 %.

5.5.2 P values for swinging into traffic or co-workers

The assumption of one vehicle every three vehicle lengths remains from 5.2. The proportion of the vehicle length that could result in an S3 injury is assumed to be ½ the vehicle length (combination of surfaces along the length and width of the vehicle where a person may be contacted by the machine tool – which is narrow compared to the exposed area) P = 1/2 × 1/3 = 1/6.

A P value of 5 % has been added to one or both sides of machines to account for co-workers who momentarily pass into the swing radius of the machine to perform tasks that are necessary for the cycle (e.g. to check trench depth or attach / release a pipe from a chain). These co-workers are aware of hazard of swinging machines and would avoid being in the swing radius whenever possible. These values are then averaged across both sides of the machine because the machine can only swing in one direction at a time.

Where there is a co-worker on both sides of the machine P = [(1/6 + 5 %) +5 %]/2 = 14 %.

Where there only is a co-worker on one side of the machine P = (1/6 + 5 %)/2 = 11 %.

5.6 Maximum foreseeable P variables for typical areas on a site

Mine haul road – other machines: P = 10 %

Mine haul road – light vehicles and pedestrians: P = 5 %

Busy construction sites: P = 20 – 50 % depending on the task, applications and machine type

Scenarios where people should not be, however specific scenarios may rarely, however legitimately, require someone to be: P = 1 - 5 %

Scenarios where it is considered machine abuse, however it is foreseeable that there may be momentary incidental exposure: P = 1 – 2 %

Site park up area (e.g. area where shift changes, breaks, maintainers and activities that may cause machines to converge on at certain times): P = 25 – 50 % depending on machine type and applications

5.7 Seat belts

Earth-moving machines with seated operators are fitted with operator restraint systems—seat belts—and all MCSSA for such machines in this document were assumed that the operator was properly restrained. It is considered machine abuse to operate a machine fitted with a seat belt without wearing it.

5.8 Maintenance tasks

Only machine maintenance tasks that require or are reasonably foreseeable to be done with the engine running are considered in these assessments. The proportion of maintenance time is calculated based on the length of time the task takes and the frequency of those tasks. The H variable is calculated from the proportion of the time the maintainer would be exposed to the hazard while performing those tasks.

Depending on the size of the machine, maintenance tasks typically involve (70 – 75) % of the tasks on machine, with the rest of the time changing tools, performing job hazard analysis and other tasks. The P variables used reflect this.

5.9 Backhoe arm out and wheeled excavator or backhoe stabilizer down while travelling or roading

When travelling or roading, if a wheeled excavator or backhoe (centre mount only) stabilizer lowers without command, the stabilizer protrudes into the space beside the existing machine envelope. A similar situation occurs when a backhoe (side shift only) arm moves out without command; however, the arc of motion is up and out rather than down and out (see Figure 8). If traffic or pedestrians are in these spaces, they could be contacted by the machine.

It is not reasonable for people or traffic to be close to a moving machine (approximately 1 m). However, at the outer most portions of the range of motion, it is possible that people or traffic are present, such that they could be contacted.

For stabilizers and arm, the portion of the motion where someone could be present is approximately 20 %. For stabilizers, a P variable of 16 % (see 5.2) for traffic has been used per 5.1. For arm, a P variable of 10 % is used (lower because of the height of the motion at this stage would only contact high vehicles) (see Figure 8).

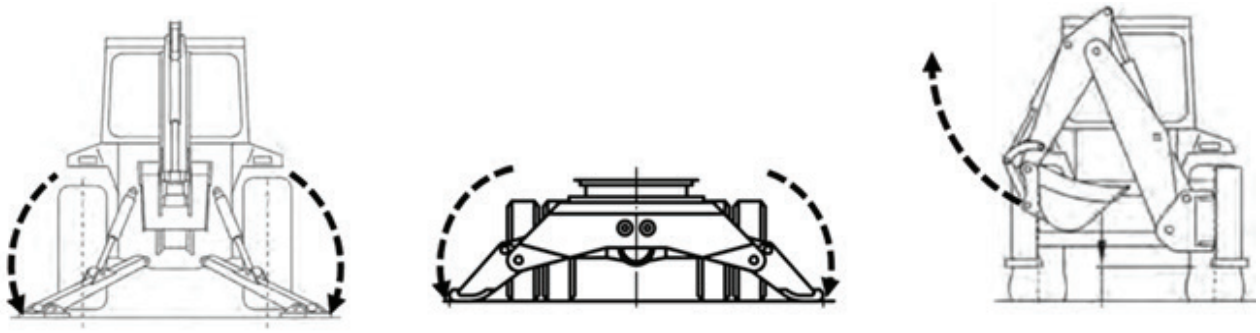


Figure 8 — Wheeled excavator, backhoe stabilizer down and backhoe arm out during travel H diagram

Annex A
(normative)

Rigid frame dump trucks performance level tables

A.1 Rigid frame dump trucks

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables A.1 to A.5) or in Clause 5.

Table A.1 — MPL_r table for rigid frame dump truck

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
RD1	**body up**	traveling	uncommanded activation	machine rolls due to body being stuck in the up position	operator	S1	80 %	100 %	100 %	E2	AC1	AW1	AR3	C2	**b**
RD2		traveling	uncommanded activation	collision with rolled machine	bystander	S2	80 %	50 %	5 %	E1	AC1	AW1	AR3	C2	
RD3	**body down**	traveling	failure to apply on demand	machine rolls due to body being stuck in the up position	operator	S1	80 %	50 %	100 %	E2	AC1	AW2	AR3	C1	**a**
RD4		traveling	failure to apply on demand	collision with rolled machine	bystander	S2	80 %	25 %	5 %	E1	AC1	AW2	AR3	C1	
RD5	**neutralize**	unloading and queuing	uncommanded deactivation	machine moves into machine in front / behind or over high wall / steep slope	operator	S3	20 %	9 %	100 %	E1	AC1	AW2	AR3	C1	**b**
RD6	**machine speed**	traveling	uncommanded activation	runaway machine - machine goes off high wall	operator	S3	90 %	55 %	100 %	E2	AC1	AW3	AR3	C0	**b**
BAD2	**machine direction**	considered to be the same unloading and queuing for articulated-frame dumpers greater than 22 000 kg													**c**

[a] For pressure vessel discharge and isolation systems, uncommanded activation of the systems has the same MPL_r as the system they are controlling.

[b] For a steering hydraulic system that automatically discharges stored energy when the machine is powered off, the controllability for failure on demand would be AC0 due to the hazard of someone moving the steering when they think the system is discharged. In this case the MPL_r would be c.

Table A.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
RD7	**slow/stop**	traveling	failure to apply on demand	runaway machine - machine goes off high wall or a collision	operator	S3	90 %	28 %	100 %	E2	AC1	AW2	AR2	C2	**d**
RD8		traveling	uncommanded activation	machine goes into uncontrollable skid - goes off high wall or head to tail collision	operator	S3	90 %	4 %	100 %	E1	AC1	AW2	AR2	C2	**c**
RD9	**hold still**	slow speed maneuvering	failure to apply on demand	machine rolls away - collision with light vehicle or pedestrian - operator out of cab	bystander	S3	20 %	10 %	25 %	E0	AC0	N/A	N/A	C3	**c**
RD10		maintenance	failure to apply on demand	maintainer run over	maintainer	S3	7 %	13 %	100 %	E0	AC0	N/A	N/A	C3	
RD11	**steering**	traveling	uncommanded activation	machine steers off high wall	operator	S3	90 %	90 %	100 %	E2	AC1	AW2	AR2	C2	**d**
RD12		traveling	uncommanded activation	collision with light vehicle or pedestrian	bystander	S3	90 %	100 %	5 %	E1	AC1	AW2	AR0	C3	
RD13	**powered access**	slow speed maneuvering	uncommanded activation	access system lowers onto person	bystander	S2	20 %	100 %	25 %	E1	AC1	AW0	AR1	C3	**c**

[a] For pressure vessel discharge and isolation systems, uncommanded activation of the systems has the same MPL_r as the system they are controlling.

[b] For a steering hydraulic system that automatically discharges stored energy when the machine is powered off, the controllability for failure on demand would be AC0 due to the hazard of someone moving the steering when they think the system is discharged. In this case the MPL_r would be c.

Table A.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
RD14	**pressure vessel discharge** [a]	maintenance	failure to apply on demand	oil injection from discharged oil	maintainer	S3	7 %	10 %	75 %	E0	AC1[b]	AW3	AR1	C2	**b**
RD15	**isolation system**	maintenance	failure to apply on demand	electrocution from electric drive system, oil injection from hydraulic system	maintainer	S3	7 %	10 %	75 %	E0	AC0	N/A	N/A	C3	**c**

[a] For pressure vessel discharge and isolation systems, uncommanded activation of the systems has the same MPL_r as the system they are controlling.

[b] For a steering hydraulic system that automatically discharges stored energy when the machine is powered off, the controllability for failure on demand would be AC0 due to the hazard of someone moving the steering when they think the system is discharged. In this case the MPL_r would be c.

A.2 Supporting explanation

A.2.1 Supporting explanations for dominant scenarios

RD1 – body up

H: Hazard exists for the entire cycle. H = 100 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – Remove foot from throttle to reduce raise rate, brake to stop moving

AW: AW1 – Only if looking in mirror or body down indicator (if fitted)

AR: AR3 – Removing foot from throttle is a natural reaction

RD2 – body up

H: Hazard only exists if machine rolls in one direction – 50 % of hazards are dangerous. H = 50 %

P: Light vehicle on haul road traffic rate. P = 5 %

AC: AC1 – Remove foot from throttle to reduce raise rate, brake to stop moving

AW: AW1 – Only if looking in mirror or body down indicator (if fitted)

AR: AR3 – Removing foot from throttle is a natural reaction

RD3 – body down

H: Worst case when downhill hauling – 50 % of hazards are dangerous. H = 50 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – brakes

AW: AW2 – Operator should be watching body lower and machine feel will be different

AR: AR3 – Operator can choose not to start moving

RD4 – body down

H: Worst case when downhill hauling (50 %), hazard only exists if machine rolls in one direction (50 %). H = 50 % × 50 % = 25 %

P: Light vehicle traffic rate. P = 5 %

AC: AC1 – Remove foot from throttle to reduce raise rate, brake to stop moving

AW: AW2 – Operator should be watching body lower and machine feel will be different

AR: AR3 – Operator can choose not to start moving

RD5 – neutralize

H: Only hazardous when dumping (queue would be at low idle and operator would have brake applied) see Table 1 and Figure 3 (17 %). 50 % failures are hazardous – moves into reverse only. H = 50 % × 17 % = 9 %

P: Operator always in cab for this use case. P = 100 %

AC: AC1 – Operator should have foot on brake or have park brake applied

AW: AW2 – Operator should be watching body lower and machine feel will be different

AR: AR3 – Operator should have foot on brake or have park brake applied

RD6 – machine speed

H: When going downhill (45 %) or trying to stop (10 %). H = 45 % + 10 % = 55 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – brakes

AW: AW3 – Not immediately hazardous – hazard increases in time

AR: AR3 – Applying brakes is a natural reaction and applying brake during the operation is considered underfoot

RD7 – slow/stop

H: When going downhill (45 %) on a curve (40 %) or trying to stop (10 %) ((45 % × 40 %) + 10 % stopping). H = 28 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – park brakes

AW: AW2

AR: AR2 – Applying park brake required (by moving their hand)

RD8 – slow/stop

H: Hazardous when on curve (40 %), downhill (45 %), high wall present (90 %), conditions conducive to a skid (25 %). H = 40 % × 45 % × 90 % × 25 % = 4 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – berm

AW: AW2

AR: AR2 – Berms are not always effective

RD9 – hold still

H: Amount of time machine could be left unattended not in V ditch or specifically designed parking area designed to prevent roll away (10 %). H = 10 %

P: Typical bystander rate in central / parking areas. P = 25 %

AC: AC0

RD10 – hold still

H: 10 % of refuel (58,6 %), 20 % of daily walk around (19,5 %), 10 % of window wash (only when on the ground - lesser severity on platform) (9,8 %), 0 % of brake test (4,9 %), 100 % troubleshooting (1 %), 25 % of camera wash (some lower severity) (4,9 %), 10 % of tyre inspection (1,4 %). H = (10 % × 58,6 %) + (20 % × 19,5 %) + (10 % × 9,8 %) + (0 % × 4,9 %) + (100 % × 1 %) + (25 % × 4,9 %) + (10 % × 1,4 %) = 13 %

P: Maintainer can be dedicated to these tasks for fleet of machines, P is considered H calculation. P = 100 %

AC: AC0

RD11 – steering

H: Hazardous when high wall present (90 %). H = 90 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – berm

AW: AW2

AR: AR2 – Berms are not always effective

RD12 – steering

H: Hazard exists during the whole cycle. H = 100 %

P: Typical haul road light vehicle rate. P = 5 %

AC: AC1 – brakes

AW: AW2

AR: AR0

RD13 – powered access system

H: Hazard exists during the whole cycle. H = 100 %

P: Typical bystander rate in central / parking areas. P = 25 %

AC: AC1 – brakes (stop machine before it hits someone)

AW: AW0

AR: AR1

RD14 – pressure vessel discharge

H: Only maintenance tasks within the system that could be charged. H = 10 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC1 – It is considered machine abuse to perform tasks where pressure could be released from a pressurized system without first checking to ensure that the energy is discharged.

AW: AW3 – Checks are performed before work commences and the hazard presents itself.

AR: AR1 – Maintainer required to move hands and feet to perform this task.

RD15 – isolation system

H: Only maintenance tasks within the system that could be charged. H = 10 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

A.2.2 Application use cases

Table A.2 — Application use case table

Application	Traveling	Loading and queuing	Unloading and queuing	Slow speed maneuvering	Maintenance
Less than 100 000 kg rigid trucks	80 %	40 %	20 %	30 %	7 %

Table A.2 *(continued)*

Application	Traveling	Loading and queuing	Unloading and queuing	Slow speed maneuvering	Maintenance
Greater than or equal to 100 000 kg payload large trucks	90 %	40 %	20 %	20 %	7 %

A.2.3 Maintenance task breakdown

Table A.3 — Maintenance task breakdown

	Time (min/day)	% Maintenance time
refuel	60	59
walk around, oil check	20	20
wash mirror and windows	10	10
brake test	5	5
troubleshooting		1
clean camera	5	5
tire maintenance	1,4	1

A.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table A.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
machine speed			1		Failure to release on demand is considered the same as uncommanded activation. Other failure types are less severe.
machine direction	1				Failure to apply is treated as a failure to change direction or changing into wrong direction. An uncommanded direction change is considered the same as uncommanded park brake.
transmission neutralize				1	Shifting out of N without command
machine start			1		Uncommanded shutdown is considered the same as uncommanded hold still or stop or N depending on machine design. Uncommanded activation is only dangerous when in maintenance and the machine is keyed on.
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

Table A.4 *(continued)*

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
body up			1		Other failure types are less or not hazardous.
body down	1		1		Failure to lower the body is less dangerous than the body lowering without command, but is still assessed.
ejector out			1		Other failure types not hazardous
ejector in					Only dangerous when in maintenance and machine is running, however it is machine abuse to be behind ejector plate when the machine is running.
slow/stop	1		1		Other failure types have the same outcome as what is being analyzed.
hold still	1				Failure to apply on demand considered the same as uncommanded release. Uncommanded activation considered the same as uncommanded slow/stop.
pressure vessel discharge	1				Uncommanded discharge is covered under system integrity of the system the pressure vessel is installed in.
steering			1		Failure to apply on demand is considered the same as uncommanded activation.
isolation system	1				Uncommanded activation is the same as uncommanded slow/stop. Uncommanded release is the same as failure to apply on demand.
powered access			1		Other failure types are less or not hazardous.

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

A.2.5 Notes and assumptions

— Due to sites with machines this size typically having controlled access, the following assumptions were made:

  — co-workers were people in other similar sized machines,

  — bystanders were co-workers in light vehicles and pedestrians.

— This assessment only considers trucks used as dump trucks and derivatives to the extent that they have common usage and features to the dump trucks considered in the MCSSA.

— Some data suggested that loading/queuing and unloading/queuing values could be higher than those used in this analysis, however it was determined that this was highly inefficient and would not be a sustainable business practice in the long term and would thus not be an accurate representation of machine usage.

— Consistent scoring guidelines:

  — S1 collision with another similar size or larger machine except for rear end collisions between 2 trucks of similar size (operator and co-worker),

  — S3 rear end collision between 2 trucks of similar size - rigid trucks only (operator and co-worker),

  — S3 machine off high wall (operator),

— S3 machine versus pedestrian or light vehicle (bystander),

— S1 rear end collision between 2 trucks of similar size - articulated trucks only (operator and co-worker),

— S1 roll over (operator).

A.3 MPL_r mapped to SCS table

Table A.5 shows function-based MPL_r (see Table A.1) mapped to SCS per the results of the MCSSA for a rigid frame dump truck. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table A.1 would also be mapped to these MPL_r.

Table A.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
body up	uncommanded activation	**b**	hoist raise
	failure to release on demand		
body down	failure to apply on demand	**a**	hoist lower
neutralize	uncommanded deactivation	**b**	gear direction control
machine speed	uncommanded activation	**b**	throttle and speed gear control
machine direction	failure to apply on demand	**c**	gear direction control
slow down / stop	failure to apply on demand	**d**	service brakes
	uncommanded activation	**c**	
hold still	failure to apply on demand	**c**	parking brakes
steering	uncommanded activation	**d**	steering
powered access	uncommanded activation	**c**	powered access ladder
pressure vessel discharge [a]	failure to apply on demand	**b**	accumulator charge system
isolation system	failure to apply on demand	**c**	machine lockout system

[a] For pressure vessel discharge and isolation systems, uncommanded activation of the systems has the same MPL_r as the system they are controlling.

Annex B
(normative)

Articulated-frame dumpers equal to or greater than 22 000 kg performance level tables

B.1 Articulated-frame dumpers equal to or greater than 22 000 kg

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables B.1 to B.4) or in Clause 5.

Table B.1 — MPL_r table for articulated-frame dumpers equal to or greater than 22 000 kg

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
LAD1	**body up**	considered to be the same articulated-frame dumpers less than 22 000 kg													**b**
LAD2	**body down**	considered to be the same articulated-frame dumpers less than 22 000 kg													**a**
BAD1	**ejector out**	traveling	uncommanded activation	hit ejected material - could tip	co-worker	S1	80 %	50 %	10 %	E1	AC0	N/A	N/A	C3	**b**
RD5	**neutralize**	considered to be the same rigid dump trucks													**b**
LAD3		considered to be the same articulated-frame dumpers less than 22 000 kg													
RD6	**machine speed**	considered to be the same rigid dump trucks													**b**
BAD2	**machine direction**	unloading and queuing	failure to apply on demand	machine reverses over high wall or steep slope	operator	S3	40 %	2 %	100 %	E0	AC1	AW2	AR0	C3	**c**
BAD3	**slow/stop**	traveling	failure to apply on demand	runaway machine - machine goes off high wall. [a]	operator	S3	80 %	6 %	100 %	E1	AC1	AW2	AR2	C2	**c**
BAD4		traveling	uncommanded activation	uncontrollable skid - machine collision with light vehicle	bystander	S3	80 %	2 %	5 %	E0	AC0	N/A	N/A	C3	**c**
RD10	**hold still**	considered to be the same rigid dump trucks													**c**
LAD8-9		considered to be the same articulated-frame dumpers less than 22 000 kg													
BAD5	**steering**	traveling	uncommanded activation	machine steers off high wall	operator	S3	80 %	30 %	100 %	E2	AC1	AW2	AR2	C2	**d**
BAD6		traveling	uncommanded activation	collision with light vehicle or pedestrian	bystander	S3	80 %	100 %	5 %	E1	AC1	AW2	AR0	C3	

[a] The severity of head to tail collision for articulated trucks is lower than rigid frame trucks due to geometry.

B.2 Supporting explanation

B.2.1 Supporting explanations for dominant scenarios

BAD1 – ejector out

H: Only hazardous while loaded. H = 50 %

P: Typical haul road machine rate. P = 10 %

AC: AC0

BAD2 – machine direction

H: Only hazardous at the precise moment when the operator goes to drive away from the dump point. H = 2 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – brakes

AW: AW2

AR: AR0

BAD3 – slow/stop

H: Only hazardous when going downhill (15 %) and on a curve (40 %). H = 6 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – park brake

AW: AW2

AR: AR2

BAD4 – slow/stop

H: Only hazardous when on curve (40 %), going downhill (15 %), 25 % conditions conducive to a skid (25 % - high wall and downhill reduced to 1/3rd of large rigid trucks). H = (40 % × 15 % × 25 %) = 2 %

P: Light vehicle on haul road traffic rate. P = 5 %

AC: AC0

BAD5 – steering

H: Only hazardous when high wall is present. H = 30 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – park brake

AW: AW2

AR: AR2

BAD6 – steering

H: Hazard exists for the whole cycle. H = 100 %

P: Light vehicle on haul road traffic rate. P = 5 %

AC: AC1 – brake

AW: AW2

AR: AR2

B.2.2 Application use cases

Table B.2 — Application use case table

Application	Traveling	Loading and queuing	Unloading and queuing	Slow speed maneuvering	Maintenance
22 000 kg and greater payload articulated-frame dumpers	80 %	30 %	40 %	30 %	5 %

B.2.3 Maintenance task breakdown

Table B.3 — Maintenance task breakdown

	Time (min/day)	%Maintenance time
refuel	10	17
walk around, grease and oil check	20	33
wash machine	5	8
wash mirror and windows	10	17
brake test	5	8
troubleshooting		1
install body-lock pins	1,7	3
install articulation lock	1,7	3
clean camera	5	8
tire maintenance	1,7	3

B.2.4 Function dominant failure type matrix

See Table A.4.

B.2.5 Notes and assumptions

See A.2.5.

B.3 MPL_r mapped to SCS table

Table B.4 shows function-based MPL_r (see Table B.1) mapped to SCS per the results of the MCSSA for a 22 000 kg and greater payload articulated-frame dumper. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in B.1 would also be mapped to these MPL_r.

Table B.4 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
body up	uncommanded activation	**b**	hoist raise
body down	failure to apply on demand	**a**	hoist lower
ejector out	uncommanded activation	**b**	ejector
neutralize	uncommanded deactivation	**b**	gear direction control

Table B.4 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
machine speed	uncommanded activation	**b**	throttle and speed gear control
machine direction	failure to apply on demand	**c**	gear direction control
slow down / stop	failure to apply on demand	**c**	service brakes
	uncommanded activation	**c**	
hold still	failure to apply on demand	**c**	parking brakes
steering	uncommanded activation	**d**	steering

Annex C
(normative)

Articulated-frame dumpers equal to or less than 22 000 kg performance level tables

C.1 Articulated-frame dumpers less than 22 000 kg

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables C.1 to C.3) or in Clause 5.

Table C.1 — MPL_r table for articulated-frame dumpers less than 22 000 kg

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
LAD1	**body up**	roading	uncommanded activation	machine rolls due to body being stuck in the up position	operator	S1	80 %	100 %	100 %	E2	AC1	AW1	AR3	C2	**b**
LAD2	**body down**	roading	failure to apply on demand	machine rolls due to body being stuck in the up position	operator	S1	80 %	50 %	100 %	E2	AC1	AW2	AR3	C1	**a**
RD5	**neutralize**	considered to be the same rigid dump trucks													**b**
LAD3		slow speed maneuvering	uncommanded deactivation	collision with light vehicle or pedestrian due to unexpected machine movement	bystander	S3	30 %	20 %	25 %	E1	AC1	AW2	AR3	C1	
LAD4	**machine speed**	roading	uncommanded activation	runaway machine - machine collision with light vehicle	bystander	S1	80 %	55 %	5 %	E1	AC1	AW3	AR3	C0	**a**
LAD5	**machine direction**	slow speed maneuvering	failure to apply on demand	collision with light vehicle or pedestrian	bystander	S3	30 %	10 %	25 %	E0	AC1	AW2	AR3	C1	**a**
LAD6	**slow/stop**	roading	failure to apply on demand	runaway machine - run over bystander. [a]	bystander	S3	80 %	1 %	100 %	E0	AC1	AW2	AR2	C2	**b**
LAD7		roading	uncommanded activation	uncontrollable skid - machine collision with light vehicle	bystander	S3	80 %	2 %	5 %	E0	AC0	N/A	N/A	C3	**c**

[a] Rear end collision with light vehicle is considered less severe than larger machines.

Table C.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
RD10		considered to be the same rigid dump trucks													
LAD8	**hold still**	slow speed maneuvering	failure to apply on demand	machine rolls away - collision with light vehicle or pedestrian - operator out of cab	bystander	S3	30 %	10 %	10 %	E0	AC0	N/A	N/A	C3	**c**
LAD9		maintenance	failure to apply on demand	maintainer run over	maintainer	S3	5 %	15 %	7 %	E0	AC0	N/A	N/A	C3	
LAD10	**steering**	roading	uncommanded activation	collision with light vehicle, pedestrian	bystander	S3	80 %	10 %	16 %	E1	AC1	AW2	AR0	C3	**d**

[a] Rear end collision with light vehicle is considered less severe than larger machines.

C.2 Supporting explanation

C.2.1 Supporting explanations for dominant scenarios

LAD1 – body up

H: Hazard exists for the entire cycle. H = 100 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – Remove foot from throttle to reduce raise rate, brake to stop moving

AW: AW1 – Only if looking in mirror or body down indicator (if fitted)

AR: AR3 – Removing foot from throttle is a natural reaction

LAD2 – body down

H: Worst case when downhill hauling – 50 % of hazards are dangerous. H = 50 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – brakes

AW: AW2 – Operator should be watching body lower and machine feel will be different

AR: AR3 – Operator can choose not to start moving

LAD3 – neutralize

H: Time when machine is idle while waiting. H = 20 %

P: Typical bystander rate in central/parking areas. P = 25 %

AC: AC1 – brakes

AW: AW2 – Operator should be watching body lower and machine feel will be different

AR: AR3 – Operator can brake as soon as movement is felt

LAD4 – machine speed

H: When going downhill (45 %) or trying to stop (10 %). H = 45 % + 10 % = 55 %

P: Light vehicle on haul road traffic rate. P = 5 %

AC: AC1 – brakes

AW: AW3 – Not immediately hazardous – hazard increases in time

AR: AR3 – Applying brakes is a natural reaction and applying brake during the operation is considered underfoot

LAD5 – machine direction

H: Only hazardous when machine is changing direction (10 %). H = 10 %

P: Typical bystander rate in central/parking areas. P = 25 %

AC: AC1 – brakes

AW: AW2

AR: AR3

LAD6 – slow/stop

H: Only hazardous when roading and stopping to avoid pedestrian (1 %). H = 1 %

P: Pedestrian always present when stopping to avoid pedestrian. P = 100 %

AC: AC1

AW: AW2

AR: AR2 – park brake

LAD7 – slow/stop

H: Only hazardous when slick underfoot conditions (25 %), curve present (40 %), downhill (15 %). H = 25 % × 40 % × 25 % = 2 %

P: Light vehicle on haul road traffic rate. P = 5 %

AC: AC0

LAD8 – hold still

H: Amount of time machine could be left unattended not in V ditch or specifically designed parking area designed to prevent roll away (10 %). H = 10 %

P: Only hazardous at this severity for pedestrians in area. P = 10 %

AC: AC0

LAD9 – hold still

H: 0 % of refuel (16,5 %), 10 % of daily walk around (33 %), 10 % of machine wash (8,25 %), 20 % of window wash (should 3 points of contact) (16,5 %), 0 % of brake test (8,5 %), 100 % troubleshooting (1 %), 50 % of body pin install (2,75 %), 100 % of articulation lock install (2,75 %) 25 % of camera wash (some lower severity) (8,25 %), 10 % of tyre inspection (2,75 %)

P: P: Typical P for maintenance tasks – 70 % of task on machine, 30 % of task off machine (changing / obtaining tools, preparation, cleaning etc.). P = 70 %

AC: AC0

LAD10 – steering

H: Not used as haul unit on the road (highway trucks are used then - more efficient), only used on road for relocation between sites. H=10 %

P: See 5.2. P = 16 %

AC: AC1 – brake

AW: AW2

AR: AR0

C.2.2 Application use cases

Table C.2 — Application use case table

Application	Roading	Loading and queuing	Unloading and queuing	Slow speed maneuvering	Maintenance
Less than 22 000 kg payload - articulated-frame dumpers	80 %	30 %	20 %	30 %	5 %

C.2.3 Maintenance task breakdown

See Table B.3.

C.2.4 Function dominant failure type matrix

See Table A.4.

C.2.5 Notes and assumptions

See A.3.

C.3 MPL_r mapped to SCS table

Table C.3 shows function-based MPL_r (see Table C.1) mapped to SCS per the results of the MCSSA for a less than 22 000 kg payload articulated-frame dumper. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table C.1 would also be mapped to these MPL_r.

Table C.3 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
body up	uncommanded activation	**b**	hoist raise
body down	failure to apply on demand	**a**	hoist lower
neutralize	uncommanded deactivation	**b**	gear direction control
machine speed	uncommanded activation	**a**	throttle and speed gear control
machine direction	failure to apply on demand	**a**	gear direction control
slow down / stop	failure to apply on demand	**b**	service brakes
	uncommanded activation	**c**	
hold still	failure to apply on demand	**c**	parking brakes
steering	uncommanded activation	**d**	steering

Annex D
(normative)

Crawler excavators less than 109 000 kg performance level tables

D.1 Crawler excavators less than 109 000 kg

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables D.1 to D.5) or in Clause 5.

This MPL_r table shall be used in conjunction with 5.4. If the assumptions in 5.5 do not apply, then an MCSSA shall be performed.

Table D.1 — MPL_r table for crawler excavators less than 109 000 kg

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CH1	**acceleration / machine speed / direction**	object handling	failure to release on demand	slow speed swing into traffic - co-worker	co-worker	S3	80 %	4 %	5 %	E0	AC1	AW2	AR0	C3	**c**
CH2		object handling	failure to release on demand	slow speed swing into traffic - collision	bystander	S3	80 %	4 %	14 %	E0	AC1	AW2	AR0	C3	
CH3		object handling	uncommanded activation	slow speed swing into traffic - collision	operator	S1	80 %	40 %	100 %	E2	AC1	AW2	AR0	C3	
CH4		travel	failure to release on demand	rotation of machine instead of stopping - collision	co-worker	S3	20 %	5 %	5 %	E0	AC1	AW2	AR0	C3	
CH5		travel	failure to release on demand	rotation of machine instead of stopping - collision	bystander	S3	20 %	5 %	5 %	E0	AC1	AW2	AR0	C3	
CH6		transport	failure to release on demand	machine rotates off truck and can tip (mini HEX could be carried on higher trucks)	operator	S2	5 %	100 %	100 %	E1	AC1	AW2	AR0	C3	

Table D.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CH7		transport	failure to release on demand	machine rotates off truck and can tip on person (mini HEX could be carried on higher trucks)	co-worker	S3	5 %	100 %	5 %	E0	AC1	AW2	AR0	C3	
CH8		trenching	uncommanded activation	collision with pedestrian or car	co-worker	S3	70 %	9 %	14 %	E0	AC1	AW2	AR0	C3	
CH9		trenching	uncommanded activation	collision with pedestrian or car	bystander	S2	70 %	14 %	14 %	E1	AC1	AW2	AR0	C3	
CH10		object handling	uncommanded activation	slow speed swing into traffic - co-worker	co-worker	S3	80 %	5 %	11 %	E0	AC1	AW2	AR0	C3	
CH11		object handling	uncommanded activation	slow speed swing into traffic - collision	bystander	S2	80 %	40 %	10 %	E1	AC1	AW2	AR0	C3	
CH12	**track width extension**	object handling	uncommanded deactivation	machine tips – no significant injury for this size machine	operator	S0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**QM**

Table D.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CH13	**boom up**	Considered to be the same as arm in													**c**
CH14		object handling	uncommanded activation	injury to fingers if in the process of lashing or unlashing	co-worker	S2	80 %	34 %	10 %	E1	AC0	N/A	N/A	C3	
CH15		travel	uncommanded activation	boom raises into overhead object or power lines	operator	S3	20 %	1 %	100 %	E0	AC0	N/A	N/A	C3	
CH13	**boom down**	Considered to be the same as arm in													**c**
CH16		object handling	uncommanded activation	crushed by boom, object on ground for parts of cycle that are hazardous	co-worker	S3	80 %	19 %	2 %	E0	AC0	N/A	N/A	C3	
CH21-28	**boom swing (L / R)**	considered to be the same as upper structure slew / swing													**c**
CH21-28	**boom offset**	considered to be the same as upper structure slew / swing													**c**
CH13	**arm in**	object handling	uncommanded activation	co-worker hit by object	co-worker	S3	80 %	5 %	5 %	E0	AC0	N/A	N/A	C3	**c**
CH17		maintenance	uncommanded activation	crushed by boom	maintainer	S3	5 %	8 %	70 %	E0	AC0	N/A	N/A	C3	
CH13	**arm out**	considered to be the same as arm in													**c**
CH13	**telescopic arm**	considered to be the same as arm in													**c**
CH13	**bucket dump**	considered to be the same as arm in													**c**
CH13	**bucket curl**	considered to be the same as arm in													**c**

Table D.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CH18	**auxiliary flow**	object handling	uncommanded activation	grabbing bucket / clamshell bucket opens dropping load.	co-worker	S2	80 %	26 %	5 %	E1	AC0	N/A	N/A	C3	**c**
WE23	**implement rotate**	considered to be the same as wheeled excavator													**c**
CH13	**blade up**	considered to be the same as arm in													**c**
CH19	**blade down / float / tilt / angle**	travel	uncommanded activation	blade lowers suddenly causing machine to come to abrupt stop – no significant injury for this type of machine due to low speed	operator	S0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**QM**
CH20	**coupler engagement**	trenching	uncommanded deactivation	bucket thrown from machine	co-worker	S3	70 %	1 %	1 %	E0	AC0	N/A	N/A	C3	**c**
CH13		considered to be the same as arm in													
CH21		travel	uncommanded activation	machine swings / slews into co-worker	co-worker	S3	20 %	50 %	5 %	E0	AC1	AW2	AR0	C3	
CH22		travel	uncommanded activation	machine swings / slews into bystander	bystander	S3	20 %	50 %	5 %	E0	AC1	AW2	AR0	C3	
CH23		trenching	failure to release on demand	collision with pedestrian or car	co-worker	S3	70 %	6 %	5 %	E0	AC1	AW2	AR0	C3	

Table D.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CH24	**upper structure swing/ slew**	trenching	failure to release on demand	collision with pedestrian or car	bystander	S2	70 %	11 %	14 %	E1	AC1	AW2	AR0	C3	**c**
CH25		trenching	uncommanded activation	collision with pedestrian or car	co-worker	S3	70 %	9 %	14 %	E0	AC1	AW2	AR0	C3	
CH26		trenching	uncommanded activation	collision with pedestrian or car	bystander	S2	70 %	12 %	14 %	E1	AC1	AW2	AR0	C3	
CH27		object handling	uncommanded activation	collision with pedestrian or car	co-worker	S3	80 %	6 %	11 %	E0	AC1	AW2	AR0	C3	
CH28		object handling	uncommanded activation	collision with pedestrian or car	bystander	S2	80 %	71 %	10 %	E1	AC1	AW2	AR0	C3	
CH21-28	**swing/slew - stop / slow / hold still**	considered to be the same as upper structure slew/swing													**c**
	cab tilt	considered machine abuse to be under cab unblocked in operation – not a safety function													
	cab elevate	considered to be the same as cab tilt													
	cab slide	considered to be the same as cab tilt													
	counterweight removal	not a safety function													
	engine speed	cannot cause increase in implement speed, therefore no significant hazard													

D.2 Supporting explanation

D.2.1 Supporting explanations for dominant scenarios

CH1 – acceleration / machine speed / direction

H: Only applicable during travel portion (4,7 %) – see Table 2, 90 % idle factor. H = 4 %

P: Co-workers are aware of hazard and avoid being directly under the boom wherever possible but may not always be able to. P = 5 %

AC: AC1 – Turn machine off or apply park brake

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH2 – acceleration / machine speed / direction

H: Only applicable during travel portion (4,7 %), 90 % idle factor. H = 4 %

P: See 5.5. P = 14 %

AC: AC1 – Turn machine off or apply park brake

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH3 – acceleration / machine speed / direction

H: See 5.5, 50 % of failures hazardous. H = 40 %

P: Operator always present. P = 100 %

AC: AC1 – Turn machine off or apply park brake

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH4, CH5 – acceleration / machine speed / direction

H: Only when in tight confines (50 %) and when stopping (10 %). H = 5 %

P: Co-workers are aware of hazard and avoid being directly under the boom wherever possible but may not always be able to. P = 5 %

AC: AC1 – Turn machine off or apply park brake

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH6 – acceleration / machine speed / direction

H: Could happen at any point while loading machine onto transport. H = 100 %

P: Operator always present during cycle. P = 100 %

AC: AC1 – Turn machine off or apply park brake

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH7 – acceleration / machine speed / direction

H: Could happen at any point while loading machine onto transport. H = 100 %

P: People should not be standing in vicinity (may be in front or behind to guide machine on). P = 5 %

AC: AC1 – Turn machine off or apply park brake

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH8 – acceleration / machine speed / direction

H: Only hazardous during dump (10 %), 90 % idle factor. H = 9 %

P: Assumes people are aware of hazard of swinging machine on work area P=5 % plus traffic rate 1/6. P = (17 %+5 %+5 %)/2 = 14 %

AC: AC1 – Turn machine off or apply park brake

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH9 – acceleration / machine speed / direction

H: Only hazardous during dump plus last 25 % of swing (16 %), 90 % idle factor. H = 14 %

P: Assumes people are aware of hazard of swinging machine on work area P=5 % plus traffic rate 1/6. P = (17 %+5 %+5 %)/2 = 14 %

AC: AC1 – Turn machine off or apply park brake

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH10 – acceleration / machine speed / direction

H: Only hazardous last 25 % of swing (2 %) and when above the surface for lower – see 5.5 for more detail (8,5 %), 90 % idle factor. H = 10,3 %

P: See 5.5. P = 11 %

AC: AC1 – Turn machine off or apply park brake

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH11 – acceleration / machine speed / direction

H: Only hazardous during lash (21,3 %), last 25 % of swing (2 %) and when above the surface for lower – see 5.5 for more detail (8,5 %), 90 % idle factor. H = 31,6 %

P: People should not be in the area; barriers should be in place. P = 10 %

AC: AC1 – Turn machine off or apply park brake

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH12 – track width extension

H: Results in no significant hazard

P: N/A

AC: N/A

AW: N/A

AR: N/A

CH13 – arm in

H: Only hazardous for half of lowering underground (50 % × 10 %) - another half at S2. 90 % idle factor. H = 5 %

P: It is considered machine abuse to be between object and pinch point, may be momentarily due to confined space. P = 5 %

AC: AC0 – No alternative controls

CH14 – boom up

H: Only hazardous for lashing and unlashing. Based on 45/10/45 breakdown of time spend unlashing and lashing and moving, 90 % of lashing / unlashing. 90 % idle factor. H = 34 %

P: Only have hands in hazardous point when connecting chains. P = 10 %

AC: AC0 – No alternative controls

CH15 – boom up

H: Rare for power lines or overhead objects to be present. H = 1 %

P: Operator always present for the cycle. P = 1 %

AC: AC0 – No alternative controls

CH16 – boom down

H: Hazardous for half of lash and unlash ((21,3 % × 2)/2), 90 % idle factor. H = 19 %

P: It is considered machine abuse to stand below boom, may be close when grabbing chains in lashing or unlashing. P = 2 %

AC: AC0 – No alternative controls

CH17 – arm in

H: See D.2.3. 10 % of daily inspection, 25 % grease, 5 % wash 0 % windows / mirrors. H = (10 % × 15 %) + (25 % × 25 %) + (3 % × 5 %) = 8 %

P: Typical P for maintenance tasks – 70 % of task on machine, 30 % of task off machine (changing / obtaining tools, preparation, cleaning etc). P = 70 %

AC: AC0 – No alternative controls

CH18 – auxiliary flow

H: Only during lower (28 %). 90 % idle factor. H = 26 %

P: Co-workers should be aware of the hazards of suspended load. P = 5 %

AC: AC0 – No alternative controls

CH19 – – blade down / float / tilt / angle

H: Results in no significant hazard

P: N/A

AC: N/A

AW: N/A

AR: N/A

CH20 – coupler engagement

H: Last 10 % of dump (10 %), 90 % idle factor. H = (10 % × 10 %) × 90 % = 0,9 %

P: It is considered machine abuse to stand below boom, may be close when grabbing chains in lashing. P = 2 %

AC: AC0 – No alternative controls

CH21-22 – upper structure swing/slew

H: Only hazardous when traveling in tight confines. H = 50 %

P: People should not be standing in swing radius but may have to momentarily. P = 5 %

AC: AC1 – Turn machine off or apply hydraulic lockout

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH23 – upper structure swing/slew – considers the bucket at height between person's waist and head (S3)

H: See 5.5. Only hazardous stopping (last 25 %) while swing/slewing from A - B (25 % of cycle), 90 % idle factor. H = 6 %

P: People should not be standing in swing radius but may have to momentarily. P = 5 %

AC: AC1 – Turn machine off or apply hydraulic lockout

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH24 – upper structure swing/slew – considers bucket at height below person's waist (S2)

H: Hazardous in both swing directions while stopping (last 25 %). 90 % idle factor. H = 11 %

P: See 5.5. P = 14 %

AC: AC1 – Turn machine off or apply hydraulic lockout

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH25 – upper structure swing/slew – considers the bucket at height between person's waist and head (S3)

H: Hazardous only during dump (10 %). 90 % idle factor. H = 9 %

P: See 5.5. P = 14 %

AC: AC1 – Turn machine off or apply hydraulic lockout

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH26 – upper structure swing/slew – considers bucket at height below person's waist (S2)

H: Only dangerous during dump and last 10 % of dig ((10 %×35 %) +10 %), 90 % idle factor. H = 12 %

P: See 5.5. P = 14 %

AC: AC1 – Turn machine off or apply hydraulic lockout

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH27 – upper structure swing/slew – considers the bucket at height between person's waist and head (S3)

H: See 5.5 for S3 material handling H, 90 % idle factor. H = 7 % × 90 % = 6 %

P: Similar to 5.5, however people on site side of machine should be aware of the hazard and not in area (additional 5 % removed from calculation). P = 14 %

AC: AC1 – Turn machine off or apply hydraulic lockout

AW: AW2

AR: AR0 – Not all operators would be able to react in time

CH28 – upper structure swing/slew – considers bucket at height below person's waist (S2)

H: See 5.5 for S2 material handling H, 90 % idle factor. H = 79 % × 90 % = 71 %

P: People should not be in the area and barriers should be in place if next to public thoroughfare. P = 10 %

AC: AC1 – Turn machine off or apply hydraulic lockout

AW: AW2

AR: AR0 – Not all operators would be able to react in time

D.2.2 Application use cases

Table D.2 — Application use case table

Application	Bucket work (truck loading, includes general digging, leveling with bucket) [a]	Trenching (co-worker may be present)	Object handling (includes truck loading objects, pipe laying, positioning etc.)	Leveling (grading with blade) [a]	Travel	Maintenance (including assembly and disassembly for transport - counterweight removal, track installation)	Transport (loading / unloading machine from truck)	Work tool (auxiliary hydraulic only - grapple, demolition, log loading) [a]
Mini HEX (Front mounted boom)	70 %	50 %	20 %	15 %	20 %	5 %	5 %	75 %
Medium HEX	80 %	70 %	80 %	15 %	20 %	5 %	2 %	90 %
Large HEX (36 000 kg – 99 000 kg)	85 %	70 %	10 %	0 %	20 %	5 %	1 %	20 %

[a] Could not find a scenario worse than trenching / object handling unless otherwise noted.

D.2.3 Maintenance task breakdown

Table D.3 — Maintenance task breakdown

	Mini / Med		Large	
Task	Time (min/day)	% Maintenance time	Time (min)	% Maintenance time
daily inspection	6	15	4	7
refuel / DEF	10	25	20	34
lube / greasing	10	25	20	34
undercarriage removal	0	0	1	2
counterweight removal	0	0	0	1
wash	2	5	2	4
oil sample	1	1	1	2
clean windows and mirrors	5	13	5	8
troubleshooting	0	1	0	1
clean cooling package (waste application)	4	10	4	7
refill window washer	1	3	1	2
flash / calibrations	0	1	0	1

D.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table D.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
accelerate / machine speed / direction		1	1		Includes travel in wrong direction, each side is independent. Uncommanded deactivation is considered the same as failure to release on demand.
track width extension				1	Operator should not start operation until width is set to requirement.
boom up			1		Failure to release on demand has same outcome as uncommanded activation. Other failure types are less or not hazardous.
boom down			1		Failure to release on demand is considered no worse than uncommanded activation.
boom swing (L / R)		1	1		Other failure types are less or not hazardous.
boom offset			1		Failure to release on demand is considered no worse than uncommanded activation. Other failure types are less or not hazardous.
arm in			1		Other failure types are less or not hazardous.
arm out			1		Other failure types are less or not hazardous.
telescopic arm			1		Other failure types are less or not hazardous. Used only with clamshell.
bucket dump			1		Other failure types are less or not hazardous.
bucket curl			1		Other failure types are less or not hazardous.
auxiliary flow			1		Various failure types could cause uncommanded movement based on the tool type. All are considered here.
blade up			1		Other failure types are less or not hazardous.
blade down			1		Other failure types are less or not hazardous.
blade float					It is considered the same as blade up.
blade tilt					Considered the same as worse of blade up and blade down
blade angle					Considered the same as worse of blade up and blade down
quick coupler engagement				1	Other failure types are less or not hazardous.
swing/slew		1	1		Other failure types are less or not hazardous.
swing/slew slow/stop / hold still	1				Uncommanded deactivation is considered no worse than failure to apply on demand. Other failure types are less or not hazardous.
rated capacity indicator	1				Other failure types are less or not hazardous.
cab tilt			1		Other failure types are less or not hazardous.
cab elevate				1	Other failure types are less or not hazardous.
cab slide			1		Other failure types are less or not hazardous.
counterweight removal			1		Other failure types are less or not hazardous.

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

D.2.5 Notes and assumptions

— Use cases requiring machine modification to be used safely are out of scope, e.g. forestry.

— Applications considered are: construction, utilities, oil and gas, agriculture, waste, demolition, general purpose (including rental), quarry.

— Machines used in material handling use cases are assumed to have appropriate control/check valves fitted (BLCV, SLCV) and be configured for lifting.

— Engine speed impact on other SCS is covered in those systems.

— Telescopic boom is not considered a common feature and thus not considered in this assessment.

— Excavators do not have active brake controls. It is part of the track control.

— Control pattern and mode change systems are the highest MPL_r of the system that are being controlled by that function.

— For swing and uncommanded propel (causes rotation) calculations values for medium excavators have been used.

— Considered lifting bollards or barriers off a truck onto the ground and found it to be no worse than a ditch scenario.

— For swing calculations considered the co-worker as the S3 scenario and S2 for bystander to consider both scenarios. Both could be present interchangeably.

— It is machine abuse to lift objects over bystanders.

— Where hazard is present from object swinging there is a co-worker guiding object from a safe distance by rope or chain.

— Quick coupler scoring assumes couplers meet ISO 13031.

— Work tools require analysis specific to the type of work tool.

— For elevated cab machines, it is considered machine abuse for people to be under the unblocked cab during operation.

— For rated capacity indicator - using the capacity indicator is considered miss use. Due care shall be taken to ensure that load restrictions are followed. Analysis done on the assumption that people should not be relying on indicator.

— For maintenance, assumed that the implement is grounded. It is considered machine abuse if this is not the case.

D.3 MPL_r mapped to SCS table

Table D.5 shows function-based MPL_r (see Table D.1) mapped to SCS per the results of the MCSSA for a crawler excavator. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table D.1 would also be mapped to these MPL_r.

Table D.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
acceleration / machine speed / direction	failure to release on demand	**c**	propel
	uncommanded activation		
track width extension	uncommanded activation	**QM**	track width extension
boom up	uncommanded activation	**c**	boom raise
boom down	uncommanded activation	**c**	boom lower
boom swing (L / R)	uncommanded activation	**c**	boom swing
boom offset	uncommanded activation	**c**	boom offset
arm in	uncommanded activation	**c**	arm in
arm out	uncommanded activation	**c**	arm out
telescopic arm	uncommanded activation	**c**	telescopic arm
bucket dump	uncommanded activation	**c**	bucket dump
bucket curl	uncommanded activation	**c**	bucket curl
auxiliary flow	uncommanded activation	**c**	auxiliary flow

Table D.5 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
blade up	uncommanded activation	**c**	blade raise
blade down/float/ tilt / angle	uncommanded activation	**QM**	blade lower / float / tilt / angle
coupler engagement	uncommanded deactivation	**c**	coupler engagement
upper structure swing/slew	uncommanded activation	**c**	swing/slew
	failure to release on demand		
swing/slew - stop / slow down / hold still	uncommanded activation	**c**	swing/slew brake
implement rotate	uncommanded activation	**c**	implement rotate

Annex E
(normative)

Wheeled excavators performance level tables

E.1 Wheeled excavators

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables E.1 to E.5) or in Clause 5.

Table E.1 — MPL_r table for wheeled excavators

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
WE1	**machine speed**	roading	failure to release on demand	machine stops later than expected due to throttle being stuck on - bystander	bystander	S3	35 %	10 %	100 %	E1	AC1	AW2	AR3	C1	**b**
WE2	**machine direction**	lifting	failure to apply on demand	machine goes in opposite direction than intended - enters area where machine is not expected	co-worker	S3	75 %	2 %	20 %	E0	AC1	AW2	AR3	C1	**a**
WE3		travel	failure to apply on demand	machine goes in opposite direction than intended - enters area where machine is not expected - Moving machine into tighter area	bystander	S3	35 %	1 %	5 %	E0	AC1	AW2	AR3	C1	
WE12-13	**boom up**	considered to be the same blade down													**c**
WE4		lifting	uncommanded activation	injury to fingers if in the process of lashing or unlashing	co-worker	S2	75 %	34 %	10 %	E1	AC0	N/A	N/A	C3	
WE5		travel	uncommanded activation	boom raises into overhead object or power lines	operator	S3	35 %	1 %	100 %	E0	AC0	N/A	N/A	C3	

[a] A car or larger vehicle would be a lower severity injury.

Table E.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
WE12-13	**boom down**	considered to be the same blade down													**c**
WE6		lifting	uncommanded activation	crushed by boom, object on ground for parts of cycle that are hazardous	co-worker	S3	75 %	19 %	2 %	E0	AC0	N/A	N/A	C3	
WE15-17	**boom offset**	considered to be the same as upper structure slew / swing													**c**
WE10		maintenance	uncommanded activation	crush body	maintainer	S3	5 %	2 %	70 %	E0	AC0	N/A	N/A	C3	
WE8	**arm in**	Considered to be the same arm out													**c**
WE7		material handling	uncommanded activation	work tool enters cab (when machine has intermediate boom)	operator	S3	90 %	1 %	100 %	E0	AC1	AW2	AR0	C3	
WE8	**arm out**	lifting	uncommanded activation	hit by object being lifted	co-worker	S3	75 %	5 %	5 %	E0	AC0	N/A	N/A	C3	**c**
WE9		roading	uncommanded activation	implement hits rear of vehicle or bystander when stopped in traffic	bystander	S3	35 %	5 %	1 %	E0	AC0	N/A	N/A	C3	
WE7	**tool dump**	considered to be the same as arm in													**c**
WE7	**tool curl**	considered to be the same as arm in													**c**
WE11	**auxiliary flow**	work tool	uncommanded activation	grabbing bucket / clamshell bucket opens dropping load.	co-worker	S2	80 %	26 %	5 %	E1	AC0	N/A	N/A	C3	**c**
WE6	**blade up**	considered to be the same as boom down													**c**

[a] A car or larger vehicle would be a lower severity injury.

Table E.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
WE12	**blade down**	roading	uncommanded activation	sudden stop from hitting ground, manhole cover, rail track	operator	S1	35 %	50 %	100 %	E2	AC0	N/A	N/A	C3	**c**
WE13		travel / roading	uncommanded activation	vehicle behind collides with rear of machine	bystander	S3	35 %	50 %	5 %	E0	AC0	N/A	N/A	C3	
WE14	**coupler engagement**	trenching	uncommanded deactivation	bucket thrown from machine	co-worker	S3	70 %	1 %	1 %	E0	AC0	N/A	N/A	C3	**c**
WE7		considered to be the same as arm in													
WE15	**upper structure swing/ slew**	trenching	failure to release on demand	machine swings into co-worker or bystander	bystander	S3	70 %	6 %	5 %	E0	AC0	N/A	N/A	C3	**c**
WE16		trenching	uncommanded activation	machine swings / slews into bystander	bystander	S3	70 %	9 %	14 %	E0	AC0	N/A	N/A	C3	
WE17		lifting	uncommanded activation	machine swings / slews into bystander	co-worker	S3	75 %	4 %	11 %	E0	AC0	N/A	N/A	C3	
WE18	**upper structure swing/ slew hold still**	roading	uncommanded deactivation	machine swings into traffic	bystander	S3	35 %	100 %	25 %	E1	AC0	N/A	N/A	C3	**d**
WE19	**cab lower**	maintenance	uncommanded activation	crush	maintainer	S3	5 %	2 %	70 %	E0	AC0	N/A	N/A	C3	**c**
WE20	**cab elevate**	travel	uncommanded activation	cab rises and hits overhead powerline or structure	operator	S3	35 %	1 %	100 %	E0	AC1	AW3	AR3	C0	**QM**

[a] A car or larger vehicle would be a lower severity injury.

Table E.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
WE21	**hold still**	bucket work	failure to apply on demand	runaway machine	co-worker	S3	80 %	5 %	20 %	E0	AC0	N/A	N/A	C3	**c**
WE22		travel	failure to apply on demand	runaway machine	bystander	S3	35 %	5 %	25 %	E0	AC0	N/A	N/A	C3	
WE23	**implement rotate**	work tool	uncommanded activation	contact with object	co-worker	S3	80 %	37 %	2 %	E0	AC0	N/A	N/A	C3	**c**
WE8	**intermediate boom up**	considered to be the same arm out													**c**
WE7	**intermediate boom down**	considered to be the same as arm in													**c**
WE24	**oscillating axle unlock**	bucket work	uncommanded activation	machine rolls over	operator	S1	80 %	100 %	100 %	E2	AC0	N/A	N/A	C3	**c**
WE25		lifting	uncommanded activation	machine rolls over	co-worker	S3	75 %	4 %	20 %	E0	AC0	N/A	N/A	C3	
WE8		considered to be the same as upper structure slew / swing													
WE24-25	**stabilizers up**	considered to be the same arm out													**c**
WE12-13	**stabilizers down**	considered to be the same blade down													**c**
WE26		roading	uncommanded activation	stabilizers lower while in traffic - collision	bystander	S3	35 %	20 %	10 %	E0	AC0	N/A	N/A	C3	
WE27	**steering**	roading	uncommanded activation	machine steers into traffic	bystander	S3	35 %	100 %	16 %	E1	AC1	AW2	AR0	C3	**d**
WE27	**steering mode change**	considered to be the same as steering													**d**

[a] A car or larger vehicle would be a lower severity injury.

Table E.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
WE28	**slow/stop**	travel	failure to apply on demand	collision	bystander	S3	35 %	50 %	10 %	E1	AC1	AW2	AR2	C2	**c**
WE29		roading	uncommanded activation	machine stops without command - collision with vehicle following	operator	S1	35 %	50 %	100 %	E2	AC0	N/A	N/A	C3	
WE30		roading	uncommanded activation	machine stops without command – Trailing vehicle or motorcycle collides with machine. [a]	bystander	S3	35 %	50 %	5 %	E0	AC0	N/A	N/A	C3	
WE31	**transmission neutralize**	travel	uncommanded deactivation	machine moves into vehicle or bystander	bystander	S3	35 %	3 %	25 %	E0	AC1	AW2	AR3	C1	**a**

[a] A car or larger vehicle would be a lower severity injury.

E.2 Supporting explanation

E.2.1 Supporting explanations for dominant scenarios

WE1 – machine speed

H: Only hazardous when braking to avoid pedestrian or vehicle. H = 10 %

P: Assumes pedestrian always present when needing to stop at pedestrian crossing. P = 100 %

AC: AC1 – brakes

AW: AW2

AR: AR3 – Applying brakes is a natural reaction and applying brake during the operation is considered underfoot

WE2 – machine direction

H: Only hazardous at the start of the travel portion. H = 2 %

P: Construction site co-worker rate. P = 20 %

AC: AC1 – brakes

AW: AW2

AR: AR3 – Applying brakes is a natural reaction and applying brake during operation is considered underfoot. Machine moves very slow during direction change.

WE3 – machine direction

H: Rarely change direction while traveling. H = 1 %

P: Rarely people between machine and object / vehicle or in parked vehicle. P = 5 %

AC: AC1 – brakes

AW: AW2

AR: AR3 – Applying brakes is a natural reaction and applying brake during the operation is considered underfoot. Machine moves very slow during direction change.

WE4 – boom up

H: Only hazardous for lashing and unlashing. Based on 45/10/45 breakdown of time spend unlashing and lashing and moving, 90 % of lashing / unlashing. 90 % idle factor. H = 34 %

P: Only have hands in hazardous point when connecting chains. P = 10 %.

AC: AC0

WE5 – boom up

H: Rare for powerlines / objects to be present. H = 10 %

P: Operator present throughout cycle. P = 100 %.

AC: AC0

WE6 – boom down

H: 50 % lash, 50 % unlash (see 5.3), 90 % idle factor. H = 18 %

P: It is considered machine abuse for co-worker to stand below boom, may be close when grabbing chains in lashing. P = 2 %.

AC: AC0

WE7 – arm in

H: Boom shall be at upper limits of heights - only likely during release when loading a high hopper. 5 % of release (see 5.3), 90 % idle factor. H = 1 %

P: Operator present throughout cycle. P = 100 %.

AC: AC1 – key switch

AW: AW2

AR: AR0

WE8 – arm out

H: Hazardous for half of lowering underground (50 % × 10 %) – the other half at S2. 90 % idle factor. H = 5 %

P: It is considered machine abuse to be between object and pinch point, may be momentarily due to confined space. P = 5 %.

AC: AC0

WE9 – arm out

H: Only when stopped in traffic. H = 5 %

P: Only when stopped behind vehicles of specific heights. P = 1 %.

AC: AC0

WE10 – boom offset

H: Only hazardous for 10 % of greasing (19 %). H = 1- % × 19 % = 2 %

P: See 5.8. Maintainer on machine for 70 % of task on smaller machine. P = 70 %.

AC: AC0

WE11 – auxiliary flow

H: Hazardous while lowering only (28 %), 90 % idle factor. H = 26 %

P: People should not be under suspended load but may be momentarily. P = 5 %.

AC: AC0

WE12 – blade down

H: Hazard present when the machine is travelling at higher speeds and not stopping. H = 50 %

P: Operator present throughout cycle. P = 100 %.

AC: AC0

WE13 – blade down

H: Only hazard when in heavy traffic. H = 50 %

P: Vehicles should be going same speed as machine, and maintaining legal safe distances, only S3 for bikes and scooters. P = 5 %.

AC: AC0

WE14 – coupler engagement

H: Last 10 % of dump (10 %), 90 % idle factor. H = (10 % × 10 %) × 90 % = 0,9 %

P: It is considered machine abuse to be standing near a load being dumped. P = 1 %

AC: AC0

WE15 – upper structure swing/slew

H: Swing from A - B (25 % of cycle), stopping in last 25 %, 90 % idle factor. See Table 3. H = (25 % × 25 %) × 90 % = 6 %

P: It is considered machine abuse to be standing within swing/slew radius of machine, could happen momentarily. P = 5 %

AC: AC0

WE16 – upper structure swing/slew

H: Only dangerous during dump (10 %), 90 % idle factor. See 5.5. H = 9 %

P: It is considered machine abuse to be standing within swing/slew radius of machine, could happen momentarily, P = 5 % in work zone, traffic rate 1/6. P = ((17 % + 5 %) + 5 %)/2 = 14 %

AC: AC0

WE17 – upper structure swing/slew

H: 90 % idle factor, 50 % failures hazardous. See 5.5. H = 8,5 % × 50 % × 90 % = 4 %

P: See 5.5.2. P = 11 %

AC: AC0

WE18 – upper structure swing/slew hold still

H: Hazard exists during the whole cycle. H = 100 %

P: For collision in one direction collision with the front of a car (bucket below roof height is hazardous) - traffic rate 1 car every 3 car lengths (33 %). For swing in the other direction collision with the rear of the car (bucket greater than approximately 1 m off ground is hazardous), traffic rate 1/6 (see 5.5.2). P = (33 % + 17 %) / 2 = 25 %.

AC: AC0

WE19 – cab lower

H: 10 % of greasing (19 %). H = 2 %

P: See 5.8. Maintainer on machine for 70 % of task on smaller machine. P = 70 %.

AC: AC0

WE20 – cab raise

H: Rare for powerlines / objects to be present. H = 1 %

P: Operator present throughout cycle. P = 100 %.

AC: AC1 – brakes

AW: AW3 – Cab raises slowly and is not hazardous until the end of the range of motion

AR: AR3 - Stop before the machine hits object

WE21 – hold still

H: When machine stopped, bucket off ground when it should be grounded. H = 5 %

P: Construction site co-worker rate. P = 20 %

AC: AC0

WE22 – hold still

H: When machine stopped, bucket off ground when it should be grounded. H = 5 %

P: See 5.6 for park up area (considered similar for longitudinal traffic). P = 25 %.

AC: AC0

WE23 – implement rotate

H: Hazardous for 33 % or grab (30 %) and release (10 %), all loaded swing (25 %). 90 % idle factor. H = [(33 % × 38 %) + (25 %) + (33 % × 10 %)] × 90 %

P: It is considered machine abuse to be in pinch area for pipe laying, or that close to swinging machine. May occur momentarily. P = 2 %.

AC: AC0

WE24 – oscillating axle unlock

H: Hazard exists during the whole cycle. H = 100 %

P: Operator present throughout cycle. P = 100 %.

AC: AC0

WE25 – oscillating axle unlock

H: Only hazardous higher speed potions of swing or lifting load high (50 % × 8 %), idle factor 90 %. H = 4 %

P: Construction site co-worker rate. P = 20 %

AC: AC0

WE26 – stabilizers down

H: See 5.9. 20 % of the arc passes through where traffic could be. H = 20 %

P: See 5.9. Traffic / pedestrians would rarely be this close to the machine. P = 10 %

AC: AC0

WE27 – steering

H: Hazard exists during the whole cycle. H = 100 %

P: See 5.2. P = 16 %.

AC: AC1 – brakes

AW: AW2

AR: AR0

WE28 – slow/stop

H: Only hazardous when wanting to stop or slow - worst case in traffic. H = 50 %

P: rarely slowing to avoid hitting pedestrian. P = 10 %.

AC: AC1 – park brake

AW: AW2

AR: AR2

WE29 – slow/stop

H: Hazard present when the machine is travelling at higher speeds and not stopping. H = 50 %

P: Operator present throughout cycle. P = 100 %.

AC: AC0

WE30 – slow/stop – S3 has been used because following vehicle could be a motorcycle. A car would be S2 or S1.

H: Only hazardous when not stopping or slowing. H = 50 %

P: Vehicles should be going same speed as machine and maintaining legal safe distances. P = 5 %.

AC: AC0

WE31 – transmission neutralize

H: Time when machine is idle while waiting and portion of travel that is low speed manoeuvring (1 / 6). H = 0,2 × 1 / 6 = 3 %

P: Typical bystander rate in central / parking areas. P = 25 %.

AC: AC1 – brakes

AW: AW2

AR: AR3 – The brakes would be under foot and the machine moves slowly

E.2.2 Application use cases

Table E.2 — Application use case table

Application	Bucket work (truck loading, includes general digging, leveling with bucket)	Trenching (co-worker may be present)	Lifting (auspended load includes truck loading objects, pipe laying, positioning etc.)	Leveling (grading with blade)	Travel	Maintenance (including assembly and disassembly for transport - counterweight removal, track installation)	Transport (loading / unloading machine from truck)	Work tool (auxiliary hydraulic only - grapple, demolition, log loading)
Construction (road and general)	80 %	70 %	75 %	15 %	35 %	5 %	2 %	8 %
Material handling (waste, forestry, demolition)	20 %	0 %	0 %	5 %	1 %	5 %	2 %	9 %

E.2.3 Maintenance task breakdown

Table E.3 — Maintenance task breakdown

	Time (min/ day)	%Maintenance Time
daily inspection	10	19
refuel / DEF	10	19
lube / greasing	10	19
tire pressure check / top up	10	19
wash	10	1
oil sample	15	1
clean windows and mirrors, cameras	5	10
troubleshooting	30	1
clean cooling package (waste application)	4	8
refill window washer	1	2
flash / calibrations	60	1

E.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table E.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
machine speed		1	1		Apply is increase, release is decrease. Other failure types are not considered hazardous.
machine direction	1				Uncommanded change in direction is considered the same as uncommanded slow/stop. Other failure types are considered the same as failure on demand.
transmission neutralize				1	Uncommanded deactivation is the same as failure to neutralize. Other failure types are not hazardous.
bucket curl			1		Other failure types are less or not hazardous.
bucket dump			1		Other failure types are less or not hazardous.
arm in			1		Other failure types are less or not hazardous.
arm out			1		Other failure types are less or not hazardous.
boom up			1		Other failure types are less or not hazardous.
boom down			1		Other failure types are less or not hazardous.
intermediate boom up			1		Other failure types are less or not hazardous.
intermediate boom down			1		Other failure types are less or not hazardous.
blade up			1		Other failure types are less or not hazardous.
blade down			1		Other failure types are less or not hazardous.
stabilizers up			1		Other failure types are less or not hazardous.
stabilizers down			1		Other failure types are less or not hazardous.
coupler engagement				1	Other failure types are less or not hazardous.

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

Table E.4 *(continued)*

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
boom offset / side shift			1		Other failure types are less or not hazardous.
implement rotate			1		Other failure types are less or not hazardous.
auxiliary flow			1		Other failure types are less or not hazardous.
slow/stop	1		1		Uncommanded deactivation is the same as failure to neutralize. Other failure types are not hazardous.
hold still	1				It is the same as uncommanded release.
steering			1		Considered all failure types within uncommanded steering.
steering mode change			1		Considered all failure types within uncommanded mode change.
cab rise			1		Other failure types are less or not hazardous.
cab lower			1		Other failure types are less or not hazardous.
oscillating axle unlock			1		Other failure types are considered in oscillating axle lock.
oscillating axle lock	1	1			Other failure types are considered in oscillating axle unlock.
upper structure swing		1	1		Includes swing lock, considers both a failure to stop and an uncommanded swing.

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

E.2.5 Notes and assumptions

— Covers wheeled excavators of all sizes.

— Travel lock MPL_r is determined by the functions it controls, which will vary by function. The system design may be broken into sub functions.

— Travel during lifting could be as high as 50 % of cycle for wheeled excavators.

— Wheeled excavators up to 25 000 kg can be used in roading applications.

— Assumptions and grounds for swing analysis shall be documented and communicated by the manufacturer in the information for use.

— Uncommanded direction change, uncommanded slow/stop and uncommanded hold still are considered to be the same hazardous outcome – the machine would stop suddenly without warning to the operator or a person following behind the machine.

E.3 MPL_r mapped to SCS table

Table E.5 shows function-based MPL_r (see Table E.1) mapped to SCS per the results of the MCSSA for a wheeled excavator. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table E.1 would also be mapped to these MPL_r.

Table E.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
machine speed	failure to release on demand	**b**	throttle and speed gear control
machine direction	failure to apply on demand	**a**	gear direction control
boom up	uncommanded activation	**c**	boom raise

Table E.5 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
boom down	uncommanded activation	**c**	boom lower
boom offset	uncommanded activation	**c**	boom offset
arm in	uncommanded activation	**c**	arm in
arm out	uncommanded activation	**c**	arm out
tool dump	uncommanded activation	**c**	tool dump
tool curl	uncommanded activation	**c**	tool curl
auxiliary flow	uncommanded activation	**c**	auxiliary flow
blade up	uncommanded activation	**c**	blade raise
blade down	uncommanded activation	**QM**	blade lower
coupler engagement	uncommanded deactivation	**c**	coupler engagement
	uncommanded activation		
upper structure swing/slew	failure to release on demand	**c**	slew / swing
	uncommanded activation		
upper structure swing/slew hold still	uncommanded activation	**d**	slew / swing brake
cab lower	uncommanded activation	**c**	cab lower
cab elevate	uncommanded activation	**QM**	cab raise
hold still	failure to apply on demand	**c**	parking brakes
implement rotate	uncommanded activation	**c**	implement rotate
intermediate boom up	uncommanded activation	**c**	intermediate boom raise
intermediate boom down	uncommanded activation	**c**	intermediate boom lower
oscillating axle unlock	uncommanded activation	**c**	oscillating axle unlock
stabilizers up	uncommanded activation	**c**	stabilizers up
stabilizers down	uncommanded activation	**c**	stabilizers down
steering	uncommanded activation	**d**	steering
steering mode change	uncommanded activation	**d**	steering mode change
transmission neutralize	uncommanded deactivation	**a**	gear direction control
slow/stop	failure to apply on demand	**c**	service brakes
	uncommanded activation		

Annex F
(normative)

Backhoe loaders performance level tables

F.1 Backhoe loaders

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables F.1 to F.5) or in Clause 5.

Table F.1 — MPL_r table for backhoe loaders

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
BH1	**machine speed**	travel / roading	uncommanded activation	machine speed increases - increased stopping distance and decreased operator ability to steer	bystander	S3	30 %	40 %	16 %	E1	AC1	AW2	AR3	C1	**b**
BH2		travel / roading	failure to release on demand	machine speed increases - increased stopping distance and decreased operator ability to steer - pedestrian	bystander	S3	30 %	50 %	10 %	E1	AC1	AW2	AR3	C1	
BH9-10	**machine direction**	considered to be the same as uncommanded hold still													**c**
BH3	**hoe boom up**	considered to be the same as hoe boom down													**c**
BH3	**hoe boom down**	lifting	uncommanded activation	crushed by object	co-worker	S3	20 %	19 %	2 %	E0	AC0	N/A	N/A	C3	**c**
BH7-8	**hoe boom offset**	considered to be the same as hoe slew / swing													**c**
BH4-5	**hoe arm in**	considered to be the same as hoe arm out													**c**
BH4	**hoe arm out**	travel	uncommanded activation	hit by bucket	co-worker	S3	30 %	2 %	100 %	E0	AC0	N/A	N/A	C3	**c**
BH5		lifting	uncommanded activation	crushed between load and trench wall	co-worker	S3	20 %	5 %	5 %	E0	AC0	N/A	N/A	C3	
BH4-5	**hoe tool dump**	considered to be the same as arm out													**c**
BH4-5	**hoe tool curl**	considered to be the same as arm out													**c**
	hoe auxiliary flow	tools used on backhoe loaders were not considered to be hazardous. If tools are used similar to crawler or wheeled excavators than the MPL_r for those machines shall be used – not a safety function													

[a] A car or larger vehicle would be a lower severity injury.

Table F.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
BH9-10	**loader boom up**	considered to be the same as uncommanded hold still													**c**
BH3		considered to be the same as hoe boom down													
BH9-10	**loader boom down**	considered to be the same as uncommanded park brake activation. If loader lower could cause a loss of steering, then the MPL_r for failure to steering shall be used													**c**
BH3		considered to be the same as hoe boom down													
BH9-10	**loader tool dump**	considered to be the same as uncommanded hold still													**c**
BH3		considered to be the same as hoe boom down													
BH9-10	**loader tool curl**	considered to be the same as uncommanded hold still													**c**
BH3		considered to be the same as hoe boom down													
BH6	**hoe coupler engagement**	hoe	uncommanded deactivation	hit by falling bucket (when lifting from a point on bucket)	co-worker	S3	70 %	1 %	1 %	E0	AC0	N/A	N/A	C3	**c**
BH3		considered to be the same as hoe boom down													
BH7	**hoe swing/ slew**	lifting	uncommanded activation	collision between hoe linkage and co-worker or bystander	bystander	S3	20 %	19 %	11 %	E0	AC0	N/A	N/A	C3	**c**
BH8		lifting	uncommanded activation	person impacted by the hoe linkage	co-worker	S3	40 %	100 %	2 %	E0	AC0	N/A	N/A	C3	

[a] A car or larger vehicle would be a lower severity injury.

Table F.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
BH9	**hold still**	roading	uncommanded activation	machine stops without command - collision with vehicle following	operator	S1	30 %	50 %	100 %	E2	AC0	N/A	N/A	C3	**c**
BH10		roading	uncommanded activation	machine stops without command – Trailing vehicle or motorcycle collides with machine. [a]	bystander	S3	30 %	50 %	5 %	E0	AC0	N/A	N/A	C3	
BH11		maintenance	failure to apply on demand	runover by rolling machine	maintainer	S3	5 %	18 %	70 %	E0	AC0	N/A	N/A	C3	
BH3	**stabilizers up**	considered to be the same as hoe boom down													**c**
BH9-10	**stabilizers down**	for a side-shift machine it is considered the same as uncommanded hold still													**c**
BH4-5		for a centre pivot it is considered the same as arm out													
BH12	**steering**	roading	uncommanded activation	collision	bystander	S3	30 %	100 %	16 %	E1	AC1	AW2	AR0	C3	**d**
BH12	**steering mode change**	Considered to be the same as steering													**d**
BH13	**slow/stop**	roading	failure to apply on demand	machine fails to stop - collision	bystander	S3	30 %	10 %	100 %	E1	AC1	AW2	AR2	C2	**c**
BH14	**transmission neutralize**	roading	uncommanded deactivation	machine moves into vehicle or bystander	bystander	S3	30 %	4 %	25 %	E0	AC1	AW2	AR3	C1	**a**
BH1-2	**engine speed**	considered to be the same as machine speed													**b**
BH9-11	**hoe arm extend out**	considered the same as uncommanded activation of the park brake													**c**
BH4-5		considered to be the same as arm out													
	loader auxiliary function	tools used on backhoe loaders were not considered to be hazardous. If tools are used similar to crawler or wheeled excavators than the MPL_r for those machines shall be used													**N/A**

[a] A car or larger vehicle would be a lower severity injury.

Table F.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
	loader coupler	no single failure to be hazardous													**N/A**

[a] A car or larger vehicle would be a lower severity injury.

F.2 Supporting explanation

F.2.1 Supporting explanations for dominant scenarios

BH1 – machine speed

H: Only hazardous when not at high idle - worse case in traffic. H = 40 %

P: See 5.2. P = 16 %.

AC: AC1 – brakes

AW: AW2

AR: AR3 – Applying brakes is a natural reaction and applying brake during the operation is considered underfoot

BH2 – machine speed

H: Only hazardous when wanting to stop or slow - worst case in traffic. H = 50 %

P: Rarely slowing to avoid hitting pedestrian. P = 10 %.

AC: AC1 – brakes

AW: AW2

AR: AR3 – Applying brakes is a natural reaction and applying brake during the operation is considered underfoot

BH3 – hoe boom lower

H: Hazardous for half of lash and unlash [(21,3 % × 2 %)/2], 90 % idle factor. H = 19 %

P: It is considered machine abuse to stand below boom, may be close when grabbing chains in lashing or unlashing. P = 2 %

AC: AC0

BH4 – hoe arm out

H and P: P×H value - see 5.9. P×H = 20 % × 10 % = 2 %

AC: AC0

BH5 – hoe arm out

H: Half of the proportion of lowering is underground (considered to be 10 % of total cycle) - another half at S2 (5 %). 90 % idle factor. H = 4,5 %

P: People should not be in this area but may be momentarily. P = 5 %.

AC: AC0

BH6 – hoe coupler engagement

H: Last 10 % of dump, 90 % idle factor. H = 10 % × 10 % × 90 % = 1 %

P: It is considered machine abuse to be standing near a load being dumped. P = 1 %.

AC: AC0

AW: AW2

AR: AR3

BH7 – hoe boom swing

H: See 5.5. Worst case considered was material handling from flatbed truck. 90 % idle factor. H = 21 % × 90 %= 19 %

P: Hitch and lift where traffic present in swing. Traffic rate (see 5.5.2), people there 5 % of the time and only dangerous for swing direction only 1 way (divide by 2). P = (17 % + 5 %) / 2 = 11 %

AC: AC0

BH8 – hoe boom swing

H: It is hazardous during the whole cycle, 90 % idle factor. H = 90 %

P: It is considered machine abuse for a person to be around the machine during truck loading. P = 2 %

AC: AC0

BH9 – hold still

H: Hazard present when the machine is travelling at higher speeds and not stopping. H = 50 %

P: Operator present throughout cycle. P = 100 %

AC: AC0

BH10 – hold still

H: Hazard present when the machine is travelling at higher speeds and not stopping. H = 50 %

P: Following vehicles should be traveling at the same speed as the machine, it is considered machine abuse to be following the machine within vehicle stopping distance. P = 5 %

AC: AC0

BH11 – hold still

H: Only hazardous for portions of tasks with loader in the air (boom lock installed) 20 %. 88 % of total maintenance. H = 18 %

P: See 5.8. Maintainer on machine for 70 % of task on smaller machine. P = 70 %.

AC: AC0

BH12 – steering

H: Only hazardous for all of time machine is on the road. H = 100 %

P: See 5.2. P = 16 %.

AC: AC1 – brakes

AW: AW2

AR: AR0

BH13 – slow/stop

H: Percentage of time slowing / stopping to avoid hitting pedestrian or vehicle. H = 10 %

P: Someone is present whenever machine is stopping to avoid hitting someone. P = 100 %.

AC: AC1 – park brake (steering may not always help avoiding collision)

AW: AW2

AR: AR2 – Operator needs to move hand to activate but is a natural response

BH14 – transmission neutralize

H: Time when machine is idle (20 %) during low speed manoeuvring (20 %). H = 20 % × 20 % = 4 %

P: Typical bystander rate in central / parking areas. P = 25 %.

AC: AC1 – brakes

AW: AW2

AR: AR3 – The brakes would be under foot and the machine moves slowly

F.2.2 Application use cases

Table F.2 — Application use case table

Application	Travel (including roading)	Loader - bucket, 4-in-1 Bucket	Loader work tools - sweepers, mulchers, snow blowers	Loader object handling	Hoe	Hoe work tools - hammer, compacting plate, auger	Hoe - object handling	Maintenance
Utility	30 %	30 %	20 %	20 %	70 %	30 %	20 %	5 %
Civil	30 %	20 %	20 %	15 %	70 %	40 %	15 %	5 %
Construction	20 %	40 %	20 %	10 %	50 %	20 %	15 %	5 %

F.2.3 Maintenance task breakdown

Table F.3 — Maintenance task breakdown

	Time (min/day)	% Maintenance time
parking brake test	2	11
clean windows	5	28
grease	5	28
transmission oil check	2,5	14
engine oil check	2,5	14
top up transmission oil	0,25	1
top up engine oil	0,25	1
troubleshooting	0,5	3

F.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table F.4 — Function dominant failure type matrix

Subsystem	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
machine speed		1	1		Activation is increase; release is decrease. Other failure types are less or not hazardous.
engine speed			1		Activation is increase; release is decrease. Other failure types are less or not hazardous.
direction change	1				Uncommanded change in direction is considered the same as uncommanded slow/stop. Other failure types considered the same as failure on demand.
loader raise					Less hazardous than loader lower
loader lower			1		Other failure types are less or not hazardous.
loader bucket dump			1		Other failure types are less or not hazardous.
loader bucket curl					Less hazardous than loader dump
loader quick coupler				1	Other failure types are less or not hazardous.
hoe boom swing			1		Failure to release on demand just as hazardous as uncommanded activation - both considered under uncommanded activation. Other failure types are less or not hazardous.
hoe boom raise					Less hazardous than boom lower
hoe boom lower			1		Other failure types are less or not hazardous.
hoe arm raise / out			1		Other failure types are less or not hazardous.
hoe arm lower / in					both in and out are hazardous - will consider both
hoe arm extend out			1		Other failure types are less or not hazardous.
hoe arm retract in					Less hazardous than out
hoe bucket dump			1		Other failure types are less or not hazardous.
hoe bucket curl					Less hazardous than hoe dump
hoe quick coupler				1	Other failure types are less or not hazardous.
loader auxiliary function			1		Other failure types are less or not hazardous.
hoe auxiliary function			1		Other failure types are less or not hazardous.
hoe side shift			1		Other failure types are less or not hazardous.
slow/stop	1				Uncommanded slow / slow stop considered under uncommanded Hold Still. Other failure types considered under failure to apply on demand or are less or not hazardous
hold still	1		1		Other failure types are less or not hazardous.
steering			1		All failure types are hazardous - considered all under uncommanded activation.
all wheel steering / crab steer			1		Uncommanded activation is more hazardous than failure on demand because the intention is to steer, but gets a different radius vs. the unexpected nature of uncommanded activation
stabilizer raise					Lower is more dangerous
stabilizer lower			1		Other failure types are less or not hazardous.

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

F.2.5 Notes and assumption

— Powered hand tools considered to not require anything of the machine control systems have not been considered in this assessment - flow rate settings are considered under loader auxiliary function.

— Implement lockout MPL_r is the same as the MPL_r of the function it is locking out.

— Uncommanded change in direction is considered to be the same as uncommanded park brake activation – sudden stop with no warning - MPL_r for this failure type from uncommanded slow/stop.

— Auxiliary functions are not assessed in this MCSSA. Due to the large number of possible tools that could be fitted, it is not possible to assess in a general sense. Machine functions based on tool combinations need to be assessed individually by the OEM, through the process outlined in ISO 19014-1.

— Uncommanded direction change, uncommanded slow/stop and uncommanded hold still are considered to be the same hazardous outcome – the machine would stop suddenly without warning to the operator or a person following behind the machine.

F.3 MPL_r mapped to SCS table

Table F.5 shows function-based MPL_r (see Table F.1) mapped to SCS per the results of the MCSSA for a backhoe loader. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table F.1 would also be mapped to these MPL_r

Table F.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
machine speed	uncommanded activation	**b**	throttle and speed gear control
	failure to release on demand		
machine direction	uncommanded activation	**c**	gear direction control
hoe boom up	uncommanded activation	**c**	hoe boom raise
hoe boom down	uncommanded activation	**c**	hoe boom lower
hoe boom offset	uncommanded activation	**c**	hoe boom offset
hoe arm in	uncommanded activation	**c**	hoe arm in
hoe arm out	uncommanded activation	**c**	hoe arm out
hoe tool dump	uncommanded activation	**c**	hoe tool dump
hoe tool curl	uncommanded activation	**c**	hoe tool curl
hoe auxiliary flow	Tools used on backhoe loaders were not considered to be hazardous. If tools are used similar to crawler or wheeled excavators than the MPL_r for those machines shall be used	**N/A**	hoe auxiliary flow
loader boom up	uncommanded activation	**c**	loader boom raise
loader boom down	uncommanded activation	**c**	loader boom lower
loader tool dump	uncommanded activation	**c**	loader tool dump
loader tool curl	uncommanded activation	**c**	loader tool curl
hoe coupler engagement	uncommanded deactivation	**b**	hoe coupler engagement
hoe swing/slew	uncommanded activation	**c**	hoe swing/slew
hold still	uncommanded activation	**c**	parking brakes
	failure to apply on demand		
stabilizers up	uncommanded activation	**c**	stabilizers up
stabilizers down	uncommanded activation	**c**	stabilizers lower
steering	uncommanded activation	**d**	steering
steering mode change	uncommanded activation	**d**	steering mode change
transmission neutralize	uncommanded deactivation	**a**	gear direction control
slow/stop	failure to apply on demand	**c**	service brakes

Table F.5 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
engine speed	uncommanded activation	**d**	throttle
hoe arm extend out	uncommanded activation	**c**	hoe arm extend out

Annex G
(normative)

Large wheel loaders equal to or greater than 24 000 kg performance level tables

G.1 Large wheel loaders equal to or greater than 24 000 kg

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables G.1 to G.5) or in Clause 5.

Table G.1 — MPL_r table for large wheel loaders equal to or greater than 24 000 kg

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
LW1	**machine speed**	travel	uncommanded activation	increased stopping distance causing higher than intended speed - off high wall	operator	S3	80 %	18 %	100 %	E2	AC1	AW3	AR3	C0	**b**
LW2		travel	uncommanded activation	collision - machine moves forward while stopped waiting	bystander	S3	80 %	5 %	100 %	E1	AC1	AW2	AR3	C1	
LW3		low to ground tool / dozing	uncommanded activation	machine fails to stop when pushing over edge – falls it is machine abuse to perform this task without additional measures in place	operator	S3	90 %	6 %	100 %	E1	AC1	AW2	AR3	C1	
LW13	**machine direction**	considered to be the same as uncommanded brake activation													**c**
LW4	**boom raise**	loading / unloading	uncommanded activation	contact with roof - potential for falling objects	operator	S1	90 %	79 %	100 %	E2	AC1	AW2	AR1	C3	**c**

Table G.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
LW5	**boom lower**	loading / unloading	uncommanded activation	boom hits truck being loaded	co-worker	S1	90 %	6 %	100 %	E1	AC0	N/A	N/A	C3	**b**
LW6		travel	uncommanded activation	Boom contacts ground, digs into ground, lifts front wheels (lost steering). Increased friction with ground, may act as dozer over high wall.	operator	S3	80 %	7 %	100 %	E1	AC1	AW2	AR3	C1	
LW7		maintenance	uncommanded activation	crushed feet	maintainer	S2	6 %	4 %	75 %	E0	AC0	N/A	N/A	C3	
LW13	**tool dump**	considered to be the same as uncommanded brake activation													**c**
LW16-17		same as auxiliary function													
LW4	**tool curl**	considered to be the same as boom raise													**c**
LW8	**hold still**	loading / unloading	uncommanded deactivation	operator out of cab - run away machine	bystander	S3	90 %	5 %	5 %	E0	AC0	N/A	N/A	C3	**c**
LW9		slow speed maneuvering	uncommanded deactivation	operator out of cab - run away machine	bystander	S3	6 %	5 %	50 %	E0	AC0	N/A	N/A	C3	
LW10	**steering**	travel	uncommanded activation	drive off high-wall	operator	S3	80 %	36 %	100 %	E2	AC1	AW2	AR2	C2	**d**
LW11		travel	uncommanded activation	collision	bystander	S3	80 %	50 %	5 %	E1	AC1	AW2	AR0	C3	
LW12	**transmission neutralize**	loading / unloading	uncommanded deactivation	collision	co-worker	S3	90 %	6 %	5 %	E0	AC1	AW2	AR3	C1	**a**

Table G.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
LW13	**slow/stop**	travel	uncommanded activation	machine skids toward high wall	operator	S3	80 %	7 %	100 %	E1	AC1	AW2	AR2	C2	**c**
LW14		travel	failure to apply on demand	machine goes off high wall	operator	S3	80 %	7 %	100 %	E1	AC1	AW2	AR2	C2	
LW15		low to ground	failure to apply on demand	machine fails to slow when pushing off edge - falls of edge	operator	S3	90 %	5 %	100 %	E1	AC1	AW2	AR2	C2	
LW16	**loader auxiliary function**	loading / unloading	uncommanded activation	load released, machine drives over the load - bottoms out seat	operator	S1	90 %	34 %	100 %	E2	AC0	N/A	N/A	C3	**c**
LW17		loading / unloading	uncommanded activation	load leaves machine hits pedestrian	bystander	S3	90 %	1 %	5 %	E0	AC0	N/A	N/A	C3	
	loader coupler	no single failure hazardous													
RD13	**powered access**	same as rigid frame trucks													**c**

G.2 Supporting explanation

G.2.1 Supporting explanations for dominant scenarios

LW1 – machine speed

H: On haul road, up to 80 % of time (block handling), high wall present up to 90 % of time, downhill 25 % (uphill not going fast enough for hazard to occur). H = 80 % × 90 % × 25 % = 18 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – brakes

AW: AW3 – Machine speed increases slowly – operator becomes aware before hazardous

AR: AR3 – Applying brakes is a natural reaction and applying brake while in operation is considered underfoot

LW2 – machine speed

H: Could be stopping to wait up to 5 % of the time. H = 5 %

P: Stopped by definition of waiting. P = 100 %

AC: AC1 – brakes

AW: AW2

AR: AR2

LW3 – machine speed

H: Only a hazard for last 1/8 or forward portion of cycle. 90 % idle factor. H = (50 % × 90 %) / 8 = 6 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – brakes

AW: AW2

AR: AR2

LW4 – boom raise

H: Whenever machine is not idle and not already raising boom (all but A1, A2 and C2). 90 % idle factor. H = 90 % × (1 - (25 % / 4) - (25 % / 8) - (25 % / 8)) = 79 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – key switch

AW: AW2

AR: AR1 – Turning machine off requires moving hand and is not a natural response

LW5 – boom lower

H: Only applicable during unloading (25 %/4), 90 % idle factor. H = (25 % / 4) × 90 % = 6 %

P: Co-worker always in truck for this use case. P = 100 %

AC: AC0

LW6 – boom lower

H: Percentage of time machine travels with bucket / forks flat / loading position, downhill 25 % (block carrying), Curve such that machine would head to high wall 40 %, high wall present 90 %, time on haul road 80 % (block carrying). H = 25 % × 40 % × 90 % × 80 % = 7 %

P: Operator is always in cab for this use case. P = 100 %

AC: AC1 – key switch

AW: AW2

AR: AR3 – brakes (lost drive torque would rapidly stop machine), tilt bucket back

LW7 – boom lower

H: All tasks boom should be on ground except troubleshooting. H = 4 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

LW8 – hold still

H: Reduced maximum idle time by 90 % to account for the times the operator does not put work tool on ground – only when stopped with load in bucket. H = 5 %

P: Light vehicle traffic rate. P = 5 %

AC: AC0

LW9 – hold still

H: Reduced maximum idle time by 90 % to account for the times the operator does not put work tool on ground – only when stopped with load in bucket. H = 5 %

P: Light vehicle traffic rate in park up / central area. P = 50 %

AC: AC0

LW10 – steering

H: Percentage of failures in dangerous direction 50 %, high wall present 90 %, time on haul road (block handling) 80 %. H = 50 % × 90 % × 80 % = 36 %

P: Operator always in cab for this use case. P = 100 %

AC: AC1 – berm

AW: AW2

AR: AR2 – Berm is not always effective

LW11 – steering

H: Failures only hazardous in one direction. H = 50 %

P: Light vehicle traffic rate. P = 5 %

AC: AC1 – brakes

AW: AW2

AR: AR0

LW12 – transmission neutralize

H: Only applicable in unloading, 90 % idle factor. H = (25 % / 4) × 90 % = 6 %

P: Based on being material handled, co-worker doing this task would not position themselves in hazard zone. This is supported by the limited visibility it is not practical for them to be in that area (immediately in front of or behind the machine). P = 5 %

AC: AC1 – brakes

AW: AW2

AR: AR3

LW13 – slow/stop

H: On haul road up to 80 % of time (block handling), High wall present up to 90 % of time, downhill 25 % (uphill not going fast enough for hazard to occur), on curve such that machine will head towards hazard 40 %. H = 80 % × 90 % × 25 % × 40 % = 7 %

P: Operator always in cab for this use case. P = 100 %

AC: AC1 – berm

AW: AW2

AR: AR2 – Berm is not always effective

LW14 – slow/stop

H: On haul road up to 80 % of time (block handling), high wall present up to 90 % of time, downhill 25 % (uphill not going fast enough for hazard to occur), on curve such that machine will head towards hazard 40 %. H = 80 % × 90 % × 25 % × 40 % = 7 %

P: Operator always in cab for this use case. P = 100 %

AC: AC1 – park brake (steering may not always help avoiding collision)

AW: AW2

AR: AR2 – Operator needs to move hand to activate but is a natural response

LW15 – slow/stop

H: Last 10 % of the push cycle (50 % of total cycle), 90 % idle factor H = 10 % × 50 % × 90 % = 5 %

P: Operator always in cab for this use case. P = 100 %

AC: AC1 – park brake

AW: AW2

AR: AR2 – Operator needs to move hand to activate but is a natural response

LW16 – auxiliary flow

H: Only when loaded moving forward - C3, D and A1, 90 % idle factor. H = (25 % + (25 % / 4) + (25 % / 4)) × 0,9 = 34 %

P: Operator always in cab for this use case. P = 100 %

AC: AC0

LW17 – auxiliary flow

H: Person guiding the unloading process / machine placing of load on truck. Last 10 % of A1, unloading. 90 % idle factor. H = (10 % × (25 % / 4) × 90 %) = 1 %

P: Based on being material handled, co-worker doing this task would not position themselves in hazard zone. This is supported by the limited visibility, it is not practical for them to be in that area (immediately in front of the machine). P = 5 %

AC: AC0

G.2.2 Application use cases

Table G.2 — Application use case table

Application	Loading/unloading (forks, hydraulic tools)	Bucket v-cycle (including truck / train loading, hopper)	Travel mode (loaded / unloaded)	Low speed maneuvering / startup / parking	Low to ground tool / dozing	Maintenance (machine running) service repair
Open - surface	90 %	90 %	80 %	6 %	90 %	6 %
Confined	90 %	90 %	80 %	6 %	90 %	6 %

G.2.3 Maintenance task breakdown

Table G.3 — Maintenance task breakdown

	Time (min/day)	% Maintenance time
daily walk around	10	10
wash camera	4	4
refuel	20	20
oil sampling	4,3	4
GET replacement	1,4	1
wash	4	0
lube / grease	38,3	39
troubleshooting	4,3	4
window wash	10	10
install articulation lock	4	4
brake testing	2	2

G.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table G.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
acceleration / propel			1		Failure to release on demand is no more dangerous than rate greater than command. Other failure types are less or not hazardous.
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

Table G.4 *(continued)*

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
direction control (F / R)	1				Uncommanded activation results in an uncommanded stop (considered under uncommanded slow/stop) primarily before starting to change direction thus has much greater response time and is less hazardous. Failure to apply on demand includes failure to change direction or changing into wrong direction.
neutralize				1	Moving into or staying in N is not considered dangerous. Uncommanded moving out of N is more dangerous than failing to neutralize because of brakes and other systems being available.
boom lift			1		Failure to move boom not considered dangerous. Other failure types are considered less hazardous.
boom lower			1		Failure to move boom not considered dangerous. Other failure types are considered less hazardous.
tool curl			1		Failure to move tool not considered dangerous. Other failure types are considered less hazardous.
tool dump			1		Failure to move tool not considered dangerous. Other failure types are considered less hazardous.
boom float					Considered the same as boom lower
auxiliary flow			1		Other failure types are considered less or not hazardous.
slow/stop	1		1		Other failure types considered under failure to apply on demand are less or not hazardous.
hold still				1	Uncommanded deactivation covers failure on demand. Other failure types are considered less or not hazardous.
steering	1		1		All failure types considered under failure to apply on demand and uncommanded activation

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

G.2.5 Notes and assumptions

— Assumed that no single failure can cause an uncommanded start.

— For the purpose of this assessment, activation means it starts from zero, deactivation means it goes to zero, changes in rate are covered by other failure types.

— Because bystanders are almost never around these machines the co-worker rows represent co-workers in a machine and the bystander rows consider a co-worker on foot or in a light vehicle.

— For loading / unloading, the travel section is not less than 25 % in each direction.

— Assumed that berms are present and sized appropriately, appropriate traffic controls are in space and roads are built wide enough for anticipated traffic.

— Slow speed manoeuvring includes transport (being loaded and unloaded from a truck).

— For dozing off an edge, recommended practice is to push a rear pile to push a front pile off to limit operator exposure to the high wall edge.

— For maintenance assume appropriate lockouts are in place.

— Maintenance tasks are only those that are reasonably foreseeable that could be done with the engine on.

— Uncommanded direction change, uncommanded slow/stop and uncommanded hold still are considered to be the same hazardous outcome – the machine would stop suddenly without warning to the operator or a person following behind the machine.

G.3 MPL_r mapped to SCS table

Table G.5 shows function-based MPL_r (see Table G.1) mapped to SCS per the results of the MCSSA for a large wheel loader equal to or greater than 24 000 kg. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table G.1 would also be mapped to these MPL_r.

Table G.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
machine speed	uncommanded activation	**b**	throttle and speed gear control
machine direction	uncommanded activation	**c**	gear direction control
boom raise	uncommanded activation	**c**	boom raise
boom lower	uncommanded activation	**b**	boom lower
tool dump	uncommanded activation	**c**	tool dump
tool curl	uncommanded activation	**c**	tool curl
hold still	uncommanded deactivation	**c**	parking brakes
steering	uncommanded activation	**d**	steering
transmission neutralize	uncommanded deactivation	**a**	gear direction control
slow/stop	uncommanded activation	**c**	service brakes
	failure to apply on demand	**c**	
loader auxiliary function	Uncommanded Activation	**c**	Loader Auxiliary Function
loader coupler	Multiple failures to be hazardous for known designs in working group	**N/A**	loader coupler

Annex H
(normative)

Medium, small and compact wheel loaders less than 24 000 kg performance level tables

H.1 Medium, small and compact wheel loaders less than 24 000 kg

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables H.1 to H.4) or in Clause 5.

Table H.1 — MPL_r table for medium, small and compact wheel loaders less than 24 000 kg

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
WL1	**machine speed**	loading / unloading	uncommanded activation	increased stopping distance causing higher than intended speed - collision	co-worker	S3	90 %	7 %	20 %	E1	AC1	AW2	AR3	C1	**b**
WL2		bucket	failure to release on demand	delayed stopping time - collision	co-worker	S3	90 %	36 %	20 %	E1	AC1	AW2	AR3	C1	
WL3		roading / traveling	failure to release on demand	increased stopping distance causing higher than intended speed - collision	bystander	S3	30 %	10 %	100 %	E1	AC1	AW2	AR3	C1	
WL4	**machine direction**	roading	uncommanded activation	machine stops without command – trailing vehicle or motorcycle collides with machine	bystander	S3	30 %	50 %	5 %	E0	AC0	N/A	N/A	C3	**c**
WL5		roading	uncommanded activation	machine stops without command - collision with vehicle following	operator	S1	30 %	50 %	100 %	E2	AC0	N/A	N/A	C3	
WL6	**boom raise**	loading / unloading	uncommanded activation	machine contacts overhead infrastructure	co-worker	S3	90 %	36 %	5 %	E1	AC1	AW1	AR3	C2	**c**

[a] Auxiliary flow is considered to be the same as large wheel loader. Tines should be tilted back. Machine should not be driven towards people.

This assessment assumes that wheel loaders have mechanical or hydrostatic drive with articulation steering, such that an increase in machine speed would cause an increase in directional velocity. If this is not true, the scoring for steering, machine speed, machine direction and slow/stop for skid steers shall be used.

Table H.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
WL7	**boom lower**	loading / unloading	uncommanded activation	crushed by protruding load	co-worker	S3	90 %	6 %	1 %	E0	AC0	N/A	N/A	C3	**c**
WL8		lifting	uncommanded activation	crushed by protruding load - only part of body under lifted load	co-worker	S2	50 %	11 %	100 %	E1	AC0	N/A	N/A	C3	
WL4-5	**tool dump**	considered to be the same as machine direction change													**c**
WL6	**tool curl**	considered to be the same as boom raise													**c**
LW8 –9	**hold still**	failure to apply on demand considered to be the same as large wheel loaders													**c**
WL4 –5		uncommanded activation considered to be the same as machine direction change													
WL9	**steering**	roading	uncommanded activation	collision	bystander	S3	30 %	100 %	16 %	E1	AC1	AW2	AR0	C3	**d**
LW12	**transmission neutralize**	considered the same as Large Wheel Loader													**a**
WL10	**slow/stop**	loading / unloading	failure to apply on demand	machine fails to stop - collision	co-worker	S3	90 %	10 %	100 %	E1	AC1	AW2	AR2	C2	**c**
WL4 –5		uncommanded activation considered to be the same as machine direction change													
WL11		bucket	failure to apply on demand	machine fails to stop - collision	bystander	S3	90 %	10 %	50 %	E1	AC1	AW2	AR2	C2	
WL12		travel	failure to apply on demand	machine fails to stop - collision	bystander	S3	30 %	10 %	100 %	E1	AC1	AW2	AR2	C2	
LW16-17	**loader auxiliary function** [a]	considered the same as large wheel loader													**c**
	loader coupler	no single failure hazardous – not a safety function													

[a] Auxiliary flow is considered to be the same as large wheel loader. Tines should be tilted back. Machine should not be driven towards people.

This assessment assumes that wheel loaders have mechanical or hydrostatic drive with articulation steering, such that an increase in machine speed would cause an increase in directional velocity. If this is not true, the scoring for steering, machine speed, machine direction and slow/stop for skid steers shall be used.

H.2 Supporting explanation

H.2.1 Supporting explanations for dominant scenarios

WL1 – machine speed

H: Only hazardous when trying to stop - last 10 % of A1, A2, C1 and C2. Added 5 % for other times may need to stop. 90 % idle factor. H = (((10 % × (25 % × 25 % × 4)) + 5 %) × 90 %) = 7 %

P: Time when trying to stop, to avoid hitting person. P = 20 %

AC: AC1 – brakes

AW: AW2

AR: AR3 – Applying brakes is a natural reaction and applying brake during the operation is considered underfoot

WL2 – machine speed

H: Only hazardous when in reverse (40 %) – See Table 4. 90 % idle factor. H = 40 × 90 % = 36 %

P: Time when trying to stop, to avoid hitting person. P = 20 %

AC: AC1 – brakes

AW: AW2

AR: AR3 – Applying brakes is a natural reaction and applying brake during the operation is considered underfoot

WL3 – machine speed

H: Only hazardous when stopping to avoid collision with vehicle or pedestrian. H = 10 %

P: Bystander present whenever trying to avoid collision. P = 100 %

AC: AC1 – brakes

AW: AW2

AR: AR3 – Applying brakes is a natural reaction and applying brake during the operation is considered underfoot

WL4 – machine direction

H: Hazardous when not stopping or slowing. H = 50 %

P: Trailing vehicle should be maintaining safe distance but may momentarily be closer. P = 5 %

AC: AC0

WL5 – machine direction

H: Hazardous when not stopping or slowing. H = 50 %

P: Operator present for during the whole cycle. P = 100 %

AC: AC0

WL6 – boom raise

H: Only hazardous when in reverse (40 %) – better awareness in forward. 90 % idle factor. H = 40 × 90 % = 36 %

P: People should not be close to the machine in tight confines. P = 5 %

AC: AC1 – brakes

AW: AW1 – Operator looking behind machine, not in front

AR: AR3 – Removing foot from throttle would stop boom motion

WL7 – boom lower

H: Only applicable during unloading (25 %/4), 90 % idle factor. H = (25 % / 4) × 90 % = 6 %

P: It is considered machine abuse to be under lifted load but there may not be anywhere else to stand in congested work area. P = 1 %

AC: AC0

WL8 – boom lower

H: Only when positioning load (25 %/4), 90 % idle factor. H = 2 × (25 % / 4) × 90 % = 11 %

P: Co-worker present for all of this portion of cycle. P = 100 %

AC: AC0

WL9 – steering

H: Hazard exists throughout cycle. H = 100 %

P: See 5.2. P = 16 %

AC: AC1 - brakes

AW: AW2

AR: AR0

WL10 – slow/stop

H: Percentage of time slowing / stopping to avoid hitting pedestrian or vehicle. H = 10 %

P: Co-worker present whenever trying to avoid collision with co-worker. P = 100 %

AC: AC1 – park brake (steering may not always help avoiding collision)

AW: AW2

AR: AR2 – Operator needs to move hand to activate but is a natural response

WL11 – slow/stop

H: Percentage of time slowing / stopping to avoid hitting pedestrian or vehicle. H = 10 %

P: Machine exits work area. See 5.4.3. P = 50 %

AC: AC1 – park brake (steering may not always help avoiding collision)

AW: AW2

AR: AR2 – Operator needs to move hand to activate but is a natural response

WL12 – slow/stop

H: Percentage of time slowing / stopping to avoid hitting pedestrian or vehicle. H = 10 %

P: Co-worker present whenever trying to avoid collision with co-worker. P = 100 %

AC: AC1 – park brake (steering may not always help avoiding collision)

AW: AW2

AR: AR2 – Operator needs to move hand to activate but is a natural response

H.2.2 Application use cases

Table H.2 — Application use case table

Application	Loading / unloading (forks, hydraulic tools)	Bucket v-cycle (including truck / train loading, hopper)	Roading (loaded / unloaded)	Transport (loading and unloading from trailer)	Lifting	Stockpiling	Low to ground tool / dozing	Maintenance (machine running) service repair
Open - Surface	90 %	90 %	30 %	5 %	25 %	50 %	90 %	3 %
Confined	90 %	90 %	0 %	1 %	5 %	10 %	50 %	3 %

H.2.3 Maintenance task breakdown

Maintenance tasks are not found to dominate any scoring.

H.2.4 Function-dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table H.3 — Function-dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
machine speed		1	1	1	Stopping machine on railroad tracks, under mining wall considered worksite responsibility. Failure to apply on demand is not considered hazardous.
machine direction	1		1		Other failure types are less or not hazardous.
transmission neutralize					Same as large wheel loader
boom raise					Not more dangerous than lower
boom lower			1		Other failure types are less or not hazardous.
tool curl					Not more dangerous than lower
tool dump			1		Other failure types are less or not hazardous.
quick coupler engagement				1	No single failure hazardous
slow/stop	1		1		Other failure types are less or not hazardous or are considered under failure to apply on demand.
hold still	1		1		Other failure types are less or not hazardous.
steering			1		All failure types hazardous and are considered in uncommanded steering.

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

H.2.5 Notes and assumptions

— Third and fourth function (additional auxiliary hydraulic oil supply function) to be assessed by machine manufacturer as potential tools are risk assessed.

— Ground level shutdowns are not fitted on all manufacturers - excluded from analysis.

— Assumed coupler compliance to ISO 13031.

— Operator is assessed as an operator until they are off the machine completely, then they are considered a bystander or co-worker.

— On lifting use case assume guide ropes are long enough to keep co-worker out of harm's way.

— Assume truck being loaded is stationary, it could be pickup, rigid frame highway or off highway, ADT or semi-trailer.

— It is considered machine abuse for anyone to be standing between loader and rock pile/truck.

— Railroad applications are excluded from this analysis.

— Tool close to ground, stock piling and transport were reviewed and determined not to yield any higher scores than the use cases already assessed.

— Assume greasing can be done without the maintainer getting into the hazard zone.

— Uncommanded direction change, uncommanded slow/stop and uncommanded hold still are considered to be the same hazardous outcome – the machine would stop suddenly without warning to the operator or a person following behind the machine.

H.3 MPL_r mapped to SCS table

Table H.4 shows function-based MPL_r (see Table H.1) mapped to SCS per the results of the MCSSA for a medium, small and compact wheel loader less than 24 000 kg. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table H.1 would also be mapped to these MPL_r.

Table H.4 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
machine speed	uncommanded activation	**b**	throttle and speed gear control
	failure to release on demand		
machine direction	uncommanded activation	**c**	gear direction control
boom raise	uncommanded activation	**c**	boom raise
boom lower	uncommanded activation	**c**	boom lower
tool dump	uncommanded activation	**c**	tool dump
tool curl	uncommanded activation	**c**	tool curl
hold still	failure to apply on demand	**c**	parking brakes
	uncommanded activation		
steering	uncommanded activation	**d**	steering
transmission neutralize	uncommanded deactivation	**a**	gear direction control
slow/stop	failure to apply on demand	**c**	service brakes
	uncommanded activation		
loader auxiliary function	uncommanded activation	**c**	loader auxiliary function
loader coupler	multiple failures to be hazardous for known designs in working group	**N/A**	loader coupler

Annex I
(normative)

Wheeled and crawler skid steer loaders performance level tables

I.1 Wheeled and crawler skid steer loaders

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables I.1 to I.5) or in Clause 5.

Table I.1 — MPL_r table for wheeled and crawler skid steer loaders

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
SSL7-8	**machine propel [a] (speed, direction, steer)**	Considered to be the same as failure to stop													**c**
	engine speed	No single failure hazardous – not a safety function													
SSL1	**boom raise**	maintenance	uncommanded activation	boom raises while accessing / egressing the machine	operator	S3	2 %	25 %	100 %	E0	AC0	N/A	N/A	C3	**c**
SSL2	**boom lower**	loading / unloading	uncommanded activation	boom lowers while accessing / egressing the machine	operator	S3	2 %	25 %	1 %	E0	AC0	N/A	N/A	C3	**c**
SSL3	**tool dump**	loading / unloading	uncommanded activation	load dumped on co-worker - whole body would not be under load	co-worker	S2	50 %	54 %	15 %	E1	AC0	N/A	N/A	C3	**c**
SSL4	**tool curl**	low to ground	uncommanded activation	trencher raises out of ground - co-worker gets caught in chain	co-worker	S3	75 %	20 %	5 %	E0	AC1	AW2	AR1	C3	**c**
This assessment assumes that skid steers have differential drive, such that an increase in machine speed would cause a machine to turn, not increase in directional velocity. If this is not true, the scoring for steering, machine speed, machine direction and slow/stop for wheel loaders shall be used.															

Table I.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
SSL5	**hold still**	bucket work	failure to apply on demand	machine rolls away (creeps away)	co-worker	S3	50 %	50 %	20 %	E1	AC1	AW3	AR3	C0	**a**
SSL6		low to ground	failure to apply on demand	machine rolls away (creeps away)	co-worker	S3	90 %	50 %	5 %	E1	AC1	AW3	AR3	C0	
	function map change	considered to be the same as whatever functions are being switched													
	offboard power supply	no single failure hazardous – not a safety function													
SSL7	**slow/stop**	bucket work	failure to apply on demand	machine fails to stop - collision	co-worker	S3	50 %	14 %	100 %	E1	AC1	AW2	AR2	C2	**c**
SSL8		demolition	failure to apply on demand	fails to stop when putting material down shoot or elevator shaft	operator	S3	50 %	1 %	100 %	E0	AC0	N/A	N/A	C3	
SSL9		travel / roading	uncommanded activation	machine stops without command - collision with vehicle following	operator	S1	30 %	25 %	100 %	E1	AC0	N/A	N/A	C3	**b**
SSL10		travel / roading	uncommanded activation	machine stops without command – trailing vehicle or motorcycle collides with machine	bystander	S2	30 %	50 %	5 %	E0	AC0	N/A	N/A	C3	

This assessment assumes that skid steers have differential drive, such that an increase in machine speed would cause a machine to turn, not increase in directional velocity. If this is not true, the scoring for steering, machine speed, machine direction and slow/stop for wheel loaders shall be used.

Table I.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person group exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
SSL11	**loader auxiliary function**	maintenance	uncommanded activation	entanglement in tool	maintainer	S3	5 %	6 %	70 %	E0	AC0	N/A	N/A	C3	**c**
SSL12		low to ground	uncommanded activation	entanglement in tool	co-worker	S3	75 %	2 %	50 %	E0	AC0	N/A	N/A	C3	
SSL13	**loader coupler**	off the ground work tool	uncommanded release	auger detaches at ground engagement - spins around and enters cab	operator	S2	25 %	1 %	100 %	E0	AC0	N/A	N/A	C3	**b**
SSL14		off the ground work tool	uncommanded release	auger detaches at ground engagement - spins around and hits co-worker	co-worker	S2	25 %	1 %	5 %	E0	AC0	N/A	N/A	C3	
This assessment assumes that skid steers have differential drive, such that an increase in machine speed would cause a machine to turn, not increase in directional velocity. If this is not true, the scoring for steering, machine speed, machine direction and slow/stop for wheel loaders shall be used.															

I.2 Supporting explanation

I.2.1 Supporting explanations for dominant scenarios

SSL1 – boom raise

A: Operator gets in or out of the machine 8 times an hour, takes 8 s. A = 64 s / 3 600 s = 2 %

H: Only while passing behind the implement. H = 25 %

P: Operator always present for this task. P = 100 %

AC: AC0

SSL2 – boom lower

A: Operator gets in or out of the machine 8 times an hour, takes 8 s. A = 64 s/ 3 600 s = 2 %

H: Only while passing behind the implement. H = 25 %

P: It is considered machine abuse to enter/exit the machine with the boom up without having it supported – would only be during emergency situations. P = 1 %

AC: AC0

SSL3 – tool dump

H: Short cycle worst case, portion "A" - if loading by hand or D if emptying by hand. Could be up to 60 %. 90 % idle factor. H = 54 %

P: Person would only be present when loading or emptying bucket. P = 15 %

AC: AC0

SSL4 – tool curl

H: Anytime trencher is in the ground (90 %), could be using a trencher up to 25 % - would get dedicated trencher in for more than that. 90 % idle factor. H =90 % × 25 % × 90 % = 20 %

P: People should not be in the area but may momentarily be while checking. P = 5 %

AC: AC1 – Turn machine off

AW: AW2

AR: AR1 – Shutting machine down may not be a natural reaction

SSL5 – hold still

H: Maximum idle time (50 %). H = 50 %

P: Person standing around the machine during landscaping. P = 20 %

AC: AC1 – Turn machine off

AW: AW3 – Operator would detect creep while exiting the machine

AR: AR3 – Tool should be on the ground

SSL6 – hold still

H: Maximum idle time (50 %). H = 50 %

P: Person standing around the machine during snow removal. P = 20 %

AC: AC1 – Turn machine off

AW: AW3 – Operator would detect creep while exiting the machine

AR: AR3 – Tool should be on the ground

SSL7 – slow/stop

H × P: Hazardous during all of A and D. 10 % of other segments. P at A is 60 %. P at D is 1 %. 90 % idle factor. H × P = [(12,5 % × 60 %) +(12,5 % × 1 %) +(75 % × 10 %)] × 90 % = 14 %

AC: AC1 – park brake (steering may not always help avoiding collision)

AW: AW2

AR: AR2 – Operator needs to move hand to activate but is a natural response

SSL8 – slow/stop

H: Last 1/8th of D. Idle factor 90 %. H = (1/8 × 1/8) × 90 % = 1 %

P: Operator always present for this task. P = 100 %

AC: AC1 – park brake (steering may not always help avoiding collision)

AW: AW2

AR: AR2 – Operator needs to move hand to activate but is a natural response

SSL9 – slow/stop

H: Only hazardous when car following. H = 25 %

P: Operator present for during the whole cycle. P = 100 %

AC: AC0

SSL10 – slow/stop

H: Hazardous when not stopping or slowing. H = 50 %

P: Trailing vehicle should be maintaining a safe distance but may momentarily be closer. P = 5 %

AC: AC0

SSL11 – auxiliary flow

H: 10 % of daily inspection, 10 % washing, 10 % of windows / camera / mirror clean and all of troubleshooting and refill window washer. H = (10 % × 22 %) +(10 % × 1 %) +(10 % × 22 %) + 1 %+ 1 % = 6 %

P: See 5.8. Maintainer is on machine for 70 % of the task on the smaller machine. P = 70 %.

AC: AC0

SSL12 – auxiliary flow

H: Only hazardous when tool is not in the ground / rotating parts exposed and not being used or hooking tool up (5 %). 90 % idle factor. Tool could be used up to 5 % of time. H = 5 % × 90 % × 5 % = 2 %

P: Could be guiding tool to work point engagement up to 50 % of the time. P = 50 %

AC: AC0

SSL13 – coupler engagement

H: Only during auger engagement with ground and first few inches (15 %). 90 % idle factor. Tool used up to (5 %). H = 15 % × 90 % × 5 % = 1 %

P: Operator present throughout cycle. P = 100 %

AC: AC0

SSL14 – coupler engagement

H: Only during auger engagement with ground and first few inches (15 %). 90 % idle factor. Tool used up to (5 %). H = 15 % × 90 % × 5 % = 1 %

P: Should not be that close, but may be momentarily to remove spoil, etc. P = 5 %

AC: AC0

I.2.2 Application use cases

Table I.2 — Application use case table

Application	Travel	Bucket work (e.g. v-cycle, truckloading)	Low to ground work tool	Material handling (e.g. forks, grapple)	Off the ground work tool	Power supply (operator not in cab)	Transport	Maintenance
Construction	10 %	50 %	75 %	20 %	25 %	5 %	10 %	5 %
Landscaping	20 %	50 %	75 %	30 %	15 %	2 %	10 %	5 %
Civil (snow removal, street sweeping)	30 %	50 %	90 %	5 %	5 %	2 %	10 %	5 %
Agriculture	30 %	50 %	5 %	50 %	5 %	2 %	2 %	5 %
Industrial (waste, conveyer clean-up, factory)	10 %	60 %	25 %	25 %	5 %	5 %	2 %	5 %
Demolition	10 %	50 %	30 %	50 %	50 %	2 %	5 %	5 %
Forestry	30 %	10 %	10 %	20 %	90 %	2 %	10 %	5 %

I.2.3 Maintenance task breakdown

Table I.3 — Maintenance task breakdown

	Time (min/day)	% Maintenance time
daily inspection	5,0	22 %
refuel / DEF	2,0	9 %
lube / greasing	2,0	9 %
tire pressure check / top up / track tension	2,0	9 %
wash	0,3	1 %
oil sample	0,5	2 %
clean windows and mirrors, cameras	5,0	22 %
troubleshooting	1,0	1 %
clean cooling package (waste application)	4,0	17 %
refill window washer	0,1	1 %
flash / calibrations	1,0	1 %

I.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table I.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
machine propel (direction, steering, speed)		1	1		Other failure types are less or not hazardous.
engine speed			1		Other failure types are less or not hazardous.
boom raise			1		Other failure types are less or not hazardous.
boom lower			1		Other failure types are less or not hazardous.
tool dump			1		Other failure types are less or not hazardous.
tool curl			1		Other failure types are less or not hazardous.
auxiliary flow			1		Other failure types are less or not hazardous.
quick coupler engagement				1	Other failure types are less or not hazardous.
slow/stop	1		1		Other failure types are less or not hazardous.
hold still	1				Failure on demand and uncommanded release are considered the same. Other failure types are less or not hazardous.
shutdown	1				Not a hazard
off board power supply			1		Other failure types are less or not hazardous.
function map change			1		Considered the same as the failure type the function controls

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

I.2.5 Notes and assumptions

— This assessment does not consider the hazards unique to single boom or telescopic boom skid steer machines.

— For skid steer machines propel covers direction control (L, R, F, R) and engine speed as control magnitude.

— Considered tool change and found it to be very similar, but no worse than hazards associated with accessing and egressing the cab (S, E and C).

— Uncommanded direction change, uncommanded slow/stop and uncommanded hold still are considered to be the same hazardous outcome – the machine would stop suddenly without warning to the operator or a person following behind the machine.

— Uncommanded slow/stop hazards have been scored lower than other machines due to the lower speeds (less than 20 km/h), smaller size and different geometry.

— Considered the hazard of boom raise while operator and maintainer are accessing machine together.

I.3 MPL_r mapped to SCS table

Table I.5 shows function-based MPL_r (see Table I.1) mapped to SCS per the results of the MCSSA for a wheeled or crawler skid steer loader. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table I.1 would also be mapped to these MPL_r.

Table I.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
machine propel (speed, direction, steer)	uncommanded activation	**c**	propel
engine speed	multiple failures to be hazardous	**N/A**	throttle
boom raise	uncommanded activation	**c**	boom raise
boom lower	uncommanded activation	**c**	boom lower
tool dump	uncommanded activation	**c**	tool dump
tool curl	uncommanded activation	**c**	tool curl
hold still	failure to apply on demand	**a**	parking brakes
function map change	considered to be the same as whatever functions are being switched		function map change
slow/stop	failure to apply on demand	**c**	service brakes
	uncommanded activation	**b**	
loader auxiliary function	uncommanded activation	**c**	loader auxiliary function
loader coupler	uncommanded release	**b**	loader coupler
offboard power supply	multiple failures to be dangerous	**N/A**	offboard power supply

Annex J
(normative)

Landfill compactor performance level tables

J.1 Landfill compactors

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables J.1 to J.5) or in Clause 5.

Table J.1 — MPL_r table for landfill compactors

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CO1	**machine speed**	compaction	uncommanded activation	machine overshoots intended compaction path - collision - hystat	bystander	S3	90 %	9 %	5 %	E0	AC0	N/A	N/A	C3	**c**
CO1	**engine speed**	considered to be the same as machine speed													**c**
CO1	**machine direction**	considered to be the same as machine speed													**c**
CO1	**neutralize transmission**	considered to be the same as machine speed/direction													**c**
CO2	**blade lower**	maintenance	uncommanded activation	crushed foot	maintainer	S2	5 %	10 %	75 %	E0	AC0	N/A	N/A	C3	**b**
CO2	**blade raise**	considered to be the same as blade lower													**b**
CO2	**blade tilt right / left**	considered to be the same as blade lower													**b**
CO3	**slow/stop**	compaction	failure to apply on demand	machine overshoots intended compaction path - collision	co-worker	S3	90 %	9 %	5 %	E0	AC1	AW2	AR2	C2	**b**
CO4		travel	failure to apply on demand	machine fails to stop - collision	co-worker	S3	15 %	9 %	25 %	E0	AC1	AW2	AR2	C2	
CO5	**hold still**	slow speed maneuvering	failure to apply on demand	machine rolls away - collision	co-worker	S3	5 %	75 %	25 %	E0	AC0	N/A	N/A	C3	**c**

Table J.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CO6	**steering**	travel	uncommanded activation	crosses onto other side of access road	co-worker	S3	15 %	50 %	5 %	E0	AC0	N/A	N/A	C3	**c**
CO7		maintenance	uncommanded activation	crushed in articulation zone	maintainer	S3	5 %	8 %	75 %	E0	AC0	N/A	N/A	C3	

J.2 Supporting explanation

J.2.1 Supporting explanations for dominant scenarios

CO1 – machine speed

H: Only hazardous at the points where preparing to change direction or stop – 10 %. 90 % idle factor. H = (10 % × 90 %) = 9 %

P: Rare for people to be in the area. P = 5 %

AC: AC0

CO2 – blade lower

H: 10 % of wash, 10 % of walk around, 75 % grease, 100 % troubleshoot. H = (10 % × 14 %) + (10 % × 24 %) + (75 % × 5 %) + 2 % = 10 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CO3 – slow/stop

H: Only hazardous at the points where preparing to change direction or stop – 10 %. 90 % idle factor. H = (10 % × 90 %) = 9 %

P: Rare for people to be in the area. P = 5 %

AC: AC1 – parking brake

AW: AW2

AR: AR2

CO4 – slow/stop

H: Only hazardous at the points where preparing to change direction or stop – 10 %. 90 % idle factor. H = (10 % × 90 %) = 9 %

P: Typical bystander rate in central / parking areas. P = 25 %

AC: AC1 – parking brake

AW: AW2

AR: AR2

CO5 – hold still

H: Machine could be idle up to 75 % of the time

P: Typical bystander rate in central / parking areas. P = 25 %

AC: AC0

CO6 – steering

H: Only hazardous in one direction – 50 %

P: Not normally travelling on access road. P = 5 %

AC: AC0

CO7 – steering

H: 10 % of refuel, 10 % walk around, and all of articulation lock install. H = (10 % × 36 %) + (10 % × 24 %) + 2 % = 8 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

J.2.2 Application use cases

Table J.2 — Application use case table

Application	Compaction	Travel	Slow speed manoeuvring	Dozing	Maintenance
Landfill compaction	90 %	15 %	5 %	25 %	5 %
Soil rolling	90 %	15 %	5 %	20 %	5 %

J.2.3 Maintenance task breakdown

Table J.3 — Maintenance task breakdown

	Time (min/ day)	% Maintenance time
wash	6,0	14 %
refuel	15,0	36 %
daily inspection	10,0	24 %
camera clean	3,0	7 %
oil sample	3,0	7 %
grease	2,0	5 %
troubleshooting	1,0	2 %
window wash	1,0	2 %
articulation lock install	1,0	2 %

J.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table J.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
machine speed			1		Other failure types are less or not hazardous.
machine direction	1				Other failure types are less or not hazardous.
engine speed			1		Other failure types are less or not hazardous.
neutralize transmission	1				Other failure types are less or not hazardous.
blade lower			1		Other failure types are less or not hazardous.
slow/stop	1		1		Other failure types are less or not hazardous.
hold still	1				Other failure types are less or not hazardous.
steering			1		Other failure types are less or not hazardous.
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

J.2.5 Notes and assumptions

— Not all machines are fitted with blades or vibration systems.

— Machines without ROPS need to be reassessed and change severity to S3 if a failure could cause a roll over.

— If blades have pitch adjustment it is considered the same as blade lower.

— Machines have low travel speed and can stop quickly, however steering was scored as an AC0 because the operator may not always be able to stop in time.

— For machine speed in compaction with hystat and e-stop fitted (no CCF with propel system) MPL_r = b (AC1, AW2, AR2).

— Wheel dozers have the same MPL_r as WL for brakes, steering and propulsion and dozers for implement.

— Machine may not have e-stop.

J.3 MPL_r mapped to SCS table

Table J.5 shows function-based MPL_r (see Table J.1) mapped to SCS per the results of the MCSSA for a landfill compactor. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table J.1 would also be mapped to these MPL_r.

Table J.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
machine speed	uncommanded activation	**c**	propel
engine speed	uncommanded activation	**c**	throttle
machine direction	failure to apply on demand	**c**	gear direction control
neutralize transmission	failure to apply on demand	**c**	gear direction control
blade lower	uncommanded activation	**b**	blade lower
blade raise	uncommanded activation	**b**	blade raise
blade tilt left / right	uncommanded activation	**b**	blade tilt left / right
slow/stop	failure to apply on demand	**b**	service brakes
hold still	failure to apply on demand	**c**	parking brakes
steering	uncommanded activation	**c**	steering

Annex K
(normative)

Roller performance level tables

K.1 Rollers

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables K.1 to K.5) or in Clause 5.

Table K.1 — MPL_r table for rollers

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
RL1	**edge cutter up / down**	maintenance	uncommanded activation	severed toes	maintainer	S2	5 %	4 %	70 %	E0	AC0	N/A	N/A	C3	**b**
RL2	**E-stop**	compacting	failure to apply on demand	Only used in emergency situations. used worst severity for all scenarios	co-worker	S3	95 %	1 %	100 %	E0	AC0	N/A	N/A	C3	**c**
RL3	**hold still**	compacting	failure to apply on demand	machine rolls away - runs over someone	co-worker	S3	95 %	17 %	10 %	E1	AC1	AW2	AR2	C2	**c**
RL4		compacting	failure to apply on demand	machine rolls away - runs over someone	co-worker	S3	95 %	17 %	50 %	E1	AC1	AW2	AR2	C2	
RL5		maintenance	failure to apply on demand	run over	maintainer	S3	5 %	43 %	70 %	E1	AC1	AW2	AR2	C2	
RL6-7	**machine direction**	considered to be the same as machine speed													**b**
RL6	**machine speed**	compacting	uncommanded activation	machine overshoots intended direction change or stopping point and runs someone over	co-worker	S3	95 %	9 %	10 %	E0	AC1	AW2	AR2	C2	**b**
RL7		compacting	uncommanded activation	machine overshoots intended direction change or stopping point and runs over someone's limb - smaller machine	co-worker	S2	95 %	9 %	50 %	E1	AC1	AW2	AR2	C2	

Table K.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
RL6-7	**engine speed**	considered to be the same as machine speed													**b**
RL6-7	**slow/stop**	considered to be the same as machine speed													**b**
RL8	**steering**	compacting	uncommanded activation	machine steers into traffic	co-worker	S3	95 %	90 %	16 %	E2	AC1	AW2	AR3	C1	**c**
RL9		compacting	uncommanded activation	machine steers into traffic	operator	S3	95 %	90 %	100 %	E2	AC1	AW2	AR3	C1	
RL10		compacting	uncommanded activation	machine steers into traffic	co-worker	S3	95 %	90 %	16 %	E2	AC1	AW2	AR3	C1	
RL11		maintenance	uncommanded activation	crushed in hitch	maintainer	S3	5 %	9 %	70 %	E0	AC0	N/A	N/A	C3	
RL12		travel	uncommanded activation	crosses onto other side of access road	co-worker	S3	10 %	50 %	5 %	E0	AC0	N/A	N/A	C3	

K.2 Supporting explanation

K.2.1 Supporting explanations for dominant scenarios

RL1 – edge cutter up / down

H: 5 % of wash, 5 % of walk around, and 100 % troubleshoot. H = (5 % × 3 %) + (5 % × 15 %) + 3 % = 4 %

P: See 5.5. Maintainer on machine for 70 % of task on smaller machine. P = 70 %.

AC: AC0

RL2 – E-stop

H: Only used in emergencies. H = 1 %

P: Always present during an emergency. P = 100 %

AC: AC0

RL3 – hold still

H: Maximum idle time (25 %), machine left on grade where it could roll (2/3). H = (2/3) × 25 % = 17 %

P: Only hazardous at this severity for pedestrians in area. P = 10 %

AC: AC1 - E-stop or hydraulic lockout

AW: AW2

AR: AR2 – Operator must move hand to apply E-stop or hydraulic lockout

RL4 – hold still

H: Maximum idle time (25 %), machine left on grade where it could roll (2/3). H = (2/3) × 25 % = 17 %

P: Light vehicle traffic rate in park up / central area. P = 50 %

AC: AC1 - E-stop or hydraulic lockout

AW: AW2

AR: AR2 – Operator must move hand to apply E-stop or hydraulic lockout

RL5 – hold still

H: 33 % wash, 10 % refuel, 33 % walk around, 90 % of grease, 10 % of window wash, all of camera clean, oil sample, troubleshoot, tire check, and articulation lock install. H = (33 % × 3 %) + (10 % × 44 %) + (33 % × 15 %) + (90 % × 3 %) + (10 % × 6 %) + 6 % + 3 % + 3 % = 43 %

P: See 5.8. Maintainer on machine for 70 % of task on smaller machine. P = 70 %.

AC: AC1 - E-stop or hydraulic lockout

AW: AW2

AR: AR2 – Operator must move hand to apply e-stop or hydraulic lockout

RL6 – machine speed

H: Only hazardous at the points where preparing to change direction or stop - 10 %. 90 % idle factor. H = (10 % × 90 %) = 9 %

P: Only hazardous at this severity for pedestrians in the area. P = 10 %

AC: AC1 – E-stop

AW: AW2

AR: AR2

RL7 – machine speed

H: Only hazardous at the points where preparing to change direction or stop - 10 %. 90 % idle factor. H = (10 % × 90 %) = 9 %

P: People working on paver. P = 50 %

AC: AC1 – E-stop

AW: AW2

AR: AR2

RL8 – steering

H: 90 % idle factor

P: See 5.2. P = 16 %

AC: AC1 – Remove propel command - slow machine speed allows reaction

AW: AW2

AR: AR3

RL9 – steering

H: 90 % idle factor

P: Always present during an emergency. P = 100 %

AC: AC1 – Remove propel command - slow machine speed allows reaction

AW: AW2

AR: AR3

RL10 – steering

H: 90 % idle factor

P: See 5.2. P = 16 %

AC: AC1 – Remove propel command - slow machine speed allows reaction

AW: AW2

AR: AR3

RL11 – steering

H: 10 % of refuel, 10 % walk around, all of articulation lock install. H = (10 % × 44 %) + (10 % × 15 %) + 3 % = 9 %

P: See 5.5. Maintainer on machine for 70 % of task on smaller machine. P = 70 %.

AC: AC0

RL12 – steering

H: Only hazardous in one direction – 50 %

P: Not normally travelling on access road. P = 5 %

AC: AC0

K.2.2 Application use cases

Table K.2 — Application use case table

Application	Travel	Compacting	Maintenance
Single / asphalt roller	10 %	95 %	5 %
Tandem / utility roller	10 %	95 %	5 %
Pneumatic roller	5 %	95 %	5 %

K.2.3 Maintenance task breakdown

Table K.3 — Maintenance task breakdown

	Time (min/day)	% Maintenance time
wash	1,0	3 %
fuel, water, DEF fill	15,0	44 %
daily inspection	5,0	15 %
camera clean	2,0	6 %
oil sample	1,0	3 %
grease	1,0	3 %
troubleshooting	1,0	3 %
window wash	2,0	6 %
tire check	5,0	15 %
articulation lock install	1,0	3 %

K.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table K.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
machine speed			1		Other failure types are less or not hazardous.
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

Table K.4 *(continued)*

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
machine direction	1				Other failure types are less or not hazardous.
edge cutter up / down			1		Other failure types are less or not hazardous.
slow/stop	1		1		Other failure types are less or not hazardous.
hold still	1				Other failure types are less or not hazardous.
steering			1		Other failure types are less or not hazardous.
E-stop	1				Uncommanded activation considered to be the same as systems it controls
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

K.2.5 Notes and assumptions

— E-stop is considered only if equipped.

— Transmission neutralize is considered the same as machine direction.

K.3 MPL_r mapped to SCS table

Table K.5 shows function-based MPL_r (see Table K.1) mapped to SCS per the results of the MCSSA for a roller. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table K.1 would also be mapped to these MPL_r.

Table K.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
machine speed	uncommanded activation	**b**	propel
engine speed	uncommanded activation	**b**	throttle
machine direction	failure to apply on demand	**b**	gear direction control
edge cutter up / down	uncommanded activation	**b**	edge cutter up / down
slow/stop	failure to apply on demand	**b**	service brakes
hold still	failure to apply on demand	**c**	parking brakes
steering	uncommanded activation	**c**	steering
e-stop	failure to apply on demand	**c**	e-stop

Annex L
(normative)

Grader performance level tables

L.1 Graders

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables L.1 to L.5) or in Clause 5.

Table L.1 — MPL_r table for graders

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
MG1	**articulation**	maintenance	uncommanded activation	maintainer crushed in articulation area	maintainer	S3	5 %	4 %	75 %	E0	AC0	N/A	N/A	C3	**c**
MG2	**blade down**	maintenance	uncommanded activation	crushed limb under blade	maintainer	S2	5 %	4 %	75 %	E0	AC0	N/A	N/A	C3	**b**
	blade pitch	Not considered hazardous													**N/A**
MG3	**blade side shift**	travel (no work, high speed roading, etc.)	uncommanded activation	collision between blade and pedestrian at speed	bystander	S3	30 %	38 %	1 %	E0	AC0	N/A	N/A	C3	**c**
MG4	**blade up**	maintenance	uncommanded activation	blade collides with maintainer	maintainer	S2	5 %	7 %	75 %	E0	AC0	N/A	N/A	C3	**b**
MG5	**circle / A-Frame L / R**	maintenance	uncommanded activation	collison between circle / A-frame and maintainer	maintainer	S2	5 %	4 %	75 %	E0	AC0	N/A	N/A	C3	**b**
MG6		travel (no work, high speed roading, etc.)	uncommanded activation	collision between blade and pedestrian at speed	bystander	S3	30 %	38 %	1 %	E0	AC1	AW2	AR2	C2	
MG7	**front implement down**	maintenance	uncommanded activation	crushed limb under implement	maintainer	S2	5 %	3 %	75 %	E0	AC0	N/A	N/A	C3	**b**
MG8	**hold still**	blading (all types - fine blading, snow wing, high speed blading, shouldering, mid frame scarifier)	failure to apply on demand	machine starts rolling while operator is out of the cab - run over	bystander	S3	80 %	5 %	20 %	E0	AC0	N/A	N/A	C3	**c**
MG9		maintenance	failure to apply on demand	run over maintainer	maintainer	S3	5 %	55 %	75 %	E1	AC1	AW2	AR2	C2	

Table L.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
MG14	**machine direction**	uncommanded activation is considered to be the same as uncommand slow/stop													**c**
MG10		blading (all types - fine blading, snow wing, high speed blading, shouldering, mid frame scarifier)	failure to apply on demand	collision when maneuvering	bystander	S3	80 %	5 %	20 %	E0	AC1	AW2	AR3	C1	**a**
MG11	**machine speed**	travel (no work, high speed roading, etc.)	uncommanded activation	collision due to increased slowing / stopping distance	bystander	S3	30 %	50 %	16 %	E1	AC1	AW2	AR3	C1	**b**
MG12	**ripper down**	maintenance	uncommanded activation	crushed limb under ripper	maintainer	S2	5 %	3 %	75 %	E0	AC0	N/A	N/A	C3	**b**
MG13	**slow/stop**	travel (no work, high speed roading, etc.)	failure to apply on demand	collision - machine fails stop	bystander	S3	30 %	10 %	100 %	E1	AC1	AW2	AR2	C2	**c**
MG14		travel (no work, high speed roading, etc.)	uncommanded activation	machine stops without command causing collision with following vehicle	operator	S1	30 %	50 %	100 %	E2	AC0	N/A	N/A	C3	**c**
MG15	**snow wing**	maintenance	uncommanded activation	crushed by snow wing	maintainer	S3	5 %	6 %	75 %	E0	AC0	N/A	N/A	C3	**c**
MG16		travel (no work, high speed roading, etc.)	uncommanded activation	collision between snow wing and bystander	bystander	S3	30 %	100 %	2 %	E0	AC0	N/A	N/A	C3	

Table L.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
MG17	**steering left / right**	travel (no work, high speed roading, etc.)	uncommanded activation	collision	bystander	S3	30 %	100 %	16 %	E1	AC1	AW2	AR0	C3	**d**
MG18	**wheel lean**	travel (no work, high speed roading, etc.)	uncommanded activation	collision, wheel lean causes slight steering change.	bystander	S3	30 %	100 %	16 %	E1	AC1	AW2	AR3	C1	**b**
MG19	**transmission neutralize**	travel (no work, high speed roading, etc.)	uncommanded deactivation	machine moves into vehicle or bystander	bystander	S3	30 %	4 %	25 %	E0	AC1	AW2	AR3	C1	**a**

L.2 Supporting explanation

L.2.1 Supporting explanations for dominant scenarios

MG1 – articulation

H: 15 % of grease, 5 % of wash, 10 % of windows wash, and all of troubleshooting. H = (15 % × 14 %) + (5 % × 6 %) + (10 % × 3 %) + 1 % = 4 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

MG2 – blade down

H: All cutting edge replace – mid-mount blade, shoe / circle adjustment, troubleshooting, and moldboard wear strip change. H = 4 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

MG3 – blade side shift

H: Only when machine is at speed (>10 km/h) (75 %) and only dangerous if it extends in the direction away from tandem and is able to extend past front tires (50 %). H = (75 % × 50 %) = 38 %

P: Only when pedestrian is present and very close to the machine (10 km/h). It is considered machine abuse to road machine without blade fully rotated to minimize machine width. P = 1 %

AC: AC0

MG4 – blade up

H: 25 % of grease and all of shoe / circle adjustment, troubleshooting, and moldboard wear strip change. H = (25 % × 14 %) + 2 % +1 % + 0,2 % = 7 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

MG5 – circle / A-Frame L / R

H: All of cutting edge replace – mid-mount blade, shoe / circle adjustment, troubleshooting, and moldboard wear strip change. H = 0,4 % + 2,1 % + 1,4 % + 0,2 % = 4 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

MG6 – circle / A-Frame L / R

H: Only when machine is at speed (>10 km/h) (75 %) and only dangerous if it rotates in an outward direction. H = (75 % × 50 %) = 38 %

P: Only when pedestrian is present and very close to the machine (10 km/h). P = 1 %

AC: AC1 – Steering

AW: AW2

AR: AR2

MG7 – front implement down

H: 20 % of grease and all of cutting edge replace - front blade. H = (20 % × 14 %) + 1 % = 4 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

MG8 – hold still

H: Only hazardous when machine stopped without the blade grounded. H = 5 %

P: Construction site park up area. P = 20 %

AC: AC0

MG9 – hold still

H: 30 % walk around, 50 % refuel, 25 % window wash, 50 % cutting edge replace - front blade, 50 % ripper teeth - replace, 50 % transmission check, and all of engine check, transmission top up, engine top up, troubleshooting, moldboard wear strip change, grease, wash, add/remove attachments, cutting edge replace – mid-mount blade, and shoe/circle adjust. H = (30 % × 14,1 %) + (50 % × 14,1 %) + (25 % × 2,8 %) + (50 % × 0,4 %) + (50 % × 0,4 %) + (50 % × 7,1 %) + 7,1 % + 0,7 % + 0,7 % + 1,4 % + 0,2 % + 14,1 % + 5,7 % + 6,2 % + 0,4 % + 2,1 % = 55 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC1

AW: AW2

AR: AR2 - It is considered machine abuse to not ground implements

MG10 – machine direction

H: Only when in tight confines (50 %) and when stopping (10 %). H = (50 % × 10 %) = 5 %

P: Construction site park up area. P = 20 %

AC: AC1 – brakes

AW: AW2

AR: AR3

MG11 – machine speed

H: Slowing down up to 50 % of time. H = 50 %

P: Traffic rate. P = 16 %

AC: AC1 – brakes

AW: AW2

AR: AR3

MG12 – ripper down

H:.20 % of grease and all of ripper teeth - replace. H = (20 % × 14 %) + 0,4 % = 3 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

MG13 – slow/stop

H: Only when slowing or stopping to avoid hitting someone. H = 10 %

P: Always present during an emergency. P = 100 %

AC: AC1 – park brake

AW: AW2

AR: AR2

MG14 – slow/stop

H: Only hazardous when machine not slowing down. H = 50 %

P: Operator present throughout the cycle. P = 100 %

AC: AC0

MG15 – snow wing

H: All of add / remove attachments. H = 6 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

MG16 – snow wing

H: Any point when traveling with snow wing up. H = 100 %

P: Only when person is beside road (rare in snow) 1 % or machine in over taking or turning lane while vehicle is in regular lane (rare) 1 %. P = 2 %

AC: AC0

MG17 – steering left / right

H: Hazard exists during the whole cycle. H = 100 %

P: See 5.2. P = 16 %

AC: AC1

AW: AW2

AR:AR0

MG18 – wheel lean

H: Hazard exists during the whole cycle. H = 100 %

P: See 5.2. P = 16 %

AC: AC1 – steering

AW: AW2

AR: AR3

MG19 - transmission neutralize

H: Time when machine is idle while waiting (20 %) during portion of travel that is low speed manoeuvring (1/5). H = 20 % × 1/5 = 4 %

P: Typical bystander rate in central / parking areas. P = 25 %.

AC: AC1 – brakes

AW: AW2

AR: AR3 – The brakes would be under foot

L.2.2 Application use cases

Table L.2 — Application use case table

Application	Travel (no work, high speed roading, etc.)	Blading (all types - fine blading, snow wing, high speed blading, shoul-dering, mid frame scarifier)	Ripping	Maintenance
Construction	5 %	80 %	20 %	5 %
Road maintenance	30 %	80 %	10 %	5 %
Mining	10 %	80 %	20 %	5 %

L.2.3 Maintenance task breakdown

Table L.3 — Maintenance task breakdown

	Time (min/ day)	% Mainte-nance time
daily inspection	10,0	28,3 %
grease	5,0	14,1 %
refuel	5,0	14,1 %
wash	2,0	5,7 %
window wash	1,0	2,8 %
add / remove attachments	2,2	6,2 %
park brake test	2,0	5,7 %
cutting edge replace – mid-mount blade	0,1	0,4 %
cutting edge replace – front blade	0,1	0,4 %
ripper teeth replace	0,1	0,4 %
shoe / circle adjustment	0,7	2,1 %
transmission oil check	2,5	7,1 %
engine oil check	2,5	7,1 %
transmission oil fill	0,3	0,7 %
engine oil fill	0,3	0,7 %
troubleshooting	0,5	1,4 %
moldboard wear strip change	0,1	0,2 %
flash / calibration	1,0	2,8 %

L.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table L.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
slow/stop	1		1		Uncommanded release no worse than failure to apply on demand
hold still	1				Uncommanded release no worse than failure to apply on demand
steering left / right			1		Failure on demand same as uncommanded steering
blade up			1		Other failure types are less or not hazardous.
blade down			1		Other failure types are less or not hazardous.
blade side shift			1		Other failure types are less or not hazardous.
blade pitch			1		Other failure types are less or not hazardous.
circle / A-Frame L / R			1		Other failure types are less or not hazardous.
circle pitch			1		Other failure types are less or not hazardous.
articulation			1		Other failure types are less or not hazardous.
wheel lean			1		Other failure types are less or not hazardous.
snow wing			1		Other failure types are less or not hazardous.
ripper up			1		Ripper up is not considered hazardous
ripper down			1		Other failure types are less or not hazardous.
front implement up			1		Other failure types are less or not hazardous.
front implement down			1		Other failure types are less or not hazardous.
machine speed			1		Failure to release on demand considered the same as uncommanded application
machine direction	1				Uncommanded application considered same as uncommanded slow/stop
transmission neutralize				1	Shifting out of neutral without command

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

L.2.5 Notes and assumptions

— Road maintenance has little to no site management.

— Towing a camper / attachment is included in other use cases.

— Co-worker is someone in similar or larger machine / vehicle.

— Bystander is a pedestrian or light vehicle.

— Where mining has lower score, only applies to large purpose built (weight greater than 60 000 kg.) graders that are not used in other applications. All smaller motor graders are considered to be used in other applications.

L.3 MPL_r mapped to SCS table

Table L.5 shows function-based MPL_r (see Table L.1) mapped to SCS per the results of the MCSSA for a grader. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table L.1 would also be mapped to these MPL_r.

Table L.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
articulation	uncommanded activation	**c**	articulation
blade down	uncommanded activation	**b**	blade down

Table L.5 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
blade side shift	uncommanded activation	**c**	blade side shift
blade pitch	no hazard	**N/A**	blade pitch
blade up	uncommanded activation	**b**	blade up
circle / A-frame - left / right	uncommanded activation	**b**	centre shift
front implement down	uncommanded activation	**b**	front implement down
hold still	failure to apply on demand	**c**	parking brake
machine direction	uncommanded activation	**c**	gear direction control
	failure to apply on demand	**a**	
machine speed	uncommanded activation	**b**	propel
ripper down	uncommanded activation	**b**	ripper down
slow/stop	failure to apply on demand	**c**	service brakes
	uncommanded activation	**b**	
snow wing	uncommanded activation	**c**	snow wing
steering left / right	uncommanded activation	**d**	steering
	failure to apply on demand	**d**	
wheel lean	uncommanded activation	**b**	wheel lean
transmission neutralize	uncommanded deactivation	**a**	gear direction control

Annex M
(normative)

Crawler dozer performance level tables

M.1 Crawler dozers

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables M.1 to M.5) or in Clause 5.

Table M.1 — MPL_r table for crawler dozers

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
TT1	**blade angle**	pushing dirt	uncommanded activation	Pinched between machine and blade	bystander	S2	95 %	60 %	1 %	E0	AC0	N/A	N/A	C3	**b**
TT2		maintenance	uncommanded activation	crush injury	maintainer	S2	5 %	0 %	75 %	E0	AC0	N/A	N/A	C3	
TT1-2	**blade tilt R**	considered to be the same as blade angle - it is considered machine abuse to be under unblocked blade													**b**
N/A	**blade pitch**	Not considered hazardous													
TT3	**blade down**	maintenance	uncommanded activation	Bumped by moving push arms	maintainer	S1	5 %	0 %	100 %	E0	AC0	N/A	N/A	C3	**a**
TT4	**e-stop**	Considered to be the same as hold still when pushing dirt													**c**
TT4	**hold still**	pushing dirt	failure to apply on demand	Machine moves when accessing machine	operator	S3	95 %	60 %	1 %	E0	AC1	AW1	AR2	C3	**c**
TT5		drawbar	failure to apply on demand	Machine moves when attaching implement	bystander	S3	90 %	1 %	90 %	E0	AC1	AW1	AR2	C3	
TT6	**machine direction (F / R)**	pushing dirt	failure to apply on demand	Machine drives off highwall	operator	S3	95 %	8 %	100 %	E1	AC1	AW2	AR3	C1	**b**
TT6	**machine speed**	Considered to be the same as machine direction													**b**
TT6	**slow/stop**	Considered to be the same as machine direction													**b**
TT7	**powered access system**	pushing dirt	uncommanded activation	Ladder raises while accessing the machine	operator	S2	95 %	1 %	100 %	E0	AC0	N/A	N/A	C3	**b**
TT8		pushing dirt	uncommanded activation	Ladder lowers hitting person	bystander	S2	95 %	60 %	1 %	E0	AC0	N/A	N/A	C3	
TT9	**ripper / scraper bowl – up / down**	maintenance	uncommanded activation	Crushed limb while using ground level service centre with ripper up	maintainer	S2	5 %	43 %	75 %	E1	AC1	AW2	AR2	C2	**b**
TT9	**ripper pitch forward / scraper apron**	Considered to be the same as ripper down													**b**
TT9	**ripper pitch reverse / scraper eject**	Considered to be the same as ripper down													**b**
TT10	**steering**	maintenance	uncommanded activation	Parking brake on for everything except transport - comes off trailer	maintainer	S3	5 %	4 %	75 %	E0	AC0	N/A	N/A	C3	**c**
TT11		pushing dirt	uncommanded activation	Operator steers off stockpile	operator	S1	95 %	36 %	100 %	E2	AC1	AW2	AR0	C3	
TT12	**engine speed**	travel	uncommanded activation	Slight increase in speed causing small increase in stopping distance when slow speed manoeuvring in shop or parking area	bystander	S3	25 %	5 %	5 %	E0	AC1	AW2	AR3	C1	**a**

M.2 Supporting explanation

M.2.1 Supporting explanations for dominant scenarios

TT1 – blade angle

H: Only hazardous when idle (maximum idle = 60 %). H = 60 %

P: Momentary exposure normally during access. P = 1 %

AC: AC0

TT2 – blade angle

H: 10 % of change blade cutting edge, 10 % of assembly / disassembly, and all of troubleshooting. H = (10 % × 1 %) + (10 % × 1 %) + 0 % = 0 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

TT3 – blade down

H: 10 % of change blade cutting edge, 10 % of assembly / disassembly, and all of troubleshooting. H = (10 % × 1 %) + (10 % × 1 %) + 0 % = 0 %

P: Maintainer there for all of task. P = 100 %

AC: AC0

TT4 – hold still

H: Only hazardous when idle (maximum idle = 60 %). H = 60 %

P: Momentary exposure normally during access. P = 1 %

AC: AC1 - It is considered machine abuse to leave machine unattended without blade on ground

AW: AW1 – May not realise the hazard

AR: AR2

TT5 – hold still

H: Only when attaching implement. H = 1 %

P: Present for most of cycle. P = 90 %

AC: AC1 - It is considered machine abuse to leave machine unattended without blade on ground

AW: AW1 – May not realise the hazard

AR: AR2

TT6 – machine direction

H: Machine stopping for maximum of 1/8th of cycle, moving forward 67 % of time, reverse 32 %, 10 % idle time. H = (12,5 % × 67 % × 32 % × 10 %) = 8 %

P: Operator present throughout the cycle. P = 100 %

AC: AC1 - It is considered machine abuse to not push berm behind the berm being pushed off edge

AW: AW2

AR: AR3 - brakes

TT7 – powered access

H: Only hazardous when accessing / egressing the machine. H = 1 %

P: Operator present throughout the cycle. P = 100 %

AC: AC0

TT8 – powered access

H: Bystanders would only be this close when at idle, maximum idle time 60 %. H = 60 %

P: Rare for person to be that close, in that specific spot, looking away from the machine. P = 1 %

AC: AC0

TT9 – ripper down / scraper bowl

H: 25 % of greasing, 25 % of wash windows, 10 % of changing ripper teeth, 10 % of assembly / disassembly, and all of refuelling, and troubleshooting. H = (25 % × 33 %) + (25 % × 7 %) + (10 % × 1 %) + (10 % × 1 %) + 33 % + 0 % = 43 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC1 – E-stop

AW: AW2

AR: AR2

TT10 – steering

H: All of transport loading / unloading. H = 4 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

TT11 – steering

H: Only hazardous when near the edge 80 %, 50 % of failures are hazardous, 90 % idle factor. H = 80 % × 50 % × 90 % = 36 %

P: Always present during an emergency. P = 100 %

AC: AC1 – brakes

AW: AW2

AR: AR0

TT12 – engine speed

H: Proportion of time machine is moving at low engine speed is small (5 %) 90 % idle factor. H = 5 % × 90 % = 5 %

P: Very rare to be standing this close to a dozer in the path of travel. P = 5 %

AC: AC1 – brakes

AW: AW2

AR: AR3

M.2.2 Application use cases

Table M.2 — Application use case table

Application	Pushing dirt	Drawbar	Pushing scrapers	Ripping	Travel	Maintenance
General construction / waste / Ag (small)	95 %	90 %	50 %	20 %	15 %	5 %
General construction / waste (medium / large)	95 %	90 %	50 %	75 %	25 %	5 %
Mining	95 %	0 %	0 %	95 %	15 %	5 %
Fire dozer	50 %	50 %	0 %	40 %	25 %	5 %

M.2.3 Maintenance task breakdown

Table M.3 — Maintenance task breakdown

	Time (min/ day)	% Maintenance time
refueling	13,0	33 %
transport loading / unloading	1,4	4 %
greasing	13,0	33 %
walk around	2,6	7 %
machine wash	4,3	11 %
window wash	2,6	7 %
change cutting edge	0,5	1 %
change ripper teeth	0,3	1 %
adjust track	0,4	1 %
troubleshooting	0,0	0 %
assembly / disassembly	0,3	1 %
oil sampling	0,3	1 %
clean undercarriage	1,0	3 %

M.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table M.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
slow/stop	1				Uncommanded stop not hazardous
hold still	1				Includes uncommanded release
machine speed			1		Includes failure to release on demand
engine speed			1		Other failure types are less or not hazardous.
machine direction (F / R)	1				Other failure types are less or not hazardous.
steering			1		Includes failure on demand
blade up					No conceivable hazard
blade down			1		Other failure types are less or not hazardous.

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

Table M.4 *(continued)*

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
blade tilt L					Combined with Down
blade tilt R			1		Other failure types are less or not hazardous.
blade angle			1		Other failure types are less or not hazardous.
blade pitch			1		Other failure types are less or not hazardous.
ripper up / scraper bowl					Combined with Down
ripper down / scraper bowl			1		Other failure types are less or not hazardous.
ripper pitch F / scraper apron			1		Other failure types are less or not hazardous.
ripper pitch R / scraper eject			1		Other failure types are less or not hazardous.
power access system			1		Other failure types are less or not hazardous.
operator presence	1				Other failure types are less or not hazardous.
e-stop	1				Other failure types are less or not hazardous.
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

M.2.5 Notes and assumptions

— Co-worker is someone in similar or larger machine / vehicle.

— Bystander is a pedestrian or light vehicle.

— Pushing off highwall cycle:

  — machine stopping for maximum of 1/ 8th of cycle, moving forward 67 % of time, reverse 32 %, 10 % idle time.

— For e-stops, the highest of PL (see ISO 13850) and the systems the e-stop controls shall be used. In this case both have PL_r = c.

— Yo-yoing is considered machine abuse; traction assist winch is under forestry.

M.3 MPL_r mapped to SCS table

Table M.5 shows function-based MPL_r (see Table M.1) mapped to SCS per the results of the MCSSA for a crawler dozer. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table M.1 would also be mapped to these MPL_r.

Table M.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
blade angle	uncommanded activation	**b**	**blade angle**
blade tilt	uncommanded activation	**b**	**blade tilt**
blade pitch	no hazard	**N/A**	**blade pitch**
blade down	uncommanded activation	**a**	**blade down**
engine speed	uncommanded activation	**a**	**throttle**
e-stop	failure to apply on demand	**c**	**e-stop**
hold still	failure to apply on demand	**c**	**parking brake**
machine direction (F / R)	failure to apply on demand	**b**	**gear direction control**
machine speed	uncommanded activation	**b**	**propel**
slow/stop	failure to apply on demand	**b**	**service brakes**
power access system	uncommanded activation	**b**	**power access system**

Table M.5 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
ripper / scraper bowl – up / down	uncommanded activation	**b**	**ripper down / scraper bowl**
ripper pitch forward / scraper apron	uncommanded activation	**b**	**ripper pitch forward / scraper apron**
ripper pitch reverse / scraper eject	uncommanded activation	**b**	**ripper pitch reverse / scraper eject**
steering	uncommanded activation	**c**	**steering**

Annex N
(normative)

Pipelayer performance level tables

N.1 Pipelayers

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables N.1 to N.5) or in Clause 5.

Table N.1 — MPL_r table for pipelayers

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
PL1	**boom up / down**	lay-in	uncommanded activation	load drops suddenly causing machine tip over	operator	S1	20 %	91 %	100 %	E2	AC0	N/A	N/A	C3	**c**
PL2		lay-in	uncommanded activation	Multiple pipelayer supporting section of pipe. Load drops suddenly causing machines to tip over	co-worker	S1	20 %	91 %	100 %	E2	AC0	N/A	N/A	C3	
PL1-2	**counter-weight in/ out**	considered the same as boom up / down													**c**
PL6-7	**engine speed**	considered same as machine speed unless it is not tied to machine speed, then no hazard													**b**
PL3	**hold still**	tow / re-trieval	failure to apply on demand	machine rolls over someone	bystander	S3	2 %	1 %	100 %	E0	AC0	N/A	N/A	C3	**c**
PL4		drawbar / winch	failure to apply on demand	machine rolls over someone	bystander	S3	5 %	1 %	100 %	E0	AC0	N/A	N/A	C3	
PL5		mainte-nance	failure to apply on demand	machine rolls over someone	maintainer	S3	5 %	4 %	75 %	E0	AC0	N/A	N/A	C3	
PL1-2	**hook up / down**	considered the same as boom up / down													**c**
PL2-8	**load moni-toring**	considered same as quick drop and boom up / down													**c**
PL6	**machine direction (F / R)**	lay-in	uncommanded activation	machine movement causes pipelayer to tip over	operator	S1	20 %	91 %	100 %	E2	AC1	AW2	AR2	C2	**b**
PL7		lay-in	uncommanded activation	Multiple pipelayer support-ing section of pipe. Machine movement causes pipelayer to tip over	co-worker	S1	20 %	91 %	100 %	E2	AC1	AW2	AR2	C2	
PL6-7	**machine speed**	considered same as machine direction													**b**
PL8	**quick drop**	welding	uncommanded activation	machine tip over	operator	S1	60 %	56 %	100 %	E2	AC0	N/A	N/A	C3	**c**
PL9		welding	uncommanded activation	crushed limb	bystander	S2	60 %	44 %	33 %	E1	AC0	N/A	N/A	C3	
PL6-7	**slow/stop**	same as machine direction - only reacting with quick drop rather than brake.													**b**

Table N.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
PL10	**steering**	maintenance	uncommanded activation	Machine comes off trailer when loading / unloading for transport. parking brake on for everything else	maintainer	S3	5 %	4 %	75 %	E0	AC0	N/A	N/A	C3	**c**

N.2 Supporting explanation

N.2.1 Supporting explanations for dominant scenarios

PL1 – boom up / down

H: 22-minute cycle, 20 min of cycle lifting and positioning when someone could be underload. H = (20 / 22) × 100 = 91 %

P: Operator present during the whole cycle. P = 100 %

AC: AC0

PL2 – boom up / down

H: 22-minute cycle, 20 min of cycle lifting and positioning when someone could be underload. H = (20 / 22) × 100 = 91 %

P: Person present during the whole cycle. P = 100 %

AC: AC0

PL3 – hold still

H: Hazardous during hook-up only - 1 % of cycle. H = 1 %

P: Person present for all of hook up. P = 100 %

AC: AC0

PL4 – hold still

H: Hazardous during hook-up only - 1 % of cycle. H = 1 %

P: Person present for all of hook up. P = 100 %

AC: AC0

PL5 – hold still

H: 40 % of walk around, 40 % of wash machine, and all of refuelling, grease, wash windows, and oil sampling. H (maintenance tasks) = (40 % × 7 %) + (40 % × 3 %) + 37 % + 37 % + 7 % + 1 % = 86 %. Maintenance is rarely done on slope steep enough to overcome rolling resistance (10 %). Hazard only exists if machine rolls towards maintainer (50 %). H = 86 % (maintenance tasks) × 10 % × 50 % = 43 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

PL6 – machine direction (F / R)

H: 22-minute cycle, 20 min of cycle lifting and positioning when someone could be underload. H = (20 / 22) × 100 = 91 %

P: Operator present during the whole cycle. P = 100 %

AC: AC1 – Quick drop or brakes

AW: AW2

AR: AR2

PL7 – machine direction (F / R)

H: 22-minute cycle, 20 min of cycle lifting and positioning when someone could be underload. H = (20 / 22) × 100 = 91 %

P: Person present during the whole cycle. P = 100 %

AC: AC1 – Quick drop or brakes

AW: AW2

AR: AR2

PL8 – quick drop

H: Only during travel portion – 2,5 / 4,5. H = (2,5 / 4,5) × 100 = 56 %

P: Operator present during the whole cycle. P = 100 %

AC: AC0

PL9 – quick drop

H: 2 min out of 4,5 min cycle of welding / travel to next section of pipe. H = (2 / 4,5) × 100 = 44 %

P: Body parts only under the pipe may get crushed during 1/3 of weld cycle (S1 for rest of underside, no hazard for top side). P = 33 %

AC: AC0

PL10 – steering

H: All transport loading / unloading. H = 4 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

N.2.2 Application use cases

Table N.2 — Application use case table

Application	Welding	Tie-in	Bending	Stringing	Lay-in	Tow / retrieval	Drawbar / winch	Travel	Maintenance
Pipelaying	60 %	40 %	25 %	20 %	20 %	2 %	5 %	20 %	5 %

N.2.3 Maintenance task breakdown

Table N.3 — Maintenance task breakdown

	Time (min/day)	% Maintenance time
refueling	13,0	37 %
transport loading / unloading	0,3	1 %
greasing	13,0	37 %
walk around	2,6	7 %
machine wash	1,0	3 %
window wash	2,6	7 %
cable and componentry inspect	0,7	2 %
adjust track	0,4	1 %
troubleshooting	0,0	0 %

Table N.3 *(continued)*

	Time (min/ day)	% Maintenance time
assembly / disassembly	1,0	3 %
oil sampling	0,3	1 %
clean undercarriage	0,5	1 %

N.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table N.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
slow/stop	1				
hold still	1				
machine speed			1		
engine speed			1		
machine direction (F / R)			1		
steering			1		
boom up / down			1		
counterweight in / out			1		
load monitoring	1				
quick drop			1		
hook up / down			1		
operator presence	1				
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

N.2.5 Notes and assumptions

— Co-worker is a person in another machine.

— Bystander is a pedestrian.

N.3 MPL_r mapped to SCS table

Table N.5 shows function-based MPL_r (see Table N.1) mapped to SCS per the results of the MCSSA for a Pipelayer. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table N.1 would also be mapped to these MPL_r.

Table N.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
boom up / down	uncommanded activation	**c**	boom up / down
counterweight in / out	uncommanded activation	**c**	counterweight in / out
hold still	failure to apply on demand	**c**	park brakes
hook up	uncommanded activation	**c**	hook up

Table N.5 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
load monitoring	failure to apply on demand	**c**	load monitoring
machine direction (F / R)	uncommanded activation	**b**	gear direction control
quick drop	uncommanded activation	**c**	quick drop
slow/stop	failure to apply on demand	**b**	service brakes
steering	uncommanded activation	**c**	steering

Annex O
(normative)

Crawler loader performance level tables

O.1 Crawler loaders

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables O.1 to O.5) or in Clause 5.

Table O.1 — MPL_r table for crawler loaders

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CL1	**slow/stop**	traveling	failure to apply on demand	machine fails to stop when a bystander steps in front of the machine	bystander	S3	20 %	10 %	100 %	E1	AC1	AW2	AR3	C1	**b**
TT4	**hold still**	considered same as crawler dozer failure to apply on demand													**c**
CL2	**steering**	dozing / spreading / compacting	uncommanded activation	machine steers off stockpile	operator	S1	80 %	30 %	100 %	E2	AC0	N/A	N/A	C3	**c**
CL3		dozing / spreading / compacting	uncommanded activation	machine steers when it should not and runs over a co-worker	co-worker	S3	80 %	50 %	2 %	E0	AC0	N/A	N/A	C3	
CL4	**tool curl**	maintenance	uncommanded activation	person contacted by implement	maintainer	S1	5 %	10 %	75 %	E0	AC0	N/A	N/A	C3	**a**
CL5	**tool dump**	maintenance	uncommanded activation	foot squashed by implement	maintainer	S2	5 %	10 %	75 %	E0	AC0	N/A	N/A	C3	**b**
CL6	**boom raise**	loading / carrying	uncommanded activation	Contacts overhead infrastructure. Crushed by falling objects	co-worker	S3	60 %	50 %	5 %	E1	AC1	AW3	AR1	C2	**c**
CL7	**boom lower**	material handling	uncommanded activation	crushed by protruding load	co-worker	S3	10 %	6 %	1 %	E0	AC1	AW2	AR0	C3	**c**
CL8	**ripper down**	maintenance	uncommanded activation	contact with ripper	maintainer	S1	5 %	9 %	75 %	E0	AC0	N/A	N/A	C3	**a**
CL9	**ripper up**	maintenance	uncommanded activation	squashed foot	maintainer	S2	5 %	9 %	75 %	E0	AC0	N/A	N/A	C3	**b**
CL7	**clam open**	considered same as boom lower													**c**
CL5	**clam shut**	considered same as tool dump													**b**
CL7	**auxiliary flow**	considered same as clam open													**c**
CL7	**implement lockout**	considered same as highest implement performance level													**c**
CL10	**machine speed**	loading / carrying	uncommanded activation	machine overshoots intended stopping position causing collision	co-worker	S3	60 %	36 %	20 %	E1	AC1	AW2	AR3	C1	**b**
CL11	**machine direction**	loading / carrying	failure to apply on demand	failure to change direction causes machine to collide with bystanders outside work area	co-worker	S3	60 %	4 %	25 %	E0	AC1	AW2	AR3	C1	**a**

Table O.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CL12	**engine speed**	loading / carrying	uncommanded activation	Machine engine speed goes to low idle causing machine to be stuck in slag pit operator exposed to heat and fumes while waiting for retrieval. Multiple failures would have to occur to be dangerous for a fire risk.	operator	S1	70 %	25 %	100 %	E2	AC0	N/A	N/A	C3	**c**

O.2 Supporting explanation

O.2.1 Supporting explanations for dominant scenarios

CL1 – slow/stop

H: Rare for people to walk in front of machines. H = 10 %

P: Always present during an emergency. P = 100 %

AC: AC1 – Bucket to ground is natural reaction for a crawler

AW: AW2

AR: AR3

CL2 – steering

H: Only while high on the stockpile and idle factor. H = 33 % × 90 % = 30 %

P: Operator present during the whole cycle. P = 100 %

AC: AC0

CL3 – steering

H: Only half of failures are dangerous. H = 50 %

P: Very rare a person would be close enough to the machine. P = 2 %

AC: AC0

CL4 – tool curl

H: 10 % walk around, 10 % machine wash, all transport load / unload, bucket GET, and troubleshooting. H = (10 % × 7 %) + (10 % × 15 %) + 7 % + 0,6 % + 0,003 % = 10 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CL5 – tool dump

H: 10 % walk around, 10 % machine wash, all transport load / unload, bucket GET, and troubleshooting. H = (10 % × 7 %) + (10 % × 15 %) + 7 % + 0,6 % + 0,003 % = 10 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CL6 – boom raise

H: Minimal time in reverse. Could happen anytime there are overhead objects. H = 50 %

P: P: Rare for people to be in the area. P = 5 %

AC: AC1 - Turn the machine off

AW: AW3

AR: AR1

CL7 – boom lower

H: Load only lifted half of 25 % at each end of the cycle 2 × 25 % × 25 % × 50 %. H = 6 %

P: It is considered machine abuse to be under the load, but it may happen momentarily. P = 1 %

AC: AC1 - Could move machine (steering or reverse)

AW: AW2 – Same as wheel loader

AR: AR0 – Same as wheel loader

CL8 – ripper down

H: 10 % walk around, 10 % machine wash, and all of transport load / unload, ripper GET, and troubleshooting. H = (10 % × 7 %) + (10 % × 15 %) 7 % + 0,4 % + 0,03 % = 9 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CL9 – ripper up

H: 10 % walk around, 10 % machine wash, and all of transport load / unload, ripper GET, and troubleshooting. H = (10 % × 7 %) + (10 % × 15 %) 7 % + 0,4 % + 0,03 % = 9 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CL10 – machine speed

H: Only dangerous in reverse (40 %). 90 % factor to account for idle time. H = 40 % × 90 % = 36 %

P: P: Construction site co-worker rate. P = 20 %

AC: AC1 - Inching pedal or bucket lower to ground which would be normal practice for crawler operators

AW: AW2

AR: AR3

CL11 – machine direction

H: Only dangerous in the last 10 % of reverse legs. 90 % idle correction. H = 4 % × 90 % = 4 %

P: Machine moves significantly less than wheel loader and would not travel as far outside of work area. P = 25 %

AC: AC1 – brakes

AW: AW2

AR: AR3

CL12 – engine speed

H: Portion of the cycle where operator is exposed to the heat. H = 25 %

P: Operator present during the whole cycle. P = 100 %

AC: AC0

O.2.2 Application use cases

Table O.2 — Application use case table

Application	Traveling	Dozing / spreading / compacting	Ripping	Loading / carrying	Excavation	Material handling	Drawbar / winch	Tow / retrieval	Maintenance
General (demolition, construction, waste)	20 %	80 %	15 %	60 %	80 %	10 %	10 %	3 %	5 %
Steel mill	10 %	30 %	0 %	70 %	0 %	0 %	0 %	5 %	5 %
Ship hold/ port handling	10 %	95 %	0 %	0 %	0 %	0 %	0 %	0 %	5 %

O.2.3 Maintenance task breakdown

Table O.3 — Maintenance task breakdown

	Time (min/ day)	% Maintenance time
refueling	5	17 %
transport loading / unloading	2	7 %
greasing	10	34 %
walk around	2	7 %
machine wash	4,3	15 %
window wash	2	7 %
change bucket / GET	0,17	0,6 %
change ripper / GET	0,11	0,4 %
adjust track	0,7	2 %
troubleshooting	0,01	0,03 %
oil sampling	0,17	0,6 %
clean undercarriage	3	10 %
install lift arm lock	0,07	0,2 %

O.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table O.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
slow/stop	1				Machine does not travel fast enough to make uncommanded brake a dangerous hazard
hold still	1				Considered same as uncommanded release
steering			1		Failure on demand considered the same as uncommanded activation
tool curl			1		
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

Table O.4 *(continued)*

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
tool dump			1		
boom raise			1		
boom lower			1		
clam open			1		
clam shut			1		
coupler				1	Multiple failures required for coupler to be dangerous. Assumes "hinged " or "hooked" coupler
ripper down			1		
ripper up			1		
winch in			1		Uncommon attachment
winch out			1		Uncommon attachment
implement lockout	1				
auxiliary flow			1		
machine speed			1		
machine direction	1				Other failure types considered no worse than failure to apply on demand
engine speed			1		
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

O.2.5 Notes and assumptions

— Winch is an uncommon attachment and was not assessed.

— Multiple failures required for coupler to be dangerous. Assumes "hinged " or "hooked" coupler.

O.3 MPL_r mapped to SCS table

Table O.5 shows function-based MPL_r (see Table O.1) mapped to SCS per the results of the MCSSA for a crawler loader. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table O.1 would also be mapped to these MPL_r.

Table O.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
slow/stop	failure to apply on demand	**b**	service brakes
hold still	failure to apply on demand	**c**	park brakes
steering	uncommanded activation	**c**	steering
tool curl	uncommanded activation	**a**	tool curl
tool dump	uncommanded activation	**b**	tool dump
boom raise	uncommanded activation	**c**	boom raise
boom lower	uncommanded activation	**c**	boom lower
Ripper down	uncommanded activation	**a**	ripper down
ripper up	uncommanded activation	**b**	ripper up
clam open	uncommanded activation	**c**	clam open
clam shut	uncommanded activation	**b**	clam shut
auxiliary flow	uncommanded activation	**c**	auxiliary flow
implement lockout	Failure to apply on demand	**c**	implement lockout

Table O.5 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
machine speed	uncommanded activation	**b**	propel
machine direction	Failure to apply on demand	**a**	gear direction control
engine speed	uncommanded activation	**c**	throttle

Annex P
(normative)

Wheeled dozer performance level tables

P.1 Wheeled dozer

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables P.1 to P.5) or in Clause 5.

Table P.1 — MPL_r table for wheeled dozer

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CO3	**blade lift**	same as landfill compactors													**b**
LW7	**blade lower**	same as large wheel loader boom lower													**b**
LW8-9	**hold still**	same as large wheel loader													**c**
LW13	**machine direction**	same as large wheel loader													**c**
LW1-3	**machine speed**	same as large wheel loader													**b**
RD13	**powered access**	same as rigid frame trucks													**c**
WD1	**ripper raise**	maintenance	uncommanded activation	no significant injury	maintainer	S0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**QM**
WD3	**transmission neutralize**	slow speed maneuvering	uncommanded deactivation	collision	bystander	S3	6 %	20 %	25 %	E0	AC1	AW2	AR3	C1	**a**
WD2	**ripper lower**	maintenance	uncommanded activation	crushed foot	maintainer	S2	5 %	5 %	75 %	E0	AC0	N/A	N/A	C3	**b**
LW8-9		no worse than uncommanded hold still													**c**
LW13-15	**slow/stop**	same as large wheel loader													**c**
LW10-11	**steering**	same as large wheel loader													**d**
LW7	**tilt left / right**	same as uncommanded blade lower													**b**

P.2 Supporting explanation

P.2.1 Supporting explanations for dominant scenarios

WD1 – ripper raise

H: N / A

P: N / A

AC: N / A

WD2 – ripper lower

H: 5 % of machine wash and all of troubleshooting and get replace – ripper. H = (5 % × 10 %) + 2 % + 2 % = 5 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

WD3 – transmission neutralize

H: Time when machine is idle while waiting. H = 20 %

P: Typical bystander rate in central / parking areas. P = 25 %.

AC: AC1 – brakes

AW: AW2

AR: AR3 – The brakes would be under foot and the machine moves slowly

P.2.2 Application use cases

Table P.2 — Application use case table

Application	Traveling	Dozing	Ripping	Slow speed manoeuvring	Maintenance
general	50 %	80 %	10 %	6 %	5 %

P.2.3 Maintenance task breakdown

Table P.3 — Maintenance task breakdown

	Time (min/ day)	% Maintenance time
walk around	20	40 %
camera clean	2	4 %
refueling	10	20 %
oil sampling	1	2 %
greasing	5	10 %
change blade / GET[a]	1	2 %
change ripper / GET[a]	1	2 %
machine wash	5	10 %
window wash	2	4 %

[a] Ground engaging Tool (GET) change only considers the portion of the task required to block the implement.

Table P.3 *(continued)*

	Time (min/ day)	% Maintenance time
troubleshooting	1	2 %
install articulation lock	1	2 %
static brake test	1	2 %
[a] Ground engaging Tool (GET) change only considers the portion of the task required to block the implement.		

P.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table P.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
slow/stop	1				
hold still	1				Uncommanded deactivation is the same as failure to apply on demand.
steering			1		Failure on demand is considered the same as uncommanded activation.
tilt left			1		
tilt right			1		
tip back			1		
tip foreword			1		
ripper raise			1		
ripper lower			1		
blade lift				1	
blade lower			1		
machine speed			1		
machine direction	1				Uncommanded activation is the same as uncommanded hold still.
powered access			1		
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

P.2.5 Notes and assumptions

— Co-worker is a person in another machine.

— Bystander is a pedestrian.

P.3 MPL_r mapped to SCS table

Table P.5 shows function-based MPL_r (see Table P.1) mapped to SCS per the results of the MCSSA for a wheeled dozer. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table P.1 would also be mapped to these MPL_r.

Table P.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
blade lift	uncommanded activation	**b**	**blade lift**
blade lower	uncommanded activation	**b**	**blade lower**
hold still	failure to apply on demand	**c**	**parking brake**
machine direction	failure to apply on demand	**c**	**gear direction control**
machine speed	uncommanded activation	**b**	**propel**
powered access	uncommanded activation	**c**	**powered access**
ripper raise	uncommanded activation	**QM**	**ripper raise**
ripper lower	uncommanded activation	**c**	**ripper lower**
slow/stop	uncommanded activation	**c**	**service brakes**
steering	uncommanded activation	**d**	**steering**
tilt left / right	uncommanded activation	**b**	**tilt left / right**
transmission neutralize	uncommanded deactivation	**a**	**gear direction control**

Annex Q
(normative)

Scraper performance level tables

Q.1 Scrapers

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables Q.1 to Q.5) or in Clause 5.

Table Q.1 — MPL_r table for scrapers

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
SC1	**slow/stop**	traveling	failure to apply on demand	collision	operator	S1	80 %	40 %	100 %	E2	AC1	AW2	AR2	C2	**b**
SC2		traveling	failure to apply on demand	collision	bystander	S3	80 %	1 %	100 %	E0	AC1	AW2	AR2	C2	
SC3		traveling	uncommanded activation	unexpected jerk of operator	operator	S1	80 %	100 %	100 %	E2	AC0	N/A	N/A	C3	**c**
SC4	**hold still**	maintenance	failure to apply on demand	run over	maintainer	S3	5 %	12 %	75 %	E0	AC1	AW2	AR3	C1	**a**
LW8-9		Considered same as wheel loader													**c**
SC5	**steering**	traveling	uncommanded activation	collision	operator	S1	80 %	100 %	100 %	E2	AC0	N/A	N/A	C3	**c**
SC6		traveling	uncommanded activation	collision	bystander	S3	80 %	100 %	1 %	E0	AC0	N/A	N/A	C3	
SC3	**bowl down**	Considered same as uncommanded stop													**c**
SC7	**apron down**	maintenance	uncommanded activation	crushed limb	maintainer	S2	5 %	1 %	75 %	E0	AC0	N/A	N/A	C3	**b**
SC8	**bail down**	slow speed manoeuvring	uncommanded activation	hit by falling bail	bystander	S2	12 %	50 %	25 %	E1	AC0	N/A	N/A	C3	**c**
SC9	**machine speed**	slow speed manoeuvring	uncommanded activation	run over by machine	bystander	S3	12 %	10 %	100 %	E1	AC1	AW2	AR3	C1	**b**
SC10	**machine direction**	slow speed manoeuvring	failure to apply on demand	run over by machine	bystander	S3	12 %	10 %	25 %	E0	AC1	AW2	AR3	C1	**a**
SC11	**transmission neutralize**	slow Speed maneuvering	uncommanded deactivation	collision	bystander	S3	12 %	20 %	25 %	E0	AC1	AW2	AR3	C1	**a**
RD13	**powered access ladder**	considered the same as trucks													**c**
SC3	**implement lockout**	same as the systems it controls													**c**

Q.2 Supporting explanation

Q.2.1 Supporting explanations for dominant scenarios

SC1 – slow/stop

H: 40 % of time is cornering. H = 40 %

P: Operator present during the whole cycle. P = 100 %

AC: AC1 - Lower bowl or use park brake

AW: AW2

AR: AR2

SC2 – slow/stop

H: Only when stopping to avoid hitting a bystander. H = 1 %

P: Always present during an emergency. P = 100 %

AC: AC1 - Lower bowl or use park brake

AW: AW2

AR: AR2

SC3 – slow/stop

H: Hazard exists during the whole cycle. H = 100 %

P: Operator present during the whole cycle. P = 100 %

AC: AC0

SC4 – hold still

H: 20 % of grease, 20 % of walk-around, 20 % of machine wash, 25 % of window wash, 50 % of oil sampling, and all of change cutting edge and troubleshooting. H = (20 % × 32 %) + (20 % × 16 %) + (20 % × 5 %) + (25 % × 3 %) + (50 % × 1 %) + 0,03 % + 0,03 % = 12 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC1 - implement on ground or chocks

AW: AW2

AR: AR3

SC5 – steering

H: Hazard exists during the whole cycle. H = 100 %

P: Operator present during the whole cycle. P = 100 %

AC: AC0

SC6 – steering

H: Hazard exists during the whole cycle. H = 100 %

P: Rare that a person is in the work zone. P = 1 %

AC: AC0

SC7 – apron down

H: Momentary during wash. H = 1 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

SC8 – bail down

H: Idle up to 50 %. H = 50 %

P: Typical park up area. P = 25 %

AC: AC0

SC9 – machine speed

H: Only hazardous when slowing down to avoid hitting someone. H = 10 %

P: Always present during an emergency. P = 100 %

AC: AC1 – brakes

AW: AW2

AR: AR3

SC10 – machine direction

H: Scrapers are rarely reversed compared to other machines. H = 10 %

P: Typical park up area. P = 25 %

AC: AC1 – brakes

AW: AW2

AR: AR3

SC11 – transmission neutralize

H: Time when machine is idle while waiting. H = 20 %

P: Typical bystander rate in central / parking areas. P = 25 %.

AC: AC1 – brakes

AW: AW2

AR: AR3 – The brakes would be under foot and the machine moves slowly

Q.2.2 Application use cases

Table Q.2 — Application use case table

Application	Traveling	Loading	Unloading	Coupling / decoupling	Slow speed manoeu-vring	Maintenance
construction	80 %	20 %	10 %	5 %	12 %	5 %

Q.2.3 Maintenance task breakdown

Table Q.3 — Maintenance task breakdown

	Time (min/ day)	% Maintenance time
refueling	26	42 %
transport load / unload	0,4	0,7 %
greasing	20	32 %
walk around	10	16 %
machine wash	3	5 %
window wash	2	3 %
change cutting edge	0,02	0,04 %
change bits	0,02	0,04 %
troubleshooting	0,02	0,03 %
oil sampling	0,33	0,5 %

Q.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table Q.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
slow/stop	1		1		
hold still	1				
steering			1		
bowl up			1		
bowl down			1		
apron up			1		
apron down			1		
ejector forward			1		
ejector back			1		
bail up			1		
bail down			1		
elevator forward			1		
elevator reverse			1		
machine speed			1		
machine direction	1				Uncommanded activation is the same as uncommanded stop.
powered access			1		
implement lockout	1				

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

Q.2.5 Notes and assumptions

— Co-worker is a person in another machine.

— Bystander is a pedestrian.

Q.3 MPL_r mapped to SCS table

Table Q.5 shows function-based MPL_r (see Table Q.1) mapped to SCS per the results of the MCSSA for a scraper. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table Q.1 would also be mapped to these MPL_r.

Table Q.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
slow/stop	failure to apply on demand	**b**	**service brakes**
	uncommanded activation	**c**	
hold still	failure to apply on demand	**c**	**parking brake**
steering	uncommanded activation	**c**	**steering**
bowl down	uncommanded activation	**c**	**bowl down**
apron down	uncommanded activation	**b**	**apron down**
bail down	uncommanded activation	**c**	**bail down**
machine speed	uncommanded activation	**b**	**propel**
machine direction	failure to apply on demand	**a**	**gear direction control**
powered access ladder	uncommanded activation	**c**	**powered access ladder**
implement lockout	uncommanded activation	**c**	**implement lockout**
transmission neutralize	uncommanded deactivation	**a**	**gear direction control**

Annex R
(normative)

Crawler excavators equal to or greater than 109 000 kg performance level tables

R.1 Crawler excavators equal to or greater than 109 000 kg

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables R.1 to R.5) or in Clause 5.

Table R.1 — MPL_r table for crawler excavators equal to or greater than 109 000 kg

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
HX1	**left track forward**	truck loading	uncommanded activation	machine falls off edge	operator	S3	90 %	27 %	100 %	E2	AC1	AW3	AR3	C0	**b**
HX2		maintenance	uncommanded activation	person run over	maintainer	S3	5 %	1 %	75 %	E0	AC1	AW2	AR2	C2	
HX3	**boom raise**	maintenance	uncommanded activation	implement knocks maintainer off platform (external to machine)	maintainer	S3	5 %	2 %	75 %	E0	AC0	N/A	N/A	C3	**c**
HX3	**boom lower**	considered same as boom raise													**c**
HX3	**bucket curl**	considered same as boom raise													**c**
HX3	**bucket dump**	considered same as boom raise													**c**
HX4	**clam open**	maintenance	uncommanded activation	crushed limb	maintainer	S2	5 %	1 %	75 %	E0	AC0	N/A	N/A	C3	**b**
HX4	**clam shut**	considered to be the same as clam open													**b**
HX3	**arm out**	considered same as boom raise													**c**
HX3	**arm in**	considered same as boom raise													**c**
HX5	**slew / swing start**	maintenance	uncommanded activation	person crushed between machine and object	maintainer	S3	5 %	7 %	75 %	E0	AC0	N/A	N/A	C3	**c**
HX6	**slew / swing stop**	truck loading	failure to apply on demand	bucket contacts cab of truck	co-worker	S3	90 %	2 %	100 %	E1	AC1	AW2	AR3	C1	**b**
HX7	**slew / swing hold still**	maintenance	failure to apply on demand	person crushed between machine and object	maintainer	S3	5 %	17 %	75 %	E0	AC0	N/A	N/A	C3	**c**
HX8	**engine speed**	cannot cause increase in implement speed, therefore no significant hazard													

Table R.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
HX9	**travel speed**	maintenance	uncommanded activation	run over by machine	maintainer	S3	5 %	1 %	75 %	E0	AC1	AW2	AR2	C2	**b**
HX10	**travel hold still**	maintenance	failure to apply on demand	run over by machine	maintainer	S3	5 %	1 %	75 %	E0	AC0	N/A	N/A	C3	**c**
HX11	**powered access ladder movement**	maintenance	uncommanded activation	legs caught in ladder causing fall backwards	maintainer	S2	5 %	7 %	75 %	E0	AC0	N/A	N/A	C3	**b**
HX12	**powered access ladder interlock**	maintenance	failure to apply on demand	person pinched between ladder and machine or wall	maintainer	S3	5 %	12 %	75 %	E0	AC0	N/A	N/A	C3	**c**
HX13	**service centre motion**	maintenance	uncommanded activation	person has service centre come down on head	maintainer	S1	5 %	3 %	75 %	E0	AC0	N/A	N/A	C3	**a**
HX14	**service centre interlock**	maintenance	failure to apply on demand	person pinched between machine and service centre	maintainer	S3	5 %	28 %	50 %	E0	AC0	N/A	N/A	C3	**c**
HX15	**machine lockout**	maintenance	failure to apply on demand	person crushed between machine and object	maintainer	S3	5 %	4 %	75 %	E0	AC0	N/A	N/A	C3	**c**

R.2 Supporting explanation

R.2.1 Supporting explanations for dominant scenarios

HX1 – left track forward

H: All of the cycle except for digging (60 %), only in one direction (50 %), and idle factor (90 %). H = 60 % × 50 % × 90 % = 27 %

P: Operator present during the whole cycle. P = 100 %

AC: AC1 - E-stop and implement

AW: AW3 - Operator becomes aware of hazard before it is dangerous because of the slow movement of the machine

AR: AR3 - Implement is in hand

HX2 – left track forward

H: All of manoeuvring (travel / swing) in maintenance area and troubleshooting. H = 0,2% + 1 % = 1 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC1 – Travel hold still and e-stop

AW: AW2

AR: AR2

HX3 – boom raise

H: 80 % of aligning linkage for exchange of components, 25 % of machine wash and all of troubleshooting. H = (80 % × 0,3 %) + (25 % × 2 %) + 1 % = 2 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

HX4 – clam open

H: 10 % of aligning linkage for exchange of components and all of troubleshooting. H = (10 % × 0,3 %) + 1 % = 1 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

HX5 – slew / swing start

H: 25 % of daily inspection and all of aligning linkage for exchange of components and troubleshooting. H = (25 % × 24 %) + 0,2 % + 1 % = 7 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

HX6 – slew / swing stop

H: 25 % of vertical, 40 % of horizontal, idle factor of 90 %, swing of 20 % of cycle. H = 25 % × 40 % × 90 % × 20 % = 2 %

P: Always present during an emergency. P = 100 %

AC: AC1 - E-stop or move implement in hand

AW: AW2

AR: AR3

HX7 – slew / swing hold still

H: 25 % of daily inspection, 50 % of machine wash, 50 % of camera clean and all of aligning linkage for exchange of components and troubleshooting. H = (25 % × 24 %) + (50 % × 2 %) + (50 % × 18 %) + 0,3% + 1 % = 17 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

HX8 – engine speed

H: All of aligning linkage for exchange of components and troubleshooting. H = 0,2% + 1 % = 1 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC1 - implement

AW: AW3 - Engine speed increases slowly

AR: AR3 - Implement control is in hand

HX9 – travel speed

H: All of manoeuvring (travel / swing) in maintenance area and troubleshooting. H = 0,2% + 1 % = 1 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC1 – E-stop

AW: AW2

AR: AR2

HX10 – travel hold still

H: All of aligning linkage for exchange of components and troubleshooting. H = 0,2% + 1 % = 1 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

HX11 – powered access ladder movement

H: 20 % of access / egress machine, 5 % of daily inspection, 5 % of machine wash, 5 % of camera clean and all of troubleshooting. H = (20 % × 18 %) + (5 % × 24 %) + (5 % × 2 %) + (5 % × 18 %) + 1 % = 7 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

HX12 – powered access ladder interlock

H: 50 % of access / egress machine, 5 % of daily inspection, 5 % of machine wash, 5 % of camera clean and all of troubleshooting. H = (50% × 18 %) + (5 % × 24 %) + (5 % × 2 %) + (5 % × 18 %) + 1 % = 12 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

HX13 – service centre motion

H: 2 % of daily inspection, 5 % of refuelling / refilling / fluid top off, 5 % of oil sampling, 2 % of machine wash, and all of troubleshooting. H = (2 % × 24 %) + (5 % × 24 %) + (5 % × 1 %) + (2 % × 2 %) + 1 % = 3 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

HX14 – service centre interlock

H: 10 % of daily inspection and all of refuelling / refilling / fluid top off, oil sampling, and troubleshooting. H = (10 % × 24 %) + 24 % + 1 % + 1 % = 28 %

P: Need to be standing in a very specific area. P = 50 %

AC: AC0

HX15 – machine lockout

H: All of machine wash and troubleshooting. H = 2 % + 1 % = 3 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

R.2.2 Application use cases

Table R.2 — Application use case table

Application	Truck loading	General excavation	Dropping balls to crush rocks	Traveling	Maintenance
mining and quarry	90 %	15 %	5 %	10 %	5 %
construction	90 %	15 %	0 %	10 %	5 %

R.2.3 Maintenance task breakdown

Table R.3 — Maintenance task breakdown

	Time (min/day)	% Maintenance time
access / egress machine	15	18 %
maneuvering (travel / swing) in maintenance area	0,25	0,3 %
daily inspection	20	24 %
refueling / refilling / fluid top off	20	24 %
aligning linkage for exchange of components	0,25	0,3 %
oil sampling	1	1 %
machine wash	2	2 %
window wash	10	12 %
troubleshooting	1	1 %

Table R.3 *(continued)*

	Time (min/ day)	% Maintenance time
camera clean	15	18 %

R.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table R.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
left track forward			1		Failure to apply on demand, failure to release on demand, uncommanded activation, and uncommanded deactivation all result in an uncommanded steer.
left track back					It is the same as left track forward.
right track forward					It is the same as left track forward.
right track back					It is the same as left track forward.
engine speed			1		
travel speed			1		
boom raise			1		
boom lower			1		
clam open			1		
clam shut			1		
arm in			1		
arm out			1		
bucket curl			1		
bucket dump			1		
Slew / swing start			1		Uncommanded activation is the same as uncommanded stop.
slew / swing stop	1				
Slew/swing hold still	1				
travel hold still	1				
powered access ladder movement			1		
powered access ladder interlock	1				Other failure types are considered no worse than failure to apply on demand.
service centre motion			1		
service centre interlock	1				
machine lockout	1				
cable reel			1		

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

R.2.5 Notes and assumptions

— It is considered machine abuse to load the truck from the front.

— Co-worker is a person in another machine.

— Bystander is a pedestrian or in a light vehicle.

— Bucket dropping onto truck body without swinging is S0.

— It is considered machine abuse to operate a shovel under power lines.

R.3 MPL_r mapped to SCS table

Table R.5 shows function-based MPL_r (see Table R.1) mapped to SCS per the results of the MCSSA for a crawler excavators equal to or greater than 109 000 kg. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table R.1 would also be mapped to these MPL_r.

Table R.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
left track forward	uncommanded activation	**b**	**track motion**
boom raise	uncommanded activation	**c**	**boom raise**
boom lower	uncommanded activation	**c**	**boom lower**
bucket curl	uncommanded activation	**c**	**bucket curl**
bucket dump	uncommanded activation	**c**	**bucket dump**
clam open	uncommanded activation	**b**	**clam open**
clam shut	uncommanded activation	**b**	**clam shut**
arm in	uncommanded activation	**c**	**arm in**
arm out	uncommanded activation	**c**	**arm out**
slew / swing start	uncommanded activation	**c**	**slew / swing start**
slew / swing stop	failure to apply on demand	**b**	**slew / swing stop**
slew / swing hold still	failure to apply on demand	**c**	**slew / swing hold still**
engine speed	no hazard	**N/A**	**throttle**
travel speed	uncommanded activation	**b**	**propel**
travel hold still	failure to apply on demand	**c**	**brake**
powered access ladder movement	uncommanded activation	**b**	**powered access ladder movement**
powered access ladder interlock	failure to apply on demand	**c**	**powered access ladder interlock**
service centre movement	uncommanded activation	**a**	**service centre movement**
service centre interlock	failure to apply on demand	**c**	**service centre interlock**
machine lockout	failure to apply on demand	**c**	**machine lockout**
cable reel	no hazard	**N/A**	**cable reel**

Annex S
(normative)

Cable excavator (front shovel) performance level tables

S.1 Cable excavator (front shovel)

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables S.1 to S.5) or in Clause 5.

Table S.1 — MPL_r table for cable excavator (front shovel)

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CS1	**engine speed**	maintenance	uncommanded activation	implement knocks maintainer off platform	maintainer	S3	5 %	7 %	75 %	E0	AC0	N/A	N/A	C3	**c**
CS2	**crowd hold still**	considered same as hoist raise													**c**
CS2	**crowd in**	considered same as hoist raise													**c**
CS2	**crowd out**	considered same as hoist raise													**c**
CS2	**hoist hold still**	considered same as hoist raise													**c**
CS2	**hoist lower**	considered same as hoist raise													**c**
CS2	**hoist raise**	maintenance	uncommanded activation	implement knocks maintainer off platform	maintainer	S3	5 %	6 %	75 %	E0	AC0	N/A	N/A	C3	**c**
CS3	**left track forward**	maintenance	uncommanded activation	run over by machine	maintainer	S3	5 %	2 %	75 %	E0	AC1	AW2	AR2	C2	**b**
CS4	**machine lockout**	maintenance	failure to apply on demand	person crushed between machine and object	maintainer	S3	5 %	4 %	75 %	E0	AC0	N/A	N/A	C3	**c**
CS5	**powered access ladder interlock**	maintenance	failure to apply on demand	person pinched between ladder and machine or wall	maintainer	S3	5 %	14 %	75 %	E0	AC0	N/A	N/A	C3	**c**
CS6	**powered access ladder movement**	maintenance	uncommanded activation	legs caught in ladder causing fall backwards	maintainer	S2	5 %	8 %	75 %	E0	AC0	N/A	N/A	C3	**b**
CS7	**slew / swing start**	maintenance	uncommanded activation	person crushed between machine and object	maintainer	S3	5 %	8 %	75 %	E0	AC0	N/A	N/A	C3	**c**
CS8	**slew / swing stop / hold still**	maintenance	failure to apply on demand	person crushed between machine and object	maintainer	S3	5 %	26 %	75 %	E0	AC0	N/A	N/A	C3	**c**
CS9	**travel hold still**	maintenance	failure to apply on demand	run over by machine	maintainer	S3	5 %	7 %	75 %	E0	AC0	N/A	N/A	C3	**c**
CS10	**travel speed**	maintenance	uncommanded activation	run over by machine	maintainer	S3	5 %	2 %	75 %	E0	AC1	AW2	AR2	C2	**b**

S.2 Supporting explanation

S.2.1 Supporting explanations for dominant scenarios

CS1 – engine speed

H: All of rope change and troubleshooting. H = 6 % + 1,4 % = 7 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CS2 – hoist raise

H: 80 % of rope change and all of troubleshooting. (80 % × 6 %) + 1,4 % = 6 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CS3 – left track forward

H: All of manoeuvring (travel / swing) in maintenance area and all of troubleshooting. H = 0,3 % + 1,4 % = 2 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC1 – Travel hold still and e-stop

AW: AW2

AR: AR2

CS4 – machine lockout

H: All of machine wash and all of troubleshooting. 3 % + 1,4 % = 4 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CS5 – powered access ladder interlock

H: 50 % of access / egress machine, 5 % of daily inspection, 5 % of machine wash, and 5 % of camera clean and all of troubleshooting. H = (50 % × 20 %) + (5 % × 27 %) + (5 % × 3 %) + (5 % × 20 %) + 1,4 % = 14 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CS6 – powered access ladder movement

H: 20 % of access / egress machine, 5 % of daily inspection, 5 % of refuelling / refilling / fluid top off, 5 % of machine wash, and 5 % of camera clean and all of troubleshooting. H = (20 % × 20 %) + (5 % × 27 %) + (5 % × 7 %) + (5 % × 3 %) + (5 % × 20 %) + 1,4 % = 8 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CS7 – slew / swing start

H: 25 % of daily inspection and all of manoeuvring (travel / swing) in maintenance area and all of troubleshooting. H = (25 % × 27 %) + 0,3 % + 1,3 % = 8 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CS8 –slew / swing stop / hold still

H: 25 % of daily inspection, 50 % of machine wash, 50 % of camera clean and all rope change and all of troubleshooting. H = (25 % × 27 %) + (50 % × 3 %) + (50 % × 20 %) + 6 % + 1,3 % = 26 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CS9 – travel hold still

H: All of rope change and all of troubleshooting. H = 6 % + 1,3 % = 7 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

CS10 – travel speed

H: All of manoeuvring (travel / swing) in maintenance area and all of troubleshooting. H = 0,3 % + 1,4 % = 2 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC1 – E-stop

AW: AW2

AR: AR2

S.2.2 Application use cases

Table S.2 — Application use case table

Application	Truck loading	Excavation (no truck)	Traveling	Maintenance
rope shovel	95 %	10 %	5 %	5 %

S.2.3 Maintenance task breakdown

Table S.3 — Maintenance task breakdown

	Time (min/ day)	% Maintenance time
access / egress machine	15	20 %
maneuvering (travel / swing) in maintenance area	0,25	0,3 %
daily inspection	20	27 %
refueling / refilling / fluid top off	5	7 %
rope change	4,2	6 %
oil sampling	1	1 %
machine wash	2	3 %

Table S.3 *(continued)*

	Time (min/ day)	% Maintenance time
window wash	10	14 %
troubleshooting	1	1,4 %
camera clean	15	20 %

S.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table S.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
left track forward			1		Failure to apply on demand, failure to release on demand, uncommanded activation, and uncommanded deactivation all result in an uncommanded steer.
left track back					It is the same as left track forward.
right track forward					It is the same as left track forward.
right track back					It is the same as left track forward.
travel speed			1		
engine speed			1		
hoist raise			1		
hoist lower			1		
hoist hold still	1				
crowd in			1		
crowd out			1		
crowd hold still	1				
bucket dump			1		It is only applicable to shovels – not drag lines.
slew / swing start			1		
slew / swing stop / hold still	1				
Travel hold Still	1				
powered access ladder movement			1		
powered access ladder interlock	1				Other failure types considered no worse than failure to apply on demand.
machine lockout	1				
cable reel			1		Grid power only

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

S.2.5 Notes and assumptions

— Taking a bucket off a drag line and putting on a clam shell causes the machine to become a foundation excavation machine falling under ISO TC 195.

— Taking off a bucket and adding a wrecking ball, material handling, or other attachments is derivation defined in ISO 6165, but will not be assessed in this assessment. Manufacturers should assess these themselves.

— Using hydraulic shovel cycle times.

— This does not consider walking drag lines.

S.3 MPL_r mapped to SCS table

Table S.5 shows function-based MPL_r (see Table S.1) mapped to SCS per the results of the MCSSA for a cable excavator (front shovel). Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table S.1 would also be mapped to these MPL_r.

Table S.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
engine speed	uncommanded activation	**c**	**throttle**
crowd hold still	failure to apply on demand	**c**	**crowd hold still**
crowd in	uncommanded activation	**c**	**crowd in**
crowd out	uncommanded activation	**c**	**crowd out**
hoist hold still	failure to apply on demand	**c**	**hoist hold still**
hoist lower	uncommanded activation	**c**	**hoist lower**
hoist raise	uncommanded activation	**c**	**hoist raise**
left track forward	uncommanded activation	**b**	**track motion**
machine lockout	failure to apply on demand	**c**	**machine lockout**
powered access ladder interlock	failure to apply on demand	**c**	**powered access ladder interlock**
powered access ladder movement	uncommanded activation	**b**	**powered access ladder movement**
slew / swing start	uncommanded activation	**c**	**slew / swing start**
slew / swing stop / hold Still	failure to apply on demand	**c**	**slew / swing stop / hold still**
travel hold Still	failure to apply on demand	**c**	**brake**
travel Speed	uncommanded activation	**b**	**propel**

Annex T
(normative)

Cable excavator (dragline) performance level tables

T.1 Cable excavator (dragline)

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables T.1 to T.5) or in Clause 5.

Table T.1 — MPL_r table for cable excavator (dragline)

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
DS1	**engine speed**	maintenance	uncommanded activation	implement knocks maintainer off platform	maintainer	S3	5 %	2 %	75 %	E0	AC0	N/A	N/A	C3	**c**
DS2	**crowd hold still**	considered same as hoist raise													**c**
DS2	**crowd in**	considered same as hoist raise													**c**
DS2	**crowd out**	considered same as hoist raise													**c**
DS2	**hoist hold still**	considered same as hoist raise													**c**
DS2	**hoist lower**	considered same as hoist raise													**c**
DS2	**hoist raise**	maintenance	uncommanded activation	implement knocks maintainer off platform	maintainer	S3	5 %	2 %	75 %	E0	AC0	N/A	N/A	C3	**c**
DS3	**left track forward**	maintenance	uncommanded activation	run over by machine	maintainer	S3	5 %	2 %	75 %	E0	AC1	AW2	AR2	C2	**b**
DS4	**machine lockout**	maintenance	failure to apply on demand	person crushed between machine and object	maintainer	S3	5 %	4 %	75 %	E0	AC0	N/A	N/A	C3	**c**
DS5	**powered access ladder interlock**	maintenance	failure to apply on demand	person pinched between ladder and machine or wall	maintainer	S3	5 %	14 %	75 %	E0	AC0	N/A	N/A	C3	**c**
DS6	**powered access ladder movement**	maintenance	uncommanded activation	legs caught in ladder causing fall backwards	maintainer	S2	5 %	9 %	75 %	E0	AC0	N/A	N/A	C3	**b**
DS7	**slew / swing start**	maintenance	uncommanded activation	person crushed between machine and object	maintainer	S3	5 %	8 %	75 %	E0	AC0	N/A	N/A	C3	**c**
DS8	**slew / swing stop / hold still**	maintenance	failure to apply on demand	person crushed between machine and object	maintainer	S3	5 %	21 %	75 %	E0	AC0	N/A	N/A	C3	**c**
DS9	**travel hold still**	maintenance	failure to apply on demand	run over by machine	maintainer	S3	5 %	2 %	75 %	E0	AC0	N/A	N/A	C3	**c**
DS10	**travel speed**	maintenance	uncommanded activation	run over by machine	maintainer	S3	5 %	2 %	75 %	E0	AC1	AW2	AR2	C2	**b**

T.2 Supporting explanation

T.2.1 Supporting explanations for dominant scenarios

DS1 – engine speed

H: All of rope change and troubleshooting. H = 1 % + 1 % = 2 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

DS2 – hoist raise

H: 80 % of rope change and all of troubleshooting. (80 % × 1 %) + 1 % = 2 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

DS3 – left track forward

H: All of manoeuvring (travel / swing) in maintenance area and all of troubleshooting. H = 0,3 % + 1,4 % = 2 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC1 – Travel hold still and e-stop

AW: AW2

AR: AR2

DS4 – machine lockout

H: All of machine wash and all of troubleshooting. 3 % + 1,4 % = 4 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

DS5 – powered access ladder interlock

H: 50 % of access / egress machine, 5 % of daily inspection, 5 % of machine wash, and 5 % of camera clean and all of troubleshooting. H = (50 % × 20 %) + (5 % × 27 %) + (5 % × 3 %) + (5 % × 20 %) + 1,4 % = 14 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

DS6 – powered access ladder movement

H: 20 % of access / egress machine, 5 % of daily inspection, 5 % of refuelling / refilling / fluid top off, 5 % of machine wash, and 5 % of camera clean and all of troubleshooting. H = (20 % × 20 %) + (5 % × 27 %) + (5 % × 27 %) + (5 % × 3 %) + (5 % × 20 %) + 1,4 % = 9 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

DS7 – slew / swing start

H: 25 % of daily inspection and all of manoeuvring (travel / swing) in maintenance area and all of troubleshooting. H = (25 % × 27 %) + 0,3 % + 1,3 % = 8 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

DS8 – slew / swing stop / hold still

H: 25 % of daily inspection, 50 % of machine wash, 50 % of camera clean and all rope change and all of troubleshooting. H = (25 % × 27 %) (50 % × 3 %) + (50 % × 20 %) +1 % + 1,3 % = 21 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

DS9 – travel hold still

H: All of rope change and all of troubleshooting. H = 1 % + 1,3 % = 2 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC0

DS10 – travel speed

H: All of manoeuvring (travel / swing) in maintenance area and all of troubleshooting. H = 0,3 % + 1,4 % = 2 %

P: Maintenance task on / off machine split. P = 75 %

AC: AC1 – E-stop

AW: AW2

AR: AR2

T.2.2 Application use cases

Table T.2 — Application use case table

Application	Truck loading	Excavation (no truck)	Traveling	Maintenance
dragline	5 %	95 %	5 %	5 %

T.2.3 Maintenance task breakdown

Table T.3 — Maintenance task breakdown

	Time (min/ day)	% Maintenance time
access / egress machine	15	20 %
maneuvering (travel / swing) in maintenance area	0,25	0,3 %
daily inspection	20	27 %
refueling / refilling / fluid top off	20	27 %
rope change	0,6	1 %
oil sampling	1	1 %
machine wash	2	3 %

Table T.3 *(continued)*

	Time (min/ day)	% Maintenance time
window wash	10	14 %
troubleshooting	1	1,4 %
camera clean	15	20 %

T.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table T.4 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
left track forward			1		Failure to apply on demand, failure to release on demand, uncommanded activation, and uncommanded deactivation all result in an uncommanded steer.
left track back					It is the same as left track forward.
right track forward					It is the same as left track forward.
right track back					It is the same as left track forward.
travel speed			1		
engine speed			1		
hoist raise			1		
hoist lower			1		
hoist hold still	1				
crowd in			1		
crowd out			1		
crowd hold still	1				
bucket dump			1		It is only applicable to shovels – not drag lines.
slew / swing start			1		
slew / swing stop / hold still	1				
travel hold still	1				
powered access ladder movement			1		
powered access ladder interlock	1				Other failure types are considered no worse than failure to apply on demand.
machine lockout	1				
cable reel			1		Grid power only

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

T.2.5 Notes and assumptions

— Taking a bucket off a drag line and putting on a clam shell causes the machine to become a foundation excavation machine falling under ISO TC 195.

— Taking off a bucket and adding a wrecking ball, material handling, or other attachments is derivation defined in ISO 6165, but will not be assessed in this assessment. Manufacturers should assess these themselves.

— Using hydraulic shovel cycle times.

— This does not consider walking drag lines.

T.3 MPL_r mapped to SCS table

Table T.5 shows function-based MPL_r (see Table T.1) mapped to SCS per the results of the MCSSA for a cable excavator (dragline). Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table T.1 would also be mapped to these MPL_r.

Table T.5 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
engine speed	uncommanded activation	**c**	**throttle**
crowd hold still	failure to apply on demand	**c**	**crowd hold still**
crowd in	uncommanded activation	**c**	**crowd in**
crowd out	uncommanded activation	**c**	**crowd out**
hoist hold still	failure to apply on demand	**c**	**hoist hold still**
hoist lower	uncommanded activation	**c**	**hoist lower**
hoist raise	uncommanded activation	**c**	**hoist raise**
left track forward	uncommanded activation	**b**	**track motion**
machine lockout	failure to apply on demand	**c**	**machine lockout**
powered access ladder interlock	failure to apply on demand	**c**	**powered access ladder interlock**
powered access ladder movement	uncommanded activation	**b**	**powered access ladder movement**
slew / swing start	uncommanded activation	**c**	**slew / swing start**
slew / swing stop / hold still	failure to apply on demand	**c**	**slew / swing stop / hold still**
travel hold still	failure to apply on demand	**c**	**brake**
travel speed	uncommanded activation	**b**	**propel**

Annex U
(normative)

Compact trencher less than 4 500 kg performance level tables

U.1 Compact trencher less than 4 500 kg

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables U.1 to U.4) or in Clause 5.

Table U.1 — MPL_r table for compact trencher less than 4 500 kg

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CTR1	**counter steer**	loading / unloading / transport	uncommanded activation	machine steers without input and moves off side of trailer	operator	S1	10 %	50 %	100 %	E1	AC1	AW2	AR1	C3	**b**
CTR2		loading / unloading / transport	uncommanded activation	machine steers without input and moves off side of trailer	co-worker	S2	10 %	50 %	5 %	E0	AC1	AW2	AR1	C3	
CTR3		loading / unloading / transport	uncommanded activation	machine steers without input and moves off side of trailer	bystander	S2	10 %	50 %	10 %	E0	AC1	AW2	AR1	C3	**b**
CTR4	**articulated steer**	travel	uncommanded activation	machine becomes unstable on side-slope	operator	S3	30 %	2,5 %	100 %	E0	AC1	AW2	AR2	C2	**b**
CTR1-3	**Ackermann steer - front only**	considered same as counter steer uncommanded activation													**b**
CTR1-3	**Ackermann steer - rear only**	considered same as counter steer uncommanded activation													**b**
CTR1-3	**Ackermann steer - front and rear combined**	considered same as counter steer uncommanded activation													**b**

Table U.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CTR5	**propel - speed**	boring	uncommanded activation	machine or boring components move unexpectedly and contact co-worker	co-worker	S2	50 %	2 %	25 %	E0	AC1	AW2	AR1	C3	**b**
CTR6		preparation/ set up	uncommanded activation	Machine moves (powered) unexpectedly. Only hazardous to pedestrian operator and machine moving towards them.	operator	S2	5 %	40 %	100 %	E1	AC1	AW2	AR2	C2	
CTR7	**direction (F / R)**	micro-trenching	uncommanded activation	machine contacts co-worker	co-worker	S2	80 %	12,5 %	10 %	E1	AC1	AW2	AR2	C2	**b**
CTR8	**slow/stop**	Loading / unloading / transport	failure to apply on demand	machine does not stop and goes off trailer	co-worker	S2	10 %	5 %	5 %	E0	AC1	AW2	AR1	C3	**b**
CTR9		Loading / unloading / transport	failure to apply on demand	machine does not stop and goes off trailer	bystander	S2	10 %	5 %	10 %	E0	AC1	AW2	AR1	C3	
CTR10		travel	uncommanded activation	machine stops suddenly and unexpectedly	operator	S0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**QM**
CTR11		Loading / unloading / transport	uncommanded activation	machine stops suddenly and unexpectedly	operator	S0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	

Table U.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CTR12	**hold still**	preparation/ set up	uncommanded deactivation	Machine moves (unpowered) unexpectedly. On pedestrian controlled machines, it comes into contact with the operator.	operator	S1	5 %	10 %	100 %	E0	AC1	AW1	AR0	C3	**a**
CTR13		preparation/ set up	uncommanded deactivation	machine moves (unpowered) unexpectedly and makes contact	co-worker	S1	5 %	10 %	10 %	E0	AC1	AW1	AR0	C3	**a**
CTR14	**blade down / up - blade tilt - blade float**	preparation/ set up	uncommanded activation	contacted by blade resulting in crushed limb	co-worker	S1	5 %	100 %	2 %	E0	AC1	AW1	AR0	C3	**a**
BH4-5	**hoe arm in**	considered the same as backhoe loader													**c**
BH4-5	**hoe arm out**	considered the same as backhoe loader													**c**
CTR15	**backhoe swing**	backhoe	uncommanded activation	contacted by linkage	co-worker	S2	10 %	50 %	10 %	E0	AC1	AW2	AR1	C3	**b**
CTR16	**boom down**	backhoe	uncommanded activation	contacted by linkage	co-worker	S2	10 %	25 %	2 %	E0	AC1	AW2	AR1	C3	**b**
BH3	**boom up**	considered the same as backhoe loader													**c**
BH3	**raise - backhoe stabilizer**	considered the same as backhoe loader													**c**
CTR17	**lower - backhoe stabilizer**	backhoe	uncommanded activation	contacted by stabilizer linkage	co-worker	S1	10 %	50 %	2 %	E0	AC1	AW2	AR1	C3	**a**
CTR18	**raise - reel carrier**	no worse than urban / lower-reel carrier / trenching / uncommanded activation / operator													**a**

Table U.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CTR18	**lower - reel carrier**	trenching	uncommanded activation	Lowering reel carrier raises machine. Machine tips onto operator limbs.	operator	S2	90 %	1 %	100 %	E0	AC1	AW2	AR2	C2	**a**
CTR19		trenching	uncommanded activation	machine tips onto co-worker limbs	co-worker	S2	90 %	1 %	2 %	E0	AC1	AW2	AR2	C2	
CTR20	**power wind / unwind - reel carrier**	trenching	uncommanded activation	Co-worker gets hands pinched in reel material guide.	co-worker	S0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**QM**
CTR20	**brake - reel carrier**	no worse than urban / power unwind / wind-reel carrier / trenching / uncommanded activation / co-worker													**QM**
CTR21	**side shift - rear attachment**	travel	uncommanded activation	machine becomes unstable and tips contacting operator	operator	S2	30 %	2 %	100 %	E0	AC1	AW2	AR1	C3	**b**
CTR22		preparation/ set up	uncommanded activation	machine becomes unstable and tips, contacting operator	operator	S2	5 %	4 %	100 %	E0	AC1	AW2	AR0	C3	
CTR23	**raise - rear attachment**	trenching	uncommanded activation	powered trenching tool (chain or wheel) comes out of trench and co-worker contacts, entanglement into tool	co-worker	S3	90 %	20 %	5 %	E0	AC1	AW2	AR2	C2	**b**
CTR23	**lower - rear attachment**	no worse than rear attachment raise													**b**
CTR24	**speed - rear attachment**	no worse than rear attachment on / off													**c**
CTR24	**on / off - rear attachment**	preparation/ set up	uncommanded activation	co-worker is contacted with rear attachment before in trench	co-worker	S3	5 %	80 %	5 %	E0	AC1	AW2	AR1	C3	**c**

Table U.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
	direction - rear attachment	no significant hazard													
CTR25	**on / off - boring**	boring	uncommanded activation	Using on / off of rear attachment to identify on / off of boring system. Hazard is that co-worker is struck by rod or entangled in rod.	co-worker	S2	50 %	2 %	25 %	E0	AC1	AW2	AR1	C3	**b**
CTR21	**swing -plow**	no worse than residential / side shift-rear attachment / travel / uncommanded activation / operator													**b**
	steer - plow	no significant hazard													
	raise - plow	no significant hazard													
	lower - plow	no significant hazard													
	float – raise / lower - plow	no significant hazard													
	float - swing - plow	no significant hazard													
CTR23	**raise - microtrencher**	no worse than urban / raise rear attachment / trenching / uncommanded activation / co-worker													**b**
CTR23	**lower - microtrencher**	no worse than microtrencher raise													**b**
CTR21	**side shift - microtrencher**	no worse than residential / side shift-rear attachment / travel / uncommanded activation / operator													**b**
	level – microtrencher	no significant hazard													
	depth - microtrencher	no significant hazard													
CTR24	**speed - microtrencher**	no worse than microtrencher on/off													**c**

Table U.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CTR24	**on / off - microtrencher**	no worse than urban / on / off rear attachment / preparation / setup / uncommanded activation / co-worker													**c**
	rotation direction - microtrencher	no significant hazard													

U.2 Supporting explanation

U.2.1 Supporting explanations for dominant scenarios

CTR1 – counter steer

H: Only in one direction. H = 50 %

P: Operator present during the whole cycle. P = 100 %

AC: AC1 - Can stop machine or ground tool

AW: AW2

AR: AR1

CTR2 – counter steer

H: Only in one direction. H = 50 %

P: People should not be in this area but may be momentarily. P = 5 %.

AC: AC1 - Can stop machine or ground tool

AW: AW2

AR: AR1

CTR3 – counter steer

H: Only in one direction. H = 50 %

P: Used a higher P value for bystander in urban application because more people may be passing through the hazard area. P = 10 %

AC: AC1 - Can stop machine or ground tool

AW: AW2

AR: AR1

CTR4 – articulated steer

H: It is considered machine abuse for the operator position to be on downhill slope of machine during travel. 10 % of travel time is across slopes and 25 % of this time the operator station is on the downhill side. H = 25 % × 10 % = 2,5 %

P: Operator present during the whole cycle. P = 100 %

AC: AC1 – Key switch or release controls

AW: AW2

AR: AR2

CTR5 – propel speed

H: 2 % of boring work cycle. Occurs at need to addition rods (no rotation) or only during the initial insert of the tool into the ground (rotation).

P: Co-worker is present only when rod guide is required or additional rods are needed, which is only 25 % of boring activities. P = 25 %

AC: AC1 – Key switch or reverse direction

AW: AW2

AR: AR1

CTR6 – propel speed

H: 80 % of time the machine is not moving during prep. Only hazardous when it moves towards a pedestrian operator in one direction. H = 80 % × 50 % = 40 %

P: Operator present during the whole cycle. P = 100 %

AC: AC1 – Engage service brake, key switch, or reduce engine speed

AW: AW2

AR: AR2

CTR7 – direction (F / R)

H: Hazard zone is only directly behind machine, 50 % of the quadrant (25 %). H = 25 % × 50 % = 13 %

P: Only in the hazard zone 10 %. P = 10 %

AC: AC1 – Engage service brake, key switch, or reduce engine speed

AW: AW2

AR: AR2

CTR8 – slow/stop

H: Co-worker can on one of the 4 sides and only a portion of that is the hazard zone. H = 5 %

P: People should not be in this area but may be momentarily. P = 5 %.

AC: AC1 – Engage service brake, engage park brake, reduce engine speed

AW: AW2

AR: AR1

CTR9 – slow/stop

H: Co-worker can on one of the 4 sides and only a portion of that is the hazard zone. H = 5 %

P: People should not be in this area but may be momentarily and more people than the co-worker are considered. P = 10 %.

AC: AC1 – Engage service brake, engage park brake, reduce engine speed

AW: AW2

AR: AR1

CTR10 – slow/stop

H: N/A

P: N/A

AC: N/A

CTR11 – slow/stop

H: N/A

P: N/A

AC: N/A

CTR12 – hold still

H: Considered operator on pedestrian machines when in the operator station and only hazardous to operator if it moves in the direction towards the operator station. H = 10 %

P: Operator present during the whole cycle. P = 100 %

AC: AC1 - Ground the implement

AW: AW1

AR: AR0

CTR13 – hold still

H: Only hazardous if it moves in the direction where co-worker is doing preparation activities. H = 10 %

P: Co-worker rarely required for preparation activities. P = 10 %

AC: AC1 – Ground the implement

AW: AW1

AR: AR0

CTR14 – blade up / down / blade float / blade tilt

H: Hazard exists anytime during preparation work. H = 100 %

P: Only hazardous when this activity has the co-worker near the raised blade. P = 2 %.

AC: AC1 – Key switch

AW: AW1

AR: AR0

CTR15 – backhoe swing

H: Only in one direction. H = 50 %

P: Co-worker is in area that backhoe linkage is working to momentarily perform work tasks (depth check, operator guidance, etc). P = 10 %.

AC: AC1 – Key switch or swing boom away

AW: AW2

AR: AR1

CTR16 – boom down

H: Only hazardous if boom down can contact co-worker, so the boom would need to be in fully or nearly fully raised configuration. H = 25 %

P: Co-worker is in the area that backhoe linkage is working to momentarily perform work tasks (depth check, operator guidance, etc). P = 2 %.

AC: AC1 – Key switch or swing boom away

AW: AW2

AR: AR1

CTR17 – lower - backhoe stabilizer

H: During positioning of machine the co-worker could be near to provide direction guidance and help with set-up while stabilizers are in raised position. H = 50 %

P: Hazardous only if the co-worker is in the area that the stabilizers can move down and contact their foot. P = 2 %.

AC: AC1 – Key switch

AW: AW2

AR: AR1

CTR18 – lower – reel carrier

H: Not every spool size would be able to get into configuration where it could raise machine. Machine does not become unstable at lowering of reel carrier, it takes time for spool to lower and contact ground and continue to lower to raise machine. H = 1 %

P: Operator present during the whole cycle. P = 100 %

AC: AC1 – Key switch

AW: AW2

AR: AR2

CTR19 – lower – reel carrier

H: Not every spool size would be able to get into configuration where it could raise machine. Machine does not become unstable at lowering of reel carrier, it takes time for spool to lower and contact ground and continue to lower to raise machine. H = 1 %

P: Only hazardous when this activity has the co-worker near the machine. P = 2 %

AC: AC1 – key switch

AW: AW2

AR: AR2

CTR20 – power wind / unwind – reel carrier

H: N/A

P: P = N/A

AC: N/A

CTR21 – side shift – rear attachment

H: Hazardous only when traveling across slope. Not recommended to travel with machine direction across slope face and would happen very infrequently. 2 % of travel cycle as machine passes through the slope face and side shift movement to the unstable configuration. H = 2 %

P: Operator present during the whole cycle. P = 100 %

AC: AC1 - Key switch off, ground the tool

AW: AW2

AR: AR1

CTR22 – side shift – rear attachment

H: Hazardous only on slope. 80 % of the time machine running, 50 % of the side shift causes instability, and 10 % of the time operating on slope. H = 80 % × 50 % × 10 % = 4 %

P: Operator present during the whole cycle. P = 100 %

AC: AC1 - Key switch off, ground the tool

AW: AW2

AR: AR0

CTR23 – raise – rear attachment

H: Raise speed on a dedicated trencher machine is slower than other machine types that have a trencher attachment. H = 20 %.

P: Operator present during the whole cycle. P = 100 %

AC: AC1 - Operator can stop the chain / wheel.

AW: AW2

AR: AR2 - Using AR2 here versus AR1 on SSL / CTC. The controls are designed for the operator to observe trenching application and machine travel and to respond quickly.

CTR24 – on / off - rear attachment

H: 80 % of time machine is running. H = 80 %

P: 5 % for extreme proximity to hazard zone required. P = 5 %

AC: AC1 - Key switch or ground the implement

AW: AW2

AR: AR1

CTR25 – on / off - boring

H: Only a hazard doing set up or disconnection of additional rods. Only 2 % of boring work cycle. H = 2 %.

P: Co-worker is required to be at the connection point when additional rods are needed. P = 25 %.

AC: AC1 – Key switch or stop boring unit

AW: AW2

AR: AR1

U.2.2 Application use cases

Table U.2 — Application use case table

Application	Preparation / set up	Loading / unloading	Trenching	Plowing	Microtrench-ing	Backfill	Back-hoe	Bor-ing	Travel	Mainte-nance
residential	5 %	10 %	90 %	90 %	80 %	15 %	10 %	50 %	30 %	0 %
rural	5 %	10 %	90 %	90 %	10 %	15 %	10 %	5 %	10 %	0 %

Table U.2 *(continued)*

Application	Preparation / set up	Loading / unloading	Trenching	Plowing	Microtrench-ing	Backfill	Back-hoe	Bor-ing	Travel	Mainte-nance
urban	5 %	10 %	90 %	90 %	80 %	1 %	5 %	1 %	20 %	0 %

U.2.3 Maintenance task breakdown

NOTE No table "Maintenance task breakdown" exists for this machine. For this size machine, maintenance is performed on a non-running machine where none of the tasks are considered hazardous.

U.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table U.3 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
counter steer		1	1		Failure to release on demand is considered the same as counter steer uncommanded activation.
articulated steer		1	1		Failure to release on demand is considered the same as counter steer uncommanded activation.
Ackermann steer - front only	1	1			Both failure types are considered the same as counter steer uncommanded activation.
Ackermann steer - rear only	1	1			Both failure types are considered the same as counter steer uncommanded activation.
Ackermann steer - front and rear combined	1	1			Both failure types are considered the same as counter steer uncommanded activation.
propel - speed			1		Can operate in creep mode while backhoe is functioning.
direction (F / R)			1		
slow/stop	1		1		
hold still	1			1	
6-way blade					See tracked excavator table for 6-way blade.
backhoe loader type func-tions					Add info on workgroup from BHL table.
raise - backhoe stabilizer			1		It is only present with backhoe.
lower - backhoe stabilizer			1		
raise reel carrier			1		
lower reel carrier			1		
power wind / unwind – reel carrier			1		
brake – reel carrier			1		Hazardous during the setup of the reel material through the brake mechanism
frame tilt			1		Only hazardous 50 %, based on direction of frame tilt to the unstable configuration.
track offset			1		Only hazardous 50 %, based on direction of track offset to the unstable configuration.
raise – elevating cab			1		Raising during travel hits overhead object.
lower – elevating cab			1		Maintenance occurring while cab is in “raised” position.

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

Table U.3 *(continued)*

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
slide out – sliding cab			1		Cab moves out and contacts an object.
slide in – sliding cab			1		Maintenance occurring while cab is in "out" position.
slide conveyor			1		
raise - conveyor			1		Raises and contacts an object.
lower - conveyor			1		
speed - conveyor					It is not worse than conveyor belt on / off.
swing or slew conveyor			1		
conveyor belt on / off			1		
discharge direction - conveyor					It is not worse than conveyor belt on / off.
raise – dirt drag					It is not worse that dirt drag lower.
lower – dirt drag			1		
raise - rock wheel stabilizer					It is not worse than rock wheel stabilizer lower.
lower - rock wheel stabilizer			1		
side shift – rear attachment			1		It is only a hazard when tool is out of the ground.
raise – rear attachment			1		The largest hazard is when the tool is operating.
lower – rear attachment					It is not worse than rear attachment raise.
speed – rear attachment					It is not worse than rear attachment on/off.
on / off - rear attachment			1		Uncommanded on is the hazard.
direction – rear attachment					No significant hazard identified.
raise – trench cleaner			1		Rear attachment fully raised and trench cleaner raises to contact object.
lower – trench cleaner			1		Pinch point during maintenance.
swing - plow			1		Hazardous only when plow is not in the ground.
steer - plow					It is not worse than plow swing.
raise - plow					It is not worse than plow lower.
lower - plow			1		Only a hazard when plow is not in the ground.
float – raise / lower - plow					It is not worse than plow lower.
float – swing - plow					It is not worse than plow swing.
raise - microtrencher			1		Refer to rear attachment raise.
lower - microtrencher					It is not worse than microtrencher raise.
side shift - microtrencher			1		Only a hazard when microtrencher is out of the ground.
level – microtrencher					No significant hazard identified.
depth - microtrencher					No significant hazard identified.
speed - microtrencher					It is not worse than microtrencher on / off.
on / off - microtrencher			1		"On" is the hazard.
rotation direction - microtrencher					No significant hazard identified.

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

U.2.5 Notes and assumptions

— During the main operation of these machines (trenching, plowing, microtrenching), the speed is at a rate that a steering failure is not more hazardous than during load/unloading activities.

— During the loading/unloading, uncommanded steering could cause the machine to go off the transport vehicle.

— A scenario for articulated steering was evaluated for travel across a slope where an uncommanded steering could cause instability of the machine.

— Because this size equipment moves at a slow rate, the greatest hazard was thought to be when the machine is at 0 and moves to a speed unexpectedly. The use case where this is thought to be most applicable is during the preparation/set-up of the machine to start its main operation (trenching, plowing, microtrenching). This is the time that the operator and co-worker will have the machine power source running but not moving the machine much. During this time the machine will be stationary for the majority of the time, for this MCSSA that will be 80 % of the time for this use case.

— Another use case was identified where a co-worker could be present. This is when the machine is used in a boring configuration for short run - undirected boring, examples being under driveways or sidewalks. On the times when this boring distance exceeds the rod length that can be outside of the bore hole there needs to be additional rods added during the operation. If unexpectedly there was uncommanded propel-speed again from 0 to a speed, the hazard of collision by the machine on the co-worker could exist.

— Because this size equipment moves at a slow rate, the greatest hazard was thought to be an uncommanded direction change during the micortrenching operation. During this operation there is often a co-worker supporting the machine. It is only hazardous to the co-worker it they are in the area directly behind the machine. The way this equipment is used for microtrenching the co-worker could possibly be in that area 10 % of the time for various support activities.

— During the preparation/set up the machine should have a hold still function (parking brake) engaged. The hazard to the operator is only on the pedestrian controlled machine where the hold still de-activates uncommanded and the machine moves (without power) and contacts the operator (considered operator when they are at the operator station) or the co-worker doing activities associated with preparing the machine for the trenching, plowing, or microtrenching operation. The movement would be slow and a severity of S1 was selected.

— Because this size equipment moves at a slow rate, the greatest hazard was thought to be when the machine is being loaded/unloaded and the requirement to stop the machine and a failure could allow machine to go off the trailer. The hazard area is only that area that would be beyond the normal (or expected) stopping distance as the operator would begin to apply slow/stop function and become aware it was not responding.

— Evaluated a travel scenario for operator (95 % of this cycle the machine could be traveling at its greatest rate) where the machine stops suddenly without warning. Because travel rate is slow for these machines the severity of S0 was selected. And even with no controllability the MPL_r comes out to QM.

— When the rear attachment (chain or wheel trencher) is engaged in the ground it is not possible for that function to alter machine path or make unstable. Scenarios that could make the machine unstable were reviewed: during travel and during preparation/set up are 2 use cases evaluated.

— For travel it is not recommended to operate direction of travel to be across face. H = 2 % to account for time of the travel cycle that the machine may pass through that orientation and the side shift moving tool towards an unstable configuration (to the down slope direction).

— For preparation / set up for using machine across a slope it would be possible to set machine in configuration that would not allow side shift towards an unstable configuration. If this is not done the logic for H and P are in the scenario comments.

— Raise speed on a dedicated trencher machine is slower than other machine types that has a trencher attachment.

U.3 MPL_r mapped to SCS table

Table U.4 shows function-based MPL_r (see Table U.1) mapped to SCS per the results of the MCSSA for a compact trencher less than 4 500 kg. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table U.1 would also be mapped to these MPL_r.

Table U.4 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
counter steer	uncommanded activation	**b**	**counter steer**
	failure to release on demand	**b**	
articulated steer	uncommanded activation	**b**	**articulated steer**
	failure to release on demand	**b**	
Ackermann steer – front only	failure to apply on demand	**b**	**Ackermann steer – front only**
	failure to release on demand	**b**	
Ackermann steer – rear only	failure to apply on demand	**b**	**Ackermann steer – rear only**
	failure to release on demand	**b**	
Ackermann steer – front and rear combined	failure to apply on demand	**b**	**Ackermann steer – front and rear combined**
	failure to release on demand	**b**	
propel - speed	uncommanded activation	**b**	**propel**
direction (F / R)	uncommanded activation	**b**	**gear direction control**
slow/stop	failure to apply on demand	**b**	**service brakes**
	uncommanded activation	**QM**	
hold still	uncommanded activation	**a**	**parking brakes**
blade up / down, blade tilt, blade float	uncommanded activation	**a**	**blade up / down, blade tilt, blade float**
backhoe swing	uncommanded activation	**b**	**backhoe swing**
backhoe arm - in	uncommanded activation	**c**	**backhoe arm - in**
backhoe arm - out	uncommanded activation	**c**	**backhoe arm - out**
backhoe boom down	uncommanded activation	**b**	**backhoe boom down**
backhoe boom up	uncommanded activation	**c**	**backhoe boom up**
raise - backhoe stabilizer	uncommanded activation	**c**	**raise - backhoe stabilizer**
lower - backhoe stabilizer	uncommanded activation	**a**	**lower - backhoe stabilizer**
raise – reel carrier	uncommanded activation	**a**	**raise – reel carrier**
lower – reel carrier	uncommanded activation	**a**	**lower – reel carrier**
power wind / unwind - reel carrier	uncommanded activation	**QM**	**power wind / unwind - reel carrier**
brake – reel carrier	uncommanded activation	**QM**	**brake – reel carrier**
side shift – rear attachment	uncommanded activation	**b**	**side shift – rear attachment**
raise – rear attachment	uncommanded activation	**b**	**raise – rear attachment**
lower – rear attachment	uncommanded activation	**b**	**lower – rear attachment**
speed – rear attachment	uncommanded activation	**c**	**speed – rear attachment**
on / off – rear attachment	uncommanded activation	**c**	**on / off – rear attachment**
direction – rear attachment	no hazard	**N/A**	**direction – rear attachment**
on / off boring	uncommanded activation	**b**	**on / off boring**

Table U.4 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
swing - plow	uncommanded activation	**b**	**swing - plow**
steer - plow	no hazard	**N/A**	**steer - plow**
raise - plow	no hazard	**N/A**	**raise - plow**
lower - plow	no hazard	**N/A**	**lower - plow**
float – raise / lower plow	no hazard	**N/A**	**float – raise / lower plow**
float – swing plow	no hazard	**N/A**	**float – swing plow**
raise - microtrencher	uncommanded activation	**b**	**raise - microtrencher**
lower - microtrencher	uncommanded activation	**b**	**lower - microtrencher**
side shift - microtrencher	uncommanded activation	**b**	**side shift - microtrencher**
level - microtrencher	no hazard	**N/A**	**level - microtrencher**
depth - microtrencher	no hazard	**N/A**	**depth - microtrencher**
speed - microtrencher	uncommanded activation	**c**	**speed - microtrencher**
on / off - microtrencher	uncommanded activation	**c**	**on / off - microtrencher**
rotation direction - microtrencher	no hazard	**N/A**	**rotation direction - microtrencher**

Annex V
(normative)

Medium trencher greater than or equal to 4 500 kg and less than 18 000 kg performance level tables

V.1 Medium trencher greater than or equal to 4 500 kg and less than 18 000 kg

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables V.1 to V.4) or in Clause 5.

Table V.1 — MPL_r table for medium trencher greater than or equal to 4 500 kg and less than 18 000 kg

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CTR1-3	**counter steer**	considered same as compact trencher													**b**
CTR4	**articulated steer**	considered same as compact trencher													**b**
CTR1-3	**Ackermann steer - front only**	considered same as compact trencher													**b**
CTR1-3	**Ackermann steer - rear only**	considered same as compact trencher													**b**
CTR1-3	**Ackermann steer - front and rear combined**	considered same as compact trencher													**b**
CTR5-6	**propel - speed**	considered same as compact trencher													**b**
CTR7	**direction (F / R)**	considered same as compact trencher													**b**
CTR8-11	**slow/stop**	considered same as compact trencher													**b**
CTR12	**hold still**	considered same as compact trencher													**a**
CTR14	**blade down / up - blade tilt - blade float**	considered same as compact trencher													**a**
BH4-5	**hoe arm in**	considered same as backhoe loader													**c**
BH4-5	**hoe arm out**	considered same as backhoe loader													**c**
CTR15	**backhoe swing**	considered same as compact trencher													**b**
CTR16	**boom down**	considered same as compact trencher													**b**
BH3	**boom up**	considered same as backhoe loader													**c**
BH3	**raise - backhoe stabilizer**	considered same as backhoe loader													**c**
CTR17	**lower - backhoe stabilizer**	considered same as compact trencher													**a**
CTR18	**raise - reel carrier**	considered same as compact trencher													**a**
CTR18-19	**lower - reel carrier**	considered same as compact trencher													**a**
CTR20	**power wind / unwind - reel carrier**	considered same as compact trencher													**QM**
CTR20	**brake - reel carrier**	Considered same as compact trencher													**QM**
MTR1	**frame tilt**	travel	uncommanded activation	machine becomes unstable	operator	S1	20 %	5 %	100 %	E1	AC1	AW2	AR3	C1	**QM**
MTR2	**side shift - rear attachment**	travel	uncommanded activation	machine becomes unstable and tips contacting operator	operator	S2	30 %	8 %	100 %	E0	AC1	AW2	AR1	C3	**b**
CTR23	**raise - rear attachment**	considered same as compact trencher													**b**
CTR23	**lower - rear attachment**	considered same as compact trencher													**b**
CTR24	**speed - rear attachment**	considered same as compact trencher													**c**
CTR24	**on / off - rear attachment**	considered same as compact trencher													**c**

Table V.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
	direction - rear attachment	no significant hazard													
CTR21	**swing -plow**	no worse than residential / side shift-rear attachment / travel / uncommanded activation / operator													**b**
	steer - plow	no significant hazard													
	raise - plow	no significant hazard													
	lower - plow	no significant hazard													
	float – raise / lower - plow	no significant hazard													
	float - swing - plow	no significant hazard													
CTR23	**raise - microtrencher**	considered same as compact trencher													**b**
CTR23	**lower - microtrencher**	considered same as compact trencher													**b**
CTR21	**side shift - microtrencher**	considered same as compact trencher													**b**
	level - microtrencher	no significant hazard													
	depth - microtrencher	no significant hazard													
CTR24	**speed - microtrencher**	considered same as compact trencher													**c**
CTR24	**on / off - microtrencher**	considered same as compact trencher													**c**
	rotation direction - microtrencher	no significant hazard													

V.2 Supporting explanation

V.2.1 Supporting explanations for dominant scenarios

MTR1 – frame tilt

H: Only hazardous when traveling across a slope (10 % of the time) and only hazardous if it tilts in the unstable direction 50 %, H = 10 % × 50 % = 5 %

P: Operator present during the whole cycle. P = 100 %

AC: AC1 - Steer and/or brake to stable condition

AW: AW2

AR: AR3

MTR2 – side shift – rear attachment

H: Hazardous only on slope. 80 % of the time machine running, 50 % of the side shift causes instability, and 20 % of the time operating on slope. H = 80 % × 50 % × 20 % = 8 %

P: Operator present during the whole cycle. P = 100 %

AC: AC1 - Key switch off, ground the tool

AW: AW2

AR: AR0

V.2.2 Application use cases

Table V.2 — Application use case table

Application	Preparation / set up	Loading / unloading	Trenching	Plowing	Microtrench-ing	Backfill	Back-hoe	Bor-ing	Travel	Mainte-nance
residential	5 %	10 %	90 %	90 %	80 %	15 %	10 %	10 %	30 %	2 %
rural	5 %	5 %	90 %	90 %	10 %	15 %	10 %	5 %	5 %	2 %
urban	10 %	10 %	30 %	5 %	80 %	1 %	5 %	1 %	20 %	2 %

V.2.3 Maintenance task breakdown

NOTE No table "Maintenance task breakdown" exists for this machine. For this size machine, maintenance is performed on a non-running machine where none of the tasks are considered hazardous.

V.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table V.3 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
counter steer		1	1		Failure to release on demand is considered the same as counter steer uncommanded activation.
articulated steer		1	1		Failure to release on demand is considered the same as counter steer uncommanded activation
Ackermann steer - front only	1	1			Both failure types are considered the same as counter steer uncommanded activation.
Ackermann steer - rear only	1	1			Both failure types are considered the same as counter steer uncommanded activation.
Ackermann steer - front and rear combined	1	1			Both failure types are considered the same as counter steer uncommanded activation.
propel - speed			1		Can operate in creep mode while backhoe is functioning.
direction (F / R)			1		
slow/stop	1		1		
hold still	1			1	
6-way blade					See tracked excavator table for 6-way blade.
Backhoe loader type functions					Add info on workgroup from BHL table.
raise - backhoe stabilizer			1		It is only present with backhoe.
lower - backhoe stabilizer			1		
raise reel carrier			1		
lower reel carrier			1		
power wind / unwind – reel carrier			1		
brake – reel carrier			1		It is hazardous during the setup of the reel material through the brake mechanism.
frame tilt			1		It is only hazardous 50 %, based on direction of frame tilt to the unstable configuration.
track offset			1		It is only hazardous 50 %, based on direction of track offset to the unstable configuration.
raise – elevating cab			1		Raising during travel hits overhead object.
lower – elevating cab			1		Maintenance is occurring while cab is in “raised” position.
slide out – sliding cab			1		Cab moves out and contacts an object.
slide in – sliding cab			1		Maintenance is occurring while cab is in “out” position.
slide conveyor			1		
raise - conveyor			1		Raises and contacts an object.
lower - conveyor			1		
speed - conveyor					It is not worse than conveyor belt on/off.
swing or slew conveyor			1		
conveyor belt on / off			1		
discharge direction - conveyor					It is not worse than conveyor belt on/off.
raise – dirt drag					It is not worse that dirt drag lower.
lower – dirt drag			1		
raise - rock wheel stabilizer					It is not worse than rock wheel stabilizer lower.
lower - rock wheel stabilizer			1		
side shift – rear attachment			1		Only a hazard when tool is out of the ground.

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

Table V.3 *(continued)*

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
raise – rear attachment			1		The largest hazard is when the tool is operating.
lower – rear attachment					It is not worse than rear attachment raise.
speed – rear attachment					It is not worse than rear attachment on/off.
on / off - rear attachment			1		Uncommanded on is the hazard.
direction – rear attachment					No significant hazard is identified.
raise – trench cleaner			1		Rear attachment is fully raised and trench cleaner raise to contact object.
lower – trench cleaner			1		Pinch point during maintenance
swing - plow			1		Hazardous only when plow is not in the ground.
steer - plow					It is not worse than plow swing.
raise - plow					It is not worse than plow lower.
lower - plow			1		Only a hazard when plow is not in the ground.
float – raise / lower - plow					It is not worse than plow lower.
float – swing - plow					It is not worse than plow swing.
raise - microtrencher			1		Refer to rear attachment raise.
lower - microtrencher					It is not worse than microtrencher raise.
side shift - microtrencher			1		Only a hazard when microtrencher is out of the ground.
level - microtrencher					No significant hazard is identified.
depth - microtrencher					No significant hazard is identified.
speed - microtrencher					It is not worse than microtrencher on/off.
on / off - microtrencher			1		“On” is the hazard.
rotation direction - micro-trencher					No significant hazard is identified.
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

V.2.5 Notes and assumptions

— During the main operation of these machines (trenching, plowing, microtrenching), the speed is at a rate when a steering failure is not more hazardous than during load/unloading activities.

— During the loading/unloading, uncommanded steering could cause the machine to go off the transport vehicle.

— A scenario for articulated steering was evaluated for travel across a slope where an uncommanded steering could cause instability of the machine.

— Because this size equipment moves at a slow rate, the greatest hazard was thought to be when the machine is at 0 and moves to a speed unexpectedly. The use case where this is thought to be most applicable is during the preparation/set-up of the machine to start its main operation (trenching, plowing, microtrenching). This is the time that the operator and co-worker will have the machine power source running but not moving the machine much. During this time the machine will be stationary for the majority of the time, for this MCSSA that will be 80 % of the time for this use case.

— Another use case was identified where a co-worker could be present. This is when the machine is used in a boring configuration for short run - undirected boring, examples being under driveways or sidewalks. On the times when this boring distance exceeds the rod length that can be outside of the bore hole there needs to be additional rods added during the operation. If unexpectedly there was an uncommanded propel-speed again from 0 to a speed, the hazard of collision by the machine on the co-worker could exist.

— Because this size equipment moves at a slow rate, the greatest hazard was thought to be an uncommanded direction change during the micortrenching operation. During this operation there is often a co-worker supporting the machine. It is only hazardous to the co-worker it they are in the area directly behind the machine. The way this equipment is used for microtrenching the co-worker could possibly be in that area 10 % of the time for various support activities.

— During the preparation/set up the machine should have a hold still function (parking brake) engaged. The hazard to the operator is only on a pedestrian controlled machine where the hold still de-activates uncommanded and the machine moves (without power) and contacts the operator (considered operator when they are at the operator station) or the co-worker doing activities associated with preparing the machine for the trenching, plowing, or microtrenching operation. The movement would be slow and a severity of S1 was selected.

— Because this size equipment moves at a slow rate, the greatest hazard was thought to be when the machine is being loaded/unloaded and the requirement to stop the machine and a failure could allow machine to go off the trailer. The hazard area is only that area that would be beyond the normal (or expected) stopping distance as the operator would begin to apply slow/stop function and become aware it was not responding.

— Evaluated a travel scenario for operator (95 % of this cycle the machine could be traveling at its greatest rate) where the machine stops suddenly without warning. Because travel rate is slow for these machines the severity of S0 was selected. And even with no controllability the MPL_r comes out to QM.

— When the rear attachment (chain or wheel trencher) is engaged in the ground it is not possible for that function to alter machine path or make unstable. Scenarios that could make the machine unstable were reviewed: during travel and during preparation/set up are 2 use cases evaluated.

— For travel it is not recommended to operate direction of travel to be across face. H = 2 % to account for time of the travel cycle that the machine may pass through that orientation and the side shift moving tool towards an unstable configuration (to the down slope direction).

— For preparation / set up for using machine across a slope it would be possible to set machine in configuration that would not allow side shift towards an unstable configuration. If this is not done the logic for H and P are in the scenario comments.

— Raise speed on a dedicated trencher machine is slower than other machine types that has a trencher attachment.

V.3 MPL_r mapped to SCS table

Table V.4 shows function-based MPL_r (see Table V.1) mapped to SCS per the results of the MCSSA for a Medium Trencher Greater Than or Equal to 4 500 kg and Less than 18 000 kg. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table V.1 would also be mapped to these MPL_r.

Table V.4 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
counter steer	uncommanded activation	**b**	**counter steer**
	failure to release on demand	**b**	
articulated steer	uncommanded activation	**b**	**articulated steer**
	failure to release on demand	**b**	
Ackermann steer – front only	failure to apply on demand	**b**	**Ackermann steer – front only**
	failure to release on demand	**b**	

Table V.4 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
Ackermann steer – rear only	failure to apply on demand	**b**	**Ackermann steer – rear only**
	failure to release on demand	**b**	
Ackermann steer – front and rear combined	failure to apply on demand	**b**	**Ackermann steer – front and rear combined**
	failure to release on demand	**b**	
propel - speed	uncommanded activation	**b**	**propel**
direction (F / R)	uncommanded activation	**b**	**gear direction control**
slow/stop	failure to apply on demand	**b**	**service brakes**
	uncommanded activation	**QM**	
hold still	uncommanded activation	**a**	**parking brakes**
blade up / down, blade tilt, blade float	uncommanded activation	**a**	**blade up / down, blade tilt, blade float**
backhoe swing	uncommanded activation	**b**	**backhoe swing**
backhoe arm in	uncommanded activation	**c**	**backhoe arm in**
backhoe arm out	uncommanded activation	**c**	**backhoe arm out**
backhoe boom down	uncommanded activation	**b**	**backhoe boom down**
backhoe boom up	uncommanded activation	**c**	**backhoe boom up**
raise - backhoe stabilizer	uncommanded activation	**c**	**raise - backhoe stabilizer**
lower - backhoe stabilizer	uncommanded activation	**a**	**lower - backhoe stabilizer**
raise – reel carrier	uncommanded activation	**a**	**raise – reel carrier**
lower – reel carrier	uncommanded activation	**a**	**lower – reel carrier**
power wind / unwind - reel carrier	uncommanded activation	**QM**	**power wind / unwind - reel carrier**
brake – reel carrier	uncommanded activation	**QM**	**brake – reel carrier**
side shift – rear attachment	uncommanded activation	**b**	**side shift – rear attachment**
raise – rear attachment	uncommanded activation	**b**	**raise – rear attachment**
lower – rear attachment	uncommanded activation	**b**	**lower – rear attachment**
speed – rear attachment	uncommanded activation	**c**	**speed – rear attachment**
on / off – rear attachment	uncommanded activation	**c**	**on / off – rear attachment**
direction – rear attachment	no hazard	**N/A**	**direction – rear attachment**
frame tilt	uncommanded activation	**QM**	**frame tilt**
swing - plow	uncommanded activation	**b**	**swing - plow**
steer - plow	no hazard	**N/A**	**steer - plow**
raise - plow	no hazard	**N/A**	**raise - plow**
lower - plow	no hazard	**N/A**	**lower - plow**
float – raise / lower plow	no hazard	**N/A**	**float – raise / lower plow**
float – swing slow	no hazard	**N/A**	**float – swing plow**
raise – microtrencher	uncommanded activation	**b**	**raise - microtrencher**
lower - microtrencher	uncommanded activation	**b**	**lower - microtrencher**
side shift - microtrencher	uncommanded activation	**b**	**side shift - microtrencher**
level - microtrencher	no hazard	**N/A**	**level - microtrencher**

Table V.4 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
depth - microtrencher	no hazard	**N/A**	**depth - microtrencher**
speed - microtrencher	uncommanded activation	**c**	**speed - microtrencher**
on / off - microtrencher	uncommanded activation	**c**	**on / off - microtrencher**
rotation direction - microtrencher	no hazard	**N/A**	**rotation direction - microtrencher**

Annex W
(normative)

Heavy trencher greater than or equal to 18 000 kg performance level tables

W.1 Heavy trencher greater than or equal to 18 000 kg

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables W.1 to W.4) or in Clause 5.

Table W.1 — MPL_r table for heavy trencher greater than or equal to 18 000 kg

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CTR1-3	**counter steer**	considered same as compact trencher													**b**
HTR1	**propel - speed**	preparation / set up	uncommanded activation	contacted by machine	co-worker	S3	10 %	80 %	10 %	E0	AC1	AW2	AR2	C2	**b**
CTR7	**direction (F / R)**	considered same as compact trencher													**b**
HTR2	**slow/stop**	preparation / set up	failure to apply on demand	contacted by machine	co-worker	S3	10 %	20 %	2 %	E0	AC1	AW2	AR3	C1	**a**
CTR12	**hold still**	considered same as compact trencher													**a**
MTR1	**frame tilt**	considered same as medium trencher													**QM**
MTR1	**track offset**	considered same as frame tilt													**QM**
HTR3	**raise – elevating cab**	considered same as lower – elevating cab													**b**
HTR3	**lower – elevating cab**	maintenance / service / repair	uncommanded activation	crushing	maintainer	S2	5 %	5 %	50 %	E0	AC0	N/A	N/A	C3	**b**
HTR3	**slide out – sliding cab**	Considered same as lower – elevating cab													**b**
HTR3	**slide in – sliding cab**	considered same as lower – elevating cab													**b**
HTR4	**slide - conveyor**	preparation / set up	uncommanded activation	struck by conveyor	co-worker	S1	10 %	80 %	2 %	E0	AC1	AW1	AR2	C3	**a**
HTR5	**raise conveyor**	considered same as lower - conveyor													**b**
HTR5	**lower - conveyor**	preparation / set up	uncommanded activation	struck by conveyor or linkage	co-worker	S2	10 %	80 %	2 %	E0	AC1	AW1	AR1	C3	**b**
HTR7	**speed - conveyor**	considered same as conveyor belt - on / off													**b**
HTR6	**swing/slew - conveyor**	trenching	uncommanded activation	material thrown to location not intended and strikes co-worker	co-worker	S2	90 %	90 %	1 %	E0	AC1	AW1	AR2	C3	**b**

Table W.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
HTR7	**conveyor belt – on / off**	trenching	uncommanded activation	struck by thrown material	co-worker	S2	90 %	5 %	5 %	E0	AC1	AW1	AR1	C3	**b**
HTR6	**discharge direction - conveyor**	considered same as swing/slew - conveyor													**b**
HTR8	**raise - dirt drag**	considered same as lower – dirt drag													**b**
HTR8	**lower - dirt drag**	preparation / set up	uncommanded activation	crushed foot	co-worker	S2	10 %	80 %	1 %	E0	AC1	AW1	AR0	C3	**b**
HTR9	**raise – rock wheel stabilizer**	considered same as lower – rock wheel stabilizer													**b**
HTR9	**lower – rock wheel stabilizer**	preparation / set up	uncommanded activation	crushed foot	co-worker	S2	10 %	80 %	1 %	E0	AC1	AW1	AR0	C3	**b**
HTR10	**side shift - rear attachment**	preparation / set up	uncommanded activation	contacted by rear attachment	co-worker	S1	10 %	80 %	5 %	E0	AC1	AW1	AR2	C3	**a**
HTR11	**raise – trench cleaner**	considered same as lower – trench cleaner													**b**
HTR11	**lower – trench cleaner**	maintenance / service / repair	uncommanded activation	struck by trench cleaner	maintainer	S2	5 %	50 %	38 %	E0	AC1	AW1	AR1	C3	**b**
CTR22	**raise - rear attachment**	considered same as compact trencher													**b**
CTR22	**lower - rear attachment**	considered same as compact trencher													**b**
CTR23	**speed - rear attachment**	considered same as compact trencher													**c**
CTR23	**on / off - rear attachment**	considered same as compact trencher													**c**

Table W.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
	direction - rear attachment	no significant hazard													

W.2 Supporting explanation

W.2.1 Supporting explanations for dominant scenarios

HTR1 – propel speed

H: 80 % of the time for setup the machine is running and stationary

P: The co-worker may be in the area that the machine moves towards (very close proximity based on maximum machine speed). P= 10 %

AC: AC1 - Apply brake, ignition switch

AW: AW2

AR: AR2

HTR2 – slow/stop

H: 20 % of the time for setup the machine is moving

P: The co-worker would not typically be in path of the machine but may cross for setup activities. P = 2 %

AC: AC1 - Steer, reverse direction, ignition switch

AW: AW2

AR: AR3

HTR3 – lower – elevating cab

H: 5 % of time cab raised cab for specific maintenance task

P: Maintainer working in area under cab (extremities only exposed below cab). P = 50 %

AC: AC0

HTR4 – slide - conveyor

H: 80 % of the time for setup the machine is running and stationary

P: Co-worker could be doing preparation activity in the hazard area. P = 2 %

AC: AC1 - ignition switch

AW: AW1

AR: AR1

HTR5 – lower - conveyor

H: 80 % of the time for setup the machine is running and stationary

P: Co-worker may be directly under conveyor for prep activity. P = 2 %

AC: AC1 - ignition switch

AW: AW1

AR: AR1

HTR6 – swing/slew - conveyor

H: 90% of truck loading conveyor used within trenching application

P: Co-worker is in unprotected location (truck driver is considered partially protected) for unintended discharge location. P = 1 %

AC: AC1 - Ignition switch, stop conveyor feed

AW: AW1

AR: AR2

HTR7 – conveyor belt – on / off

H: 10 % of the time the conveyor may not be running and 50 % of that time it may have material on it. H = 5 %

P: Co-worker would be passing through discharge area. P = 5 %

AC: AC1 - Ignition switch, conveyor direction change

AW: AW1

AR: AR1

HTR8 – lower – dirt drag

H: 80 % of the time for setup the machine is running and stationary

P: Co-worker would have to be in the small hazard zone for prep work. P = 1 %

AC: AC1 - Ignition switch

AW: AW1

AR: AR0

HTR9 – lower – rock wheel stabilizer

H: 80 % of the time for setup the machine is running and stationary

P: Co-worker would have to be in the small hazard zone for prep work. P = 1 %

AC: AC1 - Ignition switch

AW: AW1

AR: AR0

HTR10 – side shift - rear attachment

H: 80 % of the time for setup the machine is running and stationary

P: Co-worker would have to be in the small hazard zone for prep work. P = 5 %

AC: AC1 - Ignition switch, ground attachment

AW: AW1

AR: AR2

HTR11 – lower – trench cleaner

H: Chain maintenance can be done with trench cleaner in lowered configuration. H = 50 %

P: The maintainer working on chain (75 %), and in the zone that could be contacted (50 %) P = 38 %

AC: AC1 - Alternate stop required if machine is running

AW: AW1

AR: AR1

W.2.2 Application use cases

Table W.2 — Application use case table

Application	Preparation / set up	Loading / unloading	Trenching	Plowing	Microtrench-ing	Backfill	Back-hoe	Bor-ing	Travel	Mainte-nance
residential	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %
rural	10 %	5 %	90 %	0 %	0 %	0 %	0 %	0 %	5 %	5 %
urban	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %

W.2.3 Maintenance task breakdown

NOTE No table "Maintenance task breakdown" exists for this machine. For this size machine, maintenance is performed on a non-running machine where none of the tasks are considered hazardous.

W.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table W.3 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
counter steer		1	1		Failure to release on demand is considered the same as counter steer uncommanded activation.
articulated steer		1	1		Failure to release on demand is considered the same as counter steer uncommanded activation.
Ackermann steer - front only	1	1			Both failure types are considered the same as counter steer uncommanded activation.
Ackermann steer - rear only	1	1			Both failure types are considered the same as counter steer uncommanded activation.
Ackermann steer - front and rear combined	1	1			Both failure types are considered the same as counter steer uncommanded activation.
propel - speed			1		Can operate in creep mode while backhoe is functioning.
direction (F / R)			1		
slow/stop	1		1		
hold still	1			1	
6-way blade					See tracked excavator table for 6-way blade.
backhoe loader type func-tions					Add info on workgroup from BHL table.
raise - backhoe stabilizer			1		It is only present with backhoe.
lower - backhoe stabilizer			1		
raise reel carrier			1		
lower reel carrier			1		
power wind / unwind – reel carrier			1		

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

Table W.3 *(continued)*

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
brake – reel carrier			1		It is hazardous during the setup of the reel material through the brake mechanism.
frame tilt			1		It is only hazardous 50 %, based on direction of frame tilt to the unstable configuration.
track offset			1		It is only hazardous 50 %, based on direction of track offset to the unstable configuration.
raise – elevating cab			1		Raising during travel hits overhead object.
lower – elevating cab			1		Maintenance is occurring while cab is in "raised" position.
slide out – sliding cab			1		Cab moves out and contacts an object.
slide in – sliding cab			1		Maintenance is occurring while cab is in "out" position.
slide conveyor			1		
raise - conveyor			1		Raises and contacts an object.
lower - conveyor			1		
speed - conveyor					It is not worse than conveyor belt on/off.
swing or slew conveyor			1		
conveyor belt on / off			1		
discharge direction - conveyor					It is not worse than conveyor belt on/off.
raise – dirt drag					It is not worse that dirt drag lower.
lower – dirt drag			1		
raise - rock wheel stabilizer					It is not worse than rock wheel stabilizer lower.
lower - rock wheel stabilizer			1		
side shift – rear attachment			1		It is only a hazard when tool is out of the ground.
raise – rear attachment			1		The largest hazard is when the tool is operating.
lower – rear attachment					It is not worse than rear attachment raise.
speed – rear attachment					It is not worse than rear attachment on/off.
on / off - rear attachment			1		Uncommanded on is the hazard.
direction – rear attachment					No significant hazard is identified.
raise – trench cleaner			1		Rear attachment fully raised and trench cleaner raises to contact object.
lower – trench cleaner			1		Pinch point during maintenance
swing - plow			1		Hazardous only when plow is not in the ground.
steer - plow					It is not worse than plow swing.
raise - plow					It is not worse than plow lower.
lower - plow			1		Only a hazard when plow is not in the ground.
float – raise / lower - plow					It is not worse than plow lower.
float – swing - plow					It is not worse than plow swing.
raise - microtrencher			1		Refer to rear attachment raise.
lower - microtrencher					It is not worse than microtrencher raise.
side shift - microtrencher			1		Only a hazard is when microtrencher is out of the ground.
level - microtrencher					No significant hazard identified.
depth - microtrencher					No significant hazard identified.
speed - microtrencher					It is not worse than microtrencher on/off.

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

Table W.3 *(continued)*

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
on / off - microtrencher			1		"On" is the hazard.
rotation direction - micro-trencher					No significant hazard identified.
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

W.2.5 Notes and assumptions

— During the main operation of these machines (trenching, plowing, microtrenching), the speed is at a rate that a steering failure is not more hazardous than during load/unloading activities.

— During the loading/unloading, uncommanded steering could cause the machine to go off the transport vehicle.

— A scenario for articulated steering was evaluated for travel across a slope where an uncommanded steering could cause instability of the machine.

— Because this size equipment moves at a slow rate, the greatest hazard was thought to be when the machine is at 0 and moves to a speed unexpectedly. The use case where this is thought to be most applicable is during the preparation/set-up of the machine to start its main operation (trenching, plowing, microtrenching). This is the time that the operator and co-worker will have the machine power source running but not moving the machine much. During this time the machine will be stationary for the majority of the time, for this MCSSA that will be 80 % of the time for this use case.

— Another use case was identified where a co-worker could be present. This is when the machine is used in a boring configuration for short run - undirected boring, examples being under driveways or sidewalks. On the times when this boring distance exceeds the rod length that can be outside of the bore hole there needs to be additional rods added during the operation. If there was uncommanded propel-speed again from 0 to a speed unexpectedly, the hazard of collision by the machine on the co-worker could exist.

— Because this size equipment moves at a slow rate, the greatest hazard was thought to be an uncommanded direction change during the micortrenching operation. During this operation there is often a co-worker supporting the machine. It is only hazardous to the co-worker it they are in the area directly behind the machine. The way this equipment is used for microtrenching the co-worker could possibly be in that area 10 % of the time for various support activities.

— During the preparation/set up the machine should have a hold still function (parking brake) engaged. The hazard to the operator is only on pedestrian controlled machine where the hold still de-actives uncommanded and the machine moves (without power) and contacts the operator (considered operator when they are at the operator station) or the co-worker doing activities associated with preparing the machine for the trenching, plowing, or microtrenching operation. The movement would be slow and a severity of S1 was selected.

— Because this size equipment moves at a slow rate, the greatest hazard was thought to be when the machine is being loaded/unloaded and the requirement to stop the machine and a failure could allow machine to go off the trailer. The hazard area is only that area that would be beyond the normal (or expected) stopping distance as the operator would begin to apply slow/stop function and become aware it was not responding.

— Evaluated a travel scenario for operator (95 % of this cycle the machine could be traveling at its greatest rate) where the machine stops suddenly without warning. Because travel rate is slow for these machines the severity of S0 was selected. And even with no controllability the MPL_r comes out to QM.

— When the rear attachment (chain or wheel trencher) is engaged in the ground it is not possible for that function to alter machine path or make unstable. Scenarios that could make the machine unstable were reviewed: during travel and during preparation/set up are 2 use cases evaluated.

— For travel it is not recommended to operate direction of travel to be across face. H = 2 % to account for time of the travel cycle that the machine may pass through that orientation and the side shift moving tool towards an unstable configuration (to the down slope direction).

— For preparation / set up for using machine across a slope it would be possible to set machine in configuration that would not allow side shift towards an unstable configuration. If this is not done the logic for H and P are in the scenario comments.

— Raise speed on a dedicated trencher machine is slower than other machine types that has a trencher attachment.

W.3 MPL_r mapped to SCS table

Table W.4 shows function-based MPL_r (see Table W.1) mapped to SCS per the results of the MCSSA for a heavy trencher greater than or equal to 18 000 kg. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table W.1 would also be mapped to these MPL_r.

Table W.4 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
counter steer	uncommanded activation	**b**	**counter steer**
	failure to release on demand	**b**	
propel - speed	uncommanded activation	**b**	**propel**
direction (F / R)	uncommanded activation	**b**	**gear direction control**
slow/stop	failure to apply on demand	**a**	**service brakes**
	uncommanded activation	**QM**	
hold still	uncommanded activation	**a**	**parking brakes**
frame tilt	uncommanded activation	**QM**	**frame tilt**
track offset	uncommanded activation	**QM**	**track offset**
raise – elevating cab	uncommanded activation	**b**	**raise – elevating cab**
lower – elevating cab	uncommanded activation	**b**	**lower – elevating cab**
slide out – sliding cab	uncommanded activation	**b**	**slide out – sliding cab**
slide in – sliding cab	uncommanded activation	**b**	**slide in – sliding cab**
slide - conveyor	uncommanded activation	**a**	**slide - conveyor**
raise - conveyor	uncommanded activation	**b**	**raise - conveyor**
lower - conveyor	uncommanded activation	**b**	**lower - conveyor**
speed conveyor	uncommanded activation	**b**	**speed conveyor**
swing/slew - conveyor	uncommanded activation	**b**	**swing/slew - conveyor**
conveyor belt – on / off	uncommanded activation	**b**	**conveyor belt – on / off**
discharge direction - conveyor	uncommanded activation	**b**	**discharge direction - conveyor**
raise – dirt drag	uncommanded activation	**b**	**raise – dirt drag**
lower – dirt drag	uncommanded activation	**b**	**lower – dirt drag**
raise – rock wheel stabilizer	uncommanded activation	**b**	**raise – rock wheel stabilizer**
lower – rock wheel stabilizer	uncommanded activation	**b**	**lower – rock wheel stabilizer**

Table W.4 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
side shift – rear attachment	uncommanded activation	**a**	**side shift – rear attachment**
raise – rear attachment	uncommanded activation	**b**	**raise – rear attachment**
lower – rear attachment	uncommanded activation	**b**	**lower – rear attachment**
speed – rear attachment	uncommanded activation	**c**	**speed – rear attachment**
on / off – rear attachment	uncommanded activation	**c**	**on / off – rear attachment**
direction – rear attachment	no hazard	**N/A**	**direction – rear attachment**
raise - trench cleaner	uncommanded activation	**b**	**raise - trench cleaner**
lower - trench cleaner	uncommanded activation	**b**	**lower - trench cleaner**

Annex X
(normative)

Telescopic wheel loader performance level tables

X.1 Telescopic wheel loader

X.1.1 Notes and assumptions

— Retract is considered no worse than boom down when boom is up high or boom up when boom is down low.

— Extend at the end point of material handling is no worse than machine movement when unloading.

— Extend during the rest of cycle is no worse than boom up when boom is up and boom down when boom is down.

— Boom extend / retract is the same as the worse of boom up, boom down, machine speed when material handling, uncommanded stop when roading and failure slow stop when material handling.

X.2 MPL_r mapped to SCS table

Table X.1 shows function-based MPL_r (see Table H.1) mapped to SCS per the results of the MCSSA for a medium, small and compact wheel loader less than 24 000 kg. It has been adapted to telescopic wheel loaders based on X.1.1. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table H.1 would also be mapped to these MPL_r.

Table X.1 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
retract boom	uncommanded activation	**c**	**retract boom**
extend boom	uncommanded activation	**c**	**extend boom**
machine speed	uncommanded activation	**b**	**throttle and speed gear control**
	failure to release on demand		
machine direction	uncommanded activation	**c**	**gear direction control**
boom raise	uncommanded activation	**c**	**boom raise**
boom lower	uncommanded activation	**c**	**boom lower**
tool dump	uncommanded activation	**c**	**tool dump**
tool curl	uncommanded activation	**c**	**tool curl**
hold still	failure to apply on demand	**c**	**parking brakes**
	uncommanded activation		
steering	uncommanded activation	**d**	**steering**
transmission neutralize	uncommanded deactivation	**a**	**gear direction control**
slow/stop	failure to apply on demand	**c**	**service brakes**
	uncommanded activation		
loader auxiliary function	uncommanded activation	**c**	**loader auxiliary function**

Table X.1 *(continued)*

Machine function	Failure type	MPL required	Example of mapped system
loader coupler	multiple failures to be hazardous for known designs in working group	**N/A**	**loader coupler**

Annex Y
(normative)

Compact tool carrier performance level tables

Y.1 Compact tool carrier

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables Y.1 to Y.4) or in Clause 5.

Table Y.1 — MPL_r table for compact tool carrier

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CTC1	**propel**	bucket work	uncommanded activation	collision with object	operator	S1	80 %	10 %	100 %	E1	AC1	AW2	AR1	C3	**b**
CTC2		bucket work		collision from machine	co-worker	S2	80 %	2 %	25 %	E0	AC1	AW2	AR1	C3	**b**
CTC3		bucket work	failure to release on demand	collision from machine	operator	S1	80 %	2 %	100 %	E1	AC1	AW2	AR1	C3	**b**
CTC4		bucket work		collision from machine	co-worker	S2	80 %	2 %	25 %	E0	AC1	AW2	AR1	C3	**b**
CTC5	**slow/stop**	material handling	failure to apply on demand	Collision from machine or load (e.g. large tree branches) may have co-worker at each end of the work cycle helping to load and unload machine.	co-worker	S2	80 %	33 %	35 %	E1	AC1	AW2	AR1	C3	**c**
CTC1-2	**engine speed**	no worse than machine propel speed													**b**
CTC6	**hold still**	power supply	failure to apply on demand	machine could creep	co-worker	S1	5 %	5 %	75 %	E0	AC0	N/A	N/A	N/A	**a**
CTC7		low to the ground work tool	uncommanded activation	machine comes to sudden stop while using brush or sweeper	operator	S1	75 %	40 %	100 %	E2	AC0	N/A	N/A	N/A	**c**
CTC8	**boom lower**	bucket work	uncommanded activation	bucket lowers onto co-worker foot during unloading process	co-worker	S1	80 %	33 %	25 %	E1	AC1	AW2	AR2	C2	**a**
CTC9	**boom raise**	bucket work	uncommanded activation	Machine instability during movement of work cycle on uneven terrain. Machine travels between load and unload portion of work cycle with portion of the cycle over uneven terrain.	operator	S2	80 %	16 %	100 %	E2	AC1	AW2	AR2	C2	**c**
CTC10	**tool curl**	low to ground work tool	uncommanded activation	Trencher raises out of ground - co-worker gets caught in chain.	co-worker	S3	75 %	20 %	5 %	E0	AC1	AW2	AR1	C3	**c**
CTC7	**tool dump**	no worse than hold still uncommanded activation													**c**

Table Y.1 *(continued)*

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
CTC11	**auxiliary flow**	low to ground work tool	uncommanded activation	Powered attachment comes on unexpectedly when not in the correct work position. Co-worker becomes entangled with attachment.	co-worker	S3	75 %	20 %	5 %	E0	AC1	AW2	AR1	C3	**c**

Y.2 Supporting explanation

Y.2.1 Supporting explanations for dominant scenarios

CTC1 – propel

H: Only hazardous at the end of the work cycle when the machine would be stopping. H = 10 %

P: Operator is always present during the work cycle. P= 100 %

AC: AC1 - Shut machine down or alter machine direction

AW: AW2

AR: AR1

CTC2 – propel

H: Only hazardous at the end of the work cycle when the machine would be stopping. H = 2 %

P: Co-worker is not always present at the end of the work cycle. P= 25 %

AC: AC1 - Shut machine down or alter machine direction

AW: AW2

AR: AR1

CTC3 – propel

H: Only hazardous at the end of the work cycle when the machine would be stopping. H = 2 %

P: Operator is always present during the work cycle. P= 100 %

AC: AC1 - Shut machine down or alter machine direction

AW: AW2

AR: AR1

CTC4 – propel

H: Only hazardous at the end of the work cycle when the machine would be stopping. H = 2 %

P: Co-worker is not always present at the end of the work cycle. P= 25 %

AC: AC1 - Shut machine down or alter machine direction

AW: AW2

AR: AR1

CTC5 – slow/stop

H: Hazardous at the end of the work cycle as there can be a co-worker present to help guide or unload the material. H = 33 %

P: Co-worker could be present and the area they could be in is larger because of the varied shape of the load (e.g. tree limbs). P= 35 %

AC: AC1 - Shut machine down or alter machine direction

AW: AW2

AR: AR1

CTC6 – hold still

H: Hazard exists for a small portion of the work cycle. H = 5 %

P: Three of the four sides of the machine would be hazardous with the operator present. P= 75 %

AC: AC0

CTC7 – hold still

H: Only hazardous when the boom is raised for co-worker to do unloading activity. H = 40 %

P: Operator is always present during the work cycle. P= 100 %,

AC: AC0

CTC8 – boom lower

H: Only hazardous during the travel portion of the work cycle. H = 33 %

P: Co-worker not always needed to be present for unloading. P= 25 %

AC: AC1 – Shut machine down or move machine

AW: AW2

AR: AR2 - Operator has hands on machine drive controls

CTC9 – boom raise

H: Only hazardous during the travel portion of the work cycle that the boom should be lowered to maintain stability on uneven terrain. H = 16 %

P: Operator is always present during the work cycle. P= 100 %

AC: AC1 – Shut machine down or move machine

AW: AW2

AR: AR2 - Operator has hands on machine drive controls

CTC10 – tool curl

H: Hazardous when the powered attachment is being used. H = 20 %

P: Co-worker would not normally be present during use of powered attachment. P= 5 %

AC: AC1 – Shut machine down

AW: AW2

AR: AR1

CTC11 – auxiliary flow

H: Only hazardous when the powered attachment is not in the correct operating position. H = 20 %

P: Co-worker would not normally be around powered attachment. P= 5 %

AC: AC1 – Shut machine down or ground attachment

AW: AW2

AR: AR1

Y.2.2 Application use cases

Table Y.2 — Application use case table

Application	Travel	Bucket work	Low to ground work tool	Material handling	Off the ground work tool	Power supply	Transport	Maintenance
general use (construction, landscaping, property management)	5 %	80 %	75 %	30 %	5 %	5 %	10 %	5 %
arboriculture	5 %	0 %	0 %	80 %	0 %	0 %	10 %	5 %

Y.2.3 Maintenance task breakdown

NOTE No table "Maintenance task breakdown" exists for this machine. For this size machine, maintenance is performed on a non-running machine where none of the tasks are considered hazardous.

Y.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table Y.3 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
machine propel (direction, steering, and speed)		1	1		Operators are not restrained during motion and uncommanded activation may allow operator to be thrown from machine for ride on machines.
engine speed			1	1	Operators are not restrained during motion and uncommanded deactivation may allow operator to be thrown from machine for ride on machines.
boom raise			1		Failure to release on demand is not worse than uncommanded activation.
boom lower	1		1		
tool dump			1		
tool curl			1		
auxiliary flow			1		
quick coupler engagement					Assumption that coupler is ISO 13031 compliant.
slow/stop	1		1		This is part of machine propel but will be looked at specifically for technical input on determination of $MPL_{r.}$
hold still	1		1		
shutdown / power off					No hazard is identified.

NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.

Y.2.5 Notes and assumptions

— Any interlock used on a compact tool carrier shall meet the highest MPL_r of the system or systems that are being interlocked.

— Arboriculture use case has a compact tool carrier that is dedicated to collecting trimmed trees and branches and transporting them to a chipper. There could be a co-worker at one end of the work

cycle doing the work of trimming trees for transport. There could be a co-worker at one end of the work cycle managing the chipper.

— Machine propel includes direction control (forward / reverse), steering (left / right), and braking (slow/stop).

— Maintenance for this machine type does not require the machine to be energized.

— Travel use case for compact tool carrier is incidental on public roads and not intended to interact with traffic defined in this series of standards because of the travel speed and operator configuration.

— Bucket work use case consists of all activities with buckets such as stockpile management, truck / trailer loading, and material hauling.

— Low to ground work tool use case includes all powered and non-powered attachments that work at grade or below grade where lift arms are typically in a low position, excluding buckets and grapples.

— Material handing use case is for pallet forks and grapples used to move material.

— Off the ground work tool is for powered attachments that could be operated with the lift arms in a raised position. An auger would be an example of this type of attachment.

— Power supply use case is for using the machine auxiliary flow when the operator is not present at the normal operating station.

— Transport use case included the activities to load / unload the compact tool carrier for transport.

Y.3 MPL_r mapped to SCS table

Table Y.4 shows function-based MPL_r (see Table Y.1) mapped to SCS per the results of the MCSSA for a compact tool carrier. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table Y.1 would also be mapped to these MPL_r.

Table Y.4 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
machine propel	uncommanded activation	b	**propel**
	failure to apply on demand	b	
slow/stop	failure to apply on demand	c	**brakes**
engine speed	uncommanded deactivation	b	**throttle control**
hold still	uncommanded activation	c	**parking brake**
	failure to apply on demand	a	
boom lower	uncommanded activation	a	**boom lower**
boom raise	uncommanded activation	c	**boom raise**
tool curl	uncommanded activation	c	**tool curl**
tool dump	uncommanded activation	c	**tool dump**
auxiliary flow	uncommanded activation	c	**auxiliary flow**

Annex Z
(normative)

Powered attachments performance level tables

Z.1 Powered attachments

Scores and percentages for S, A, H, P, E, AC, AW and AR and C are given in the tables for dominant scenarios along with the dominant MPL_r for the function. More details can be found in the subsequent subclause (Tables Z.1 to Z.4) or in Clause 5.

Table Z.1 — MPL_r table for chipper

Ref #	Machine function	Use case	Failure type	Hazardous outcome	Person exposed	S	A variable	H variable	P variable	E	AC	AW	AR	C	MPL_r
PA1	**chip**	usage	uncommanded activation	person standing near outlet when machine starts - gets covered in chips	operator	S2	95 %	20 %	10 %	E1	AC0	N/A	N/A	C3	**c**
PA1	**feed**	considered no worse than chipping													**c**
PA2	**chipper interlock**	usage	failure to release on demand	feed control bar fails to stop someone getting sucked into feed	operator	S2	95 %	90 %	5 %	E1	AC0	N/A	N/A	C3	**c**

Z.2 Supporting explanation

Z.2.1 Supporting explanations for dominant scenarios

PA1 – chip

H: Only when in ready state (20 %). H = 20 %. It is considered machine abuse to stand near outlet while chipping.

P: Percentage of time someone stands near the discharge. P= 10 %

AC: AC0

PA2 – chipper interlock

H: Anytime they are feeding the machine (10 % idle factor). H = 10 %

P: Only when close enough to the inlet - when feeding small material (large material would be fed from further back). Inlet shoots are designed to be a long way from the feed wheel (distance guard). P= 5 %

AC: AC0

Z.2.2 Application use cases

Table Z.2 — Application use case table

Application	Usage	Maintenance
general (construction, landscaping, and utilities)	95 %	5 %

Z.2.3 Maintenance task breakdown

NOTE No table "Maintenance task breakdown" exists for this machine. For this size machine, maintenance is performed on a non-running machine where none of the tasks are considered hazardous.

Z.2.4 Function dominant failure type matrix

Function-dominant failure type matrices reflect the approach that was taken during the MCSSA and outline where some truncation occurred. The notion is that some failure types result in the same hazardous outcomes as other failure types and, therefore, result in the same performance level required (e.g. failure to apply on demand and uncommanded deactivation of the park brake would result in the same hazardous outcome; park brake is off when the operator expects it to be on).

Table Z.3 — Function dominant failure type matrix

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
mixer - mix			1		Considering failure to stop is the same as uncommanded activation.
mixer - discharge			1		Considering failure to stop is the same as uncommanded activation.
pump - pump			1		Considering failure to stop is the same as uncommanded activation.
chipper - chip			1		Considering failure to stop is the same as uncommanded activation.
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

Table Z.3 *(continued)*

Function	Failure to apply on demand	Failure to release on demand	Uncommanded activation	Uncommanded deactivation	Notes
chipper - feed			1		Considering failure to stop is the same as uncommanded activation.
chipper interlock			1		
NOTE A "1" has been placed in the cell for function - failure type combination that would or could potentially cause the most hazardous failure.					

Z.2.5 Notes and assumptions

— Powered attachments that do not require an operator to operate them outside of the operator station were not considered.

— Concrete pump was assessed and found to be non-hazardous.

— Concrete mixer was assessed and found to be non-hazardous.

— Certain powered attachments that are used outside the scope of ISO TC 127 were ignored.

Z.3 MPL_r mapped to SCS table

Table Z.4 shows function-based MPL_r (see Table Z.1) mapped to SCS per the results of the MCSSA for powered attachments. Other systems that fail in a way that cause a hazardous outcome similar to the function failures in Table Z.1 would also be mapped to these MPL_r.

Table Z.4 — MPL_r mapped to SCS

Machine function	Failure type	MPL required	Example of mapped system
chip	uncommanded activation	**c**	**chip**
chipper feed	uncommanded activation	**c**	**chipper feed**
chipper interlock	uncommanded activation	**c**	**chipper interlock**

Annex AA
(normative)

Miscellaneous functions

AA.1 Operator presence systems

AA.1.1 General

This assessment shall apply if an operator presence system is fitted to a machine and is associated with a SCS output (indicators and alarms that are the primary output are not considered). Operator presence systems primarily considered in this assessment consist features for detecting if the operator is present (e.g. seat sensors). Levers intended to isolate machine functions may also be applicable. The assessment is not suggesting the provision of these systems is required. The design features of operator presence systems can vary based on machine type and application.

AA.1.2 Failure on demand

AA.1.2.1 General

Failure to detect and react to the operator not being at the operator station.

Operator presence systems mitigate the hazard of inadvertent activation of controls while the machine is not in a safe state; it can also be a control function that the operator expects to be activated under given conditions to prevent a hazard (e.g. a park brake being applied).

The hazardous outcome of a failure on demand of an operator presence system is:

a) machine function operates due to inadvertent actuation while operator is egressing or is not at the operator station causing contact with the machine from implement movement (e.g. an implement control),

b) or machine moves while operator is egressing or is not at the operator station causing a run over due to a function not applying (e.g. a park brake).

AA.1.2.2 Severity

The severity associated with this SCS failure is the same as the highest severity in scenarios where the operator may not be at the operator station while the machine is not in a safe state as part of the work cycle or tasks associated with the machine lifecycle. It would not be the severity of control system failures associated with scenarios where the operator would always be present at the operator station (e.g. while digging, loading a truck or traveling).

AA.1.2.3 Exposure

The exposure in this case would only be the time in the lifecycle or task that the operator would not be at the operator station while the machine is not in a safe state. It does not include scenarios where the machine would be left in an energized state that are considered machine abuse (e.g. the machine with implements raised).

For operator presence implement and steering systems this should be E0 but may be higher in specific applications outside the typical use for earth-moving machines. If the operator presence system is addressing a failure of a system to apply (e.g. park brake systems) the exposure assessment for the

operator presence system failure to apply on demand shall be the same as the exposure for a failure to apply on demand or uncommanded release of that system.

AA.1.2.4 Controllability

Because the operator, by nature of these systems, is not at the operator station, there are not normally alternative controls. Therefore, the controllability shall be AC0. An exception to this would be where a machine lockout is fitted that prevents the operator from getting out of the operator station without engaging the lockout, which may be AC1, AW2, AR3 = C1.

AA.1.2.5 Example

A wheel loader that isolates the implement when the operator is not at the operator station would have the following MPL_r.

Severity:

The highest severity of implement movement in maintenance and slow speed manoeuvring use cases is S3.

Exposure:

The operator presence system is mitigating the hazard of inadvertent activation of the implements while accessing and egressing the machine. The operator is near the controls 30 s each time the operator accesses and egresses the operator station combined. The most an operator enters and leaves the cab in different applications is in construction, which is once an hour.

(0,5 min / 60 min) × 100 % = 0,8 % - E0

Controllability:

If there is no implement lock out lever on the machine, there is no means of avoiding an inadvertent command while the operator is not at the operator station. AC0, C3.

If there is an implement lock out lever that cannot be maneuvered around, the controllability would be AC1, AW2, AR3 (natural reaction – the operator must move it to get out of the operator station). C1.

MPL_r Calculation:

Without an implement lock out lever – $MPL_r = c$

With an implement lock out lever – $MPL_r = a$

Uncommanded activation – falsely detecting operator is not at the operator station

The MPL_r for each function controlled by the operator presence system shall be the same as the highest MPL_r of an uncommanded activation of that system or function.

AA.2 E-stops

AA.2.1 General

This document does not dictate the provision, location or class of e-stop; it only assesses the required system integrity if the e-stop could fail in a way that puts people at risk of injury.

NOTE Notwithstanding any guidance in AA.2, ISO 13850 provides guidance on e-stop design and requirements, including a minimum MPL_r of c.

AA.2.2 Failure on demand

AA.2.2.1 Severity

The severity associated with this SCS failure is the same as the highest severity in scenarios where a person is in a situation where they could be exposed to a hazard while the machine is not in a safe state as part of the work cycle or tasks associated with the machine lifecycle.

AA.2.2.2 Exposure

E-stops are only safety related when they are being used to immediately avoid a hazard and are intended to be a complementary protective measure, not to substitute a safeguarding measure. Normally on earth-moving machines this is rare so the exposure shall be assessed at E0.

AA.2.2.3 Controllability

Because e-stops are only safety related when they are being used to immediately avoid a hazard and are intended to be a complementary protective measure, not to substitute a safeguarding measure, controllability shall be assessed at C3.

AA.2.3 Uncommanded activation

For systems where the uncommanded activation is hazardous, the MPL_r for each function controlled by the e-stop system shall be the same as the highest MPL_r of an uncommanded activation of that system or function.

AA.3 Remote control

AA.3.1 General

Remote-control technology is being developed and deployed across the earth-moving industry at a rapid rate. The tables in this document have been developed based on the industry consensus of applications, limits and system features of base machine functions. For remote-control systems and applications, this consensus has not yet been reached across the industry and applications are too broad to develop specific tables for remote control functions.

The MPL_r in the tables in this document may be used for remote control. However, upon reviewing the assessment, if the scenarios in the tables do not accurately describe the remote-control machine application considered, an MCSSA shall be performed per ISO 19014-1 (see Clause 4).

NOTE There can be scenarios where the MPL_r in the tables in this document are higher than is necessary for remote control.

The guidance in this document assumes that the remote-control systems and the machines under remote control are designed in conformance with the ISO 20474 series, including system safety standards (e.g. ISO 15817, ISO 5010, ISO 3450, ISO 13850, ISO 5006 and ISO 16001). Such International Standards can identify functions that are not associated directly with the base machine in the tables in this document; those functions shall be assessed through an MCSSA per ISO 19014-1 (e.g. mode change, remote stop, e-stop). Additional safety measures can result in additional safety functions, or fault reactions, based on application specific conditions (e.g. loss of signal).

NOTE Some MPL_r in the tables in this document assume a fail-operable system. This is not possible for some remote-control technologies.

This document applies to both wired and wireless remote-control systems.

When considering applications for a remote-control system, particularly those extending the limits of machine use from a direct controlled machine, attention shall be given to new hazards created and how existing hazards have changed. An example of an extended application is the use of a remote-controlled

hydraulic excavator operating on weak foundation or under an unsupported roof while demolishing a building.

AA.3.2 Work area restrictions

An important factor when determining MPL_r of remote-control systems is the extent to which access to the work area is restricted. The purpose of the restriction is to keep remote-controlled machines in the work area and keep unauthorized people, vehicles and machines out. This restriction can be achieved through various means, e.g. administrative controls, physical barriers, electronic systems. It is the responsibility of the worksite to conduct a risk assessment to manage risks associated with remote-control work areas.

MCSSA that are performed assuming a level of restriction of the work area shall provide all assumptions and limits of the machine use to the user of the machine.

NOTE Some work cycles can have machines moving between work areas with varying levels of restriction

AA.3.3 Significance of remote stop functions

When operating in restricted work areas, the remote stop function may be considered the primary safety function, which can result in fewer safety functions. When using the remote stop as the primary safety function, all functions that are controlled by the remote stop function shall be assessed for the applicable failure types and applications, the highest MPL_r of these functions shall be used. If the MCSSA determines there will not be enough time to react to a failure, the remote stop may not be used as the primary safety function. (See Table AA.1.)

NOTE If the remote stop is the primary safety function, it is not considered an e-stop.

Table AA.1 — Example of how a function-based assessment would map to a remote stop MPL_r

Remote control function-based assessment MPL_r		Remote stop MPL_r	
slow/stop	**c**	remote stop	**c**
propel	**b**		
steering	**c**		
direction	**b**		
boom down	**a**		

AA.3.4 Differences between direct control and remote-control machine assessments

The following is a non-exhaustive list of aspects that can affect the severity for a remote-control application compared to a direct controlled application.

— The injury to the operator:

  — based on location, visibility, and site conditions (e.g. restricted space around machine),

  — dominant scenarios in the base machine assessment involving an operator injury due to being on or in the machine may be omitted from the remote-control machine assessment.

— The injury to the maintainer:

  — minimal maintenance would be performed on a machine in remote-control mode (e.g. troubleshooting the remote-control system on machine stands),

  — scenarios in the base machine assessment considering other maintenance tasks may be omitted from the remote-control machine assessment.

— The injury to co-workers and bystanders based on:

  — the level of restriction of the work area,

- whether machines operated around the remote-controlled machine are direct controlled or remote-controlled,
- activities occurring outside of, but near the work area.

The following is a non-exhaustive list of aspects that can affect the exposure for a remote-control application compared to a direct controlled application.

- The A variable:
  - application use cases percentages may vary between direct and remote-control modes,
  - specific remote-control applications that are not relevant to a direct controlled machine may need to be added to the MCSSA.
- The H variable:
  - the percentage of the work cycle where there is potential for interaction between the remote-control machine and other direct controlled machines, light vehicles and pedestrians may vary between direct and remote-control modes. Some examples are:
    - mode change,
    - remote-control machines loading direct controlled machines,
    - other persons associated with the work task,
    - direct controlled machines working in parallel,
    - operators of other remote-control machines,
  - the type of technology used to restrict the area, including the limitations and degradation of the technology; based on the level of restriction, the H variable may vary between direct and remote-control modes,
  - h variable of the operator can change based on site operating conditions and practices.
- The P variable:
  - the level and method of restriction of the work area.

The following is a non-exhaustive list of aspects that can affect the controllability for a remote-control application compared to a direct-controlled application.

- Remote control design can be such that the main and alternative controls can have a common cause failure; if this is the case, the AC score shall be AC0.
- Reactions associated with stop functions are only applicable if the operator is aware of the hazard and can react in time.
- Remote-control operators can detect, and react to, failures of control systems differently than operators of direct controlled machines. Examples of aspects to consider in this context are:
  - visibility,
  - operators can evade uncontrolled machine motion if the work area has the appropriate ground and space conditions. Other person groups around the remote-control machine operation could be unaware of machine motion; therefore, their ability to avoid cannot be considered.
- Layers of protection, beyond the remote-control system, that are used to prevent unauthorized exiting and entering the remote-control work area.

Bibliography

[1] ISO 13031, *Earth-moving machinery — Quick couplers — Safety*

[2] ISO 13850, *Safety of machinery — Emergency stop function — Principles for design*

[3] ISO 15817, *Earth-moving machinery — Safety requirements for remote operator control systems*

[4] ISO 5010, *Earth-moving machinery — Wheeled machines — Steering requirements*

[5] ISO 3450, *Earth-moving machinery — Wheeled or high-speed rubber-tracked machines — Performance requirements and test procedures for brake systems*

[6] ISO 5006, *Earth-moving machinery — Operator's field of view — Test method and performance criteria*

[7] ISO 16001, *Earth-moving machinery — Object detection systems and visibility aids — Performance requirements and tests*

(*Continued from second cover*)

The Committee has reviewed the provision of the following International Standard referred in this adopted standard and has decided that it is acceptable for use in conjunction with this standard:

International Standard	*Title*
ISO 19014-2 : 2019	Earth-moving machinery — Functional safety — Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system
ISO 19014-4	Earth-moving machinery — Functional safety — Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system

For the purpose of deciding whether a particular requirement of this standard is complied with, the final value, observed or calculated expressing the result of a test or analysis, shall be rounded off in accordance with IS 2 : 2022 ‘Rules for rounding off numerical values (*second revision*)’. The number of significant places retained in the rounded-off value should be the same as that of the specified value in this standard.

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 2016 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the website-www.bis.gov.in or www.standardsbis.in.

This Indian Standard has been developed from Doc No.: MED 07 (23239).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.gov.in

Regional Offices:		*Telephones*
Central	: 601/A, Konnectus Tower -1, 6th Floor, DMRC Building, Bhavbhuti Marg, New Delhi 110002	2323 7617
Eastern	: 8th Floor, Plot No 7/7 & 7/8, CP Block, Sector V, Salt Lake, Kolkata, West Bengal 700091	2367 0012 2320 9474
Northern	: Plot No. 4-A, Sector 27-B, Madhya Marg, Chandigarh 160019	265 9930
Southern	: C.I.T. Campus, IV Cross Road, Taramani, Chennai 600113	2254 1442 2254 1216
Western	: 5th Floor/MTNL CETTM Technology Street, Hiranandani Gardens, Powai, Mumbai - 400076	283 25838

Branches : AHMEDABAD, BENGALURU, BHOPAL, BHUBANESHWAR, CHANDIGARH, CHENNAI, COIMBATORE, DEHRADUN, DELHI, FARIDABAD, GHAZIABAD, GUWAHATI, HARYANA (CHANDIGARH), HUBLI, HYDERABAD, JAIPUR, JAMMU, JAMSHEDPUR, KOCHI, KOLKATA, LUCKNOW, MADURAI, MUMBAI, NAGPUR, NOIDA, PARWANOO, PATNA, PUNE, RAIPUR, RAJKOT, SURAT, VIJAYAWADA.

Published by BIS, New Delhi