DO NOT DISTRIBUTE.

This is an Urban Robotics Foundation (URF) member-only review edition, confidential to ISO/TC204/WG19 and URF.

This doc has been prepared by ISO WG19 and URF. It is work in progress, subject to change and therefore unreliable.

This document represents NO commitment by the ISO to publish.

Progress: 75%; Expected completion: Fall 2024

– Bern Grush (2024.06.02)

ISO 4448-16:2024(X)

ISO TC 204/WG 19

Secretariat: ANSI

Intelligent transport systems — Public-area Mobile Robots (PMR)—Part 16: Safety and Reliability

WD stage

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204 WG19.

A list of all parts in the ISO 4448 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The ISO 4448 series[1] is concerned with public-area mobile robots (PMRs) and their interactions with human bystanders in regard to the safety and social comfort of those bystanders. Some of these concerns are robot behaviour or capability concerns within the immediate, social and physical presence of individual bystanders, while other concerns relate to system (fleet) management capabilities that address livability matters within the effective social region of a PMR or a PMR fleet.

This part of the ISO 4448 series addresses three groups of subjects related to safety and reliability of PMRs. In all cases, this document is concerned for proximate human or animal bystanders, whether such bystanders are pedestrians, cyclists, micromobility users, motorists, or pets.

This document makes the fundamental assumption that such bystanders are often uninvolved with the relevant PMR task or activity, unprotected from any such PMR activity or behaviour as it moves or works, untrained in any form of collaboration with a proximate PMR, and inattentive to the activity of any proximate PMR.

This document is agnostic to the design, purpose, or task of a PMR or a PMR fleet. It is agnostic as to whether the PMR is controlled via teleoperation, remote oversight, on-board and cloud-based autonomy, or a combination of these. It is agnostic as to whether the PMR is owned by a commercial entity performing a commercial activity, a public entity performing a public (government) task, or is owned and deployed by a private individual within a public space. Lastly, it is agnostic as to whether the PMR is operating outdoors, or indoors, whether it is operating in private commercial space such as in a hospital, airport or retail facility, or within a government jurisdiction such as in government buildings, public parks, sidewalks, crosswalks, or roadways.

This document may not be applicable to a mobile robot that is operating in a private space where there are no uninvolved bystanders. An example of this, would be a maintenance robot, such as one mowing a lawn or scrubbing a floor, wherein the operator of that robot excludes all bystanders from the operating space or activity of that robot.

The distinction between a mobile robot and a PMR is the presence of proximate, uninvolved bystanders—a PMR is defined by its context of deployment, rather than by the specifics of its design.

[1] See ISO DTR 4448-1

Intelligent transport systems — Public-area Mobile Robots (PMR)—Part 16: Safety and Reliability

1 Scope

This document describes multiple properties and capabilities required for public-area mobile robots (PMRs) to operate safely and reliably in public spaces shared with human bystanders.

The scope of properties and capabilities includes physical, telecommunications and management properties related to PMR capabilities

- within their immediate location
- relative to the physical safety (integrity) of the PMR itself, and
- relative to the safety of proximate humans when in direct interaction with PMRs.

The scope is exclusive to times and locations when PMR properties, behaviours, and actions interact with, or have the potential to impact, human bystander safety and wellbeing.

The scope of human bystanders includes pedestrians, cyclists, micromobility users, motorists, or pets.

The scope of PMR safety and reliability includes the equipment, software, and management oversight related to the operation of PMRs and fleets of PMRs. Such safety and reliability must ensure no alarm or confusion to proximate persons, pets or property

The scope of PMR safety and reliability risk related to location includes any unintended or unexpected loss or crash because of a location that a PMR has navigated to. (A PMR shall always be capable of safe operation or recovery for whatever location it is in.)

The scope of PMR safety and reliability related to itself includes harms incurred to or by a PMR including harm to any attached tool or load from such things as crash or fire, seizure or vandalism. (A PMR shall be designed, constructed, and managed to minimize harm to itself, it surroundings and proximate humans during any interaction with humans.)

The scope of safety and reliability related to proximate humans is related to direct human interaction with PMRs regardless of whether the interaction is initiated by the PMR or a bystander. (A PMR shall be able to communicate and behave to maximize human safety including compliance in emergency circumstances.)

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.

EN 60529 Degrees of protection provided by enclosures (IP code)

IEC TC125 WG6 General requirements for autonomous cargo e-transporters (check first)

ISO 7176 (Parts 1,2,3,6,7) — “Wheelchairs”

ISO 10218-1: Robots and robotic devices — Safety requirements for industrial robots — Part 1: Robots

ISO 13482:2014 Robots and robotic devices—Safety requirements for personal care robots.

ISO 19091 “Using V2I and I2V communications for applications related to signalized intersections”

ISO 19649: Mobile robots — Vocabulary

ISO 26262 “Road vehicles — Functional safety”

ISO/SAE PAS 22736: Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles

SAE J2735 “V2X Communications Message Set Dictionary Set”

UL 2271 Standard for Batteries for Use in Light Electric Vehicle (LEV) Applications

UL 3300 7.2 “Safeguards for Mobility”

3 Terms and definitions

For the purposes of this document, the terms and definitions in ISO/TS 14812:2022 and ISO/TR 4448-1:202X apply.

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

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

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

3.1
minimal risk condition
see SAE J3016

3.2
pathway
use TR 4448-1

3.3
public-area mobile robot
PMR
use TR 4448-1

3.4
shyDistance
xxx

3.5
teleoperator
use TR 4448-1

3.6
xxx
xxx

4 Abbreviations

ADS automated driving system

AMR automated mobile robot

IMR industrial mobile robot

ODD operational design domain

PMR public-area mobile robot

5 Safety System Descriptions

5.1 Overview

In this part of the ISO 4448 standard series, system safety is defined in terms of integrated subsystem outcomes rather than specific technology components. Because of the highly variable nature of the design and task intentions of PMRs, the intention of this document is to describe safety and reliability subsystem outcomes as well as enable measures and tests of these subsystems regardless of the specific nature of the sensor, effector, power or software components that might be used in the design and operation of any particular PMR.

For example, this document is concerned with reliable perception under all *ODD* circumstances rather than with specifications for vision or audition devices or their resolutions. As well, the standard is concerned that PMRs maintain appropriate distances (defined as *shy distances*) from all other objects and persons for both safety and social acceptance reasons. Hence, such things as braking distance and reliable braking combine with reliable perception and measurement to serve that primary goal.

The sensors and software that enable a PMR to measure and calculate shy distances are critical, but are not specified. Only system and subsystem outcomes are specified. This implies that any tests to certify behavior may treat systems and subsystems as black boxes, measuring only the required safety outcomes. This maximizes opportunities for innovation and optimization while focussing on safety outcomes. The downside is that any test regime must retest all related aspects of a system since there are no specifications for the integration of its parts.

This emphasis on systems rather than components is made because a system or subsystem may comprise subsystems or components of varying reliabilities while itself comprising a reliable system or subsystem. This outcome may be the effect of software or component redundancy or specific forms of human oversight or even systems that rely partly or entirely on teleoperation. Hence, a focus on specific component elements can lead to unnecessary concern or false reliance.

Regardless of any definition of safe behaviour, safe systems or safe outcomes, in this document primary PMR safety is about the safety of proximate humans—of any ability—whether walking, using an assistive or a micromobility device, using a motor vehicle with a proximate area such as a crosswalk and whether or not interacting with the PMR (e.g., removing its cargo, receiving information, crossing its path, or apprehending the device). There is a secondary interest that any PMR avoid self-harm from crash, fire, seizure, becoming lost or physically unstable. Should any of these forms of PMR self-harm become a risk to proximate humans then they would become a primary concern. When interpreting the clauses of this document, risk or harm to humans or their pets must take precedence over property damage, including damage to the PMR itself.

This document is concerned with PMR capability and fitness to perform safely rather than any software capability that manages specific, defined behaviours. For example, specific PMR behaviours including

behaviours in respect to other users, specific infrastructure components, and traffic management rules as it traverses a pathway are addressed in other parts of this series.

One exception to this is the subsystems that ensure safe crossing of roadways. Currently, crossing at some types of signalized intersections may require specific V2X signals so that PMR behaviour in regard these aspects of the specification are constrained by related standards for signalized intersections.

5.2 Compliance

All designs and forms of PMR shall comply with all safety aspects in this document in order to claim compliance. All regulations for PMRs that comply only partially with these safety standards shall indicate exact exemptions.

NOTE This document applies equally to wheeled, legged and tracked PMRs. Any regulation that sites this document but does not or cannot accept both types of mobility effector, or wishes to regulate certain exceptions, must include that explicitly.

NOTE The same applies to all other elements such as power source, remote operation, enforcement, etc.

NOTE It is almost certain that many PMR designs in commercial use will be inadequate as innovation continues, hence this document anticipates that many innovations and design improvements that are currently unexpressed, and that government regulations should remain aware of this.

5.3 Three safety system categories

This document identifies several safety subsystems organized into three critical categories related to location, device and human interaction. **Location Safety** concerns PMR safety related to motion, stability, and location; **Device Safety** concerns the safety of PMR electrical and mechanical systems; and **Human Interaction Safety** concerns PMR safety in relation to interaction with humans, such as bystanders, law-enforcement personnel, and teleoperators. These categories are shown in **Table 1**.

This document is focused on the safety-efficacy of subsystems; hence, it is the safety outcomes or safety requirements that are described and measured. These outcomes are described to support system and subsystem safety relative to proximate humans.

The standard is silent as to whether any PMR test described or implied is:

- carried out by its manufacturer or fleet operator;
- promised by a vendor in the form of a reliability guarantee or evidence of insurability;
- carried out by an independent third party for certification (certification is not in scope).

Regardless of how system and subsystem safety may be certified or guaranteed, a potential test is whether the user or fleet operator of any vehicle or PMR is able to obtain liability insurance sufficient to permit its operation within a stated ODD. In this way, certifying parties or certification processes would use the standard as a guideline and insurability as its guarantee.

Considering the nature of actuarial sciences and subrogation practices, this approach could maximize the safety outcome as long as jurisdictions insist on fleet registration and evidence of adequate liability coverage. This approach assumes financial penalties would cause vendors and fleet operators to act more conservatively (safer) than would governance penalties alone.

Table 1: Safety components relate to surroundings, devices and humans.

Location safety	● Movement and stability ● Perception reliability ● Localization and odometry

Relates to proximate surroundings of the PMR (to keep proximate humans safe)	• Road crossing systems
Device safety Relates to self-containment of the PMR (to keep proximate humans safe)	• Power safety • Task component safety • Electronics safety • Failure recovery systems
Human Interaction safety Relates to human interaction with the devices (to keep proximate humans safe)	• Communication safety • PMR-to-human communication reliability • Emergency compliance systems • Seizure compliance systems

5.4 Shy Distance as a location-sensitive metric

shyDistance (SD) is a variable distance within this document, becoming a fixed value during an implementation of the standard.

The term *shy distance* refers to:

- The buffer distance between vehicles or pedestrians as they pass each other;
- The buffer distance from any object in motion to objects it is passing, such as the difference between a pedestrian and a wall or between a car and a curb;
- A buffer distance between any two objects in motion such as the distance between a PMR and a pedestrian;
- The distance between two humans as they are standing and speaking to each other.

This latter meaning differs among cultures and contexts with some people being willing to stand very close, and others keeping a greater distance.

Distances to be measured and maintained between a PMR and other object are given in multiples of the unit, shyDistance (SD). The purpose for this derived metric is to respect cultural or social differences and well as to be able to scale numerous distances as variables which can be manipulated to suit local social preferences, regulations, and deployments.

E.G.: "A PMR shall attempt to ensure a lateral space of 1.0 SD when passing a pedestrian in the opposite direction, and to ensure a lateral space of 1.5 SD when overtaking a pedestrian travelling in the same direction." In some locations, shyDistance might be set to 0.5 m and in others 1.1m. In other words, shyDistance can be set differently in one city compared to another, or set differently inside an airport compared to a hospital. Once set within a context, the spatial-distance dynamic changes throughout that deployment.

Human active transportation environments are not so structured as this definition implies; hence, these numbers are provided to inform the PMR's ADS system or teleoperator of the expected distances to be respected. These systems and operators will be required to find safe and workable solutions within this fluid environment.

NOTE With respect to shyDistance compliance, the demand for a defined distance between a PMR and another object (animate or inanimate) cannot currently be done practically using GNSS. The standard assumes that a machine that is to locate itself in space amongst other objects must have a means of measuring the (dynamic) distances between itself and other objects. There are a number of technologies to accomplish this. This document does not identify those. This is left to the maker of the PMR.

5.4.1 shyDistance table

Table 2: Shy distance metrics. All other SD metrics are multiples of these

Purpose	Pathway descriptor	Toler -ance	Default	Comment
Core unit	SD	100	1000	All units in mm
Comfort, Safety	SDdynamic	60	600	Shy distance to Dynamic (non-stationary) objects observed by PMRs while moving or passing. (pedestrian, pet, wheelchair, or another bot. Default is to assume an unmapped object is non-stationary). (FHWA recommends 24 inches = 609mm). There are many circumstances and narrow passages where this will not be possible. This is meant for normal travel and the rules to deal with very narrow passages are elsewhere.
Comfort, Safety	SDstatic	20	20	Shy distance to static (stationary) objects (to be observed by PMRs while moving or passing). (Wall, steps, sign, garbage bag. A human sleeping on the pavement is not a stationary object but could easily be mistaken as such.)
Comfort, Safety	SDstandback	180	1800	Shy distance to stand back from intersections and curb cuts while waiting. This is to allow room for pedestrians to gather to wait and to proceed first at intersections and for disabled users to access curb cuts unhampered by idling or waiting PMRs.

5.5 Location Safety

Location Safety pertains to safety regarding location-dependent circumstances. This includes reliable PMR abilities to:

- move and maintain stability within the location a PMR is travelling within its ODD;
- perceive sufficiently the surrounding navigation context of the location a PMR is travelling in;
- position itself within its navigation context and to report that position; and
- cross roadways within its navigation context.

For each subclause, the intention is to ensure that PMRs and their support systems and operators operate safely and successfully in their ODD. This recognizes that many types of mishap hold risks of confusion, discomfort, or harm to human bystanders.

5.5.1 Location Safety: Movement and stability

The Location Safety group of measures relates to reliability and control regarding travelling on a surface or within a space so that a PMR or train of PMRs moves safely and predictably through its intended pathway. “Safely” means without collision or near collision, without confusing or alarming any proximate pedestrian or other user, and without harm to the PMR itself.

5.5.1.1 Choice of motion effectors

The choice of motion effectors such as wheels, legs, and tracks for PMRs depends on factors such as ODD terrain, payload, tasks, intended speed, manoeuvrability, etc. This document applies equally to all forms and combinations of motion effectors.

5.5.1.2 Longitudinal and lateral control

Longitudinal and lateral control reliability and safety measures all aspects of safe, physical control of the navigational motion of a PMR. Lateral and longitudinal orientation are defined with respect to the direction of motion.

A PMR navigating in any circumstance in which it cannot meet the requirements for longitudinal or lateral control, shall attempt to adopt a **minimal risk condition** and wait for the circumstance to revert to a safe circumstance or to be rescued.

A PMR experiencing loss of longitudinal or lateral control shall signal its remote oversight operator, or its condition shall be immediately discovered by its remote oversight operator.

In no case shall a PMR be able to experience loss of longitudinal and lateral control without being able to signal its remote oversight operator except in the cases of severe crash or loss of communication including from power failure.

5.5.1.2.1 Maneuverability

A PMR shall be able to avoid obstacles and navigate safely given the immediate operating conditions within an ODD such as low surface friction, high winds, fast-moving obstacles, damage of or loss to a sensor or an effector which would diminish its ability to maneuver, etc.

5.5.1.2.2 Stability

A PMR shall be able to sustain or regain an upright posture that is sufficient for both longitudinal and lateral control.

5.5.1.2.3 Longitudinal control

A PMR shall be able to maintain longitudinal control, including:

5.5.1.2.3.1 Braking

Braking; both for safety (not crashing) and for maintaining shy distance; note that maintaining shy distance always exceeds the zero-crash criteria.

A PMR navigating on a footway, shall maintain a speed such that it can stop in {1000, ±200} mm. This applies to any surface condition and any reaction time—i.e., whether the PMR is controlled via ADS or teleoperator.

NOTE **Braking distance**, when travelling 1.67m/s will be 0.4 - 0.6 m when best (braking on 2 of 4 wheels, like a powered brake on dry tiles/asphalt)

NOTE With respect to braking under teleoperator control, AASHTO allows humans 1.5 seconds for perception time and 1.0 second for reaction time. If traveling 6 k/h (1.67m/s), then a "begin braking response under teleoperator control" means 2.5s x 1.67m/s = 4.175m of travel is possible before braking is started, Hence, a stopping distance of 1.0m is infeasible. Teleoperation has important limitations so that automated braking will be critical. (should this be mandated?)

A PMR navigating on a bikeway, shall maintain a speed such that it can always stop in {3000, ±300} mm. This applies to any surface condition and any reaction time—i.e., whether the PMR is controlled via ADS or teleoperator.[2]

[2] References regarding human reaction time: [1] https://www.tac-atc.ca/sites/tac-atc.ca/files/site/volume1-errata-dec09.pdf [2] https://www.ottawasafetycouncil.ca/stopping-distances-and-distracted-driving

5.5.1.2.3.2 Slipping

Slipping (friction) due inadequate tire/wheel materials or designs for the ODD surface; this can cause an inability to maintain shy distances and possibly contribute to crashes.

A PMR shall only navigate on a surface such that the coefficient of friction, COF (kinetic) for its tires/feet/tracks is 0.5 or more.

NOTE Related to surface friction, wheels, feet can slip/slide. Rubber COF on wet asphalt is ~0.5; on dry concrete, COF is ~0.8

5.5.1.2.3.3 Bunching

Bunching applies to trains of PMRs (*Longitudinal string stability*)

Relative speed management between adjacent PMRs in a train shall be managed to ensure sufficient space between adjacent PMRs so that they

- Do not crash into each other
- Do not obstruct other users, such as pedestrians, who may cross between adjacent PMRs in a train

5.5.1.2.3.4 Traps

Wheels, feet, and other effectors or parts shall be sized to avoid getting stuck in or on a pathway element when moving on terrain with holes, bumps, discontinuities, heaving, cracks, fissures, etc. The minimum width for the tires, feet, or tracks for a PMR shall be {55, ±5}mm

NOTE this is related to gaps in or on the travel surface. Wheels, feet, armatures, can get stuck/wedged in cracks, grates, rails, potholes.

5.5.1.2.4 Lateral control

A PMR shall be able to maintain lateral control, including retaining control:

- On curves, or when making U-turns
- When following (e-tethered) (*Lateral string stability*)

PMRs traveling in a train shall maintain lateral string stability such that the lateral displacement of any follower PMR relative to the leader PMR shall be a maximum of {150,±50}mm.

NOTE a “train” of PMRs means that each is electronically tethered to the one before it, and the entire group is led by the first in the train. This also applies to one or more PMRs following a human leader of a train.

5.5.1.3 Stability (static and dynamic)

Along a cross slope a PMR may encounter a steep in-line driveway ramp, pavement heaved by tree roots, or construction disturbance. Along a running slope, a PMR may encounter deep potholes, high curbs, or unsloped curb ramps. There may be circumstances in which a PMR must leave a footway to use a road shoulder or bike lane while circumventing an obstacle. Such a robot may have to dismount and remount a steep, uncut curb.

PMR stability concerns the ability to remain upright in the case of an infrastructural challenge such as a steep curb or deep pothole or a navigational failure such as the wheels or feet on one side slipping off the edge of a curb or step. For example, a PMR must be able to mount or dismount a curb to exit or enter a crosswalk, respectively. Curb heights are approximately 15 cm. Not all curbs are sloped for ease of mounting by a wheelchair.

A PMR shall be able to remain or regain its upright posture relative to its design within the terrain and conditions of its ODD.

A PMR manufacturer shall specify the maximum height a vehicle can mount without tipping.

NOTE Mounting a step change may depend on the slope of the pathway leading up to the step change.

Stability for a PMR is the tendency to remain upright when at rest (static) or in motion, especially under acceleration (dynamic).

The static and dynamic stability of a PMR shall allow it to remain upright on a running slope of 60% (31°) and a cross slope of 60% (31°).

NOTE This is very steep. The FHWA recommends against "any man-made grade that exceeds 8 percent" (https://safety.fhwa.dot.gov/ped_bike/univcourse/pdf/swless13.pdf). *This clause is not a recommendation for infrastructure, it is a safety margin for a device to be untippable at the moment of climbing, a curb or a step. It must exceed almost any gradient a city can present.* A balance must be struck between overengineering and disabled PMRs in public spaces. Here is a paper describing tipping stability for wheelchairs: Thomas L., Borisoff J., and Sparrey C. (2018) "Manual wheelchair downhill stability: an analysis of factors affecting tip probability"

NOTE Running slope is measured from the center of the front wheel(s) to the center of the back wheel(s). Cross slope is measured from outer edge of the left wheel(s) to the outer edge of the right wheel(s).

The consequences of a PMR tipping over shall not include risk of fire or spillage of hazardous material.

A PMR reasonably challenged shall not tip over regardless of wheel configuration, wheelbase dimension or mobility effector type or design. This is exclusive of vandalism or police action during an apprehension or emergency action.

The risk of tipping imposing harm on proximate humans shall be expressly covered by a liability policy.

PMR stability may be evaluated through a variety of tests. The angle at which a PMR begins to tip shall be evaluated for a suitable variety of orientations and configurations (standing, moving at normal speeds, brakes applied, brakes not applied, zero load, max load).[3] If an anti-tipping or self-righting mechanism is deployed, then that mechanism shall be considered part of the PMR for purposes of this metric.

NOTE Test specifications for tipping are out of scope.

5.5.1.4 Braking/stopping

PMR stopping distance is critical for longitudinal control.

Stopping distance depends on the nature and condition of the brakes, friction of the tires/feet/tracks relative to road surface conditions, PMR speed and gross weight. The maximum stopping distances for PMR operation on footway and bikeway are listed in 5.5.1.2.3.1.

In the case of a legged PMR, braking mechanisms may differ but maximum stopping distance shall not be greater.

In cases where surface friction is reduced, a PMR shall reduce its speed so that it can satisfy stopping distance requirements. Tests shall be conducted at ODD-related speeds in a variety of conditions (normal, wet, snow, ice, sand) to gauge the effectiveness of brakes in bringing the PMR to a controlled stop. Brakes

[3] Test setups for tipping are not specified within the standard.

shall be tested to verify they function in the expected temperature range of their intended ODD (another part of ISO 4448 addresses *environmental worthiness*).

NOTE the shyDistance metrics in **Table 2** are intended to ensure that there is sufficient distance so that PMRs are a safe (and comfortable?) distance from other pathway users. By their definition, these values (>> 0) are significantly greater than what is needed for a PMR to avoid a collision (>0).

5.5.1.5 Traction

In addition to braking, it is important that a PMR is able to accelerate in a controlled manner on a variety of surfaces, grades and conditions. Traction tests may be performed in order to measure the minimum friction and maximum grade on which a PMR can safely climb. Additional tests may be performed for water, snow, ice, sand, gravel, and leaf cover to verify a PMR can accelerate safely under these conditions.

NOTE Each of these conditions present different acceleration/braking challenges that are compounded by factors such as weight, load, wheel/tire design, software control, and possibly by wind. It may be that tests such as these are misplaced — for example it may be more appropriate that the orchestration system indicate conditions along the assigned pathway, and require that the fleet operator make the decision regarding safe operation. This approach removes the very difficult problem of an authority designing and executing these tests, which may be better performed in the hands of the device manufacturer. Unfortunately, this places a difficult onus on the orchestration manager to ensure that surface conditions are adequately represented on the orchestration maps.

Something else to consider is the consequences of failure. The failure of a P-Class PMR to have sufficient traction would be less consequential than that of a C or R-Class one.

5.5.1.6 Surface challenges within an ODD

Concerning its mobility effectors (feet, wheels/tires, and tracks), a PMR shall be able to travel in a stable, controlled manner over the full variety of surfaces and surface elements it may encounter within its ODD. PMR operators shall be able to verify a PMR's ability to traverse:

- Surface roughness;
- Surface firmness;
- Cross gradients;
- Surface openings such as grates and storm drain covers;
- The maximum step it is able to mount in low friction conditions;
- Accumulated precipitation within its ODD (rain, snow, ice, leaves, sand)

PMR's mobility effectors shall be sufficiently wide, strong, durable and capable to handle the surface conditions in its intended ODD. These shall be large enough to navigate bumps, crevices, drain grates, potholes, and rail tracks safely.

While mobility effector choices may be offered by a PMR manufacturer, size and capability shall be selected by the fleet operator, and approved within the operating jurisdiction to suit the intended ODD. Within reason, a jurisdiction shall minimize the probability of a PMR being stuck, stranded, or disabled due to a wheel or foot that is too small or has insufficient traction for the pathway it is using.

There is no perfect mobility effector. A jurisdiction shall assess its intended ODD pathways and specify appropriate minimum sizes for fleet registration for use on those ODD(s).

5.5.1.7 Steering/Lateral motion

A PMR shall be able to steer precisely and in a controlled manner in order to avoid both static and dynamic obstacles. Low-speed steering precision and obstacle avoidance at normal travel speeds shall be tested to include the variety of surfaces expected within the ODD of a PMR. These tests are on the same surfaces for which braking (5.5.1.4) and traction (5.5.1.5) tests are made.

5.5.1.8 Reversing travel direction

A PMR shall be able reverse travel direction (U-turn) within a pathway. A PMR shall not be used on a pathway for which it requires more than three direction changes to execute a reversal of travel direction.

NOTE By definition, a PMR able to rotate around its Z-axis is able to execute a reversal of travel direction with a single directional change.

5.5.1.9 Longitudinal string stability

Longitudinal string stability applies to PMR trains. Such a train of PMRs shall not "bunch up" (slinky-effect) to cause inter-PMR spaces smaller than **SDstandBack (Table 2).**

NOTE A PMR train is a string of one or more PMRs following a leader. That leader may be PMR, pedestrian, cyclist, micromobility device, or aerial drone.

NOTE PMR trains longer than two that stand or navigate too closely comprise a safety hazard, a traffic management issue, and an inconvenience to pedestrians. A train of PMRs without inter-robot space sufficient for pedestrians to pass through could cause a pedestrian barrier such as might block a pedestrian leaving a building to enter a sidewalk or might create a barrier at road crossings.

Inter-PMR distances within e-tethered PMR trains shall be internally managed using intra-train distributed control and shall not be under teleoperation via central control. Only the lead vehicle may rely on teleoperation for navigational control.

Inter-PMR distances shall not be managed by physical means such as ropes, chains, wires, rods, or similar.

5.5.1.10 Lateral string stability

Lateral string stability applies to PMR trains (see 5.5.1.9). Such a train of PMRs shall closely follow the pathway initiated by the lead element of that train.

Such a PMR train shall ensure that no follower PMR:

- deviates from the path if the lead PMR changes directions abruptly ("crack-the-whip" effect);
- tilts or sways from side to side, possibly tipping over, especially on rough or uneven terrain, or in strong winds.

Lateral stability among e-tethered robot trains shall be internally managed using intra-train distributed control rather than teleoperated via central control. Only the lead vehicle can rely on teleoperation for navigational control.

The lead robot in a PMR train shall be programmed or teleoperated to travel at an appropriate speed and with changes in direction constrained to avoid lateral instability.[4]

The maximum permitted lateral path deviation of a follower PMR compared to the path taken by the lead PMR shall be 0.5 **SDdynamic (Table 2).**

5.5.2 Location Safety: Perception reliability

A PMR shall be equipped with sensory and decision capabilities vital to detect its surroundings. These components, together with any integrated software and possible human oversight shall facilitate situational awareness and together with the PMRs effectors maintain safe operation.

[4] de Geus, J.A. (2021) Practically string stable, lateral control solution for a homogeneous platoon of vehicles: A Centralized vs Distributed MPC approach.

NOTE This clause is concerned with PMR awareness, responsiveness, redundancy, and recoverability; it is agnostic about the number or types of sensors, the degree of decision-making made on board, and the degree of remote oversight or teleoperation.

A PMR shall have a

- 360° field of view for full-surround awareness including for vandalism behaviours [5]
- minimum visual detection ellipsoid:
  - forward: to anticipate and plan; [6]
  - back: for a full arterial intersection width to be able to reverse, protect or record;
  - side: to anticipate cross traffic.

Some of the reasons that a PMR must have a 360° view are:

- To execute a U-turn a PMR must understand what is behind it to plan and execute. This is especially important if a U-turn will be executed within a crosswalk.
- A PMR that is being followed closely by another entity (pedestrian, jogger, PMR, etc.) shall to be able to provide a warning ("social alarm" sound). An example of this is a robot that may be stopped for a traffic reason, and a distracted pedestrian is about to walk into it from behind.
- A PMR subject to vandalism would be at a disadvantage if it had a rear-facing blind spot.

Sensors adopted for this task shall be deployed to meet the following criteria:

- Sensor units shall continue to function if a PMR is tipped. (UL 3300 7.3)
  - An exception to this is the sensor(s) on the side on which a PMR has fallen
  - The teleoperation system shall correct image orientation to maximize teleoperator comprehension
  - An exception to this is a sensor(s) that is pointing up after being tipped
- Sensors shall be self-checkable or remotely checkable by a teleoperator in real time
- It is desirable that sensors be easily removable and replaceable for rapid on-site repair (UL 3300 8.7)

NOTE Quick-repair sensors are less disruptive than sending a motor vehicle to pick up the PMR and take it to a depot. It will be possible to send a repair person on a bike and snap a new sensor. This would be safer, cleaner, and more efficient.

5.5.3 Location Safety: Localization and Odometry

PMRs shall be able to accurately and reliably determine their location and orientation in any environment within their ODD.

NOTE Odometry is the use of data from motion sensors to estimate change in position over time.

NOTE Localization may include urban canyon conditions for GNSS signals. Such PMRs may employ a variety of GNSS or wireless technologies in order to perform this task.

A PMR shall not become lost and unrecoverable, accepting in the case of a disaster or theft.

NOTE While theft is a business security problem rather than a shared infrastructure safety problem, any factor that contributes to stranded, abandoned, and lost devices—which theft can do—adds a potential risk to bystanders.

[5] This is 2D. Presumably, all will be able to look down to the pavement; would we want to specify a minimum vertical range? Covered below in "blind-spots".

[6] This PMR reports seeing 60m forward: https://www.wevolver.com/specs/starship-technologies-starship-robot

A PMR shall maintain static location accuracy of {500, ±2000} mm, 99% of operating time relative to ground truth. (“First fix” may be worse when using GNSS.)

NOTE The tolerance is higher than the measure because of the first-fix and urban canyon effect

A PMR shall maintain dynamic location accuracy of {150, ±50} mm, 99% of operating time relative to ground truth.

NOTE Dynamic location accuracy is generally better than static location accuracy given the urban canyon effect, and the ability of Kalman filtering on dynamic positioning

A PMR shall have a method to return to a pathway. This may rely on map-matching, remote oversight, or a teleoperator. In the event of failure, a PMR shall execute a Partial Machine Breakdown (para 6.2.1).

NOTE A PMR is expected to relocate itself on its trip map even if it departs from a fixed pathway. For example, if a PMR must leave an assigned pathway to circumnavigate a barrier or wait for an unload or other event to pass, it must be able to find its way back to its assigned pathway. An example of this is an automated wheelchair in an airport that has departed its pathway to allow its passenger to use a bathroom facility.

A PMR shall be able to accept map updates within {24, ±4} hours of their availability. No PMR may operate in public spaces with a map that is more than 24 hours out of date unless a teleoperator is providing oversight.

A PMR shall be able to determine and recover from a map error. In the event it is unable to recover, a PMR shall execute a Partial Machine Breakdown (para 6.2.1).

NOTE A PMR needs to be able to determine when there is a disabling mismatch between its map and what is on the ground and know to recover or request help. A significant map error is likely to require a teleoperator as a backup function, exclusive of automatically downloading a repair which may not always be feasible. *This may be a difficult problem to resolve without false alarms.*

A PMR shall be able to recover from a navigation service failure, such as a GNSS failure. In the event it is unable to recover, a PMR shall execute a Partial Machine Breakdown (para 6.2.1).30, ±

NOTE A navigation service may fail or may provide a significant misreading. A PMR must have a method to recognize, recover, re-synchronize, or be guided by a teleoperator without the benefit of a correctly operating navigation service.

A PMR shall be able to remain safe in the case of telco loss. For the period of telco loss, the PMR shall execute and maintain a Partial Machine Breakdown (para 6.2.1).

NOTE There may be telco blind spots causing PMR connection to its remote operator to fail. The PMR must be able to come to a safe place, and await recovery.

A PMR shall leave bread crumbs every **breadCrumbSeparation** {30, ±10} m. A PMR control center shall acknowledge each of these. If this acknowledgement loop is broken, the PMR shall execute a Partial Machine Breakdown (para 6.2.1), and the PMR control centre shall initiate a PMR recovery procedure.

NOTE A PMR should never be more than **breadCrumbSeparation** m away from its last acknowledge location.

breadCrumbSeparation shall be set so that the disabled PMR will not be waiting further away than the next block-face in the event it is travelling on a sidewalk. A PMR shall complete any road crossing and wait no closer than 3 x SDstandback from any traffic intersection.

ISSUE What happens when a PMR stands in the same location for an extended period of time? It would not report its location. It is possible that a situation could occur such that the device could be out of communication, then moved in a way that the fleet operator would not be able to find it. This is unresolved.

5.5.4 Location Safety: Road crossing considerations

The default behaviour for a PMR at a road crossing shall be the same as the correct and safest behaviour of comparable users sharing the same aspects of the infrastructure at that road crossing such as pedestrians, bicycles, micromobility devices, or motor vehicles. When crossing roadways:

1. PMRs shall access the relevant road crossing signals as do other comparable users
2. PMRs shall obey relevant road crossing rules and signals
3. PMRs shall operate preferring V2I signals, remote oversight or teleoperation
4. PMR road-crossing behaviour shall comply regardless of PMR automation "level"
5. PMRs shall operate conservatively while crossing roadways
6. PMR crosswalk behaviour may be protective of other crosswalk users

5.5.4.1 PMRs shall access the relevant road crossing signals as do other comparable users

A PMR's ADS, remote overseer or teleoperator shall have visual, auditory, or electronic access to all appropriate signs and signals used to control a roadway crossing. This includes analogue formats such as signs, light and auditory (sirens) signals and digital formats such as METR (ISO 24315) and V2I standards SPaT & MAP (ISO 19091, SAE J2735).

A PMR shall have sufficient visual, auditory, and telecommunication subsystems to sense and receive these signals.

A PMR shall have the software or teleoperator connection and rules to correctly interpret and execute safe road crossing according to these signals.

NOTE With respect to systems such as V2I (SPaT & MAP) and METR, it is indeterminate and possibly unsafe to engage two types of automated systems such as automated vehicles and automated robots using an intersection without respecting the same control system signals

5.5.4.2 PMRs shall obey relevant road crossing rules and signals

A PMR shall obey the appropriate crossing signals when crossing a roadway.

PMRs shall obey the appropriate crossing signals either by receiving and interpreting the signals and acting accordingly or by relying on a teleoperator to receive and interpret these signals and to control the PMR accordingly.

In the event a PMR is unable to obey appropriate crossing signals at an intersection, the PMR shall not cross that intersection.

Analog data shall be received via the PMR's sensory systems and interpreted by its ADS or its teleoperator, then transmitted to the PMR's effectors.

Digital data may be received via the PMR communication systems and interpreted by its ADS or received and interpreted by the teleoperator then transmitted to the PMR effectors.

PMRs shall be able to detect emergency sirens with a decision system strongly biased toward false alarms and against misses.

On detection of an emergency siren a PMR shall

- effectively and efficiency exit any road crossing it may currently be in
- not enter or approach a roadway crossing
- withdraw to or remain a minimum of 2 x SDstandback m from any road crossing
- wait until the vehicle generating the siren signal leaves the area before proceeding

In the event of PMR teleoperation, the teleoperator may override these rules, but in doing so shall become fully liable.

5.5.4.3 PMRs shall rely on V2I signals, remote oversight or teleoperation

Whenever possible, a PMR shall use available V2I signals with remote oversight or teleoperation fallback.

In all cases in which a PMR is crossing a roadway or other traffic intersection independently of V2I, or without remote oversight or teleoperator fallback, the PMR shall:

- obey all relevant crossing rules
- yield to cross traffic
- judge crossing opportunities so as not to cause the other traffic to alter its path of travel

In the event of failure to comply with these guides, the fleet operator shall assume all liability.

5.5.4.4 PMR road-crossing behaviour shall comply regardless of PMR automation "level"

A PMR shall comply with appropriate crossing rules including the reception and execution of any V2I messages regardless of the SAE J3016 automation level of the PMRs driving automation system. If the PMR is unable to obtain and/or execute these messages, then those messages shall be mediated via teleoperation.

NOTE This clause implies a system that makes available to the teleoperator human-readable V2I messages (SPaT and MAP) that pertain to the intersection for which the teleoperator is currently operating.

5.5.4.5 PMRs operate conservatively while crossing roadways

When a PMR has a range of opportunities with respect to speed, overtaking other users or PMRs, competing spatially with any other pathway user, changing sides of the crosswalk to gain advantage, etc., the PMR shall choose the most conservative and safest action with respect to all other human users.

If choosing a higher speed, passing another user, or changing sides of the crosswalk means a greater level of safety for other proximate users or the PMR itself (for example clearing a crosswalk toward the end of the pedestrian signal phase without additional risk to any other user, or safely clearing a road crossing in the event of an emergency siren), then the PMR shall take the safest decision in the circumstance.

The determination of this safety criteria shall be embodied in the PMR algorithms or teleoperator operating manual provided it is complying with other suitable behaviour rules provided in other 4448-series clauses.

5.5.4.6 PMR crosswalk behaviour may be protective of other crosswalk users

It is possible for a PMR or its teleoperator to become aware of any proximate or following pedestrians as it uses a roadway crossing such that the PMR is able to calculate that a pedestrian is unlikely to clear the intersection safely, for example during the pedestrian-crossing phase of a signalized intersection. In such cases, a PMR may slow down and may display alarm lights and alarm sounds in order to act as a protective crossing guard on behalf of the slower pedestrian.

NOTE This behaviour is not required by this standard. It creates risk for the PMR, while possibly reducing the risk of the non-involved pedestrian. It is included here as a safety measure for non-involved pedestrians and has the advantage of engendering greater acceptance of PMRs.

5.6 Device Safety

Device Safety pertains to safety regarding the physical self-containment of a PMR in order to keep proximate humans safe. This includes reliable PMR abilities for:

- power safety;
- attachment, tool or cargo (task-related component) safety;
- electronics safety; and
- recovery from failure.

For each subclause, the intention is to ensure that PMR operators and their support systems contain (minimize harm from) any physical failure of a PMR in any circumstance where there may be bystanders. This recognizes that many types of failures hold risks of confusion, discomfort, or harm to human bystanders.

5.6.1 Device Safety: Power safety

PMRs require power comprising elements such as motors, engines, fuel or batteries. Power systems generate heat or have moving parts that produce friction. Such system components may be subject to or generate fire, chemical or other hazards.

PMRs shall have a method to self-detect failures including overheating or fire among its parts, failure of critical sensors, effectors, computation or communication systems that rely on power, its tool or storage elements, and any other reasonably self-detectable, power-related or power-caused failure.

A PMR (or its operator) shall have a method to estimate when it must recharge or refuel so that the probability of being stranded without power is 0.0001. What % should this be set at? This shall include a method that ensures recharging or refuelling.

NOTE These imply the development of a requirements matrix for PMR fleet operator responsibilities for which the operator would carry liability — equivalent to “vehicle user requirements” common in most motor vehicle codes.

NOTE Setting any low-battery safety margin admits that some circumstance could bring a power system below that safety margin. We need the right model to determine that number, since it will differ by circumstance. Setting the number too high would be inefficient. Given that PMRs operate in public spaces without human accompaniment, fleet operators will have to address this problem related to their ODD.

A PMR shall not be permitted to be drained of power during a roadway crossing. This means that a PMR could not commence crossing a roadway without assurance of sufficient power to complete the crossing

A PMR failure self-detection system shall operate by including its status string in the bread crumb message (see clause 5.5.3).

In the case of a PMR shutdown, its execution shall be made safely, swiftly and, where possible, by the PMR locally using one of Partial or Complete Machine Breakdown, 6.2.1 or 0, as appropriate. If this is not possible locally then it shall be executed by the fleet operator or teleoperator. Failing that, there shall be a procedure for the device to be apprehended as quickly and safely as possible. This latter circumstance requires sharing device location with the apprehending authority. (see_____)

In all cases in which PMR safety is compromised, the PMR shall attempt to adopt a **minimal risk condition** that maximizes its distance from surrounding objects (because of potential fire risk) and wait for the circumstance to revert to a safe circumstance or to be rescued.

5.6.1.1 Fire Safety

The most common causes of motor vehicle fires are mechanical and electrical. For PMRs that are commonly battery powered, this may pose a higher risk than mechanical issues. In the case of hazardous (flammable) loads such as a compartment to actively heat its contents, or carry flammable fuels additional risks may be incurred.

PMR fleet operators shall adopt fire standards suitable to the ODD and task for which their PMRs are designed. List fire standards here and in normative references)

5.6.1.2 Battery Safety

PMRs are most commonly powered by batteries and it's important that these batteries do not degrade the safety and reliability of a PMR, particularly concerning the risk of fire and electrocution.

PMRs shall have reliable systems for self-detecting battery fires and the conditions leading to battery fires.

NOTE Battery fire detection systems may involve detecting odours, excessive heat, or battery deformities. (Any others to list here?)

PMRs use shall use UL 2271-certified batteries as certified for electric vehicle applications.

The sheathing or casing of PMR batteries shall be designed to withstand temperatures of CCC degrees Celsius for TTT minutes. Such batteries shall be deployed within PMR housing to withstand freefall drops of MMM meters

5.6.1.3 Engines and Motors

PMRs shall comply with any noise and emissions requirements defined for each pathway segment it traverses.

In the absence of any other guidance, noise or emissions generated by a PMR shall comply with the noise or emissions standards of similar human-operated vehicles in the jurisdiction of operation.

NOTE A jurisdiction may create noise or emissions requirements specific to PMRs. These are beyond the scope of this document.

5.6.1.4 Mechanical Safety

PMRs shall be equipped with fail-safe brakes that engage in the circumstance of a power failure. Stopping shall not rely on means of internal friction or traction or battery-state of charge (UL 3300 8.8).

NOTE This prevents a PMR that loses power on an incline from becoming an uncontrolled projectile.

PMRs shall have a brake release capability, allowing them to be moved by law enforcement personnel.

5.6.2 Device Safety: Task component safety

NOTE PMRs may be equipped with extensions or tools, such as an armature, blade, cooker, grasper, refrigerator, or storage container, an attachment to sweep, mop, spray or vacuum, or a warning flag, etc.

Any PMR extensions or tools shall

- remain within the designed radius of those extensions or tools;
- remain securely attached to the PMR; and
- have an operating radius that is correctly understood by the PMR navigation algorithms.

The physical extent of any PMR extensions or tools shall be included in all shyDistance calculations.

5.6.2.1 Dangerous Goods Storage

Any PMR registration regime shall include an appropriate demand or assurance of compliance with dangerous goods standards.

In the absence of a local standard dangerous goods shall be categorized according to the *2015 UN Recommendations on the Transport of Dangerous Goods: Manual of Tests and Criteria (sixth revised edition).*

PMRs carrying dangerous goods shall only travel where and when they are authorized to do so.

PMRs carrying dangerous goods shall be equipped with containers capable of safely transporting such hazardous goods according to their classification.

A PMR dangerous goods container shall be able to continue to safely store those goods after the PMR is tipped over or after crashing into a solid barrier at two times the top-rated speed for the PMR carrying the hazardous goods.

A PMR shall be able to contain its hazardous load safely for a period of 120 minutes after a crash.

A PMR shall be able to contain its hazardous load safely for a period of 30 minutes after commencement of an onboard fire.

5.6.3 Device Safety: Electronics safety

NOTE PMRs can be expected to function in a variety of temperature and weather conditions.

A PMR's electronic systems shall function within its ODD's environment's expected temperature range and be protected against water and dust.

PMRs shall be subject to appropriate temperature, water and particulate tests related to their ODD.

5.6.3.1 Temperature protection (range)

All critical PMR electronic components shall be certified to operate in temperatures

- 5° C lower than the lowest recorded temperature in the ODD for the most recent five years
- 5° C higher than the highest recorded temperature in the ODD for the most recent five years

5.6.3.2 Ingress protection against dust and water

The enclosure(s) of the electronics, power and energy systems of a PMR shall have a minimum effective IP rating of IP55.

- An IP5x rated enclosure is protected in a dusty environment but is not dust tight; this is suitable for most urban environments, but an IP6x rating would be more suitable in a dust storm.
- An IPx5 rated enclosure is protected from water spray from any direction; this would protect the electronic components in a PMR against heavy rains, splashes from road vehicles, sprays from lawn sprinklers, etc., but it might not protect the electronic components against a strong water jet as might be used for vandalism or other intentional attack.
- An IPx6 rating protects the enclosure from strong water jets.

A PMR to be used for firefighting, enforcement or surveillance shall have a minimum effective IP rating of IP56

A PMR to be used in an ODD that might be subjected to dust storms shall have a minimum effective IP rating of IP6X

A PMR to be used for firefighting, enforcement or surveillance in an ODD that might be subjected to dust storms shall have a the highest effective IP rating — IP66.

A PMR a fleet operator shall always select a higher IP rating if it reduces the risk of a PMR failing while crossing a traffic roadway.

5.6.4 Device Safety: Failure recovery systems

NOTE To recover from a failure means that a PMR takes the best possible course of action available to it in the circumstance. It does not imply self-repair. That means that some PMRs will only be able to report failure and possibly shut down, while others may exhibit some self-recovery behaviors.

A PMR shall be able to recover from (respond to) any failure in a way that minimizes the probability of harming humans, pets, property, or itself, in that order.

A PMR shall be able to correctly identify and report the type of failure it has experienced in near real time, including:

- failure in the power system
- a vandalism-induced failure
- a failure in its attached tool
- a fire on board or in any part
- a failure in its navigation capability, or
- a mechanical failure in the device (platform).

A PMR failure shall be distinguishable by the PMR, or its remote overseer without a human agent physically present at the PMR.

NOTE This ability is critical to minimize contingent harm and recovery cost.

A PMR shall be able to determine who to notify in the event of a failure.

NOTE For example: should a PMR notify only its remote operator or both its remote operator and the relevant emergency authority? A PMR with a low battery condition needs only to inform its remote operator, while a PMR that has been disabled in a crosswalk needs to notify both its operator and an emergency authority. In the case where an independent orchestration authority is scheduling multiple fleets, it may be necessary to notify the orchestration authority for scheduling reasons.

A PMR shall be able to correctly identify any circumstance in which it must execute either a Partial or Complete Machine Breakdown procedure. It shall then execute that procedure.

A PMR shall be able to correctly identify any circumstance in which it must move away from its current position, or change course significantly, or request to be rerouted.

NOTE In all cases, it is sufficient for a human teleoperator to detect, identify, and resolve all breakdown procedures, provided detection and identification can be done in near real time.

5.7 Human Interaction Safety

Human Interaction Safety pertains to safety regarding any form of interaction with bystanders and operations and enforcement personnel. This includes reliable PMR abilities to:

- communicate reliably with its fleet management centre;
- communicate its intentions or circumstances to bystanders;
- cooperate/comply in emergency circumstances; and
- cooperate/comply in seizure circumstances.

For each subclause, the intention is to ensure that PMRs are able to interact safely with humans that are proximate or are managing them.

5.7.1 Human Interaction Safety: Communication Safety

This clause relates to communication to and from a PMR, such that the PMR, its operations, and any human involved or proximate is safe, that those communications are transmitted correctly, and with an acceptable lag. Any communication that is delayed, lost, altered, blocked, or otherwise deflected from its purpose, is an unsafe communication.

A PMR shall be able to signal local emergency services whenever an emergency signal is justified. This signal must have near-zero lag, and be secure from cyber-attack. The same signal shall be forwarded concurrently to the PMR's remote operator.

NOTE It may be desirable for an emergency signal to be routed through the PMR operator to local emergency services, but this shall not incorporate lag or error. Hence, this approach may add an additional risk.

NOTE We may need a set of universal emergency codes. This would start with existing codes used for motor vehicle emergencies. Where to source this?

A connection between PMR and remote operator shall be maintained at all times and shall be secure from cyber-attack. In the event that this connection is interrupted for more than __5?__ secs, such as in a blind spot, the PMR shall execute a **Partial Machine Breakdown** procedure.

In the event of a detected or suspected cyber-attack, whether detected or suspected at the PMR, or by its remote operator, a PMR shall execute a **Complete Machine Breakdown** procedure.

NOTE It is reasonable, given an agreement between a PMR and its remote operator that a PMR may continuously operate in a telecommunications blind spot for a pre-agreed period of time or geography. This time should be very short or geography limited. The decision to tolerate such an interruption, while continuing to operate implies liability shared between the PMR fleet operator and the telecommunications operator. A regulator may impose limitations on this. This matter is out of scope for this document.

A PMR shall not commence a road crossing if the communication between remote operator and PMR is not operating, or if there is reason to suspect uncertainty during the crossing.

In the event of loss of communication beyond __10?__ secs, or beyond other pre-agreed time between a remote operator and a PMR shall trigger the execution of a machine breakdown procedure and the appropriate recovery procedure. Refer to bread crumbs for PMR recovery (see clause 5.5.3).

5.7.1.1 Communication with Teleoperator

Fleet operators shall use reliable technologies to communicate with their PMR fleet. Each PMR shall be guaranteed a communications lag of less than 100ms.

PMR communications shall be tested to verify communication between PMR and operator is not interrupted, except in the case of blind-spots of constrained duration or outright telecommunication failure.

Communication systems shall be near failsafe. This may be achieved with resilience such as may be offered by redundancy.

At scale, orchestration providers will select telecommunications providers to serve each jurisdiction.

NOTE There may be reasons to use or not use the same telecommunications provider for orchestration as for teleoperation. That decision is out of scope for this document.

5.7.1.2 Data Transmission Protection

Data protection and resistance to cyberattack are to be addressed in another part of the 4448 series.

5.7.1.3 Help Button??

A PMR shall have a help button in the event there is an issue with the PMR such that it needs to be immobilised. The height of a help button shall be between 0.75 m and 1.5m above ground level. It shall be clearly legible (50mm to 80mm in diameter, red, clearly visible and understandable). The button may have a protective casing to preventing mistaken or accidental usage. The effectiveness of the Help Button system shall be tested.

NOTE This may be too prescriptive, and this needs careful consideration for **false alarms**... 50-80mm seems large for a small PMR

+NOTE Help buttons or emergency buttons on a PMR are known to be a problem. They attract pranks, they will require penalties for misuse, they are demanded by statute in some countries (Denmark, for example, specifies a size and configuration that may be unsuitable for many PMRs).

+NOTE Originally designed as emergency shut off buttons in industrial environments to be used by a machine operator, on PMRs they would be designed as a help or shut off button that could be triggered by any bystander in the same way that a passenger might pull the emergency brake on a train. It is not be enough simply to talk about the size and position of such a button; we must consider its abuse. The most egregious example would be a prank in which someone might strike the help button while passing a PMR in a busy crosswalk, possibly causing the robot to simply halt in the middle of a road crossing.

+NOTE We must consider is they are easy to see/find; vision disabled; older pedestrian using cane to hit the button; to hit easily and get out of way (fear component); AND not easy to hit in error (recessed?), etc. Emergency buttons provide a lot of design and human complexity.) We need to consider the safety risk to a human required to physically touch a machine which behaviour may not be fully understood or may not be safe. I know that a physical emergency shut down may be required, but this is a mobile device. How do we keep proximate pedestrians safe in the case of a rogue device?

+NOTE Before we specify a help or emergency button, it will be important to ensure that we introduce no unintended consequences. This single matter is so important, and its unintended consequences so insidious that it may deserves a standalone part. Consider also that the problem of a shut off button on a social robot would be highly related, and possibly with even more nuances. Perhaps: "Standard for Halting and Securing PMRs and Social Robots.

5.7.2 Human Interaction Safety: PMR-to-Human communication reliability

PMRs are expected to deploy a variety of visual, auditory and gestural cues to indicate their actions and intentions to proximate humans in a shared public pathway. This clause describes the minimum failsafe capability of the equipment used to generate light, sound, haptic and gestural signals.

Note Some observers have suggested the use of a screen to display lights, pointing out that a screen could allow deaf persons to read or be used to show facial expressions for an improved pedestrian social experience or for the cognitively challenged. The screen approach has been tried frequently for personal delivery devices. There are four reasons the standard does not require or rely on screens. [1] the light emitted from a PMR for communicating its intentions must be seen from a distance at any angle (360°) around the device, [2] many PMR circumstances cannot safely wait to be within the reading range or require a bystander to pause and read before communicating their intentions, [3] any PMR operating in poor weather (e.g., snow) likely would be unable to broadcast from a screen, and [4] the standard must remain necessary and sufficient. Screens may be used but are not be required by the standard.

Any sound emanating from a PMR shall be heard {5, ±0.5}m from the center of a PMR, by a bystander within a normal range of hearing including one aided by personal hearing aids. Any bystander for whom this is not true may need to rely on other PMR communication methods such as light, gestural, or haptic signals.

Any decibel level selected for audible sound signals must ascertain that the level used would be appropriate to then-current ambient sound level. This means that the sound must be audible within the required distance in noisy environments, but must not be excessively loud in quiet environments.

Note more here about these limits from 4448-x

Any light emanating from a PMR shall be visible {20, ±2}m from the center of a PMR, by a bystander with normal vision, wearing their normal corrective lenses. Any bystander for whom this is not true may need to rely on other PMR communication methods such as sound, gestural, or haptic signals.

Any test for the visibility of light signals must assume that the light levels generated would be appropriate to then-current ambient light level. This means that the light must be seen within the required distance in very bright environments, but must not be excessively bright in darker environments, in order to avoid visual obstruction of other environmental elements.

Any gestural display from a PMR shall be visible (interpretable) {5, ±0.5}m distant from the center of the PMR, by a bystander with normal (including corrected) vision and who is looking in the direction of the PMR.

Any gestural display from a PMR shall be visible (interpretable) at a one to three m height range (±0.2m) form the center of the PMR. This assumes that a gestural display can be viewed and understood by a person sitting low in a wheelchair, or a person sitting very high in the cab of a heavy goods vehicle.

NOTE Gestural displays assume that the human viewing it has a normal range of (corrected) sight, and that such person is visually focussed on the PMR.

Any haptic signal from a PMR shall be receivable {10, ±1}m from the center of the PMR.

NOTE It is assumed that haptic signals would be broadcast locally to smart phone apps for those who require these signals, such as deafblind pedestrians.

NOTE It is also possible to deliver haptic signals using very low frequency sound. Since these signals travel further than high frequency sounds, the required distance is very short. Low frequency sound can be harmful even to people who do not hear it, and can be distressing to a portion of the population. Hence, this standard recommends against this approach and recommends delivering haptic signals via mobile phone apps.

5.7.2.1 Visual Signal Components

PMRs shall use lights and reflectors to be visible to other users, aid the detection capability of its cameras, and signal its actions.

A PMR shall have these visual signal devices, at a minimum:

- Brake lights;
- Turn signal lights;
- Flag (for short-stature PMRs);
- Illumination visible from all directions;
- Reflectors visible in any directions; and
- Any lights required for PMR-to-bystander communication

NOTE Uniform visibility distances are defined for footways, bikeways, and roadways, based on the stopping distance of bicycles in all circumstances. This is because stopping distances for bicycles are longer than either motor vehicles or pedestrians. The prescribed differences are modulated by the expected reasonable upper speed of bicycles on each of these three pathways, then tripled as a safety margin to account for slow response time, faulty brakes, and human (including teleoperator) distraction.

Table 3: Requirements for each type of visual signal device

Capability	Measure	Tolerance	Comment
Brake light visibility[7]	3 x stopping distance of bicycle	10%	Brightness: Must be visible in bright sunlight, and in fog. Note that the brightness of PMR brake lights could limit the ability to operate in some fog circumstances. (See bike rules)
Brake light visibility footway	25m	10%	See stopping distance for bicycles as the critical operating constraint. [8] Assume ambient traffic is 15kph
Brake light visibility bikeway	60m	10%	Stopping distance for bicycles. Assume ambient traffic is 25 kph
Brake light visibility roadway (posted 50kph)	120m	10%	Stopping distance for bicycles. Assume ambient traffic is 40 kph
Turn signal lights (footway, bikeway, roadway)	Same as brake lights	10%	Turn signal brightness is subject to all of the same issues as brake light visibility.
Flag[9]	Same as brake	10%	The purpose of a flag is for a PMR to be seen among other vehicles or among other pedestrians and to increase the likelihood of capturing the visual attention of proximate, distracted humans. A flag cannot be relied on for a motor vehicle to see a PMR at a distance on a roadway — that is one purpose of lights on a PMR. PMR safety at intersections must consider motor vehicles turning and crossing crosswalks. Consider the visibility of a PMR in the side- or rear-view mirror of a motor vehicle making a right turn-on-red. This is an additional, critical value for flags.
Illumination visible from all directions	360°	0	This is unrelated to distance. Rather, there is no angle at which any required illumination would be invisible. E.g., if illumination is used to transmit a PMR-to-bystander signal, then that signal must be visible, regardless of the bystander's angle of observation.

7 https://mrstewartsdriversed.weebly.com/uploads/1/5/5/4/15543134/distances_you_should_know.pdf

8 Stopping distances (including human reaction time) for bicycles are longer than for motor vehicles. It is possible for bicycles to be following robots in all three environments (footway, bikeway, roadway) https://bicycles.stackexchange.com/questions/15572/what-is-the-braking-stopping-distance-for-bicycles

9 Total height? Size of flag? Colour? Illumination (active light emission)?

Capability	Measure	Tolerance	Comment
Reflectors visible from all directions	360°	0	This is unrelated to distance. It simply indicates there is no angle at which any required illumination would be invisible. E.g., if reflectors are required for passive-visibility at night, then those reflectors must be visible, regardless of the bystander's angle of observation. Note that reflectors require that the human observing a PMR must be emitting light. This corresponds to the headlamps on a bicycle or motor vehicle. This applies to a pedestrian if they were carrying a light-emitting device or have an appropriate nearby emitter. A related, typical regulatory description is: *"a red reflector that has a diameter of at least 2 inches of surface area on the rear so mounted and maintained as to be visible from all distances from 50 to 500 feet to the rear when directly in front of lawful upper beams of headlamps on a motor vehicle."*
Headlights (Head lamps)	Visible from front 60° to both left and right of direction of travel	15°	Headlights are intended to illuminate the pathway for the PMR, and to ensure the PMR is visible from a distance by others who are approaching. Headlights are signalling distance and, by inference, speed.

5.7.2.2 Auditory Signal Components

Auditory signals shall be used by a PMR as one means to indicate its presence, intentions, and actions to bystanders on or near the PMR's pathway. It is important that these auditory signals are loud enough to be heard by bysyanders over the current ambient noise level but not so loud as to be a nuisance or harmful.

The loudness and spectrum, and therefore human auditability, of auditory signal to be used by a PMR shall be:

- Clearly audible for normal (?) human hearing in all operating ambient noise conditions (up to 85 dB) (?) from a distance of 10 m (?)
    - This range shall be 40 m (?) in the event of an emergency as legally determined in the jurisdiction in which the PMR is operating.
    - In the case of emergency or security PMRs, the range and loudness of auditory signals may exceed these levels with guidance from the authority within a security jurisdiction.
    - Care shall be taken not to harm bystanders by exceeding standard sound volumes
    - Care shall be taken not to alarm bystanders by using a sharp attack[10]

[10] This needs to be defined. Refer to a standard for other emergency sounds.

  - In all cases, the loudness of auditory signals shall not exceed 120 dB.[11]

- Harmless to normal human hearing from a distance of 1 m.
  - Sound volume shall not be set higher than 85 dB,[12] unless in a setting wherein proximate humans are required to wear hearing protection.
- A sound may be repeated two or more times in any circumstance in which ambient noise conditions vary and may occlude sound.
  - A PMR may repeat an auditory message up to three times in succession in the event it does not understand the ambient noise conditions.
- A sound may be repeated continuously once every 10 seconds, during critical and emergency circumstances.
  - It is not a critical circumstance to repeat the signal for “I apologize” or “I am waiting here”
  - It is a critical circumstance to repeat the signal for “I have a failure, please call for help”
  - It is an emergency circumstance to repeat a signal such as “I have a fire” or “I see an injured person”
- The minimum loudness shall be 12-15 dB (?) [13] above the current ambient level.
- The maximum loudness level shall be the minimum of 20 dB[14] above current ambient or 110 dB[15] whichever is lower. (120 is damage threshold.)
- The default loudness level of 70 dB [?] shall be used for intention-signalling in the absence of ambient noise measurement.[16]
  - This level carries the risks of being inaudible in louder-than-average urban locations
  - This level carries the risks of startling a human in a quiet environment, which shall be mediated by using a gentle attack of sound warning.

The **sound spectrum** used to project the auditory signal used by a PMR shall be _____.[17]

[11] It will be possible for a PMR to be weaponized with sounds well above 120dB. How can this possibility be minimized? This should be handled in the certification, licensing and enforcement.

[12] 85 dB is the level above which hearing protection is recommended.

[13] Sanders, M. and McCormick, E. (1993). Human Factors in Engineering and Design (7th Ed.). McGraw Hill, Inc. "... A minimum level of 15 dB above masked threshold to ensure detectability and a maximum of 25 dB above the masked threshold to guard against annoyance and disruption." — ("masked threshold"=ambient noise) Additional source for audibility above ambient? https://www.engineeringtoolbox.com/voice-level-d_938.html

[14] Lee, J., Wickens, C., Liu, Y. and Boyle, L. (2017). Designing for People: An Introduction to Human Factors Engineering. CreateSpace, Charlston, SC.
"... The alarm should be set at least 15 dB above the noise level, and to guarantee detection, set at 30dB above the noise level."

[15] 120 dB is the level above which hearing can be damaged.

[16] A lower level shall be determined for “presence signalling.”

[17] This needs to be identified and a reference provided. A default could match the spectrum of the normal human ear, but I think this is wrong (Ask Michael Clamann)

A PMR shall not operate in a location known to experience an ambient noise level above 110 dB (excepting emergency sirens). This can be waived by a jurisdictional authority with appropriate safety precautions.

The method for measuring ambient noise shall provide measurements that are accurate within 3 dB [?] 95% during the time a PMR uses that measurement to set its sound loudness in real time. A PMR may use a real time sensor to determine the current, immediate ambient noise level, or the PMR may use an historical map by location and time, but that map must be accurate within 3 dB [?] 95% at the time of its application.

5.7.3 Human Interaction Safety: Emergency compliance systems

This clause assumes that a PMR fleet is operating in a defined ODD under the authority of an appropriate governmental body which shall have reserved to itself the authority to direct any PMR or PMR fleets away from any emergency incident or area without notice. This clause relates to occasions on which an authority requires one of more PMRs to leave or avoid a defined pathway or area.

There shall be a protocol agreed between the governmental authority (licensing authority), and PMR fleet operator(s) such that an emergency instruction can be forwarded to, then received and acted on, by these fleet operator(s). Such protocols are planned for other parts of this series.

Any PMR emergency instruction including its spatial and temporal time constraints shall be delivered to the affected PMR(s) by direct delivery to each PMR fleet operator, followed by immediate onward distribution to its affected PMRs.

This shall be done so that all affected PMRs receive the appropriate instruction within 120 secs [?] of initiation by the authority, and all affected PMRs shall respond within 180 secs [?] of initiation.

No PMR under emergency instruction shall exceed any behavioural rule, except to proceed to its instructed destination, and enter its instructed state.

NOTE As an example, a PMR that is in the process of crossing a roadway, shall continue to complete that action, within the speed constraints provided, before beginning to execute the emergency instruction. It is possible that after completing that road crossing the emergency instruction requires the PMR to recross the same roadway. Such a PMR shall not execute a U-turn in the middle of a roadway crossing solely to begin an emergency evacuation.

In the event that a PMR does not comply with an emergency instruction, that PMR shall be subject to seizure by the governing authority. In that case, clause 5.7.4 shall govern the activity of seizure.

5.7.4 Human Interaction Safety: Seizure compliance systems

This clause assumes that a PMR fleet is operating under the authority of an appropriate governmental body which shall have the authority to commandeer or seize a PMR that is out of compliance in a way that compromises the safety of bystanders or property.

A jurisdiction shall have authorized personnel that may require a PMR to leave or avoid an area, disturbance, event, incident, pathway. etc.

Any required compliance actions that cannot be performed autonomously shall be caused to be performed or executed by a teleoperator.

Failing the ability or willingness of a teleoperator to execute any lawfully demanded action, such as an enforcement or emergency authority demanding a PMR in a public pathway to halt, change course, shut down, evacuate from or to a location, follow emergency personnel, unlock a secure compartment, or surrender to emergency personnel such PMR may be seized. This assumes that all agreed

communications to the PMR or to its teleoperator have failed and the PMR must be disabled, commandeered and or seized.

Regardless of whatever person, machine or communication provides a direction, in the event that a PMR disobeys or disregards a lawful direction, the governmental authority shall have the legal right and an appropriate method, whether physical or electronic, to:

- force the PMR to comply;
- redirect the movement of the PMR;
- constrain the movement of the PMR;
- seize the PMR;
- impound the PMR;
- disrupt the operation of the PMR;
- open any PMR storage bay;
- collect a fee for the return of the PMR to its owner; or
- retain the PMR as evidence in a crash or for a crime.

It is outside of the scope of this part of this standard to describe how any of these actions shall be taken. Rather, these actions shall be defined by the governing authority, understood by the fleet operator and be listed as part of the operating licensing arrangement.

It shall be up to the governing authority to arrange any necessary regulations, train its staff, to have the appropriate equipment, and have the requisite storage arrangements for any of these outcomes.

If the governing authority wishes to reserve the right to retain the property of a fleet operator beyond a reasonable period of time, that right shall be described in the licensing agreement.

6 Safety-related emergency procedures

This clause describes what a PMR must do when operating within its ODD and without immediate teleoperator oversight. This is expressly for the circumstance in which a teleoperator is in a standby state and not currently attentive. This may be considered behaviourally equivalent to remote readiness SAE J3016 “Level 4.”

- self-detection of mishap;
- procedure during mishap;
- procedures during emergency

6.1 Classes of emergencies/breakdowns

A breakdown is an event from which a PMR cannot self-determine a resolution within a short wait as defined by its operating software (these wait purposes may need more definition), unless there is a change in the event.

- Fire;
- Machine fail (includes drained battery);
- Major vandalism;
- Seizure (police, theft, vandal);
- Telecommunication failure;
- Trapped.

NOTE Resisting seizure, theft, or vandalism risks increased harm to a PMR. Resisting seizure risks collateral harm to proximate humans, depending on the nature of the resistance. It may be appropriate a PMR to record the event of a seizure for later analysis. A PMR decision to “play dead” which would mean to simply lock down and go silent, or to unlock and go silent (protect any event recording, in either case).

NOTE A PMR under seizure in a public space (regardless of the reason) shall not resist. To resist a police seizure would likely become equivalent to “resisting arrest.” In the case of a police seizure, it might be better to unlock. In the case of theft or vandalism, it might be better to lock. The case of theft is less certain because a lockdown might precipitate a break-in, which would likely damage the PMR, but it would also prevent the loss of property in the event of less determined thieves. In all cases, the state of the PMR must consider safety of any humans near or touching the device, regardless of nature of the intentions of such humans.

Table 4: Permitted time delays until a PMR must raise an alarm depending on the reason for the alarm.

Event	Response	Tolerance	Comment
Machine fail	3 sec	1 sec	This assumes that the PMR is able to self-detect a failure. This applies to battery or mechanical failures in the PMR itself, as well as wheel stuck or tipping mishaps.
Major vandalism	3 sec	1 sec	This is equivalent to a machine fail, except for a criminal involvement. It may include circumstances in which the PMR is no longer able to move under its own power or navigational capability, including theft.
Minor vandalism	10 sec	2 sec	The extra time is for certainty of the necessity to declare a breakdown. Include circumstances in which a PMR is physically able to continue its task, but may have to wait for investigation.
Fire	1 sec	1 sec	Fire detection circuits should be very rapid.
Seizure	0 sec	0 sec	The PMR should be aware that seizure is imminent. It is possible for the response time to be negative.
Telecom failure	n/a		This failure makes PMR response impossible until failure resolution. In the case of a communications failure, the only thing the PMR can do is retry. Hence, the lag for that is given by the bread crumb algorithm (**Error! Reference s ource not found.**), so it falls on the teleoperator to decide recovery, rather than the PMR.

6.2 Machine Breakdowns

There is a distinction between a Partial Breakdown and a Complete Breakdown. A Partial Breakdown means a PMR has detected an issue but is still functional, at least for a short period of time (This is analogous to a vehicle engine overheating while being close to a repair depot and being able to drive slowly to get there). A Complete Breakdown is a breakdown that renders a PMR currently inoperable, such as being struck by a motor vehicle or being tipped over.

6.2.1 Partial Machine Breakdown

In the case of a Partial Breakdown, a PMR has detected a breakdown that has rendered it temporarily unsafe to continue unimpeded operation or will shortly disable it. In this case, the PMR shall:

1. Immediately report the issue, location, and cause to its fleet manager, orchestration manager, or both;

2. Move a short safe distance to a place that would minimize traffic disruption. That might be a generous space at the edge of a sidewalk, or it may be to exit a bike lane to move onto the pedestrian pavement. This is situation specific, and assumes remote oversight or teleoperation.
3. Position itself as closely as possible to the edge of the pathway (walkway, bikeway, roadway), choosing the side and a spot that causes the least disruption of other traffic (relying, when necessary, on teleoperator guidance or takeover)
4. Issue any necessary communication (sound, light or gesture) to bystanders

Minimizing bystander traffic disruption may be different in each of walkway, bikeway, or roadway. Fleet operators shall develop clear instructions for teleoperators to handle each case.

6.2.2 Complete Machine Breakdown

In the case of a Complete Breakdown, a PMR has detected a breakdown that has rendered it unable or unsafe to move. In this case, the PMR shall:

1. Immediately report the issue, location and cause to its fleet manager, orchestration manager, or both;
2. The fleet operator shall commence emergency notice and recovery procedures according to appropriate circumstances;
3. The PMR shall report any emergency notice for which it is responsible according to its fleet licensing agreement.

Minimizing bystander traffic disruption may be different in each of walkway, bikeway, or roadway. Fleet operators shall develop clear instructions for teleoperators to handle each case.

NOTE In the case of a complete breakdown it is possible that the communication system will be inoperable. In this case, the fleet operator will rely on the bread crumb system (clause 5.5.3) to locate the failed PMR.

6.2.3 Journey Data Recorder (JDR)

A journey data recorder ensures the capture of specific PMR behaviours, warnings, and circumstances. This is useful for understanding crashes, potential incidents, complaints from pedestrians or others, undesired events, or unintended spatial behaviours (for example, those related to shy-distance infractions).

It is recommended that a commercial (non-experimental) PMR fleet not be licensed without a minimum, standardized JDR. If a JDR is required by the licensing authority, every such licensed PMR shall have:

- a correctly operating JDR
- a 1Hz self-inspection circuit to check that its JDR is operating correctly and that its data is being captured
- confirmation of correct operation included in its bread crumb message (clause 5.5.3)

6.2.4 Recovery of a PMR

Recovery of a PMR has several meanings. Resolution of a breakdown may take any of these principal forms:

- recovery of telecommunication failure or error;
- over-the-air update of software or map;
- use of PMR-to-human communication to recover from vandalism;
- use of PMR-to-human communication to recover by asking a proximate human to help;
- send an emergency service to extinguish a fire;
- send an emergency service to seize a PMR;
- send a human to repair a PMR;

- send a method to remove the PMR to another location;

NOTE A full list of coded breakdown messages is required here.

A PMR fleet shall have a documented method:

- to identify and execute each of these methods of resolution;
- to escalate the procedures the fleet operator will execute for each breakdown;
- for procedures expected from the governing jurisdiction when emergency services are required;
- to record the time and place of initiation of the event;
- to record the time and place of resolution.

The fleet operator shall make the following decisions by way of teleoperator instruction, ADS code, or both:

- when to declare a breakdown;
- the precise definition of the initiation of a breakdown;
- which resolution to assign to a breakdown;
- when and who to contact regarding emergency services.

A jurisdiction licensing PMRs or PMR fleet(s) shall request and negotiate this documented method as a component of its due care in the licensing process.

NOTE Not every breakdown implies a simple, single recovery approach. For example, the "use of PMR-to-human communication" may be tried, but may fail. Hence, this might still require the fleet operator to "send a human to make a repair."

6.3 Vandalism

A PMR shall be permitted, for purposes of self-protection (and the owner's property protection), to record and retain acts of vandalism relative to its security of property including cargo. Such data as may be used to assess damages, support arrest, lay charges, or as evidence in prosecution shall be gathered, stored, protected, surrendered, and destroyed according to the locally prevailing laws regarding captured data in public spaces.

A PMR shall be able to perceive its surroundings for navigation purposes (ISO 4448-6). This almost certainly includes transient image capture, even in the case of full teleoperation (SAE J3016, Level 1). In addition to its value for navigation, proof-of-task-completion, monitoring, inspecting, surveillance, or insurance subrogation, image capture has value in deflecting, recording, and prosecuting vandalism. The rules for data retention for purposes of recording vandalism should be defined and agreed between the licensing authority and the fleet operator. Such agreements shall provide a reasonable ability to defend against vandalism, but shall also regard applicable data and privacy laws.

According to the determination of locally applicable rules, the fleet operator shall arrange for PMR data retention. If such rules are not otherwise pre-agreed, a PMR fleet operator shall be able to defend itself from vandalism using any data captured leading up to, during, and immediately following acts of vandalism.

NOTE Most PMR imaging systems, especially considering ISO 44806 (journey planning sufficiency), will capture unrelated activity from some distance. Specifically, it is possible to record criminal activity unrelated to the PMR merely because the PMRs cameras were facing in that direction. In this case, locally-prevailing laws regarding data captured by security systems installed in public spaces shall apply.

NOTE There almost always exist applicable privacy laws including matters of data retention appropriate to the operating jurisdiction. Local agreements should endeavour to use these wherever possible and refrain from adding new rules to this complex issue.

NOTE A PMR may be equipped with a capability to announce its intention to record an act of vandalism. Unless such an announcement is proscribed in the licensing agreement or other local legislation, the PMR shall make such announcement in order to reduce the probability of vandalism, and to increase the weight of evidence, if vandalism proceeds.

6.3.1 Minor vandalism

Minor vandalism occurs when any damage inflicted on the PMR does not hinder the PMR's ability to continue its task. This includes temporarily interfering with the progress of a PMR, e.g., a prank, riding on a PMR, depositing human or animal waste on a PMR, inappropriately placing a barrier in front of a PMR, attaching foreign objects to a PMR (such as a sign), etc.

In this case, a PMR shall:

- report the incident to its fleet operator and orchestration manager (if one);
- be permitted to retain any recording of the incident including a recording of proximate, involved humans;
- continue with its travel plan and task.

6.3.2 Major vandalism

Major vandalism a machine breakdown. In this case, a PMR shall follow the appropriate procedure for partial machine breakdown (6.2.1) or complete machine breakdown (6.2.2).

6.4 Fire

Three types of fire are identified in order to distinguish between methods of safe handling and of privacy and property (in the case of a fire of contents):

- Electrical
- Battery
- Contents

Containment: how the fire is extinguished. This should follow guidelines for the type of fire.

Removal: how, and how quickly the subject PMR is to be removed from public space (this is advisory only, and dependent on local bylaws and capabilities)

Reporting: what is to be reported, to whom, and how quickly. The standard sets a minimum. The local jurisdiction might add more.

6.4.1 Electrical Fire

Containment should follow the guideline for extinguishing fire in an automotive electrical system. (ref.)

Removal: a disabled PMR must be removed within 30 [?] minutes after a fire is extinguished.

Reporting: If a PMR experiences an electrical fire, it shall report it to its fleet operator and orchestration manager and execute any further procedure as defined in its licensing agreement.

6.4.2 Battery Fire

Battery fires pose a unique challenge as they can potentially be dangerous and tend to be more difficult to extinguish.

Containment should follow the guideline for extinguishing fire in an automotive battery system. (ref.)

Removal: a disabled PMR must be removed within 30 [?] minutes after a fire is extinguished. Care shall be taken during removal related to any hazardous aspect of the damaged battery. The fleet operator or public authority shall follow whatever safety guidelines are locally applicable for handling and disposing such batteries.

Reporting: If a PMR experiences a battery fire, it shall report this to its fleet operator and orchestration manager and execute any further procedure as defined in its licensing agreement. It shall signal to any public and emergency responders the signal reserved for battery fires. Emergency responders shall be trained how to identify this signal.

6.4.3 Contents Fire

Containment: how the fire is extinguished. This should follow the guideline for xxx (ref)

Removal: if the contents are not hazardous goods, removal would be the same as any other salvage. If the contents are hazardous, then removal must follow the guidelines for the type of hazardous goods represented. (ref.)

Reporting: If a PMR experiences a contents fire, it shall report it to its fleet operator and orchestration manager. Summary reports, filed later, should contain concerns regarding property rights to the contents.

6.4.4 Multiple source fire

Any type of fire (electrical, battery or contents) might quickly evolve into one or the other two. It is not sufficient to expect a sole class of fire. In the case of a multiple-source fire, containment, removal, and reporting shall follow this priority:

- Hazardous contents
- Battery
- Electrical
- Non-hazardous contents

6.5 Stop and Seizure

This clause is included to ensure that there are safe methods to halt and take control of a PMR that is operating illegally or out of the control of the fleet operator. These methods will involve the law-enforcement system operating in or near the jurisdiction of the PMR fleet's ODD.

As with motor vehicles, there may be occasions such that law enforcement is required to stop and/or seize (Impound) a PMR. There shall be a documented method for law enforcement to carry out this task in a secure and reliable fashion. Such methods require awareness, training and equipment readiness.

One or more of the following shall be mandatory:

- Be able to demand that the assigned teleoperator cause a PMR to halt by way of hand gesture, observed by the teleoperator through the PMR's vision system
- Be able to demand that the assigned teleoperator cause the PMR to halt by way of an agreed telecommunications method. This requires:
    - A unique device ID to be clearly visible on at least 2 surfaces of the body of the PMR;
    - a direct, reliable telecommunication connection to the teleoperator
- Have a physical or electro-mechanical backup method that enables law-enforcement officers to immobilize a PMR. A method to immobilize a PMR shall:
    - maximize the safety of any bystander
    - maximize the safety of any involved law-enforcement personnel

Optional approaches to the mandatory requirement:

- A method to immobilize a PMR should:
  - deploy a way to halt the PMR's means of locomotion (wheels or legs)
  - choose a way to cause the least damage to the PMR
  - be highly portable for transportation to the scene
- A method to immobilize a PMR could:
  - Use blocks or a snare for the wheels or legs
  - Use a blanket to blind the PMR visual sensors
  - Tip it over (if it is wheeled) (that will likely cause unnecessary damage)

NOTE Any of these solutions could be defeated by an ambulatory PMR, especially one with arms. This will be inadequate in a few years.

NOTE Many legged robots will be self-balancing, making it difficult to tip them over. Tipping should only be used as a last resort.

6.5.1 Emergency Disabling/Unlocking Procedure

There shall be a formal procedure, based on the property and privacy laws of the local jurisdiction in which a PMR is operating, to safely cause a PMR to halt, remain stopped, and to shut down or disengage its source of power for locomotion.

A full power shutdown shall not be required except for reasons of safety such as fire, as power may be required for communication or temperature control of tools or cargo contents.

This jurisdiction-relevant procedure shall:

- Include disabling, unlocking, opening, breaking into, inspecting, moving, and removing contents;
- Include seizing, relocating, fining, impounding, damage description, and cost assessment;
- Include a reporting procedure;
- Be clearly written in the language of the local authority;
- Be incorporated into the training program for the relevant enforcement and emergency officers;
- Be made available to all PMR operators within the relevant jurisdiction to understand the rights and process of seizure and entry permitted to the local public safety and enforcement authority.

6.5.2 Data Transmission Requirements (this needs external advice)

Should this be included under Stop and Seizure? Is it a requirement for emergency commands and messaging to the teleoperator? I.e., messages from a short-range communication device? I don't like to rely on a lot of technology for these emergency situations, especially if the source for the emergency is criminal, in which case the technology would be easy to defeat.

6.6 Communication Breakdown

A breakdown in communication between a PMR and its fleet operator (including its teleoperator) is defined as:

- A notice to the PMR of pending disruption in communication
- A denial of a PMR request for assistance from the teleoperator
- No response for 10 seconds

If a PMR experiences a breakdown in communication with its fleet operator, it shall perform partial machine breakdown procedure (6.2.1)

[end current draft]

