ISO 4448-16:2023(X)

ISO TC 204/WG 19

Secretariat: SCC

Intelligent transport systems — Public Mobile Robots (PMR) and automated pathway devices — Part 16: Safety and Reliability

Key: Tracts that need work
Matters that are unsettled
Notes from stakeholders under resolution

To: URF Members:

On this round (March 21-23, 2023) the project team asks:

1. Have all necessary efficient elements been included (i.e., anything missing?)
2. Is the draft solution for each of these elements in the best/appropriate direction?
3. Is anything confusing, or ambiguous?

Remember:

1. This part (-16) sits in a much broader context that deals with behavior, orchestration, social and environmental (ODD) constraints and more.
2. The data dictionary is in 4448-2
3. The JDR (in 4448-20) is a critical companion and -20 is still an incomplete first draft.

WD stage

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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.

The parts of ISO 4448 are proposed as deliverables, as a foundation for instantiation.[1]

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.

[1] Additional standard deliverables may be required, later, for specific applications.

Introduction

The purpose of the ISO 4448 series is to define the data, communication, behavioural, and safety systems needed to organize and expedite the flow of automated ground traffic devices in public spaces. This includes the loading and unloading of robotic passenger and goods vehicles at the kerb[2] as well as ***public mobile robots*** or **PMR**s engaged in construction, food carts, inspection, garbage removal, last-mile delivery, mopping, parking management, repair, snow removal, surveillance, sweeping, washing and any other robotic service conducted on sidewalks (pavements), cycle paths, crosswalks or any other public, pedestrianized space.[3] PMRs are inclusive of automated wheelchairs, trolleys, return-to-base micromobility devices, and 'follow-me' devices, etc.

The term *public mobile robot* is used in distinction from *industrial mobile robot*. A full definition for PMRs can be found in ISO 4448-2. Parts 1-20 of ISO 4448 specify different aspects of these devices.

PMRs travel on pedestrian footways, cycle lanes etc. (as permitted by local regulations) to reach their destination, and may have to cross roadways, and may sometimes travel on roadways and road shoulders. There they may encounter persons, animals, wheeled devices propelled by humans, other PMRs (who may be travelling to a destination, or performing a task such as snow clearing or street cleaning), etc. PMRs may also be moving in other public, pedestrianized spaces, such as in airports, hospitals, hotels and shopping malls. The ISO 4448 series specifies how they do this and interact with humans and other PMRs they encounter. It predominately defines operational behaviours rather than detailed device specifications.

One of the purposes of ISO Standard 4448 is to facilitate the safe loading and unloading of Automated Vehicles (AVs) and the safe movement of Public Mobile Robots (PMRs)[4] in an urban environment. Ensuring that a PMR is operating safely requires the PMR to meet certain capability thresholds and for emergency procedures to be defined.

4448-16 is focused on the characteristics and capabilities needed to ensure safe operation of PMRs. Procedures to be performed by Teleoperators, Fleet Operators and Orchestration Managers in emergency scenarios are also defined.

Safety matters are described independently of matters of orchestration (4448-5), integration with mothership vehicles (4448-6), and PMR behaviours while operating (4448-7). However, while executing a TripPlan (orchestration), while interfacing with mothership vehicles (4448-6), and while exercising appropriate behaviours according to 4448-7, PMRs shall do so safely. Hence any safety prescription or procedure within 4448–16 applies throughout all PMR-related parts of 4448.

[2] Both on the sidewalk and carriageway?
[3] Cycle paths are not pedestrianized spaces. What about robots cleaning the carriageway side of the kerb?
[4] Are you explicitly varying standards for AVs and for PMRs? Very different types of machines.

Title (Introductory element — Main element — Part #: Part title)

1 Scope

The scope of 4448-16 includes the capabilities, characteristics and certification of public mobile robots (PMRs) required for safe operation in public spaces. This is focused on safety aspects of PMRs operating in pedestrianized spaces and is exclusive of automated vehicles (AVs) for passenger and goods transport, which are defined in 4448-2, 4448-5 and 4448-6.

PMRs must be reliably and sufficiently equipped, programmed, and managed to ensure no harm (including alarm or confusion) to proximate persons, pets or property. Details about machine design (including motion control) that are within the machine control envelope that do not affect its surroundings are not in scope — i.e., any machine design aspect that has no safety impact on external participants in the involved space (the device ODD) is not in scope.

4448-16 also describes the procedures that shall be performed in emergency situations, but does not include *robot behaviours* during operation. The latter is the purpose of 4448-7. 4448-16 does specify that PMRs be appropriately equipped to execute robot behaviours as described in 4448-7.

A journey data recorder (JDR) is specified in 4448-20 to record specific elements of a PMR journey. Such a JDR is a critical safety element and is closely aligned to 4448–16

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"

UN 38.3 Transportation Testing for Lithium Batteries and Cells [necessary? Only if the PMR is transporting batteries (?)]

Probably delete these:

- ~~IEC 63281 Personal e-transporters~~
- ~~ISO/TS 15066: Robots and robotic devices — Collaborative robots~~ ~~[Need to review this; according to the online review, it "does not apply to non-industrial robots, although the safety principles presented can be useful to other areas of robotics."]~~
- ~~ANSI/RIA R15.08-1-2020 Industrial Mobile Robots - Safety Requirements - Part 1: Requirements for the Industrial Mobile Robot~~ ~~[Need to review this. Is it different from ISO 102180-1? And it focusses on IMRs]~~
- ~~ISO 13849-1: Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design~~
- ~~ISO 22737: Intelligent transport systems — Low-speed automated driving (LSAD) systems for predefined routes — Performance requirements, system requirements and performance test procedures~~
- ~~ISO/TS 5255-1: Intelligent transport systems — Low-speed automated driving system (LSADs) service — Part 1: Role and functional model~~

3 Terms and definitions (moved to 4448-2)

For the purposes of this document, the terms and definitions provided in 4448-2 apply.

4 Safety System Descriptions

ISO 4448-16 defines system safety in terms of integrated subsystems rather than as individual technology components. This part of the standard is concerned with providing safety and reliability definitions as well as measures and tests of these subsystems regardless of the specific nature of the components that might be used in the design and assembly of any particular PMR.

For example, the standard is concerned with reliable perception under all *ODD* circumstances rather than with specifications for vision or audition devices or their resolution. As well, the standard is concerned that PMRs maintain appropriate distances (defined as *shy distances*) from all other persons and objects for both safety and social acceptance reasons. Hence, such things as braking distance and reliable braking[5] in addition to reliable perception and measurement are critical to 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 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, hence a focus on specific component elements can lead to unnecessary concern or to false reliance.

Whatever the breakdown and description of safe behaviour, safe systems and safe components, primary PMR safety is about the safety of proximate humans—of every ability—whether walking, using an assistive device, on a bike or scooter, using a proximate vehicle, and whether or not interacting with the PMR (e.g., removing contents, 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 4448-16, risk or harm to humans and their pets must be considered above property damage.

Many safety-related matters are detailed in several other parts of 4448. For example, 4448-7 describes PMR behaviour as it traverses a pathway. In these other parts, safety is usually described within specific detailed contexts of PMR behaviour, while 4448-16 is generally (but not solely) concerned with *fitness* to perform safely more than any software capability that manages a specific behaviour in question.[6]

One exception to this is the subsystems that ensure safe crossing of roadways. Currently, such subsystems require specific V2X signals so that these aspects of the specification are more constrained than most others.

ISO 4448-16 identifies several safety subsystems clustered 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 elaborated in **Table 1**.

[5] Plus maneuverability?

[6] These matters are integrated and the boundaries between subsystems may shift prior to final publication.

In spite of the focus on the safety-efficacy of subsystems, component behaviours are more easily described and measured, hence, where suitable, these may be named and described (but not specified) in support of understanding what contributes to a safe subsystem. This is done by setting out the physical elements and, where possible, a quantitative description of those elements that comprise each subsystem.

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

- carried out by its manufacturer or fleet operator and then provided as a guarantee
- promised by the system vendor in the form of a reliability guarantee (evidence of sufficient insurance might be considered as an appropriate form of guarantee, but the definition of sufficient insurance is out of scope)
- carried out by an independent third party (for certification)[7]

Table 1: Safety components relate to surroundings,[8] devices and humans.[9]

LOCATION safety Relates to proximate surroundings of the PMR (to keep proximate humans safe)	• Movement and stability • Perception reliability • Localization and odometry • Road crossing systems
DEVICE safety[10] 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[11]

Regardless of how system and subsystem safety may be certified or guaranteed, the ultimate test[12] is whether the user or fleet operator of any vehicle or PMR is able to obtain adequate liability insurance sufficient to permit its operation within the stated ODD of the vehicle or PMR within a governing jurisdiction. In this way, certifying parties or certification processes would use the standard as a guideline and insurability as its guarantee.[13]

Considering the existence of well-honed actuarial sciences and subrogation practices, this approach will maximize the safety outcome as long as jurisdictions insist on fleet registration and evidence of adequate

---

[7] Third party certification was preferred by one stakeholder. We agree, but assert that some components carry less risk and that self-certification, insurance premiums, product liability and market reputation may be sufficient in some cases. We will set this up so as to let the superior jurisdiction decide per subsystem, rather than dictating what must be third-party certified.

[8] Anything about weather conditions: ability to withstand an Xmph wind speed, or minimum degree of water proofing, or be able to operate in a puddle of at least y inches depth? (see 4448-11)

[9] This is an initial list; categorization of the topics may change. Have all subsystems per category been identified?

[10] Cyber security? (See 4448-3)

[11] ~~Stakeholder comment: "Seizure compliance and emergency compliance are similar enough that it feels redundant and overly specific given the general nature of both." *We agree these are related but different enough to require separate and clarifying treatments. See the updated versions.*~~

[12] PMRs will be largely managed in commercial fleets. Relying to a significant degree on insurance and subrogation allows insurance premiums to act as a conservative, "invisible-hand," safety control system.

[13] Matters of formal certification may need to be addressed after all certifiable elements are fully defined.

insurance coverage. This approach assumes financial penalties would cause vendors and fleet operators to act more conservatively (safer) than would governance penalties alone.

4.1 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 predictively through its intended pathway. “Safely” means without collision or near collision, without confusing or alarming any proximate pedestrian or other user, and without self-harm (i.e., to the device itself).

4.1.1 Wheels and legs

The choice between using wheels or legs for public mobile robots depends on factors such as ODD terrain, payload, intended speed, and manoeuvrability.

Wheels are more efficient on smooth, flat surfaces, providing higher speed and better manoeuvrability than legged designs commercially feasible in the early 2020s. Legs are more effective at traversing rough or uneven terrain, and have less difficulty climbing stairs and navigating other obstacles. Legs are generally slower and less efficient than wheels, and may require more complex and costly mechatronics to operate.

It may be necessary to use alternate wheel designs or combinations of wheels and legs in order to achieve future desired performance and functionality. It is almost certain that the current designs in commercial use for last mile delivery will be inadequate for wide-spread use throughout cities, hence this standard must anticipate that there are many innovations and design improvements that are currently unexpressed.

4.1.2 Longitudinal and lateral control[14]

Longitudinal and lateral control reliability and safety measures all aspects of safe, physical control of the navigational motion of a PMR.

Maneuverability, the ability to avoid obstacles given the immediate operating conditions within an ODD such as low surface friction, high winds, fast-moving obstacles, etc.

Stability, the tendency to remain upright is critical to both longitudinal and lateral control.

Longitudinal control pertains to:

- Braking; both for safety (not crashing) and for maintaining shy distance; note that maintaining shy distance always exceeds the zero-crash criteria.
- 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.
- Bunching; this applies to trains of PMRs (*Longitudinal string stability*)
- Traps; wheel, foot, or other appendage getting stuck in or on a pathway element

Lateral control pertains to retaining control:

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

[14] Lateral and longitudinal orientation are defined with respect to the direction of motion.

Table 2: Location Safety Parameters

Capability	Measure	Tolerance	Comment
Braking distance[15] (footway)	1000mm[16]	200mm	All surface conditions; teleoperator and ADS must slow speed accordingly. **4448 is agnostic to reaction time;** *4448 is standardizing PMR behavior, not differentiating among forms of automation or operation.* **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)
Braking distance[17] (bikeway)	3000mm[18]	300mm	All surface conditions. Teleoperator and ADS alike must slow speed accordingly. See prior comment.
Respect shyDistances (footway)	According to trip-plan	10% of shy distance *(note, there are several sD metrics)*	All conditions, any speed, any surface condition. 4448-2 provides a separate shy distance for bike lanes; auxSpacingInterval, which is time based.
Respect shyDistances (bikeway)	2000 ms (Set this according to trip Plan)	100 ms	Minimum time interval behind bikeway user. Similar to time intervals used by motor vehicle users. This metric is irrespective of light condition (time of day) or surface condition (dry, wet, sand, ice). Shy distance is for the safety of other users. PMRs, including those under teleoperation, must operate according to conditions.
Follow-me bots lateral string stability	150mm	50mm	Lateral displacement from leader of train. • Applies to a train of "follow-me bots". • Applies to a personal device following a human.

[15] The focus is on braking distance as operational control. In all cases, it is the distance that must be met hence the device must travel at or the teleoperator must be prepared for meeting the distance criteria.

[16] Regarding braking under teleoperator control: AASHTO allows humans 1.5 seconds for perception time and 1.0 second for reaction time. If driving 6 k/h (1.67m/s), then a "begin braking response under teleoperator control" at 2s + 0.5s will equal a driven path = 2.5s * 1.67m/s = 4.175m even before braking is started, as such a stopping distance of 1.0m will not be possible. Hence teleoperation has important limitations.

[17] 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

[18] URF Member, Mads, suggested 4000mm; asked whether this distance includes reaction time, and how many sigma. @lee reviewed the calculations and asserts that 3000 mm is appropriate. We wish to err on the side of shorter distance, relying on responsiveness of sensors and software, or the caution of teleoperators. (3.3m for a device moving at average cycling speed)

Capability	Measure	Tolerance	Comment
Coefficient of friction (kinetic); for tire/foot	0.5	(or more)	Related to surface friction; Wheels, feet can slip/slide ● rubber on wet asphalt is ~0.5 ● rubber on dry concrete is ~0.8
Min width for tire/foot	55mm	5mm	Related to gaps in/on the surface. Wheels, feet, armatures, can get stuck/wedged in cracks, grates, rails, potholes.

4.1.3 Stability (static and dynamic)

A PMR shall be deployed to remain upright relative to its design, and within the terrain and conditions of its ODD.[19]

Stability for a PMR is the tendency to remain upright when at rest (static) or in motion, especially under acceleration[20] (dynamic).

Stability concerns the ability of a PMR to remain upright in the case of an infrastructural challenge such as a steep kerb or deep pothole or a navigational failure such as the wheels or feet on one side slipping off the edge of a kerb. For example, a PMR must be able to mount or dismount a kerb to exit or enter a crosswalk, respectively. Kerb heights are approximately 15 cm.[21] Not all kerbs are sloped for ease of mounting by a wheelchair.

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 kerbs, or unsloped kerb 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 kerb.

The static and dynamic stability of a wheeled robotic device must allow it to remain upright on a running slope of 60% (31°)[22] and a cross slope of 60% (31°).[23]

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.

---

19 A self-righting device able to recover from tip-over is compliant.

20 Or deceleration? (this is just negative acceleration)

21 Would the manufacturer need to specify the maximum height the vehicle could mount? Possibly. We need to think about where to put this and how to express it. Mounting a particular height, also depends on the slope of the roadway leading up to the level change…

22 This is REALLY steep – is it too demanding? Cross slopes rarely exceed 10% in the UK. See the next footnote. This 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 needs to exceed almost anything a city can present…

23 A 60% slope is fairly steep and would be important in cities with very steep sidewalks, steep, uncut kerbs. This number must be chosen so that the likelihood of a PMR tipping would be extremely small; it may be sensible to have this number vary according to its applicable ODD. 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"

Regardless of wheel configuration, wheelbase dimension or leg design a PMR reasonably challenged in any of these ways shall not tip over.[24]

The risk of tipping imposing harm on proximate humans shall be covered by a suitable insurance 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).[25] 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.

4.1.4 Braking/stopping

Stopping distance is critical for longitudinal control.

Stopping distance depends on the nature and condition of the brakes, friction of the tires/feet relative to road surface conditions, robot speed and its gross weight. The maximum stopping distances for PMR operation on footway, bikeway, roadway are listed in 4448-2 Table 5.

In the case of a legged PMR, braking mechanisms may differ but maximum stopping distance shall remain the same.

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 footway, bikeway, and roadway 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 shall be tested to verify they function in the expected temperature range of their intended ODD (see 4448-11).

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

4.1.5 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 shall be performed in order to measure the minimum friction and maximum grade on which a PMR can safely climb. Additional tests shall be performed with ~~simulated(?)~~ water, snow, ice, sand, gravel, and leaf cover (others?) to verify a PMR can accelerate safely under these conditions.

Each of these conditions present different braking challenges that are compounded by factors such as weight, load, wheel and 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 may be less than that of a C or R-Class one. This may mean that tests are justified for the latter but not the former. (…or different tests and different criteria)

[24] This is exclusive of vandalism or police action during an apprehension or emergency action.

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

Should be a part of the standard that describes something like demerit points when a fleet operator is at fault for an issue. The method of enforcement and the type of punitive measures would be up to the municipality. At best they might use the standard to write bylaws, but the enforcement would be of their own choosing.

4.1.6 Controlled forward motion

A PMR shall be able to travel on its trajectory in a stable, controlled manner over the variety of surfaces it may encounter in its ODD. PMRs shall be tested to verify the roughness, firmness, cross gradients, and surface openings such as grates and storm drain covers, over which they can sustain controlled travel. The maximum step a PMR can mount in low friction conditions shall also be tested.[26]

For wheeled PMRs, tires shall be sufficiently wide, strong and durable to handle the surface conditions in its intended ODD. Wheel radius shall be large enough to navigate bumps in the pavement, potholes, railway tracks and drains safely. For ambulatory PMRs, the feet shall be large enough that they do not get stuck in crevices, drain grates or rail tracks.[27]

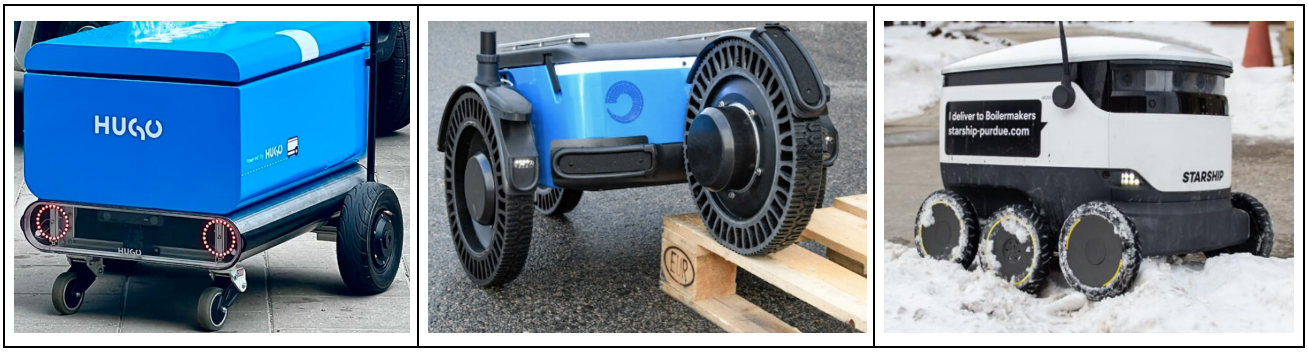

Figure 1: The tiny wheels on the left may be suitable for the intended indoor, smooth tile floor ODD of this PMR. The larger wheels on the center PMR are intended for difficult rough terrain and may be necessary for delivery in snow or for maintenance applications. The wheels on the right can climb kerbs, but not stairs and are suitable for very modest snow depth.

In **Figure 1**, the PMR on the left has a very small wheel for indoor floor use but would likely constitute a hazard when moving in and out of an urban crosswalk (no accompanying human to help it over the curb). The PMR in the centre has a substantial wheel radius and width for fairly difficult terrain and might be able to navigate a majority of urban settings, but they would make the device larger perhaps demanding more space. The PMR on the right with a more typical radius wheel for small deliveries, might get stuck in slightly deeper snow, as it is here. There is no perfect wheel radius or foot size, but a jurisdiction shall assess its intended pathways for use and to specify appropriate minimum sizes for fleet registration whether for delivery, surveillance, maintenance, or other tasks.

Wheel diameter or foot size shall be suitable to the ODD. While choices may be offered by the manufacturer, size 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.

[26] 4448-18 will address testing for PMRs

[27] There is a video (2022) of a delivery PMR whose wheel(s) caught in a train track was subsequently struck by a train on that track. https://www.youtube.com/watch?v=XMzdyesno_Y ~~There have more than one case of these robots hit by trains.~~ ~~https://www.tiktok.com/@anna.sno03/video/6947410475994959110~~

4.1.7 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 (4.1.4) and traction (4.1.5) tests are made.

4.1.8 Turning (reversing travel direction)

When a PMR is operating in narrow, constrained pedestrianized spaces, it is valuable, but not required that a robot be able to rotate around its Z axis, rather than turning in a wider-radius U-turn or a more complex multi-point turn. A PMR must execute a clean U-turn or a 3-point turn within the width of the pathway where the turn is executed.

4.1.9 Longitudinal string stability

Longitudinal string stability applies to trains such as a string of PMRs following a lead vehicle and includes the case of PMRs following a natural pedestrian or cyclist (4448-14). Such a train of PMRs shall not "bunch up" (slinky-effect) to cause inter-PMR spaces smaller than **shyDistanceStandBack.**

Bunching of trains longer than two PMRs implies an additional concern. 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.

This may be both a safety issue and a traffic management issue.

A PMR train shall set and maintain a separation of 1.0 **shyDistanceStandBack** between each of its PMR members. This allows free passage of pedestrians to pass through (cross in the middle of) such a train, *when the train is stationary.*

Inter-PMR distances within e-tethered robot trains shall be internally managed using intra-train distributed control rather than teleoperated via central control. In the case of an e-tethered PMR train, only the lead vehicle can rely on teleoperation for navigational control.

4.1.10 Lateral string stability

Lateral string stability applies to road-trains such as a series of PMRs following a lead vehicle enabled via tethering or e-tethering. Depending on the nature of the control system that keeps the second, third, etc., PMR on the same travel path as set by the lead PMR, it is possible for a PMR following such a lead to:

- deviate from the path if the lead PMR changes directions abruptly ("crack-the-whip" effect)
- tilt or sway 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. In the case of an e-tethered PMT train, 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.[28]

[28] Reference: Masters thesis, Justin de Geus

The maximum permitted lateral path deviation of a follower PMR compared to the path taken by the lead PMR shall be 0.5 **shyDistanceDynamic**.

4.2 LOCATION Safety: Perception reliability

Sensors and other components used for environmental detection are vital for a PMR to detect its surroundings. These components and their integrated software facilitate situational awareness in order to maintain safe operation.

The standard is concerned with PMR awareness, responsiveness, redundancy, and recoverability; it is agnostic about the number or types of sensors.

A PMR shall have a

- 360° field of view for full-surround awareness including vandalism[29]
- minimum visual detection bubble
    - forward: 50m[30] for anticipating and planning
    - back: 20m to cover a full arterial intersection width in case of a need to reverse, protect or record
    - side: 10m 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 too closely by another entity (pedestrian, jogger, PMR, etc.) needs 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
    - What about sensors pointing up or down it the event of being tipped?
- Sensors shall be self-checkable or remotely checkable by a teleoperator in real time
- Sensors shall be easily removable and replaceable for rapid on-site repair (UL 3300 8.7) (necessary?)[31]

4.2.1 Journey planning for public mobile robots

The activity of determining, via computation or teleoperation, the optimal movement of a mobile robot is known as path planning. This is a still-developing field of robotics innovation having many forms and purposes and addressing many objective functions. Typical objective functions might be to optimize

[29] 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".

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

[31] I cannot see a use case for this. The idea is to ensure that it is easy to repair a robot in the street. Less disruptive than sending a truck to pick up the PMR and take it to a Depot. Just send a repair person on a bike and snap in a new sensor. Safer, cleaner, more efficient for all concerned.

journey time, cost of journey, energy use, or safety.[32] In the case of PMRs, there may be additional objective functions. For example, minimizing travel in busy pedestrian areas, avoiding difficult urban terrain, avoiding an area of high likelihood of vandalism, avoiding dangerous intersections, etc. These might be understood by the path planner or they may be imposed on the path planner as initial conditions. It is very likely that the overall journey planning activity for public mobile robots, would include a high number of objective functions. Automated path planning for PMRs would generally be complex, and would involve multiple levels of planning each with different inputs and computational paradigms.

A human example illustrates this. Ruth, a pedestrian, intends a 2 km walk to a fixed destination. Ruth plans an overall route to get to the destination, deciding which sidewalks or trails (pathways) to use. On the way, she would be closely focussed on each "next step" so as not to stumble, slip on ice, or bump into anything. At a wider proximity radius, she would retain some awareness of what is a several meters around her, especially those things further ahead in order to anticipate anything she needs to prepare for or be ready to avoid. Her perceptual and decision focus would fall off over a distance, so that she would be relatively unconcerned for something that was 40 m away, and likely even less for something 80 m further on. These example distances would differ if Ruth had decided to jog or take a bike instead of walking.

Public mobile robots have an analogous planning problem. To provide context for PMR journey planning, three levels of mobility planning are defined.

4.2.1.1 Macro planning for PMR journeys

Macro planning for a PMR journey or task is determined by a fleet operator prior to the beginning of a task. This activity would be sufficient to provide a rough plan for the entire task-journey on the assumption that finer details (micro plan) would be computed as the journey unfolds. For example, the macro plan for a snow ploughing task would include the time and route to re-locate from a starting position (A), to the place where snow is to be ploughed (B), the activity of ploughing the snow, then returning (A), or proceeding to a new location (B'). The ISO 4448 standard is silent in regard to the *activity* of macro planning, but assumes that such planning must occur (4448-5) and that there must be specific inputs available to the process (e.g., 4448–10, –11, –13). The data source for macro planning may be a fleet operator who operates a fleet within an ODD, or it may originate with a regional orchestration manager (OM) that provides a TripPlan on request to the fleet operator for the target PMR (4448-5).

4.2.1.2 Micro planning for PMR journeys

Micro planning for a PMR is the close-range, second-by-second or cm-by-cm planning required during a journey. This is central to a mobile robot's intelligence in addition to whatever specialized task a robot may undertake during or at the end of a journey. It is the part of the robot's activity that a teleoperator would be overseeing or possibly assisting as a PMR journey unfolds. In general, micro-planning during a package delivery journey might include continuous planning of the next tens or hundreds of centimeters, depending on the ODD context. This standard is silent in regard to the *activity* of micro planning, except that journey plans be executed in a safe, structured and transparent manner (4448-7, -8, -16, -20). This standard recognizes that no PMR can proceed without micro-planning specific to the task, the ODD, and the PMR design — for all of which 4448 is agnostic.

4.2.1.3 Planning for mobile robots in unstructured environments

Inside a factory or a warehouse, the paired roles of macro planning (fleet orchestration) and micro planning (path planning for IMR or AMR mobility) are generally designed to leave no operating gap. Such

[32] Sánchez-Ibáñez, J.R., Pérez-del-Pulgar, C.J., García-Cerezo, A. Path Planning for Autonomous Mobile Robots: A Review. Sensors 2021, 21, 7898. https://doi.org/10.3390/s21237898

structured ODDs are fully understood (mapped in detail) by the macro planner, diligently managed by the business operator to remain spatially structured and fully recognizable (computable) by the micro planner (software).

This is not the case in unstructured, public, pedestrianized spaces for PMR journeys that easily extend over two or three km and where there may be significant gaps between macro and micro planning. Unstructured navigation spaces from a PMR perspective may change rapidly, may differ from hour to hour, and may only approximately match mapped expectations. A tree may have just fallen, a house may have caught fire, an arrest might be in progress, a small crowd may have gathered around a bus stop or a store front, a crash may have occurred at a crosswalk, several dozen children from a school may entering the sidewalk in a surge beside the school, a UPS van may have parked on the pavement, or someone may be walking behind the PMR to execute a prank (vandalism). These are all things that may happen without notice and within the duration and space of a macro plan, but occur outside the close range of micro planning. Controlled factory or warehouse spaces would not admit these as common occurrences. The same cannot be said of public, shared-space environments.

When unmapped, unexpected circumstances occur within a PMR ODD, a near-sighted PMR would more readily move into circumstances that may become a barrier. Having insufficient advanced awareness, a near-sighted PMR may have to reverse or find itself trapped. Because the micro planning range is constrained, the PMR may find itself entangled in unplanned situations among unappreciative human bystanders. Many of these situations might be edge cases.

Another common problem behaviour inherited from near-sighted micro planning in unstructured environments is the sudden path adjustments and recoveries which exhibit as rapid micro changes in PMR acceleration (|jerk|). A related behaviour is exhibited by pedestrians, who are looking at a phone or other distraction, as they approach another pedestrian and suddenly find themselves jumping aside or oscillating side-to-side to negotiate passage. Encountering this micro-acceleration (|jerk|) behaviour in a PMR that is moving in front of a pedestrian who is attempting to overtake that PMR, or in a PMR that is approaching and about to pass a pedestrian is confusing and disconcerting.

How can a PMR afford the necessary and sufficient understanding of its surrounding environment to avoid journey traps while flowing smoothly — MIN(AVG (ABS(jerk))) — among the dynamic obstacles and humans that share its ODD? The answer to this question is currently poorly resolved, differs among ODD circumstances and according to PMR speed.

4.2.1.4 Meso planning for PMRs

Nothing in this sub-clause describes how a PMR is to perform meso planning; rather this clause specifies only that a PMR shall be enabled way of sensors, software and or teleoperation to be able to carry out meso planning, and what the range and impact of that planning, shall be. The perception of any threats to the PMR macro plan that may be discovered through the meso planning process shall be carried out automatically or via a teleoperator or in cooperation between the two.

In between the macro and micro levels of journey planning for PMRs is meso-planning. In regard to PMRs moving among pedestrians and other dynamic, active transportation users in shared landscapes such as sidewalks, parking lots, crosswalks, parks and airports, it is critical that a PMR is able to make approximate plans for its surrounding area by anticipating further out than is required for micro planning. This is important for things such as:

- Planning the complete crosswalk traversal of a multilane roadway
- Estimating the probability that the PMR can complete the remainder of a pathway segment (4448-2) immediately in front of it (tens of meters) without requesting a change in macro planning (a new TripPlan)

- Awareness of a sufficient distance forward to assess that a PMR is approaching a police, fire or medical emergency with enough notice to plan avoidance, such as asking for a new TripPlan)
- Recognizing that something to be avoided is happening a few meters to the rear or the side (one case is a motor vehicle that may not to be stopping in time prior to a crosswalk boundary
- General awareness of what is to the side or to the rear so that a PMR can develop a quick response if necessary

Meso planning does not plan micro responses; meso planning operates at a much higher level than micro planning, but at a lower level than macro planning.

Meso planning shall:

- assess multiple seconds and multiple meters into the future, depending on task, speed, and ODD (**Table 3**)
- ensure that the PMR will be highly unlikely (threshold?) to find itself trapped on the way to this intermediate place (note: being trapped is not the same as being unable to complete)

Meso planning shall answer two questions:

- How likely (threshold?) will the PMR be able to continue on its macro plan when it reaches this intermediate place?
- How likely (threshold?) will the PMR be able to determine and execute a micro plan when it reaches this intermediate place? (this second question is redundant; by definition a PMR must be able to determine and execute a continuous micro plan in order to complete a macro plan)

A PMR shall have sufficient sensors to perceive all threats to its macro plan within a 360° surround to estimate with 99% certainty that it can continue its macro plan within its meso planning radii.

A PMR shall have sufficient software and/or be assigned sufficient teleoperator bandwidth and attention to continuously assess potential threats within the appropriate radii as defined in **Table 3**. The intention is that the collaboration between PMR software and teleoperator is sufficient to ensure that the PMR shal be unlikely to become stranded or trapped or behave is ways that confuse, alarm, startle or disrupt bystander mobility.

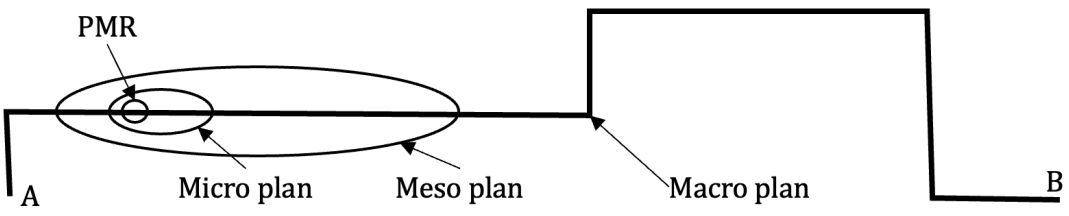

Figure 2: How the three PMR planning levels are related. The PMR direction of travel is from A toward B. The radius of micro and meso plans are shown as ellipses (radii) with the major axes along the direction of travel, and the PMR situated toward the relative lagging foci of the ellipses. Think about driving a car—the majority of driver attention is forward, with much less behind and to the sides. While, this illustration shows nothing novel about following a path (macro plan) current meso planning for PMRs is often poor or ineffective.

The measures in **Table 3** pertain to the ability of a PMR and/or its teleoperator to understand its near-surroundings. This local awareness must be sufficient to permit a PMR to make near-range crash avoidance decisions (micro-planning), mid-range navigational decisions (meso-planning), and to execute an alarm immediately prior to a mishap such as pending fear of tipping or other vandalism.

Table 3: The meso planning capability of a PMR must be able to detect barriers or threats to the completion of the current macro plan (Trip Plan). These must be detected with sufficient time (at sufficient distance) for a PMR to request a new macro plan in order to avoid a delay or trap.[33] Within this same sensory radius (or generally much less than), the PMR must also be able to adjust its current micro plan to minimize |jerk|.[34] There shall be no radial blind spots in the ellipse so described, although there may be a small blind area at the base of the PMR depending on how cameras are mounted. (See **Figure 3**).

Capability	**Time horizon**	**On Walkway** 6kph = 1.7 m/s	**On Bikeway** 25kph = 7 m/s	**On Roadway** 40kph = 11.1 m/s
Forward awareness	10-12 sec	17-21 m	70-85 m	111-133m
Side awareness	4-5 sec	7-9 m	28-35 m	45-56 m
Rear awareness	8-10 sec	14-17 m	56-70 m	88-111 m

Any PMR perception system(s) shall be tested to ensure that objects can be identified.[35]

Any PMR effector system shall be tested to ensure that obstacles can be avoided.[36]

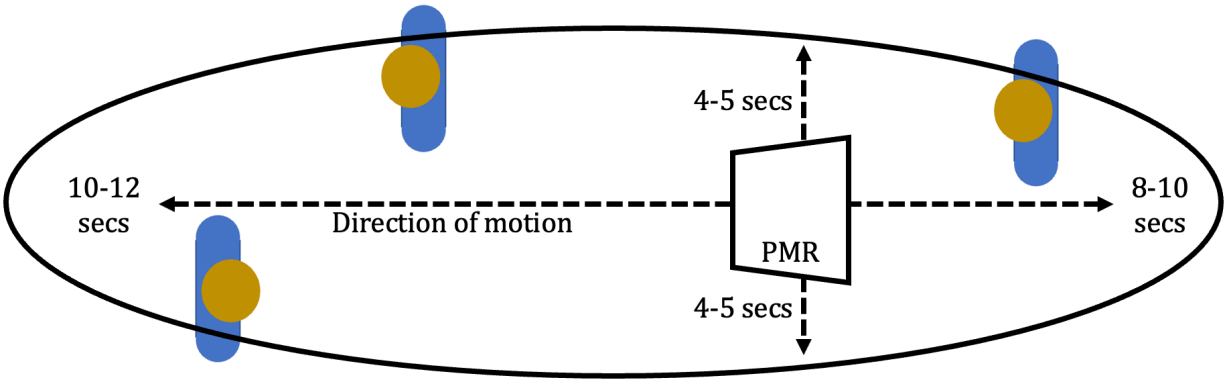

Figure 3: The surround-awareness ellipse within which a PMR (or its teleoperator) is able to detect and determine the presence of objects and events for micro-planning, meso-planning, macro-plan replacement, self-protection and recording in regard to intersection safety or vandalism.[37] (See **Table 3**)

---

33 "The numbers proposed need some evidentiary backup before they can be set as a standard. Until they are properly defended, they should to be set as variables." *(See the Grush-Kretz conversation at the back…)*

34 For smooth flow among pedestrians

35 We are talking about a perception envelope, so do we need to either prescribe a minimum sized envelope, or add some more dimensions – e.g. what about at 45°, as your figure below suggests. Otherwise, you could have a forward and side sensor that gives 0m range at some angles. This subclause has been completely rewritten since this comment was provided…The intention is for the entire space within this ellipse to be fully perceivable to the PMR. The standard does not prescribe the type of sensors only that this space be perceivable to the PMR or to its teleoperator. I will review to see if it need to be expressed better…

36 A stakeholder asked: "Physical testing or computer simulation? There should be a distinction made between these." This needs more investigation.

37 The "surround-awareness ellipse" or the "navigation confidence envelope" in the PRIOR VERSION of the figure above, caused considerable disquiet among stakeholders at our winter roundtable. Concerns included: [1] over specifying the ability of the robot, [2] many things would occlude the view of the robot sensors (buildings, parked cars), [3] little need to see behind, [4] some bicycles in bikelanes go very fast, hence this should be specified in terms of response *time* instead of *distance*, [5] it won't be possible to have zero blind spots. This update addresses many of these comments. **Blind-spots** will depend on how sensors are mounted. It would be easy for the PMR to have a significant blind-spot at its base & unable to see at its wheels or feet. This would

The test to determine whether a PMR has sufficient configuration of sensors, software, and teleoperator attention for meso planning can be determined by:

- the average |jerk| recorded by the JDR (how to determine how low this should be ?)[38]
- the frequency of a PMR being caught by surprise, any circumstance that requires high |jerk| to recover or avoid mishap, bystander complaint, sounding of a last-second warning alarm, a PMR being trapped (unable to U-turn), or_____.

The specification is intended for safe navigation, and bystander comfort; it does not consider the current state of technology or preferred cost expectations. The specification relies on the ability of a fleet operator to provide a teleoperator to satisfy any meso planning requirement that is not reliably automated.

In addition to confirming the viability of forward planning in completion of a macro plan, a PMR may require:

- a plan for a U-turn (the worst case for which would be in a road crossing); having some understanding of what is unfolding behind the PMR during such a manoeuvre would be invaluable; extra seconds could save bystander lives
- Rearward and side-visibility to anticipate vandalism, wayward vehicles or pedestrians

4.2.2 Graceful recovery of perception reliability

A PMR shall have sufficient perceptual capability to ensure that it is able to safely navigate.

A PMR shall have sufficient self-awareness of, or its teleoperator shall be able to detect, a decline or failure of perceptual capability below the threshold required.

In the event of a decline of perceptual capability, a PMR shall have sufficient system redundancy to return to its depot safely.[39]

In the event of a failure of perceptual capability, a PMR or its teleoperator shall be able to decide to execute either a Partial Machine Breakdown (para 5.2.1) or a Complete Machine Breakdown (para 5.2.2) procedure, whichever is appropriate.

A PMR *in collaboration with its teleoperator* shall have location and orientation capabilities equivalent to the sensory abilities of an aware, attentive pedestrian. Any combination of technologies such as cameras, LIDAR, GNSS, accelerometers, ultrasound, high-resolution maps, telecommunications and others may be used to enable this capability.

---

make it vulnerable to being ensnared maliciously. It was understood a robot would have a blind-spot equivalent to at least its footprint or more. One suggestion was 1 m beyond the footprint. That was not acceptable, because small children like to run to robots, to engage, and such a child, would very quickly be within the blind-spot (dangerous), so an extension of 5 cm beyond the footprint was suggested… There was considerable discussion of the importance of shrinking any blind-spot. The blind-spot aspect is undecided.

[38] There are innumerable online videos (social media, YouTube), showing a PMR approaching a pedestrian and making sudden micro-direction changes (|jerk|) in the final meter before passing that pedestrian. This has the effect of confusing or alarming the pedestrian. Such last-second direction changes amount to delayed gestural communication. If the pedestrian is distracted, (looking at a phone), then there is a risk that the PMR would startle such a pedestrian by turning aside only at the last moment.

[39] Does this mean the need to specify minimum battery level when leaving the depot? We would not specify a minimum battery level in terms of a percentage, or KWh, what the standard says, a PMR shall not find itself in a situation where its battery cannot get it to a charge station. So that has to be decided by the fleet operator who understands the TripPlan and the ODD conditions, etc.

4.3 LOCATION Safety: Localization and Odometry[40]

PMRs shall be able to accurately and reliably determine their location and orientation in any urban environment to which they are subjected. This includes urban canyon conditions for GNSS signals. Such PMRs may employ a variety of GNSS or wireless technologies in order to perform this task. Under no circumstance can a PMR become lost and unrecoverable, with the exception of a disaster or being stolen.[41]

Table 4: Location capability, regardless of deployment geography

Capability	Measure	Tolerance	Comment
Location accuracy, dynamic	{150mm,[42] 99%}	50mm	This is relative to ground truth, not to the map the PMR may be using
Location accuracy, static	{500mm, 99%}	2000mm[43]	Relative to ground truth. First fix may be worse if using GNSS
Return to pathway (e.g., map matching)	1	0 Execute a Partial Machine Breakdown (para 5.2.1)	A PMR is expected to locate itself on its map even if it departs from a fixed pathway (sidewalk or bike lane). For example, if a PMR must leave an assigned pathway (footway, bikeway) to circumnavigate a barrier or wait for an unload, it must be able to find its way back to its assigned pathway. Relying on a teleoperator is acceptable.
Be able to accept map updates	Within 24 hours of availability	4 hours	Relying on a teleoperator in lieu is acceptable. In other words, no PMRs may operate in public spaces with a map that is more than 24 hours out of date unless a teleoperator in attendance.

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

[41] Theft is a business security problem, not a shared infrastructure safety problem. This aspect of the standard is about public space, and wishes to avoid stranded, abandoned, and lost devices.

[42] Why would dynamic locational accuracy be better than a static one? That is the impact of the urban Canyon effect, and the ability of Kalman filtering on dynamic positioning.

[43] Why is the tolerance higher than the measure? Because of first-fix and urban canyon signal problems

Capability	Measure	Tolerance	Comment
Be able to determine and recover from a map error.	1	0 Execute a Partial Machine Breakdown (para 5.2.1)	A PMR must 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. *(This may be a difficult problem to resolve without false alarms.)*[44] A significant map error is likely to require a teleoperator, exclusive of automatically downloading a repair which may not always be feasible.
Be able to recover from a navigation service failure (e.g., GNSS)	1	See comment; Else execute a Partial Machine Breakdown (para 5.2.1)	GNSS 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.
Be able to remain safe in the case of telco loss.	1	See comment; Else execute a Partial Machine Breakdown (para 5.2.1)	There may be telco blind spots causing PMR connection to its teleoperator to fail. The PMR must be able to come to a safe place, and await recovery.
A PMR must leave bread crumbs	breadCrumbSeparation default=30m	10m	The PMR shall report its location (and have it acknowledged by the Fleet Operator) every {breadCrumbSeparation}[45] metres so that it can be easily recovered if the PMR loses connection with its teleoperator. [46] If the location acknowledgement loop is broken: ● The PMR shall execute a Partial Machine Breakdown (para 5.2.1) ● The teleoperator must initiate the (xxxx) PMR recovery procedure @lee suggests define this in 4448-7 or -12. Best is -12 as recovery procedure also applies to collisions)

[44] A possible solution may be for the PMR to attempt at least once before raising an alarm. Retrying is more suitable for human problem solving. As a machine gets smarter, it's programmers would seek to find a solution to the point of exhaustion before raising an alarm. So what I meant by a "false alarm" is that a solution to the problem that is computationally available, had not been coded into the system, so that the "mismatch" could have been resolved. I think I am just admitting that minor map errors may stump a PMR. I am not actually sure about that. Need to re-think this!

[45] This distance is to ensure that a PMR that has lost contact waits within a known radius of last contact. The default of 30m means that the PMR would usually be on the same block-face (in the event it is travelling on a sidewalk. One exception is that a PMR ***must*** complete any road crossing and wait no closer than five x shyDistance from any crosswalk, Hence, the PMR to be recovered will occasionally be found on the next or ajacent block-face.

[46] What happens when a PMR stands in the same location for an extended period of time? It would not report its location. Is there any mishap that could occur such that the device could be out of communication, then moved

4.4 LOCATION Safety: Road crossing systems

*Some of this section will be moved to 4448-7 Device Behavior (i.e., "**what**" the PMR must do); here we are concerned whether the PMR is "**able**" to do it. It is developed initially in one location before split and partial relocation to 4448-7.*

A PMR, with or without a teleoperator, shall know how to cross roads in these ways:

1. acquiring/using V2I messages[47]
2. obeying a WALK signal; a *scramble* crossing is a special case
3. using traffic signals at intersections with no walk signals
4. observing traffic at intersections with no signals
5. using V2I messages at mid-block crossing
6. using teleoperator oversight at mid-block crossing
7. a roadway without crossing infrastructure (and PMR shall know when not to attempt)
8. asking a pedestrian ~~for help~~ to push the walk button (4448-8) (this could be indeterminate if no proximate pedestrians)
9. using a connection between teleoperator and the intersection control system (this would mimic V2I, but without SPaT and MAP, and would be unworkable at most intersections)
10. using a pedestrian bridge, or subway
11. rely on a local bylaw that permits a teleoperator to cross ON GREEN and NOWALK (this would likely place full liability on the teleoperator)
12. by not crossing a roadway when it is not equipped to do one of the above and to request an alternate route from the PMR orchestrator (4448-5)

A PMR shall not cross a roadway in the absence of a controlled intersection and without teleoperator oversight.

If a PMR crosses a roadway in the absence of a controlled intersection, the teleoperator shall be liable in every such circumstance.

PMR behaviours regarding how to wait at, enter, cross and exit an intersection are described in ISO 4448-7. The present paragraph is solely concerned that a PMR be able to understand signals that grant crosswalk right-of-way access to pedestrians and to which PMRs shall conform unless explicitly determined otherwise, such as in the case of dedicated infrastructure.

4.4.1 PMRs using V2I standards

A PMR may be expected or permitted to use pedestrian infrastructure such as pavement, sidewalk, road shoulders, and crosswalks. PMRs using V2I-enabled intersections shall understand and comply with relevant V2I messages. Whenever using pedestrian crossings, PMRs shall enter and clear them according to existing V2I standards SPaT and MAP as directed in ISO 19091 and defined in SAE J2735.[48]

in a way that the fleet operator would not be able to find it. I think that is possible due to failure, or theft, so this is unresolved.

[47] Early-minority; describe SWARCO example generically, as a case-study; do not publish brand. This is the SAE intention.

[48] It may eventually be necessary to include the utilization of V2I messages in any "SAE Level 4" ODD claim that includes intersections, but it is too early to know or insist on that. It is expected that regulatory construction will require PMRs to follow pedestrian crossing rules. This has been the case to-date.

Whenever a road crossing is guided or handled by a teleoperator, there shall be a procedure that a PMR teleoperator must follow, regardless of the form of teleoperation. This includes:

- Request pedestrian crossing messages (V2I); and/or
- Receive and recognize pedestrian crossing signals at the teleoperator's workstation
- Cause the PMR to obey the pedestrian crossing rules

Many PMRs may face critical barriers in their ability to independently cross intersections:

- PMRs may be much lower in height than the average human pedestrian. This implies reduced visibility and awareness on the part of drivers of motor vehicles.
- PMRs may be unable to independently request a pedestrian walk signal—i.e., by physically or wirelessly activating the pedestrian signal request button.
- Intersections with non-trivial signal combinations—advanced left turn, transit priority, delayed green, independent pedestrian signals, scramble—imply differing or additional risk to PMRs, proximate pedestrians, and vehicle drivers using such intersections.

A PMR shall rely on one of three principal ways to cross any roadway as listed in **Table 5**. Even as V2I signals become available at intersections not all PMRs will be directly conversant so that the teleoperator shall mediate.[49]

Table 5: Crossing roadways with or without V2I signals

Capability	Measure	Tolerance	Comment
Direct reading of SPaT and MAP messages	0 or 1	1	The PMR reads and responds autonomously; however, very few intersections are expected to deploy V2I messaging over the next decade.
Indirect reading of SPaT and MAP messages	0 or 1	1	PMRs may rely on teleoperators to mediate during intersection crossing if the PMR cannot read and interpret these messages.
PMR is able to be guided through any intersection	0 or 1	0	The PMR must have teleoperator oversight at any intersection for which either SPaT and MAP signals are not available, not readable by the PMR, or not working

The summary of default rules is:

1. PMRs have access to the same crossing signals as do pedestrians
2. PMRs obey pedestrian crossing signals
3. PMRs shall operate according to V2I signals where they are available: they may do that directly or indirectly through teleoperator mediation
4. PMRs operate conservatively in crosswalks
5. PMR crosswalk behaviour shall conform regardless of its SAE J3016 "level" of automation

[49] We need to add an indicator of the type of PMR intersection control mechanism that a PMR can be expected to encounter at each road crossing to the tripPlan map (4448-5). Such a PMR must be able to rely on fallback teleoperator mediation in the event that V2I messages are not operational.

4.4.2 PMRs have access to the same crossing signals as do pedestrians

V2I-equipped intersections broadcast SPaT and MAP messages. There are two ways for a PMR to take advantage of these messages:

1. The PMR may receive and interpret the message and make appropriate crossing decisions
2. A teleoperator may receive and interpret these messages in order to appropriately control the PMR at the crossing

For V2I-equipped intersections:

- SPaT and MAP (or similar) messages are available
- It shall be possible to certify whether a PMR is able to obey V2I signals
- Certification may be done by a third-party or via self-certification by the PMR fleet operator or manufacturer
- The governing authority shall have access to confirmation of certification
- The certifying party may be subject to liability during subrogation in the event that a PMR that did not obey V2I signals is a fault in a crash at a crossing with correctly, operating V2I signals

For non-V2I-equipped intersections:

- A PMR may be guided through the crossing by a teleoperator
- In the case that a fleet operator relies on a PMR to proceed without the remote assistance of a teleoperator, the fleet operator may be subject to additional liability

Regardless of how a PMR is proceeding operationally, the fleet operator shall remain responsible and often at least partially liable. The degree of responsibility, the nature of insurance and the process of subrogation are out of scope of 4448.[50]

4.4.3 PMRs obey pedestrian crossing signals

A PMR crossing an intersection shall obey pedestrian crossing signals. PMRs can do that either by reading V2I messages and acting accordingly or they can do that under teleoperator signal or control. In the event that a PMR is unable to obey pedestrian crossing signals at an intersection, the PMR shall not cross that intersection.[51]

4.4.4 PMR crossing a roadway without V2I or teleoperator mediation

In all cases in which a PMR is crossing a roadway or other traffic intersection independently of V2I or teleoperator oversight, the PMR shall:

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

---

[50] Liability ultimately rests with a human agent whether operator, maker, designer, maintainer, etc. Generally, in the case of a corporation, that corporation would be liable, and if an individual (employee) was negligent that would be handled internally, but from an insurance subrogation perspective the commercial entity would most likely be liable (at least in Western jurisprudence). This footnote might be removed from the final version of the standard. This is a technical standard and as such cannot offer legal opinions. Liability is a huge question, and we have access to developing answers in this matter (refer to the Hatch-URF document in progress, here).

[51] This is likely redundant. We mentioned it at the beginning of the session, and an equivalent procedure exist in 4448–7. At the moment it is here for completeness. We will filter redundancies before we submit for CD, but we want to make sure that we have everything before we make that pass…

In the event of failure to meet these guides, the fleet operator shall assume all liability.[52]

4.4.5 PMRs operate conservatively in crosswalks

A PMR shall operate conservatively in a crosswalk. In the event that a PMR has a range of opportunities with respect to speed, overtaking other PMRs or other pedestrians, competing spatially with any other crosswalk 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.[53]

If choosing a higher speed, passing another user, or changing sides of the crosswalk means a greater level of safety for proximate pedestrians or the PMR itself (for example clearing an intersection toward the end of the ***pedestrian phase*** without additional risk to any other user), then the decision the PMR shall take is the safest decision in the circumstance. The measure of this safety would be embodied in the PMR algorithms or teleoperator operating manual provided it is following all other applicable 4448-7 behaviour rules.

4.4.6 PMR crosswalk behaviour shall conform regardless of its automation "level"

A PMR shall conform to pedestrian crossing rules including the possible reception and execution of V2I messages regardless of the SAE J3016 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 by a teleoperator.

This 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.

4.4.7 PMR crosswalk behaviour may be protective of other pedestrians

It is possible for a PMR to become aware of pedestrians following it as it crosses a signalised intersection such that the PMR is able to calculate that the pedestrian is unlikely to clear the intersection during the pedestrian-crossing phase of the light. 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.[54]

4.5 DEVICE Safety:[55] Power safety

Power systems involve energy in the form of fuel or batteries[56] as well as motors and engines that may generate heat or have moving parts. Such system components may be subject to or generate fire, chemical or other hazards.

---

[52] There may be appropriate exceptions for emergency PMRs such for fire or police. These are out of scope.

[53] See 4448-7 for greater detail.

[54] This behaviour is not required by the standard. It creates risk for the PMR, while trying to reduce the risk of the non-involved pedestrian. It has been included here as a safety measure for non-involved pedestrians and has the advantage of engendering greater collaboration between PMRs and pedestrians. If a fleet operator incorporates such behaviour in its PMRs, careful consideration should be taken regarding fleet insurance.

[55] Once we understand the full requirement, we need to develop a table of fleet operator responsibilities for which the fleet operator would carry liability. This would be similar to "vehicle user requirements" common in most motor vehicle codes.

[56] How to prevent a fleet operator from having a PMR run out of power on a trip? (this is mentioned in a couple places 4.2.2 and 4.5.2 and maybe more) Should it report its remaining energy left to the Orchestrator? (No, the PMR cannot communicate with the OM, and this problem is the responsibility of the FM. If the PMR actually runs out of energy (therefore becoming disabled), then that needs to be reported to the OM because of the scheduling implications.) This also has implications potentially for 4448-5. (yes, as discussed in the previous sentence).

Table 6: Status and emergency procedures regarding device safety

Capability	Measure	Tolerance	Comment
Self-detection procedure	1	0	PMR systems shall be able to detect a range of failures, such as overheating or fire among its parts, failure of its tool or storage elements, and any other reasonably self-detectable failure. It will not always be possible to accurately self-detect every failure, but every effort shall be made to ensure that a machine or machine part defect that may be hazardous to proximate humans or property does not go undetected. This is analogous to the responsibility commonly expected of a driver of a human-operated motor vehicle to ensure that a vehicle is being operated in safe conditions, a fleet operator shall be diligent about the condition of the PMRs in that fleet.
Notification procedure	1	0	The self-detection system shall operate by including its status string in the breadcrumb message (**Table 4**) and in the JDR storage (4448-20).[57]
Shutdown procedure	1	0	If a shutdown decision is taken, its execution shall be made safely, swiftly and, where possible, by the PMR locally using one of 4448-16, 5.21 or 5.2.2 as appropriate. If it is not possible to take this decision locally then it shall be taken safely and swiftly by the teleoperator and executed in the same way. If it cannot be taken locally and cannot be taken by the teleoperator, then 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.
Move away procedure/rules	0 or 1	1	We could use one of 4448-16 5.2.1 or 5.2.2 or the Pullover procedures defined in 4448-7.

4.5.1 Fire Safety[58]

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 food, or carry flammable fuels additional risks may be incurred.

[57] We need to specify a list of "reason codes" for self-detected failures. These codes must be vendor and operator independent.

[58] Adopt other vehicle fire standards where possible. Identify suitable pass-fail criteria.

4.5.2 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. These systems may involve detecting odours, excessive heat, deformities in the battery, or other methods.

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

The battery casing of PMRs shall be designed to minimize the probability of the metal housing being breached and causing a fire.

A PMR power supply shall not be permitted to fall below 10% [?] remaining power or fuel regardless of its energy type.[59]

A PMR energy management system shall not permit it to be drained of energy during a roadway crossing in.

4.5.3 Engines and Motors

PMRs shall meet the noise and emissions requirements defined on each path segment that it traverses (see 4448-2).

Any PMR that releases combustion emissions shall meet the emissions requirements of other motor vehicles in the jurisdiction of operation, scaled by size.

A jurisdiction may create emissions requirements specific to PMRs, but these are beyond the scope of 4448-16.

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

4.5.4 Mechanical Safety

For the circumstance of a power failure, PMRs shall be equipped with fail-safe brakes. Stopping shall not rely on means of internal friction or traction or battery-state of charge (UL 3300 8.8). This prevents a PMR that loses power on an incline from becoming an uncontrolled projectile. (PMRs shall also have a brake release capability, allowing them to be moved by law enforcement personnel or systems. (See 5.5.)

4.6 DEVICE Safety: Task component safety

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. At all times, such extensions or tools shall remain within the designed radius of those extensions or tools, they shall remain securely attached to the PMR, and their operating radius shall be correctly understood by the PMR

[59] A 10% margin admits that unforeseen circumstances could easily bring a power system below that safety margin. We need confirmation that 10% is the right number. If 5% is enough five-nines, then 10% may be inefficient. And if traffic and navigation uncertainties mean that 10% is not enough, then this needs to be reconsidered. In the end, a fleet operator that does not pay close attention to this problem, given that these devices are out in public spaces, without human accompaniment means that such operators will have to understand this problem related to their ODD. As a professor once told me: "you can design for fools, you can design for damned fools, but you can't design for goddamned fools."

navigation algorithms. The physical extent of all such extensions or tools shall be included in all shyDistance calculations.

4.6.1 Dangerous Goods Storage

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).* Any PMR registration regime shall include an appropriate demand or assurance of this compliance.

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. The 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 and for 30 minutes in the event of fire.

4.7 DEVICE Safety: Electronics safety

PMRs will need to be able to function in a variety of temperature and weather conditions. Their electronic systems shall function within the 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 planned ODD to ensure they can safely operate.

Temperature range: all 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

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 minimum effective IP rating of IP66 — the highest IP rating.

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

4.8 DEVICE Safety: Failure recovery systems

A PMR shall be able to recover from (respond to) any failure in a way that minimizes the probability of harming humans, property, or itself, in that order. To *recover from* a failure does not imply that the failure can be self-repaired by the PMR. To recover from a failure means that a PMR takes the best possible course of action technically available to it in the circumstance. That means that some PMRs will only be able to report failure and possibly shut down, while others may be able to exhibit more self-recovery behaviors. The capability of *recovery from failure* is expected to improve as PMR technology matures.

Table 7: a PMR, possibly in conjunction with its teleoperator, shall be able to recognize classes of failure, notify the right parties in the event of failure, shutdown safely and, when physically possible, move out of the way safely.

Capability	Measure	Tolerance	Comment
Failure categorization	.99	0.01	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 machine proper. Failures would be distinguishable by the PMR, *or its teleoperator* without a human agent physically present at the PMR. This ability is critical to minimize contingent harm and to maximize recovery success.
Notification procedure	.99	0.01	A PMR shall be able to correctly decide who to notify in the event of a failure. One critical decision is whether to notify only its teleoperator or to notify both its teleoperator and the relevant emergency authority. *The FM needs to inform the OM because PMR failures impact the schedule that the OM is managing. Note that the PMR is not connected to the OM.* For example, a PMR, with a low battery only needs to inform its teleoperator or FM, and proceed to solve that issue, while a PMR that has been tipped over in an intersection, has to notify both its teleoperator and an emergency authority.[60] The FM of a PMR that is disabled shall also inform the OM for scheduling reasons.
Shutdown procedure	1	0	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.
Move away procedure/	1	0	A PMR shall be able to correctly respond to any circumstance in which it must move away from its current position or

[60] A longer list should be provided here, for certainty.

rules			change course significantly (e.g., request to be rerouted). This may be in the case of an emergency in which it should evacuate its current location, in the case of making space for humans to pass by, or any other similar circumstance.

In all cases, it is sufficient for a human teleoperator to detect, identify, and resolve all breakdown procedures.

4.9 HUMAN INTERACTION Safety: Communication Safety

This paragraph 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.

Table 8: Elements of communication safety cover all safety related communications that are transmitted by radio. This table does not include analogue communications from PMR to human such described in 4448-8.[61]

Capability	Measure	Tolerance	Comment
PMR to emergency services	1	0	A PMR shall be able to signal local emergency services whenever such a signal is justified (see paragraph 4.8). This signal must be without lag, and must be secure from cyber-attack. The same signal shall be concurrently communicated to the PMR teleoperator.[62] It is appropriate for an emergency signal to be routed through the PM auto operator to local emergency services, but this shall not incorporate lag or error.
PMR to teleoperator	1	0	The connection between teleoperator and PMR 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 (0).
PMR cyberattack (4448-3)	1	0	In the event of a detected or suspected cyber-attack, whether detected or suspected at the PMR, or by its teleoperator, a PMR shall execute a complete machine breakdown procedure.
PMR in a telco blind spot	1	0	It is possible, given an agreement between a teleoperator and a PMR that a PMR may continuously operate in a telecommunications blind spot for a pre-agreed period of time. This time should be very short, but is not constrained by this standard. It may vary according to circumstances that

[61] Communication safety could encompass more than human-PMR interactions to include PMR-to-PMR communication (currently out of scope). In future, "many PMRs from many operators" would benefit from an agreement on a direct PMR-to-PMR protocol and vocabulary. This is something to be considered later.

[62] We need a body of universal emergency codes. This would start with existing codes used for motor vehicle emergencies. Source?

Capability	Measure	Tolerance	Comment
			may only be understood by the fleet operator. 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, but 4448–16 is silent. Under no circumstance, can a PMR enter a traffic intersection if the communication between teleoperator and PMR is not operating, or is uncertain to remain operating during the crossing.
Loss of communication	1	0	Any loss of communication beyond __10__ secs, or beyond a predetermined agreement between a teleoperator and a PMR (whichever is greater) shall trigger the execution of a machine breakdown procedure and the appropriate recovery procedure. Refer to bread crumbs (see 4.2.1)

4.9.1 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. PMRs 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. There may be reasons to use the same telecommunications provider for orchestration as for teleoperation, but that decision is not constrained by this standard.

4.9.2 Data Transmission Protection

Data protection and resistance to hacking are described in 4448-3.

4.9.3 Help Button

A PMR shall have a help button in the case 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 in a simulation.[63]

[63] @lee, this is too prescriptive! And this needs careful consideration for **false alarms**... 50mm seems large for a help / emergency stop button for a small PMR. (if this stays in, we must consider: easy to find, see if 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*

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 was one of them, where they have to be a specific size and configuration, that may be unsuitable for many PMRs). 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. And it will not be enough simply to talk about the size and position of such a button, but we must consider circumstances of its abuse. One of the examples mentioned was that as a prank someone might strike the button while passing a PMR in a crosswalk, possibly causing the robot to simply halt in the middle of a road crossing.

This particular problem is easy to describe in the pages of a standard, but before we specify a help or emergency button, it will be important to ensure that we introduce no unintended consequences. In my opinion, this single matter is so important, and its unintended consequences so insidious and complicated that it 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. Hence, I propose a "Standard for Halting and Securing Public Mobile Robots and Social Robots.

4.10 HUMAN INTERACTION Safety: PMR-to-Human communication reliability

PMRs shall use a variety of visual, auditory and gestural cues to indicate their actions and intentions to proximate humans in the shared public pathway. This paragraph enumerates the minimum-required reliability of the *equipment* used to generate **light**,[64] **sound, haptic** and **gestural** signals. These signals and communication details are described in detail in ISO 4448-8. In this part, 4448-16, we need to be certain that whatever is required for that communication is reliable (failsafe).

Table 9: Measures of the radius within which signals for proximate human can be received.

Capability	Measure	Tolerance	Comment
Distance from the center of a PMR from which a sound can be heard	5m	0.5m	This assumes that humans within this distance have a normal range of hearing unaided by hearing aids. Any such human for which this is not true, would necessarily have to rely on hearing aids, or the PMR's light, gestural or haptic signals. Any test for this capability must assume that the sound generated will accommodate the then-current ambient noise level. This means that the sound must be heard clearly within the required distance in very noisy environments, but not very much further in very quiet environments, in order to avoid noise pollution.

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?

64 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." The latter has been done 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.

Capability	Measure	Tolerance	Comment
Distance from which a light display can be seen	20m	2m	This assumes that humans within this radius have normal vision, possibly corrected with glasses or contact lens. Any such human for which this is not true, would necessarily have to rely on the PMR's sound, gestural, or haptic signals. Any test for this capability must assume that the light levels generated would accommodate the then-current ambient light levels. This means that the light must be seen within the required distance in very bright environments, but must not be excessively bright ("blindingly bright") in darker environments, in order to avoid visual obstruction of other environmental elements.
Distance from which a gestural display can be seen	5 m	0.5m	This assumes that a gestural display might not be observable by a human situated more than 5 m away.
Height from which a gestural display can be seen	1m-3m (range)	0.2m	This assumes that a gestural display might be viewed by a person sitting low in a wheelchair, or a person sitting very high in the cab of a heavy goods vehicle. Gestural displays assume that the human viewing it has a normal range of sight, possibly corrected with glasses or contact lens, and that that person is visually focussed on the PMR.
Radius, within which a haptic signal can be received	10m	1m	It is assumed that haptic signals would be broadcast locally to smart phone apps for those who require the signals — especially a human with both hearing and vision problems. 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. This standard recommends against this approach and recommends restricting haptic signals via mobile phone apps.

4.10.1 Visual Signal Components

PMRs shall have a series of lights and reflectors in order to be visible to other users, aid the detection capability of its cameras, and signal its actions.

At a minimum, a PMR shall have these minimum visual signal devices:

- Brake lights
- Turn signal lights

- Flag (for short-stature PMRs)
- Illumination visible from all directions
- Reflectors visible from all directions
- Any light(s) defined as required for PMR-to-human social communication (4448-8)

Uniform visibility distances are defined for walkways, 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 10: Lists the requirements for each type of visual signal device

Capability	Measure	Tolerance	Comment
Brake light visibility[65]	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 heavy fog. (See bike rules)
Brake light visibility walkway	25m	10%	See stopping distance for bicycles as the critical operating constraint. [66] 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 (walkway, bikeway, roadway)	Same as brake	50% (i.e., 12, 30, 60m, respectively)	Turn signal brightness is subject to all of the same issues as brake light visibility, except at half the distance, hence tolerance is 50%
Flag[67]	Same as brake	75% (i.e., 6, 15, 30m, respectively)	The purpose of a flag is to be seen above the level of 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 the purpose of its lights. It is the case that at intersections PMR safety needs to be maximized as motor vehicles are turning. One example is the visibility of a PMR in the rear-view or side mirror of a motor vehicle that is

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

66 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 (walkway, bikeway, roadway) https://bicycles.stackexchange.com/questions/15572/what-is-the-braking-stopping-distance-for-bicycles

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

Capability	Measure	Tolerance	Comment
			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. It simply indicates there is no angle at which any required illumination would be invisible. E.g., if illumination is used to transmit a PMR-to-human signal, then that signal illumination would be visible, regardless of the angle in which the human is observing.
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 would be visible, regardless of the angle in which a human is observing. 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 would only apply to a pedestrian if they were carrying a light-emitting device. A 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 the left and right of the direction of PMR 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.

4.10.2 Auditory Signal Components

Auditory signals are used by a PMR as one means to indicate its intentions and actions to proximate humans on or near the PMR's pathway. (These signals are detailed in 4448-8.) It is important that these auditory signals are loud enough to be heard by nearby pathway users over the current ambient noise level but not so loud as to be a nuisance.

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

- Clearly audible in all operating ambient noise conditions (up to a defined level) for normal human hearing 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 the recommended levels in this paragraph with stated permission from the authorities within a security jurisdiction.
- Care shall be taken not to harm non-involved, proximate humans.
- In all cases, the loudness of auditory signals shall not exceed 120 DB.[68]

- Harmless to normal human hearing from a distance of 1 m.
  - It shall not be set higher than 85 DB,[69] unless in a setting wherein proximate humans are required to wear hearing protection.
- Repeated at least twice in any circumstance in which ambient noise conditions vary and may occlude sound.
  - A PMR may repeat an auditory message twice in the event it does not understand the ambient noise conditions.
- Repeated continuously once every 10 seconds, given 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”

Table 11: Loudness levels of PMR auditory signals

Default loudness	Minimum loudness	Maximum loudness
A loudness level of 70 DB shall be used in the absence of ambient noise measurement. This level carries the risks of [1] being inaudible on louder than average streets and [2] startling a human in a very quiet environment.	12-15 DB[70] above current ambient.	The minimum of 20 DB[71] above current ambient or 110 DB[72] maximum whichever is lower. (120 is damage threshold.)

[68] This is redundant with table 12. 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.

[69] 85 DB is the level above which hearing protection is recommended.

[70] 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

[71] 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."

[72] 120 DB is the level above which hearing can be damaged.

The **sound spectrum** used to project the auditory signal used by a PMR shall be _____.[73]

If a location is known to experience an ambient noise level above 110 DB (excepting emergency sirens), a PMR shall not operate there without jurisdictional authority accompanied by appropriate safety precautions in consideration of its inability to satisfactorily broadcast auditory signals.

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. In other words, the 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.

4.11 HUMAN INTERACTION Safety: Emergency compliance systems

This standard assumes that a PMR fleet is operating in a defined ODD under the authority of a jurisdiction. The governmental body is expected to have reserved to itself the authority to direct any plurality of PMRs or PMR fleets away from any emergency incident or area without notice.

This sub-paragraph relates to occasions on which an authority requires a PMR or PMRs to leave or avoid a pathway, a set of pathways or an area.

There shall be a protocol agreed between the governmental authority (licensing authority), and PMR fleet operator(s) such that the emergency instruction can be forwarded to, then received and acted on, by these fleet operator(s). Such a protocol is defined for a jurisdiction that is using an orchestration system (4448–5), but is undefined for a jurisdiction not so equipped. In this latter case, such a protocol would be provided outside of the scope of the standard.

This emergency instruction with its spatial and temporal time constraints shall be delivered to the affected PMR(s) as follows:

- In the case of an operational orchestration system (4448–5), this instruction shall first be delivered to the regional orchestration system and forwarded from there to fleet operators then onward to the appropriate PMRs. This shall be done so that PMRs can respond within __60__ seconds of the original instruction.
- In the event that the ODD is not under the management of an orchestration system, this instruction would be delivered to each PMR fleet operator independently followed by onward distribution to its PMRs. This shall be done so that PMRs can respond within __300__ seconds of the original instruction.
- No PMR under emergency instruction shall exceed any behavioural rule, except to proceed to its instructed destination, or state.

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, paragraph 4.12 shall govern the activity of seizure.

4.12 HUMAN INTERACTION Safety: Seizure compliance systems

This standard assumes that a PMR is operating in a defined ODD under a jurisdictional authority. On that basis, a government should have authorized personnel that may direct a PMR away from any area,

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

disturbance, event, incident, pathway etc. Any of these compliance actions that cannot be performed autonomously shall be performed or caused to be executed by a teleoperator.

Failing the ability or willingness of the teleoperator to execute any lawfully demanded action, this sub-paragraph relates to occasions on which an enforcement or emergency authority requires a PMR to halt, change course, shut down, evacuate from or to a location, follow emergency personnel, unlock a secure compartment, or surrender to emergency personnel. It assumes that 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 the PMR storage bay
- collect a fee for the return of the PMR to its owner
- retain the PMR as evidence in a crash or for a crime

It is outside of the scope of this standard, to describe how any of these actions shall be taken, rather the standard says there shall be a body of such actions defined by the governing authority and understood by the fleet operator. This agreement should be part of the licensing arrangement.

It shall be up to the governing authority to train its staff and to have the appropriate equipment and 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.

5 Safety-related Emergency Procedures

This paragraph describes what the PMR must do when operating within its ODD and without immediate teleoperator oversight. The teleoperator may be "on call" but not currently attentive. This may be considered behaviourally equivalent to SAE J 3016 "Level 4."

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

5.1 Classes of Emergencies/Breakdowns

A breakdown is an event from which a PMR cannot self-determine a way out (within a short wait[74] defined by its operating software), unless there is a change in the event.

- Machine fail (includes drained battery)
- Major vandalism
- Fire
- Seizure (police, theft, vandal) [75]
- Telecommunication failure
- Trapped

Table 12: 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.
Minor vandalism	10 sec	2 sec	The extra time is for certainty of the necessity to declare a breakdown.
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.

[74] Such waits must be listed. For example, a PMR must report an on-board fire without lag, but not report a trapped state until a short time is passed in the possibility of a self-resolution (precipitating a false alarm).

[75] A PMR under seizure in a public space (regardless of the reason) shall not resist. To resist a police arrest would likely become equivalent to "resisting arrest." Resisting theft or vandalism, would likely risk increased harm to the PMR. In fact, resisting seizure risks collateral harm to proximate humans, depending on the nature of the resistance (consider a PMR similar to Boston dynamics, Atlas robot). It makes sense for a PMR to record the event of a seizure, for later analysis. A decision to "play dead" which would mean to simply lock down and go silent, or to unlock and go silent (protect the JDR in either case). [Advisory: 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, thereby encouraging a higher volume of petty theft.]

Event	Response	Tolerance	Comment
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 breadcrumb algorithm (**Table 4**), so it falls on the teleoperator to decide recovery, rather than the PMR.

5.2 Machine Breakdowns

There is a distinction between Partial Breakdowns and Complete Breakdowns. 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 inoperable, such as being struck by a motor vehicle or being tipped over.

5.2.1 Partial Machine Breakdown

In the case of a partial machine breakdown, a PMR has detected a breakdown that has rendered it unsafe to continue unimpeded operation or will disable it in the near future. In this case, the PMR shall perform the procedure PathwayPullover or AuxiliaryPullover depending on whether the breakdown occurs on a footway or bikeway (both defined in 4448-7).

5.2.2 Complete Machine Breakdown

In the case of a complete machine breakdown, a PMR has detected a breakdown that has rendered it unable or unsafe to move. In this case, the PMR shall perform the procedure ImmobilizedAlert as defined in 4448-7.

5.2.3 Journey Data Recorder (JDR)

A journey data recorder is defined in 4448-20 to ensure 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 that its JDR is operating correctly and that its data is being captured
- confirmation of correct operation included in its bread crumb message (**Table 4**)

5.2.4 Recovery of a PMR

Recovery of a PMR has several meanings. Resolution of a breakdown may take any of these principal forms: [76]

1. recovery of telecommunication failure or error
2. over-the-air update of software or map

[76] A full list of breakdowns will be provided here, and each will be given a code that shall be used in the JDR.

3. use of PMR-to-human communication to recover from vandalism
4. use of PMR-to-human communication to recover by asking a proximate human to help
5. send an emergency service to extinguish a fire
6. send an emergency service to seize a PMR
7. send a human to repair a PMR
8. send a method to remove the PMR to another location

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 in the JDR (4448-20)
- to record the time and place of resolution in the JDR (except if a PMR is destroyed/disposed)

The fleet operator shall make the following decisions:

- when to declare a breakdown
- the precise definition of the initiation of a breakdown
- which resolution to assign to a breakdown
- when to contact emergency services

Not every breakdown implies a simple, single recovery step. 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".

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

5.3 Vandalism

A PMR shall be permitted, for purposes of self-protection (and the owner's property protection), to record and retain any 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 video data in public spaces.

A PMR shall be able to perceive its surroundings for navigation purposes. This almost certainly includes image capture, even in the case of full teleoperation ("SAE automation 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 this latter use (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.

According to the determination of such 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.[77]

- Default rules regarding data capture for security are found in 4448-3
- Default rules regarding data privacy are found in 4448-17

[77] There almost always exist privacy laws including matters of data retention appropriate to the operating jurisdiction. Local agreements should endeavour to follow these wherever possible and not to add new rules to this complex issue. We can add a passage to 4448–3 because of its relationship to security.

- Default rules regarding data retention are found in 4448-19

Some PMRs may have 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.

This is the minimum standard.

There is an important caution. An PMR may in its travel process also capture other images, sounds, or activities that are unrelated to the PMR or to vandalism to the PMR in question. Depending on the capability of a PMR's imaging system(s), wholly unrelated activity from some distance might be captured. In this case, locally-prevailing laws regarding data captured by systems installed in public spaces shall apply.[78]

5.3.1 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 (in the sense of 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 the Orchestration Manager
- be permitted to retain any recording of the incident including a recording of proximate, involved humans

5.3.2 Partial Vandalism Breakdown

A partial vandalism breakdown occurs when vandalism results in a partial machine breakdown. In this case, a PMR shall:

- perform the procedure defined for Partial Machine Breakdown in section 0
- be permitted to retain any recording of the incident including a recording of proximate, involved humans

5.3.3 Complete Vandalism Breakdown

A complete vandalism breakdown occurs when vandalism results in a complete machine breakdown. In this case, a PMR shall:

- perform the procedure defined for Complete Machine Breakdown in 5.2.2
- be permitted to retain any recording of the incident including a recording of proximate, involved humans

[78] Cameras on PMRs, as compared to stationary cameras will considerably extend the space of public space surveillance. Governing jurisdictions may seek to limit the use, retention and potential abuse of such captured data. Specifying such constraints is beyond the scope of this standard.

5.4 Fire

Three types of fire are identified in order to distinguish differential 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 the guidelines for the type of fire (see subparagraphs).

Removal: how, and how quickly the subject PMR is to be removed (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.

5.4.1 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 employ the procedure EmergencyFire defined in 4448-7.

5.4.2 Battery Fire

Battery fires pose a unique challenge as they can potentially be very 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 employ the procedure EmergencyFire defined in 4448-7. It shall signal to the public and emergency responders using the signal *EmergencyFireBattery*. Emergency responders shall be trained on how to identify the *EmergencyFireBattery* signal.

5.4.3 Contents Fire

Containment: how the fire is extinguished. This should follow the guideline for _____ (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.

5.4.4 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

5.5 Stop and Seizure

This paragraph is included in the standard 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 a PMR. There shall be at documented method for law enforcement to carry out this task in a secure and reliable fashion. Such methods require awareness, training and equipment readiness.

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[79]
- Be able to demand that the assigned teleoperator cause the PMR to halt by way of an agreed telecommunications method. This requires:
  - ***uniqueDeviceID*** to be clearly visible on at least 2 surfaces of the body of the PMR
  - a direct, emergency 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 proximate human
  - 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 freeze 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:[80]
  - 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)[81] (that will likely cause unnecessary damage)

---

[79] See ~~what Waymo is doing with police department in Chandler, Arizona. AV is able to respond to police gestures / sounds. Might be good parallels to apply to PMRs~~. (We have to consider compute power and energy requirements. Hence "necessary and sufficient" are our guideposts; we have not included this requirement. However, 5.5, with respect to a teleoperator response.)

[80] Any of these solutions may be defeated by an ambulatory PMR, especially one with arms. So, such early thinking will become inadequate in a few years. Every ISO standard is reviewed in three then five years...

[81] Many legged robots will be self-balancing, making it difficult to tip them over. Tipping should only be used as a last resort, because it is likely to cause damage unnecessarily.

5.5.1 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 mobile power.

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 enjoyed by the local public safety and enforcement authority

5.5.2 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.

5.6 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 the Pullover procedures defined in 4448-7.

6 Safety-related Reliability Certification

Here we need a necessary and complete checklist with reference to respective parts of 4448 for details. We will recommend that each element on this checklist be certified by the maker or operator of a PMR. We need to say that "there shall be" a method to confirm the veracity of the maker's or operator's assertions, and that "there shall be" a form of consequence for misleading the certification process and for restitution in the event of a safety or security failure due to such actions. 4448-16 can outline methods of such confirmation.

There shall be a formal method to certify the safety and reliability of a PMR operating in a public space. The parts of ISO 4448 to be incorporated in this certification are:

6.1 4448-3 for reliable communications and cybersecurity

TBD

6.2 4448-7 for the ability to follow the "rules of the road"

TBD

6.3 4448-8 for the ability to use all required sounds and signals

for PMR-to-human communications

- 4448-16 in regard to all device components that may impact safety and be subject to wear, fatigue, or obsolescence
- 4448-16 in regard to all software updates and expiry rules set by manufacturer and understood by the certification authority.

6.4 4448-20 for the operation of a journey data recorder (JDR)[82]

TBD

6.5 Certification NOTES — TBD

An operating hour is an hour during which a PMR is turned on and loading, waiting or moving. To be reliable for a particular jurisdiction a PMR shall be certified for:

- ***MTBF_CB*** operating hours for Communication Breakdown
- ***MTBF_PMF*** operating hours for Partial Machine Breakdown
- ***MTBF_CMF*** operating hours for Complete Machine Breakdown

MTBF_CB is dependent on the local communication infrastructure.

Each of these three need a default, and a tolerance.

How does this apply to:

- Footway use
- Bikeway use

[82] Winfield, A., van Maris, A., Salvini, P., Jirotka, M. (2022) An Ethical Black Box for Social Robots: A Draft Open Standard https://arxiv.org/pdf/2205.06564.pdf

- Roadway use

Should this be the same for all PMRs?

Potentially we might want to hold footway, cycleway and roadway use to differing standards. [e.g., we might want to consider how an entire network is disrupted. A sidewalk or road getting blocked may not be a problem if many alternative routes are available.] A PMR breaking down in a bikeway would likely be much more disruptive (to cyclists) due to the nature, use, speed, and momentum of bike infrastructure (compared to a PMR breaking down on a footpath disrupting pedestrians). Of course, that would depend on the width of the footpath, and whether or not pedestrians were using a wheelchair. I tend toward a clear guidance that applies to both bikeway and footway. The existing users of footways and bikeways should not experience diminished access to their respective infrastructures. Sharing this infrastructure is one thing, losing access is entirely different.

Where should we put tests with respect to collision safety, say if someone runs into a PMR? [in 4448-18]

Here follows a LinkedIn conversation between Bern Grush and Tobias Kretz PTV

Week of 2023 03 06: (I'm not sure how to document this or if I should. It adds some weight to the meso planning table.

BG: I am trying to understand the buffer distance approaching sighted pedestrians need to be visually aware to avoid oscillating back-and-forth while negotiating opposite-direction passage on walkway. (Relates to cell phone distraction). You seem to understand this.

TK: You mean in reality or in a particular model of pedestrian dynamics?

BG:

My problem is "in reality", but I am drafting an ISO standard, so I have to think about "models". I am trying to define the minimum sensor-perception envelope required for a public mobile robot (PMR) moving in pedestrianized space. (Common examples of PMRs are delivery or surveillance robots moving on sidewalks, but there are many more types and places than those.)

Industrial Mobile Robots (IMR) operating in factories and warehouses have two key levels of planning. Macro planning sets out the general plan for an entire journey, including any task embedded in that journey ("From A, go to B, pick up object X, take it to C, return to A"). Micro planning deals with the close-up, cm-x-cm, or metre-x-metre, execution of that journey ("there is an unplanned object 600 cm ahead, turn 19° to the right to go around it").

In structured environments (factory, warehouse, farm field) careful pairing of macro and micro planning are generally sufficient for a navigation problem-solving approach. Once you move a mobile robot into an unstructured space, such as sidewalk, bike lane, or parking lot, a robot with a detailed micro planning capability that extends only a metre or two, is extremely nearsighted, and micro-planning at longer ranges becomes explosively expensive very quickly.

It can very easily occur that something happening 10-20 m ahead might require a modified macro plan, but the PMR won't determine that, until it is much closer, and this can lead to "traps" in which a PMR comes so close to a barrier, that it becomes very hard for it to reverse course or otherwise extract itself from the problem. A robot can become stranded. (e.g., it becomes entangled in a group of 20 people waiting at a bus stop.)

What I'm looking to define are the requirements for a level of planning (meso planning) that permits a PMR to begin rough planning out in front of its micro plan, far enough ahead to dramatically reduce the probability of becoming trapped, but not so far out (and also without fine detail), as to become computationally unaffordable. Basically, we want the PMR to estimate far enough ahead to confirm a very high likelihood that the current macro plan remains sustainable. The answer is related, of course, to speed, visibility, the ability of the PMR to change course, and several others.

So, I turned to you a suggest a minimum distance related to the distance that an able-bodied, fully-sighted, attentive, adult pedestrian, without children in hand, would use in anticipating oncoming pedestrian traffic on a sidewalk, without bicycles, on a clear day, so that said pedestrian would never find herself having to oscillate left and right, trying to negotiate passage on a narrow sidewalk? Would you venture a proposed distance? Everything goes up from there!

By the way, the distance used today by our primitive PMRs is likely less than whatever number you will propose and this is causing difficulties for pedestrians trying to anticipate what a PMR is about to do AND it causes a lot of non-zero jerk in PMR travel paths. Jerk should be near zero during PMR flow among proximate pedestrians.

TK:

It's an interesting question. For you to estimate the reliability of my answer: I have actually thought about variants of it for years, but it has not had a high relevance in my work of developing pedestrian simulation software.

The first value I would say comes not from my professional experience, but from my experience as an amateur runner who practiced for years in a group. At some point I became aware how large the distance is at which the group reorganises its internal distribution in case that another group is approaching in opposite direction or if it appears that another group must be overtaken. It's almost "as soon as they get into sight", 30, 40, 50 meters.

On the other hand, at a crowded festival no one reacts to someone that far away, as it means that one has to react to hundreds of people. As a variant: if you see a family member or a friend 100 m away on an empty field or hill, you would recognise them, if they are part of a crowd (but still visible in geometric terms) there is only a small chance. In terms of photons which reach the eye, it's the same amount of information in both situations. However, obviously, we are not able to scan for a familiar person in a crowd of strangers as effectively as we can when they are in an inanimate environment. People occlude people from the mind.

In our simulation software we have two cut-offs for interaction between pedestrians: the number of people taken into account and the distance. The default values are 8 people and 15 meters (for reasons of computational efficiency, these are guaranteed minimum values for cut offs. It can happen, that more than 8 people at a larger distance than 15 m mutually trigger a change of speed). This rule of 15 m applies only to pedestrian-pedestrian interaction. Navigation planning always reaches to the next destination, i.e. in our simulation a pedestrian knows in each moment the direction of the shortest path (considering static obstacles, and as - as a computationally costly option - also crowded regions as "soft obstacles" which means that there can be very far reaching interactions between people in an aggregated - "meso" - form) to its next destination, no matter how far away it is. This means that they never can get trapped in dead-ends formed from static obstacles. A second annotation is that there can be settings where the 15 m are not sufficient and a user complains that pedestrians bump into each other. I'm not sure, if this has a relevance for reality, because the pedestrians in the simulation are quite dumb and real people in the same situation would have found a way to resolve this. Therefore, I would add: the smarter the conflict resolution algorithm is, the shorter can be the awareness distance.

The "people occlude people from the mind" thought has led to a publication:
https://www.researchgate.net/publication/310606375

The navigation method is described here: https://www.researchgate.net/publication/51916028

