An Active Safety System for Wheeled Mobile Driving Simulators

Vom Fachbereich Maschinenbau an der
Technischen Universität Darmstadt
zur Erlangung des Grades eines
Doktor-Ingenieurs (Dr.-Ing.)
genehmigte

Dissertation

vorgelegt von

Melina Sofia Lutwitzi M. Sc.

aus Mainz

Berichterstatter:	Prof. Dr. rer. nat. Hermann Winner
Mitberichterstatter:	Prof. Dr.-Ing. Günther Prokop
Tag der Einreichung:	29.11.2022
Tag der mündlichen Prüfung:	07.02.2023

Darmstadt 2023

D 17

Preface

Diese Forschungsarbeit entstand während meiner Zeit als wissenschaftliche Mitarbeiterin am Fachgebiet Fahrzeugtechnik (FZD) der TU Darmstadt im Rahmen des Projektes MORPHEUS 2.0. Dieses wurde vom Bundesministerium für Bildung und Forschung (BMBF) durch die Förderlinie VIP+ finanziert (FKZ: 03VP06090).

Mein besonderer Dank gilt Prof. Dr. rer. nat. Hermann Winner für die fachliche Betreuung dieser Arbeit auch über seine aktive Amtszeit als Professor hinaus. Ebenso bedanke ich mich herzlich bei Prof. Dr.-Ing. Günther Prokop für die Bereitschaft zur Übernahme des Korreferats und die Möglichkeit der Zusammenarbeit mit der TU Dresden im Bereich des reifengebundenen Fahrsimulators.

Bedanken möchte ich mich vor allem auch bei meinen aktuellen und ehemaligen Kolleginnen und Kollegen am Fachgebiet FZD. Eure große Hilfsbereitschaft hat maßgeblich zum Erfolg dieser Arbeit beigetragen. Besonders zu schätzen ist jedoch das familiäre Umfeld bei FZD, das auch in schwierigen Zeiten stets für gute Stimmung und Freude bei der Arbeit sorgt - danke an alle, die dieses Klima formen und fördern!

Zuletzt gilt mein Dank meinen Eltern und Großeltern für jegliche Unterstützung und Investitionen in meinen Bildungsweg, die mir die Promotion erst möglich gemacht haben.

Darmstadt, 29.11.2022.

Table of Contents

List of Symbols and Indices

Latin formula symbols:

Symbol	Unit	Description
a	$\mathrm{m/s^2}$	acceleration
$\boldsymbol{a}$	m	point of reference point set A
A	-	reference point set of true landmarks
$\boldsymbol{b}$	m	point of reference point set B
B	-	reference point set of perceived landmarks
C	-	set of correspondences
D	$\mathrm{m/s^2}$	deceleration
d	m	distance
h	m	height
i	-	index
j	-	index
k	-	index
l	m	length
l	-	index
LC	-	detection loss count
M	-	set of perceived landmarks
N	-	set of true landmarks
n	-	number
p	m	position
$\boldsymbol{R}$	-	rotation matrix
R	m	radius
r	m	range
s	$-$	score
t	s	time
$\boldsymbol{T}$	-	transformation matrix
$\boldsymbol{t}$	-	translation vector
v	$\mathrm{m/s}$	velocity
w	m	width
x	m	displacement in x direction
y	m	displacement in y direction
z	m	displacement in z direction

Greek formula symbols:

Symbol	**Unit**	**Description**
δ	rad	steering angle
Δ	$-$	difference
κ	$1/\mathrm{m}$	curvature
μ	$-$	coefficient of friction
ω	$\mathrm{rad/s}$	wheel speed
ϕ	rad	roll angle
Φ	rad	azimuth angle
ψ	rad	yaw angle
$\dot{\psi}$	$\mathrm{rad/s}$	yaw velocity
$\ddot{\psi}$	$\mathrm{rad/s^2}$	yaw acceleration
τ	s	duration
θ	rad	pitch angle
ϑ	rad	elevation angle

Indices:

Symbol	**Description**
0	initial
7	velocity of 7 m/s
10	velocity of 10 m/s
a	act
ball	ball
brake	braking
buffer	buffer zone around the workspace
c	center
con	consistent detection
cyl	cylinder
dec	decelerating
det	first detection
DS	driving simulator (WMDS)
ebf	emergency brake flag
exp	expected
fit	fitness score
h	horizontal
hred	reduced height

Symbol	Description
in	inliers
ini	initial
LCexc	LC threshold exceeded
lim	limited
LM	landmark
loss	loss
m	measured
man	manual
match	matched
max	maximum
merge	merge within line run clustering
min	minimum
MS	motion space
multi	multiple
nom	nominal
obj	object
op	operational
PZ	protected zone
r	radial
r0	range measurement of 0
react	reaction
run	run within line run clustering
s	sensor
SA	segment area
sp	sense and process
stop	stopping
t	tangential
TH	threshold
v	vertical
WS	workspace

List of Abbreviations

AGVS	automated guided vehicle system
COG	center of gravity
DS	driving simulator
E/E/PE	electric/electronic or programmable electric
EEBS	external emergency brake system
ESPE	electro-sensitive protective equipment
FDIIR	fault detection, isolation, identification and recovery
FI	fault indicators
FOV	field of view
FTA	fault tree analysis
FZD	Institute of Automotive Engineering Darmstadt
HARA	hazard and risk assessment
HAZOP	hazard and operability study
HE	hazardous events
HMD	head mounted display
IMU	inertial measurement unit
LLLPS	Lidar and Landmark Based Local Positioning System
LRC	Line Run Clustering
MC	motion control
MCA	motion cueing algorithm
MTTF	mean time to failure
ODD	operational design domain
OH	object hypothesis
PFH	probability of dangerous failure per hour
PL	performance level
PLr	required performance Level
PZ	protected zone
RANSAC	Random Sample Consensus
RH	research hypothesis
ROS	Robotic Operating System
SA	segment areas
SF	safety function
SFR	safety function requirements

SG	safety goal
SIL	safety integrity level
SOTIF	safety of the intended functionality
SRP/CS	safety related parts of control systems
TLH	top level hazards
TUDa	Technical University Darmstadt
UR	usability requirements
WMDS	Wheeled Mobile Driving Simulator

List of Figures

List of Tables

Kurzzusammenfassung

Mobile, reifengebundene Fahrsimulatoren (Wheeled Mobile Driving Simulators, WMDS) stellen ein innovatives Konzept in der Fahrsimulatortechnologie dar, das sich von herkömmlichen Systemen durch seine Unabhängigkeit von einer festen Infrastruktur unterscheidet. Stattdessen bewegen sich WMDS wie mobile Roboter ungebunden innerhalb eines vorgegebenen Freiraums, was neuartige Ansätze zur Gewährleistung der Sicherheit erfordert. Bisherige Sicherheitskonzepte ermöglichen zwar die ständige Kontrollierbarkeit eines WMDS, erfordern aber zum Schutz vor Kollisionen den Eingriff der bedienenden Person. In der folgenden Arbeit wird die Forschungsfrage behandelt, ob die ungebundene Bewegung eines WMDS mit einer ebenfalls mobilen Sicherheitsarchitektur aktiv abgesichert werden kann. Hierzu werden Anforderungen definiert und anhand dessen die Machbarkeit praktisch untersucht.

Es wird abgeleitet, dass eine aktive Sicherheitsarchitektur für WMDS zwei weitere Sicherheitsfunktionen benötigt: Eine *Arbeitsraum-Einhaltungs-Funktion*, die den WMDS zwingt, seinen vorgeschriebenen Arbeitsraum während einer Fahrsimulation nicht zu verlassen, und eine *Kollisionsschutz-Funktion*, die Probanden und Personen in der Umgebung aktiv vor Kollisionen schützt. Die funktionalen Mindestanforderungen an diese Funktionen werden in Form von erforderlichen Messgrößen und Entscheidungslogiken abgeleitet. Daraus ergibt sich ein Konzept, das die Anwesenheit und den *Abstand von Objekten* innerhalb einer geschwindigkeitsadaptiven Schutzzone um den WMDS sowie die Einhaltung lokaler, positionsabhängiger Geschwindigkeitsbegrenzungen überwacht, was zuverlässige Informationen über die *Position und Geschwindigkeit* des WMDS im gesamten Arbeitsraum verlangt.

Bislang sind keine sensorischen Systeme für diese Messgrößen für eine Anwendung für WMDS realisiert worden. Daher werden in dieser Arbeit Hard- und Softwarekomponenten untersucht, die die vorgesehenen Funktionen innerhalb der Operational Design Domain (ODD) eines WMDS zuverlässig erfüllen können. Es wird ein auf Lidar-Sensoren basierender Ansatz gewählt, um alle erforderlichen Messgrößen unter Hinzunahme von künstlichen Arbeitsraum-Landmarken zu realisieren. Die Hardware- und Softwareanforderungen werden konkretisiert, ausgewählte Sensoren in einem physischen Prototyp implementiert und Softwarealgorithmen werden vorgestellt. Schließlich wird das resultierende Sicherheitssystem in einer repräsentativen Umgebung praktisch evaluiert. Die Evaluation adressiert die *Sicherheit der beabsichtigten Funktion* unter allen denkbaren Betriebsbedingungen, *Fehlererkennungsfähigkeit* und *Robustheit gegen unerwünschte Eingriffe während des WMDS-Betriebs*. Wenn sich die Funktionen unter den schwierigsten denkbaren Betriebsbedingungen bewähren, gelten sie als geeignet für das Sicherheitskonzept.

Die Ergebnisse der Arbeit zeigen, dass die landmarkenbasierte Positions- und Geschwindigkeitsermittlung die Anforderungen an eine sicherheitsbezogene Funktion zur Arbeitsraumeinhaltung

erfüllen kann. Für die Objekterkennung kann die Erfüllung der Sollfunktion aufgezeigt werden, allerdings nur unter ODD Beschränkungen des WMDS. Die generelle Anwendbarkeit von Lidar-Sensoren für das aktive Sicherheitssystem wird mit den Ergebnissen somit nicht als widerlegt angesehen, aber durch weitere Anforderungen, beispielsweise an die Bodenbeschaffenheit des Arbeitsbereichs eingeschränkt. Durch die Erkenntnisse dieser Arbeit werden Anforderungen, vielversprechende Lösungsansätze und Testfälle für ein aktives Sicherheitssystem für WMDS bereitgestellt, die in zukünftigen Arbeiten weiterverfolgt und optimiert werden können.

Abstract

Wheeled mobile driving simulators (WMDS) represent an innovative concept in driving simulator technology that differs from conventional systems in its independence from a fixed infrastructure. Instead, WMDS move like mobile robots on wheels within a given open space, requiring novel approaches to establish safety. Previous safety concepts ensured continuous controllability of the WMDS, but required the intervention of operators to protect against collisions. The following work addresses the research question of whether the unbound movement of a WMDS can be actively safeguarded with a likewise mobile safety architecture. For this purpose, requirements are defined and based on this, the feasibility is practically examined.

It is deduced that an active safety architecture for WMDS requires two further safety functions: A *workspace compliance function* that forces the WMDS to maintain its prescribed workspace during a driving simulation, and a *collision protection function* to actively protect the test person and people in the WMDS environment from collisions. Minimum functional requirements are derived in terms of required measurement quantities and decision logics. This results in a concept that monitors the presence and *distance of objects* within a speed-adaptive protection zone around the WMDS as well as the compliance with local, position-dependent speed limits, demanding reliable information of the WMDS *position and speed* in the entire workspace.

So far, no sensory systems for those measurement quantities have been realized for an application for WMDS. Therefore, this work investigates hardware and software components that can reliably perform the intended functions within the operational design domain (ODD) of a WMDS. An approach based on lidar sensors is chosen to implement all required measurement variables with the addition of artificial workspace landmarks. The hardware and software requirements are concretized, selected sensors are implemented on a physical prototype and software algorithms are presented. Finally, the resulting safety system is evaluated in a representative environment. The design goals and the evaluation address the *safety of the intended function* under all conceivable operational conditions, *fault detection capability* and *robustness against undesired interventions during WMDS operation*. If the functions prove themselves under the most difficult conceivable operational conditions, they are considered suitable as a safety relevant function.

The results of the work show that landmark-based position and velocity detection can fulfil the requirements of a safety-related function for workspace compliance. For object detection, the fulfilment of the target function can be shown, but only under ODD limitations of the WMDS. The general applicability of lidar sensors for the active safety system is thus not considered to be falsified with the results, but limited by further requirements, e.g. on the ground conditions of the workspace. The findings of this work provide requirements, test cases and promising approaches for an active safety system for WMDS that can be followed up and optimised in future work.

1. Introduction

1.1. Motivation for Wheeled Mobile Driving Simulators

The application of advanced driver assistance systems and automated driving functions are one of the major trends in the automotive industry and have significantly increased within the last years. Thereby, a driving simulator (DS) is a versatile development tool that is becoming increasingly important.[1,2] The key advantages of DS as a validation tool are reproducibility of test conditions, hazard reduction when testing safety-critical scenarios as well as cost and time decrease by eliminating expensive prototypes.[3] The use of highly dynamic driving simulators in particular is gaining in importance, as a high degree of immersion can be achieved with these. Highly dynamic driving simulators address not only the visual, auditory and tactile channels but also the vestibular organ of the test person by performing highly dynamic driving maneuvers themselves - but only in a limited motion range.

The current state of the art in DS technology mainly comprises rail-based motion systems, as shown in Fig. 1-1. However, the size of the movement space is directly linked to the mass of the rail structure. Therefore, the costs for production and operation rise enormously as the required movement space increases. Thus, the concept reaches its limits when it comes to driving scenarios with long-lasting combined longitudinal and lateral accelerations, like a turning maneuver at an intersection as a typical element of driving maneuvers in urban traffic.[4]

A Wheeled Mobile Driving Simulator (WMDS) is a novel concept to overcome this limitation.[6,7,8] The sled-based motion system is replaced with tire based drive units, resolving the linkage between system mass and motion space. It is supplied by on-board accumulators and can therefore possibly operate on any obstacle free, planar surface. The vision is that a WMDS can be transported to and operated at different test sites, independent of fixed infrastructure. As a result, the motion representation for a specific experiment is expected to be improved by operating on a larger workspace without significantly increasing the operating costs. Compared to a rail system, the

[1] Boer, E. R. et al.: The role of DS in developing AV (2015).

[2] BMW PressClub Global: The new BMW Driving Simulation Center (2020).

[3] Schöner, H.-P.: Erprobung und Absicherung im dynamischen Fahrsimulator (2014).

[4] Schöner, H.-P.; Morys, B.: Dynamic Driving Simulators (2016).

[5] Toyota Motor Cooperation: Toyota Driving Simulator (2016) .

[6] Donges, E.: Fahrsimulator (2001).

[7] Slob, J. J. et al.: The wall is the limit (2009).

[8] Betz, A.: Diss., Feasibility and design of WMDS (2015).

Figure 1-1.: Driving Simulator at Toyota's Higashifuji Technical Center in Susono City, Japan, built in 2007. The motion range is 35 m x 20 m.[5]

mobile, compact and low-cost design promises not only to make the DS more affordable for smaller companies, but also to make the application of driving simulation more resource-efficient.

In the past, the feasibility of a WMDS has been investigated in theory[8,9] and with a physical, down-scaled prototype[10] at the Institute of Automotive Engineering (FZD) at TU Darmstadt. Two different full-scaled WMDS are currently realized in independent research projects at TU Darmstadt and TU Dresden, shown in Fig. 1-2. The concepts mainly vary by the design of the cockpit, the number of drive units and the degrees of freedom, as the TU Dresden concept comprises an additional turning table between the hexapod and the dome. The goal of the individual research projects is to validate the tire based concept with regard to the achievable immersion within test person studies. It still remains to be proven whether the demanded quality of motion representation can be achieved with such a motion system, which requires precise control algorithms and the elimination of disturbance factors caused by e.g. the tire characteristics or the ground.[11]

In addition to the indicated difficulties, the topic of *safety* is another challenge for the applicability of WMDS: The decision for a tire based motion platform transforms a previously physically guided system into an automated vehicle with theoretically infinite range of motion. It must nevertheless be ensured that this vehicle in motion neither is hazardous for the test persons within, nor for persons in its operative environment. As a result, keeping the WMDS in a safe state of motion at all times is a major safety goal. As the system is unique in design and use case compared to other mobile vehicles, there is no state of the art safety system that can be readily adopted.

[9] Tüschen, T.: Diss., Konzeptionierung eines hochimmersiven und selbstfahrenden Fahrsimulators (2019).

[10] Wagner, P.: Practical Feasibility and Functional Safety of WMDS (2018).

[11] Albrecht, T. et al.: Design and Challenges of WMDS (2021).

Figure 1-2.: Left: WMDS Design of TU Darmstadt with three wheel units. Right: Design of TU Dresden with four wheel units and turn table.[11]

1.2. The Current State of Safety of WMDS

Requirements for the safety of machinery in general are specified in various international standards and must be considered in the development of an individual safety concept. This basically requires a careful identification of any hazards, an assessment of the associated risk, a definition and implementation of appropriate risk reduction measures and verification and validation activities.[12]

In Wagner's work[10], the functional safety aspect of WMDS was investigated based on the scaled prototype at FZD. A hazard and risk analysis was performed regarding functional failures of the WMDS architecture under worst-case conditions in order to identify the highest possible risk of a WMDS. Then, it was investigated whether a safety architecture exists that achieves to reduce this risk to an acceptable level. A main result is that an external emergency braking system, which functions independently of any components responsible for controlling and executing the movement of the WMDS, is a solution to acceptably reduce the risk of uncontrollable WMDS motion due to functional failure. A safety architecture for this braking system and respective failures that require its action were derived. Although this is an important contribution to the safety of WMDS, the safety architecture created so far has weaknesses when it comes to the safe, collision-free movement of a WMDS, as it mainly provides a measure by which collisions **can** be avoided, but not yet actively and automatically **are** avoided:

First, Wagner's approach does not assess human error that can lead to collisions. The assessed hazards refer only to failures that originate from basic functions required for the driving simulation. The used procedure implies that persons do not have access to the intended motion space of a WMDS. Otherwise, manual actuation of the emergency braking system by the WMDS operators is required in the event of hazards that originate from external factors, like inattentive persons.

[12] ISO: ISO 12100:2010 - Safety of machinery — Risk assessment and risk reduction (2010).

These conditions are considered unsuitable for a mobile use of WMDS in large workspaces. If the need for action by the operators of the system in safety-critical situations is to be avoided, further protective measures are necessary to safeguard from collisions with persons or objects in the environment.

Second, the so far derived requirements for failure monitoring do not yet include a specification of the fault conditions with thresholds, which, if exceeded, require the activation of the emergency braking system. Only if these are safely specified and verified as automatically detectable by appropriate measures during WMDS operation, a collision can actually be avoided.

It therefore still remains to answer whether a WMDS can really be operated as flexibly and mobile as intended by finding an intrinsically safe protective system that safeguards from collisions under any operational conditions without the required counteraction of operators. This also includes defining the permissible operational design domain (ODD) and workspace design requirements of a WMDS under safety aspects, which is to date undefined.

1.3. Research Objectives and Methodology

The main objective of this work is to contribute to the previous work on a safety architecture for WMDS by answering the research question whether safety functions exist that can resolve the aforementioned weaknesses and enable safe motion of WMDS at any time and in any operative environment conceivable to perform driving simulations. The functions therefore must consider the regulations from applicable safety standards. The following research hypothesis (RH) is formulated:

RH1: *The WMDS with a proposed active safety architecture can conduct driving simulations under flexible, mobile conditions without its motion posing an unacceptable level of risk to human.*

Since a generally valid proof including all contingencies is not possible, this hypothesis shall be falsified in the course of the work by suitable criteria, also referred to as *falsification aspects (FA)*. If this is not successful, the hypothesis can be seen as proven. For this purpose, the reasonably conceivable operating conditions most critical to safety are assumed and an attempt is made to falsify the successful development of a suitable safety architecture in theory as well as with practical experiments. As it will be derived from the state of the art in machine safety, this development shall include:

- Adequately reducing the estimated risk to an acceptable level with vehicle bound safety functions while the highest-risk operating conditions - including hazardous behaviour of human - are assumed.

- Successfully transferring identified safety functions to a technical solution achieving the intended protective effect even under hardest conditions of the WMDS' ODD, without unacceptably reducing its availability for the driving simulation.
- Creating an intrinsically safe system by enabling a self-diagnosis that indicates faults occurring in the safety functions.

The overall methodology is illustrated in Fig. 1-3. The structure of the thesis follows this procedure. Based on the research hypothesis, there are two main objectives of this work: First, the *identification and specification of required safety functions* to achieve the intended risk mitigation and second the *evaluation of feasibility towards safety and usability with help of exemplary implementations within representative operational conditions*.

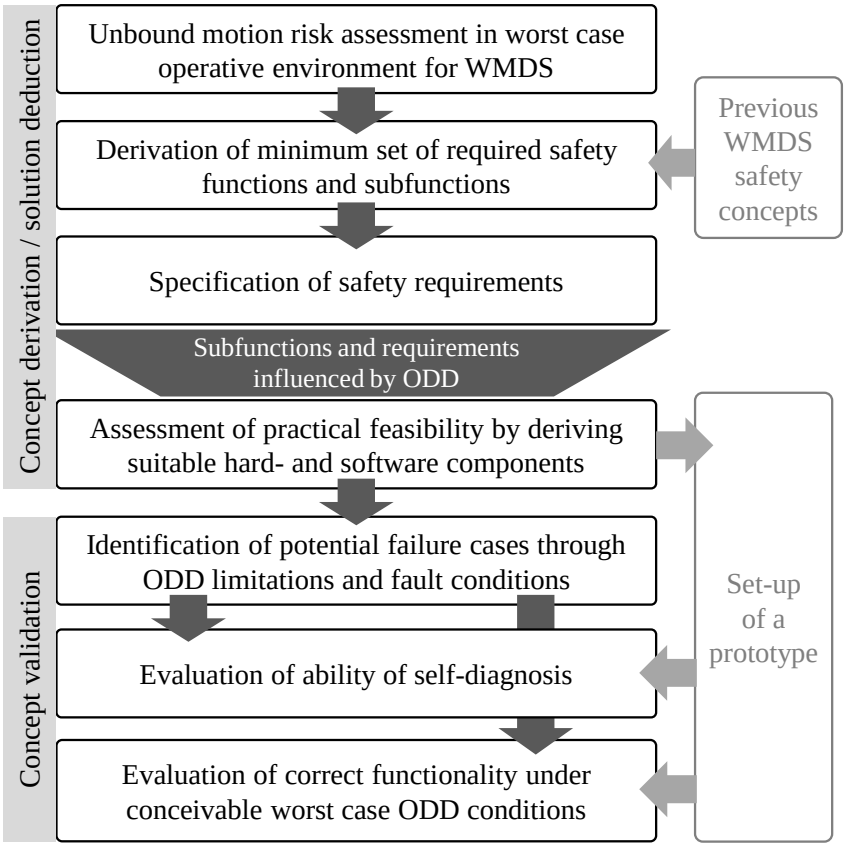


Figure 1-3.: Methodology and structure of the dissertation

The first step is to identify the risk a human is exposed to by the unbound motion of the WMDS, considering worst case conditions under flexible operation strategies, human failure and machine failure. The risk assessment procedure is compliant to machine safety standards, but differs from the procedure conducted by Wagner, as it evaluates the initial risk on an observable level, not particular failure of components. Then, safety goals required to mitigate the risk of all identified hazards are derived. Thereby, overlaps with the previous safety concept for WMDS are evaluated. This highlights the need for additionally required safety concept elements that are addressed in the further steps.

The next step is to derive a minimum set of required safety functions and subfunctions with which the intended protective effect, formulated in the safety goals, is achievable. The minimum set thereby refers to weighing up the lowest possible complexity of the safety-relevant subfunctions and the effect on regular WMDS operation. The subsequent requirement specification intends to identify criteria under which the safety functions are considered to be safe, including required measurement quantities and threshold values to be observed, requirements for the workspace design and functional safety requirements.

From this point on, only the subfunctions that are considered crucial for validation in the given ODD are considered further. It first shall be shown, that the derived functions are practically feasible by allocating the subfunctions to hardware and software components and presenting exemplary implementations that achieve the desired functionality. For the subsequent evaluation, the respective safety functions are implemented on a real prototype as a research tool.

The concept evaluation aims to assess whether the assumed protective effect of the functions is in fact achievable under any conceiveable operative conditions and that the functions are inherently safe by detecting insufficiency to perform the intended task. In a failure analysis, system states, external conditions and potential misuse cases are elaborated that are likely to cause a failure of the safety functions. This delivers boundary requirements and worst case conditions for test cases of the functions, as well as self-diagnosis requirements. The ability to diagnose identified fault conditions is first assessed by deriving fault indicators and respective thresholds. Then, it is investigated in practical experiments that the implementations pass identified test cases under worst case conditions. The strategy is here to challenge the functions on their limits, attempting to falsify their ability to correctly perform their safety-related reaction within the ODD.

The overall procedure aims to assess the feasibility of an active safety system for WMDS and to identify the conditions under which this can or cannot fulfill its intended task safely. This further defines or narrows the ODD of a WMDS under safety aspects. With an active safety system, the potential of mobile and flexible use of WMDS under safe conditions shall be further exploited. This helps to promote the applicability of the novel DS concept. Furthermore, the proven safety of a WMDS is indispensable for first studies with test persons and therefore an essential step for further real-world experiments with a WMDS.

2. State of the Art / of Research

The following subchapters summarize the state of the art and of research relevant for the understanding of this thesis. The current state of a *WMDS' basic design and technology* is described. The presentation of the relevant state of the art in *machine safety* as well as previous work on *safety of WMDS* helps to justify the further safety activities this work comprises. Additionally, a brief insight into *safety systems for other mobile vehicles* is given. The results of this chapter are used to develop the methodology for analyzing hazards of a WMDS on a system level and deriving further measures for a safety architecture that complies with the state of the art.

2.1. Safety of Machinery

The use of any technical system is accompanied with the exposure to hazards, as machine or human failure can lead to damage, injury or even death. As a result, the use of each system presents a specific risk. Since it is not possible to reach a zero-risk system, the goal in machine safety is to reduce a system's risk to a tolerable level. In the European Union, the safety of machinery and thus its risk treatment is standardized in a series of norms based on the so-called *Machinery Directive*[13a]. The machinery directive introduces harmonized safety requirements and conformity assessment procedures. It is prescribed that "a risk assessment is carried out in order to determine the health and safety requirements which apply to the machinery. The machinery must then be designed and constructed taking into account the results of the risk assessment."[13b] In order to meet the requirements of the Machinery Directive, a standardization program of so-called harmonized standards exists, which further specify its requirements. These include basic safety standards (Type A) that deal with fundamental safety design principles. Generic safety standards (Type B) deal with specific safety aspects or types of safeguards applicable to a variety of machines. Furthermore, machine safety standards (Type C) exist that provide detailed requirements for a particular machine.

Starting with important term definitions, safety standards relevant for this work are described in the following chapters.

2.1.1. Term Definitions

The following definitions are extracted from relevant safety standards, which will be presented in following chapters, as well as from thematically corresponding guides and manuals.

[13] 2006/42/EC: Machinery Directive (2006). a:- ; b: p. 12.

Safety is generally defined as the absence of unacceptable risk. It can be further described as the "ability of a system not to cause danger to persons or equipment or the environment"[14a]. In machine safety, a distinction is made between different types of safety as part of the overall safety.

Functional Safety relates to the part of safety that depends on the correct functioning of a safety-related system and other risk-reducing measures.[15] Functional Safety measures therefore determine the behaviour of a machine in case of functional failure of safety-related components.

Safety in use or safety of the intended functionality deals with the hazards associated with the intended use or expected misuse of a machine and thus refers to the parts of a machine that can be dangerous even without the presence of a fault. In this context, an intended functionality is considered unsafe if the system behavior is not sufficiently known and not safely specified.[16]

Risk describes the combination of the probability of harm occurring and the severity connected to it.[15]

Severity is the estimation of the extent of harm to one or more individuals that can occur in a potentially hazardous situation.[15]

Hazard is a potential source of damage caused by a malfunction. It can be described as a combination of a failure and its consequence.[15]

Hazardous event is the combination of a hazard and a critical operational situation.[15]

Safety Function is a measure that is intended to achieve or maintain a safe state for the equipment with respect to a specific hazardous event.[15]

Safety Goal is a top-level safety requirement as a result of the hazard and risk assessment that is assigned to a system with the purpose of reducing the risk of one or more hazards to a tolerable level.[17]

Safety Integrity is described as a system's ability to detect faults in its own operation and to inform a human operator.[14b]

Operational Design Domain (ODD) refers to "operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics."[18]

[14] Isermann, R.: Fault-diagnosis systems (2006). a: p. 23; b: p. 24.

[15] IEC: IEC 61508-4:2010 - Functional safety of E/E/PE systems - definitions (2010).

[16] Schnieder, L.; Hosse, R. S.: Leitfaden SOTIF (2019). p. 7.

[17] ISO: ISO 26262-1:2018 - Road Vehicles: Functional Safety (2018). p. 14.

[18] SAE: SAE-J3016:2021 - Taxonomy for Driving Automation Systems (2021).

Fault is an abnormal condition that can cause a reduction in or loss of the capability of a system to perform a required function.[15]

Systematic Faults are related in a deterministic way to a certain cause during the development process, e.g. a mistake in a system's specification and design. It therefore can originate from human error and can occur in hardware or software components.[15]

Random Faults only occur at hardware components at random time due to degradation mechanisms, especially in electronic hardware components. In contrast to systematic faults, a random hardware fault can be predicted with a reasonable accuracy based on the experience with a large number of the respective hardware part.[15] Examples are failure due to wear, corrosion or fatigue.

Failure is a permanent interruption of a system's ability to perform a required function under specified operating conditions. It can be seen as an event that results from one or more faults.[19]

Error is a discrepancy between a computed, observed or measured value or condition, and the true, specified, or theoretically correct value or condition.[15]

Availability describes the probability that a system will operate satisfactorily and effectively at any period of time. This respects the time until a failure or malfunction of a system occurs and the time needed for its correction/repair. Therefore, high availability can be reached by either a large operation time through highly reliable components or a high fault tolerance, or by small repair times.[19]

Fault Tolerance describes the effect that faults of a system are compensated in such a way that they do not lead to system failures.[19]

2.1.2. ISO 12100 and ISO 14121-2

The standard *ISO 12100 - Safety of machinery — General principles for design — Risk assessment and risk reduction*[20a] "specifies basic terminology, principles and a methodology for achieving safety in the design of machinery. It specifies principles of risk assessment and risk reduction to help designers in achieving this objective. Procedures are described for identifying hazards and estimating and evaluating risks during relevant phases of the machine life cycle, and for the elimination of hazards or the provision of sufficient risk reduction. [...] The standard is also intended to be used as a basis for the preparation of type-B or type-C safety standards."[20b]

The standard ISO/TR 14121-2 "*Safety of machinery - Risk assessment - Part 2: Practical guidance and examples of methods*"[21] supplements ISO 12100 with selected hazard identification and risk

[19] Isermann, R.: Fault-diagnosis systems (2006). pp. 21-25.

[20] ISO: ISO 12100:2010 - Safety of machinery — Risk assessment and risk reduction (2010) a: - ; b: p. 6.

[21] ISO: ISO/TR 14121-2:2013 - Safety of machinery - Risk assessment - Practical guidance (2013).

assessment procedures as a guide for implementing the requirements from the standard.

The basic procedure of ISO 12100 complies with the approach stated in the Machinery Directive and comprises the *Risk Analysis* by definition of the limits of the machinery, identification of hazards and risk estimation, the *Risk evaluation* and *Risk mitigation*. The *definition of the limits of the machinery* shall thereby respect:

- Intended use: including operational modes and functions, the area of application, possibilities of intervention by the user, expected skills of potential users.
- Spacial limits: including required space, the intended area of motion, interfaces to the user and to energy.
- Temporal limits: life time, maintenance intervals
- Environmental limits: including weather, temperature, sunlight, etc.

The *identification of hazards* shall include all phases of the machine's life, from development and commissioning to operation and disposal. The operation must thereby respect the operation under normal conditions as well as deviating conditions like the failure of a component, external disturbances, mistakes in construction or software design or disturbance of the energy providence. Additionally, unintended misconduct by the user must be respected, e.g. through loose of control, inattention or reflexive behaviour. A checklist is provided in the appendix of the standard, which helps to identify the hazards comprehensively. It divides hazards from their origin into mechanical, electrical, thermal or ergonomic hazards as well as hazards trough noise, vibration, radiation, material or substances. The description of a hazardous situation should include the description of the task to be executed, the type of hazard, the hazardous area and potential consequences. Typical hazardous situations stated in the appendix arise from work close to moving parts, objects with high temperature or noise, exposition towards ejected parts or work underneath a load. ISO 14121-2 recommends the combination of a top-down hazard based analysis and a bottom-up task based analysis in order to comprehensively identify all hazards. The top-down approach starts with potential harm from the hazard checklist, e.g. squeezing, collision or electrical shock, and then concludes on possible hazardous events and hazardous areas of the machine. The bottom-up approach starts with a description of any tasks that are performed in conjunction with the machine and from there concludes on possible hazardous situations and the resulting harm.

As part of the *risk estimation*, every identified hazardous situation shall be evaluated using the risk elements *severity* and *probability of occurrence*. The latter is a function of the *exposure* of persons within the hazardous area, the *probability of occurrence* of the hazardous event and the technical or human *possibilities to avoid* or reduce potential harm, for example by the possibility of escape from the hazardous area. Exemplary metrics to evaluate these risk elements can be found in ISO 14121-1. These include risk matrices, risk graphs (Fig. 2-1) or risk points. Nevertheless, the precise assessment of risk is stated less important than the systematic and holistic identification of potential hazards and the definition of appropriate risk mitigation measures.

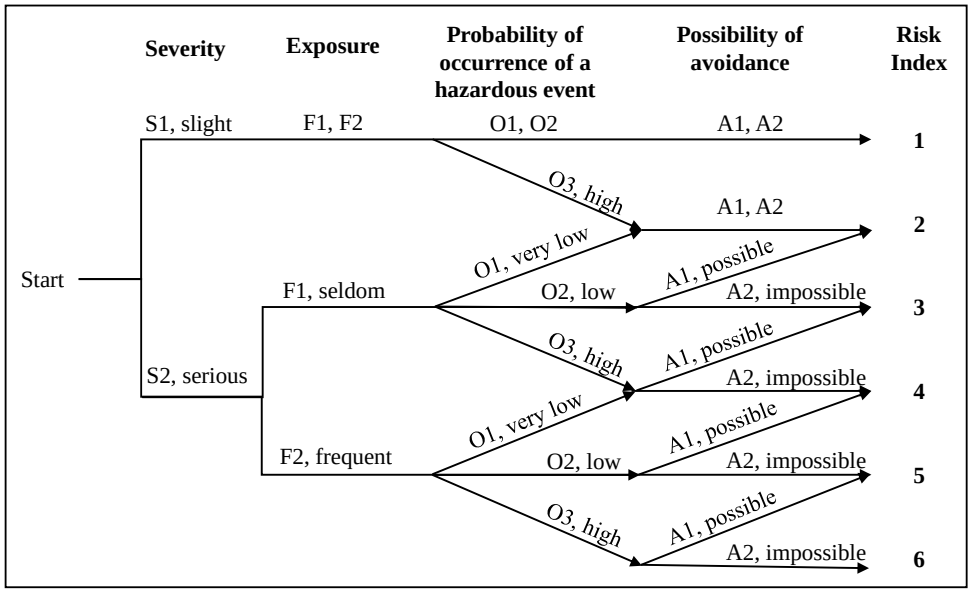


Figure 2-1.: Example of a risk graph, own illustration according to ISO 14121-2.[22]

In the course of the *risk evaluation*, it is to assess whether further risk mitigation measures are required to mitigate the risk to an acceptable level or if this level is already reached.

The process of *risk mitigation* includes a three step approach that helps to either minor the severity of a hazard or the probability of its occurrence. Therefore, the choice of a risk mitigation measure can be based on the origin of a hazard or the resulting consequence. The three step approach is to be understood as a hierarchical process and includes:

1. *Inherent safe construction:* choosing appropriate design characteristics, e.g. materials suitable for the expected loads, intrinsically safe electrical equipment, standing stability, ergonomic design or inherently safe control units.
2. *Technical protective devices:* serve to limit machine functions or detect / prevent the access of persons to a hazardous area. These include e.g. separating devices or sensitive protective equipment for the detection of approach or presence of persons in the hazardous area. *Complementary protective devices* serve, for example, to shut down the machine in an emergency, to disconnect or dissipate energy or to rescue trapped persons.
3. *User Instructions:* including signals and warning devices, markings and pictograms.

Once the risk mitigation process has been passed, the *residual risk* of the machine should be re-evaluated under the above-mentioned aspects with the inclusion of all defined measures. The overall approach is therefore iterative and can require multiple cycles. Once functions have been added to the system, new risks connected to these must be assessed.

[22] ISO: ISO/TR 14121-2:2013 - Safety of machinery - Risk assessment - Practical guidance (2013). p. 19.

Additionally, the effectiveness of a risk reduction measure must be validated to confirm that adequate risk reduction is reached in practice under any cases. This includes to consider all expected operating conditions within the ODD of a system.

2.1.3. Functional Safety

EN ISO 13849

ISO 13849-1 *Safety of machinery - Safety-related parts of control systems*[23a] is a Type B1 safety standard that addresses functional safety by design and validation guidelines for safety related parts of control systems (SRP/CS) of machines, including hard- and software. The standard applies to the design of protective equipment (according to step 2 of the risk mitigation process) that depend on a control system or other operational functions with safety relevance and therefore is included in the overall risk assessment and reduction process of ISO 12100. The main goal is to reduce the probability of failure of a safety relevant function due to random hardware faults, and to avoid systematic faults during the development. Fig. 2-2 shows the procedure of ISO 12100 and the dependencies to ISO 13849 within the overall risk reduction process.

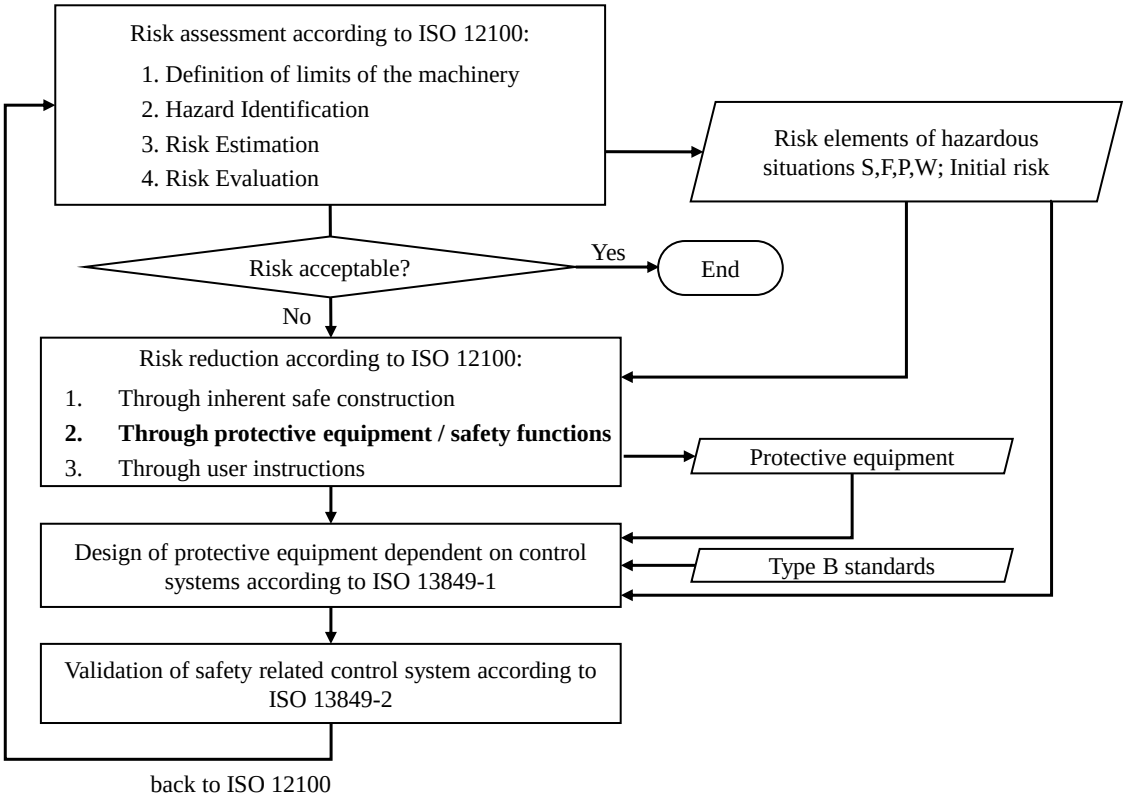


Figure 2-2.: Dependencies between ISO 12100 and ISO 13849 for risk reduction. Own illustration based on ISO 13849[23b]

[23] ISO: ISO 13849-1:2015 - Safety-related parts of control systems (2015). a:- ; b: p. 21 ; c: p. 63.

The standard uses a performance level (PL) to express the required reliability of a SRP/CS to perform the dedicated safety function, which differentiates between PL a, b, c, d and e. A PLa sets the lowest requirements on the safety performance, respectively PLe the highest. The determination of this PL is risk based and the levels are classified by the probability of a hazardous failure per hour of the safety function. For this risk evaluation, the same risk parameters as described in ISO 12100 are to be used, but special metrics that lead to a resulting PL apply, e.g. a PL-based risk graph. The risk estimation performed according to ISO 12100 must therefore not necessarily be repeated, unless other risk reduction measures have already been taken, that lead to a deviating remaining risk. The higher the risk connected to the malfunction of the controlled safety function, the higher is the required performance Level (PLr), meaning the less likely may a functional failure of this function occur.

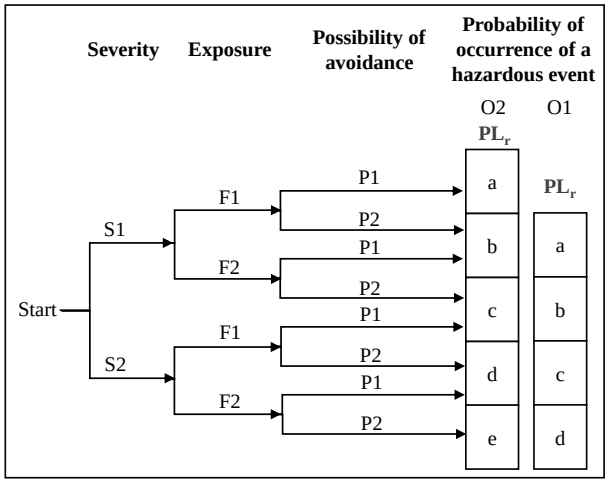


Figure 2-3.: Risk graph to determine the required performance level from risk parameters. Own illustration according to ISO 13849.[23c]

Depending on the PLr, requirements on the hardware and the overall functional structure of the safety function apply, which is specified in EN ISO 13849-1. Therefore, a safety function must first be characterized profoundly for the task to be executed. Often, the high level description of a safety function is expressed by a *safety goal*. Then, it is divided into subfunctions, which are allocated to subsystems and subsystem elements. This mostly builds a chain of action from *sensors*, to *logic systems* and to *actuators* which altogether represent the safety function. To determine the resulting performance level, the failure rate of the components as well as further structural characteristics of the function are of importance. The failure rate is expressed as a mean time to failure (MTTF) or probability of dangerous failure per hour (PFH). These values must be determined per element and then calculated to a total value of the function. The values of individual elements are specified by manufacturers, for example on the basis of endurance tests, or can be extracted from a comparison table in the annex of the standard.

For the structural characteristics, so called *categories* are introduced, which characterize the behaviour of a function under fault conditions through architectural aspects. The categories are classified as B, 1, 2, 3 or 4, with rising demands concerning the diagnosis of failures and on the

fault tolerance of the function. The structural principles of the categories, inputs from a sensor, a logic component and an output to an actuator, are visualized in Fig. 2-4.

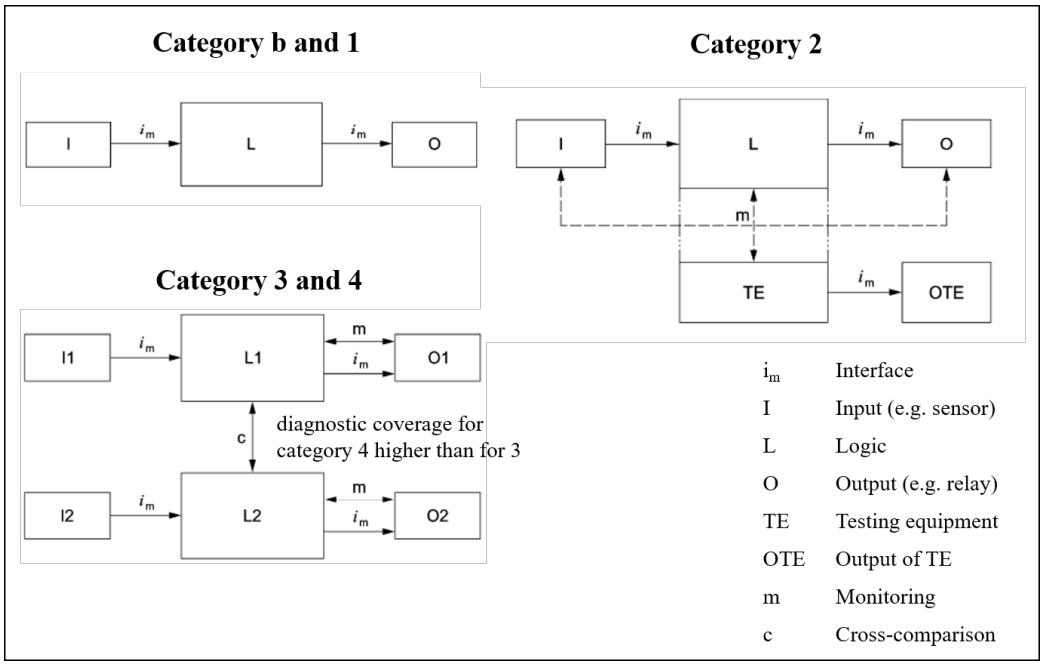


Figure 2-4.: Structural requirements of categories, own illustration according to ISO 13849.[23]

Category 1 requires no diagnostics but only the application of proven components and safety principles, with a failure resulting in a loss of the function. *Category 2*, building on the previous categories, requires a low level of diagnostic coverage through regular testing of the function by an external testing facility. The so-called *diagnostic coverage* is understood as the ratio of the failure rate of the noticed dangerous failures and the failure rate of the total dangerous failures of a function. In the event of a diagnosed fault, a *safe state* must be established, which is to be defined for the respective function. *Category 3* requires medium diagnostic coverage and a redundant structure so that simple failures are not safety critical. Based on category 3, *category 4* additionally requires multiple fault safety or diagnosis of latent faults in the system in order to detect a failure of the safety function in time. Consequently, measures to influence the performance of a safety function are the implementation of diagnostic functions to increase the diagnostic coverage or the addition of redundancies to enhance the fault tolerance.

The failure rates and the category lead to a resulting PL of the safety function, which can be determined by using tables or graphs from the standard. The resulting PL must be at least equal to PLr to adequately reduce the risk of the machine associated with the particular hazard to be protected.

The second part ISO 13849-2[24] deals with the verification and validation of the SRP/CS. Verification and validation activities mainly include analysis and tests to proof the systematic safety integrity of the developed function. The analysis activities include checking the documentation

[24] ISO: ISO 13849-2:2012 - Safety-related parts of control systems - Validation (2012).

with regard to compliance with the requirements from the standard, for example for calculating the achieved performance levels, the correctness of fault lists, circuit diagrams, software documentation, etc. Functional tests must be used to demonstrate the safety function and its correct definition, implementation and compliance with the specification. This includes verification of the functions against environment-related influences, testing of the resistance towards interference and testing of safe failures through targeted fault injection. Here, the standard mainly gives the requirement that comprehensive testing under these aspects must be done, without providing concrete methods on how to ensure proper testing.

IEC 61508

IEC 61508 *Functional Safety of electric, electronic and programmable-electric safety-related systems* does not belong to the harmonized standards in the sense of the machinery directive, but is a worldwide valid standard considered as the basic standard for functional safety. Other application-specific standards of various industrial branches (e.g. process industry, nuclear industry, automotive industry etc.) have evolved from it, as also EN ISO 13849. It applies to electric/electronic or programmable electric (E/E/PE) safety-related systems, but also sets a framework for safety-related systems based on other technologies. It follows a similar procedure as proposed by ISO 12100 and ISO 13849, but is much more detailed in terms of concrete hardware and software requirements, which is why ISO 13849 often refers to IEC 61508 for more specific requirements, especially concerning software. Overall, it consists of seven parts. IEC 61508-1[25] introduces an overall safety life cycle approach for systematical performance of the necessary activities to establish functional safety of a safety related E/E/PE system. The phases of risk assessment comply with the previously described phases of ISO 13849. Instead of the PLr, it introduces a risk-based safety integrity level (SIL) to express the target levels of safety integrity as an acceptable dangerous failure per hour for the safety functions. The relation between a PL and a SIL are shown in Tab. 2-1. The metric by which a system is assessed is a developer's own decision.

Table 2-1.: Relation between PL and SIL, own illustration according to ISO 13849[26] and IEC 61508[25].

Performance Level (PL)	PFH in 1/h	Safety Integrity Level (SIL)
a	$\geq 10^{-5}$ to $< 10^{-4}$	No correspondence
b	$\geq 3 \cdot 10^{-4}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \cdot 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

[25] IEC: IEC 61508-1:2010 - Functional safety of E/E/PE systems (2010).

[26] ISO: ISO 13849-1:2015 - Safety-related parts of control systems (2015).

2.1.4. Safety of the Intended Functionality

ISO 21448 is a standard arising from the automotive industry that describes safety of the intended functionality (SOTIF), which is ”the absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality, or by reasonably foreseeable misuse by persons”.[27a] With the ISO 26262[28], a standard for functional safety for road vehicles exists, which is derived from IEC 61508. In contrast to the issue of functional safety, which deals with systematic and random failures of safety-relevant functions, SOTIF deals with hazards caused by an incomplete specification or expected (mis)use of safety-relevant functions, which gains more importance as the complexity of automated driving functions rises. Concluding, the guideline complements the functional safety standards, since a hazard in terms of SOTIF is present when a system can still be transferred to an unsafe state while complying with all pre-specified functional safety requirements. The goal of SOTIF is to define a structured design process for avoiding safety violations caused by a faulty target function. The guideline especially applies to limitations of the intended functions that are based on environment perception.[29] ”For some systems, which rely on sensing the external or internal environment, there can be potentially hazardous behaviour caused by the intended functionality or performance limitation of a system that is free from the faults addressed in the ISO 26262 series. Examples of such limitations include:

- the inability of the function to correctly comprehend the situation and operate safely. This also includes functions that use machine learning algorithms.
- insufficient robustness of the function with respect to sensor input variations or diverse environmental conditions.”[27b]

An example is the application of sensor data processing functions in an automated road vehicle. It is possible that physical effects distort the raw data from sensors, e.g. a polluted sensor cover, which can lead to a limited detection performance. The next step in the data processing, the extraction of object data, can also lead to uncertain system states, e.g. through the use of false object hypotheses. For example, an object hypothesis valid for pedestrians cannot be applied to skateboarders due to higher speeds of the latter. Consequently, an object is not recognized as such, so that the safety-oriented reaction of the vehicle automation system is omitted in this case.[29]

The process steps of ISO 21448 include a specification of the system, a risk identification by misbehavior of the considered function as well as the user and identification of dangerous use cases and triggering events of an unintended system behavior. This is followed by risk reduction measures, which include system improvements (e.g. different choice of sensors), functional limitation of automated functions (e.g. reduction of speed), or reduction of reasonably foreseeable misuse (e.g. through HMI design). Verification is the next step and includes the proof that the

[27] ISO: ISO 21448:2022 - Road vehicles - SOTIF (2022) a: p. 1, b: p. vi.

[28] ISO: ISO 26262-1:2018 - Road Vehicles: Functional Safety (2018).

[29] Schnieder, L.; Hosse, R. S.: Leitfaden SOTIF (2019). pp. 7-16.

sensors, algorithms and actuators behave as expected in known uncertain scenarios, i.e. that the system has been implemented according to the specification. Validation, on the other hand, involves investigating whether the system is suitable for the intended application by subjecting the system to a variety of scenarios in selected test scopes and investigating whether the intended system behavior occurs and that no unknown unsafe events occur.[29]

Although safety in use or reasonably foreseeable misuse is part of regular product safety, this guideline was created explicitly for road vehicles because the complexity of their functions increases with increasing automation, so that methodical guidelines for ensuring the safety of the target function become necessary. Therefore, the importance of this guideline should also be considered for other domains where vehicles operate based on automated functions.

2.1.5. Fault Tolerance

According to Isermann[30a], the reliability of a system can be achieved by either *perfectness* or *tolerance*. Perfectness refers to the avoidance of faults and failures by means of an improved design. Tolerance refers to the ability to compensate the consequences of faults and failures such that systems remain functional. This requires the ability to detect the occurrence of faults and failures in systems. It is particularly important in systems with high safety integrity requirements and where the occurrence of faults cannot be avoided by the design process.

Degradation Concepts[30b]

In terms of fault tolerance, it is distinguished between different degradation concepts:

- *Fail-operational:* A fail-operational component remains operational after a failure. This is required if the component can not be transferred to a safe state immediately after the failure. A common measure is redundancy in respective components.
- *Fail-safe:* a fail-safe component immediately transfers to a safe state after one or several failures. It is distinguished between passive fail-safe components that reach the safe state without external power, or active fail-safe, where the component is brought to a safe state by an action with external power. The basic prerequisite for this concept is that a safe state exists at any time. For systems in motion, such as vehicles or machines, a safe state often is a stand still. In some cases, the establishment of a safe state as a reaction to a fault is more convenient than keeping a system operational with redundant components.
- *Fail-silent:* a fail-silent component is externally switched off after one or several failures and stays passive for the further course of operation so that it does not influence other components in a wrong way.

[30] Isermann, R.: Fault-diagnosis systems (2006). a: p. 347 ; b: p. 352 ; c: p. 347-349.

Redundancy Concepts[30c]

Redundancy is a measure to increase the fault tolerance or fault diagnosability of a system. Redundancy concepts are divided into *static* and *dynamic redundancy*. The latter is further divided into ”hot” and ”cold standby”. The *static redundancy* principle uses a so called voter, that compares the output of multiple similar hardware or software components connected in parallel, which all receive the same input information. The voter compares the output information of the components and identifies the valid information by the majority. Therefore, an odd number of redundant components is required, whereby three is the minimum. At the voter's output, the faulty value is masked. The system thereby remains fail operational. With a lower number of only two redundant systems, a fault identification would be possible, but it can not be identified, which is the faulty and which is the true component. The disadvantages of static redundancy are high costs, high energy consumption and high weight in the case of redundant hardware components and increased computing time in the case of redundant software components. It is to note that software faults are generally systematic, which is why a diverse design of redundant software is required rather than a duplication.

In the case of *dynamic redundancy*, at least two components of the same type must be present. One component is always actively in operation. If it fails, the back-up component takes over. The system thus remains fail-operational and has a fault tolerance of one in a two-component setup. For fault detection, a monitoring component is required that is able to detect a failure of the active component, deactivates the faulty and activates the back-up component. Fault detection methods e.g. include consistency checks at the output signal, comparison with redundant modules or watchdog timers. Depending on whether the back-up component also operates continuously during normal operation or only begins to operate as a result of a detected fault, it is referred to either ”cold standby” or ”hot standby”. The advantage of dynamic redundancy is a lower number of parallel components. With the cold standby, another advantage is that the back-up component must not operate in the inactive state, which saves operating time and wear in hardware components. A hot standby is useful for systems that require short transfer times in case of a required switch over due to a fault. Since redundancy increases complexity and cost, a compromise between the degree of fault tolerance and the number of redundant components must be found.

2.1.6. IEC 61025

The IEC 61025 *Fault tree analyses*[31] is an international standard that describes a method for identification and analysis of conditions that cause or contribute to the occurrence of a specific top event. This top event is often a safety related event, such as a performance degradation or a failure condition, while the underlying conditions to identify are contributing root causes. This helps to organize fault events in large complex systems that lead to an undesired, known top event.

[31] IEC: IEC 61025:2006 - Fault Tree Analysis (FTA) (2006).

It is for example used for systematic fault identification on lower system levels, which helps to design systems either fault free or fault tolerant. The standard describes a graphic model and standardized symbols that link tree elements to parent elements in AND or OR conditions. It differs between qualitative analyses that focus on the identification of fault tree elements, and quantitative fault tree analyses that include the probability of occurrence of an event. The fault tree analysis (FTA) will be used in several phases of this work.

2.2. Wheeled Mobile Driving Simulators

The first concept idea of a DS on wheels dates back to a patent by Donges/BMW[32] in 2001. The concept proposes a motion platform with at least three wheels topped by a dome with simulation environment. In contrast to the actual idea of a mobile DS, the energy is supplied via a cable suspended from the ceiling. The idea is followed by further concept propositions, as the 24-wheeled motion base DS of Eindhoven University together with BOSCH Rexroth.[33]

Nevertheless, the concepts remained theoretical ideas and where never brought to full scaled prototypes used for practical validation with test persons. The first step into practical implementation was taken by Betz[34], who designed a down scaled prototype of the tire-based motion platform for feasibility evaluation in 2015 (cf. Chapter 2.2.3). The first full-scaled WMDS designs suitable for test person studies are introduced by TU Darmstadt and TU Dresden (cf. Fig. 1-2). This work focuses on the TU Darmstadt concept, since this is part of the project MORPHEUS 2.0[35], this work is based on. Its basic design and functions are described in the following.

2.2.1. WMDS Design[36]

The target function of a WMDS is to represent a virtual vehicle, which is controlled by the inputs of a test person sitting within the cabin of the WMDS, with visual, auditory, tactile and motion cues. Therefore, the following basic components are required:

- *Simulator Dome:* This comprises the simulation environment, which is a simplified mock-up with separate seat, pedals and steering wheel at TU Darmstadt, whereas the test person is wearing a head mounted display (HMD) for the visualization of the simulated experiment. At TU Dresden's concept, the cabin comprises a real vehicle mock-up (Porsche Taycan) and the visualisation is realized with projectors and a screen. In both cases, a seat shaker

[32] Donges, E.: Fahrsimulator (2001).

[33] Slob, J. J. et al.: The wall is the limit (2009).

[34] Betz, A.: Diss., Feasibility and design of WMDS (2015).

[35] Institute of Automotive Engineering Darmstadt (FZD): Research Project: MORPHEUS (2022).

[36] Content mainly extracted and further extended from Albrecht, T. et al.: Design and Challenges of WMDS (2021).

is placed below the driver's seat to represent high frequent vibrations, imposed e.g. by a combustion engine or while driving over cobblestones. Further typical components within the cabin are the computers running the simulation software, lighting, air conditioning, surveillance camera, fan and a door to enter the cabin. The TU Dresden WMDS is further equipped with a turntable between hexapod and cabin, enabling a decoupled 360° rotation of the whole cabin.

- *Hexapod:* A 6 degree of freedom motion system mainly used to tilt the cabin in order to represent low frequency accelerations (tilt-coordination).
- *Platform Body and Suspension:* The hexapod and cabin are carried by a main platform body, which further houses the required components for on-bord energy supply (high voltage accumulator for the drive system supply and low voltage accumulators for the auxiliary devices) and further processors and sensors required for the motion control and other auxiliary functions. The suspension to the wheel units is a double wishbone suspension with spring and active damper unit. It has the task to eliminate vertical excitation by the road while suppressing yaw and roll motion when accelerating the WMDS or moving the hexapod.
- *Wheel Units:* These are electrically propelled, separated into a drive system and a steering system enabling 360° rotation at each wheel. The drive system further includes an electro-magnetical safety disc brake, that is electrically open and closed when de-energized. This enables that the WMDS can be stopped at any time. Pneumatic SUV tires are used for the force transmission to the ground. TU Darmstadt's WMDS comprises three wheel units, while TU Dresden has four wheel units due to higher wheel loads generated by the heavier cabin with full vehicle mock-up.
- *External Operator Station:* The WMDS is controlled and observed from an external operator station communicating via WLAN. From there, communication with the test persons and video streaming from the cabin is enabled, the simulation experiment is started/stopped and relevant WMDS states are controlled and observed. Additionally, a radio remote control device is available to control the WMDS motion manually.

A detailed illustration of TU Darmstadt's concept MORPHEUS 2.0 is shown in Fig. 2-5. The Darmstadt concept is characterized in particular by its lightweight construction. Using an HMD saves mass for a vehicle mock-up and the projection systems. As a result, the cabin size and therefore weight can be reduced to a minimum and an overall comparatively low center of gravity can be achieved.[37] This enables a reduction in wheel load variations, which facilitates the motion control. This is also crucial for the required wheelbase, which must provide rollover stability under the most dynamic conditions. The TU Darmstadt WMDS has a resulting mass of approx. 3000 kg with a wheel-base of 5 m and a height of 3.5 m.

[37] Plaettner, S. et al.: Impact of Visualization System on WMDS Design (2022).

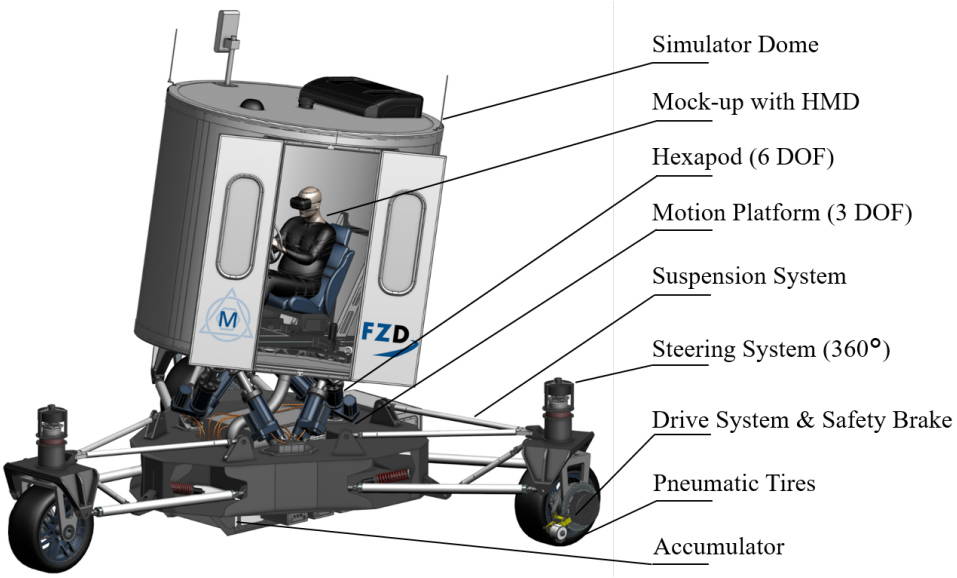


Figure 2-5.: Design and basic components of the WMDS MORPHEUS 2.0 at FZD.

The advantage of the TU Dresden concept is the more realistic simulation environment with a higher resolution visualization system and a real vehicle mock-up whose functions can be included in a simulator experiment. Nevertheless, the price is an overall system mass of approx. 4700 kg.[37] This limits the portability of the WMDS and therefore its mobile application. Tab. 2-2 summarizes some design features of both WMDS concepts.

2.2.2. WMDS Motion Concept

The motion concept is described by means of the TU Darmstadt concept. During a driving simulation, the individual inputs of the test person are processed in a vehicle model of the simulation software, which determines the dynamic behaviour of the virtual vehicle within the simulation. Further processing concerns e.g. the sound of the virtual vehicle as well as the visual representation of the scenery and other traffic participants in the virtual world.

The motion quantities of the virtual vehicle are to be represented by the motion system of the WMDS. Therefore, the simulation software delivers a target acceleration vector containing x and y coordinates $\vec{a}_{\mathrm{V,dem}}$ and a target yaw rate $\dot{\psi}_{\mathrm{V,dem}}$ to be represented. The so-called *motion cueing algorithm (MCA)* for WMDS is described by Betz[38a] and transforms the target values into a part to be represented by the hexapod (tilt-coordination) and a part to be represented by the motion platform ($\vec{a}_{\mathrm{DS,dem}}$, $\dot{\psi}_{\mathrm{DS,dem}}$). Optionally, a predefined *scaling factor* < 1 is applied to the longitudinal accelerations, which reduces the demanded motion of the WMDS and is typically implemented in MCA of DS. A scaling factor of 0.7 is a preferably chosen factor, since it has been shown that up to this value, test persons do not perceive a difference towards a scaling of 1.[39]

[38] Betz, A.: Diss., Feasibility and design of WMDS (2015). a: p. 51 ; b: pp. 58-70.

[39] Berthoz, A. et al.: Motion Scaling for High-Performance Driving Simulators (2013).

Table 2-2.: Comparison of specifications between the WMDS at TU Darmstadt and at TU Dresden.[36]

		WMDS Darmstadt	WMDS Dresden
Motion platform (3 DOF*) * active	$\ddot{x}; \ddot{y}$ (m/s²) $\ddot{\psi}$ (°/s²)	5.4; 5.4 126	9; 9 206
	$\dot{x}; \dot{y}$ (m/s) $\dot{\psi}$ (°/s)	15; 15 360	14; 14 320
	$x; y$ (m) ψ (°)	inf; inf inf	
Yaw Bearing (1 DOF)	$\ddot{\psi}$ (°/s²)	-	180
	$\dot{\psi}$ (°/s)	-	220
	ψ (°)	-	inf
Hexapod (6 DOF)	$\ddot{x}; \ddot{y}; \ddot{z}$ (m/s²) $\ddot{\phi}; \ddot{\theta}; \ddot{\psi}$ (°/s²)	6; 6; 9 300; 300; 500	
	$\dot{x}; \dot{y}; \dot{z}$ (m/s) $\dot{\phi}; \dot{\theta}; \dot{\psi}$ (°/s)	0.45; 0.45; 0.42 50; 50; 45	
	$x; y; z$ (m) $\phi; \theta; \psi$ (°)	0.15; 0.15; 0.13 17; 17; 15	
Seat shaker	$\ddot{z}$ (m/s²)	10	
Dimensions l; w; h (m; m; m)		5; 4.4; 3.5	4.4; 4.4; 4.6
Mass (kg)		~ 3000	~ 4700
Amount corner modules		3	4
Accumulator Energy (kWh)		30	22
Visualization system		HMD	3 projectors
Tire size		315/35 R20	

An important component of the MCA is the so called *washout algorithm*, which enables a DS to realistically represent motion of the virtual vehicle while keeping the DS within the limits of its workspace. This is achieved by moving the DS back to its starting position below the human perception threshold for motion or by masking the washout motion with tilt coordination to avoid influence on the driving simulation. The washout algorithm therefore requires feedback of the measurement quantities of actual WMDS position $\vec{d}_{\mathrm{DS,act}}$ and speed $\vec{v}_{\mathrm{DS,act}}$, which are further multiplied by feedback gains. Additionally to the MCA designed by Betz, a mechanism for adapting the regular MCA to the workspace limits[40] is foreseen: If the regular washout returns do not succeed in preventing the virtual workspace boundaries from being exceeded, which is identified by crossing radial limits, either the return weight is increased by applying an opposing correction acceleration or, in the worst case, a braking with subsequent return is initiated. A

[40] Jargon, E.: Bachelor Thesis, Bewegungsraumadaption des MCA für WMDS (2018).

similar mechanism is briefly described by Tüschen[41] for the TU Dresden concept, including a return zone and an emergency brake zone as part of the workspace design, whereby further specifications of these zones are not given.

The MCA outputs concerning the motion platform are further transferred to the *motion control (MC)*, within which the steering angles and respective motor speeds required to realize these accelerations are determined. The concept is described in Betz[38b] and includes estimating the required horizontal tire forces under the constraint of equal friction value utilization and consideration of dynamic wheel loads. The received target values are converted by the electric drive controllers into individual drive and steering motor speeds and angles, which results in the actual motion of the platform. The aim of the MC is to minimize the deviation of the actual acceleration from the target acceleration. It therefore receives feedback from an inertial measurement unit, which delivers the WMDS' actual accelerations $\vec{a}_{\mathrm{DS,act}}$ and yaw rates $\dot{\psi}_{\mathrm{DS,act}}$. The overall processing from driver inputs to WMDS platform motion is illustrated in Fig. 2-6.

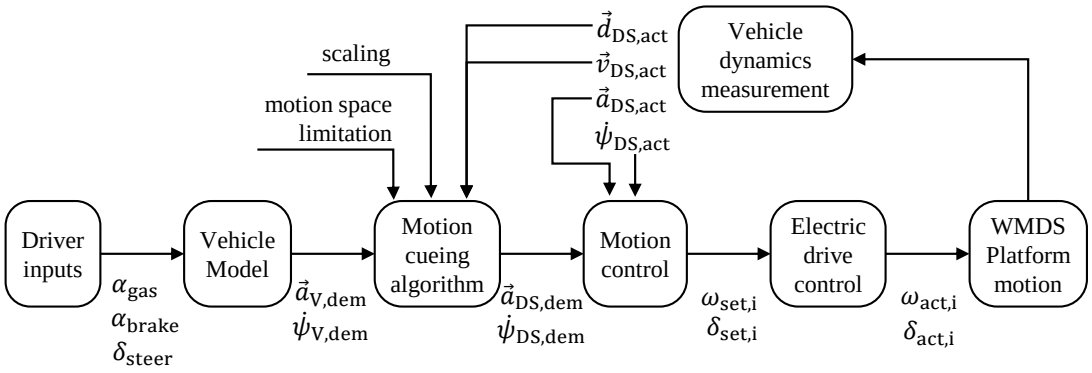


Figure 2-6.: Control concept of the WMDS motion during driving simulation mode, adapted and further complemented from Zöller[42a].

A driving simulation can basically become more realistic, the less often and less strongly the washout has to superimpose the target motion. This can be reached by a larger workspace size, which mainly motivates the development of WMDS. The smaller the scaling factor is chosen, the smaller the accelerations and hence the speeds and required movement space of the motion platform are[42b], which can also prevent from often and strong washout interventions.

[41] Tüschen, T.: Diss., Konzeptionierung eines hochimmersiven und selbstfahrenden Fahrsimulators (2019).

[42] Zöller, C. A.: Application of WMDS to uneven grounds (2019). a: p. 17; b: p. 24.

2.2.3. Scaled WMDS Prototype

The WMDS prototype MORPHEUS 1 is a scaled version of the previously presented WMDS design and was preliminary used to evaluate the technical feasibility of the wheeled concept.[43,44a] The design is shown in Fig. 5-2. The wheel base is $2.3\,\mathrm{m}$ and therefore half of the size of the full scaled WMDS MORPHEUS 2.0, which is possible because it does not carry a dome and therefore has a lower center of gravity. The drive and steering system has the same omnidirectional concept as the full scaled WMDS, but is directly attached to the rigid platform body without a suspension system. The tires are full rubber tires instead of pneumatic tires. The scaled prototype can accelerate with approximately $8\,\mathrm{m/s^2}$ and has a maximum speed of approximately $12\,\mathrm{m/s}$.[44b] Since the presented full scale WMDS MORPHEUS 2.0 is still under construction, this scaled prototype is used for practical experiments in this work.

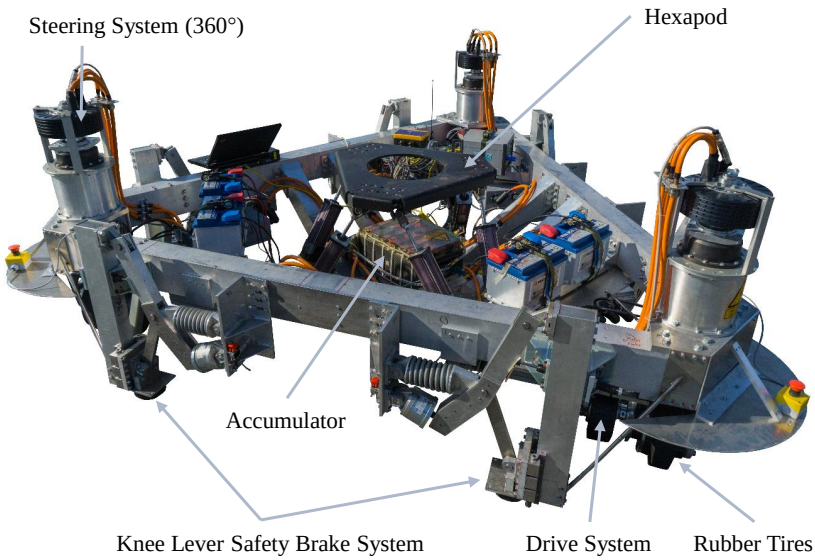


Figure 2-7.: WMDS prototype MORPHEUS 1 and its components.

2.2.4. Virtual Prototype and Test Maneuvers

A virtual prototype of the WMDS is created as a Simulink and CarMaker model within the project, which includes the previously described MCA and control concept. It therewith is possible to simulate and analyse the induced platform motion of the WMDS with regard to desired, pre-recorded driver inputs. As long as no real data from the WMDS can be generated in driving simulations, the virtual prototype is used in this work to obtain representative motion variables that are relevant for the design of the safety system. The following driving simulation data sets exist:

[43] Betz, A.: Diss., Feasibility and design of WMDS (2015).

[44] Wagner, P.: Diss., Practical Feasibility and Functional Safety of WMDS (2018) a: -, b: p. 47.

- Real City Drive 1-4: A representative city drive course through the German city Darmstadt was developed within the thesis of Graupner[45]. This developed course was driven in a real road vehicle by four drivers with different driving styles and the motion quantities serving as an input to the MCA were recorded with respective measurement equipment. These scenarios were initially used as a reference for a design and evaluation of the motion control system of the WMDS when used for urban driving scenarios. The driving style is most dynamic for City drive 1 and decreases towards City Drive 4.
- SILAB Optimized City Drive: Based on this, a student project extracted characteristic driving maneuvers from the Real City Drive by Graupner and created a motion space-optimal virtual driving scenario in the SILAB software. This is the driving simulator software for the virtual environment and vehicle model used in MORPHEUS 2.0.[46] The scenario combines city-typical driving maneuvers with sections of constant speed so that the WMDS can be returned to its initial position frequently. It also coordinates left-right combinations to the extent that the WMDS approaches its movement space limits as little as possible. The scenario is developed for a validation of the WMDS concept for urban driving scenario simulation and intends to optimize the DS experiment towards the available motion space and thereby to avoid false cues due to motion space limitations. From this scenario, two recorded data sets of the vehicle motion are available, from a normal driver as well as from a sporty driver.[47]

2.2.5. Functional Safety of WMDS

The aspect of functional safety of WMDS is addressed by Wagner by following the major steps of ISO 13849 to perform a HARA, but using the risk metrics of IEC 61508.[48a] Other than described above, a prior general hazard identification and risk reduction process according to ISO 12100 is not carried out. Instead, functional faults on component level of the basic WMDS functions are identified via the so-called hazard and operability study (HAZOP) method and their risk is assessed, which is subsequently expressed by a SIL. In this way, it is identified which existing functions and components of the machine are safety-relevant. Afterwards, requirements are defined and suggestions are made for risk reduction measures that compensate or eliminate functional faults of the main WMDS functions. The procedure is carried out for the scaled prototype presented in Chapter 2.2.3 and Fig. 5-2.

In the first phase of *Determination of the Limits of the Machinery*, a complete description of the system WMDS and the connections and signals of individual elements to each other is created.

[45] Graupner, M.: Bachelor Thesis, Stadtparcours (2011).

[46] WIVW GmbH: Driving Simulation and SILAB (2022).

[47] Coors, F. et al.: Advanced Design Project, Virtuelle Fahrszenarien für WMDS (2021).

[48] Wagner, P.: Diss., Practical Feasibility and Functional Safety of WMDS (2018). a: pp. 56-59 ; b: pp. 87-94 ; c: pp. 95-96 ; d: pp. 97-100.

For modeling the WMDS's architecture, Wagner subdivides the overall system into seven E/E/PE subsystems and models the power and data signal flow between the different components within each subsystem and beyond the boundaries to other subsystems.[48b] This phase considers the basic functions that a WMDS conceptually requires and that were known at this stage of WMDS development. This includes functions for generating a WMDS motion from test person inputs, simulation environment, energy supply, and options for external control and communication by operators. Consequently, the architecture is not based on an initial risk mitigation process.

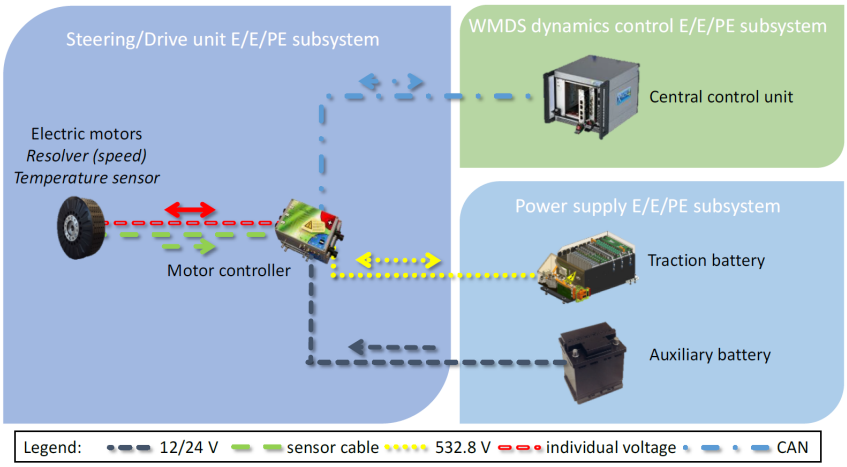


Figure 2-8.: Modelling of the WMDS' drive and steering unit E/E/PE subsystem for preparation of the hazard analysis by Wagner.[48b]

The next phase is the *hazard identification process*, where the HAZOP analysis[49] is applied. The procedure includes to associate predefined guidewords to intended functions of the system to identify potential failures or malfunctions. The obtained combinations must then be reviewed to examine possible consequences resulting from each failure resulting in a hazard.[48c]

The next step is the *risk estimation process*, where a SIL in compliance with IEC 61508 is assigned to each identified hazard. First, hazardous events are formulated by assigning hazards to the most critical conceivable situations. Thereby, the driving simulation operation itself as well as maintenance work is considered. Then, the SIL is determined by evaluating a hazard's consequences, the exposure in the hazardous area, the controllability of the hazard and its probability of occurrence. The hazard parameters and a risk graph introduced by IEC 61508 are applied. The result of the process is a list of identified, critical hazardous situations and the corresponding risk levels. Applying this method, Wagner has obtained a list of 186 evaluated hazardous situations with corresponding estimated SIL for the scaled WMDS prototype.[48d]

[49] IEC: IEC 61882:2017 - HAZOP application guide (2017).

An exemplary hazard identified and assessed within this process is:

Failure:	No or insufficient low voltage energy supply to steering unit
Consequence:	Demanded steering angle cannot be provided, WMDS trajectory is uncontrollable
Situation	Driving simulation with test person, high velocity, close to boundary of WMDS workspace
Consequence (C):	C3 (death to several people) The test person and/or bystanders and/or the system operator(s) may be injured and/or killed
Frequency (F):	F2 (frequent to permanent exposure in the hazardous zone) The driving simulation is the standard application of the WMDS. The boundaries of the work space are reached often and high velocities are driven.
Poss. of avoid. (P):	P2 (almost impossible) A power cut occurs very suddenly and can hardly be foreseen prior to the hazardous event. Once the hazard has occurred, the system operator has no possibility of mitigating the event, because he cannot steer the WMDS anymore.
Probability (W):	W1 (A very slight probability that the unwanted occurrences will come to pass, and only a few unwanted occurrences likely) Standard accumulators and a standard battery management systems are used, which makes a power cut unlikely.[48d]

The combination of the risk parameters results in a SIL2 for the described hazardous event.

In the *risk evaluation phase*, a safety function requirement list is derived by describing safety functions that intend to reduce the risk of a hazardous event with the minimum SIL they must fulfill. A total of twelve safety function requirements is defined by Wagner. The safety function requirement with the highest SIL rating and the highest number of underlying hazardous situations is:

- ”The DS trajectory must remain controllable so that collisions with objects and subjects can be avoided. (SIL 4)”[50a]

This safety function requirement addresses the issue of safe motion of WMDS and the avoidability of collisions. It covers a large number of the hazards connected to WMDS malfunctions identified within the process. Concluding, a common consequence of a malfunction of the WMDS is that

[50] Wagner, P.: Diss., Practical Feasibility and Functional Safety of WMDS (2018) a: p. 106 ; b: pp. 111-113.

the WMDS motion becomes uncontrollable or does not meet the expected motion. Hazards with this consequence have been assigned the highest SIL, since uncontrollable or unexpected motion can lead to harmful collisions with people or objects in the environment. Concluding, without further measures, the components for energy supply, motion control and motion execution of a WMDS are of high safety relevance. It thereby is to note that the requirement only includes a measure to enable that collisions **can be avoided** at any time, while it does not represent an active measure with that collisions **are avoided**.

The risk evaluation process is repeated after safety measures are defined by means of a proposed safety architecture for WMDS, revealing that all SIL are reduced to a level SIL a, which is interpreted as sufficient reduction of risk.[50b]

It is to note, that the analysis and evaluation performed by Wagner refers to the specific architecture and characteristic of a scaled WMDS prototype built at FZD, TU Darmstadt. Additionally, a risk estimation is always a subjective process and highly depends on the applying person. The determined hazards and connected risk therefore are not to be interpreted as valid for all specific WMDS designs or a generic WMDS concept. Rather than a precise determination of specific SIL requirements, the process should be viewed as a demonstration of the application of accepted HARA methods to determine hazards from functional failures during a WMDS operation. The risk estimation thereby is conducted conservatively in order to demonstrate that the defined measures are effective in risk reduction even under the most critical situations.

2.2.6. Safety Architecture for WMDS

Instead of choosing a fail operational strategy and assigning a SIL to all components involved in the motion control and motion execution process of WMDS, Wagner proposes an *external emergency brake system (EEBS)* as a fail safe risk reduction measure and central part of the WMDS safety architecture. For this purpose, Wagner further used the hazard analysis to define those malfunctions to be monitored in order to trigger the EEBS. These result in, for example, but are not limited to, the following malfunctions:[50b]

- General malfunction of motor controllers, electric drive or steering motors, central control unit, vehicle dynamics measurement unit and external command device (SIL1)
- Traction or auxiliary battery overvoltage or battery power cut (SIL2/SIL1)
- Faulty data transmission between the central motion control unit and other components responsible for the motion planning or execution (vehicle dynamics measurement unit, motor controllers, external command device, ...) (SIL2/SIL1)
- Incorrect measurement data from the vehicle dynamics measurement unit (SIL2)

Based on the risk analysis performed by Wagner, the EEBS itself must be designed according to a SIL4. In addition, the diagnostic functions that shall detect failures in the motion control and execution and initiate the trigger of the EEBS also inherit a SIL based on the evaluation of the respective associated hazard. Beyond these functional requirements, the malfunctions and thus the requirements for the diagnoses are not further specified, e.g. by thresholds. In addition, it is only briefly mentioned that the WMDS must always be able to come to a stop within its workspace, without this being further specified.

The EEBS for WMDS shall be able to transfer the WMDS to a fail safe standstill at any time in order to establish a safe state in case of hazards. Thereby, the condition of continuous controllability is fulfilled with a fail safe strategy. To solve this task, the EEBS must function detached from any components whose failures and malfunctions it is intended to counteract. This includes the WMDS' drive and steering system, internal or external motion control and overall energy providence.[50d] Therefore, an electromagnetic knee lever brake system[51] was developed for the special WMDS prototype, which is tensioned by electromagnets and springs. When the power supply is interrupted, the springs press brake pads to the ground via the knee lever system, which lifts the overall WMDS platform simultaneously. As a result, the system acts in the event of a complete power failure. In addition, a relay can be actuated at any time according to a defined logic to trigger the braking system in the event of detected fault conditions, or manually by the system operators when pressing the emergency stop buttons on a handheld control device.[52]

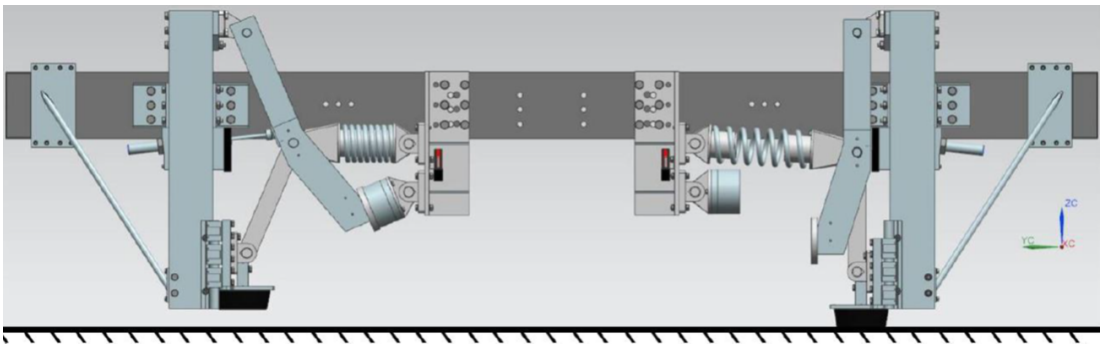


Figure 2-9.: Emergency braking system. Left: engaged, right: deployed.[52]

In Tüschen[53], another concept for an EEBS for WMDS is presented, but aligned with the WMDS design proposed by TU Dresden. In contrast to the lifting knee lever approach, the platform of the WMDS is lowered to establish contact to a friction body underneath the main platform. This is enabled by loosening spring-damper elements of the drive unit's suspension, which is also initiated by a magnetically preloaded spring. Nevertheless, besides this concept description, no further requirements on the conditions under which this system is to be deployed are given.

In today's WMDS designs of TU Darmstadt and TU Dresden, the concept of an EEBS as a fail

[51] Betz, A. et al.: Development and Validation of a Safety Architecture of a WMDS (2014).

[52] Wagner, P.: Diss., Practical Feasibility and Functional Safety of WMDS (2018) p. 114-115.

[53] Tüschen, T.: Diss., Konzeptionierung eines hochimmersiven und selbstfahrenden Fahrsimulators (2019) p. 123.

safe electromagnetic brake system is adopted, but differs in the technical implementation. The two approaches described, using lowering and lifting methods, were discarded due to their high complexity and expected discomfort for the test person. Instead, electromagnetic disc brakes on the wheel units are used, which function according to the same fail safe principle as described above and thereby fulfill the requirements on independence of specific safety related components. Since ground contact of the tires is not eliminated with this concept, a counteraction of the drive units must be avoided. At TU Darmstadt, the circuit for emergency braking consists of the brake system itself, a safety certified programmable logic controller, safety relays to open the magnets as well as power contactors to remove the energy of the electric drive systems.[54]

The described risk assessment process was repeated for a preliminary design of MORPHEUS 2.0 within the master thesis by Lutwitzi[55] to further extend the safety architecture for the full scale WMDS. In this work, object detection for collision avoidance has already been proposed as an extension of the WMDS architecture for the purpose of personal protection, without this being able to emerge directly from Wagner's method. A technical and economic analysis regarding suitable sensor hardware for object detection for WMDS has already been done in the bachelor thesis of Lutwitzi[56]. However, the framework conditions considered at that time for the derivation of requirements referred to the scaled prototype of WMDS and a development status at which no requirements were known on the part of machine safety. In addition, no functional specification took place, respectively no actual implementation in hardware and software and corresponding feasibility analyses were carried out. However, the derived requirements of the work can be used as a reference.

2.3. Excursion to Safety Systems of Driverless Transportation Systems

Since there are no Type C safety standards for driving simulators, and in particular self-driving mobile simulators, this section deals with cross-domain systems with similarity character to the WMDS safety problem. An obvious system is the *road vehicle*, which has already been addressed by the explanation of the ISO 26262 and SOTIF standards in previous chapters. On the other hand, safeguarding the movement of a road vehicle is a much more complex task, comprising the correct perception of the environment with a high number of dynamic elements such as other road users and the planning and execution of collision-free trajectories while complying with traffic rules, which all does not correspond to conditions of the WMDS operation. A safety standard for mobile systems that are as similar as possible to the present use case due to a more limited ODD

[54] Albrecht, T. et al.: Design and Challenges of WMDS (2021).

[55] Lutwitzi, M.: Master Thesis, Safety Architecture for WMDS (2019).

[56] Lutwitzi, M.: Bachelor Thesis, Umfelderkennung für WMDS (2016).

leads to driverless transportation systems, in particular to *driverless industrial trucks*.

A driverless industrial truck, as specified in ISO 3691-4[57], is an automated conveyor with its own traction system, which is automatically controlled and guided without contact. The primary task is to transport materials along defined paths in plant environments inside and outside of buildings. ISO 3691-4 specifies safety requirements for driverless industrial trucks, among others on their braking system, emergency stop system, power supply and personal protection systems. The latter describes measures to detect persons in the driving path of the vehicle in order to initiate a transfer to standstill. These can be contact based, such as tactile bumpers, if the contact forces are small enough to avoid harm to persons. Otherwise, electro-sensitive protective equipment (ESPE) needs to be applied that reacts without contact. A virtual safety buffer is defined, in which the ESPE detects persons and initiates a braking to standstill that is to be completed before contact between the person and the vehicle can occur. This shall respect the braking distance of the vehicle as well as the distance travelled during the reaction time of the ESPE. When the safety buffer is cleared again, the vehicle continues after applying a warning signal. The dimensioning of the safety buffer does not respect motion of persons and rather is designed towards static objects, since it is expected that persons will stop when recognizing the vehicle. The protected area must at least enclose the full width of the industrial truck in driving direction. If the system has a protective field switching mechanism, the virtual buffer can be switched dynamically depending on actual driving speed, steering angle and eventually underground slope. The outputs of the protective system must act on the safety-related parts of the control system in order to initiate the braking. With a protective field switching mechanism, the respective inputs like vehicle speed must also be available in the ESPE. All inputs and outputs as well as the respective control and actuation parts must correspond to the required safety level of the protective system. Person detection systems are rated at PLd or SIL2 performance for driverless trucks. All subfunctions included in the person detection function therefore inherit this performance requirement.

For the release of the protective system for the application in industrial trucks, testing procedures are defined in the standard. These define the size and reflective properties of test objects as well as the driving maneuvers during the tests. The test objects shall have ”an external surface reflectance of 2 % to 6 % and an optical density of 1.22 (e.g. black). The industrial trucks must be tested under the most adverse conditions (e.g., loading, tilt, rotation, forward direction, reverse direction) in combination with the parameters specified for the industrial truck for those conditions.”[57] The test shall be performed at maximum speed and with two different specimen A and B: The test specimen for test A is cylindric with a diameter of 200 mm and a length of 600 mm. It is placed horizontally on the floor at right angle to the movement path of the industrial truck. In test B, a cylinder with a diameter of 70 mm and a length of 400 mm is placed vertically. The cylinder sizes are oriented on the basis of the lower leg dimensions of a lying person and a standing person. In both cases, the vehicle must approach the test piece and must stop before contact occurs.

[57] ISO: ISO 3691-4:2020 - Driverless industrial trucks (2020).

EN 61496-1[58] defines application-independent requirements for the design, construction and testing of non-contact ESPE. These include light grids and light barriers, ultrasonic or camera systems, laser scanners and such like. A distinction is made between three types of systems, that differ in their performance in the presence of faults and under influences from environmental conditions. These correspond to the categories defined by EN ISO 13849. Depending on the required performance level of the safety function, the ESPE must be designed and tested according to one of these types. A type 2 ESPE is required for a SIL1 or PLc requirement and shall have a periodic test to reveal a failure, which is for example loss of detection capability or a response time exceeding the specified, which must be performed at least before turning on the system (equals category 2). A type 4 ESPE is required for a SIL3 or PLe requirement, which must detect all faults at any time that can lead to a hazardous failure of the system (equals category 4).

The standards can be considered as an orientation for the WMDS in terms of safe motion and personal protection. However, due to its individuality, the WMDS must be evaluated separately for risks and specific requirements.

2.4. Conclusion on the State of the Art, Previous Work and Further Steps

In the previous chapters, relevant safety standards describing the process of risk reduction of machines have been presented. These prescribe an initial process of *hazard identification and risk assessment* and the definition of *risk-reducing measures*, including the addition of safeguards. Since there is no type C standard for WMDS, this process must be perfomed.

For those safety-relevant functions that depend on an electrical system or a control system, the *functional safety* standards further apply. Based on the associated risk, a level of required safety integrity of a safety function is determined. Consequently, the functional safety standards require the application of ISO 12100 to identify risks and the need for the addition of safety relevant functions to a system and add further requirements on their development, design and testing. From a functional safety perspective, a function can be considered safe, if the dangerous failures have either been avoided by the development process or if they can be diagnosed during operation and the system can be brought to a safe state by a fault response. The integrity/performance levels lead to concrete requirements for acceptable hardware failure rates of sensors, processors and actuators, as well as structural requirements for the fault diagnosis and fault tolerance, software requirements and verification and validation requirements.

Wagner's work represents an important step in this process chain. Identifying the hazards associated with functional failures of the basic functions of a WMDS, and the awareness that an

[58] IEC: IEC 61496-1:2020 - Safety of machinery - Electro-sensitive protective equipment (2020).

external emergency braking system can control most of these hazards, is an important step towards providing safe motion for WMDS. The fact that an EEBS has been implemented in both WMDS approaches of TU Darmstadt and TU Dresden shows the transferability into practice. However, this procedure does not include the complete process of risk evaluation and reduction of the system WMDS. Wagner's results show the safety relevance of components and subfunctions of the WMDS in terms of functional safety, but do not reveal whether an initial risk exists even in fault-free states of the basic WMDS components. Therefore, this step must be performed in order to discuss requirements for further safety functions in terms of protective measures, which might be strongly dependent on the environment the WMDS is operated in.

Another important aspect is to enable that a system's target functions are designed safely and do not hold any unknown uncertainties for its users, even without the occurrence of failures. This implies the proof that a function's specification is complete and appropriate for the use case, meaning the ODD of the system. Even though the term SOTIF is mainly specified by a guideline for the automotive industry, the safety issues targeted are applicable to other machines, especially those that operate autonomously with help of environmental perception. In order to be able to fully qualify a safety function as safe, it is necessary to prove that it has been correctly specified for the intended protective effect and prevailing conditions, as well as against conceivable misuse.

Based on these findings, the three safety proof evidences *risk assessment and reduction, safe specification of safety functions* and *failure avoidance or diagnosability* are considered relevant for the addition of safety functions to a machine. Therefore, it shall be shown in this work, that proposed additional safety functions are necessary and sufficient for risk reduction. Then, however, the aim is not to deliver a profound specification of functional safety requirements to the lowest levels of hardware and software design for these safety functions. Rather, a concept in the form of a safe functional specification of the target safety function is to be derived for the evaluation of the general feasibility, whereby potential failures are to be excluded by design as far as possible and the remaining failures are to be examined for their diagnosability in operation. Then, representative test cases shall be derived, that reveal whether the derived safety functions are applicable to the ODD of a WMDS without disturbing a driving simulation. These goals are summarized in Fig. 2-10.

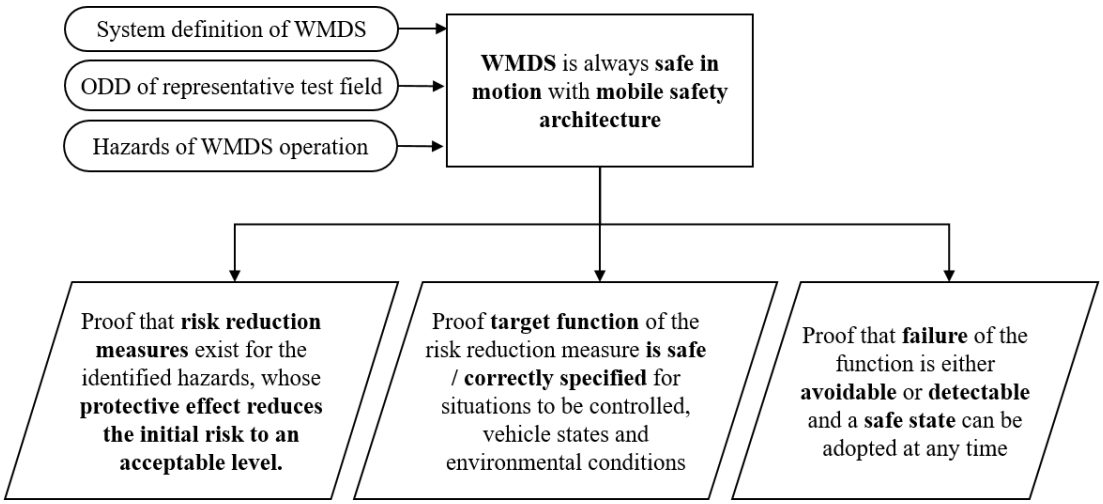


Figure 2-10.: Summary of required safety proofs extracted from the state of the art in machine safety relevant for this work.

Building on these findings, the following sub hypotheses are developed from the main research hypothesis introduced in Chapter 1.3, to which will be referred at various points in this work:

RH1: The WMDS with a proposed active safety architecture can conduct driving simulations under flexible, mobile conditions without its motion posing an unacceptable level of risk to human.

RH1.1 The safety functions reduce the estimated risk of all identified hazards to an acceptable level.

RH1.2 The safety functions are able to perform their intended function under all conditions as specified within the ODD of the WMDS, while not unacceptably disturbing the WMDS operation in situations uncritical to safety.

RH1.3 The safety functions are intrinsically safe by detecting unsafe deviations from the target conditions causing failure of the functions.

3. Hazard Analysis and Safety Goals Derivation

This chapter presents the application of an initial risk assessment at system level in accordance with the state of the art in machine safety. According to the provisions of IOS 12100 and ISO 14121-2, relevant operational conditions of a WMDS are described by means of an ODD and potential hazards are analysed. In contrast to Wagner's approach, the method applied is also intended to identify hazardous situations that do not only originate from the failure of a component but, for example, also from an unsecured operating field and human error. This identifies the need for further protective measures and to derive the required safety integrity levels. As proposed in the safety standards, safety goals are defined as top-level requirements for the safety functions.

At the end of this chapter, a set of intended safety goals shall be available, with that RH1.1 ("The safety functions reduce the estimated risk of all identified hazards to an acceptable level") is fulfilled.

3.1. Operational Design Domain of WMDS

Building on the descriptions in Chapter 2.2, the ODD of a WMDS is described by means of system modes and states, users, workspace and environment characteristics.

3.1.1. WMDS Modes, States and Users

Fig. 3-1 illustrates the system states of a WMDS in operation and the responsible users in a simplified state chart. The operation of the WMDS is managed by the *system operator*. After the power is turned on, the WMDS is in the *run off* superstate, meaning the motion system is turned off. In the *mode selection*, the operator can select between three different modes: *manual drive mode*, *driving simulation mode* with test persons and *maneuver mode*, where a pre-programmed maneuver is driven with or without test persons in the cabin. Depending on the mode, a *boarding* takes place, which includes approaching the vehicle, walking up the stairs to the cabin and being introduced to the driving simulation equipment with the help of the *operation assistant*. It further is ensured that the test person closes the safety belt. All run modes are initiated by a *run release check* with automated function checks, which must be passed to transfer to the *run on* superstate, which finally releases energy to the motion system. If the WMDS is started in its parking position, it is first operated in the *manual drive* mode and transferred to the workspae with a remote control device. The *driving simulation* and *maneuver* modes are only applicable while the WMDS is within its designated workspace. The run mode is left either when the chosen maneuver is finished

or when the operator manually aborts the operation. Then the WMDS is transferred to standstill by a soft braking. Furthermore, in case of an emergency, the run on state is left into the *emergency state*, where the EEBS is triggered to safely transfer the WMDS to a standstill as fast as possible. This can be triggered manually by emergency stop buttons, which are in the cabin, at the operator station and on the remote control devices. Additionally, the emergency state can be entered by an automatically detected fault within the machine. The emergency state is only left after the fault was cleared.

During all modes of operation, *bystanders* can be directly or indirectly involved as spectators or parallel users of multipurpose operating sites.

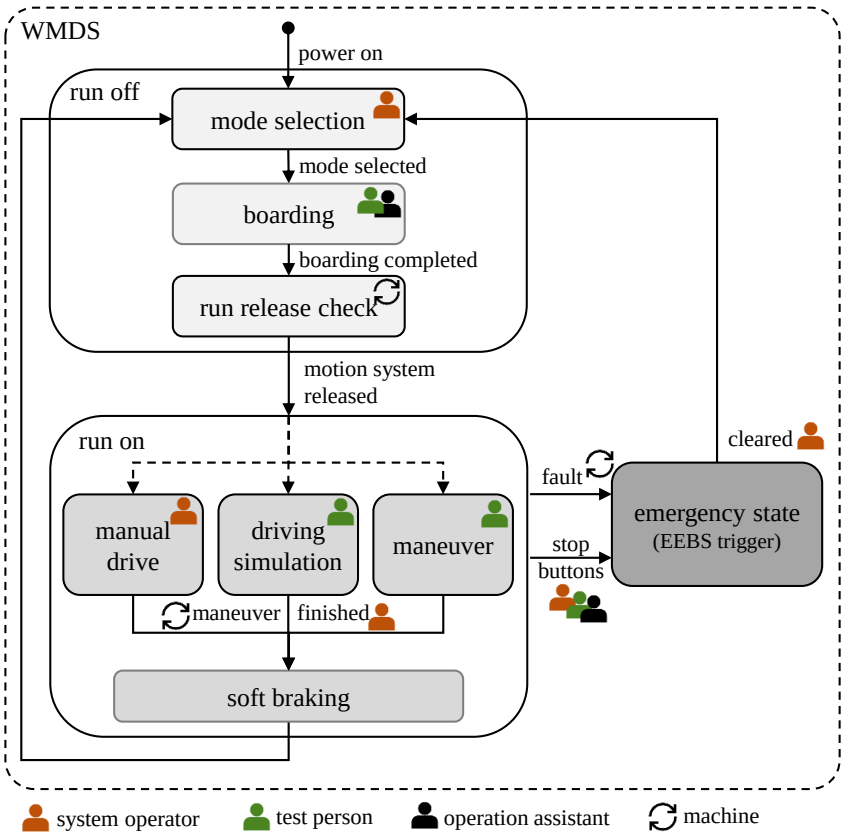


Figure 3-1.: State chart of the WMDS operation and involved persons.

Driving Simulation Mode

During the driving simulation, the WMDS moves in a designated operating range according to the inputs of the *test person*. Such a workspace has at least a virtual boundary, which is considered in the MCA and not to be crossed by the vehicle while performing the driving simulation maneuvers. Therefore, the WMDS senses its actual position and speed and superimposes the target motion representation maneuvers with return maneuvers. The basic structure of the motion cueing and control concept has been presented in Chapter 2.2.2. The test persons only indirectly controls the motion of the WMDS and has no insight in the real world surrounding of the WMDS. Due to its omnidirectional motion platform, the WMDS can suddenly change its direction of motion to any

spacial direction. The concrete trajectory of a WMDS is dependent on the driving style in the virtual world and not predictable for a known scenario. The required motion space can only be estimated but not concretely determined in advance. Additionally, the WMDS can be in motion even without actual drive inputs from the test person while performing washout maneuvers. Therefore, the WMDS can be considered as an autonomously driving vehicle in the driving simulation mode.

The motion capabilities of the WMDS are specified by a maximum translational speed $v_{\mathrm{DS,max}}$, a maximum yaw rate $\dot{\psi}_{\mathrm{DS,max}}$ and a maximum acceleration or deceleration $a_{\mathrm{DS,max}}$. The WMDS MORPHEUS 2.0 is estimated to reach a maximum translational speed of $15\,\mathrm{m/s}$, maximum yaw rates of $360\,^{\circ}/\mathrm{s}$ and a maximum acceleration of $5.4\,\mathrm{m/s^2}$ (cf. Tab. 2-2). The speeds a WMDS reaches within a driving simulation are dependent on the demanded accelerations, which is further determined by the scaling factor in the MCA and driving style of a test person, as well as the given space. Due to the washout intervention, the speeds are required to decrease towards the borders of the workspace. The left side of Fig. 3-2 illustrates the maximum driven translational speeds and yaw rates of a WMDS in dependence of varying motion space radii R_{MS} for two different city drive simulations described in Chapter 2.2.4. Thereby a scaling factor of 0.7 is applied. The right side shows the distribution of the driven WMDS speed within the SILAB City Drive maneuver for changing scaling factors.

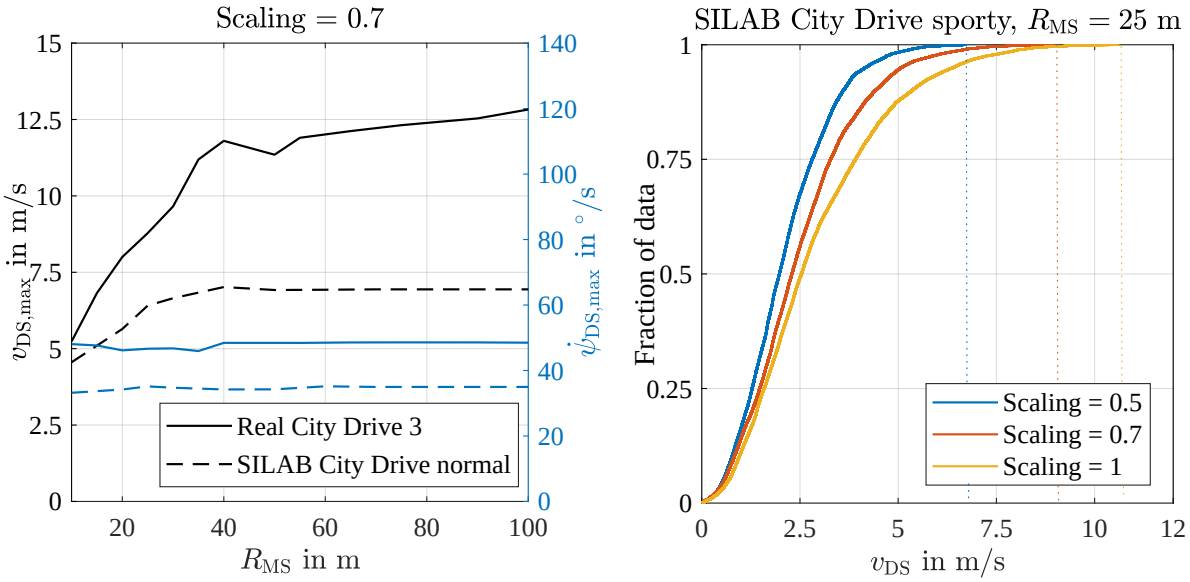


Figure 3-2.: Maximum WMDS speeds depending on the given motion space for different maneuvers, and distribution of WMDS speed within the same maneuver depending on the scaling factor.

It is shown that the maximum translational speed increases with rising workspace radii for both data sets. Since the SILAB City Drive has been optimized in such a way that the center of the motion area is frequently re-entered, no motion area larger than a $40\,\mathrm{m}$ radius is required. Therefore, the maximum speed reached within this maneuver also stagnates from this radius. The maximum yaw rates remain almost constant within a test maneuver for all workspace sizes,

since they correlate with the driving style of the test person, but not the available motion space. City Drive 3 represents more dynamic driving maneuvers, which is shown by higher maximum yaw rates and velocities even though the same motion space is provided. A rising scaling factor additionally leads to rising speeds within the same driving simulation maneuver.

Maneuver Mode

In the *Maneuver Mode*, the same motion characteristics and workspace limits as in the *Driving Simulation Mode* apply, besides that the drive inputs do not stem from spontaneous inputs of the test person, but are replayed from a preprogrammed file, which makes the WMDS trajectory more predictable. The respective maneuver is selected and a start of motion is initiated by the *system operator*. The preprogrammed maneuvers are either represented to a test person in the cabin, by means of a passive driving simulation, or aim to assess system dynamics of the WMDS in unmanned testing sessions, e.g. in acceleration or braking maneuvers.

Manual Drive Mode

In contrast, the WMDS motion is under direct human control in the *manual drive mode*. Thereby, the *system operators* can directly control the inputs to the steering and drive units by the radio remote control device. Different manual drive modes are conceivable, e.g. a one wheel steering or an all-wheel steering mode, forward and backward drive or pure rotation. The fact that no mechanical guidance is given and that the operator only has an external point of view and therefore not necessarily full insight into the movement corridor, demands high control skills of the operator. Additionally, the manual drive is not bound to a prescribed workspace with set limits. The following use cases can apply for a direct manual control:

- *Maneuvering:* The WMDS is manually transferred to its parking position (e.g. storage, battery charge, maintenance) or to its initial workspace position prior to a driving simulation. This can require precise maneuvering, e.g. into parking slots or through hall gates. Therefore, a limitation of the maximum drivable speed for the maneuvering mode $v_{\mathrm{DS,man,max}}$ is forseen.
- *Sensor calibration:* Prior to a driving simulation, some sensors, e.g. the vehicle dynamics measurement unit, might require a calibration drive with dynamic maneuvers. Besides the possibility to automatically perform this maneuver with pre-programmed inputs, this can be performed manually.
- *Test drives:* Especially during the commissioning and testing phase, several test drives might be required, e.g. to identify system parameters or to verify the functionality of specific functions. Equivalent to the calibration, such maneuvers can be pre-programmed and automatically executed, or manually controlled.

3.1.2. Workspace Characteristics

On a conceptual basis, possible workspaces of a WMDS are limited by the following aspects, which shall be checked prior to operation:

- The *tire-underground pairing* must provide the required friction to perform the accelerations demanded by the driving simulation experiment. In order to fully exploit the friction potential of tires, asphalt is recommended and low-friction coating like ice should be avoided.
- The workspace *surface* should be as *even* as possible and *free of slope* that generates forces perceptible to the test persons and interferes with the motion control. Zöller determined a maximum tolerable ground roughness[59] of $0.15\,\mathrm{m}^3$ to avoid an influence of vertical excitations on the immersion of the test person.[60] Height differences in the ground or slope that affect the tilt stability of the WMDS can especially become critical to safety.
- The intended movement area should be an open free space, i.e. *free of obstacles* that would require evasive maneuvers, which would influence the driving simulation experiment.
- The *workspace size* is theoretically infinitely increasable with the unbound motion concept. The *workspace shape* can also take on different characteristics. Nevertheless, a circular workspace is considered most appropriate for combined longitudinal and lateral motion of the WMDS and respective washout maneuvers. The size of the intended workspace is to be implemented in the MCA prior to operation.

3.1.3. Workspace Environments

The operative strategy of a WMDS is dependent on its user. When using the WMDS in a stationary location, only this specific environment must be respected in the ODD. With a mobile application and frequent change of test sites, the ODD concerning workspace environments increases for a WMDS.

A *stationary operated WMDS* can be designed to operate in a designated location, with a fixed workspace size determined by the available infrastructure. This is possibly a hall with the advantage of being independent of weather and other environmental influences and physically controlling the access to the hazardous area of motion. This would be similar to the operating conditions of previous rail-based simulators.

In contrast, a *high flexibility WMDS* is to be designed to actually be portable and operate indoors or outdoors. The more often a WMDS changes its workspace, the less time it should take to set

[59] The roughness coefficient is a parameter used by Zöller to describe the quality of a driving surface and corresponds to the power spectral density of the surface excitation at a reference frequency of $1\,\frac{1}{m^3}$.

[60] Zöller, C. A.: Diss., Application of WMDS to uneven grounds (2019).

up the infrastructure. This means that a WMDS operating zone is not physically separated from the environment but is, for example, only made visible by ground markings or punctual barriers like pylons. This requires to adapt the system towards external users and objects moving in the environment, as well as to weather influences.

In order to develop a safety architecture that can prevent any hazard reasonably conceivable during WMDS operation, an operative environment most prone to hazards is assumed for the following steps of this work. The August Euler Airfield is an example for such a worst case operative environment for WMDS. This is where MORPHEUS 2.0 is planned to be operated in a first phase. It is characterized by its multi purpose use (driving dynamics test track and airfield), which does not enable the built-up of fixed protecting infrastructure. This bears the potential of third persons being present during a driving simulation and while maneuvering the vehicle manually to intended positions. Persons are mainly adults, but small persons / children and general bad visibility due to dark cloths can not be excluded. Additionally, vehicles are moving in close proximity to the workspace and infrastructural objects like trailers and hangars are in close proximity to the test field. Since the site is located in a nature reserve, even wildlife are possible objects of interference. Fig. 3-3 shows the top view of the location. The designated workspace is a circle with 50 m in diameter. Outside this diameter, the underground switches from asphalt to grassland with slope and strong unevenness.

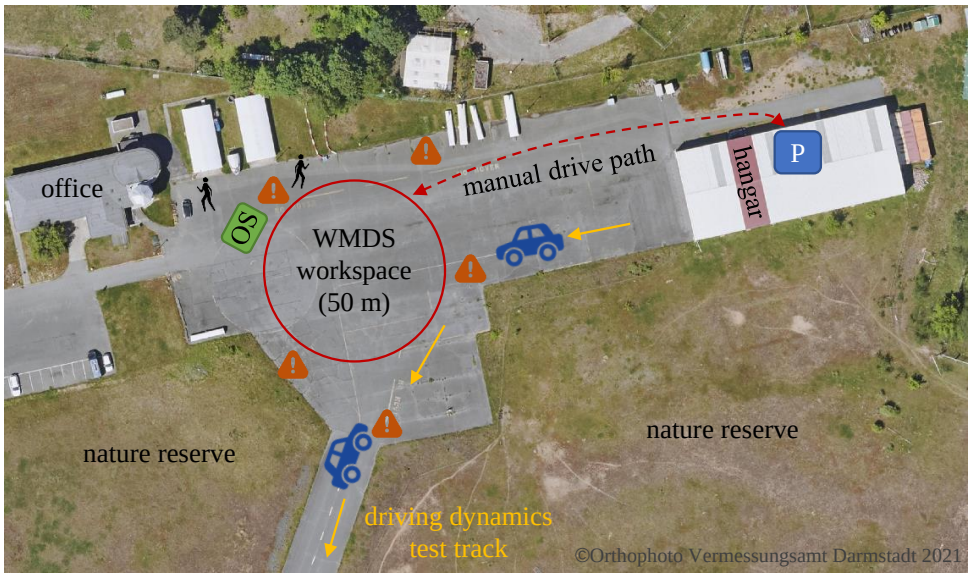


Figure 3-3.: Operative environment of MORPHEUS 2.0: August Euler Airfield in Griesheim, multi-purpose area with hangar and vehicle dynamics test track. The operator station (OS) is portable and placed next to the workspace.

3.1.4. Weather

With an outdoor application of WMDS, weather influences must be either mastered or excluded from the ODD, meaning a limitation for the operational conditions and availability of a WMDS. The prototype MORPHEUS 2.0 is designed water proof. This is mainly chosen to protect the

hardware in case of downtime or during transport under sudden rain. The actual applicability of the WMDS under light rain is conceivable but has not yet been investigated, while heavy rain should be excluded as it affects the friction of the tires and the noise in the WMDS cabin. Therefore, the ability to operate during light rain is not mandatory, but seen as an additional benefit. Fog, hail and snow are nevertheless excluded. Operation should take place only at bright times of day (no nightly operation), with possible low angles of sunlight.

3.2. Hazard Analysis and Risk Assessment

As part of the development of MORPHEUS 2.0 at TU Darmstadt, a comprehensive hazard and risk analysis in compliance with the steps of ISO 12100 and ISO 14121-2 was performed as a starting point for an overall safety concept, in combination with the HARA performed by Wagner[61]. Within this course, hazards relevant for the basis of this work were revealed, as they motivate the addition of further protective measures. Rather than describing the results of the overall HARA, the basic procedure is explained, but the focus is on collision hazards relevant for this work.

3.2.1. Hazard Identification

Hazardous areas and respectively possible harm of the machine to persons are identified with help of the checklist of Annex B in ISO 12100[62]. From this, the following top level hazards (TLH) are formulated as a starting point for the further hazard analysis:

- TLH1: *Collision of any external person* on the *workspace* with (parts of) the WMDS in motion (driving simulation, manual drive, maneuver drive)
- TLH2: *Collision of the test person* within the *cabin* during driving simulation or during boarding / unboarding the cabin
- TLH3: *Crushing of external persons* within moving parts of the *WMDS hardware* during boarding (test person and assistant), system startup / testing (operators) or maintenance (mechanics)
- TLH4: *Motion sickness* or general *physical or mental discomfort of the test person* in the *cabin* during driving simulation
- TLH5: Harm due to *inaccessibility of the test person in the cabin* in emergency situations during driving simulation

[61] Wagner, P.: Diss., Practical Feasibility and Functional Safety of WMDS (2018).

[62] ISO: ISO 12100:2010 - Safety of machinery — Risk assessment and risk reduction (2010). pp. 64 ff.

- TLH6: *Electrical shock of any person* touching the *WMDS hardware* during boarding (test person and assistants), driving simulation (test person), system startup / testing (operators) maintenance / battery charging (mechanics)

The focus in this work is to establish safe motion of WMDS, therefore to avoid collisions between the WMDS and environmental objects or persons interacting with it. Thus, only **TLH1 and TLH2** are further examined in this work, while the other TLH are treated in an overall safety concept within the project MORPHEUS 2.0. Even though TLH4 also refers to the motion of the WMDS, this hazard was identified to not cause irreversible harm to persons and to be solvable with communication and human intervention.

A collision hazard between the WMDS and external objects (TLH1) exists when the WMDS is in motion and the object in question is within a critical distance for either the object or the WMDS to take an avoiding action. A collision hazard for the internal test person (TLH2) is a possible consequence of strong inertial forces that cannot be secured by the seat belt. These are possibly generated by an impact of the WMDS when colliding with external objects, which further refers to TLH1. Furthermore, loosing tilting stability and a possible overturn would create a strong impact on the WMDS cabin. Besides this, highly dynamic driving maneuvers could generate high forces acting on the test persons as well, depending on the maximum accelerations the WMDS drive system can generate. This is not further respected in the following, as the WMDS drive system of MORPHEUS 2.0 can generate maximum accelerations of $5.4\,\mathrm{m/s^2}$, which is below the possibilities of most road vehicles. Additionally, WMDS motion generally is hazardous while the test person is not secured with a seat belt or not even seated. This is a common safety issue in highly dynamic DS and is also not further addressed here, as it can be solved with seat belt sensors and user instructions, which was addressed in Lutwitzi's master thesis[63].

In the following, the collision hazard between the WMDS and its environment is further addressed, with the potential consequence of harm to external persons as well as to the test person within the simulator dome. Therefore hazardous events (HE) are derived, that lead to TLH1 or TLH2 and which are caused by deviations from the human or machine target behaviour in the respective operative modes:

Driving Simulation:

As the WMDS requires an obstacle free space, the operation is expected to be started when the workspace is completely cleared. To remain the WMDS within a safe state, the workspace must remain cleared during the operation and the WMDS must not move outside this cleared, prescribed workspace, as the surrounding might contain obstacles and the ground surface might not meet the specifications. Respectively, the WMDS must perform washout maneuvers and approach the center of the workspace in the meantime. When approaching the border, braking and

[63] Lutwitzi, M.: Master Thesis, Safety Architecture for WMDS (2019).

return maneuvers must be induced, which is noticeable in a reduction of the radial driving speed towards the border. HE resulting from possible deviation of this target behaviour are accordingly:

- HE1: Persons or objects enter the WMDS workspace during driving simulation, possible collisions with persons (TLH1) or objects (leading to TLH2).
- HE2: The WMDS does not adapt its trajectory sufficiently in the border area and leaves its designated workspace during driving simulation
  - HE2.1: with possible collisions with persons (TLH1) or objects (leading to TLH2).
  - HE2.2: with a possible turn-over leading to TLH2.
- HE3: The WMDS moves unintended from standstill prior to driving simulation with an unprepared environment leading to collisions with persons (TLH1) or objects (leading to TLH2).

These identified HE equivalently apply to the automated maneuver mode, despite TLH2 is not a respective consequence as long as no test person is within the cabin.

Manual Drive:

During manual drive, the WMDS must react with the expected motion according to the drive inputs given by the operator. Thereby, a safety distance of persons to the WMDS shall be established and the operator must control the WMDS without hazardous approaches to persons. Since it is not intended to transfer persons within the cabin during manual drive, a potential collision with infrastructure is not hazardous to human, but should of course be avoided to prevent from mechanical damage of the vehicle. Hazardous events resulting from possible deviation of this target behaviour are accordingly:

- HE4: The WMDS moves unintended from standstill in manual drive mode with an unprepared environment leading to possible collisions with persons (TLH1).
- HE5: The WMDS performs an unintended trajectory during manual drive with possible collisions with persons (TLH1).

3.2.2. Risk Estimation

To evaluate the risk associated to HE, causal factors are derived by investigating possible sources of human or machine failure causing the HE. Rather than identifying machine failures up to component levels, these failures remain on the highest possible level to keep the overall scope small when evaluating the risk of the hazards. The results are expressed as scenarios. A profound list of the hazard analysis is available in Annex A.

The risk of each scenario is estimated with the risk parameters *severity of harm* (S), *frequency of exposure* to the hazardous area (F), *avoidability* of the harm (A) as well as the *probability* of the

HE occurring (O). The parameters S, F, A and O are transferred into a PL / SIL with help of the risk graph according to Fig. 2-1. The availability of previous safety functions defined by Wagner is not considered in this risk assessment, since the method used is intended to determine the initial risk of the machine without safety functions. Nevertheless, previously determined measures are considered in the later definition of safety goals. This allows novel and previous risk reduction measures to be determined in combination and with a new distribution of the required safety integrity levels.

Scenario 1 (HE1): Persons/Objects enter the workspace during driving simulation / maneuver mode and collide with the WMDS: Assuming that the WMDS has a dedicated area of motion, that is not physically fenced, persons / vehicles or wildlife could (unconsciously) enter the workspace during operation. This can be attributed to inattention, poor marking of the operating area or deliberate disregard of the boundaries, for example, because the passage is needed by other users of the multi purpose area. The exposure of a person working close to the workspace is considered a regular situation (F2). As the trajectory of the WMDS within this permitted workspace is not predictable and especially not adapted to sudden obstacles, rapid changes in the direction at high speeds can occur, possibly leading to hazardous approaches. This might be underestimated by respective objects and, in the worst case, an own evasion can become impossible. An action on the part of the WMDS would have to be initiated by the operators, e.g. by an emergency brake. However, the larger the workspace is and the further away the operator station is from the borders accordingly, the more difficult it can become to correctly detect such dangerous approaches between WMDS and objects entering the workspace (A2). The probability of occurrence of an undesired entering of the workspace is estimated to low, but depends on the compliance with instructions (O2). A collision with the WMDS can cause death to the external person in the worst case (S2). Depending on the structure of the collision object, the person within the WMDS can also be harmed seriously by the impact.

The risk is estimated to a risk index of 3 (S2, F1, O2, A2) according to the risk graph in Fig. 2-1.

Scenario 2 (HE2.1): The WMDS leaves its designated workspace during driving simulation / maneuver mode and collides with persons / objects: In the immediate vicinity of the operating area, there could be rigid objects such as trees, buildings or other vehicles, as well as people relying on the WMDS to stay within the designated area. The WMDS performing highly dynamic maneuvers in close proximity to the workspace borders occurs often (F2). Even though the permissible workspace is limited within the MCA, the failure of a function or component required for motion execution or control possibly causes a WMDS's trajectory to deviate from the expected / permissible one, thus exceeding the workspace. This corresponds to the danger of an uncontrollable WMDS as described within Wagner's HARA (cf. Chapter 2.2.5). Additionally, the MCA or MC algorithms can fail to plan and execute the return maneuvers sufficiently, due to control flaws or systematic faults in the software programming. Despite functional fault, human failure can be responsible, e.g. when the workspace size has not been adequately implemented in

the MCA or the initial workspace point has been set faulty. Without taking into account existing measures to safeguard motion controllability according to Wagner, the probability of occurence is expected to be high, since a single fault in any component can cause the WMDS to perform an undesired trajectory (O3). A reaction on the part of the operators by manual stopping is considered hardly possible equivalent to Scenario 1 (A2). Outside of its specified field of movement, the ground conditions can cause extended braking distances, which also complicate controllability by manual braking. The possible severity of harm is also evaluated equivalent to Scenario 1 with a possible serious injury or death to the internal or external persons (S2).

A risk index of 6 (S2, F2, O3, A2) is assigned to the scenario.

Scenario 3 (HE2.2): The WMDS leaves its designated workspace during driving simulation and turns over: The WMDS is designed to remain stable against turning over by its wheel base. Nevertheless, this design is with respect to a certain specification concerning possible acceleration forces, estimated height of center of gravity, drag through wind forces and surface slope. When moving out of its intended workspace, as described in scenario 2, a possible consequence is that by entering an environment that no longer meets the WMDS' specification of underground, the tilt stability can be affected, which in the worst case leads to a turnover and ground collision of the WMDS cabin. The consequences for the test person are a strong impact with possible serious injury or death (S2). The avoidability of a turn over once this happens evaluated as low (A2). Nevertheless, the actual occurrence of surface properties leading to a turn over is evaluated to very low, since the WMDS is designed towards standing stability respecting safety factors (O1).

The risk index for this scenario is evaluated to 4 (S2, F2, O1, A2).

Scenario 4 (HE3, HE4): Unintended start of motion from standstill (start-up or boarding mode): Prior to the operational modes, various tasks need to be absolved in direct proximity to the vehicle, especially during boarding mode. Hence, it is required to wait with the actual start of motion until each person or equipment is moved away from the hazardous area. Nevertheless, an early or unexpected start can occur with an unintended start input from the operator due to an accident or insufficient insight into the area around the vehicle. This is especially dangerous, if the active mode of operation is a preprogrammed maneuver with a sudden acceleration of the vehicle. The avoidability once this occurs therefore is expected low (A2). Nevertheless, as the operator is trained in its tasks, the probability of occurence of such a fault is evaluated to very low (O1). The frequency is high (F2), as the starting and stopping of the WMDS is a regular task absolved multiple times within a regular day of operation. The consequence is a collision with external persons possibly leading to serious harm (S2).

The risk is estimated to a risk index of 4 (S2, F2, O1, A2).

Scenario 5 (HE3, HE4): Unintended operational mode: Furthermore, an active run mode deviating from the intended run mode can become hazardous during the starting process, when e.g. a pre-programmed maneuver with fast acceleration is started instead of an intended manual

drive mode that would require less safety distance. This could be attributed to human error as well as systematic errors in the software development. The consequence is a collision with external persons possibly leading to serious harm. The risk estimation is equivalent to scenario 4, with a risk index of 4.

Scenario 6 (HE5): Unintended trajectory during manual drive: Manual control is a frequent task in the operation of a mobile WMDS (F2), as the vehicle must be moved to the workspace and to a boarding position for the test persons. Thereby, the skills of the operators are of importance. Accordingly, human error is a major hazard. Distraction, overstrain, unintuitive control elements or even insufficient insight into the travel corridor of the WMDS can lead to unintended or impermissible commands. Since the operator is trained in its task, the propability of occurence nevertheless is evaluated as low (O2). From part of the machine, functional failure in the remote control device or in the drive system of the WMDS can cause a loss of control, which is evaluated as highly probable due to a high number of potential failure causes (O3). The hazardous event can cause dangerous approaches to surrounding objects and collisions in the worst case (S2). Since the presence of persons in the cabin can be excluded during manual control, persons are only endangered externally. The avoidability of this event can be enhanced by limiting the drivable speeds within the manual drive mode (A1).

The risk is estimated to a risk index of 4 for human failure (S2, F2, O2, A1) and a risk index of 5 for machine failure (S2, F2, O3, A1).

3.2.3. Conclusion

The presented method enabled the evaluation of risk connected to potential sources of danger from a behavior-oriented system level, which includes humans as part of the overall WMDS system. In contrast to Wagner's inductive approach, which assumes malfunctions in the system and concludes from this to dangerous behavior of the WMDS, this approach especially considers human failure and therefore leads to hazards that have not been evaluated by Wagner so far. Additionally, due to the high level of risk assessment, only a small number of hazards is derived. On the other hand, Wagner's approach provides causal factors for the occurrence of machine-related failures that would, for example, further specify HE2, and evaluates the connected risk separately. If new safety-related functions are defined for the WMDS based on the previously identified initial risk, a possible next step is to evaluate their functional safety using Wagner's method. The two methods should therefore be regarded as complementary.

The risk assessment performed is subjective and conservative, considering worst-case conditions for flexible WMDS operation. These are primarily characterized by direct access of people or other objects to the test site, unsafe underground conditions externally, and the difficulty of operators to react to hazards due to the hard overview of the test site. All scenarios are rated with a risk index greater than 1, which requires further risk mitigation methods.

3.3. Safety Goals

From the hazards and connected risk identified, the next step is the definition of safety goals that define the level of intervention of safety measures. Each HE is assigned a safety goal (SG), while it is attempted to define common safety goals as far as possible. Considered measures either reduce the probability of occurrence of the hazardous situation or control the hazard by avoiding harmful consequences once the hazardous situation occurs. If the measures refer to a function executed by the WMDS, a PLr / SIL requirement is added according to the risk parameters identified, as well as Fig. 2-3 in combination with Tab. 2-1.

Scenario 1 (HE1) - Persons/Objects enter the workspace during driving simulation and collide with the WMDS: Reducing the probability of a collision with external persons means measures must be taken to ensure that people cannot get into a collision-critical proximity to the WMDS. This would be achieved by an inherently safe design of the operating area, meaning the access is not possible for human due to physical barriers. As this does not match with the intention of a mobile and flexible operation, since physical fences require build up times and must be fitted to the actual workspace size, this variant is not further considered.

Control of the occurring hazardous situation includes that the situation must be detected and a countermeasure avoiding a collision must be triggered, by means of the addition of a safety function as step two of the risk reduction procedure. By sensing the hazardous approach of a person, the WMDS initiates a counteraction that avoids the actual collision. The protection can be initiated once a person enters the workspace, which requires the observation of the workspace borders, or once a person is actually in a collision critical proximity to the WMDS, which requires the observation of a specified vehicle-bound area. In the latter case, the counteraction can be an evasive maneuver, which is not favored due to a required trajectory planning around a detected object, or a simple braking to standstill. Since the driving simulation is disturbed by any intervention and a braking to standstill is always considered safe, this is chosen as a reaction. Linked to this condition is the safety goal that the WMDS must be able to stop at any time. This could be further treated by an inherently safe design of the drive and braking system, which was discarded by Wagner, or with the addition of an external safeguard, which corresponds to the EEBS. From the risk parameters identified for scenario 1, applied to a PL based risk graph, the required safety performance is PLc or SIL1 for all safety functions intending to achieve the safety goals derived for Scenario 1:

- SG1: The WMDS shall be stoppable at any time. (SIL1)
- SG2.1: The WMDS shall detect objects entering the WMDS workspace and shall initiate a braking maneuver so that a collision is avoided (SIL1), or
- SG2.2: The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided (SIL1).

Thereby, SG2.1 and SG2.2 are alternatives both sufficiently reducing the risk of scenario 1, whereby SG2.1 additionally requires that the workspace is initially checked for objects and confirmed as cleared, before the operation can start. The WMDS performs a braking maneuver once a person or an object is within a critical area with the effect that a collision is avoided.

Scenario 2 (HE2.1) - The WMDS leaves its designated workspace during driving simulation and collides with persons / objects: The hazardous event is caused by an hazardous approach of the WMDS to objects or subjects standing outside the workspace due to a violation of its workspace limits. Reducing the probability of a collision occurrence in this case means it must be avoided that failures occur that lead to leaving the workspace. These correspond to the safety critical failures identified by Wagner leading to uncontrollability of the WMDS. Avoidance of such failures has already been excluded by Wagner due to the need for a high number of redundant components. On the other hand, initiating a counteraction, e.g. a braking, once a failure occurs that bears the potential of exceeding the workspace is a possibility of hazard avoidance. A respective safety goal therefore is that the WMDS shall avoid to leave its predefined workspace in case of failures, which at least requires a fail safe braking system and a diagnosis to apply the braking at the right time before leaving the workspace.

Controlling the hazardous situation means that the hazardous approach towards objects outside the workspace must be detected and a countermeasure must be started. This is already achieved by SG2.2 as defined for scenario 1, but requires that once the workspace is left, the braking process is still predictable and not disturbed e.g. by insufficient friction conditions. As this is difficult to guarantee outside the intended workspace or would further limit the place of application of WMDS, the safety goal is considered insufficient for appropriate risk reduction. The risk parameters identified for scenario 2 lead to a PLe or SIL3 for the safety goals preventing risk in scenario 2:

- SG1: The WMDS shall be stoppable at any time. (SIL 3)
- SG3: The WMDS shall detect failure that can cause leaving its predefined workspace and initiate a braking maneuver so that the workspace limits are not exceeded. (SIL3)

Scenario 3 (HE2.2) - The WMDS leaves its designated workspace during driving simulation and turns over: The hazardous event includes a hazardous approach of the WMDS towards unsafe undergrounds outside its workspace. Excluding that the WMDS workspace is surrounded by hazardous undergrounds would limit the applicability of the WMDS to flexible test sites. SG2.2 has no effect in this case as long as unsafe undergrounds cannot be detected likewise possible collision objects. Otherwise, the workspace is required to be framed with physical installations that enable a detection of workspace borders likewise a collision object. Therefore, SG3 in combination with SG1 must be fulfilled to reduce the risk. The risk parameters identified for scenario 3 lead to a PLd or SIL2 and the following safety goals:

- SG1: The WMDS shall be stoppable at any time. (SIL 2)

- SG3: The WMDS shall detect failure that can cause leaving its predefined workspace and initiate a braking maneuver so that the workspace limits are not exceeded. (SIL2)

Scenario 4, 5, 6 (HE 4, 5, 6): These scenarios refer to unintended trajectories of the WMDS while the vehicle is in hazardous distance to objects. If it is not avoidable that persons must be present in the proximity to the WMDS, the probability of occurrence of faults on side of the operators could be avoided by an intuitive design of control elements, counter checks of start and mode inputs and enhanced insight on the area around the vehicle. Nevertheless, the success of such measures is hardly predictable. The safer possibility therefore is to prevent from human error by safeguards. While these scenarios also refer to operating modes outside a predefined workspace, SG2.1 is not effective. On the other hand, SG2.2 refers to protection from collisions independently of the workspace and therefore reduces the risk in these scenarios as well, in combination with SG1. If the hazardous approaches result from a failure in the remote control or drive system, SG2.2 is also effective to reduce the risk of a potential collision. The highest risk of these scenarios stems from scenarios 5 and 6 and leads to a PLd or SIL2.

- SG1: The WMDS shall be stoppable at any time. (SIL 2)
- SG2.2: The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided. (SIL2)

The risk es evaluated as sufficiently minored, as with the active collision protection by braking of the WMDS, any unintended drive or start input or unintended maneuvers will finally not lead to a collision.

Resulting Risk Reduction Strategy

The need for an active collision avoidance function becomes apparent unless it can be guaranteed that the WMDS will only operate in an area inaccessible to persons, including automated and manual drive mode. At the same time, active collision avoidance is not sufficient to avert all hazards, since the person within the WMDS may be in danger even if a collision object is not present, if it leaves its specified operating range in an automated mode. Therefore, a second function is required that ensures the compliance with its workspace limits. The continuous controllability of the system, at least by emergency braking, is to be seen as a basic requirement for the effectiveness of both. Concluding, three different safety goals must be fulfilled in order to reduce the risk of all identified hazards concerning motion and collision risk for internal or external persons. The highest SIL assigned to a common safety goal is the finally valid requirement to sufficiently mitigate the risk in all cases. This leads to the following safety goals for risk reduction of a WMDS concerning its safe motion:

- SG A: The WMDS shall be stoppable at any time. (SIL 3)
- SG B: The WMDS shall detect failure that causes leaving its predefined workspace and initiate a braking maneuver so that the workspace limits are not exceeded. (SIL3)

- SG C: The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided. (SIL2)

Since the EEBS ensures that the WMDS is stoppable at any time and thereby fulfills SG A, this function is not required to be further specified within this work, but is considered available and safe. SG B is also addressed by Wagner's safety function requirements, but is required to be further specified with monitoring requirements and trigger conditions. Therefore, it is also treated as a novel safety function within this work. SG C is a new function for the WMDS and will therefore also be specified in the further course of the work.

With the definition of the three safety goals, all hazards identified within the analysis are treated. A profound reevaluation of the HE is shown in Annex A, where it can be seen that the risk index is reevaluated to 1 in all cases. Therefore, RH1.1 could not be falsified and thereby is corroborated.

4. Derivation of Safety Functions and Requirements

Within this chapter, the safety goals SG B and SG C are decomposed in required safety functions and subfunctions as a division into *sensory detection*, *evaluation/decision logic*, and *action*. In the decision logic, based on the sensed quantities, a decision is made whether a safety-related action must be performed or not. It is shown in the following that different variants of sensed quantities and corresponding triggers for the action are possible, but thereby effects on the usable range of motion occur. The minimum set of required subfunctions is evaluated by weighting up the lowest possible complexity of safety relevant functions and the effect on the regular WMDS operation. Thereby, the concepts are developed fail safe instead of fail operational to reduce system complexity, and respective requirements of failure diagnosis and fault reaction are included (cf. Fig. 4-1). Furthermore, requirements on the subfunctions are derived, concerning the *general target function* and *functional safety*. Requirement categories for this are derived by analysing possible sources of failure, originating from functional failure, faulty specifications or the crossing of system limits. By the end of this chapter, requirements for the functions shall be available to such an extent that a feasibility analysis of the safety functions is possible.

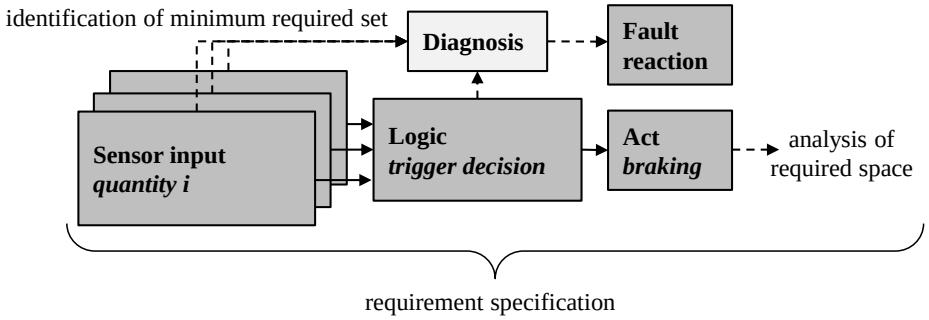


Figure 4-1.: Scheme of safety function derivation and requirement definition applied in this work.

4.1. Prerequisites

Since it has been set in the safety goals, that the hazard reaction of the WMDS is a braking to standstill, the braking procedure and relevant motion quantities are analyzed and the stopping distance of the WMDS is characterized as a prerequisite to the requirement definition.

Braking Process and Critical Stopping Distance

At the time the braking requirement occurs, the WMDS moves at speed v_{DS}. Starting from the event requiring a braking, the overall reaction time τ_{react} passes until the vehicle is actually decelerated. This reaction time includes the process of sensor data acquisition and braking trigger processing, both summarized here in the quantity $\tau_{\mathrm{react,sp}}$, and reaction time required for actuation $\tau_{\mathrm{react,a}}$, including the braking force built-up time:

$$\tau_{\mathrm{react}} = \tau_{\mathrm{react,sp}} + \tau_{\mathrm{react,a}} \tag{4-1}$$

In order to cover all eventualities, critical characteristics of the determining parameters of the stopping distance must be taken into account. Within the reaction time of sensing and processing, in the worst case, the WMDS is possibly further accelerated with its maximum possible acceleration $a_{\mathrm{DS,max}}$, until a maximum speed $v_{\mathrm{DS,max}}$ is reached. Once the braking trigger is set after $\tau_{\mathrm{react,sp}}$ passed, no more actuation of the regular drive train is possible. After the brake force build up time passed, the WMDS is decelerated, for which a conservative value for the minimum reasonably expected deceleration D_{brake} is assumed. This leads to the overall equation for the stopping distance d_{stop} for a given speed v_{DS} (Equ. 4-2) or for maximum drivable speed $v_{\mathrm{DS,max}}$ (Equ. 4-3):

$$d_{\mathrm{stop}} = v_{\mathrm{DS}} \cdot \tau_{\mathrm{react}} + \frac{1}{2} a_{\mathrm{DS,max}} \cdot \tau_{\mathrm{react,sp}}^2 + \frac{1}{2} \frac{(v_{\mathrm{DS}} + \tau_{\mathrm{react,sp}} \cdot a_{\mathrm{DS,max}})^2}{D_{\mathrm{brake}}} \tag{4-2}$$

$$d_{\mathrm{stop,max}} = v_{\mathrm{DS,max}} \cdot \tau_{\mathrm{react}} + \frac{1}{2} \frac{v_{\mathrm{DS,max}}^2}{D_{\mathrm{brake}}} \tag{4-3}$$

This equation assumes a purely straight stopping path of the WMDS. Actually, deviations from a straight-line path during the braking are possibly caused by friction value differences at the tires. Also, the stopping path can be elongated by insufficient friction between tires and road surface. Both is the case if the friction coefficient μ falls below the quotient of maximum brake system specific deceleration and gravity constant:

$$\mu < \frac{D_{\mathrm{brake}}}{g} \tag{4-4}$$

For the MORPHEUS 2.0 prototype, the maximum brake deceleration D_{brake} induced by the electromagnetic EEBS is specified to $5.7\,\mathrm{m/s^2}$. The maximum braking torque transmissible by the clamping force of the electromagnetic braking system at the brake disc does not generate braking forces for a higher deceleration. This was designed as a trade-off between an acceptable stopping distance and the mass of the braking system on the wheel, which undesirably increases the inertia around the steering axis and thereby can influence the driving performance of the WMDS. As a conclusion, only a friction coefficient of approximately $\mu < 0.6$ actually reduces the braking performance of MORPHEUS 2.0. Therefore, the considered deceleration is already a conservative value including friction deviations of the tires.

The maximum acceleration $a_{\mathrm{DS,max}}$ is limited by the maximum torque of the electric drive motors and is estimated to approximately $5.4\,\mathrm{m/s^2}$ for the MORPHEUS 2.0 prototype (cf. Tab. 2-2).

The reaction time $\tau_{\mathrm{react,a}}$ of the brake actuation given by the brake system manufacturer is $0.4\,\mathrm{s}$ until the full braking force at the clamps is available. In fact, a deceleration is reached even before that, so this estimate is conservative. The other parts of the reaction time are to be specified for the novel safety functions of the WMDS.

WMDS Dimensions

If the braking distance of the WMDS is referenced to its center point, additional knowledge of the dimensions of the vehicle in the direction of motion is essential to fully characterize the space occupied during braking. Since the WMDS has no preferred direction, it can be moved at any angle originating from its center point. However, the largest distance from the center to the edge of the vehicle is the length $l_{\mathrm{c,DS}}$ shown in a schematic illustration in Fig. 4-2. This length will be considered in the further process for the worst case alignment of the WMDS in the direction of motion. For the MORPHEUS 2.0 WMDS, this length amounts to approximately $2.9\,\mathrm{m}$, which is calculated from the wheel base parameter $l_{\mathrm{t,DS}} = 5\,\mathrm{m}$ (cf. Tab. 2-2).

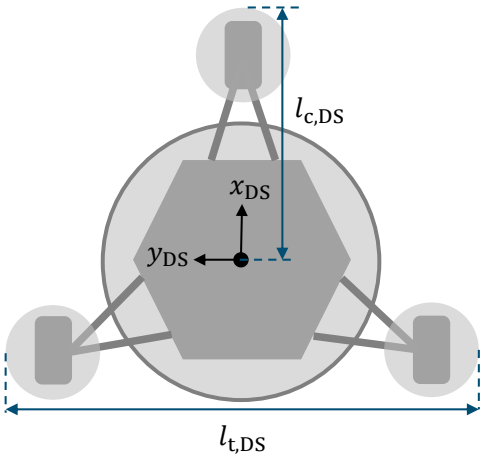


Figure 4-2.: Top view of the WMDS and maximum vehicle excursion from the center point to the outermost edge.

WMDS Motion Quantities

For a generally applicable safety function design, the maximum values for the motion quantities of the WMDS are to be assumed for the derivation of the requirements. However, the actually reached motion quantities within driving simulations can differ from the theoretically reachable values. Tab. 4-1 summarizes the mean and maximum values of $v_{\mathrm{DS,max}}$, $\dot{\psi}_{\mathrm{DS,max}}$ and $a_{\mathrm{DS,max}}$ reached within simulations of the virtual prototype of different test maneuvers on an available motion space radius of $25\,\mathrm{m}$ and a scaling factor of 0.7. This corresponds to the available space at the Griesheim Airfield, as shown in Fig. 3-3. Despite several driving styles, the WMDS does not reach its maximum speed of $15\,\mathrm{m/s}$ within the given motion space in any of the maneuvers. Also, the reached yaw rates remain below $60\,^\circ/\mathrm{s}$ for all driving styles, which corresponds to

the observations in Fig. 3-2. From this, it can be derived that limiting the WMDS speed to $10\,\mathrm{m/s}$ in the target workspace would be possible without restrictions of the driving simulation. Nevertheless, this only applies for the given workspace dimensions. On the other hand, yaw rates can be generally limited to, for example, $100\,^{\circ}/\mathrm{s}$ without leading to restrictions in any workspace size.

Table 4-1.: Simulated mean and maximum motion values of the WMDS for different representative maneuvers in a workspace radius of 25 m and a scaling of 0.7. Compared to the theoretically maximum achievable values, suggested limitations for the present workspace are given.

		Optimized City Drive (normal)	**Optimized City Drive (sporty)**	**City Drive 1**	**City Drive 3**	**City Drive 4**	**Max. values**	**Limited values****
Parameter	Unit	$R_{\mathrm{WS}} = 25$ m, scaling $= 0.7$						
$\lvert v_{\mathrm{DS,mean}} \rvert$	$\frac{\mathrm{m}}{\mathrm{s}}$	1.94	2.49	2.69	2.63	2.41	15	10
$\lvert v_{\mathrm{DS,max}} \rvert$*		6.06	8.59	8.43	7.44	7.79		
$\lvert a_{\mathrm{DS,mean}} \rvert$	$\frac{\mathrm{m}}{\mathrm{s}^2}$	0.52	0.88	1.00	0.90	0.82	5.4	-
$\lvert a_{\mathrm{DS,max}} \rvert$*		4.59	5.06	5.06	5.07	4.91		
$\lvert \dot{\psi}_{\mathrm{DS,mean}} \rvert$	$\frac{^{\circ}}{\mathrm{s}}$	2.67	3.45	3.35	3.35	3.08	360	100
$\lvert \dot{\psi}_{\mathrm{DS,max}} \rvert$		35.14	54.05	54.61	54.59	52.24		

* 99,9 % quantile

** for conditions: $R_{\mathrm{WS}} = 25$ m and scaling $= 0.7$

4.2. Workspace Compliance Function

A safety function (SF) is required, that ensures the WMDS remains within its designated workspace during a driving simulation at any time in order to fulfill SG B. This *Workspace Compliance Function (SF1)* is derived and specified in the following.

4.2.1. Safety Function Decomposition

The basic function to ensure that the WMDS remains within its designated workspace originates in the MCA, as described in Chapter 2.2.2, consisting of a reduction of demanded accelerations according to the actual position and speed as well as braking and return maneuvers. Nevertheless, such functions must be further designed towards safety in order to be applicable as a safety function, which requires the treatment of faults leading to an undesired failure of the function. With the inductive procedure of Wagner, as described in Chapter 2.2.5, faults that cause an uncontrollability of the WMDS have been identified on component level. These can possibly lead to a failure of the described function and respectively a violation of the workspace boundaries.

Furthermore, unsafe specifications or implementation faults in the MCA or MC can lead to a violation. A possible strategy, as proposed by Wagner, is that all these faults / failures must be avoided or diagnosed within the safety concept. The application of the EEBS helps to avoid that the whole system must be tolerant against failure of the relevant components. Nevertheless, if failures are not avoidable, failure diagnosis is required for every component and control logic in order to deploy the EEBS, and all of these must comply with SIL3 / PLe. As this does not support the intention of a low complexity safety concept, it is investigated, whether the safety function can be simplified by defining a higher level of failure diagnosis. Besides observing or avoiding a *failure on the component level*, an observance of *failure on the behavioural level* of the WMDS is an option. If it is possible to stop the WMDS without a collision as soon as a maximum tolerable position limit is exceeded due to any functional fault in the respective components, it is sufficient to observe this position limit with the respective SIL/PL.

In the following, possible designs of such limits (sensing quantities) and the consequences for the usable workspace are investigated.

Concept 1: Virtual Barrier

A first option is to define a motion space limit that is observed within the actual WMDS workspace and triggers a braking when crossed. The term *virtual barrier* is introduced, which refers to this observed limit. Respectively, the motion space limit within the MCA must be defined smaller, so that an exceeding of the virtual barrier only occurs when failures are present. The virtual barrier must be defined safely, meaning in such a way that the actual workspace limitation is not crossed when conducting the emergency brake maneuver. This requires the availability of roll out zones between the virtual barrier and the workspace border, further referred to as *safety buffer* in the following. The safety buffer design is an important part for the avoidance of unsafe function specifications leading to a violation of the safety goal. It must allow a deceleration to standstill in any case, which is dependent on the actual speed of the WMDS. Although the motion cueing adaptation described in Chapter 2.2.2 induces a reduction of the WMDS speed towards the workspace boundary, it cannot be relied upon that this speed reduction really is achieved with the respective SIL requirement, unless all sensor, processing and actuation components of motion control and execution involved in this are classified with SIL3 as well. Therefore, this buffer zone is required to be scaled according to the overall maximum achievable WMDS speed to cover all eventualities, meaning according to Equ. 4-3. Thereby, pure radial motion must be considered as a worst case, so that an unexpectedly non-straight-line braking path or sudden change of direction is nevertheless no danger to compliance with the limit. When assuming that the WMDS' position is referenced to its center point, the dimensions of the WMDS from the center to the outer edge $l_{\mathrm{c,DS}}$ must be further included in the buffer.

For a given workspace (WS) radius R_{WS} on a WMDS test field, the radial buffer d_{buffer} leads to a

reduction of the actually usable motion space (MS) radius R_{MS} for a fault free state:

$$d_{\mathrm{buffer}} = d_{\mathrm{stop,max}} + l_{\mathrm{c,DS}} \tag{4-5}$$

$$R_{\mathrm{MS}} = R_{\mathrm{WS}} - d_{\mathrm{buffer}} \tag{4-6}$$

The safety function is described by the following subfunctions, which all require to fulfill the SIL / PL requirement of SF1 (SIL3/PLe):

- SF1.1: (sense) An exceeding of the WMDS of the virtual barrier is determined.
- SF1.2: (logic) A braking trigger is set, if the virtual barrier is crossed.
- SF1.3: (act) The WMDS is transferred to standstill after a braking trigger is set.

Since this motion space reduction is unfavorable especially for small workspaces, further adaptions of this concept are considered in the following.

Concept 2: Virtual Barrier and Global Speed Limitation

A global limitation of the maximum drivable WMDS speed is conceivable to reduce the required buffer zone size. As the WMDS may not reach its maximum speeds within the driving simulation in smaller workspaces (cf. Fig. 3-2), it is possible to globally limit the WMDS speed towards an expected maximum driven speed, depending on the workspace size. Then it becomes possible to design the buffer zone towards this limited speed $v_{\mathrm{lim,max}}$. However, it must be ensured with a SIL3 / PLe requirement that this limited speed is actually never exceeded. This can be achieved by an additional measurement unit that checks the speed of the WMDS continuously and initiates an emergency braking if the maximum permissible value, for which the buffer zone was designed, is exceeded. Concluding, the safety function is extended by a further measurement quantity.

In Fig. 4-3, the benefit of a global WMDS speed limit in dependence on the intended motion space is illustrated. Within simulations with the data set *Real City Drive 3*, the motion space size is varied and the maximum driven WMDS speeds are determined in order to estimate reasonable speed limits for the given motion space. Then, the required buffer zone is estimated by the stopping distance according to Equ. 4-3, leading to a value for the required overall workspace size (Equ. 4-6). The left y-axis of Fig. 4-3 shows the ratio of the required workspace radius towards the motion space radius for a safety buffer design according to the maximum WMDS speed and the limited WMDS speed. The underlying maximum driven speeds in dependence on the motion space diameter are illustrated on the right y-axis.

The results show, that when adapting the buffer to a limited speed according to the maximum driven speed from the experiment, the required increase of the workspace is $80\,\%$ for small motion space radii of $10\,\mathrm{m}$ and decreases towards $25\,\%$ for large motion space radii. On the other hand, when adapting to the absolute maximum WMDS speed, the additional need for space for a $10\,\mathrm{m}$

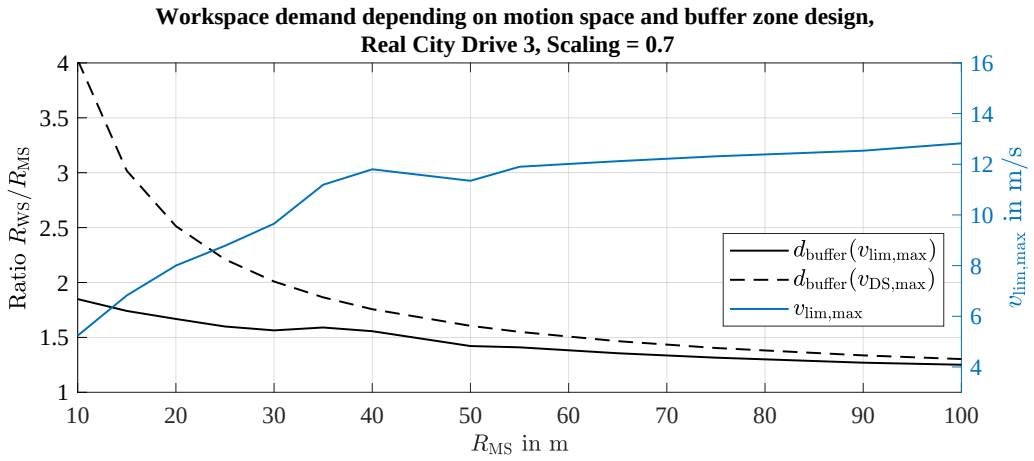


Figure 4-3.: Required workspace increase by buffer zone depending on the motion space and the applied speed limit. Suitable speed limits are estimated by the maximum driven speeds within the simulation of the Real City Drive 3. Without a speed limit, the buffer zone is designed towards the maximum WMDS speed.

radius is $300\,\%$ and therefore unreasonably high.[64] A speed limitation and monitoring for the purpose of a smaller required buffer zone is therefore highly valuable. The difference between the two approaches decreases as the workspace radii increase, but only from a motion space size of more than $100\,\mathrm{m}$, an equalization between both concepts is expected.

The results justify that a speed limitation and observation is useful for workspace sizes below $100\,\mathrm{m}$ for the current WMDS design with a maximum speed of $15\,\mathrm{m/s}$ to enhance the usable motion area. Nevertheless, more than $50\,\%$ of the theoretically available workspace is still lost for the buffer zone for workspace sizes below $40\,\mathrm{m}$. The concept further extends the required subfunctions as follows:

- SF1.1: (sense) An exceeding of the WMDS of the virtual barrier is determined.
- SF1.2: (logic) A braking trigger is set, if the virtual barrier is crossed.
- SF1.3: (sense) The WMDS speed is determined throughout the motion space.
- SF1.4: (logic) A braking trigger is set, if the global speed limit is exceeded.
- SF1.5: (act) The WMDS is transferred to standstill after a braking trigger is set.

Concept 3: Local Speed Limitations

Another possibility to further enhance the usable motion space is to observe local speed limitations that apply throughout the workspace in dependence on the radial distance of the WMDS to the outer workspace limit. Thereby, the WMDS is allowed to achieve higher speeds in proximity to the workspace center, but is limited to lower speeds in the workspace border area, respectively to the MCA implementation. The compliance check of the *Workspace Compliance Function*

[64] The WMDS can theoretically still reach its maximum speed of 15 m/s in a motion space with a radius of 10 m if it accelerates fully from one boundary to the opposite side over a distance of correspondingly 20 m.

therefore is not only applied to a specific border limit, but the combination of position and speed is continuously checked towards limitations throughout the workspace. Whenever a limit is exceeded, an emergency braking is initiated. Therefore, the limitations must respect that for the given speed at actual position, there is always enough space to the outer workspace limit for an emergency brake. Here as well, the limits set in the MCA must be below the limits of the safety function, so that emergency braking only occurs when the regular motion control has actually failed. This eliminates the further need of a safety buffer around the workspace and makes the whole workspace usable, but further extends required subfunctions in the safety function.

To determine the position dependent speed limits, a braking maneuver with straight line path in purely radial direction as a worst case is considered. The maximum tolerable radial position of the center of the WMDS towards the workspace center $p_{r,\mathrm{DS,lim}}$ is determined by the given workspace size R_{WS}, the actual absolute WMDS speed v_{DS} as an input to Equ. 4-2 or Equ. 4-3 and the dimensions of the WMDS from the center to the outer edge $l_{\mathrm{c,DS}}$. This results in the radial position limit of the WMDS $p_{r,\mathrm{DS,lim}}$ for a given driving speed, in order to be able to come to a standstill inside the workspace under worst-case conditions:

$$p_{r,\mathrm{DS,lim}}(v_{\mathrm{DS}}) = R_{\mathrm{WS}} - d_{\mathrm{stop}}(v_{\mathrm{DS}}) - l_{\mathrm{c,DS}} \tag{4-7}$$

The actually usable motion space towards the workspace size with this concept is only limited by the remaining components of the stopping distance calculation for $v_{\mathrm{DS}} = 0$ and the dimensions of the WMDS body:

$$R_{\mathrm{MS}} = R_{\mathrm{WS}} - d_{\mathrm{stop}}(v_{\mathrm{DS}} = 0) - l_{\mathrm{c,DS}} \tag{4-8}$$

According to the previous calculation, the current absolute driving speed of the WMDS is limited on the basis of the worst case of purely radial motion. In fact, for the same radial position, higher speed limits can be tolerated for purely tangential motion, as the remaining distance towards the workspace border is larger in tangential direction. The radial limit for purely tangential motion is calculated as follows:

$$p_{r,\mathrm{DS,lim}}(v_{\mathrm{t,DS}}) = \sqrt{R_{\mathrm{WS}}^2 - (d_{\mathrm{stop}}(v_{\mathrm{t,DS}}) + l_{\mathrm{c,DS}})^2} \text{ for } v_{\mathrm{r,DS}} = 0 \tag{4-9}$$

However, in order to limit the speed in consideration of the radial and tangential speed components, the speed of the WMDS in the earth-fixed coordinate system must be known and the current speed vector must be evaluated for the remaining distance towards the workspace border. Such a separate consideration of the speed components is worthwhile if the limits designed for radial motion restrict the motion space of the WMDS such that the driving simulation quality suffers from this. However, this introduces additional sources of error and is also sensitive to deviations in the actual direction of movement of the WMDS during emergency braking. A design of the absolute speed for the worst case of purely radial motion accroding to Equ. 4-7 is thus more robust against deviations of the measured variables or braking paths, which is why this method is further considered.

An exemplary calculation for $R_{\mathrm{WS}} = 25\,\mathrm{m}$, the MORPHEUS 2.0 specific parameters given in Chapter 4.1, as well as an estimated sensing and processing time of $\tau_{\mathrm{react,sp}} = 0.1\,\mathrm{s}$ yields the limits for position dependent absolute WMDS velocity shown in Fig. 4-4. It becomes visible that the maximum WMDS speed of $15\,\mathrm{m/s}$ is not tolerable in this given motion space. However, the maximum tolerable speed is still above the suggested global speed limit $v_{\mathrm{lim,max}}$ for this workspace size, which was determined from maximum values reached throughout the simulated driving simulation maneuvers with the given workspace size (cf. Tab. 4-1).

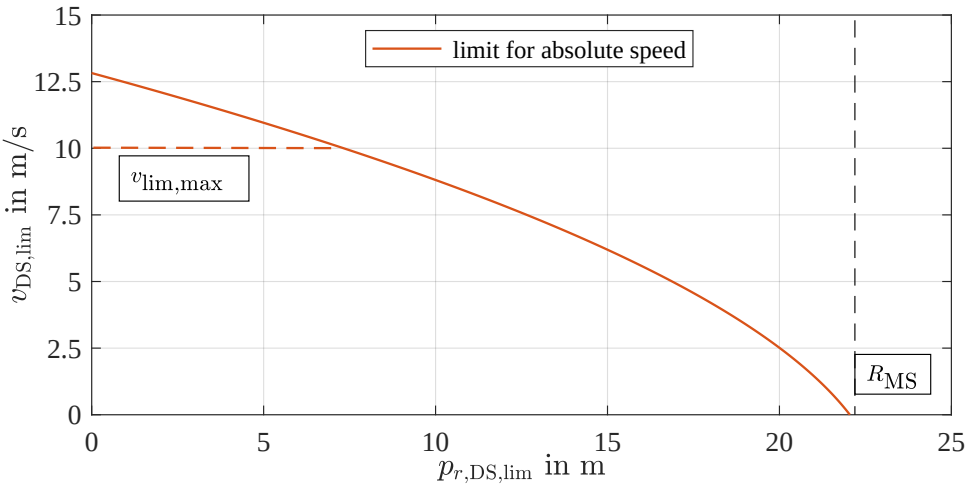


Figure 4-4.: Radial speed limits determined for the absolute WMDS speed in a workspace radius of 25 m. The limits refer to the center of the WMDS.

With this concept, the safety function is adapted by the following subfunctions:

- SF1.1: (sense) The radial position of the WMDS is determined throughout the motion space.
- SF1.2: (sense) The absolute WMDS speed is determined throughout the motion space.
- SF1.3: (logic) The WMDS speed and radial position are checked for compliance with absolute speed limits. A braking trigger is set, if an absolute speed limit is exceeded.
- SF1.4: (act) The WMDS is transferred to standstill after a braking trigger is set.

Conclusion

The local speed limitations (concept 3) are considered a valuable compromise between usable workspace and functional complexity of the safety relevant function, as the motion space size is increased. In the future, an adaption of the MCA to these limits is required. Concepts 1 and 2 only add value if an exclusive position detection at the virtual barrier offers advantages compared to a continuous localization across the workspace. This could be the case, for example, if contact sensors or light barriers were to be used as safety related sensors at the virtual barrier. However, such an infrastructure bound solution may have an impact on the flexibility of the WMDS in terms of location and worksapce sizes. Therefore, concept 3 *radial speed limits* is further investigated for

the development of the safety function. Fig. 4-5 exemplary visualizes the three different concepts for the *Workspace Compliance Function*.

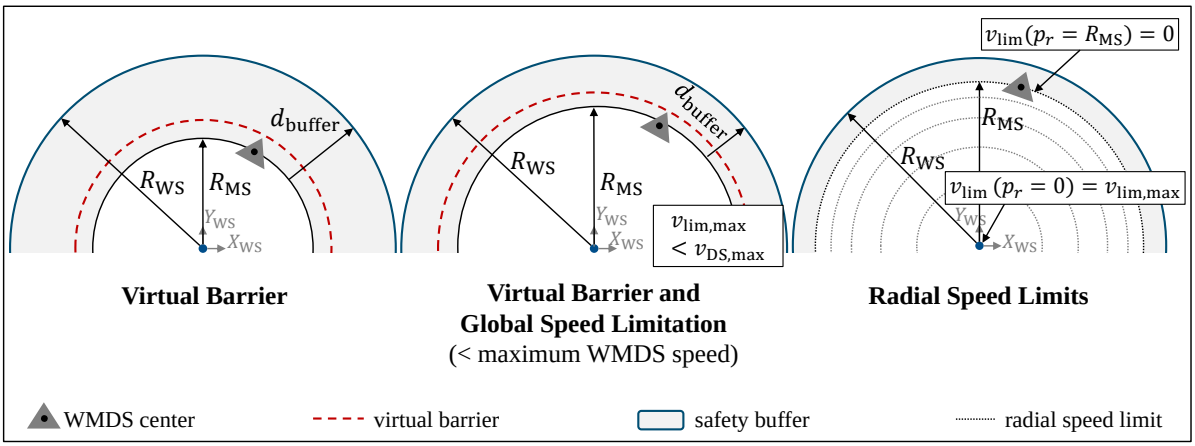


Figure 4-5.: Workspace Compliance function concept overview. Left: the virtual barrier perceives crossing of the WMDS body, the buffer is designed for the maximum possible WMDS speed. Center: The maximum WMDS speed is safely limited by the SF, the buffer zone can therefore be dimensioned smaller. Right: radial speed limits are observed throughout the workspace, which enables more extended usage of the workspace.

4.2.2. Requirement Specification

To derive requirements on the defined subfunctions, a failure analysis is conducted, assuming the failure of the intended tasks and assessing respective sources. At the highest level, a distinction is made between *sense*, *logic*, and *act* failures. This intends to achieve a systematic and large coverage of relevant requirements on the function. The failure analysis is performed with respect to the *Radial Speed Limits* function and is shown in Fig. 4-6. The failures are not developed to the deepest level within the figure due to space limitations. An undeveloped failure case is indicated by a diamond.

Sensing Requirements

The function fails in the *sense* part if the position or speed information of the WMDS is not available or deviates from the true value such that the position dependent speed limits are insufficient for workspace compliance. In the fault tree, this is further specified for the position determination. The failure can be caused by either hardware faults in the sensors, or specification faults. If the sensing capabilities of the sensors are not sufficiently adapted to the prevailing conditions in terms of the ODD of the WMDS, only inaccurate sensor data might be available. This can concern the WMDS motion states or external influence from the environment. Exact causes need to be determined once a technical solution for the sensors is chosen. On the other hand, the system can fail when the intended ODD of the WMDS is left during operation, since the sensors then might not be designed for the prevailing conditions.

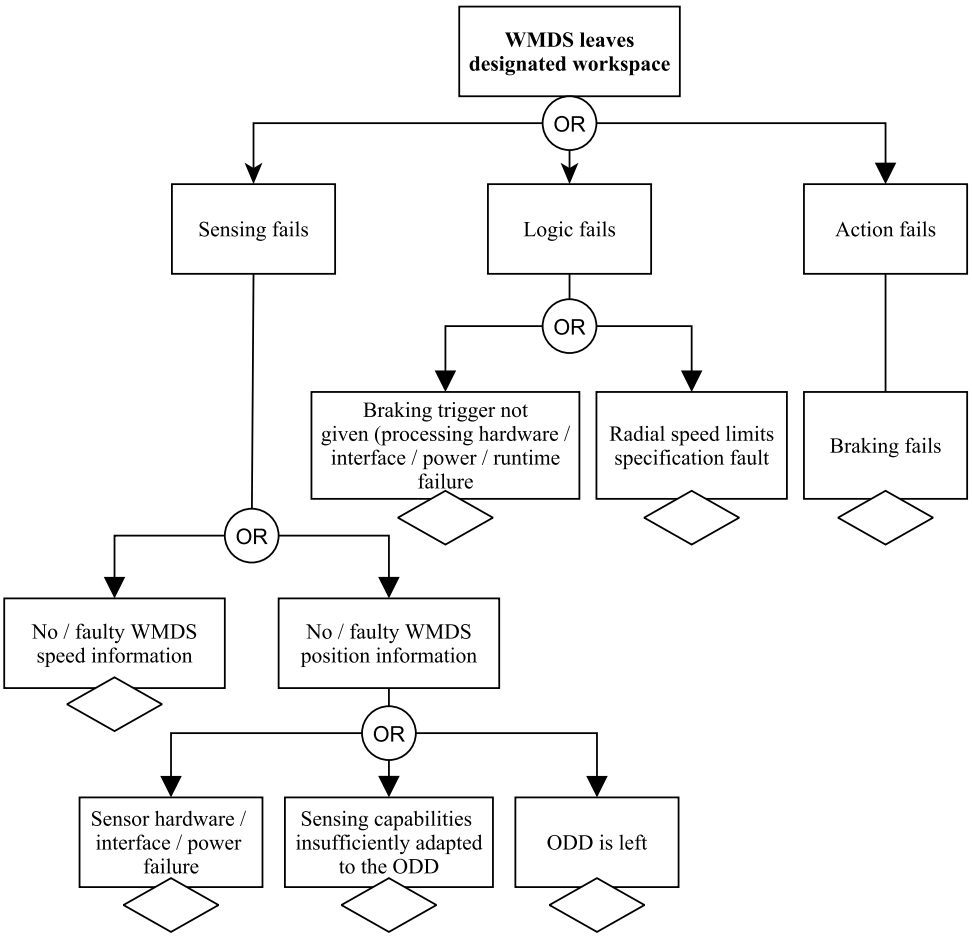


Figure 4-6.: FTA of violation of SG B with the application of local radial speed limits.

Therefore, it is required that the function diagnoses if the sensor delivers no data at all, or unreliable position or speed measurements. A usually occurring maximum measurement error $\Delta p_{r,\mathrm{DS}}$ and Δv_{DS} compared to the ground truth position and speed must be known. Additionally, the operation shall be stopped if the ODD is left.

Logic Requirements and Workspace Adaption

The processing subfunction decides whether a limit is exceeded on the basis of the measured position and velocity variables. It therefore fails if the radial position dependent speed limits are not specified sufficiently to avoid leaving the workspace. So that all eventualities are covered, the consideration of conservative values for all parameters in the determination of the limits is necessary. In addition to the specification in Equ. 4-7, it must be taken into account that both the measured radial WMDS position $p_{\mathrm{r,DS,m}}$ and the measured absolute velocity $v_{\mathrm{DS,m}}$ contain a measurement error Δv_{DS} and $\Delta p_{r,\mathrm{DS}}$ that must be considered in the limit compliance check. Then an emergency brake must be triggered if the following criteria is fulfilled:

$$p_{r,\mathrm{DS,m}} > p_{r,\mathrm{DS,lim}}(v_{\mathrm{DS,m}} + \Delta v_{\mathrm{DS}}) - \Delta p_{r,\mathrm{DS}} \tag{4-10}$$

Another type of failure concerns the processing unit itself, which can be either a power or interface fault, a run time fault or random hardware failure. It is required to be diagnoses whether any of these faults occur.

Acting Requirements

A fail safe braking system is required that is available at any time. If the limit exceedance braking is conducted by the regular motion system, this means that failure in the motion system must be diagnosed as part of the functional safety concept and the EEBS must trigger in case the motion system fails. If the EEBS itself performs the braking whenever a limit exceeding is detected, no further diagnosis of the regular motion system to the respective SIL is required. Therefore, the EEBS is used as the responsible braking system for all braking tasks within SF1.

Failure in the act part still include the failure of the brake system itself or the force transmission between tire and ground (not further specified in Fig. 4-10), leading to either an increased braking distance or even a missing braking. The EEBS as an external system is designed fail safe against failure in the electric parts. Nevertheless, failure of the brake system can still be caused by mechanical damage of the force transmitting parts of one or more brake units. Insufficient force transmission between tire and ground is possibly caused by a burst tire or slippery workspace surface conditions. In addition to ensuring the electrical fail-safety of the braking system and a standard-compliant mechanical design, workspaces with slippery surfaces that decrease the assumed brake deceleration ($\mu < 0.6$) must be avoided. Compliance with this requirement must be ensured by the system operators, e.g. by an inspection of the workspace prior to operation. In addition, the tire pressure should be monitored during operation in order to transfer the system to a safe state in the event of a burst tire.

Fault Detection Requirements

The previous requirement categories included diagnosis requirements concerning failures that can occur during operation and impede a correct functioning of the safety function. All failures to be diagnosed shall therefore be considered in a diagnosis function. By means of a fail safe concept, a diagnosed failure requires the transfer to a safe state, which is also a braking to standstill with the EEBS. The diagnosis either requires a redundancy of two components to identify failure or a single component with a sufficient self-diagnosis.

Usability Requirements

Besides safety requirements derived from failures, general requirements for the usability of the function within the driving simulation apply. A false positive braking trigger outside of a safety critical situation is undesired, as this reduces the availability of the WMDS for its intended task. It therefore shall be avoided, that the WMDS brakes as a reaction to a failure diagnosis without an actual failure being present. Additionally, the return mechanism within the MCA must be

sufficiently adapted to the implemented radial speed limits so that the safety function only triggers if a failure in the MCA or MC components is actually present.

4.2.3. Resulting Requirements on SF1

The requirements on SF1, elaborated in the previous chapters, are summarized in Tab. 4-2. These are classified as safety function requirements (SFR) describing requirements on the intended functionality and functional safety of the SF, as well as general usability requirements (UR).

Table 4-2.: Resulting Requirements on SF1 Workspace Compliance Function.

Category	Requirement Description	SIL
SF1.1 / SF 1.2	The radial position and absolute speed of the WMDS within the motion space is determined	3
SFR1.1.1	The position and speed measurement equipment shall be functional under all possible conditions described by the ODD of the WMDS	
SFR1.1.2	The position and speed measurement error shall not exceed the error respected in the PZ design	
SF1.3	The WMDS' position and speed are checked for compliance with predefined radial speed limits. A braking trigger is set, if a radial speed limit is exceeded	3
SFR1.3.1	The radial speed limits shall be sufficiently dimensioned to enable a braking to standstill before the workspace is left. The radial speed limit design shall respect:	
SFR1.3.1.1	worst case reaction times of the sensing, logic and act functions	
SFR1.3.1.2	maximum measurement errors of WMDS position and speed	
SFR1.3.1.3	a maximum acceleration of the WMDS during the sensing and processing reaction time	
SFR1.3.1.4	a worst case braking deceleration (minimum for ODD)	
SFR1.3.2	The processing time of the check shall not exceed reaction times respected in the radial speed limit design	
SF1.4	The WMDS is transferred to standstill after a braking trigger is set	3
SFR1.4.1	The braking system shall be fail safe	
SF1.5	Faults / failures of the subfunctions are diagnosed	3
SFR1.5.1	A fault condition shall be triggered and a safe state adopted in case of:	
SFR1.5.1.1	no / unreliable WMDS speed information	
SFR1.5.1.2	no / unreliable WMDS position information	
SFR1.5.1.3	failure of the logic processing systems	
SFR1.5.1.4	leaving the ODD of the WMDS	
SFR1.5.2	The safe state is a braking to standstill with a fail safe braking system	
	Usability Requirements	
UR1.1	False positive limit exceedance trigger shall be avoided	
UR1.2	False positive failure diagnoses shall be avoided	
UR1.3	The MCA shall be sufficiently adapted to the implemented radial speed limits so that the safety function only triggers if a failure in the regular drive or control system is actually present	

4.3. Collision Avoidance Function

A second safety function is required, that detects collision hazards and initiates an emergency brake in order to fulfill SG C. This *Collision Avoidance Function (SF2)* is further detailed in the following.

4.3.1. Safety Function Decomposition

The WMDS is not supposed to evase a potential collision object, which would require information of the object's size and motion state. Instead, the function is designed to avoid a collision through emergency braking. For this purpose, a strategy is required according to which objects are perceived and the decision to initiate emergency braking is made.

The *protected zone (PZ)* is introduced, which refers to the safety critical area that must be monitored for objects in order to perceive collision hazards before a collision can occur. When occupied, a braking shall be induced. The safety function therefore requires the safe definition of the PZ for given motion conditions of the WMDS. Also, a reliable information about the relevant motion states of the WMDS influencing the PZ is required, which depends on the actual variables determining the PZ. Furthermore, a reliable detection of hazardous objects within that zone with appropriate sensing equipment is required. Only the presence of an object and its relative position to the PZ is needed as information. Besides these, a reliably executed braking maneuver is required.

Possible designs of the PZ in dependence on observed motion state variables of the WMDS are elaborated in the following. The PZ must at least cover those areas within which the WMDS cannot or can only just come to a standstill under the actual motion conditions and the brake must be triggered at the latest when an object enters this zone. The minimum area to cover by the PZ is first derived, then further adaptions on the PZ design are presented with the goal of simplifying the safety function.

Concept 1: Speed and Course Dependent PZ

The minimum zone to be protected depends on the travelled path of the WMDS during the braking process. This is determined in its length by the current driving speed, in its direction by the current driving direction and in its width by the vehicle width, the driving curvature and any changes in direction during the braking process. In order to design the protected zone safely for all eventualities, worst case conditions of the WMDS motion state must be conceived.

Fig. 4-7 shows a qualitative representation of a required vehicle-bound PZ in dependence of the actual velocity vector of the WMDS. The overall stopping distance of the WMDS d_{stop}, as specified in Equ. 4-2, consists of a distance travelled during a reaction time and a subsequent distance travelled while decelerating to standstill. Within the reaction time of an object trigger

($\tau_{\mathrm{react,sp}}$), changes in the direction are still possible. The maximum curvature $\kappa_{\max}$ drivable for a given friction coefficient $\mu_{\max}$ at a given WMDS speed v_{DS} is estimated by Equ. 4-11. The higher the initial driving speed, the lower the maximum curvature that can be driven. At maximum drivable curvature, the WMDS still follows the curve during the reaction time while traveling the distance d_{react} and moves tangentially in the deceleration phase due to reaching the tire's friction limit, thereby travelling the distance d_{dec}. At lower curvatures, however, the curve travel is continued depending on the magnitude of the braking force.

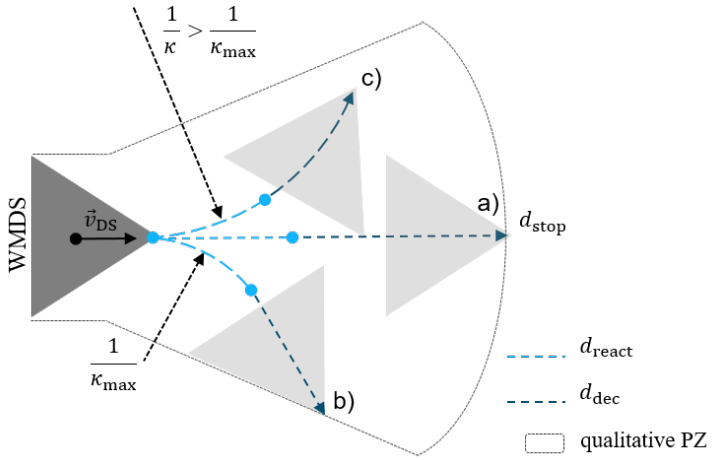


Figure 4-7.: Qualitative minimum PZ design for a WMDS in motion; a) longitudinal drive, b) combined longitudinal and lateral drive with maximum curvature and straight deceleration, c) with smaller curvature followed when decelerating.

$$\kappa_{\max} = \frac{\mu_{\max} \cdot g}{v_{\mathrm{DS}}^2} \tag{4-11}$$

Assuming that the reaction time is sufficient to suddenly change the driving direction to the maximum drivable curvature, the protected zone must cover at least the area spanned by the longitudinal braking distance at maximum achievable speed and the lateral area defined by maximum drivable curvature. Theoretically, it is sufficient to always protect only this area, whereby a safe switchover of the PZ according to the driving speed and course becomes necessary. This requires sensory equipment for the driving speed and course. These input variables are to be considered as functional failure sources for an insufficient PZ adaption during operation. Additionally, not only the distance of an object but also its angular position towards the WMDS must be known reliably. Since there is no designated driving direction of a WMDS due to the omnidirectional motion platform, this PZ must be switchable to every course angle of the WMDS.

SF1 specifies to the following subfunctions:

- SF2.1: (sense) The absolute speed and the course of the WMDS is perceived.
- SF2.2: (logic) The required PZ is determined for the estimated braking distance and possible course change at current state of motion of the WMDS.

- SF2.3: (sense) The distance and angular position of objects towards the WMDS, at least within the PZ, is perceived.
- SF2.4: (logic) An object trigger is set, if the perceived object is within the PZ.
- SF2.5: (act) The WMDS is transferred to / kept at standstill, after / as long as an object trigger is set.

Concept 2: Speed Dependent PZ

Due to the intention to simplify the SF as far as possible, it is further investigated whether the PZ can be designed with less dependencies. A possible simplification includes to eliminate the course information of the WMDS, so that the PZ is only dependent on the absolute driving speed of the WMDS and no longer of the direction. This creates a circular PZ around 360° of the WMDS, referenced to its center with a radius $R_{\mathrm{PZ}}(v_{\mathrm{DS}})$, thereby covering at least the stopping distance at actual absolute speed $d_{\mathrm{stop}}(v_{\mathrm{DS}})$ or $d_{\mathrm{stop,max}}$. This shall include the overall reaction time of the subfunctions, plus the dimensions of the WMDS from the center to the outer edge $l_{\mathrm{c,DS}}$. The minimum required PZ size calculates to:

$$R_{\mathrm{PZ,min}} = \begin{cases} d_{\mathrm{stop}}(v_{\mathrm{DS}}) + l_{\mathrm{c,DS}} & d_{\mathrm{stop}} < d_{\mathrm{stop,max}}, \\ d_{\mathrm{stop,max}} + l_{\mathrm{c,DS}} & \text{else} \end{cases} \tag{4-12}$$

The estimated dimensions of the PZ according to this equation and the specifications for the WMDS prototype MORPHEUS 2.0 in dependence of the actual driving speed are visualized in Fig. 4-8. Thereby, an object detection sensing and processing time $\tau_{\mathrm{react,sp}} = 0.1\,\mathrm{s}$ is assumed. For the maximum WMDS speed of $15\,\mathrm{m/s}$, a PZ size of $30\,\mathrm{m}$ is required. When limiting the maximum speed within the target workspace to $10\,\mathrm{m/s}$, the maximum PZ size reduces to $17\,\mathrm{m}$. The actual dimensions are required to be updated once the final reaction times are known.

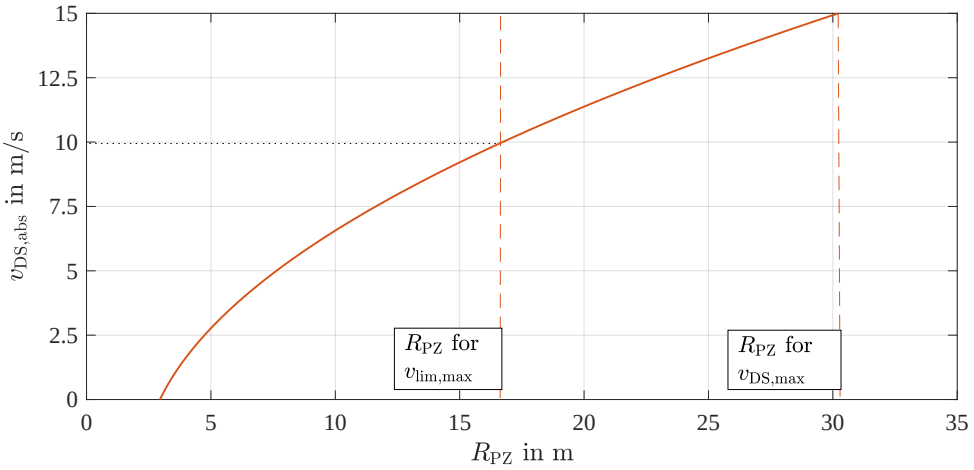


Figure 4-8.: PZ size in dependence of the WMDS absolute speed. The maximum values are indicated for the maximum possible WMDS speed and a limited maximum WMDS speed to 10 m/s.

With a 360° PZ, the object perception only requires a distance information of an object towards the WMDS, not an angular position. The sensory equipment is reduced to measuring the absolute WMDS speed and the distance of the closest point of an object towards the WMDS. The respective subfunctions specify to:

- SF2.1: (sense) The actual absolute speed of the WMDS is perceived.
- SF2.3: (sense) The radial distance of objects towards the WMDS is perceived.

This *speed dependent PZ radius* design is sufficient for safety, but leads to an observation for objects in areas that are not critical to safety, which bears the potential of unnecessary interruption of operation. Since the workspace is to be kept cleared from objects during the operation anyways, this is solely a problem when the PZ reaches areas outside the workspace, where objects are allowed to be present. It therefore must be ensured that the required observed area does not include areas that are permitted for persons or objects as long as this is not actually critical for safety. Thereby, alignment with the *Workspace Compliance* concept becomes necessary. Since the WMDS is required to reduce its speed towards rising radial positions, the PZ will adopt its minimum size as specified for standstill at the outest radial position of the motion space. The allowed motion space must therefore yield a buffer to the workspace border of the size of that minimum PZ at any time, that neither objects nor the WMDS are allowed to enter in a fault free state. Since the definition of the speed limits as well as the definition of the PZ depend on the braking distance of the WMDS at a given speed, there is a correlation between the remaining distance to the border and the PZ size. The only different parameters concern the reaction times and measurement errors of the different measured variables in the two safety functions. Thus, for the two functions to be compatible, it is desirable that the reaction times and measurement errors are of similar magnitude. If these are larger in the object detection function, they have to be compensated for in the workspace design, e.g. by an additional buffer zone around the workspace. The concept is illustrated in the center of Fig. 4-9.

Concept 3: Static PZ

A further option of PZ adaption is a *static PZ radius* design (Fig. 4-9 left). This means the PZ size is adapted towards the maximum permissible speed of the WMDS, meaning no more speed input is required for the safe function of the collision avoidance and SF2.1 is omitted. This is only an option in combination with the concept *virtual barrier and global speed limitation*, since this ensures that the PZ size matches with the safety buffer around the workspace adapted to the limited maximum speed. Otherwise, a static PZ would cancel the advantages of the reduced buffer zone by *radial speed limits* described for the *workspace compliance* function.

During the manual drive mode, it is required to reduce the static PZ size to a low speed mode, as otherwise the function disturbs maneuvering in narrow spaces, e.g. for parking.

Concept 4: Workspace-bound PZ

A different possibility is to scale the PZ size to the actual workspace size during driving simulation mode (Fig. 4-9 right). This is not essential for safety, but allows to keep the workspace clear from objects at any time. As the detection of objects is to be conducted from a vehicle referenced sensing system, the measured position of objects from a vehicle point of view must be transferred to the workspace coordinate system. Therefore the WMDS position and orientation within the workspace must be known. Also, not only the objects distance, but its relative position towards the WMDS is a required information. Then it is possible to evaluate whether a detected object is within the workspace or not. This concept can be applied for any of the different *Workspace Compliance* concepts. A disadvantage is that the concept adds further complexity to the function. Also, sensor technology for object detection must always be able to cover the entire workspace, which can lead to limitations in applicability to flexible workspace sizes. Therefore, it is not considered valuable.

The discussed PZ design concepts 2-4 are illustrated in Fig. 4-9.

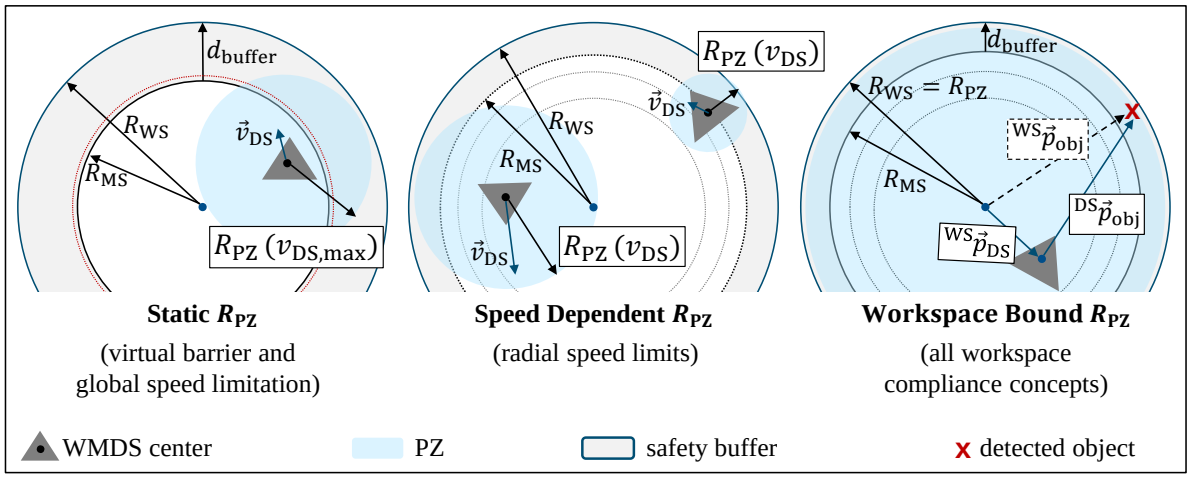


Figure 4-9.: PZ designs in dependence of the workspace compliance concept. Left: static PZ dimensioning according to the maximum permitted WMDS speed. Middle: dynamic PZ dimensioning according to the actual measured WMDS speed. Right: PZ covers the whole workspace by transforming the vehicle bound sensing system to workspace coordinates with help of the measured WMDS position.

Conclusion

The *speed dependent PZ* design is considered a useful minimum functional design as a compromise between complexity and motion space limitation. This concept is further considered for the *Collision Avoidance* function in combination with the *radial speed limits* concept of the *Workspace Compliance* function. It is to note that a dependency between both safety functions and their respective concepts exist: First because both functions rely on a speed measurement, second because the radial speed limits, i.e. the remaining distance to the workspace border, and the PZ size shall be aligned with each other to avoid disturbance by objects present outside the workspace.

4.3.2. Requirement Specification

To derive requirements on the defined subfunctions, an FTA is conducted, assuming the failure of the intended tasks and assessing respective sources, equivalently to the analysis performed for the *Workspace Compliance* function. The fault tree is shown in Fig. 4-10.

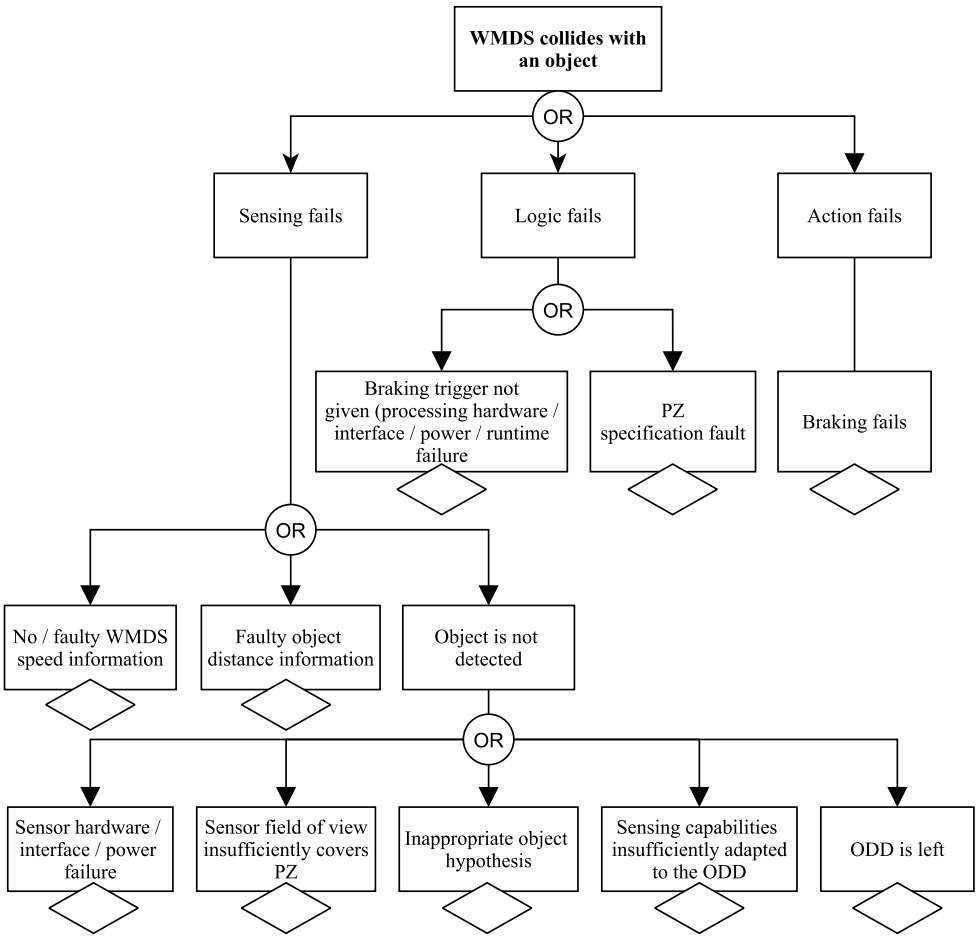


Figure 4-10.: FTA of violation of SG C: The WMDS collides with an object due to failure of the *Collision Avoidance* function.

Sensing Requirements

The function fails in the *sense* part if an object present in the PZ is not detected or its position is perceived outside the PZ due to measurement errors. Both can occur due to general hardware failure of the sensor. Also, the field of view of the sensor may insufficiently cover the PZ, leading to missing an object. This can be due to improper mounting of the sensor hardware on the vehicle or occlusion of the sensor during operation. Therefore, it is required that the function diagnoses if the sensor delivers no data at all, or data of an incomplete field of view or unreliable distance measurements. A usually occurring maximum object distance measurement error Δd_{obj} must be known.

As highlighted in Chapter 2.1.4 (SOTIF) as an explicit hazard for environment-sensing systems, the sensing function can fail due to misspecification of a sensing system with respect to the ODD and environmental influences therein, which can lead to insufficient sensor raw data quality. This can concern the WMDS motion states, properties of objects to detect, or weather influence, which was specified for the WMDS in Chapter 3.1. A safe specification of the sensory equipment for the ODD of the WMDS therefore is a crucial requirement. In addition, as also noted in Chapter 2.1.4, the object hypothesis may be insufficiently adapted to appearing objects. This hypothesis is implemented in the object detection software, and must be designed in such a way that a relevant object cannot be discriminated by the algorithm under any circumstances. For WMDS operation, everything that is either a person itself or causes such an impact that the person within the WMDS is harmed, is a potential hazardous collision object. Potential hazardous objects to detect therefore include human, varying from infant size to grown with different reflection properties ranging from low (e.g. black clothes) to very high reflectivity (e.g. safety vest). Vehicles, e.g. for driving dynamic tests on outdoor test fields or transportation vehicles in industrial environments are also potential objects. Potential infrastructural collision objects include trees, buildings, trailers, pillars or curbsides. In case of an outdoor operation, wildlife from the surrounding is also respected as potential collision objects. Flying animals like birds are not considered due to their low mass. Items such as toolboxes or bags should also be detectable in order to avoid damage of the WMDS. For an outdoor operation, the function must be robust against low-angle sunlight and eventually light rain. Strong rain, snow or fog are excluded from the ODD of a WMDS.

On the other hand, the system can fail when the intended ODD of the WMDS is left during operation, since the sensors then might not be designed for the prevailing conditions. The WMDS operation therefore must be stopped before the ODD is left. This can for example concern changing weather or daylight conditions.

The function also fails if the speed information fails or deviates from the true value due to measurement inaccuracies such that the PZ is insufficiently dimensioned to avoid a collision. Reasons can be, for example, hardware failures of the sensor, but also specification issues and external conditions. Therefore, it is required that the function diagnoses if the speed sensor delivers no data at all, or unreliable speed measurements. A usually occurring maximum measurement error Δv_{DS} must be known.

Logic Requirements

During the design process, wrong assumptions about the parameters describing the required PZ are critical to safety, as a too small PZ size causes a collision even if an object is detected. This requires knowledge of maximum occurring reaction times in the process of object perception, braking trigger and braking force built-up time to be included in the calculation of the actual stopping distance according to Equ. 4-2 or Equ. 4-3. Also, in addition to the specifications in Equ. 4-12, it must be included that the WMDS speed measurement $v_{\mathrm{DS,m}}$ and object distance measurement $d_{\mathrm{obj,m}}$ both include measurement errors, whereby the maximum occurring errors

under regular conditions Δv_{DS} and Δd_{obj} are to be considered. The actual PZ radius therefore is adapted to:

$$R_{\mathrm{PZ}} = d_{\mathrm{stop}}(v_{\mathrm{DS,m}} + \Delta v_{\mathrm{DS}}) + \Delta d_{\mathrm{obj}} + l_{\mathrm{c,DS}} \tag{4-13}$$

The emergency brake must be triggered, if the minimum measured object distance, referenced to the WMDS center, fulfills the following criteria:

$$d_{\mathrm{obj,m}} \leq R_{\mathrm{PZ}} \tag{4-14}$$

Another type of failure concerns the logic processing unit itself, which can be either a power or interface fault, a run time fault or random hardware failure. It is required to be diagnoses whether any of these faults occur.

Act Requirements

A fail safe braking system is required that is available at any time. Thereby, the same failure cases and respectively the same requirements for the act system apply as for SF1. The EEBS is chosen as the responsible braking system for SF2 as well.

Diagnosis Requirements

The previous requirement categories included diagnosis requirements concerning failures that can occur during operation and impede a correct functioning of the safety function. All failures to be diagnosed shall therefore be considered in a diagnosis function. By means of a false safe concept, a diagnosed failure requires the transfer to a safe state, which is also a braking to standstill with the EEBS.

Usability Requirements

Besides safety requirements derived from failures, general requirements for the usability of the function within the driving simulation apply. Besides the failure to avoid a collision hazard, a false positive braking trigger outside of a safety critical situation is undesired, as this reduces the availability of the WMDS for its intended task. It therefore shall be avoided, that the WMDS brakes as a reaction to an object trigger or a failure diagnosis without an actual object or failure being present. Additionally, objects outside the WMDS workspace shall not trigger emergency brakes as long as the WMDS remains within the workspace, which means the workspace must be adapted so that objects do not get into a collision critical proximity as long as prescribed limits are not crossed. This means once the reaction times and measurement errors for all quantities in the *Collision Avoidance* function and *Workspace Compliance* function are known, an equalization of R_{PZ} and the remaining distance of a radial position limit $p_{r,\mathrm{DS,max}}$ towards the workspace border for a given speed v_{DS} is required.

4.3.3. Resulting Requirements on SF2

The requirements on SF2 are summarized in Tab. 4-3, classified by SFR and general UR.

Table 4-3.: Resulting Requirements on SF2 Collision Avoidance.

Category	Requirement Description	SIL
SF2.1	The actual absolute WMDS speed is perceived	2
SFR2.1.1	The speed measurement equipment shall be functional under all possible conditions described by the ODD of the WMDS	
SFR2.1.2	The speed measurement error shall not exceed the error respected in the PZ design	
SF2.2	The required PZ is determined for the estimated worst case braking distance at current state of motion of the WMDS	2
SFR2.2.1	The PZ shall form a circular zone around 360° of the vehicle with speed variant radius	
SFR2.2.2	The PZ radius shall be sufficiently dimensioned to enable a braking to standstill before a collision can occur. The PZ radius shall respect:	
SFR2.2.2.1	worst case reaction times of the sensing, logic and act functions	
SFR2.2.2.2	maximum measurement errors of WMDS speed and object distance	
SFR2.2.2.3	a maximum acceleration of the WMDS during the sensing and processing reaction time	
SFR2.2.2.4	a worst case braking deceleration (minimum for ODD)	
SF2.3	The relative distance of objects towards the WMDS is perceived	2
SFR2.3.1	The object detection equipment shall be functional under all possible conditions described by the ODD of the WMDS	
SFR2.3.2	The object hypothesis shall not discriminate relevant collision objects as part of the ODD of the WMDS	
SFR2.3.3	The field of view of the object detection equipment shall sufficiently cover the PZ at any time	
SFR2.3.4	The object distance measurement error shall not exceed inaccuracies respected in the PZ design	
SF2.4	An object trigger is set, if the perceived object is within the PZ	2
SFR2.4.1	The reaction time until the trigger is set shall not exceed reaction times respected in the PZ design	
SF2.5	The WMDS is transferred to / kept at standstill, after an object trigger is set	2
SFR2.5.1	The braking system shall be fail safe	
SF2.6	Faults / failures of the subfunctions are diagnosed	2
SFR2.6.1	A fault condition shall be triggered and a safe state adopted in case of:	
SFR2.6.1.1	no / unreliable WMDS speed information	
SFR2.6.1.2	no / unreliable environment perception data	
SFR2.6.1.3	failure of the logic processing systems	
SFR2.6.1.4	leaving the ODD of the WMDS	
SFR2.6.1.5	an occluded or misplaced environment perception equipment	
SFR2.6.2	The safe state is a braking to standstill with a fail safe braking system	
	Usability Requirements	
UR2.1	False positive object detections shall be avoided	
UR2.2	False positive failure diagnoses shall be avoided	
UR2.3	Objects present outside the workspace shall not lead to object triggers as long as the WMDS remains within its designated workspace	

4.4. Interim Conclusion and Proposed Safety Architecture

In the previous chapters, two essential safety functions for the safe motion of WMDS have been specified within multiple concepts, varying in the dependency of measurement variables and observed components. An important outcome is that the safe information of the actual WMDS speed is crucial for both functions. A faulty or unavailable speed information causes the WMDS - in the worst case - to leave the workspace first, and then to collide with objects outside the workspace due to an insufficient PZ size. It has been further shown, that to avoid the requirement of a functionally safe speed information is generally possible, but must be compensated with large buffer zones that can limit the usable workspace size unreasonably. Therefore, the inclusion of the *WMDS speed*, in combination with the *WMDS radial workspace position* and *distances of detected objects* is the recommended minimum subset of safety-related functions to safeguard the WMDS motion, in combination with a fail safe external emergency brake system and the two logic functions processing the decision of an EEBS trigger. Requirements for the avoidance of failure of the functions have been derived on a high level. The proposed architecture is illustrated in Fig. 4-11.

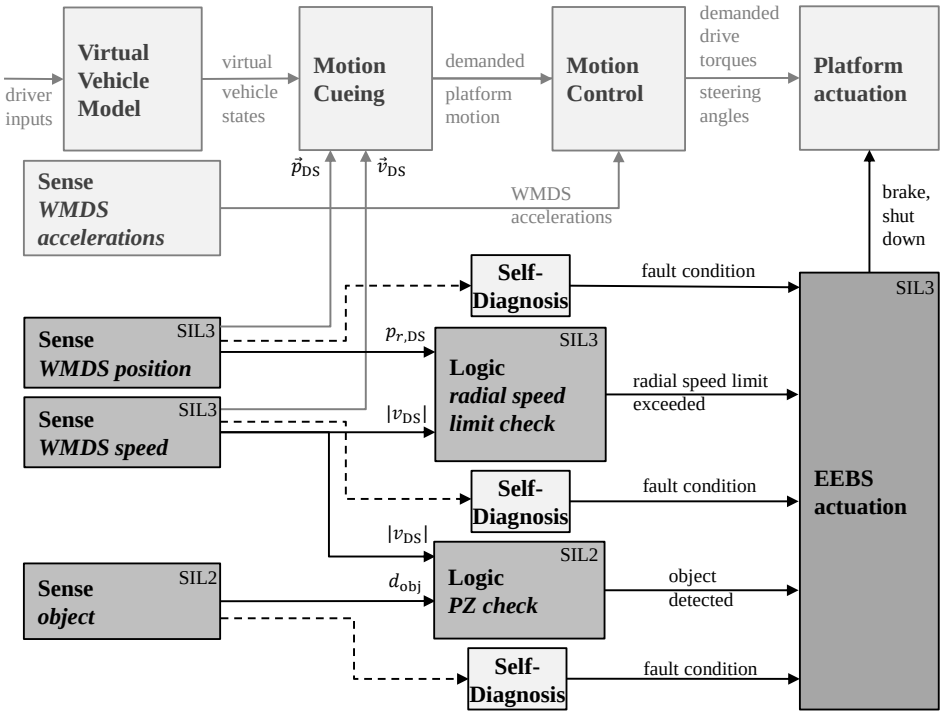


Figure 4-11.: Proposed safety architecture to safeguard the motion of a WMDS.

Each subfunction requires at least a self-diagnosis to identify failure. The WMDS position and speed are also an inputs into the MCA of the regular driving simulation task, as the measurement units are processed within the washout algorithm. All other components from the driving simulation task are not required to be included in the safety concept. It is to note, that this does not mean,

that e.g. the failure of a motor controller shall not be diagnosed and the operation be aborted by an EEBS trigger. But since no harm to human can happen as long as no collision occurs, which is avoided by SF2, this diagnosis and trigger receives no safety integrity level.

The high importance of the position and speed determination with a SIL3 in SF1 means that there must be a high degree of diagnostic coverage in the event of failures. Therefore, a redundant system for measurement of position and speed and the respective limit check is also conceiveable, shown in Fig. 4-12. This is especially required, when failure cases of the position and speed determination exist, that deliver falsified measured values without this beeing detectable in a self-diagnosis. Either if an inacceptable discrepancy is detected between the measured values of the two systems, or a single system fails, or the radial speed limits are violated, the EEBS is triggered. The redundant speed measurement thereby also enhances the diagnostic coverage of SF2. The necessity of redundant systems depends on the technical implementation of the sub-functions, their possible fault cases and the possibility of fault detection.

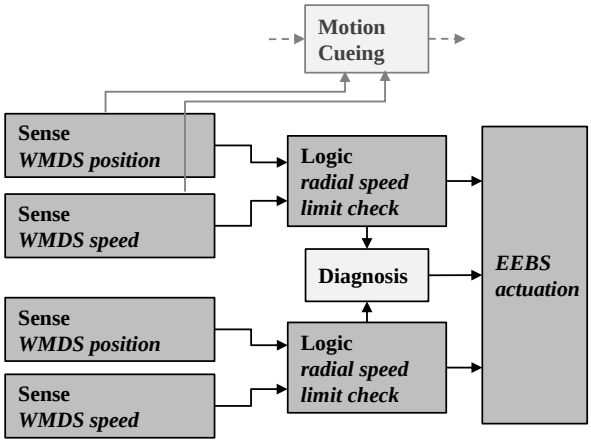


Figure 4-12.: Schematic illustration of redundant design of SF2.

5. Function Allocation and Experimental Hardware Set-up

The feasibility and suitability of the derived safety functions for the WMDS operation shall be evaluated. For this purpose, the further work concentrates on those function which are particularly dependent on the ODD of the driving simulator. The correct functionality and fail-safety of the processor units are considered state of the art problems of functional safety. With regard to the braking system, reference is made to previous work[65,66,67,68]. On the other hand, the realization of the sensory subfunctions of SF1 and SF2 and their self-diagnosis within the ODD of the WMDS have not yet been addressed and therefore need to be further investigated concerning the feasibility under the derived framework conditions. For this purpose, the subfunctions are to be allocated to possible technical implementations in hard- and software. Suitable hardware is derived in this chapter. The software is discussed in the following chapter.

5.1. Concept and Requirement Specification

The sensing subfunctions for *WMDS position*, *WMDS speed* and *distance of objects* are required to be allocated to appropriate sensor hardware. Therefore, the functional requirements previously derived are further developed in terms of sensor specifications.

The evaluation and selection of sensor technologies for the WMDS with respect to object detection and position determination was first addressed in the bachelor thesis of Lutwitzi[69]. However, the work refers to a different state of conceptualization of the WMDS and to partly deviating intended functionalities. Therefore, the requirements and arguments stated there are revised for the specified safety functions of the full scaled WMDS in the context of this work.

Position and Speed Determination

For the position and speed determination subfunctions, a system is required that is either fully vehicle bound or *applicable to flexible workspaces with temporal low effort*. Further criteria for the selection of sensor technologies are the suitability for *indoor and outdoor use*. There is no hard limit for the *measurement accuracy*, but it should be within a range that does not unreasonably

[65] Wagner, P.: Diss., Practical Feasibility and Functional Safety of WMDS (2018).

[66] Betz, A.: Diss., Feasibility and design of WMDS (2015).

[67] Betz, A. et al.: Development and Validation of a Safety Architecture of a WMDS (2014).

[68] Lutwitzi, M.: Master Thesis, Safety Architecture for WMDS (2019).

[69] Lutwitzi, M.: Bachelor Thesis, Umfelderkennung für WMDS (2016).

restrict the usable workspace. As a reference for a selection of technology, a target value is the *positioning accuracy of* $\leq 1\,\mathrm{m}$, which depends on the sensor based measurement error, resolution and frequency. Last but not least, economic factors are relevant, as a low cost DS intended.

In Lutwitzi's bachelor thesis[69], suitable systems for localization for WMDS have already been worked out. Common methods from the field of robotics and automated vehicles were analyzed and evaluated with respect to the criteria mentioned above. These mainly include the application of GPS, inertial measurement units, odometry, active beacon positioning systems, as well as the visual navigation via landmarks or map matching approaches.[70] GPS combined with inertial measurement units was identified as particularly suitable due to high measurement accuracy and update rates, but is limited to outdoor applications of WMDS. The usability of active beacon systems turned out to be less suitable due to high effort in installation and cost. On the other hand, the usage of a vehicle-bound environment perception system and the visual detection of artificial workspace landmarks to establish a local positioning system is advantageous: Since the WMDS is to be equipped with environment perception sensors anyway for the purpose of object detection, this is a possibility that does not require additional measurement units, at least if the requirements for both functions can match in a single sensor technology. The idea is an installation of artificial landmarks around the workspace to a known position, and to detect them by the environment perception sensors, which allows to infer a position of the WMDS via the measured relative distance between landmarks and WMDS.[71]

Under the current aspects of this work, this method is still considered advantageous. The speed of the WMDS can be determined by a derivative of the position. The mobility of the system is kept, if the placement of the artificial landmarks can be achieved with low effort and if the landmark architecture is scalable to different workspace sizes. The achievable measurement accuracy is influenceable by the choice of the sensors. The concept can be realized with triangulation or trilateration methods as well as a map matching approach. When applying the WMDS in an outdoor area, the redundant usage of a GPS based system is possible, which increases the detectability of system failures.

With this choice of principle, the function of position and speed determination further divides into *landmark perception* and *WMDS position and speed processing*. For the choice of appropriate sensor technology for the landmark perception, typical specification fields of environment perception sensors are concretized. At the point where requirements depend on a certain workspace size, the workspace radius of the August Euler Airfield (cf. Fig. 3-3) is assumed. The following requirements apply:

- Measurement quantities: The relative distance and angular position in azimuth of landmarks towards the WMDS are to be measured.

[70] Borenstein, J. et al.: Mobile robot positioning: Sensors and techniques (1997).

[71] Lutwitzi, M.: Bachelor Thesis, Umfelderkennung für WMDS (2016) p. 49.

- Object detectability: No limitations on object surfaces or sizes apply, as the landmarks can be designed towards the sensor capabilities.
- Measurement range: This depends on the landmark architecture, which is to be placed outside the workspace to avoid disturbance within the driving simulation. If all landmarks are required to be detectable from all workspace positions, the detection range is determined by the workspace size. A detection range of at least $50\,\mathrm{m}$ is required for application at the target workspace with a radius of $25\,\mathrm{m}$.
- FOV horizontal: The field of view (FOV) in horizontal direction must fully cover 360° around the WMDS due to the omnidirectionality of the WMDS.
- FOV vertical: 2-D sensing, meaning in an x-y-plane, is sufficient if it is ensured that a landmark is still distinguishable from other environmental elements and always within the FOV despite pitch and roll motion of the WMDS. Otherwise, 3-D sensing is required. This is dependent on the landmark height and the height above ground of the sensor. Inclinations of approximately 2° are estimated for the scaled WMDS prototype on the August Euler Airfield. For the full scaled WMDS, which will have a larger wheel base and a suspension system compensating road excitation, smaller inclination angles are expected.
- Measurement resolution and accuracy: The WMDS position measurement accuracy is dependent on the spatial measurement resolution and measurement error as well as the output frequency in the product with the driving speed of the WMDS. In combination, these characteristics shall be sufficient to reach the target position data accuracy of $\leq 1\,\mathrm{m}$. It thereby is to consider that the frequency of position data output is not only determined by the measurement frequency of the environment perception sensors, but also the run time of the processing algorithms. With e.g. a position data frequency of $20\,\mathrm{Hz}$ at a maximum WMDS speed of $10\,\mathrm{m/s}$, an error of $0.5\,\mathrm{s}$ is introduced. Then, the system must have a position measurement error $\Delta p_{r,\mathrm{DS}}$ below $0.5\,\mathrm{m}$ to still reach the target accuracy. This measurement error is further determined by the accuracy in landmark distance and angular position measurement. The extent to which the measurement accuracy of a landmark affects the position error of the WMDS cannot be determined to this state, since this will also depend on the actual landmark architecture and the processing algorithms. As a guideline, the following estimates are made: A lateral landmark position measurement accuracy of $0.5\,\mathrm{m}$ in a maximum distance of $50\,\mathrm{m}$ requires an angular measurement accuracy of $< 0.6°$. With an additional distance measurement error, the angular measurement accuracy requirement is supposed to be even higher.
- Environment compatibility: The sensor must be compatible for indoor and outdoor usage, particularly for direct sun radiation and if possible for light rain.

Object Detection

For object detection, the conceptual design of the vehicle-bound PZ determines that the WMDS must be equipped with on-board environment sensing equipment. Infrastructure-bound systems such as light barriers would restrict the mobility and additionally would not provide protection in manual maneuvering mode. The following requirements apply for the specification fields of environment perception sensor technology for the task of collision object detection:

- Measurement quantities: The relative distance of objects towards the WMDS is to be measured.
- Object detectability: Non-transparent objects with lambertian or retroreflective reflection properties (e.g. human/animal, textile, metal, plastic, wood) are required to be detectable. Colors can vary from bright to dark black with low contrast to the ground. For the worst case of a person standing sideways, $0.2\,\mathrm{m}$ wide objects are chosen as a conservative benchmark still to be detected within the entire PZ. In case the sensor FOV is oriented in a way that only the legs of human beings are within the FOV, a minimum width of $0.1\,\mathrm{m}$ shall be detectable. A minimum object height of $0.2\,\mathrm{m}$ shall still be detectable at maximum distance, which corresponds to a lying person or small items. The sensors shall be capable of separating object detections from ground detections, as this avoids false positive triggers that impede the driving simulation.
- Measurement range: This must at least comply with the requirements imposed by the definition of R_{PZ} for highest operating speed of the WMDS in dependence of the sensor measurement frequency and processing times. With a maximum WMDS speed of $15\,\mathrm{m/s}$ and an object detection frequency of 10 Hz, the required detection range for objects with respect to the vehicle center was estimated to $30\,\mathrm{m}$ according to Fig. 4-8. When limiting the maximum WMDS speed to $10\,\mathrm{m/s}$, this requirement is reduced to a range of $17\,\mathrm{m}$. Maximum sensor ranges shall nevertheless be larger to provide a buffer.
- FOV horizontal: This must cover 360° around the vehicle due to the omnidirectionality of the WMDS.
- FOV vertical: This shall allow coverage of the ground area to enable that small objects of 0.2 m height are already detectable. Blind spots in close proximity to the vehicle shall be reduced such that small objects left lying on the ground in close proximity can be detected before the start of the WMDS. All other objects are detected when entering the PZ from the outside during operation. The vertical FOV must generally not cover the full body size of objects in order to detect their presence. Nevertheless, the vertical FOV must respect pitch and roll motion of the WMDS, which is estimated to 2° on the August Euler Airfield. This means the desired maximum detection range must be fully covered even if the elevation angle of the sensors relatively to the horizontal is changed.

- Measurement resolution, accuracy and frequency: As described above, the required minimum measurement frequency in combination with the maximum driving speed is dependent on the detection range of the sensor. Furthermore, the required PZ size shall comply with the remaining distance towards the workspace border in dependence of the position dependent speed limits (cf. Tab. 4-3). Therefore, the reference applies here as well, that the combination of object distance measurement accuracy, distance measurement resolution and measurement frequency shall not increase the PZ size by more than $1\,\mathrm{m}$ in total.
- Environment compatibility: The sensor must be compatible for indoor and outdoor usage, particularly for direct sun radiation and if possible for light rain.

5.2. Choice of Sensor Principle

The sensor technologies lidar, radar and (stereo) camera are generally suitable for distance and angular measurement of objects within a suitable range and are commonly used in automated driving functions.[72] The following paragraphs give a brief insight into the advantages and disadvantages of those sensors with respect to the stated requirements to justify the final choice. Thereby, a sensor technology is sought that fulfills both requirements of collision object detection and landmark detection.

Camera-based stereo vision[73] calculates depth from the displacement of visual features in the acquired images of two carefully calibrated cameras. Thereby, dense 3D maps of the environment can be generated. Nevertheless, camera vision relies on the appearance of contrasts, so the detectability of small low-contrast objects compared to the ground is considered difficult, which could nevertheless be a relevant object for the WMDS collision avoidance. Furthermore, so-called motion blurring occurs with cameras, which can be generated especially by the high yaw rates of a WMDS. In addition, cameras are sensitive to sunlight and rain. Therefore, cameras are excluded for the application in WMDS.

Radar sensors[74] use high frequency electromagnetic waves with frequency modulation for distance measurements. These are emitted through an antenna in a lobe shape. By making use of the Doppler Effect, the relative speed towards a detected object can be determined as well. A significant advantage of radar sensor technology is its low sensitivity to weather conditions such as rain and sun. Furthermore, distance measurements are performed with high accuracy. A limitation of radar sensors for the application in the WMDS nevertheless is the wide radar lobe of most standard products and therefore coarse spacial resolution of $> 1°$ in azimuth.[74,72] This is considered insufficient for a precise landmark localization. Emerging technologies of

[72] Marti, E. et al.: Sensor Technologies for Perception in Automated Driving (2019)

[73] Punke, M. et al.: Automotive Camera (Hardware) (2016).

[74] Winner, H.: Automotive RADAR (2016).

high-resolution radar sensors can overcome this limitation in the future, so that a radar sensor is then potentially also suitable for the use case.

Lidar sensors[75], especially laser scanners, are capable of generating a 3-D map of the environment with highly accurate distance measurements by emitting bundeled laser beams over rotating mirrors in multiple vertical layers. The emitted beams are reflected back into a receiver unit by objects in the environment. The time of flight of the light is measured to determine the distance of the object. However, the principle includes gaps between the discrete measurement points where objects can be lost. To avoid this, a high vertical and horizontal resolution is required that satisfies the above stated minimum object heights and landmark position determination accuracy. Products on the market vary between one scan beam[76] and 128 vertical scanning layers[77], which also implies huge price differences. Furthermore, angular resolutions in azimuth of $< 0.2°$ are possible. The maximum detection distance decreases with decreasing light reflectivity of objects, whereby translucent or specular objects might not be detectable. Nevertheless, lidar technology is still considered suitable for the use case, as relevant objects will only partly contain translucent or specular areas, but shall always include lambertian reflectors (e.g. a vehicle). The lidar beams can be limited in detection range by rain, fog or other particles in the air, which is nevertheless dependent on specific products.[78]

As a conclusion, lidar sensors are considered the most suitable technology for both tasks of collision object detection and landmark detection due to their high spacial resolution and accurate measurement. Therefore, lidar sensors are further considered for the intended functions. A multi-layer lidar sensor is to be used, to fulfill the requirement of coverage close to the ground as well as in larger distances under pitch and roll motion of the WMDS. This further prevents misdetections due to total reflection or due to transparent or specular surfaces on relevant objects. Spacial gaps between individually emitted laser beams in the horizontal and vertical directions shall not cause objects or landmarks to be missed. While landmarks can be designed towards the sensor resolution, the critical case are persons and small objects on the ground. The available resolution must enable multiple beams reaching the objects in vertical and horizontal direction, whereby the actual detection capabilities must be evaluated under all influences occurring during operation. Therefore, a possibly high resolution lidar sensor is to be chosen.

[75] Gotzig, H.; Geduld, G.: Automotive LIDAR (2016).

[76] e.g. SICK AG: SICK Safety laser scanners (2022).

[77] e.g. Ouster, Inc.: OS2 Long-range lidar sensor for autonomous vehicles, trucking, and drones (2022).

[78] Linnhoff, C. et al.: Environmental Influence on Automotive Lidar Sensors (2022).

5.3. Hardware Implementation

5.3.1. Sensor Specifications

To select a sensor, the requirements for a reduced maximum velocity of the WMDS to $10\,\mathrm{m/s}$ are further considered as a hard criterion. This enables to decrease requirements on the sensor resolution, which was desirable for reasons of cost efficiency within the project and is sufficient for the operation of the WMDS at the target workspace. In the future, the finally obtained concept can be adopted and the hardware can be scaled towards higher WMDS speeds.

Systems for industrial transportation systems as well as road vehicles are considered for the product research of lidar sensors satisfying the above stated requirements. Due to very different dynamic characteristics and use cases of driverless transportation systems in comparison to the driving simulator, sensors from this branch are not designed for the required ranges, outdoor use or for the vertical FOV, as especially these scan in only two dimensions, meaning with only one vertical layer.[79] On the other hand, lidar sensors from the automotive sector often scan in three dimensions, are specified with a larger detection range and are certified for outdoor use.

From lidar sensors meeting the requirements, the sensor *Ouster OS1-32 Gen2*[80] is chosen. The sensor scans with 32 layers and can satisfy the vertical and horizontal resolution and FOV requirements. This is mainly because the beams are structured in a gradient configuration, which is characterized by an increasing vertical resolution towards the horizontal line (cf. Fig. 5-3). This enables a finer vertical resolution in the target object distance even for pitch and roll motion, while less sensor beams are directed towards sky or ground. The next highest number of layers available would be 64 layers, which would further increase the probability that a small object is detected, but is not considered due to the greatly increasing costs involved. Relevant specifications of the chosen sensor are given in Tab. 5-1. The horizontal resolution can be set to 512, 1024 or 2048 increments per 360° scan. The rotation rate of the sensor can be chosen between 10 and $20\,\mathrm{Hz}$ depending on the horizontal resolution. The detection range for 10 % lambertian reflectivity, which corresponds to a black object, is specified as $45\,\mathrm{m}$, thereby meeting the range requirement for objects. The detection range for 80 % reflectivity is specified to $100\,\mathrm{m}$. The sensor further has an included inertial measurement unit (IMU) containing a 3-axis gyroscope and a 3-axis accelerometer.

[79] An example are the products from SICK AG: SICK Safety laser scanners (2022).

[80] Ouster, Inc.: OS1 Mid-Range High-Resolution Imaging Lidar Datasheet (2022)

Table 5-1.: Extract from specifications of Ouster OS1-32 Gen 2 given by the manufacturer[80].

Category	Specification
range (80% Lambertian reflectivity, 1024 @ 10 Hz mode)	100 m @ 90% detection probability, 100 klx sunlight 120 m @ 50% detection probability, 100 klx sunlight
range (10% Lambertian reflectivity, 1024 @ 10 Hz mode)	45 m @ 90 % detection probability, 100 klx sunlight 55 m @ 50 % detection probability, 100 klx sunlight
range accuracy	3 cm for lambertian targets, 10 cm for retroreflectors
range resolution	0.3 cm
minimum measurement range	0.25 m
vertical field of view	+13°, - 16°
vertical resolution	32 channels
horizontal resolution (and max. rotation rate)	512 (20 Hz), 1024 (20 Hz) or 2048 (10 Hz) (configurable)
vertical resolution	0.35°- 2.8°(gradient set-up)
beam divergence	0.18°
number of returns	1 (strongest)

The obtained sensor data for each segment within each sensor layer are so called points, representing a received detection. Each point is obtained in a spherical coordinate system, defined by $[\Phi, \vartheta, r]$, as shown in Fig. 5-1, and is characterized by further point attributes, summarized in Table 5-2.

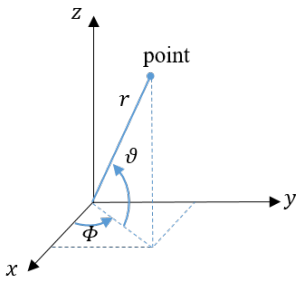


Figure 5-1.: Lidar coordinate system in spherical and cartesian coordinates.

Table 5-2.: Point attributes provided by the lidar sensor for each measured point[80].

Point Attribute	Description
measurement ID	a sequentially incrementing measurement in azimuth (Φ) counting up from 0 to 511, or 0 to 1023, or 0 to 2047 depending on the chosen resolution
timestamp	timestamp of the measurement in nanoseconds
channel	refers to the ID of a sensor layer, ranging between 0 (highest layer) and 31 (lowest layer), each layer is emitted at a discrete elevation angle (ϑ)
range	range (r) in millimeters, discretized to the nearest 3 millimeters.
signal photons (intensity)	signal intensity photons in the signal return measurement, unitless value between 0 and 65535
reflectivity	signal photon measurements are scaled based on measured range and sensor sensitivity at that range, providing an indication of target reflectivity, unitless value between 0 and 255
ambient noise photons	ambient noise photons in the ambient noise return measurement, related to natural environmental illumination

5.3.2. Sensor Setup on the WMDS

The resulting FOV must cover full 360° at close proximity to the vehicle. A 360° FOV is fulfilled by only one sensor, but requires mounting on the highest point to have a full overview of the vehicle environment. This creates large blind spots at close range. Furthermore, it requires a construction that carries the sensor above the cabin and that is independent of its motion, which conflicts with the lightweight WMDS concept. A motion platform mounting of the sensor therefore is considered. It is important to avoid interruption of the FOV by platform components so that all laser beams can reach the workspace area (except when pointed towards hexapod and cabin). Therefore, a set of three individual sensors is chosen to be mounted on the platform of the WMDS.

The system is implemented on the scaled prototype of the WMDS as shown in Fig. 5-2, as the final WMDS according to the design described in Chapter 2.2 is still under construction to the time of this work. Since the actual design and vehicle size does not influence the environment perception based functions, it is considered a representative tool for the implementation and evaluation of the safety functions. A limitation however is that the prototype does not have a suspension system, and therefore will react to uneven ground with larger pitch and roll angles than it is expected for the platform of the full scale WMDS.

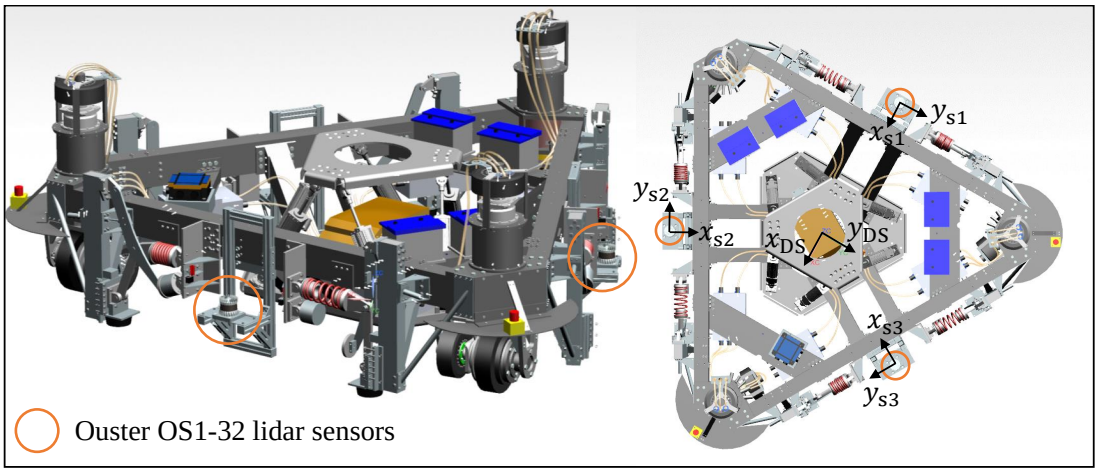


Figure 5-2.: Sensor hardware implementation on the scaled WMDS prototype and indication of the sensors' coordinate systems.

Fig. 5-3 illustrates the vertical and horizontal FOV of the sensor set up. The sensor center is mounted at a height of $0.375\,\mathrm{m}$. The vertical FOV is spread over $29°$ in total. The gradient beam alignment of the sensor is shown as a schematic illustration, indicating that the sensor gaps are smaller close to the horizontal line and increase towards the outer angles. The horizontal FOV of each sensor covers $180°$ and overlaps for about $60°$ between adjacent sensors. To obtain a representation of the merged points of all three sensors in the 3-D space, the points are transformed to a common cartesian coordinate system, a so called *point cloud* representation, where each lidar point is further described by an $[x, y, z]$ coordinate. The sensor mounting pose of each sensor is specified and a point transformation to a WMDS-centered coordinate system is conducted.

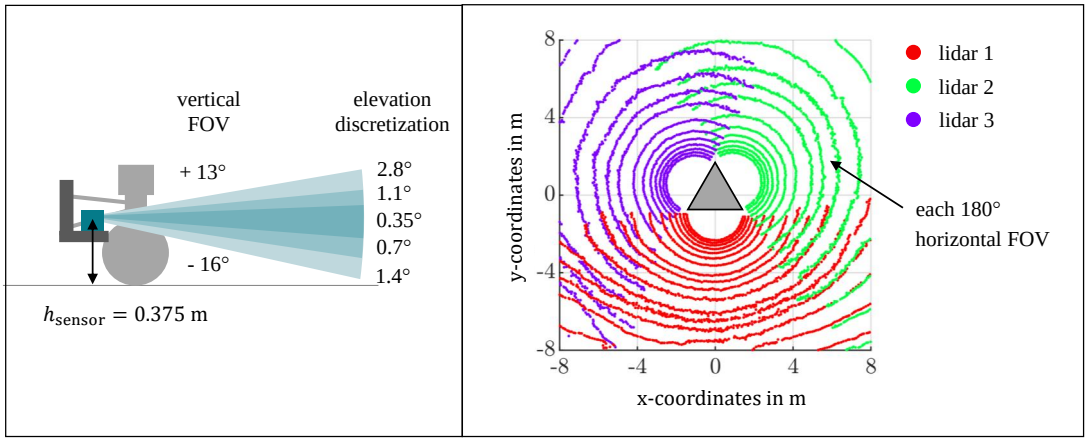


Figure 5-3.: Overall sensor field of view on the WMDS. Left: Vertical field of view in a schematical illustration, showing the gradient beam alignment. Right: horizontal field of view of all three sensors in a point cloud illustration.

5.3.3. Sensor Gaps Analysis and Mode Selection

The vertical beam structure and FOV of the Ouster lidar sensor as implemented on the WMDS is shown in Fig. 5-4. This enables to investigate the theoretical object detectability in the target distances as well as the required landmark sizes. The maximum detection distances are illustrated in the distance of $R_{\text{PZ,max}}$ for the limited maximum WMDS speed ($v_{\text{lim,max}}$) and the absolute maximum WMDS speed ($v_{\text{DS,max}}$). Up to a distance towards the sensor of approximately $2.3...3\,\text{m}$[81], the upper beam reaches a maximum height of $1\,\text{m}$. Up to this range, denoted as $d_{\text{h,red}}$, it is possible that only the legs of a person are within the FOV, which is why the minimum object width to detect is set to $0.1\,\text{m}$ up to this distance. From this range onward, the critical width of a person is its body width when standing sideways, which is conservatively estimated to $0.2\,\text{m}$. As indicated, a standing person is always hit by multiple beams in the vertical direction throughout the detection range. A lying person defines the minimum height of $0.2\,\text{m}$ of objects to detect, which also includes small items that are left on the ground. The theoretical illustration shows that an object with this height should be met by at least 2 laser beams up to the PZ size for limited WMDS speed, while only one beam would detect such an object at the PZ size for maximum WMDS speed. In Fig. B-1 in Annex B, the vertical FOV illustration is given for an inclined sensor of $\pm 2°$, indicating that the required vertical FOV is still sufficiently covered.

Fig. 5-5 illustrates the theoretical horizontal gap between two emitted laser beams in dependence of the number of azimuthal scan segments. This can be set-up between 512, 1024 and 2048 segments per $360°$ scan. Furthermore, the previously explained minimum object widths in dependence of the detection range are indicated. It can be derived, that a resolution of 1024 segments is sufficient to hit objects of minimum width with at least one laser beam within $R_{\text{PZ,max}}$ for the maximum WMDS speed. Until $R_{\text{PZ,max}}$ for the limited speed, the resolution is just sufficient to detect an object of minimum width with two laser beams. This enables to operate the sensor at 20 Hz. With

[81] This interval considers a sensor inclination between -2°and 2°, estimated for present unevenness at the Griesheim Airfield. In the figure, the value is indicated for a horizontal sensor.

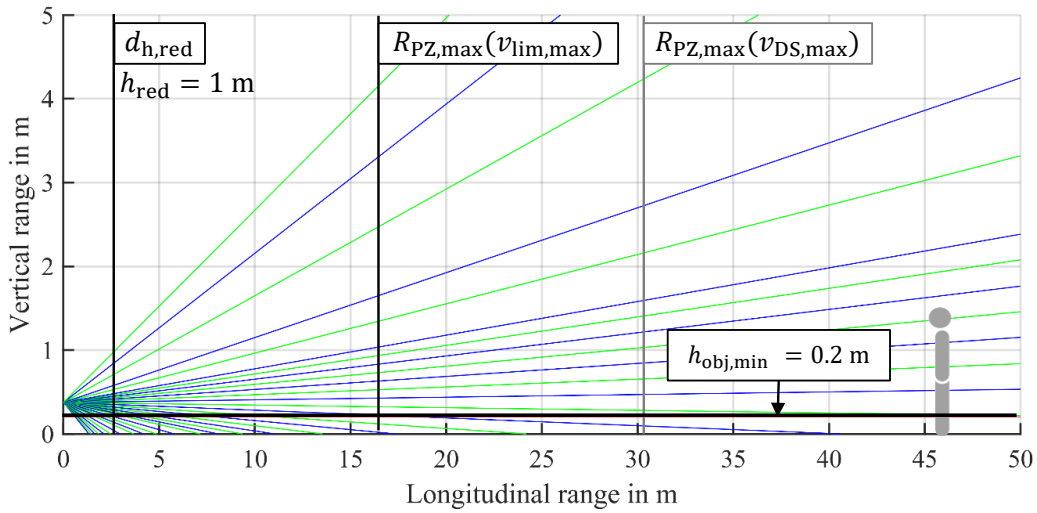


Figure 5-4.: Vertical beam structure and gaps towards the intended detection distances and object heights.

a resolution of 2048 segments, only a scan frequency of 10 Hz is available. This would increase the reaction times for both safety functions. Therefore, the sensor mode is set to 1024 segments and 20 Hz scan frequency. It is further to consider, that the lidar beams have a beam divergence that can lead to even smaller gaps than illustrated in both figures.

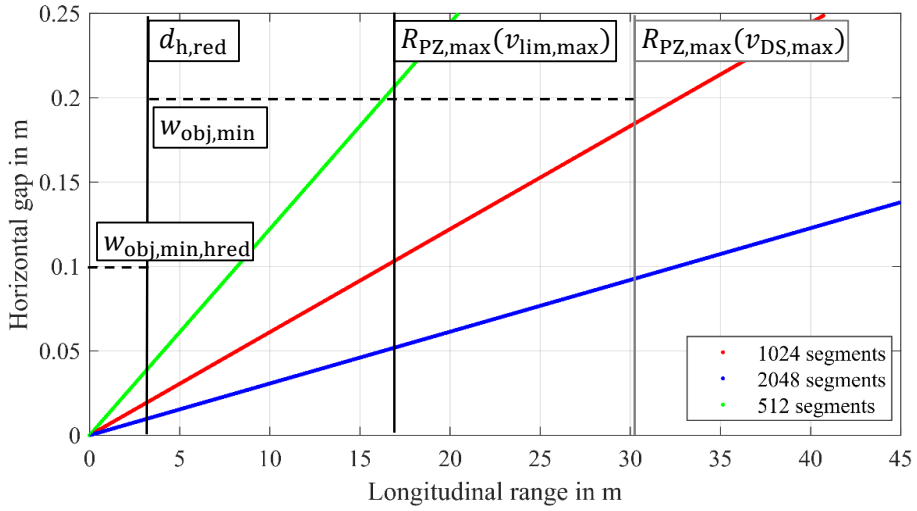


Figure 5-5.: Horizontal gap between two laser beams in dependence of the horizontal resolution and the distance towards the sensor. Minimal object widths to detect are shown for d_{hred} and $R_{\mathrm{PZ,max}}$.

6. Safety Function Implementation

In this chapter, software implementations for the lidar based sensing functions concerning position and speed determination within SF1 *Workspace Compliance* and object detection within SF2 *Collision Avoidance* are presented as a basis for subsequent evaluation. The goal is to work out which functional software building blocks are at least necessary to fulfill the target function, while the algorithms used are to be understood as exemplary.

For the implementations, the Linux-based open source framework Robotic Operating System (ROS)[82] is used. ROS is a modular concept that enables easy communication between different functional modules, so called nodes, which publish or subscribe to so called topics of other nodes. This faciliates the combination of several functions and inputs from different components. It is to note, that while ROS is suited for the set-up and demonstration of the intended functions, it is not considered suitable for a final safety-relevant application in practice according to the requirements on safety relevant software. Nevertheless, as this work is not intended to verify that all software requirements for safety-relevant systems are met, but rather aims to demonstrate the general feasibility of functions, the system is considered applicable.

6.1. Position and Speed Determination

The realization of a landmark based positioning system via the lidar sensors requires an algorithmic concept as well as a landmark architecture that is conducive to this concept and that meets the detection capabilities of the sensors in the given environment. Since the use case of the WMDS for a lidar and landmark based positioning system is unique, the adoption of an existing system is not possible. Therefore, use case specific requirements must be derived and realized in a suitable concept. The following chapter presents the *Lidar and Landmark Based Local Positioning System (LLLPS)* developed for the WMDS. After a description and selection of common landmark based localization principles, a suitable landmark design is derived and the software implementation is presented.

The content of this chapter is mainly taken from a previous publication of the author[83], which summarizes the results of the Master Thesis of Betschinske[84], and is extended with additional content. Results that are not included in the publication, but taken from the Master Thesis, are referenced accordingly.

[82] Open Source Robotics Foundation, Inc.: ROS - Robotic Operating System (2022).

[83] Lutwitzi, M. et al.: Lidar and Landmark based Positioning System for WMDS (2022).

[84] Betschinske, D.: Master Thesis, Position Determination with Lidar Sensors for WMDS (2022).

6.1.1. Localization Principle

A common approach for locating objects with respect to known landmarks is *trilateration*, where the position of an object in 2D space is determined via at least three distance measurements d_i towards the object to locate and landmarks. In relation to a single landmark, possible locations of the object correspond to a circle around the landmark with the radius of the measured distance. The actual position of the object is then determined by the intersection of all circles, which is mathematically solved by least-squares estimations. Trilateration corresponds to the principle that is used in GPS localization. A similar approach is *triangulation*, where additionally the azimuth angles Φ_i of the distance measurement towards the longitudinal axis of the object is known and therefore only two distance measurements are necessary. However, unambiguous positioning for both methods further requires that the measurements can be clearly associated to a specific landmark with a known position.[85] For the present use case of the WMDS, this means that the landmarks must be distinguishable in the optical perception of the lidar sensors. Fig. 6-1 visualizes both principles schematically.

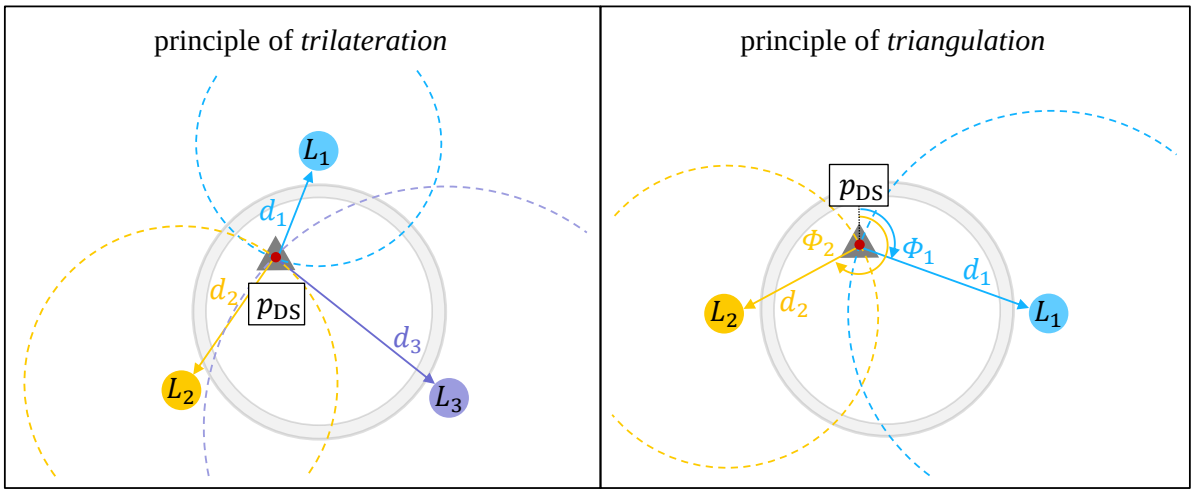


Figure 6-1.: Left: Trilateration with three distinguishable landmarks around the WMDS workspace. The intersection of all three circles indicates the position. Right: Triangulation with two landmarks. The distance measurements deliver two possible positions, but with the associated azimuth angles, only one plausible position is obtained.

The concept of *map matching* is another approach that allows deriving the position of an object relative to detected landmarks and is often used in robotic applications. The concept uses a previously stored map of the environment and matches perceived environmental features to this stored map, which ideally contains intersections. This facilitates the association problem of detected landmarks to known reference points and thus the unambiguous positioning, because landmarks are examined in the context of their environment and thus distinguishing features are created. In a feature-rich scenery, artificial landmarks are not even needed, but natural environmental elements such as curbs, trees, or buildings serve as landmarks.[85] However, in the context of WMDS operation, where only a flat surface is available in the close environment, the

[85] Tzafestas, S. G.: 12 - Mobile Robot Localization and Mapping (2014) p. 493-499.

addition of a to be determined number of distinguishable landmarks outside the workspace is required as well.

The map matching is considered less sensitive towards incorrect assignments of detected landmarks, which would lead to wrong position estimates, and therefore is applied instead of trilateration or triangulation. With this concept, two major tasks include the association of perceived landmarks to the landmarks in the stored map and the determination of the transformation required to map the perceived landmarks towards those of the map. This enables to estimate a position and orientation of the WMDS. This is schematically visualized in Fig. 6-2.

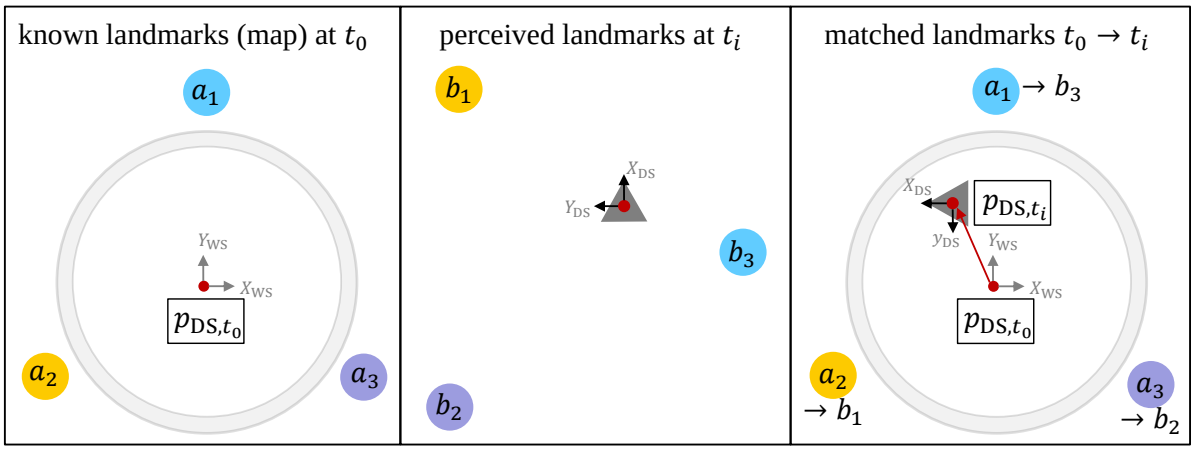


Figure 6-2.: Left: landmark positions are saved in a reference map at the time t_0. The initial position is the workspace center. Center: the landmarks are perceived in the WMDS coordinate system at a time t_i. Right: After determining correspondences between perceived and known landmarks (same colour), the position at the time t_i towards the initial position is determined by the transformation required to match both sets of landmarks.

Assuming a set of N landmarks around the WMDS workspace, a reference map is created, containing the reference point set of map landmarks $A = \{\boldsymbol{a}_j \in \mathbb{R}^2 \,|\, j = 1, ..., N\}$ in two dimensional space. These correspond to the true landmark positions. During operation, the WMDS perceives M landmarks at a specific time t_i, which can be more or less or the exact number of the N landmarks. These are represented by the point set of perceived landmarks $B = \{\boldsymbol{b}_k \in \mathbb{R}^2 \,|\, k = 1, ..., M\}$. The correspondences between the landmarks in the stored map $\boldsymbol{a}_j$ and the physical landmarks $\boldsymbol{b}_k$ perceived by the sensors are determined. The output is a set of K correspondences $C = \{[\boldsymbol{a}_j \rightarrow \boldsymbol{b}_k]_l \,|\, l = 1, ..., K \leq N, M\}$. The rigid transformation that aligns the corresponding points $\boldsymbol{a}_j$ and $\boldsymbol{b}_k$ is then described by a translation vector $\mathbf{t} \in \mathbb{R}^2$ and a rotation matrix $\mathbf{R} \in \mathbb{R}^{2x2}$ and the transformation is executed with a matrix multiplication.[86]

$$\mathbf{T} = \begin{bmatrix} \mathbf{R} & \mathbf{t} \\ 0 & 1 \end{bmatrix} \tag{6-1}$$

$$^{\mathrm{DS},t_0}\mathbf{a}_j = {}^{\mathrm{DS},t_i \rightarrow t_0}\mathbf{T}\, {}^{\mathrm{DS},t_i}\mathbf{b}_k \tag{6-2}$$

$$\mathbf{p}_{\mathrm{DS},t_i} = {}^{\mathrm{DS},t_i \rightarrow t_0}\mathbf{T}^{-1}\, \mathbf{p}_{\mathrm{DS},t_0} \tag{6-3}$$

[86] Betschinske, D.: Master Thesis, Position Determination with Lidar Sensors for WMDS (2022) p. 26-27.

6.1.2. Design Goals

The architecture of landmarks as well as the algorithms to determine a WMDS position and speed from the obtained lidar point cloud via map matching are to be designed towards the following goals:

- Functionality: The LLLPS must enable unambiguous position and speed determination of the WMDS for every position and orientation within the workspace, while the landmarks are required to be positioned outside the workspace. The system shall be adaptable to varying workspace sizes, which means the landmark setup must be portable and flexible.
- Performance: The accuracy of position and speed determination is relevant for the radial speed limit design and therewith for the usable motion space. To avoid undesired space limitations, the function shall be developed towards a possibly high measurement accuracy, which is not only influenced by the used sensor hardware, but also the landmark design. Furthermore, the algorithm itself and the usage of post processing filters influences the data quality. In the same way, the cycle time of the LLLPS algorithm is of interest, as it affects the reaction time for detecting a limit violation, which is also included in the calculation of the radial speed limits. If the algorithm stays below a cycle time of 50 ms, no additional influence on the reaction time takes place, since the lidar sensors operate at 20 Hz. The previously set target is that the combination of measurement accuracy and cycle time restrict the available motion space radius by less than $1\,\mathrm{m}$. With a cycle time of 0.05 s at a maximum speed of 10 m/s, this means the measurement error shall remain below 0.5 m.
- Safety: The safety of the system is endangered if measurement errors become larger than assumed under normal conditions. This can result from the loss of landmarks in the sensor data, as well as when a misattribution of correspondences occurs, e.g. because another environmental element is erroneously considered a landmark. In addition, errors can arise if the true landmark positions do not correspond to those saved in the reference map, for example because they have been moved, which should also be avoided. Both should be prevented by a robust and uniquely identifiable design of the landmarks and a robust algorithm that excludes implausible measurement values.

6.1.3. Landmark Architecture

Design Criteria

The previously stated design goals require a landmark architecture that meets the perceptual capabilities of the lidar sensor system and is clearly highlighted in the sensor data from other environmental features. Furthermore, the individual landmarks must be distinguishable from each

other in the obtained lidar point cloud. Appropriate design can further influence the performance and the robustness of the function. The following criteria are considered for the landmark design:

- From the goal of overall *system mobility*, it follows that the landmarks should be portable by individuals and applicable to varying workspace sizes.
- A *robust stand position* to avoid a turn over requires low air resistance or a high stability.
- The *number of landmarks* shall allow unambiguous position determination, which requires at least two landmarks in two-dimensional space, that are uniquely identifiable and distinguishable from each other. However, the actual number of landmarks should be higher to preserve the function in case of false-negative detections or loss of single landmarks.
- The *distinctiveness of the landmarks from other environmental features* shall enable the software to extract the landmarks from the point cloud and prevent the risk of misidentification. Retroreflective surfaces on the landmarks are, among others, a suitable measure to highlight their detections in the point cloud.
- Another criterion is the *distinguishability of landmarks from each other* enabling unambiguous identification of the landmarks in the point cloud. Therefore, possibilites of landmark coding are considered. This includes different shapes of single landmarks, the varying distribution of reflecting areas within a landmark, varying reflectivity of the surfaces and the variation of the relative position of the landmarks to each other.
- The *landmark shape* shall enable uniform detection properties from every position and orientation of the WMDS within the workspace. It therefore is advantageous to choose a design that provides a projected area and reflective properties regardless of the angle of observation.
- The *required size* of the landmarks depends on the resolution of the lidar sensors. The required minimum width and height of the effectively reflecting area are determined by the horizontal and vertical resolution of the sensor at the maximum landmark distance (cf. Fig. 5-4 and Fig. 5-5). This shall be designed such that the landmarks are hit by multiple laser beams in the maximum distance.

Chosen Landmark Architecture

The final landmark architecture is the result of a concept variation and evaluation process with respect to the design criteria mentioned above. The selected setup consists of eight retroreflective cylinders arranged in four pairs, as shown in Fig. 6-3. The cylinders provide a projected area and salient reflective properties invariant to the angle of observation. The pairwise arrangement serves as coding of the landmarks: Each pair has a uniquely large distance d_i in between $(4, 6, 8, 10\,\mathrm{m})$. The total arrangement of the landmarks is distinctive to other objects and a unique assignment of the identified cylinders to a known map becomes possible. The spatial distribution of the

landmarks is considered to be a particularly robust feature, hardly affected by the angle of incidence and the distance to the landmarks. Furthermore, the high number of individual landmarks makes the system insensitive to individual losses of landmarks, which also enables an application on large workspaces, where possibly not all landmarks are within the sensors' FOV at the same time.

The concept is implemented using oil barrels with a height of $0.88\,\mathrm{m}$, a diameter of $0.61\,\mathrm{m}$ and RA3A-graded retro reflective sheeting. The cylinder pairs are connected with ropes of the length of the individual d_i to allow easy and failsafe placement on the workspace.

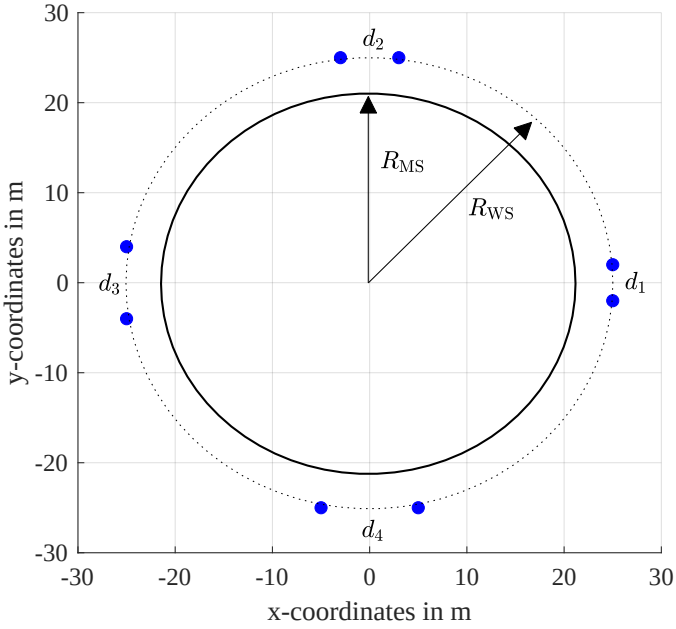


Figure 6-3.: Final landmark architecture. Four pairs of landmarks with individual distances d_i are located on the outer workspace radius.

6.1.4. Software Implementation

Prerequisites

Due to the time passing during a 360° rotation of the sensor unit, not all points in the environment are scanned at exactly the same time. As a result, the so-called *motion scan effect* occurs at high relative speeds between the WMDS and landmarks. The effect is represented by multiple, spatially distorted appearances of detections, which actually belong to the same object. In the areas where the FOV of two neighboring sensors are overlapped, additional time transition zones further strengthen this effect. In particular at rotational movements, the distortion increases linearly with the distance of an object and therefore is of more significance than linear motion (cf. Annex C). Since the distorted appearance of landmarks in the point cloud is a potential thread to finding the correct correspondences, the following preprocessing steps are conducted:

- The time stamps of the three lidar sensors are synchronized using the Precision Time Protocol (PTP) according to IEEE 1588[87].
- The sensor phases are synchronized in a way that the complete FOV around the WMDS is covered after a 180° rotation of each sensor. This halves the time required to obtain the fully relevant point cloud and thereby reduces time shifts in the overlapping areas of two sensors (cf. Fig. C-1 in Annex C).
- The point cloud is rectified using the so-called *de-skew* approach, inspired by He et. al.[88]. An estimate of the rotation of the WMDS, measured by the sensor's built-in IMU and averaged over a scan period and all three sensors, is applied to all points in the point cloud.

Fig. 6-4 visualizes a distorted point cloud due to the motion scan effect and the results after the described measures are implemented, indicating that the measures are successful in avoiding multiple appearances of landmarks.

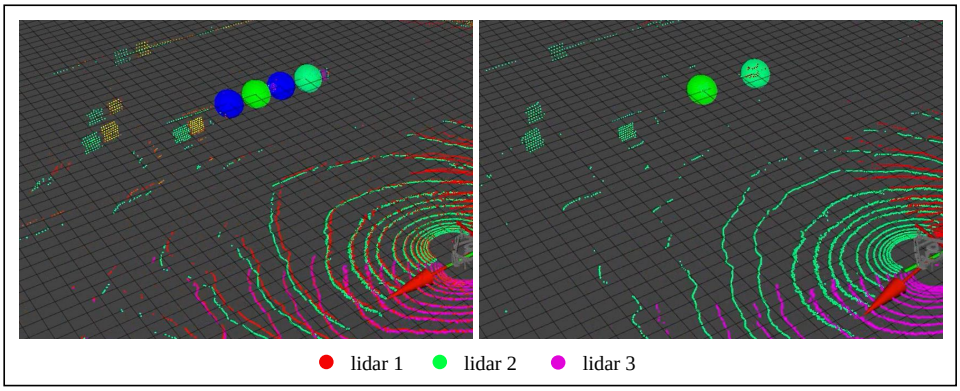


Figure 6-4.: Left: without measures against motion scan, two landmarks (bubbles) and other environmental features are multiply detected at different positions by the individual lidar sensors. Right: with the measures applied, the detections of individual sensors are overlapping and only the true number of landmarks is detected.

LLLPS Algorithm

The final software implementation is the result of an iterative process of developing and testing with reference data. The primary inputs for the algorithm are a rotation-rate estimate based on the data of the lidar's IMU and the merged point cloud of all three sensors. It is implemented using the ROS framework and the Point Cloud Library[89]. The architecture is divided into six elementary modules shown in Fig. 6-5 and briefly described below.

1. The *preprocessing* aims at reducing quantity and increasing quality of the points in the merged point cloud. As the retroreflective landmarks provide both high intensity and reflectivity, a large part of the other points can be removed by intensity and reflectivity

[87] IEEE 1588: Precision Clock Synchronization Protocol (2008).

[88] He, L. et al.: De-Skewing LiDAR Scan for Refinement of Local Mapping (2020).

[89] Rusu, R. B.; Cousins, S.: 3D is here: Point Cloud Library (PCL) (2011).

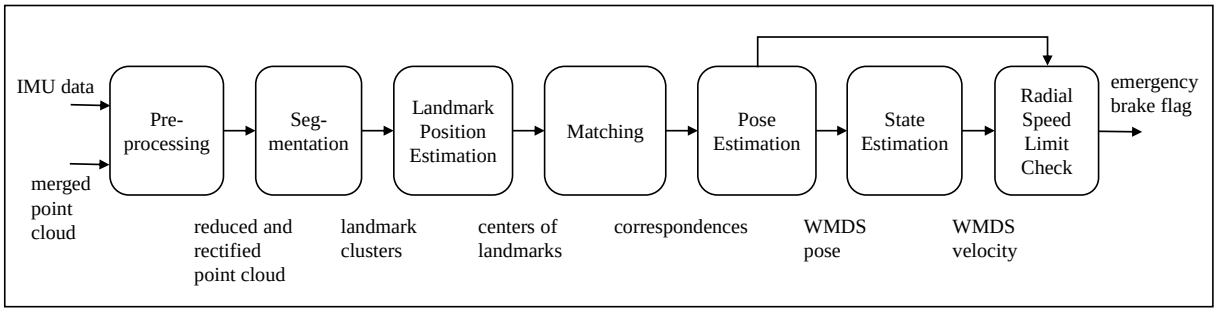


Figure 6-5.: Modules with inputs and outputs of the LLLPS algorithm.

threshold filtering. With the current landmark architecture, reductions of the point cloud of over 99% is achieved without significantly affecting the perception of the landmarks. Furthermore, the point cloud is de-skewed with the approach discussed above.

2. The *segmentation* joins the remaining point accumulations within a predefined search radius into clusters using DBSCAN [90]. The z-component of the clustered points are eliminated to reduce the scans to a two-dimensional point set.

3. The *landmark position estimation* aims to estimate the center point of the cylinders represented by the obtained clusters. After determining the cluster centroids, a constant offset Δr is applied in the radial direction of the angle of incidence of the sensor towards a landmark. This offset is an experimentally determined estimation including theoretical geometric considerations and observed near-field distortion effects of the retroreflective surface. Especially in close proximity to the landmarks of $< 10\,\mathrm{m}$, it is observed that the scans do not necessarily represent the cylinder's geometry correctly, which is exemplary illustrated in Fig. 6-6. The effect varies dependent on the distance of the sensors to the landmarks, meaning the surface is represented more precisely at larger distances (cf. Fig. C-2 in Annex C). Therefore, the necessary displacement is only roughly approximated. The manufacturer of the Ouster lidar sensors indicates in the data sheet, that the precision is lower for retroreflectors than for lambertian reflectors (cf. Tab. 5-1). Further research on the near range effects of retroreflection could enable a more precise approximation of the required offset, e.g. by a dynamic offset correction according to a distance dependent reflection model.

4. The *matching* defines the correspondences between detected landmarks and reference landmarks in an iterative procedure. The reference map contains the actual landmark distribution on the workspace and is generated at the beginning of the operation through an initial map creation process. The determination of correspondences is implemented by a vector-based brute-force iteration approach that aligns the estimated center points of the

[90] Ester, M. et al.: A Density-Based Algorithm for Discovering Clusters (1996).

[91] Betschinske, D.: Master Thesis, Position Determination with Lidar Sensors for WMDS (2022) a: p. 129, b: p. 84-86.

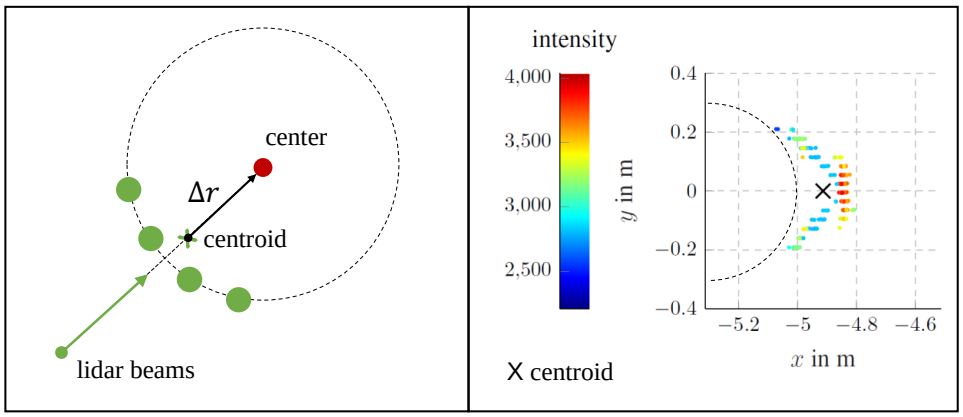


Figure 6-6.: Offset correction of the cluster centroids to the estimated landmark center. Left: theoretical concept of the offset correction. Right: reflection properties of the retroreflective sheeting do not represent the landmark surface for a landmark in 5 m distance to the lidar sensor, adapted from Betschinske[91a].

detected landmarks with the landmarks in the map with an initial estimated transformation. Then, for each landmark point of the reference map a_j, the nearest neighbors of the aligned set of detected landmark center points b_k are determined within a predefined search radius ξ_{max}. These represent the current estimate of the correspondences K. The sum of the nearest neighbor distances $d_{a_j b_k}$ of all correspondences within K is then used as a *fitness score* s_{fit} that indicates the matching quality of the current iteration (cf. Equ. 6-4). If no nearest neighbour is found for a point a_j within the search radius, the size of the search radius is accounted in the fitness score (cf. Equ. 6-5). This ensures that a matching of all 8 landmarks is preferred towards a matching of a low number of landmarks with smaller deviations to the map. After a full iteration, the correspondences with the minimum fitness score represent the best fitting match and are returned for the further steps.[91b]

$$s_{\text{fit}} = \sum_{l=1}^{L} \left[d_{a_j b_k} \right]_l \tag{6-4}$$

$$d_{a_j b_k} = \begin{cases} |a_j - b_k| & \text{for } |a_j - b_k| < \xi_{max} \\ \xi_{max} & \text{else} \end{cases} \tag{6-5}$$

5. The *pose estimation* determines the optimized transformation matrix as specified in Equ. (6-1) and Equ. (6-3) between the found correspondences under application of the Iterative Closest Point algorithm[92].

6. The *state estimation* derives the pose over time to obtain the linear and angular velocity with respect to the workspace coordinate system.

7. The *Radial Speed Limit Check* observes compliance with the radial speed limits according to the logic defined in Equ. (4-7) in Chapter 4.2. The emergency brake flag is set to 1, if a

[92] Point Cloud Library: Iterative Closest Point (2021).

limit is exceeded.

Fig. 6-7 illustrates basic steps of the lidar data processing.

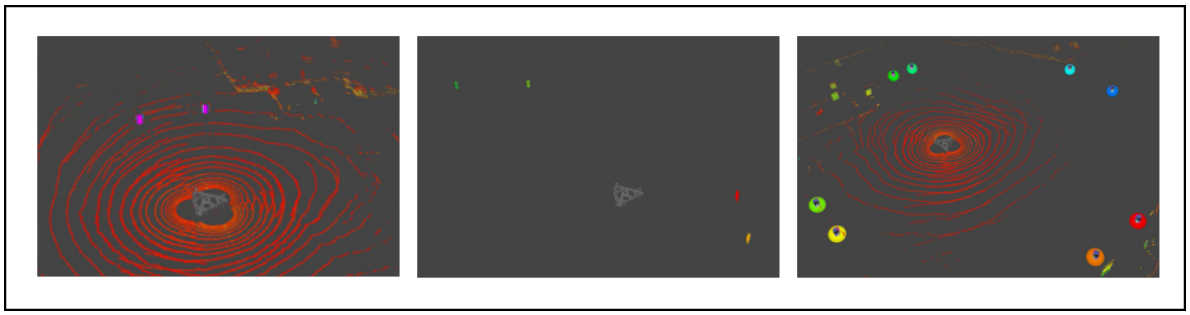


Figure 6-7.: Visualized processing steps of the LLLPS algorithm. Left: unprocessed point cloud with reflectivity color transformation. Center: point cloud filtered for intensity and reflectivity, after the detections of individual landmarks are assigned to a common cluster. Right: landmark clusters are matched with the reference map.

6.1.5. Calibration and Verification

The presented approach for the determination of the WMDS' position and speed within the workspace is to be verified in its basic functionality. It further must be calibrated towards a possibly high measurement accuracy, which requires the avoidance of false positive or false negative detected landmark clusters and an accurate matching. A second calibration goal is a possibly low cycle time of the algorithm. Both requires the calibration of several parameters of the algorithm, such as thresholds for intensity and reflectivity filters in the preprocessing, the DB scan search radius and minimum cluster size, the radial offset for landmark center estimation and the fitness score search radius. This is conducted by iterative change of the parameters within plausible ranges and the simultaneous observation of position and speed data quality and algorithm cycle time.

As a reference for the verification and the effect of the parameter variations to the measurement accuracy, the position and speed data obtained by the LLLPS is compared to a second positioning system installed on the scaled WMDS prototype. The reference measurement system is an ADMA-G-Pro+[93], which is a GPS-aided fiber-optic gyroscope with inertial sensors for high-precision vehicle dynamics measurements. The device is further supplemented by an NTRIP-DGPS-Box to enable correction of the GPS data with respect to DGPS ground-based reference stations. According to the manufacturer, this set-up enables positioning with an accuracy of $0.01\,\mathrm{m}$. Representative driving maneuvers of a driving simulation are used as a main data source for the verification and calibration, containing combinations of longitudinal, lateral and rotational motion, exploiting the entire workspace while crossing the workspace center regularly, as shown in Fig. 6-8. The obtained position signals of LLLPS and DGPS are correlated in time and adjusted

[93] GeneSys Offenburg: ADMA data sheet (2022).

for an installation-related offset in position and orientation of both measurement systems on the vehicle.

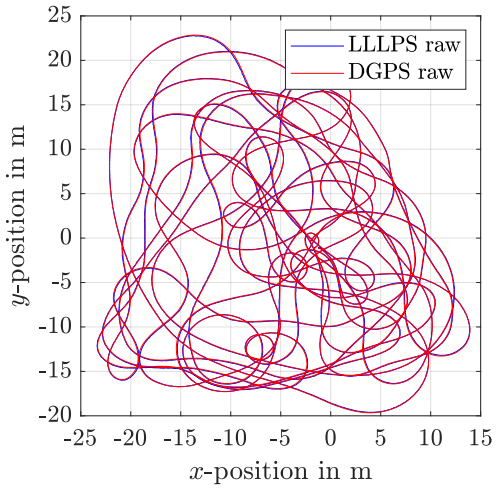


Figure 6-8.: Path of representative dynamic maneuver of the scaled WMDS prototype on the August Euler Airfield for calibration and verification of the LLLPS. The maximum driven speed is 3.6 m/s, the maximum yaw rate is 80 °/s.

The parameter calibration is conducted by replaying the data collected in the maneuver and processing it with varying parameters. In this chapter, only the data quality and performance of the final parameter set-up is shown. For further details about the process of determination of the target values, reference is made to the work of Betschinske[94].

With the calibrated parameters, the algorithm presented in Fig. 6-5 has a maximum measured total processing time of 34.4 ms within the representative maneuver, the 99.9 %-quantile is 17 ms. It therefore remains below a cycle time of 50 ms on the development hardware and thus within one rotation cycle of the lidar sensors (cf. Fig. C-4 and Fig. C-3 in Annex C). The algorithm itself therefore does not increase the reaction time of the sensing and processing subfunctions $\tau_{\mathrm{react,sp}}$.

The signal deviations between DGPS and LLLPS are shown in Fig. 6-9. The left figure presents the absolute deviation between the GPS and LLLPS position data in a raw state and a filtered state. For the raw data, the maximum deviation is $0.28\,\mathrm{m}$, the 99 % quantile is at $0.20\,\mathrm{m}$. The second graph illustrates the deviation between GPS and LLLPS data after a centered moving average filter with a window size of three elements is applied to both signals. This reduces the maximum deviation to $0.22\,\mathrm{m}$ and the 99 % quantile to $0.15\,\mathrm{m}$. The reduction of the deviations by applying the filter shows that the signals are affected by noise.

In the right side of Fig. 6-9, the absolute velocity deviation between the two measurement sets is shown in a raw state and a filtered state. The maximum velocity deviation for the raw data is $1.84\,\mathrm{m/s}$, the 99 % quantile is $0.98\,\mathrm{m/s}$. The noise causing these high deviations is also reduced by the application of a moving average filter with a window size of 3 elements, reducing the

[94] Betschinske, D.: Master Thesis, Position Determination with Lidar Sensors for WMDS (2022) p. 117-118.

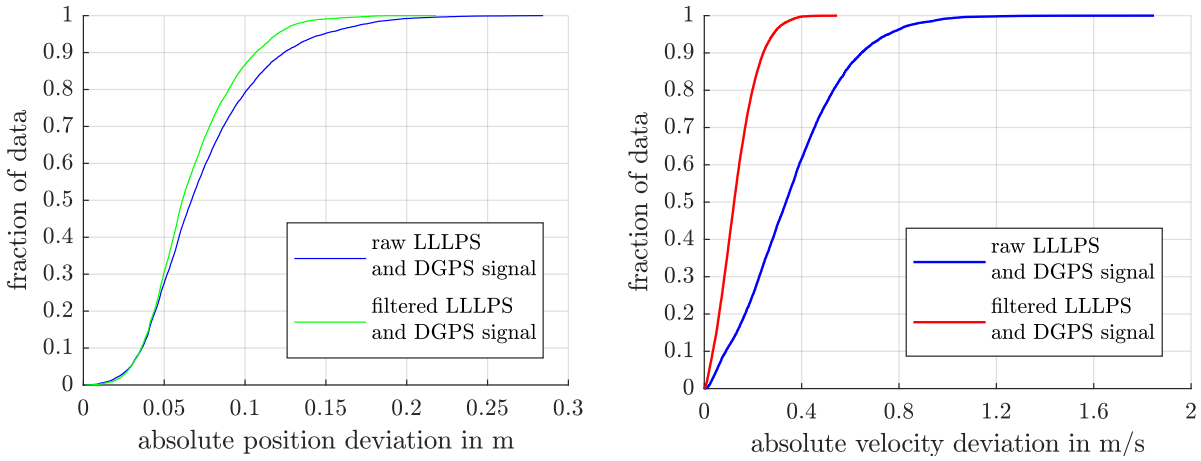


Figure 6-9.: Position and velocity deviation between DGPS and LLLPS for the representative dynamic test maneuver.

maximum deviation to $0.54\,\mathrm{m/s}$, while the 99 % quantile is $0.36\,\mathrm{m/s}$. It can be seen that the influence of noise is noticeably greater for velocity than for position.

Reducing the data noise by filtering reduces the maximum measurement uncertainty Δp_{DS} and Δv_{DS} to be expected, which has a direct influence on the measurement error to be respected in the dimensioning of the radial speed limits (cf. Equ. 4-10). A smaller maximum measurement uncertainty can thus favor the usability of the workspace. Nevertheless, filtering induces an additional run time of the algorithm, influencing the reaction time $\tau_{\mathrm{react,sp}}$ of the safety function. This on the other hand increases the critical stopping distance of the WMDS linearly with WMDS speed. Therefore, the reduction of the maximum measurement deviation by filtering towards the extension of the stopping distance of the WMDS by the extended reaction time is of interest for the choice of a filter. For the exemplary applied centered moving mean filter with a window size of 3, the additional reaction time is 2 time steps. This increases $\tau_{\mathrm{react,sp}}$ from 0.05 to $0.15\,\mathrm{s}$. Considering the measurement deviations towards the DGPS reference shown in Fig. 6-9 to be the measurement errors Δp_{DS} and Δv_{DS} of the system, the effect of filtering on the radial speed limits is analyzed. This is shown in Fig. C-5 in Annex C and reveals that even though an additional reaction time is induced, a greater usage of the overall workspace is possible with filtered data, which is mainly influenced by the effect of the filtering on Δv_{DS}. In the future, it is recommended to further design and analyse appropriate filters to obtain the best results for both measurement quantities, e.g. by an Extended Kalman Filter. Nevertheless, even the simple moving mean filter can demonstrate a positive effect.

Since the LLLPS provides consistent data to the GPS measurements across the representative maneuver with no significant outliers, the functionality is verified. Safety and availability under extreme conditions are investigated in Chapter 8.1.

6.2. Object Detection

The following implementation intends to realize SF2.3 and SF2.4 (object detection within the PZ). After deriving minimum functional requirements on the algorithm, the final software implementation is described.

6.2.1. Design Goals and Object Hypotheses

The object detection algorithm is to be designed towards the following goals:

- Functionality: It is attempted to reduce the functional requirements on the detection algorithm to a minimum to avoid uncertainties for a safe object detection. Therefore, an object must not be classified and its direction of motion or ego velocity must not be known. Simply the presence of a relevant object (as specified in Chapter 4.3.2) and its minimum distance towards the WMDS is to be determined.
- Performance: The cycle time of the object detection algorithm influences the reaction time towards the detection of an object and the trigger of an emergency brake. This quantity influences the PZ size and thereby the size of the safety buffer around the workspace, reducing the usable space in a given workspace (cf. Chapter 4.3.1). If the algorithm stays below a cycle time of $50\,\mathrm{ms}$, no additional influence on the reaction time takes place, since the lidar sensors operate at 20 Hz. There is no hard limit for a tolerated safety buffer, but an alignment of the PZ with the position dependent speed limits is necessary (cf. UR2.3 in Tab. 4-3). Considering the exemplary applied moving mean filter for the LLLPS, which adds two further cycles to the reaction time of the workspace compliance function, the same reaction time increase can be tolerated for the object detection.
- Safety: The algorithm is considered safe if objects are detected at any time and under any considerable environmental condition. Of course, the algorithm can only identify objects that have been detected by the sensors. But from a software point of view, it is required that no relevant object, although detected by the sensors and appearing in the sensor data, is discriminated by the algorithm (cf. SFR2.2.3 in Tab. 4-3).
- Usability: The system shall interrupt WMDS operation only in safety-critical cases, i.e., when collision hazards are present. Therefore, the algorithm shall be robust against false positive object detections, possibly induced e.g. by atmospheric elements or sensor specific effects, to prevent from reduction of the availability of the WMDS (cf. UR2.1 in Tab. 4-3).

A main challenge therefore is to eliminate false detections as far as possible, while not discriminating relevant objects. The definition of an object must be translated into a description adapted to the data provided by the lidars. As the sensor data depicts the environment in a three dimensional representation of points (point cloud), lidar detections belonging to the non-hazardous

environmental elements are included in the obtained data. Therefore, an *object hypothesis (OH)* is defined, according to which the lidar detections are attributed to a potential collision object or the environment, thereby avoiding the false negative detection of objects and the false positive detection by environmental elements.

If initially every detectable object within the PZ is to be considered as a relevant object, a discrimination according to spatial properties is possible. Thus, any sensor detection at a distance outside the PZ is not relevant. Likewise, a detection is not relevant if it is a ground detection. The following object hypothesis is derived from this:

- *OH1: Every detection within the PZ, which is not a ground detection, constitutes a relevant object.*

Therefore, the object detection algorithm must at least reliably separate between ground detections and non-ground detections within the PZ. With this method, nevertheless a single detection above the ground would trigger an emergency brake when within the PZ. As this is prone to false positive detections, e.g. through insufficient ground filtering or reflections from atmospheric particles, further criteria for a relevant object is required. Assuming that relevant objects always have a certain minimum size by which more than one detection of them occurs and, in contrast, atmospheric reflections are only appearing with single detections, the following refinement of OH1 is made:

- *OH2: Detections within the PZ, which are not ground detections, and belong to a cluster of at least* $n_\mathrm{v} \times n_\mathrm{h}$ *points, constitute a relevant object.*

Thereby, the cluster refers to the accumulation of neighboring detections and is defined by a number of neighboured vertical detections n_v and horizontal detections n_h. Further thresholds must be set that determine until which distance points are considered neighbours. The defined threshold of the cluster size must be large enough to separate from false positive detections. On the other hand, the cluster size shall not be chosen beyond the detection capabilities of the sensors and therefore is limited upwards by the minimum object height $h_\mathrm{obj,min}$ and width $w_\mathrm{obj,min}$, maximum object distance $d_\mathrm{obj,max}$ within the maximum PZ radius and the vertical and azimuthal sensor resolution $\Delta\vartheta_\mathrm{s}$ and $\Delta\Phi_\mathrm{s}$. To ensure that the condition can be met for the given sensor specification, the set cluster size threshold must fulfill the following relations:

$$n_\mathrm{v} \leq \frac{h_\mathrm{obj,min}}{2\, d_\mathrm{obj,max}\, \sin(\frac{\Delta\vartheta_\mathrm{s}}{2})} \tag{6-6}$$

$$n_\mathrm{h} \leq \frac{w_\mathrm{obj,min}}{2\, d_\mathrm{obj,max}\, \sin(\frac{\Delta\Phi_\mathrm{s}}{2})} \tag{6-7}$$

These values are determined under the theoretical assumption that the sensors scan the environment at discrete intervals according to the resolution specified by the manufacturer (cf. Tab. 5-1). In reality, the gaps in which no detections can occur may be deviating, whereby beam divergence

can lead to actually smaller gaps, while deviating beam emission angles compared to the sensor specifications can lead to larger gaps. The calculated value should therefore be verified in practice.

Another possibility is to include a temporal condition to the object hypothesis. As relevant objects appear over several time steps and, in contrast, atmospheric reflections might only appear randomly for single time steps, the following refinements of the OH is possible:

- *OH3: Every detection within the PZ, which is not a ground detection, and appears for at least n_{cyc} cycles in a row, constitutes a relevant object.*

Thereby, n_{cyc} is a to be determined number of cycles of evaluation whether an object is within the ground filtered protected zone. For the safety of this criterion, it is important that the assignment of an object detection to preceding or following cycles does not include errors that cause the temporal condition to be missed. It further is to consider that such a temporal criterion increases the run time of the algorithm, which is to be taken into account in the reaction time for the PZ dimensioning.

Further criteria concerning the reflectivity or intensity properties of object detections are not included in possible object hypotheses, as these characteristics are hard to estimate for all reasonably conceiveable environmental conditions and object properties. The applicability of the presented object hypotheses is investigated within the software implementation process.

6.2.2. Software Implementation

The software implementation is realized with help of existing algorithms from the Point Cloud Library[95], which is an open source library for point cloud processing algorithms. Representative lidar data for the development is obtained from driving maneuvers with the prototype vehicle on the target workspace according to Fig. 3-3. While the process was iterative to elaborate the most suitable solution in accordance with previously described object hypotheses, only the final implementation is presented here. This is a combination of OH2 and OH3. The required basic elements of the algorithm are respectively extracted from these object hypotheses, including a ground segmentation, a clustering and a temporal check. The algorithms are mainly extracted from the work of Zermas et. al.[96], which provides a processing pipeline for fast 3D segmentation of point clouds that satisfies the identified basic elements. These algorithms are modified to suit the use case and are further supplemented with other processing steps, which was implemented within the bachelor thesis of Gresek[97]. The overall algorithm is divided into four main modules shown in Fig. 6-10.

[95] Rusu, R. B.; Cousins, S.: 3D is here: Point Cloud Library (PCL) (2011).

[96] Zermas, D. et al.: Fast segmentation of 3D point clouds (2017).

[97] Gresek, P. M.: Bachelor Thesis, Collision Protection with Lidar for WMDS (2022).

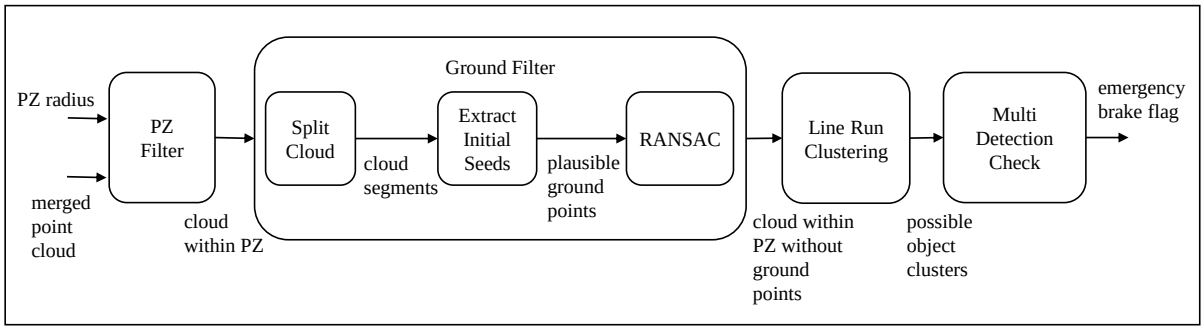


Figure 6-10.: Modules with inputs and outputs of the object detection algorithm. Own illustration according to Gresek[97].

Input to the algorithm are a merged point cloud of the three sensors according to Fig. 5-3 as well as the PZ radius, which is previously adapted to the actual speed of the WMDS. Within the development of the function, this is obtained from a DGPS based measurement unit installed on the WMDS prototype. To filter the ground detections from the point cloud, a Random Sample Consensus (RANSAC) algorithm is applied.[98] This is an algorithm for identifying parameters of a mathematical model that represents a set of data in order to distinguish data into outliers and inliers. All data points that lie outside a specified height threshold $h_{\mathrm{TH,in}}$ to the found model are considered outliers. Within a predefined number of iterations and for the predefined threshold, the model parameters with the highest number of inliers are returned. The mathematical model in this application respectively is a plane, while it is attempted to represent the actual ground plane as precisely as possible. The application of this algorithm is considered, rather than simply erasing all points with a specific height close to 0, since the workspace surface contains unevenness and slope. Without the application of the RANSAC, the threshold for height filtering would be required to be set higher, so that the minimum size of detectable objects is increased. If the WMDS is operated on a sufficiently flat surface and the sensors can be isolated from inclinations of the WMDS body, this step is supposed to be avoidable. When implementing such a measure, it is important to avoid miscalculations of the ground plane, that in a worst case lead to an object discrimination. Since the determination of the plane model parameters is based on the maximum number of inliers, precautions are necessary to ensure that this plane is always an approximated plane to the true ground, even if the majority of points belong to raised objects.

The implemented algorithm includes the following general modules that enable an processing of the point cloud with respect to the aforementioned OH. Exact parameter values chosen for the final implementation are specified in Chapter 6.2.3.

1. The *PZ Filter* erases all detections from the point cloud that are outside the radius of the PZ and also those that are in a range less than 0.01 m, as these are detections that appear in the sensor housing itself.

2. The *Split Cloud* module separates the point cloud into smaller segments, through which

[98] Fischler, M. A.; Bolles, R. C.: Random sample consensus (1981).

the RANSAC algorithm is allowed to fit multiple smaller planes instead of a single large plane. This enables to find a more precise fitting of the actual workspace ground. The split is based on the three individual sensors, meaning for each sensor a separate plane is approximated. Finer splits are also conceivable, but will increase the algorithm run time.

3. In the *Extract Initial Seeds*[96] module, all points are sorted by height and only the lowest 10 % of points are used as input for the RANSAC application. This ensures that only plausible ground points are used for the plane fitting, and reduces the influence of objects raised above the ground on the plane calculation.

4. The actual *RANSAC* algorithm is applied to the extracted points of step 3, delivering a fitted plane model. Then, all points of the overall point cloud within a height threshold $h_{\mathrm{TH,in}}$[99] towards this plane are assigned as inliers, the others as outliers. The goal of this parameter is to ensure reliable ground detection without impairing the object detection. Respectively, a too small threshold does not include all ground points, which leads to false positive detections. On the other hand, a too large threshold cuts off detections from objects, in the worst case resulting in a small object not to be detected. The selected threshold therefore must be set as a compromise between both criteria. The output is a point cloud that only includes the outliers of the RANSAC application. An additional safety check is implemented, that compares the resulting angle between the plane determined by RANSAC and the expected ground plane, to avoid a hazardous miscalculation, e.g. that a wall would create a vertical ”ground” plane. This angle threshold considers plane angle deviations towards the expected ground plane due to present slope on the workspace.

5. The *Line Run Clustering (LRC)*[96] is an iterative approach to assign adjacent points first inside a scan line and then across following scan lines to a common cluster. A distance threshold $d_{\mathrm{TH,run}}$[99] is defined, by which points within the same scan line are close enough to be considered a single block. These are assigned to the same *run* and receive a common label. This starts with the uppest scan line. Afterwards, the following scan line is investigated for runs that are nearest neighbors to the runs in the previous scan line. This nearest neighbor distance is calculated as the euclidean distance in only x- and y-coordinates of a point. When the nearest neighbour distance is below another distance threshold $d_{\mathrm{TH,merge}}$[99], the label of the previous run is propagated to the new run. This procedure is applied with the modification that all runs within a scan line must at least contain n_{h} points, and a run must at least be merged with n_{v} further runs in following scanlines. Thereby, a minimum cluster size condition for detected objects is created according to OH2. The output of this step are all clusters with individual IDs that contain detections that fullfil the LRC distance thresholds and the minimum number of points.

6. The *Multi Detection Check* serves to trigger emergency braking only for consistent object clusters. While collision objects are consistently present for a certain period of time when

[99] Deviating notation of this parameter from the original source to unify formula characters within this work.

entering the PZ, false positive detections can appear and disappear randomly for single time steps. Therefore, an object clusters must be present for $n_{\mathrm{TH,multi}}$ in a row until the actual emergency brake flag is set. If the multi-detection check is fullfilled, an emergency brake flag is set. To avoid having to assign clusters of successive time steps to each other, which would require a cluster tracking and could create additional detection uncertainty, only the global presence of object clusters without a specific identification is evaluated for $n_{\mathrm{TH,multi}}$ cycles. This would still lead to false positive emergency brakes, if false positive clusters from different areas around the WMDS occurred in succession coincidentally. Nevertheless, the selected procedure turned out to be robust enough to avoid false positives, as it will be described later.

Fig. 6-11 visualizes basic steps of the algorithm in a point cloud illustration.

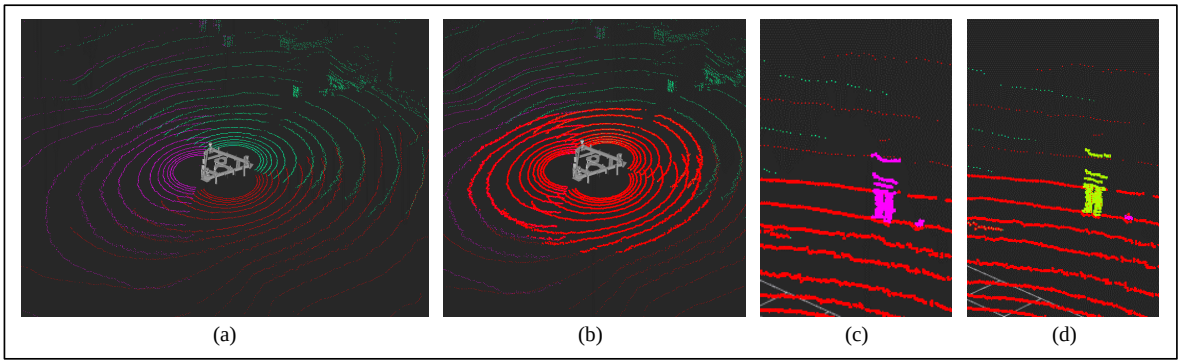


Figure 6-11.: Point cloud illustration of the object detection algorithm steps. (a) Unprocessed point cloud with sensor ID color transformation. (b) Highlighted points within the PZ. (c) Separation between ground inliers (red) and outliers (pink) after RANSAC application. (d) Clustering of the outliers assigns a different color to each cluster.

6.2.3. Calibration and Verification

The presented approach for object detection requires the calibration of suitable values for the RANSAC height threshold $h_{\mathrm{TH,in}}$, the LRC thresholds $d_{\mathrm{TH,run}}$ and $d_{\mathrm{TH,merge}}$, the cluster size thresholds $n_{\mathrm{v}} \times n_{\mathrm{h}}$ as well as the number of cycles for the multi detection check $n_{\mathrm{TH,multi}}$. This calibration focuses on eliminating false positive object detections, while at the same time limiting the actual function as little as possible. The calibration goals are divided into the avoidance of false-positive emergency braking due to ground detections and false-positive emergency braking due to atmospheric reflections. First, limitations on the parameter values are derived, then the resulting values from the calibration are presented.

Ground Filtering Threshold Limits

In Fig. 6-12, the effect of varying RANSAC inlier thresholds $h_{\mathrm{TH,in}}$ is exemplarily shown for momentary snapshots of dynamic point clouds. The WMDS is positioned in the center of the workspace, the PZ is set to 10 m and cleared from objects. The ground inliers and outliers are

investigated for different thresholds in standstill and during a fast rotation with 259 °/s around the WMDS center. It is observed that motion increases the outliers compared to standstill, which is due to the unevenness of the ground and associated WMDS body movements. At standstill with a threshold of 0.1 m, all detections are correctly assigned to the ground. However, the rotation of the WMDS strongly increases the number of outliers. The threshold must thus be set to > 0.1 m to eliminate all ground detections from the outliers in this maneuver and for this particular PZ size.

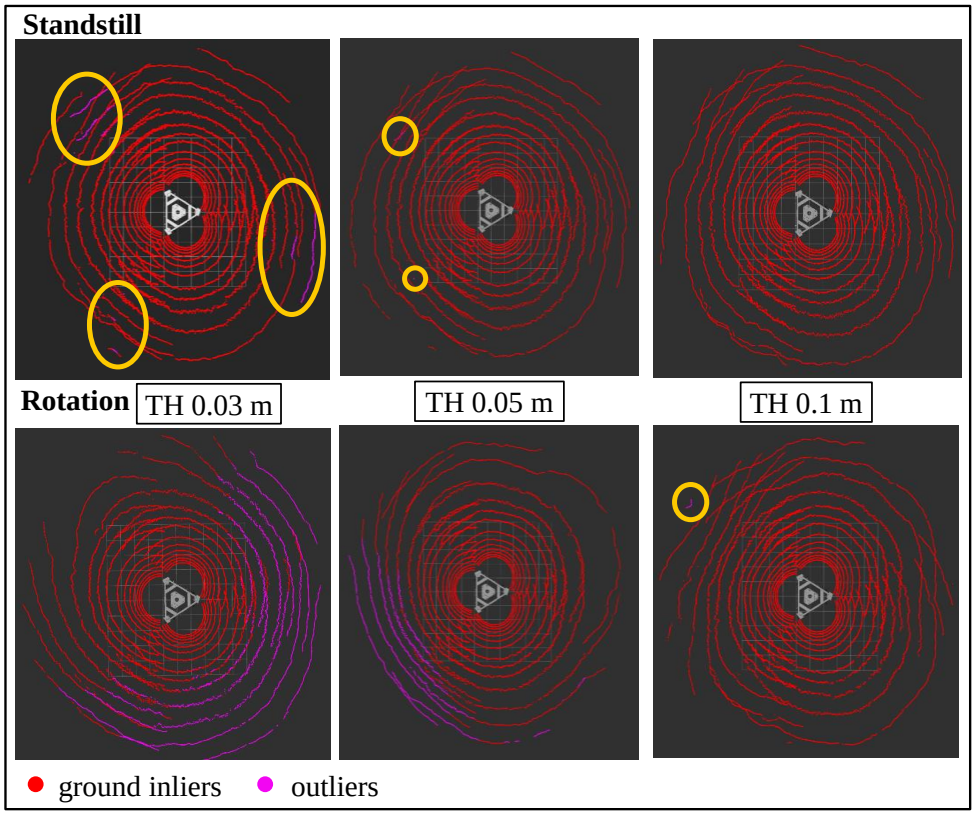


Figure 6-12.: Distribution of ground inliers (red) and outliers (pink, small areas are indicated by yellow circles) for varying thresholds $h_{\mathrm{TH,in}}$ (TH) of a static WMDS vs. a rotating WMDS. The number of outlying ground detections rises for smaller thresholds as well as when the WMDS is in motion.

Nevertheless, a largely chosen threshold induces object detections to be assigned to the ground, which is illustrated in Fig. 6-13 for a human standing in 10 m distance to the WMDS. A threshold of 0.1 m leads to the assignment of object detections from the two lowest layers as ground inliers, which is not acceptable for the detection of small objects. On the other hand, from a threshold of 0.03 m, all detections are correctly assigned to the human. It is to note that the figure shown only represents momentary snapshots. With live sensor data, it is observed that the detections fluctuate even for static objects, so that ground inliers and outliers slightly vary with each time step. A conflict of objectives becomes apparent from these both illustrations, which is to be solved with the combined calibration of all parameters.

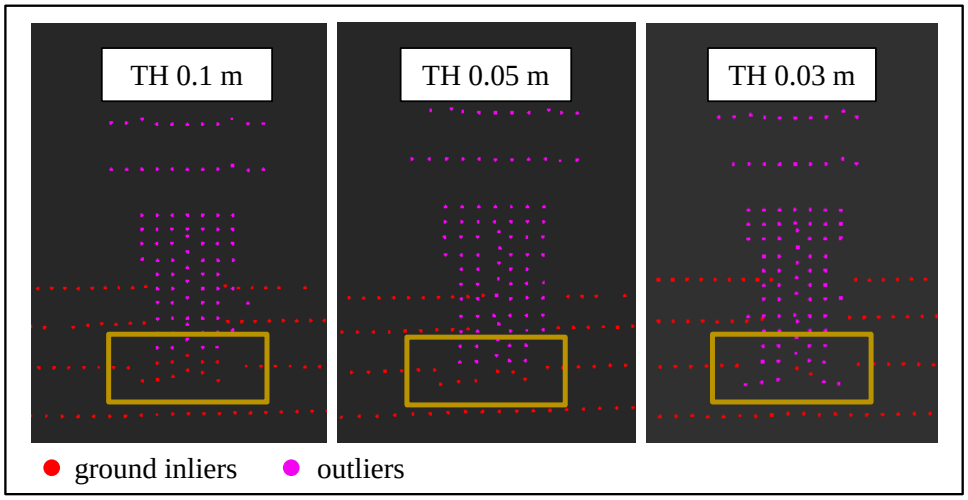


Figure 6-13.: Effect of varying thresholds $h_{\mathrm{TH,in}}$ (TH) on detections of a human standing in 10 m distance.

Minimum Cluster Size Limits

Without a clustering, a single detection above the ground, existing for at least $n_{\mathrm{TH,multi}}$ cycles, would lead to an emergency brake. The origin of such detections is difficult to deduce from the sensor data, but in principle conceivable by e.g. sensor errors or insects as well as particles in the air. In Fig. D-1 in Annex D it is shown how several ghost point detections occur in a cleared PZ in a rotation maneuver of the WMDS, after eliminating all points below a height of 0.3 m. Additionally, increased atmospheric detections can be expected with potential application under light rain. To identify a minimum cluster size applicable for the chosen sensor Ouster OS1-32, Equ. 6-7 and Equ. 6-6 are considered in combination with Fig. 5-5 and Fig. 5-4. Accordingly, only from a distance of approximately 17 m, a clustering becomes possible, since 2 vertical layers and 2 horizontal segments are supposed to impact an object of the minimum size. This equals just $R_{\mathrm{PZ,max}}$ for a limited WMDS speed of 10 m/s. Concluding, n_{v} and n_{h} cannot be set higher than 2, and at the same time, the maximum allowed WMDS speed is to be further reduced if the reaction time of the algorithm increases. Additionally, not a single detection may fail with these thresholds, so that objects of minimum size are reliably detected at all times. A limiting factor is also the RANSAC inlier threshold $h_{\mathrm{TH,in}}$, which may filter out the object detections closest to the ground, as shown in Fig. 6-13.

LRC Thresholds Limits

The LRC includes the threshold $d_{\mathrm{TH,run}}$ for neighboured detections within the same scanline to be considered a common cluster. Furthermore, the distance threshold $d_{\mathrm{TH,merge}}$ sets a minimum value for the distance of nearest neighbors between runs in two scanlines to merge and thereby add to the cluster in vertical direction. For both values, the euclidean distance in only x- and y-coordinates are considered. The larger both thresholds, the more certain that object detections are fully clustered. Too large thresholds can lead to merging of different objects, which is not considered a safety thread for the function, since the closest distance to a detected cluster

is only relevant, not its shape or its expansion. Nevertheless, large thresholds are also more probable to lead to clustered atmospheric detections, e.g. due to rain, which causes undesired false positive detections. For detections of the same scanline, the resolution in azimuth as well as distance measurement deviations must be taken into account for a minimum threshold $d_{\mathrm{TH,run}}$. For neighboring points of subsequent scanlines, the distance measurement deviations are also decisive. Here, the manufacturer specifies 0.03 m for lambertian objects and 0.1 m for retroreflective objects (cf. Tab. 5-1). Additionally, distance deviations due to curvatures in the surface of objects are to be considered for both values. Too small chosen thresholds will avoid detections of the same object to be assigned to one cluster, which can lead to an object discrimination if the minimum cluster size is not fulfilled. Based on the specified measurement deviations and horizontal resolution, and taking into account a buffer for uneven objects, the value for $d_{\mathrm{TH,run}}$ shall not be set lower than 0.3 m, and $d_{\mathrm{TH,merge}}$ shall not be set lower than 0.2 m.

Multi-Detection Cycles

Theoretically, there is no limit for this cycle, since the extended detection time of an actually existing object can be compensated by the PZ dimensioning. However, this means the required distance of initial detection of an object is enlarged towards the original PZ size and must still comply with the given sensor resolution. Therefore, an additional cycle time can in the worst case mean a required limitation of the WMDS speed. As a compromise and also to stay in line with the radial speed limits, $n_{\mathrm{TH,multi}}$ is intended to not be set higher than 3 cycles.

Resulting Calibrated Parameters

To solve the conflicting goals of small object detectability and clean ground detection filtering, the threshold $d_{\mathrm{TH,merge}}$ is used. As shown in Fig. 6-12, mainly the outer rings of ground detections lead to outliers when $d_{\mathrm{TH,in}}$ is chosen too low. The euclidean distance in x- and y- direction of these scan planes is high compared to the distances belonging to a vertically raised object. Therefore, a minimally chosen $d_{\mathrm{TH,merge}}$ can be used to discriminate outlying ground detections in the LRC. To find a final set of parameter values, $d_{\mathrm{TH,merge}}$ is set to 0.2 m and the smallest $d_{\mathrm{TH,in}}$ is iteratively determined, for which no undesired false positive emergency brake triggers are set. To evaluate the occurence of false positive object detections, the representative dynamic drive maneuver, as shown in Fig. 6-8, is used, as this covers a large area of the given workspace and represents expectable motion of the WMDS during a driving simulation. To also verify the correct detection of objects, persons enter the PZ at various time steps during the maneuver. The emergency brake flag is observed for correct object triggers as well as triggers in situations where no object is in the PZ. With this procedure, it is identified, that $d_{\mathrm{TH,in}}$ can be reduced to a minimum of 0.06 m. Even though this does not fully include all ground detections in the RANSAC plane, the LRC discriminates most of them. Outliers that still occur at individual time steps in the near range are eliminated by the multi-detection check, which is finally required to be set to $n_{\mathrm{TH,multi}} = 3$. Fig. D-2 in Annex D shows the results of the object detection function

evaluated on the dynamic drive, indicating that a set of parameters is found that eliminates false positive detections fully. The revised PZ dimensions with this modification of reaction time are given in Fig. D-4.

With this approach, it is obvious that clustering is needed not only to avoid false positives due to atmospheric detections, but also to minimize the ground threshold. To strengthen this argument, it was also investigated how large $d_{\mathrm{TH,in}}$ is to be set if vertical clustering is ommitted. This is advantageous if small objects are detected more reliably because they only have to be hit by one scanline. However, even a threshold of $0.12\,\mathrm{m}$ did not help to ensure that the representative drive maneuver remains false positive free (cf. Fig. D-3), which is why this approach is discarded.

6.2.4. Conclusion

The chosen parameter values are to be understood as the most suitable values for the conditions at the Griesheim Airfield and the chosen sensors, while deviating ground conditions or other sensor specifications could lead to another set of optimal values. The unevenness of the ground represents a particular challenge of the function to avoid false positives while reliably detecting small objects close to the ground. Without this influence, it will be possible to set the ground filter threshold much smaller. As it was shown in Fig. 6-12, ground outliers appeared at a greater extent when the WMDS was in motion, potentially through the additional excitation by ground unevenness. It therefore is expectable, that the influence of motion on the ground filter is reduced when implementing the sensor set-up on the full scale WMDS, which has a suspension system and therefore will compensate the ground excitation to some extent. It is to reevaluate then, whether the RANSAC threshold can be set to a lower value.

Another further step that potentially helps to compensate the influence of unevenness is a finer segmentation of the ground within the RANSAC application to allow multiple smaller planes to be approximated. A radial separation of the current three segments in to be specified distances towards the WMDS is recommended. This will help to obtain a more precise approximation of the ground plane in the near field, which will reduce the number of outliers in this area where ground detections are least probable to be filtered by the threshold $d_{\mathrm{TH,merge}}$. Further possibilities for software adaptation in the future are to investigate approaches that do not filter out the ground, but recognise objects based on irregularities in the ground reflections, for example.

Since with the chosen parameters, the object detection functions without false positive or false negative triggers, the basic functionality is verified. The need for detection clustering is demonstrated, nevertheless, the detectability of small objects will thereby be reduced to smaller distances than required for the maximum speed limit. The safe detection of such critical objects under extreme conditions is investigated in Chapter 8.2. An evaluation of discrimination of atmospheric detections by light rain with this clustering approach was not possible since the WMDS prototype is not water proof, which has to be done in future work.

7. Fault Analysis and Fault Detection

The developed safety functions *LLLPS* and *Object Detection* are already designed to fulfill their intended task. In this process, value was placed on a design that is as resistant to errors as possible. Nevertheless, the functions may fail due to insufficient design or external influences. To evaluate their suitability as safety-related functions, the following sub-hypotheses of the main research hypothesis of this thesis are still to be investigated:

- RH1.2: The safety functions are able to perform their intended function under all conditions as specified within the ODD of the WMDS, while not disturbing the WMDS operation in situations uncritical to safety.
- RH1.3: The safety functions are intrinsically safe by detecting unsafe deviations from the target conditions causing failure of the functions.

RH1.2 is premised on the evidence that failure of the functions due to insufficient design and related to the intended use does not occur within the ODD of the WMDS. RH1.3 refers to the requirement that it can be identified by appropriate methods when undesired deviant conditions by means of external influence or internal hardware malfunctions exist that lead to failure. In this case, the functions shall transfer to a safe state.

An automated detection of fault states that prevent correct functionality is dealt with in this chapter. This is preceded by an analysis of failure cases and causes of the functions, which are then divided into faults that stem from insufficient design towards the ODD and faults due to deviant conditions that can be detected within a self-diagnosis. Possible fault indicators are derived and investigated towards suitable thresholds. This is introduced by a short insight into limitations of lidar sensing and known fault detection methods. Finally, the achievable diagnostic coverage is discussed at the end of the chapter. Furthermore, conditions for final validation tests as corner cases of the ODD are derived for the subsequent chapter.

7.1. Fundamentals on Lidar Sensor Faults and Fault Detection

Goelles et. al.[100] provide a systematic and profound literature review on sensor fault detection, isolation, identification and recovery (FDIIR) systems for automotive perception sensors, with a focus on lidar. In this context, the work provides classification schema for sensor faults and fault

[100] Goelles, T. et al.: FDIIR Methods for Automotive Perception Sensors (2020).

detection methods according to the state of the art. Thereby, faults occurring in the sensor data generation, leading to an insufficient quality of the sensor raw data to fulfill the target function, are considered. The fault classes refer to faults in terms of functional safety, as well as such faults caused by the environment, as thematized in SOTIF. The fault classification scheme shall help to identify sources of failure of both WMDS safety functions related to the lidar sensors. It summarizes the following fault classes:

- *Defect subcomponent:* defect internal parts of the sensor, e.g. transmitter or receiver
- *Mechanical damage to sensor cover:* e.g. scratches, cracks, missing or deformed cover
- *Layer on sensor cover:* e.g. dirt, water, ice
- *Mounting issue:* a change of the sensor's position or vibrations while driving
- *Unfavorable environmental conditions:* limitations of the FOV due to e.g. precipitation, fog, sunlight
- *Sensor crosstalk:* a sensor's detector accepts an echo of another sensor's emitter, leading to an erroneous point in the point cloud
- *Security attack:* e.g. denial of service, false data injection, electronics hack over a wired or wireless connection to the sensor

The first fault class - defect subcomponent - concerns the sensor function itself and therefore is a typical functional safety issue of electric equipment according to IEC 61508 or ISO 13849. The other faults rather are limitations due to influences of the environment while the sensor itself is functional, which refers to SOTIF.

Sensor crosstalk of the WMDS's lidar sensors can be excluded, as the sensors are distributed on the motion platform without directly targeting one another with the sensor beams. Nevertheless, other vehicles with lidar sensors operating in the environment of the WMDS workspace are possible sources of crosstalk effects. This is particularly conceivable on a vehicle dynamics field where several test vehicles operate. Nevertheless, this undesired error case is neglected in this work, since it would lead only to false positive detections in the object detection, but not to false negatives. For the LLLPS, interference is not expected due to the high overdetermination of the system. Security attacks are also not considered as relevant for the use case.

Defect subcomponents, mechanical damage or layers on the sensor cover, a misplaced sensor or unfavorable environmental conditions are considered relevant for the WMDS use case. Experiments with damaged lidar sensor covers reveal falsified range measurements.[101] Observed effects of layers on a lidar sensor cover, e.g. due to dirt or dew, are increased scatter in range measurements and falsified range measurements as well as creation of blind spots.[102] A misplaced

[101] Schlager, B. et al.: Effects of Lidar Sensor Cover Damages (2022).

[102] Schlager, B. et al.: Contaminations on Lidar Sensor Covers (2022).

sensor changes the field of view in relation to the vehicle and in a worst case leads to blind spots or a reduced range, if the sensor is e.g. pointed towards the ground. Unfavorable environmental conditions in the WMDS use case are especially (light) rain and deep sun light, as hail, fog and snow are excluded from a WMDS' ODD. In previous experiments, rain proved not to influence range measurements, but to attenuate the laser beams, leading to a reduced intensity of detections or even missing detections on objects, while rain drops itself can produce undesired lidar echos.[103] Sunlight affects the backscatter noise and creates potential false positive detections.[104] Concluding, the relevant fault classes can lead to a drop out of the whole sensing function, a limitation in the FOV or distorted range measurements.

Typical methods for FDIIR from disturbed sensor data according to Goelles et. al.[100], which shall be considered for a fault detection function of the WMDS sensor system, include:

- *Monitoring sensor output:* signal analysis and plausibility check of single sensor output
- *Comparison to sensor model:* e.g. objects detected by the sensor model compared to the real sensor
- *Comparison to static ground truth:* Infrastructure in the environment detected by the sensor compared to ground-truth infrastructure
- *Comparison to other sensor of same type*: compare detections of e.g. two lidar sensors
- *Comparison to other sensor of different type:* compare detections of two different sensor types, e.g. lidar and radar
- *Monitoring internal interfaces:* signal analysis and plausibility check of the output

7.2. Fault Case Identification

7.2.1. Fault Cases of the LLLPS Subfunction

Fig. 7-1 shows a fault tree analysis of the LLLPS subfunction. The fault cases are separated on two different layers. The first layer is the software layer (information processing) and shows at which steps in the sensor data processing a fault can occur. On this layer, failure occurs either through an insufficient number of detected landmarks, or an insufficient matching of the detected landmarks to the reference map, or a runtime error of the whole function. An insufficient landmark matching can be traced back to erroneous distance determination of the detected landmarks, or to a false positive landmark detection. While the first can occur due to insufficient data quality of the processed point cloud (e.g. due to a contaminated sensor cover), the latter occurs if objects in the

[103] Filgueira, A. et al.: Quantifying the influence of rain in LiDAR performance (2017).

[104] Linnhoff, C. et al.: Environmental Influence on Automotive Lidar Sensors (2022).

environment are erroneously determined as a landmark, e.g. because they have similar reflection properties and are within the landmark search radius.

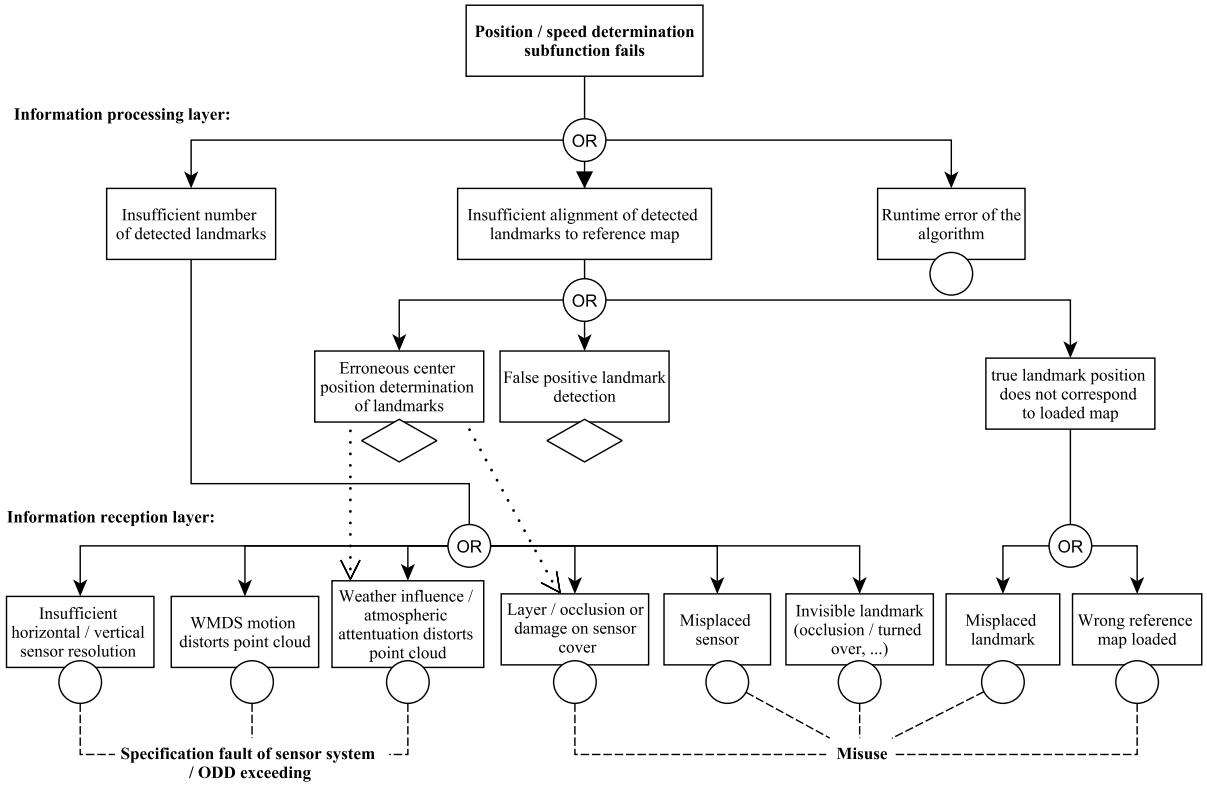


Figure 7-1.: Failure analysis of the LLLPS subfunction. The events on the information reception layer can apply to multiple failures in the information processing layer, but are only depicted once due to space limitations.

Root causes for the misdetection of a landmark are elaborated in the information reception layer. Here, the lidar sensor fault classes as provided by Goelles et. al.[100] are considered, among others. If a landmark is too small to be detectable at a given distance, a specification fault is present. In this case, the system has not been designed sufficiently for landmarks to be detectable at the required distance. If motion scan effects create disturbed point clouds that prevent a detection or create a false positive detection, this is also a specification fault because the system was not sufficiently adapted to the WMDS's own motion. The occurrence of such failures is to be avoided, which was targeted in the software development with the de-skewing approach. It either must be proven that the system has been correctly specified from the outset for all eventualities and is robust against such failures, or it must be identified from which conditions such failures occur and the ODD must be narrowed accordingly, until the specification is safe again. Weather influences such as light and precipitation are external influences that can lead to poor sensor data quality according to the fault classification described above. Here as well, the sensitivity of the system to such interfering factors as light or precipitation must be investigated. Especially if the WMDS is to be used within light rain, it has to be investigated, whether within (or up to which strength of) rain the lidar-based functions are still working properly. These potential sources of failure referenced to the ODD are investigated in Chapter 8.

Further fault cases are referenced to misuse. These are a layer on the sensor cover or a damage of the sensor, as well as a misplaced sensor. All of these failures can lead to a limited field of view of the sensor that can impede the landmark detection. These failure cases are classified as a misuse by the operator, who has to make sure that only correctly positioned, sufficiently clean and damage-free sensors are used. Also, the intentional occlusion of a sensor is considerable as such a misuse. Further misuse related faults are a pour landmark visibility, misplaced landmarks or a faulty reference map. As these failure cases are undesired deviant conditions from regular operation conditions, a diagnosis is intended to detect such deviations to impede the operation.

The FTA does not show the fault case of a hardware drop out of a sensor or processing unit, which would lead to no arriving data packages and therefore no possible information processing. Such an abnormal condition is to be detected as well.

7.2.2. Fault Cases of the Object Detection Subfunction

Fig. 7-2 shows a fault tree elaborated for the failure of detecting a present object within the PZ. The failure cases in the information processing layer include that an object is discriminated either within the line run clustering, if the minimum cluster size condition is not fulfilled, or within the temporal check, or by erroneously assigning the object detections to the ground. Additionally, an erroneous distance measurement beyond deviations considered in the PZ design can cause an object to be attributed outside the PZ. A general runtime error of the algorithm can also lead to a failure of the object detection.

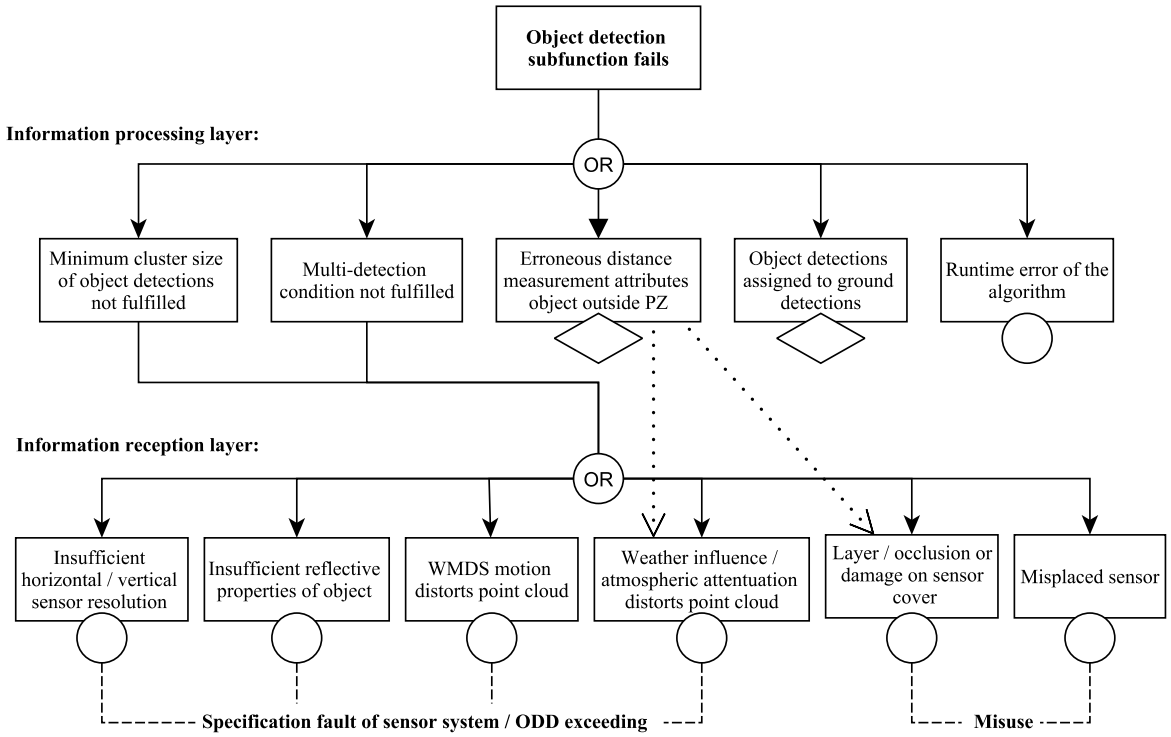


Figure 7-2.: Fault tree analysis of the object detection subfunction.

Root causes in the information reception layer are exemplary shown for the case of an insufficient number of detections on an object, but they partly also apply to an insufficient number of time steps or erroneous distance measurements in the processing level. These are mostly equivalent to the root causes identified for the failure of the LLLPS subfunction. These include specification faults like insufficient sensor resolution to detect the object, insufficient reflection properties of the object, motion scan effects that disturb the point cloud, and external weather influences such as light rain or low sun light. The robustness of the function within corner cases of the ODD representing such failure prone conditions is to be investigated in the final function validation. Further failure cases in terms of misuse describe an occluded or damaged sensor cover as well as a misplaced sensor, which is intended to be automatically detectable to impede the operation of the WMDS and transfer to a safe state.

7.3. Fault Detection Concept

In general, different levels of fault detection are considerable. If this is performed at the information processing level, a direct identification of a function's failure must be possible. If this is not available, a diagnosis in the information reception layer must detect insufficient conditions within the incoming sensor data, presuming that the function will fail under these conditions.

In the following, it is assessed whether the aforementioned fault conditions are detectable. To ensure that the WMDS is only operated when a fault-free state is present, an *initial system check* is intended for both safety functions as a release condition for the WMDS operation. This can be integrated into the *run release check*, as presented in the WMDS state chart in Fig. 3-1. The check shall comprise a reproducible maneuver for a defined period of time. Within this initial check, fault indicators (FI) are compared towards designated thresholds $FI_{i,\mathrm{TH,ini}}$. It should only be possible to switch to a motion mode and release the drive system, if these tests are passed.

Furthermore, it should be possible to detect sudden faults during operation in an *continuous system check* and trigger a fault detection, which then interrupts operation by emergency braking. Therefore, the FI are compared to designated thresholds $FI_{i,\mathrm{TH,op}}$. To ensure that this is effective, the time intervals at which such a detection during operation can be carried out is decisive. This is investigated in the following.

First, possible fault indicators are identified. Then threshold values are derived for each fault indicator, both for the initial check and for the continuous check during operation. There are basically two methods conceivable for identifying suitable thresholds: Either, regular values of the fault indicators under fault-free conditions are examined and thus the threshold is chosen slightly above or below them. This then indicates an undesired deviation from the regular system state. For this, representative data is required that represents all conditions that can occur in the regular state. However, this deviation may not yet be dangerous for the safety of a function, which

can lead to unnecessary interventions. On the other hand, this creates a safety buffer. The second option is to determine conditions under which the safety of the function is actually in danger and then extrapolate them back to the fault indicators. However, this requires precise knowledge of the relationships between a fault and its impact on the function's safety. In the following, both variants are considered depending on the specific fault indicator. However, the selected threshold values are only to be considered as examples and need to be further verified or adapted in the future, when a larger set of representative data is available. Nevertheless, the procedure presented here can be adopted for this.

7.3.1. LLLPS Fault Detection

For the present use case, the variants *monitoring sensor output*, *comparison to static ground truth* and *comparison to other sensor of same/different type*, as proposed by Goelles et. al.[105], are generally conceivable. Nevertheless, as it is intended to keep the system complexity low, it rather is aimed to apply a fault detection without the addition of further measurement devices.

In the LLLPS, a *static ground truth* as a reference is available at the information processing level, in the form of an expected number of detected landmarks and quality of the matching algorithm. Under the presumption that erroneous position and speed measurement data are preannounced in the matching process, a fault detection of the LLLPS is considerable by the following failure indicators:

- *Number of matched landmarks:* if less than 8 landmark clusters are matched, either less clusters were detected, or the position estimation of a cluster centroid was faulty, the loaded map was faulty, or the landmark position was shifted. If one of the matched clusters is a false positive, this is not diagnosed. The number of matched landmarks can be further compared to a number of detected landmark clusters, which would allow to differentiate between a non detected landmark and a non-matched landmark.
- *Mean residual of the matching process:* In the matching process, residuals remain between the centers of matched landmarks from the reference map and the current detections. From this, an average distance residual can be calculated for the amount of matched landmarks. Significant measurement errors of the WMDS position are expected to be announced in exceptionally large residuals. If the mean residual is outside of an ordinary value, but a sufficient number of landmarks have been matched, it is expected that the quality of the data will be insufficient to achieve the desired positioning quality. This happens if the sensor data quality is not sufficient to localize the detected landmarks correctly, the landmarks have been shifted, a faulty reference map was generated or false positive landmarks are matched.

[105] Goelles, T. et al.: FDIIR Methods for Automotive Perception Sensors (2020).

Besides the named indicators, it is further required to observe the run time of the algorithm for delays to ensure that at least after the regular cycle time, a novel position and speed output is available. Furthermore, it is required to check that lidar data packets are received within the scan cycle time and that they have the regular package size without losses. Both is not further targeted here. With these indicators, all fault cases shown in the FTA are theoretically covered. Accordingly, insufficient lidar raw data quality, like a partly occluded sensor, do not necessarily have to be detected at the raw data level for the LLLPS to obtain a high coverage of possible faults. As long as the number of detected landmarks and the matching process itself do not show any loss of quality, there is no need to switch to a fault state. A threshold for the minimum number of landmarks to be matched before the system diagnoses a fault is required. In addition, a maximum tolerable mean residual of distances between matched landmarks is to be set, above which the system triggers a fault condition. This prevents positions and speeds with unacceptable deviations from the ground truth from being returned by the system. The concept and potential thresholds are explained in the following.

Minimum Number of Matched Landmarks

The minimum number of matched landmarks, denoted as n_{LM}, is predictable for a specific workspace size. Within the currently considered workspace with a radius of $25\,\mathrm{m}$, 8 landmarks shall be matched from every workspace position. Even though a lower number of matched landmarks would still enable to maintain the regular positioning quality, less than 8 matched landmarks would indicate a deviating condition from the regular and therefore a present fault. At larger workspaces, it is initially to determine which minimum number of matched landmarks regularly occurs from the most critical workspace positions, i.e. border positions. A prerequisite is, that it has been verified that this minimum number is still sufficient to obtain the desired measurement quality. Then it is considerable to perform the initial check within the workspace center, where the threshold $n_{\mathrm{LM,TH,ini}}$ must be set to 8[106], but to define a lower threshold for the ongoing operation ($n_{\mathrm{LM,TH,op}}$). Within the initial check, at least one full rotation of the WMDS around its center is to be performed. This is required since a partial blind spot of a sensor is possibly not detected during standstill, if a landmark within the blind spot is detected by another sensor at the same time.

Observing the number of matched landmarks during the representative dynamic drive (cf. Fig. 6-8), it is found that usually 8, but occasionally only 7 landmarks are matched, while single losses occur only for individual time steps (cf. Fig. E-1 in Annex E). The losses can be attributed to the fact that the WMDS was shortly maneuvered over the workspace border, so that one landmark was obscured by another. This is not expected to occur during regular operation. Nevertheless, to increase the availability of the system and tolerate single short time losses, it is considerable to define two operational thresholds: $n_{\mathrm{LM,TH,op,low}}$ shall trigger a fault condition immediately in the

[106] Within a tolerable maximum workspace size, all 8 landmarks are still required to be detectable from the center to perform the initial map creation.

first timestep, in which it is undercut. $n_{\mathrm{LM,TH,high}}$ shall only trigger a fault condition, if it persists for a predifined number of subsequent cycles (n_{cyc}), e.g. for 3. Respectively, a lower threshold is chosen for $n_{\mathrm{LM,TH,op,low}}$. For the currently used workspace size, $n_{\mathrm{LM,TH,op,low}}$ is set to 7 and $n_{\mathrm{LM,TH,op,high}}$ as well as $n_{\mathrm{LM,TH,ini}}$ are set to 8.

The fault detection function triggers a fault condition within the initial check (full rotation) if the following condition is fulfilled:

$$n_{\mathrm{LM}} < n_{\mathrm{LM,TH,ini}} = 8 \tag{7-1}$$

The fault detection function triggers a fault condition during ongoing operation if any of the following conditions is fulfilled:

$$\begin{aligned} n_{\mathrm{LM}} &< n_{\mathrm{LM,TH,op,high}} = 8 \quad \text{for} \quad n_{\mathrm{cyc}} = 3 \quad \text{or} \\ n_{\mathrm{LM}} &< n_{\mathrm{LM,TH,op,low}} = 7 \quad \text{for} \quad n_{\mathrm{cyc}} = 1 \end{aligned} \tag{7-2}$$

Maximum Mean Matching Residual

The previous diagnosis did not include measurement faults due to false landmark matching, faulty position measurements of true landmarks, shifted landmarks within the search radius or a faulty reference map. These cases will not be indicated by a reduced number of matched landmarks, but nevertheless can decrease the positioning quality. For these cases, a termination of the operation triggered by an exceeded threshold for a tolerable mean matching residual is investigated in the following. The mean matching residual thereby is obtained as follows:

Within the regular matching process, the fitness score is used as a matching quality indicator and a termination criterion of the matching iterations. It is build from the sum of remaining residuals between matched landmarks, but is ”penalized” with the maximum search radius $\xi_{\max}$ for each unmatched landmark to prevent a small number of matched landmarks from leading to a termination in the matching process (cf. Chapter 6.1.4). Since single losses of landmarks are still tolerable for a high quality position value, as derived above, for the failure diagnosis the search radius penalty $\xi_{\max}$ is substracted from the fitness score for each loss of landmarks $n_{\mathrm{LM,loss}}$ and the obtained value is averaged towards the number of matched landmarks $n_{\mathrm{LM,match}}$ within the current cycle, avoiding to obtain a small matching residual and therefore an indication of higher quality for measurements where landmarks are lost. This delivers the arithmetic mean value of the distances between individually matched landmarks $\overline{d}_{\mathrm{LM}}$:

$$\overline{d}_{\mathrm{LM}} = (s_{\mathrm{fit}} - n_{\mathrm{LM,loss}} \cdot \xi_{\max}) / n_{\mathrm{LM,match}} \tag{7-3}$$

Theoretically, the matching residual can take on a maximum value of $1\,\mathrm{m}$, which corresponds to the search radius in the matching process and is reached if all matched landmarks have that maximum distance towards the reference map. In a fault free system, meaning all 8 landmarks are correctly matched, it is expected that the occurring matching residuals vary in dependence of

the quality of the detected landmark center estimation, which can depend on the distance of the WMDS towards landmarks. As described in Fig. 6-6, the distance towards landmarks influences the landmark detection characteristics due to the reflection behaviour of the retroreflective foil and therefore can lead to a more or less accurate estimation of the landmark center.

Fig. 7-3 shows the data of averaged matching residuals ($\bar{d}_{\mathrm{LM}}$) and positioning deviation between DGPS and LLLPS ($\Delta p_{\mathrm{LLLPS,GPS}}$) over time for a constant circle drive of the WMDS at a non concentric workspace position. In total, 3 circles are driven. The trajectory is shown in Fig. 7-3 in Annex E. The position data of both measurement systems as well as the matching residual are filtered with a moving mean filter and a window size of 3 to reduce data noise and increase the visibility of the course of data in the plot. The non-concentric workspace position has the effect that the minimum distance of the WMDS towards landmarks oscillates with the circular movement. This finally causes the matching residuals to increase and decrease in a sinus-shape with different amplitudes. The figure shows temporally correlating maxima of the position deviation between LLLPS and DGPS signal towards the maxima of the matching residuals. The same effect is to expect, when the residuals rise due to shifted landmarks, a faulty reference map or false positive matched landmarks.

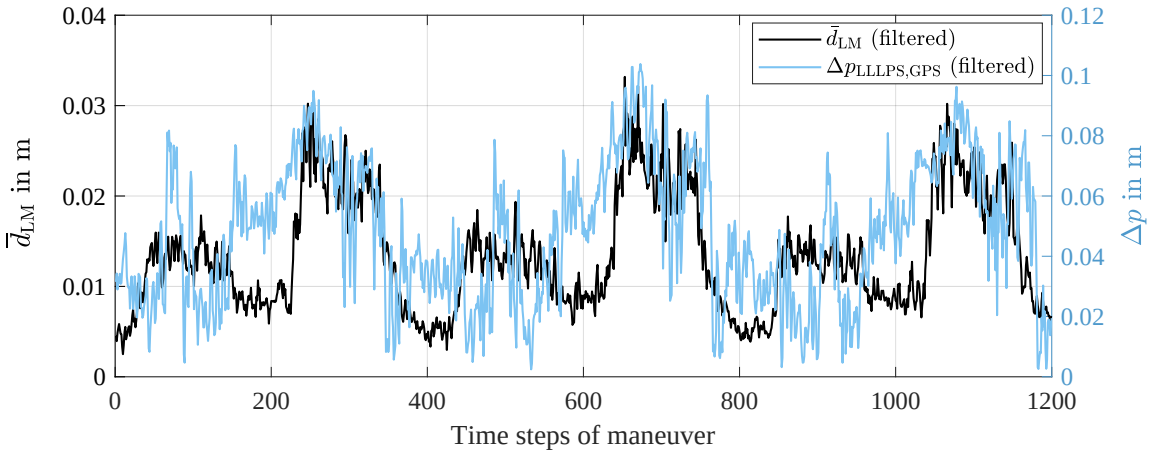


Figure 7-3.: Positioning quality and averaged matching residuals in a non-concentric circle drive. Due to increasing and decreasing minimum distances towards landmarks during the drive, the landmark detection data quality and therefore the matching residuals vary in a sinus-shaped course with varying amplitudes.

The maximum mean matching residual is expected to occur when the WMDS moves at the workspace border, the minimum is expected to occur while the WMDS is positioned in the workspace center. To identify suitable thresholds for the initial an the continuous check, the regularly occurring matching residuals under acceptable positioning deviations are further investigated. Therefore, a standstill at the workspace center as well as the representative dynamic drive are both considered.

In Fig. 7-4, the mean matching residual are shown for a centered standstill, the aforementioned circle drive and the representative dynamic drive are illustrated as an ECDF plot. In all data sets, the maximum position deviation towards the DGPS reference system remains below $0.3\,\mathrm{m}$ for

unfiltered data. During the standstill, $\overline{d}_{\mathrm{LM}}$ has an average value of $0.007\,\mathrm{m}$. The dynamic drive is the representative maneuver of a driving simulation as shown in Fig. 6-8. In this maneuver, the position of the WMDS in the workspace changes continuously and even shortly exceeds the regular border, resulting in a higher spread of the mean matching residuals compared to the circle drive. While the 99 % quantile is at $0.03\,\mathrm{m}$, the maximum value is $0.06\,\mathrm{m}$. Individual peaks are caused by very small distances to the landmarks for short fractions of time, which are actually smaller than expected in regular operation. It is therefore expected that the maximum residuals occurring in this data set are worst case values occurring in a fault-free system that determines the WMDS position with an acceptable accuracy.

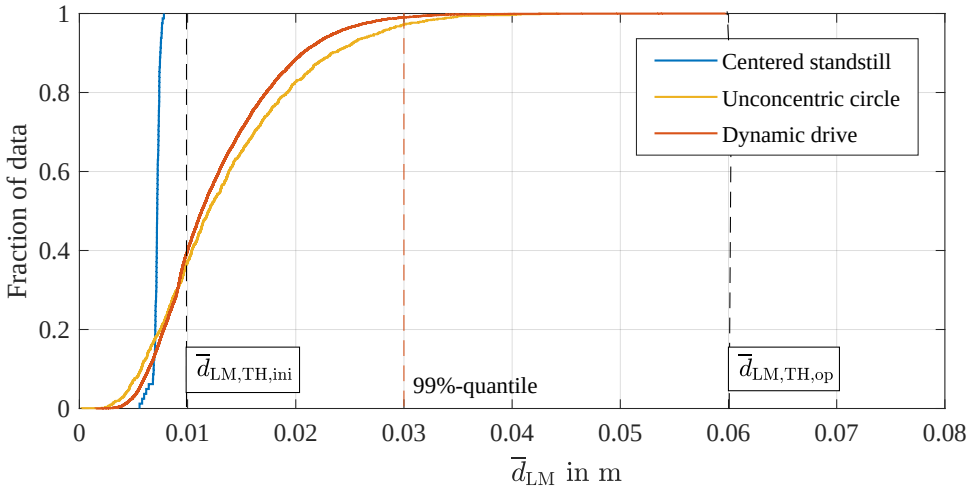


Figure 7-4.: ECDF plots of the average matching residuals in various maneuevers.

On the basis of these observations, the threshold for the initial check, $\overline{d}_{\mathrm{LM,TH,ini}}$ is set to $0.01\,\mathrm{m}$ to obtain a small buffer to the determined value in Fig. 7-4. The check can be conducted while the WMDS performs the full rotation in the workspace center, as prescribed for the landmark check. In the future, it is to further assess whether $\overline{d}_{\mathrm{LM}}$ in the center workspace position is sufficiently reproducible and below the proposed threshold. The threshold for the ongoing operation, $\overline{d}_{\mathrm{LM,TH,op}}$, is set to $0.06\,\mathrm{m}$, since the obtained values are already expected to represent an extreme corner case.

The fault detection function triggers a fault condition within the initial check (full rotation) if the following condition is fulfilled:

$$\overline{d}_{\mathrm{LM}} > \overline{d}_{\mathrm{LM,TH,ini}} = 0.01\mathrm{m} \tag{7-4}$$

The fault detection function triggers a fault condition during ongoing operation if any of the following conditions is fulfilled:

$$\overline{d}_{\mathrm{LM}} > \overline{d}_{\mathrm{LM,TH,op}} = 0.06\mathrm{m} \tag{7-5}$$

In order to determine actually occurring maximum values during operation more reliably in the

future, a circular drive with the radius of the motion space R_{MS} is recommended. This would lead to minimum possible distances between WMDS and landmarks and thereby to the strongest possible disruption of the landmark detections. Further investigations of the retroreflective effect in dependence of the distance towards a landmark and a possible distance dependent radial offset for the landmark center detection could decrease the matching residuals under regular conditions. Then a smaller threshold can be chosen.

7.3.2. Object Detection Fault Detection

For the object detection function, sensor occlusion and a misplaced sensor is to be detected, besides regular run time errors and incomplete incoming data packets of the lidar sensors. For the LLLPS, the advantage was that the landmarks could be used as a reference, and thus no diagnosis had to be done at the raw data level to detect a fault condition. Unfortunately, it is not sufficient to transfer these fault indicators to the object detection function, since they do not cover the entire relevant FOV, especially not the lower sensor levels, which already hit the ground at close range. Therefore, another *static ground truth* is required for the object detection subfunction.

Since the lower sensor layers with a negative elevation angle shall always receive detections from the ground under normal functionality, the ground detections can generally be considered a static ground truth. The idea is that if the sensors are not able to detect the ground properly due to any of the stated fault cases, an object detection within this range is endangered as well. This leads to a fault detection from the following characteristics:

- *The number of detections:* 20 of the 32 sensor layers have a negative elevation angle and therefore point towards the ground. The number of detections that shall appear in this FOV is predictable. If less points are obtained than usual, either the sensor FOV is impeded by occlusion or damage of the sensor cover, or a defect sensor hardware is present. Otherwise, a total reflection or other disturbances might have occurred.
- *The measured range towards the ground:* If detections do not match the expected range to the ground, a mounting issue / misplaced sensor is present.

In the following, it is assessed whether, and under which constraints, these indicators are suitable fault indicators. Furthermore, thresholds are exemplary defined based on existing representative data.

Number of Ground Detections

The expected number of ground detections for each sensor layer are determined by the sensor discretization in azimuth. With the implemented discretization of 1024 and a 180° limited FOV, 512 detections shall theoretically appear per sensor layer that is directed towards the ground. This concerns the sensor layers with ID31 to ID12. Nevertheless, it is to be expected that disturbing

effects occur which lead to deviations of this number even if the sensor is not occluded. Therefore, it is to be identified:

1. In which layers a robust number of ground detections can generally be obtained.
2. How much this regularly deviates from the expected number under normal conditions.
3. How a fault condition can be distinguished from these regular conditions.

A missing detection within a segment is reflected in the point attribute *range*, which takes the value 0 if no detection is present. This can be, on the one hand, because no reflection of the emitted beam was obtained, so the measured range is infinite. Another reason can be that the measured distance is smaller than the minimum measurement distance of $0.25\,\mathrm{m}$ (cf. Tab. 5-1). In the sensor layers considered for the fault detection, the lidar beams shall neither reach in the infinite, nor be reflected in a smaller distance than $0.25\,\mathrm{m}$. Then a range value $r_{ij} = 0$ for a segment i within a layer j is set as a criterion for a lost detection.

When examining the regularly occurring ground detection losses per sensor layer on the basis of the representative dynamic drive, a limitation of the concept becomes apparent: In Fig. 7-5 it is shown that gaps in the ground detection rings appear in the alignment of a landmark towards the sensor. It is assumable, that a kind of overexposure occurs in the sensor receiver units through the highly reflecting landmarks. As this will lift the noise level by ambient light, the reflections from the ground are no longer prevailing. Since the extent and duration of such a disturbance is dependent on the actual WMDS trajectory, the ground detections become unpredictable and therefore an unreliable fault indicator within the WMDS operation, if not a larger space towards the landmarks can be ensured. Since a larger distance towards the landmarks would mean an increased space requirement, this is undesirable. In the future, less reflective types of landmark sheeting that do not cause such interference should be assessed. Otherwise, the operational fault detection can only be active for an additional position constraint, e.g. when the WMDS crosses the workspace center.

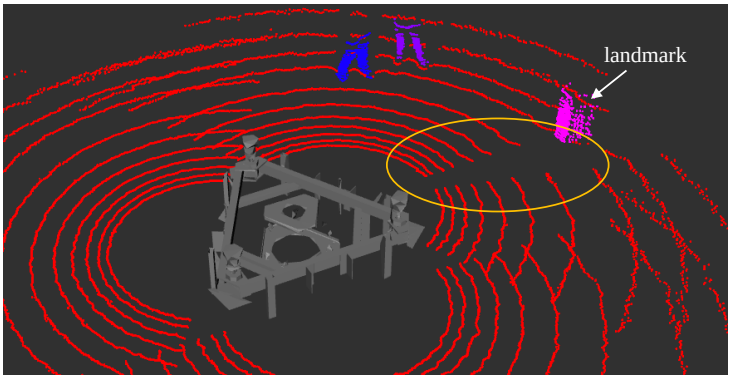


Figure 7-5.: Lost ground detections in the alignment towards a landmark (yellow circle), appearing during the representative dynamic drive. The other detected clusters are the legs of two humans.

To hide the influence of the landmarks, only maneuvers in which the WMDS moves in or through the workspace center are further considered. In Fig. 7-6, the mean number of segments with a range measurement of 0 (n_{r0}) are shown per layer ID within a slow translation[107] ($v_{\mathrm{DS}} < 1\,\mathrm{m/s}$) and a fast rotation ($\dot{\psi}_{\mathrm{DS}} = 259\,°/\mathrm{s}$). The error bars indicate the standard deviation throughout the maneuver. From layer ID12 onward, the laser beams have a negative elevation angle. Layer

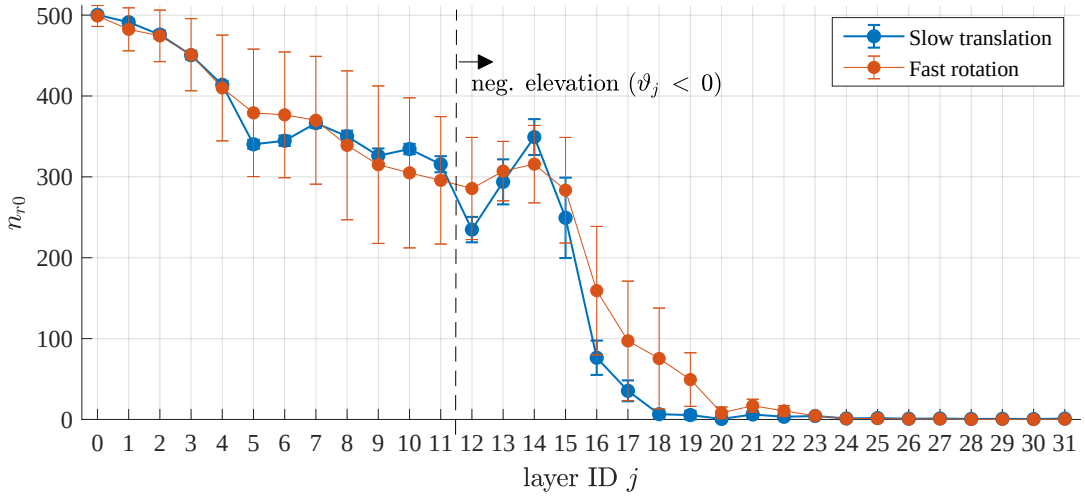


Figure 7-6.: Mean number of segments with $r_{ij} = 0$ (n_{r0}) per layer ID for a slow translation and a fast rotation maneuver. Layers with ID12-31 have a negative elevation angle and therefore point towards the ground.

ID13 shall theoretically reach the ground within a radius of 25 m (cf. Fig. 5-4). Nevertheless, the elevation angles of the layer IDs 12-21 deviate less than 3° from the horizontal line[108]. Within the slow translation, layer ID18 and ID19 still show a low number of detection losses, nevertheless, during the fast rotation, a strong increase in the mean value and the standard deviation is visible from layer ID19 onward. From this it is to conclude, that no more than the layers from ID20 to ID31, i.e. the lowest 12 sensor layers, are considerable as a reference for the ground detection diagnosis when the WMDS is in the workspace center, as other layers will show regular fluctuations in detection losses that will mask a potential sensor occlusion. Layer with ID12 hits the ground at a distance of approximately 8 m. This means only half of the maximum PZ radius is covered by the diagnosis. Due to the slope on the workspace, the number of layers directed towards the ground will be further decreased at different workspace locations. From the illustration of the vertical sensor FOV with an inclination of 2° (cf. Fig. B-1), it can be estimated that only layers with ID31-24 will deliver continuous ground detections throughout all segments.

For the considerable lidar layers, thresholds for a fault indication are required. To fulfill the minimum cluster size even with objects of minimum size, theoretically not a single segment of the sensor shall be blocked with the given sensor resolution. However, it is observed that fluctuating losses of ground detections at a small scale occur in every layer. These can be explained by total reflections or internal sensor effects. With that, it is clear that a single lost ground detection

[107] This is chosen instead of standstill, since in standstill a steady total reflection of single segments can occur.

[108] The detailed beam spacing of the sensor is given in Fig. B-2 in Annex B.

is not a suitable fault criterion, as this appears frequently. A large scale occlusion of a sensor would be characterized by the number of losses being significantly greater than under regular conditions. However, a small scale occlusion requires a further distinguishing criterion. Therefore, not only the *absolute number of losses* is observed, but also the *loss consistency*. To achieve this, the so-called *loss counter (LC)* is introduced. The loss counter LC_{ij} counts for each individual segment $i = 256...768$[109] per sensor layer ID $j = 20...31$, whether the point attribute *range* r_{ij} is equal to 0 in the current time step. If this is the case, LC_{ij} is added with 1. For each further time step in which the same segment measures a range of 0, LC_{ij} is further incremented with 1, otherwise it is reset to 0:

$$LC_{ij}(t) = \begin{cases} LC_{ij}(t-1) + 1 & \text{for } r_{ij}(t) = 0 \\ 0 & \text{else} \end{cases} \tag{7-6}$$

The diagnosis shall then check whether a predefined threshold LC_{TH} is exceeded. This can be indicated for a single blocked segment. A further possibility is to link the LC threshold with a threshold for the number of segments $n_{r0,LC,TH}$ to which the respective LC_{TH} applies. The fault detection interval then is determined by the regular amount of successive time steps in which the losses remain consistent for the set amount of segments. Setting multiple thresholds allows larger occlusions to trigger within smaller fault detection intervals than it would be possible for small scale occlusions. Since the fault detection interval during an ongoing operation is required to be added to the reaction time $\tau_{\mathrm{react,sp}}$, a short fault detection interval is desirable.

To exploit the feasibility of this concept, regularly occurring losses are examined for selected maneuvers, shown in Fig. 7-7. Therefore, data sets of a slow translation close to standstill ($v_{\mathrm{DS}} < 1$ m/s), an accelerated translation ($v_{\mathrm{DS}} = 2...6$ m/s), and the fast rotation ($\dot{\psi}_{\mathrm{DS}} = 259$ °/s) are considered. Within all maneuvers, the WMDS moves in or through the center of the workspace and no objects are present within the observed layers, so that detections only stem from the ground.

The first plot (left) shows the maximum occurring $LC_{j,\max}$ per sensor layer throughout the maneuvers. For the fast rotation and the slow translation, an increase towards the lower layer IDs is observed, while $LC_{\max}$ remains below 10. In the slow translation, the distribution is almost equal throughout all layers and $LC_{\max}$ remains below 4. Concluding, with the obtained data, $LC_{\mathrm{TH,ini}}$ must be set above 3 and $LC_{\mathrm{TH,op}}$ must be set above 9. This means the time interval to detect a single blocked segment is at least 10 time steps during operation, which equals 0.5 s. In between, an occlusion affecting a single segment remains undetected.

The second plot shows the maximum number of segments i per layer j with $r_{ij} = 0$ ($n_{j,\mathrm{r0}}$) occurring within one time step of the maneuvers. The number of losses remains at a maneuver specific level until layer ID24, but then strongly rises. Nevertheless, the maxima appear not in layer ID20 but in layer ID21 for all maneuvers. These remain below 21 lost detections for the slow translation, and rise to up to 75 lost detections within layer ID21 in the fast translation maneuver.

[109] These are the segment numbers in the horizontally limited FOV of 180°.

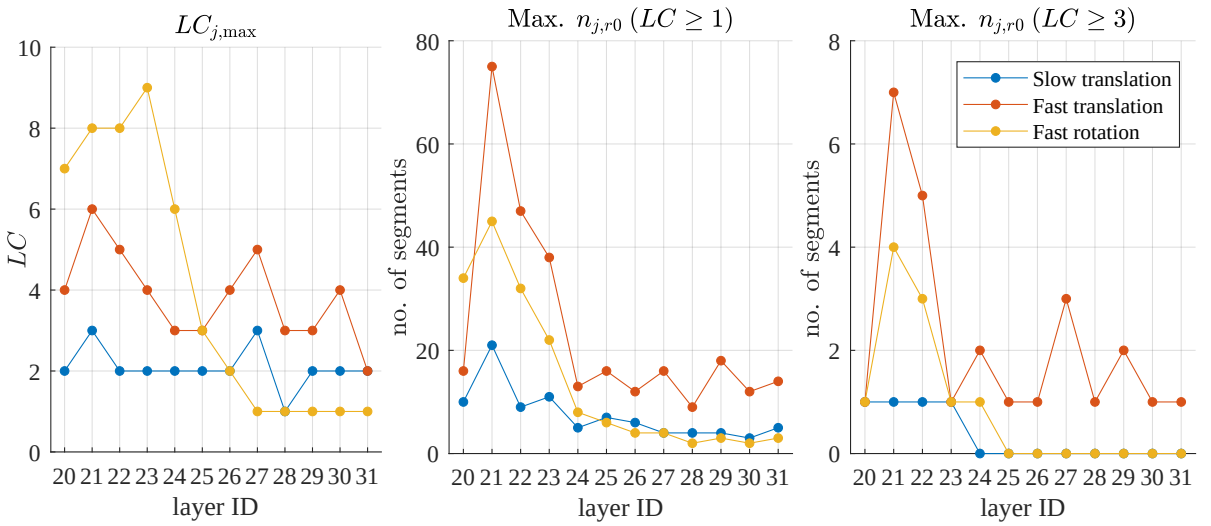


Figure 7-7.: Examination of $LC_{j,\max}$ and $n_{j,\mathrm{r0}}$ per sensor layer for three different maneuvers.

Concluding, thresholds for the absolute number of losses $n_{\mathrm{r0,TH}}$ are recommended to be set layer specific with lower thresholds for ID31 to ID24 and higher thresholds for ID23 to ID20. With the obtained data, $n_{\mathrm{r0,TH,ini}}$ must be set above 7 and $n_{\mathrm{TH,r0,op}}$ above 19 for ID31-ID24. For layers with ID23 to ID20, $n_{\mathrm{TH,r0,ini}}$ must be set above 21 and $n_{\mathrm{TH,r0,op}}$ above 75. This defines the scale of occlusions that can be detected after one timestep ($LC \geq 1$).

The third plot shows the maximum $n_{j,\mathrm{r0}}$ that have a $LC_{\max} \geq 3$. No segment within the slow translation, only 1 segment within the fast rotation and 1-3 segments within the fast translation appear to lose its detection for more than 2 time steps within layers ID31 to ID24. Within layers ID23 to ID20, the maximum is 7 segments for the fast translation. It is observable that the number of detections lost consistently over 3 time steps ($LC \geq 3$) is approximately an order of magnitude lower than the absolute losses occurring per time step ($LC \geq 1$). Thus, a threshold is recommended, which indicates smaller scale occlusions over multiple segments within a time interval of e.g. 3 timesteps. Respectively, the diagnosis triggers only if $n_{j,\mathrm{r0}}$ for which applies $LC_{j,\max} \geq 3$ is greater than $n_{j,\mathrm{r0,3,TH}}$. This threshold can also be set layer specific. With the observed data, $n_{j,\mathrm{r0,3,TH}}$ must be set above 3 for layers ID31 to ID24 and above 7 for ID23 to ID20. The advantage compared to the maximum LC observation for single segments is that the fault detection time interval is reduced to only 3 timesteps. Since a reduction of the time interval is not important in the initial check, this threshold is only advantageous for the ongoing operation.

The proposed thresholds serve only as an demonstration of the concept and are to be calibrated more accurately in the future when a larger amount of data is available. Furthermore, it is possible to define several LC level specific thresholds. The concept cannot be executed at standstill, since total reflections possibly then occur consistently. Consequently, the initial check shall be conducted within a slow rotational maneuver and the operational fault detection should only be triggered when an additional speed threshold is exceeded. The overall loss detection concept

summarizes as follows. In the initial check, a fault condition is present, if:

$$\begin{aligned} n_{j,\mathrm{r0}} &> n_{j,\mathrm{r0,TH,ini}} \quad or \\ LC_{ij} &> LC_{j,\mathrm{TH,ini}} \end{aligned} \tag{7-7}$$

In the operational check, a fault condition is present, if:

$$\left.\begin{aligned} n_{j,\mathrm{r0}} &> n_{j,\mathrm{r0,TH,op}} \quad \text{or} \\ n_{j,\mathrm{r0}}(LC_{ij} \geq 3) &> n_{j,\mathrm{r0,3,TH}} \quad \text{or} \\ LC_{ij} &> LC_{j,\mathrm{TH,op}} \end{aligned}\right\} \text{and } v_{\mathrm{DS}} > 0 \tag{7-8}$$

To demonstrate the concept, one sensor is partly covered with adhesive tape, another sensor is covered with a dust film[110] and the third sensor is kept normal. While the WMDS is at standstill, $LC_{\max}$ over time as well as $n_{j,\mathrm{r0}}(LC_{ij} \geq 3)$ are observed, shown in Fig. 7-8. For the clean sensor, $LC_{\max}$ varies between 1 and 2. For the concealed sensors, as expected, $LC_{\max}$ increases linearly with time, which means there is at least one segment per sensor that is consistently blocked. The amount of segments $n_{j,\mathrm{r0}}(LC_{ij} \geq 3)$ exceeds previously suggested thresholds within all layers for the taped sensor. For the dusty sensor, only from layer ID24 onward, but therefore more significantly. A possible explanation is that despite the dust film, the lower sensor layers still receive the strongest return from the ground due to its closer proximity, while at the higher layers, the ground detection intensity is not strong enough.

It follows that the sensor occlusion performed would be detected by the fault detection function in both cases. Although the occlusions affected a large FOV of the sensor, the LC observation would still strike through even if there is only a single blocked segment. The detectablity of

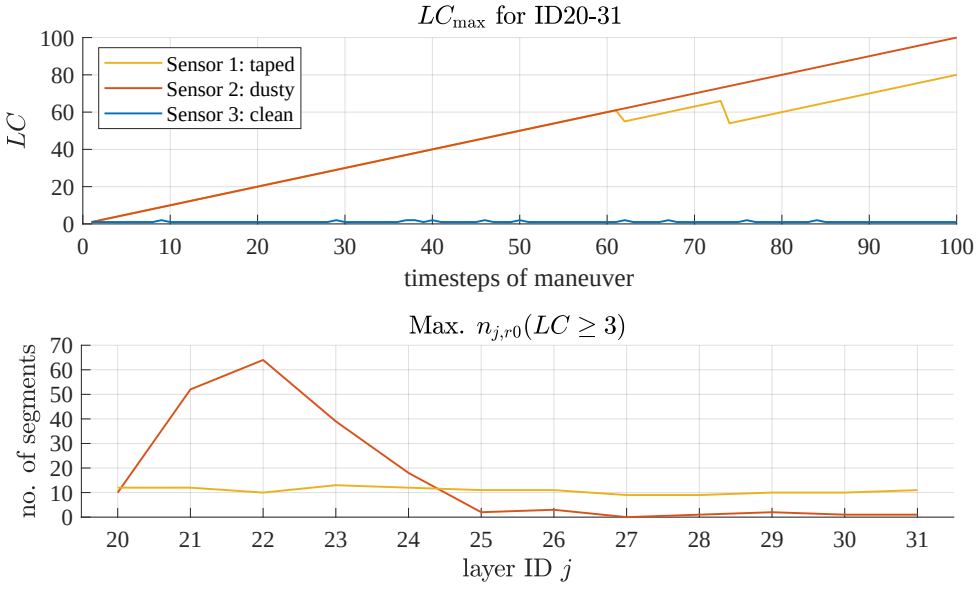


Figure 7-8.: Maximum LC per sensor for a clean and occluded sensors. All data is recorded during standstill.

[110] Pictures of the sensor housings with these modifications are shown in Fig. E-3 in Annex E.

large scale occlusions is generally considered high with this concept. Future work should further investigate how small, punctual occlusions affect the overall number of lost segments. A remaining limitation of the concept is that small-scale occlusions affecting only the layers above ID12 are not detected. However, the higher the occluded layer, the less critical this is for reliable object detection, provided that the objects are still detected by at least 2 layers below the occluded layer. Nevertheless, an unmonitored FOV remains in the area between ID19 and ID12, which in particular must not fail for the detection of small objects at a greater distance.

During an ongoing operation, the occurring detection losses can be influenced by the local position of the WMDS, respectively the prevailing ground unevenness. The previously observed maneuvers were executed in the center of the workspace. However, when the WMDS moves along the workspace borders, it is no longer guaranteed that the ground conditions are sufficient to obtain detections within all considered layers. As a conclusion, the monitoring of ground detections during operation is accompanied by additional limitations that make continuous diagnostics difficult. Furthermore, the time interval until a blocked segment is detected as such increases the required PZ size.

In order to completely cover the entire sensor FOV for an occlusion check, it would be conceivable to set up vertical elements in front of each sensor during the initial check. The height of the test objects must be large enough to be hit by all sensor layers at the respective distance. Either the test object is large enough in width to cover all segments at the same time, or it is observed during rotation whether each segment on each layer provides a detection when passing the test object. This would at least ensure that the WMDS does not start if there is a FOV limitation.

Another conclusion from the investigations of the ground detections and their losses is that missing detections occur consistently and are thus a potential thread for reliable object detection. The chosen cluster size of 2x2 detections does not allow for a single detection loss. If as many losses occur with vertically raised objects as observed for the ground detections, the number of detections on objects of minimum size must be increased, either by a higher resolution sensor or by reduced maximum detection distances, e.g. through a further limitation of the WMDS speed.

Range of Ground Detections

Considering an ideal even ground surface as well as an ideally oriented sensor, the expected range of a ground detection is predictable by the ground truth mounting height of the sensor h_s, and the nominal elevation angle of the sensor layer $\vartheta_{j,\mathrm{nom}}$. The nominal range of all segments i for a sensor layer j ($r_{ij,\mathrm{nom}}$) shall be equal throughout all segments and measure as follows:

$$r_{ij,\mathrm{nom}} = -\frac{h_\mathrm{s}}{\sin(\vartheta_{j,\mathrm{nom}})} \tag{7-9}$$

In reality, the measured ranges $r_{ij,\mathrm{m}}$ to the ground deviate from its nominal value in dependence of elevations or subsidence on the current workspace position, temporal effects of pitch and roll

motion of the WMDS and fluctuating range measurement errors. To detect an actual fault, these regular deviations are to be considered by a tolerated, layer specific threshold $\Delta r_{j,\mathrm{TH}}$. For the detection of a misplaced sensor, it is sufficient to observe a single layer. Measurements lying outside this expected range indicate that the sensor orientation changed unintendedly due to mounting issues:

$$r_{ij,\mathrm{nom}} - \Delta r_{j,\mathrm{TH}} \geq r_{ij,\mathrm{m}} \geq r_{ij,\mathrm{nom}} + \Delta r_{j,\mathrm{TH}} \tag{7-10}$$

To realize the concept, it is to be identified:

1. Which layer and which measured values are to choose as a robust indicator for a range measurement deviation.
2. How much the range measurements deviate from the nominal value under regular conditions.

The lowest sensor layer (ID31) is chosen as the reference, since in this layer the ground detections have the lowest distance towards the tire contact points of the WMDS. This will reduce the influence of local ground unevenness. Comparing the measured value of each of the 512 segments to the reference is omitted, as individual outliers may occur. On the other hand, averaging the range measurements over all segments within the layer can eliminate range deviations caused by angular displacements. Therefore, the mean range of three segment areas (SA) within the 180° FOV of the layer is observed separately - on the left end, the center, and the right end. The three SA are built with 50 segments each:

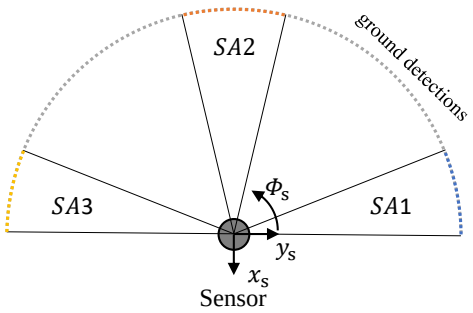


Figure 7-9.: Schematic illustration of three segment areas evaluated towards range deviations within one sensor layer.

After all segments with a range value of 0 are eliminated, the mean range over all remaining segments is calculated per SA. The obtained mean ranges are denoted as $\overline{r}_{\mathrm{SA1}}$, $\overline{r}_{\mathrm{SA2}}$ and $\overline{r}_{\mathrm{SA3}}$. For an ideally even underground and ideally mounted sensors, the three SA shall have an equal mean range measurement over all three sensors. This is to be verified in an initial sensor calibration. When observing a spread between the mean range of the three segment areas, an angular misplacement is present. If only one segment area shows mean range deviations that differ from the nominal value by more than $\pm\,\Delta r_{31,\mathrm{TH}}$, a fault condition shall be triggered:

$$\begin{aligned} |\overline{r}_{SA1} - r_{31,\mathrm{nom}}| &> |\Delta r_{31,\mathrm{TH}}| \quad or \\ |\overline{r}_{SA2} - r_{31,\mathrm{nom}}| &> |\Delta r_{31,\mathrm{TH}}| \quad or \\ |\overline{r}_{SA3} - r_{31,\mathrm{nom}}| &> |\Delta r_{31,\mathrm{TH}}| \end{aligned} \tag{7-11}$$

The minimum range deviation thresholds that can be set for operation ($\Delta r_{31,\mathrm{TH,op}}$) as well as for the initial check ($\Delta r_{31,\mathrm{TH,ini}}$) are limited by the regular occurring range deviations. For the initial check, a possibly even surface can be chosen to reduce the influence of workspace unevenness. It is recommended to always use the same spot within the workspace, e.g. the center, as this enables reproducible range measurements. For the operational check, the worst case workspace unevenness is the limiting factor. On the other hand, it was specified in the sensor set-up design (cf. Fig. B-1) that sensor inclinations are only tolerated up to 2° so that the FOV of the sensor still reliably covers the workspace. Concluding, $\Delta r_{31,\mathrm{TH,ini}}$ and $\Delta r_{31,\mathrm{TH,op}}$ are limited upwards in such a way that larger inclinations than considered in the sensor design shall not be tolerated. Thereby, the fault detection function will also impede that the WMDS is used out of its ODD, meaning on a workspace with unevenness that leads to larger pitch or roll angles. However, it shall be generally ensured that before using a workspace, it has been verified that the unevenness is not greater than the ODD allows.

To assess expectable mean range measurement deviations during operation, the representative dynamic drive maneuver is considered, as this uses a major part of the workspace and therefore will include worst case pitch and roll angles of the WMDS. Furthermore, the fast rotation maneuver is considered, as this includes high relative speeds towards the ground. To assess possible threshold for the initial check, a data set of a standstill in the workspace center is considered. For all maneuvers, the maximum occurring range deviation of any SA i towards the nominal value of 1.5 m ($\max(|\overline{r}_{SAi} - r_{31,\mathrm{nom}}|)$) is determined for each timestep. The results are illustrated in an ECDF plot, shown in Fig. 7-10. With an additional IMU implemented on the WMDS, actual pitch and roll angles of the WMDS are observed.

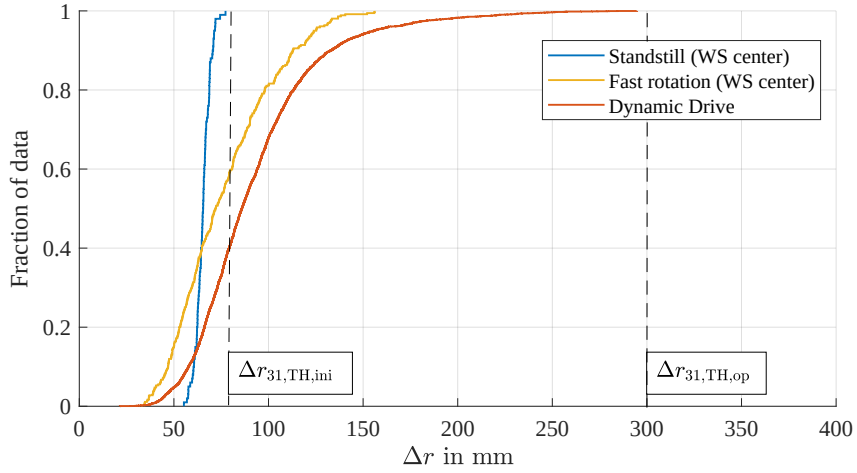


Figure 7-10.: Distribution of maximum range deviations of the mean SA ranges towards nominal range in layer ID31 within different maneuvers.

For the standstill in the workspace center, a roll-angle of $\phi_{\mathrm{DS}} = -0.67°$ and a pitch angle of $\theta_{\mathrm{DS}} = 0.26°$ are determined. This leads to maximum range deviations of 77 mm from the nominal value. In 40% of the fast rotation maneuver, lower maximum range deviations occur compared to the standstill. However, the maximum values are increased to 156 mm. Within 95 % of the

dynamic drive maneuver, the range deviation is below these 156 mm. Nevertheless, 5 % of the maneuver include greater range deviations of up to 300 mm. Observing the maximum mean range deviations over time throughout the maneuver reveals temporary correlating peaks in the WMDS' pitch and roll angles of approximately 2° (cf. Fig. E-4 in Annex E). This shows that the maximum range deviation determined for the dynamic drive is not only a representative threshold for the used workspace, but also an absolute limit for the applicability of the WMDS, since larger angles would lead to a safety relevant limitation of the sensor's FOV.

Possible thresholds for $\Delta r_{\mathrm{TH,ini}}$ and $\Delta r_{\mathrm{TH,op}}$ can be determined from the maximum values, as indicated in the figure. For the operational check, the threshold shall not be set higher than 300 mm. For the initial check, a threshold below 100 mm is considered to be possible, but it needs to be further verified in the future whether the measurements are sufficiently reproducible. The influence of local unevenness can be further minored by a slow rotation around the center of the WMDS with constant speed during the initial check. A subsequent time averaging of the measured values per segment area for a predetermined time interval shall reduce influences from local unevenness and further eliminate the regular measurement fluctuations.

A demonstration of the effect of the concept is given in Fig. 7-11. At the beginning of the maneuver, the WMDS is at standstill. The mean range measurements of the three SA of each sensor are overlapping at approximately 1.5 m. After 50 timesteps, the WMDS drives up a ramp with one wheel (between sensor 2 and sensor 3), so that a pitch angle θ_{DS} of up to $-4°$ is created. The angle is measured with an inertial gyroscope sensor mounted on the WMDS. While some SA obtain their original range measurement, others significantly deviate, so that a spread between the segment areas is generated at all sensors. With the threshold previously suggested for the ongoing

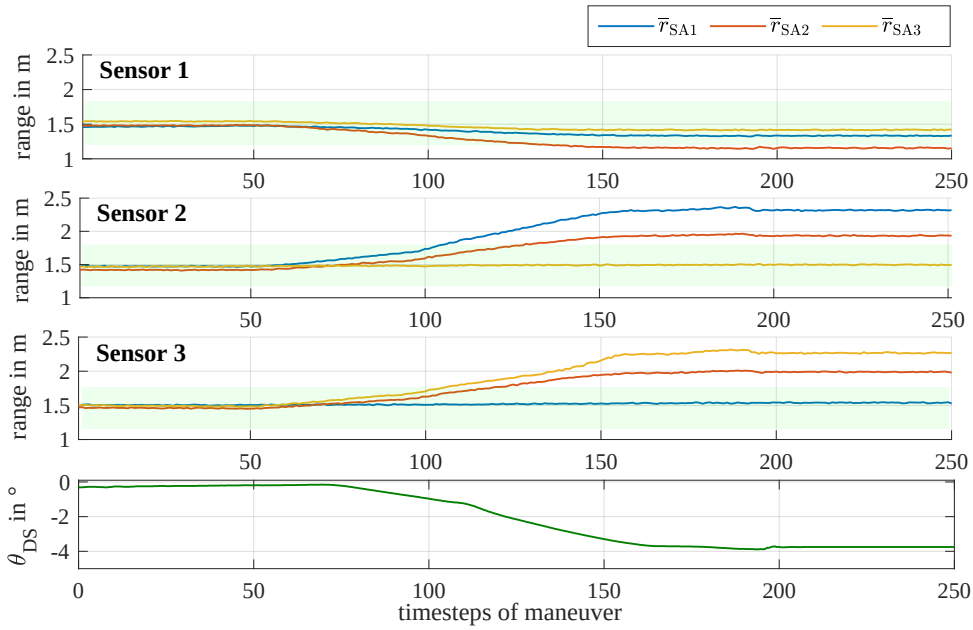


Figure 7-11.: Mean range measurements per segment area on layer ID31 and WMDS pitch angle during an elevation change maneuver. A suggested range deviation threshold of 300 mm is indicated by the green bar.

operation, indicated by the green bar, the fault detection will trigger for all three sensors slightly before -2° of inclination are reached.

7.3.3. Conclusion and Concept Limitations

For the LLLPS, robust fault indicators are available in terms of the number of matched landmarks and the matching residuals. Since the fault detection works on the level of the function's output, theoretically any fault case causing a false output is detectable. Therefore, the diagnostic coverage is considered as high for this function. The proposed threshold for the mean matching residual is to be further verified and possibly adapted in the future. When using the WMDS on larger workspaces, it is to assess whether a smaller threshold is to be chosen for $n_{\mathrm{LM,TH,op}}$, which is dependent on the actual workspace size.

The fault detection concept for the object detection function relies on the availability of ground detections under regular conditions. However, there is the restriction that a reference is not consistently available for all sensor levels. The proposed concepts seem promising for an initial check prior to operation, while placing the WMDS in the workspace center and performing a slow rotation. This enables to minor influence from unevenness and, in combination with the landmark detection check, will indicate a large scale occlusion also from the upper layers close to the horizontal line. However, small scale occlusions that only affect the upper scanlines but do not lead to a landmark loss will thereby not be detected. Therefore, it is suggested to include test objects within the initial check that enable to check the occurrence of detections for each layer. The probability to detect a hazardous, large or small scale sensor occlusion in the initial check is therewith considered high.

For the ongoing operation, further unreliabilities in the ground detections were revealed, which complicate a sensor occlusion detection. The following limitations apply:

- Ground slope and unevenness: Local unevenness creates gaps in the ground detection rings, reducing the number of detections compared to the expected values, especially in the scanning layers close to the horizontal. Furthermore, the inclination angles of the WMDS induced when driving over such uneven areas temporally shift the vertical sensor FOV. Therefore, a fault detection in ongoing operation turned out to be only possible within an increased time interval towards the time interval of object detection. To improve this, a ground with less slope and unevenness is demanded. Furthermore, a pitch and roll compensation by a suspension system can minor the inclination based limitation.
- Workspace borders: Even for an ideal even workspace surface, it is not guaranteed that sufficient ground conditions are available outside the workspace border. This can limit the applicability of the concept for large radial positions of the WMDS. A wall around the workspace would possibly enhance the potential of the concept, as then a reference would be available even for the upper layers.

- Retro-reflective disruption: it is observed, that ground detections are missing in the aligned areas between sensors and retro-reflective landmarks of the LLLPS. Lidar sensors from other manufacturers potentially show a differing behaviour, which is to assess in the future. Otherwise, the landmarks would need to be coated with less reflective foil, which is considered possible since the actual reflectivity difference towards other environmental elements provides a large buffer.
- Water accumulations: It is observed, that water on the ground can cause the laser beams to be reflected away instead of back into the sensor. If they do not hit another object afterwards, a ”hole” is created in the ground (cf. Fig. E-5). The formation of water accumulations is linked to ground unevenness, which also argues that the system should be operated only on even ground that does not allow such accumulations.

Since the occlusion detection function does not check whether the detections are actually made at a distance from the ground, light rain is not seen as a limitation of the function. If the detections of individual segments are not made from the ground but from raindrops, this does not result in a difference in the count of losses.

The concept of sensor misplacement detection refers only to the lowest layer ID31, which is always available despite unevenness on the ground and therefore is considered a robust method. However, a sensor misplacement can only be determined above the degree of regular occurring inclinations during operation. Therefore, the method would also benefit from an application on a more even ground. With an application during light rain, individual atmospheric detections can decrease the mean range per segment area. However, since only the lowest layer is considered, only low influence is to be expected. Otherwise, the threshold can be slightly adapted.

8. Safety Function Evaluation

This chapter presents a procedure of practical experiments to assess whether the functions are safe within the ODD of the WMDS, meaning if they are reaching their intended function under all conditions. Aiming to falsify the main research hypothesis, experiments are sought that represent extreme corner cases of the ODD. If the tests pass, it can be assumed that under less complex conditions, the systems will also pass. If the tests do not pass, new limits of the ODD can be set accordingly. The following falsification aspects and corner case conditions are derived:

FA1: The LLLPS is not able to determine position and speed with sufficient quality under any operating conditions as part of the ODD. This shall be falsified by experiments with the following corner cases:

- The WMDS is at maximum speed
- The landmarks are at minimum / maximum distance
- Other retroreflective objects surround the workspace
- During light rain / low sun light

FA2: Relevant objects are not detected within the PZ under any operating conditions as part of the ODD. This aspect shall be falsified by experiments with the following corner cases:

- Objects of minimum size and minimum reflectivity
- The WMDS is at maximum speed and the objects are at maximum distance
- During light rain / low sun light

The experiments are conducted with the the scaled prototype as described in Chapter 5.3.2. The experiment location is the August Euler Airfield in Darmstadt as described in Chapter 3.1. Due to unreliabilities and limitations of the WMDS prototype in the experimental phase, not all tests were performed under the derived extreme conditions. Therefore, this chapter describes the actually test cases as well as the deviating conditions under which they were performed. For example, the influence of varying weather conditions could not be assessed within the experiments, however results from an external set-up enable an outlook towards the expected influence. The tests derived here are to be understood as release tests for the safety system in the future and the results shown are thus initial indicators of the capabilities of the system.

8.1. LLLPS Evaluation

8.1.1. Test Case Specification

Experiments are required that investigate the robustness of the LLLPS in critical prevailing operating conditions. Within Fig. 6-9, the functionality of the LLLPS in a representative driving simulation maneuver was already approved. At this point, it is intended to conduct more extreme driving maneuvers as corner cases of the ODD, such that the missing of landmarks as well as the false positive detection of landmarks is provoked. The goal is to show that the system remains functional, meaning the position[111] is determined without larger deviations compared to regular operating conditions, and the failure conditions are not met. The following test cases are considered:

1. Fast rotation: Due to the high speeds, motion scan effects can occur in areas where two sensors detect the same landmark. These potentially prevent the correct positioning of the detected landmarks, which impedes the matching process, i.e. decreases the position data quality. To assess this, the WMDS is rotated on the spot with a yaw rate $> 100\,°/s$, which was specified as a maximum limit for yaw rates occurring during driving simulations. This leads to maximum occurring relative speeds between landmarks in far distance and the WMDS. The position measurement deviation towards the DGPS reference shall remain below $0.5\,\mathrm{m}$ (Δp_{DS}) and the matching residual shall remain below $0.06\,\mathrm{m}$ ($\overline{d}_{\mathrm{LM,TH,op}}$). For the current workspace size, all 8 landmarks shall be detected throughout the maneuver.

2. Workspace traversion: In a straight traversion through the workspace, the WMDS takes both minimum and maximum distances to landmarks. At the starting and ending point, this first provokes a high measurement error due to the retroreflective interference effects of landmarks in the near range, and the loss of individual landmarks in the far range. High speeds further provoke motion scan effects. If the quality of the position determination can be maintained during the entire workspace traversion, this shall also be possible at any other position within the workspace. The position measurement deviation towards the DGPS reference shall remain below $0.5\,\mathrm{m}$ (Δp_{DS}) and the matching residual shall remain below $0.06\,\mathrm{m}$ ($\overline{d}_{\mathrm{LM,TH,op}}$). For the current workspace size, all 8 landmarks shall be detected consistently.

3. Increased workspace: The flexibility of the system towards varying workspace sizes shall be demonstrated. For this purpose, the workspace shall be successively enlarged, while observing the quality of the position data with respect to the visible landmarks. As long as the position deviation towards the reference remains below $0.5\,\mathrm{m}$, the LLLPS can be applied with the current set-up.

[111] Since the speed is a calculated value from the position, and therefore the quality of the position data has a direct effect on the speed data quality, only the quality of the position data is considered here.

4. External interference: To ensure the system remains functional under disturbance of other retroreflective objects, an object with similar reflection properties to the landmarks is moved around the workspace to provoke a false positive landmark matching. The test is passed if no mismatching of landmarks occurs.

A release of the system additionally includes verifying that the exceeding of a radial speed limit is detected and that braking is initiated in time. However, since the critical part of this task is the correct determination of the measured variables, only the robustness of the measurement quality is discussed in the following.

8.1.2. Test Execution and Results

Fast Rotation and Workspace Traversion

For the rotation experiment, the WMDS is placed in the center of the workspace. The maximum reached yaw rate is $259\,^\circ/\mathrm{s}$. This is far above the yaw rate limit within driving simulations, which were determined to $< 100\,^\circ/\mathrm{s}$ in Fig. 3-2, and therefore is an extreme corner case.

Secondly, the workspace is traversed in a straight line with a maximum translational speed of $7.9\,\mathrm{m/s}$, which was the maximum the scaled WMDS prototype was able to reach within the given space. In Fig. 8-1, the displacement of the WMDS during both maneuvers is illustrated. The straight traversion starts and ends outside the actual borders of the motion space, so that maximum distances to landmarks are reached. Actually, a diagonal traversion through the center point would have been favored, but was not possible due to the lack of acceleration and run out zones on the right side outside the workspace. During the experiments, the position deviation towards the DGPS measurements, the average matching residual and the number of detected landmarks are observed.

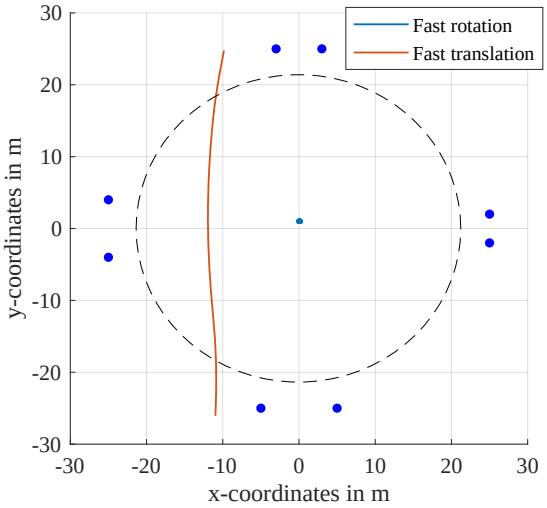


Figure 8-1.: Path driven during the fast rotation and workspace traversion maneuver. The dark blue dots indicate the landmark positions, the circle indicates the motion space.

The results are indicated in Fig. 8-2. The mean matching residual during the rotation remains below 0.01 m and therefore is in compliance with the fault detection threshold set for the initial test in the workspace center. During the traversion, the mean matching residual remains below the previously defined threshold of $0.06\,\mathrm{m}$. The number of matched landmarks is illustrated in the bottom of the figure, which remained constantly at 8 landmarks for both maneuvers. The position deviation towards the DGPS reference remained below 0.24 m with unfiltered data for the fast rotation and below 0.32 m for the fast translation[112], which is below the maximum tolerated deviation. The experiments are thus considered as passed - the LLLPS proves to be robust under the extreme driving maneuvers and therefore also under all regular occurring maneuvers.

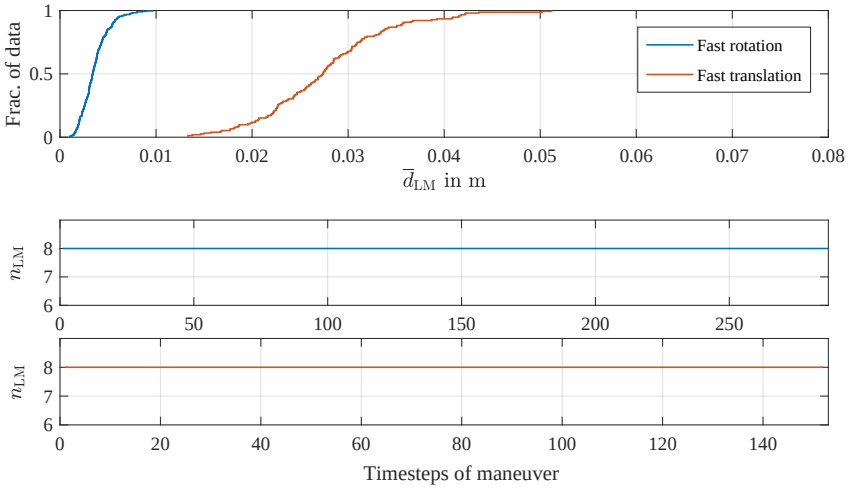


Figure 8-2.: Mean matching residuals and matched landmarks during fast rotation and workspace traversion.

Increased Workspace

Due to space limitations on the August Euler Airfield, the workspace size cannot be increased to assess the ability of functionality in an increased workspace. Therefore, instead, it is investigated, if the LLLPS remains functional even if less than 8 landmarks are available on the regular workspace. To investigate this, the LLLPS algorithm is modified so that only a predetermined number of detected landmark clusters is retained for the map matching per calculation step. The discarded clusters are always those with the lowest number of contained detections, so that the clusters associated with the most distant landmarks are deleted, corresponding to the case of a too large workspace. The number of discarded clusters is varied from 1 to 5. The deviation of the position measurement towards the DGPS signal is observed.[113a]

The results are shown in Fig. 8-3. Until the deletion of 3 clusters, no decrease in the positioning performance is observable. From only 4 visible landmarks, a slight decrease in positioning quality becomes noticeable, but still generally remains below a deviation of $0.5\,\mathrm{m}$ and even below $0.3\,\mathrm{m}$

[112] Fig. F-3 and Fig. F-4 in the Annex give an insight in the position deviation over time for both maneuvers.

[113] Betschinske, D.: Master Thesis, Position Determination with Lidar Sensors for WMDS (2022) a: p. 106 ff. ; b: pp. 98-99.

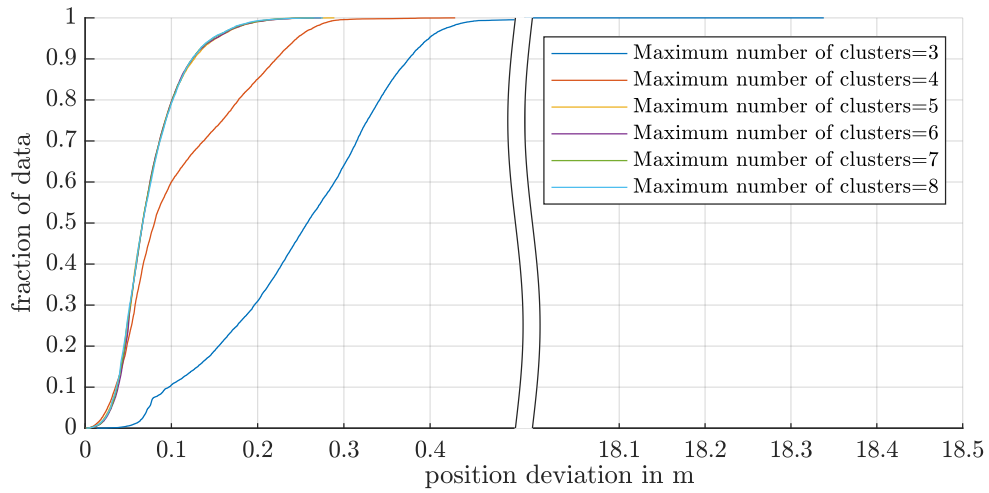


Figure 8-3.: ECDF plot of the position deviation between LLLPS and DGPS signal (raw) during the dynamic drive maneuver for a varying number of discarded landmark clusters.[113a]

for 99 % of the data set. After more than 4 visible landmarks are deleted, the position quality remains below 0.5 m for 99 % of the data set, but shows single peaks to unreasonably high values. This allows to conclude that the system is able to maintain the demanded positioning quality under the requirement that at least 4 landmarks are visible at any time. Assuming that a landmark is detected up to a maximum distance of 50 m, it is estimated that under the condition of at least 4 detectable landmarks from each workspace position, the workspace radius can be increased up to 37 m (cf. Fig. 4-3). In the future, this needs to be verified with an actually increased workspace. However, the experiment is a first indicator that a usage on larger workspaces is possible.

External Interference[113b]

To assess the robustness against false positive landmark detections, additional retroreflective objects are moved in close proximity to the workspace border and respectively to the landmarks, while the WMDS performs a representative dynamic drive as shown in Fig. 6-8. The disturbance objects wear the same reflective foil as the landmarks and therefore will still appear in the point cloud after the preprocessing filters are applied. This experiment aims to represent the case that reflective objects moving in the environment, e.g. vehicles or persons wearing safety vests, possibly confuse the LLLPS. The experiment is passed, if the LLLPS manages to discriminate the additional clusters within the matching process.

With additional retroreflective objects, a mismatching is not observed throughout the whole maneuver. Only if the objects are in direct proximity to the landmark (< cluster search radius), the clustering algorithm merges the true landmarks and the additional objects, which leads to a slight deviation in the position determination of the cluster centroid. It can be assumed that uninvolved third persons in the surrounding area will maintain a greater distance from the workspace than the search radius around each landmark. However, system operators and spectators, especially if dressed retroreflectively, should take care to keep distance from the landmarks. Nevertheless, the

position deviation in this experiment remains below 0.2 m and therefore is within the range of the regular performance (cf. Fig. F-6).

8.1.3. Conclusion

The LLLPS passes all the experiments performed. The availability of the system is shown to be robust from all workspace positions and even under very high rotational speeds of the WMDS. Since the experiments exceeds regularly occurring yaw rates and the maximum workspace position without a quality decrease, the LLLPS can be considered robust and suitable for the regular application for the WMDS. Compared to object detection, the LLLPS is not sensitive to the influences of ground unevenness, since the landmarks were dimensioned with sufficient buffer with respect to the sensor resolution. In addition, the landmark detections prevail as the strongest return due to the high reflectivity differences towards the environment. Thus, it can be concluded that the selected hardware is already sufficient for the application and no higher temporal or spatial sensor resolution is required. Another reason for the high robustness of the system is the used principle of map matching with the high overdetermination of the system. It was shown that individual landmark losses are not critical, so that the system should also be operational on larger operating sites. Due to the limited search radius and the coding by the individual landmark distances, a false positive landmark matching is nearly impossible. Only if disturbing objects with comparable reflectivity are located within the search radius of a landmark, a distorted landmark center estimation may occur. In the future, the performed tests shall be repeated under additional sever weather conditions to further challenge the functionality of the system. An outlook towards the applicability under rain and low sunlight is given in Chapter 8.3.

So far, an actual limit of applicability of the system only applies for the usable workspace size. For the current landmarks, the extensibility to a workspace radius of 37 m was estimated, since a detection capability up to a distance of about 50 m was shown for the current landmarks. However, for larger workspaces, enlarged landmarks could be used until the detection range limits of the lidar sensors are generally reached. This is specified to 100 m for retroreflectors by the manufacturer. However, smaller limits can apply if less reflective landmarks are used in the future, which was recommended due to interference with the ground detections.

8.2. Object Detection Evaluation

8.2.1. Test Case Specification

A release test of the object detection system must prove the detection capabilities of objects with a minimum size and minimum conceivable reflective properties under critical distances and weather conditions for the object detection system. This includes two cases:

1. Maximum speed / maximum distance: The WMDS moves with maximum translational speed $v_{\mathrm{DS,max}}$ which leads to a required maximum PZ with $R_{\mathrm{PZ}}(v_{\mathrm{DS,max}})$. The object of sizes $w_{\mathrm{obj,min}}$ and $h_{\mathrm{obj,min}}$ must be detected such that the emergency brake flag is set before a critical distance $d_{\mathrm{obj,ebf,min}}$ between object and WMDS is reached (cf. Fig. 8-4). This critical distance considers the regular PZ dimension minus the distance already covered during the sensing and trigger processing reaction time, and is determined as an adaption of Equ. 4-13:

$$d_{\mathrm{obj,ebf,min}} = v_{\mathrm{DS,max}} \cdot \tau_{\mathrm{react,a}} + \frac{1}{2}\frac{v_{\mathrm{DS,max}}^2}{a_{\mathrm{brake}}} + \Delta d_{\mathrm{obj}} + l_{\mathrm{c}} \tag{8-1}$$

2. Reduced vertical FOV: Within the distance $d_{\mathrm{h,red}}$ towards a sensor, objects with a reduced width of $w_{\mathrm{obj,min,hred}}$ must be detectable, which covers the case that only slim legs are visible in the near field where the vertical sensor FOV does not exceed $1\,\mathrm{m}$ height above the ground. Approaching an object of this minimum width, an emergency brake flag must be set before the critical distance of an object towards a sensor $d_{\mathrm{h,red}}$ is reached. Whether the experiment is conducted during standstill or motion, and up to which speed, is dependent on whether $d_{\mathrm{h,red}}$ is smaller or larger than $R_{\mathrm{PZ}}(v_{\mathrm{DS=0}})$. This must therefore be determined in dependence of a resulting sensor's FOV in its mounting pose on the vehicle.

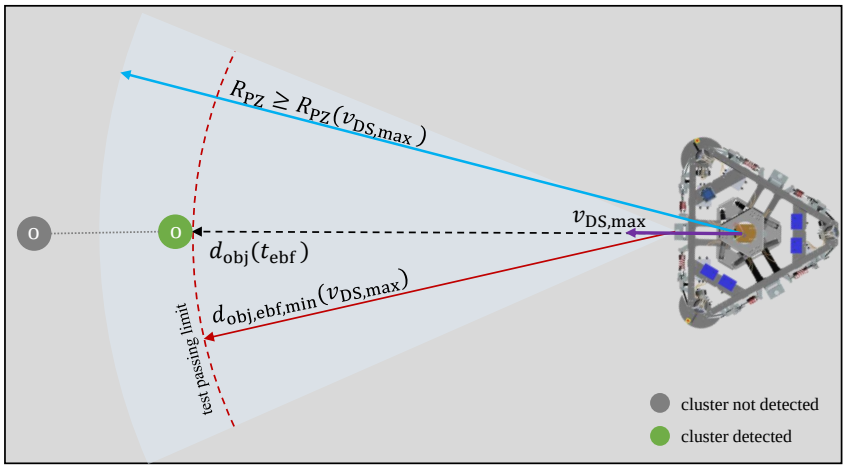


Figure 8-4.: Set-up of maximum speed test.

For both cases, the WMDS must be oriented towards the objects in such a way that only the FOV of a single sensor covers the objects, since the detection probability would be higher in overlapping areas of two sensors. The tests shall therefore be repeated for each sensor. The experiments must be conducted for light rain as well as low sunlight with direct radiation into the sensor. For the most critical reflectivity properties of objects, the specification of tests for protection systems of automated guided vehicles presented in Chapter 2.3 are followed. This suggests black, cylindrical objects to obtain a reflectivity $< 10\%$.

Tests under high yaw speeds of the WMDS are not additionally foreseen for object detection.

High yaw speeds could lead to motion scan effects in the areas where two sensors overlap (cf. Fig. 6-4), making an object appear twice with a spacial offset resulting in the time gap of the rotations of the two sensors. However, since object tracking was deliberately omitted from the multidetection check, spatially offset objects due not pose a risk of false negative detection. A high rotation of the WMDS would only be dangerous if, with the same rotation direction to the lidar scan, the spatial offset between two segment scans is widened such that the minimum cluster size in horizontal direction cannot be fulfilled. With the present rotation rate of 20 Hz and 1024 segments in azimuth, however, this time gap between two segment scans is so small that a rotation rate of 100° at distances of $30\,\mathrm{m}$ would lead to a spatial widening of the horizontal gap of at most $0.0025\,\mathrm{m}$ (cf. Annex F). Therefore, this case is not considered to be additionally critical to the cases specified above.

8.2.2. Test Execution and Results

Test Objects

To investigate the capabilities of the system, the actual test execution includes various objects of different sizes, as shown in Fig. 8-5. The ball represents the object of minimum size in height and width in combination and is coated with a matt black varnish. Its convex surface adds further difficulties, since the actual area reflecting back to the sensor is even smaller. To be able to test the critical dimensions isolated from each other, a cylinder out of black matt cardboard with a diameter corresponding to $w_{\mathrm{obj,min}}$ / $h_{\mathrm{obj,min}}$, but a larger height, is additionally provided. This will be applied once standing upright and once lying on the ground, thereby mimicking a slim person standing and lying. For the tests within the reduced FOV, where stricter requirements for the minimum width of objects apply, a slim cylinder with the same matt black varnish and a diameter $< w_{\mathrm{obj,min,hred}}$ is used.

Object	$w_{\mathrm{obj}} = D_{\mathrm{obj}}$ in m	h_{obj} in m
O1: ball	0.22	0.22
O2: large cylinder	0.20	0.5
O3: slim cylinder	0.09	0.55

Figure 8-5.: Object detection test objects used in the experiments.

Test Execution Procedure

Within this work, the test is only carried out exemplary for one sensor. Each object is placed separately in a distance larger than the required PZ. The WMDS is moved centered towards the

objects in a straight line. This straight line is not exactly the same for each run, so the road profile can slightly vary within the maneuvers. To examine the influence of the driving speed on the object detection, the approach is conducted at different speed levels, while each speed level is tested at least three times. The lidar sensor data is recorded in raw format and evaluated in a post processing. Due to a defect in the WMDS prototype's battery system, the WMDS could not be driven via its own drive system. Therefore, it was pushed by another vehicle (Mercedes-Benz Unimog). Shortly before reaching the object, the WMDS is braked to standstill. With this set-up, it was not possible to achieve the desired maximum speed of $10\,\mathrm{m/s}$. The tested speed interval is between 2 and $7\,\mathrm{m/s}$. The actually driven speed is measured by a GPS measurement system installed on the WMDS. Furthermore, pitch and yaw rates and angles of the WMDS are measured with an inertial measurement system installed on the WMDS.

In order to compare the detection capability without WMDS motion and thus without disturbing excitation of the ground, in one experiment the WMDS is not moved towards the ball but the ball is rolled flat over the ground towards the WMDS. This is repeated 5 times with different speed levels. The speed of the ball is estimated from the measured object distance over time as a mean speed throughout the ball approach.

For the test within the reduced vertical FOV, the slim cylinder is investigated while the WMDS is approaching the WMDS with $< 1\,\mathrm{m/s}$. This test is repeated 3 times.

Test Evaluation Procedure

The minimum distance to a detected object d_{obj}, measured by the lidar sensors, is observed. As long as no cluster is detected, the distance is correspondingly 0. As soon as an object is detected as a cluster, the minimum measured distance to it is returned. From the course over time of this measured object distance, three characteristics are evaluated, as exemplary indicated in Fig. 8-6.

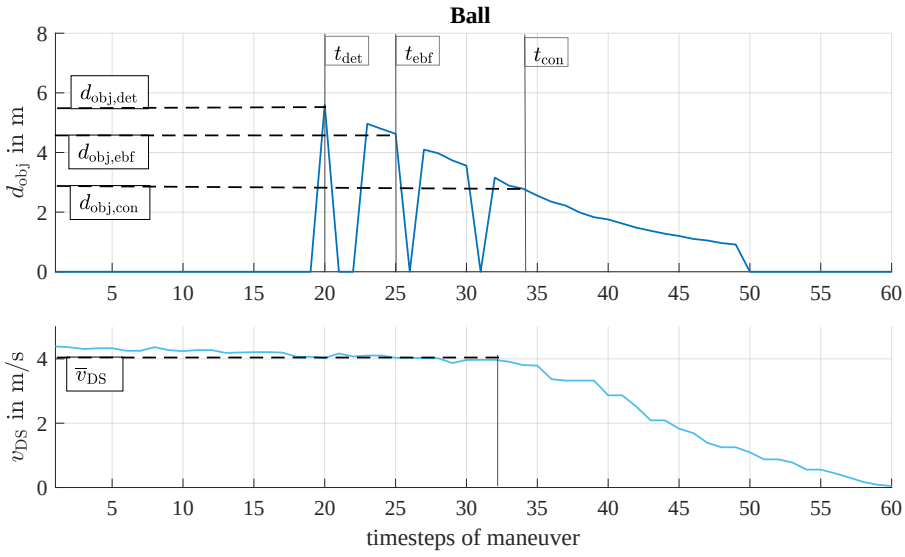


Figure 8-6.: Indicators for the evaluation of the object detection tests on the example of a straight drive towards the ball.

The distance at which the object is detected for the first time is denoted as $d_{\mathrm{obj,det}}$. This indicates from which distance the sensors are generally able to capture an object. The distance at which an emergency braking condition is fulfilled for the first time is denoted as $d_{\mathrm{obj,ebf}}$. This indicates the distance from which the WMDS would trigger the emergency brake, which must finally comply with the critical object distance described in Equ. 8-1. For this, the object must have been detected 3 time steps ($n_{\mathrm{TH,multi}}$) in a row. Single losses of the object can increase the time delay between first detection and emergency brake flag. Since such losses appear frequently, the third indicator is the distance from which the emergency brake flag remains consistently, i.e. remains at 1 without single drops until the maneuver is finished, denoted as $d_{\mathrm{obj,con}}$. This indicates how failure-prone the detection of an object is during the approach of the WMDS. All distances are evaluated in combination of the mean approaching speed to obtain a relation towards object detectability and driving speed.

Results: Maximum Detection Distance

Fig. 8-7 summarizes the results of all conducted tests with the ball, the vertical and the horizontal positioned large cylinder with respect to the first appearing object detection and emergency brake flag towards the driven speed. The x-axis indicates the object distance d_{obj}, the y-axis the WMDS speed or the ball speed. The colored markers indicate the object distances at first emergency brake flag trigger $d_{\mathrm{obj,ebf}}$, grey markers indicate initial object detection distances $d_{\mathrm{obj,det}}$. The dashed grey line is the test passing limit in dependence of the driven speed according to Equ. 8-1. Since the tests are intended to be representative for the maximum speed of $10\,\mathrm{m/s}$ and maximum distance, respectively, the general passing limit is drawn as the vertical line at $d_{\mathrm{obj,ebf,min,10}}$. The vertically standing cylinder passes the test in all cases, since $d_{\mathrm{obj,ebf}}$ is larger than the critical object distance. An initial detection of the standing cylinder takes place between $18...20\,\mathrm{m}$. According to the theoretical investigation of the horizotal sensor gaps in Fig. 5-5, an object of 0.2 m is only detectable from a distance of 16 m. This shows that the detectability is even increased towards the theoretical estimation, which can be explained by the beam divergence. At higher speeds, $d_{\mathrm{obj,ebf}}$ is only slightly smaller and the delay towards the initial detection is only slightly greater than at lower speeds. This is due to the fact that at higher speeds the WMDS covers a greater distance within the 3 time steps. It therefore is to conclude that the actual speed has no significant influence on the detection capability of this object.

The horizontally lying cylinder passes in only 4 of the 9 tests, which are those in the low and medium speed range. The distances of initial detection $d_{\mathrm{obj,det}}$ are all between $16...20\,\mathrm{m}$. This meets the expectations from the theoretical investigation of the vertical beam gaps in Fig. 5-4. However, the spread to $d_{\mathrm{obj,ebf}}$ is very large in the 5 non-passing cases, meaning the object is lost frequently after the first detection. All tests with the lying cylinder pass the test for a maximum speed of 7 m/s, which is indicated by the vertical line at $d_{\mathrm{obj,ebf,min,7}}$.

The ball has the approximately same height as the lying cylinder, and the same width as the standing cylinder, nevertheless it does not pass in any of the tested cases. The distance $d_{\mathrm{obj,ebf}}$ is

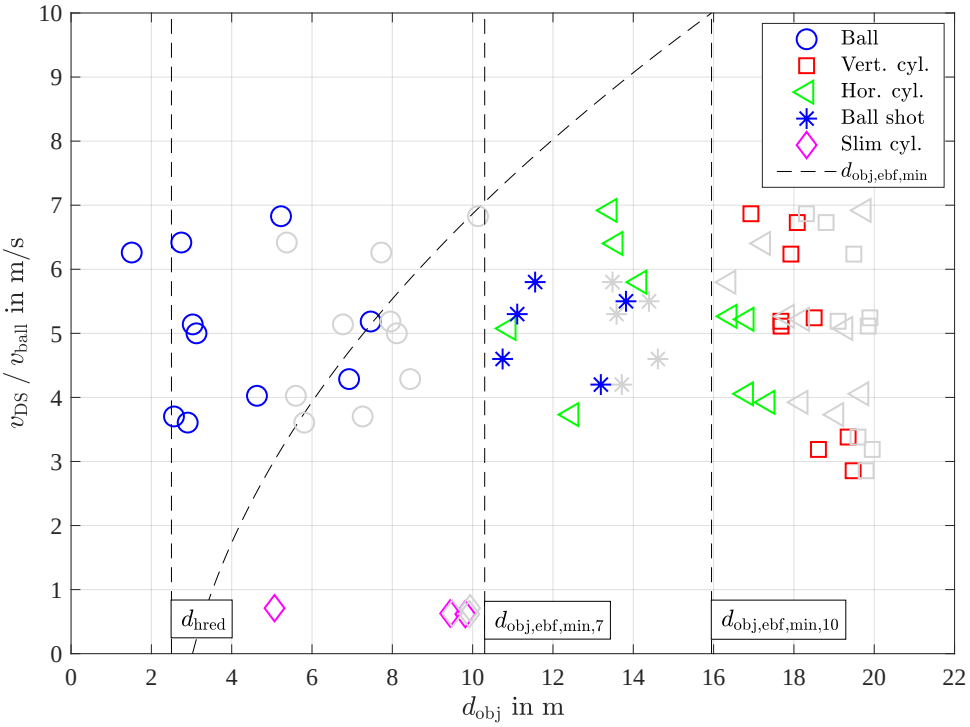


Figure 8-7.: Evaluation of the maximum object detection distance with all test objects towards the test passing limit in dependence of the WMDS speed. The colored markers indicate the distance at first emergency brake flag. The grey markers indicate the distance of first object cluster detection.

strongly scattered between $1.5...7.5\,\mathrm{m}$. The initial detection distance $d_{\mathrm{obj,det}}$ is scattered between $5.5...10\,\mathrm{m}$. It is remarkable that the larger detection distances tend to occur at the higher speeds. However, since both evaluated distances fluctuate greatly for the ball, they appear to be rather random than reliable.

Compared to this, the shot ball with static WMDS shows larger values for both evaluated distances. $d_{\mathrm{obj,det}}$ scatters between $13.5...14.5\,\mathrm{m}$ and $d_{\mathrm{obj,ebf}}$ scatters between $10.5...14\,\mathrm{m}$. Thus, the time delay between initial detection and braking trigger is significantly smaller than for the lying cylinder or the ball at a moving WMDS. This indicates that the inherent motion of the WMDS is responsible for the frequent object losses and the resulting delay between initial detection and emergency brake flag. On the other hand, the distance of initial detection is still lower than for the lying cylinder despite the same height. Concluding, the maximum detection distance of the object is limited by the external properties, i.e. the spherical surface of the ball.

In Fig. 8-8, the distance of first emergency brake flag $d_{\mathrm{obj,ebf}}$ is plotted over the distance of consistent emergency brake flag $d_{\mathrm{obj,con}}$ for the same set of tests. Results that lie on the diagonal line indicate that the first emergency brake signal remained consistent.

The consistent detection of the vertical cylinder is achieved shortly after the initial emergency brake flag. For the objects with minimum height, there is a significant delay compared to the initial emergency brake flag in all cases. In some tests, the objects are only consistently detected from about half the distance of the initial brake signal. Theoretically, the consistency of an emergency

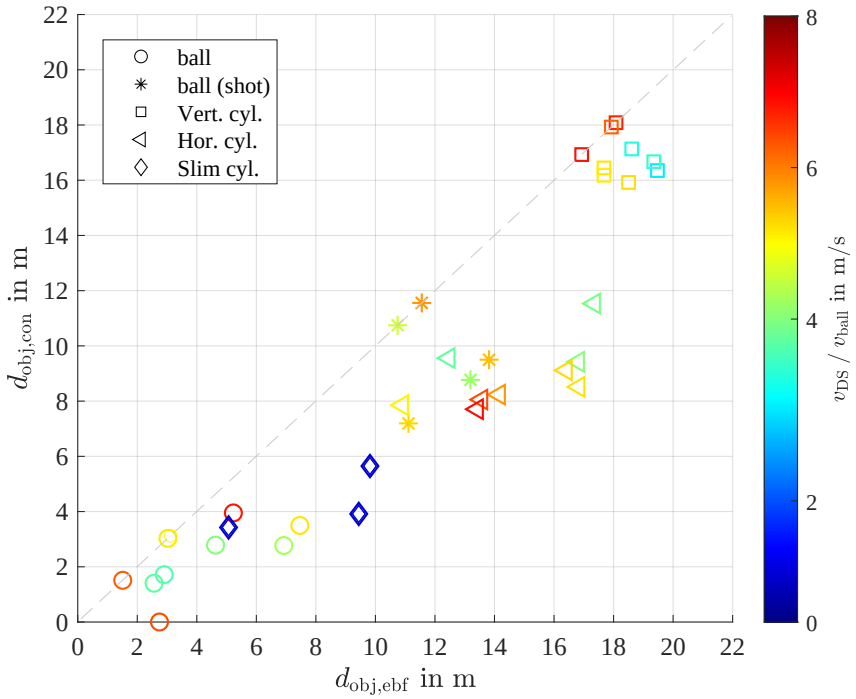


Figure 8-8.: Evaluation of the distance of first emergency brake towards the distance of consistent emergency brake for all test objects. The color scale indicates the speed of the WMDS / the shot ball.

brake flag signal is not important in real operation, as long as the first flag appears in time. After this, a braking will be initiated. On the other hand, a certain randomness or uncertainty must be assumed for those tests, in which the delay between the initial and the consistent emergency brake flag is large. Therefore, the object detection is only considered reliable for those distances, in which an object is consistently detected.

The combination of minimum height and minimum width in a convex surface of the ball leads to a strongly reduced detection distance and at the same time to more frequent losses than with the cylinder. Considered in isolation, the object height is more critical for the detection distance than the width, which can be seen from the comparison of the horizontal vs. the vertical cylinder. The reason for the frequent losses of the objects during WMDS motion is explained by vehicle pitching and rolling motion, which disturb the ground segmentation and shift the sensor's FOV. This can lead to larger cut-offs of the lower object points and to their assignment to the ground. Furthermore, regularly occurring detection losses, as observed within the ground detection diagnosis, can enhance the sensitivity of object losses. The impact of this on the object detectability is greater on objects of lower height, since for these a lower buffer of detections towards the minimum cluster size is obtained. It is assumable, that on a sufficiently flat underground, the distance of first and consistent detection will deviate less from another than shown in the present experiments. Fig. F-1 exemplary shows that there are temporal correlations between peaks in the pitch and roll angles and rates of the WMDS and losses of the detected object during the approach towards the horizontal cylinder, which strengthens this assumption. The overall distribution of pitch an roll motion of the WMDS measured during the approaches towards the objects is given in Fig. F-2.

Absolute pitch and roll rates ($\dot{\theta}_{\mathrm{DS}}, \dot{\phi}_{\mathrm{DS}}$) up to 20 °/s and pitch and roll angles ($\theta_{\mathrm{DS}}, \phi_{\mathrm{DS}}$) up to 1.5°, both referenced to the WMDS coordinate system, were measured.

Results: Reduced FOV

For the current sensor set-up, $d_{\mathrm{h,red}}$ applies to $3\,\mathrm{m}$ according to Fig. 5-4. This is the minimum distance from which the slim cylinder must trigger an emergency brake flag during an approach. The resulting detection distances for all three tests are also depicted in Fig. 8-7 and Fig. 8-8. In all cases, the cylinder is detected and the emergency brake flag is set at a further distance than the critical distance $d_{\mathrm{h,red}}$. First detections appear at 10 m distance. A consistent detection is obtained at a minimum distance of $3.8\,\mathrm{m}$, which still satisfies the test passing limit. Similar to the standing larger cylinder, the initial detection distance is larger than according to the theoretical consideration from Fig. 5-5. An object with a width of 0.09 m should actually only be detected by two laser beams at a distance from 7 m. This is again explainable by the beam divergence. On the other hand, consistent detection occurs later than expected from the theoretical considerations.

In Fig. 8-9, the object detection distance during an approach towards the slim cylinder and the WMDS pitch and roll motion quantities are illustrated over time. The maneuver is started with the slim cylinder placed in a distance of approximately $6.5\,\mathrm{m}$ to the sensor, while the vehicle is in standstill. It is shown, that the object is detected consistently during standstill. When the

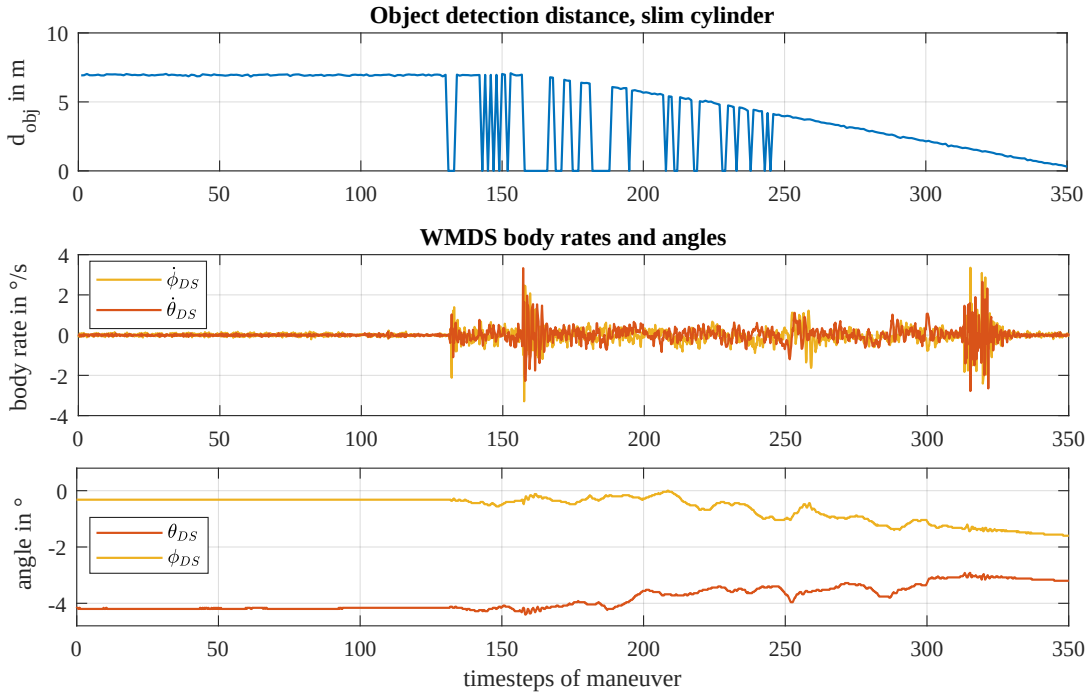


Figure 8-9.: Evaluation of object detection during the approach of the slim cylinder. Highly frequent drop-outs are observed as soon as the WMDS starts to move, temporally correlating with peaks in the WMDS' body rates.

WMDS starts to move, noticeable at the peak in the body rates, frequent drop outs appear until a distance of $4\,\mathrm{m}$ is reached. This means that the sensing capabilities towards an object small in width are also disturbed by the motion of the WMDS. Since no significant change in the pitch

or roll angle are visible, this is possibly due to vibrations of the WMDS. The WMDS is rigidly connected to the pushing Unimog, which is exposed to strong vibrations from the moment of its engaged clutch, so the transmission of these vibrations could also be a factor that disturbs the sensor. Although this does not prevent the detection of the object beyond the critical distance, it is an unexpected phenomenon that should be investigated further in the future.

8.2.3. Conclusion

Limits of the System

Based on the determined detection distances, limitations of the applicability of the system are inferred. Since the vertical and horizontal cylinders represent a standing and lying person of minimal size and reflectivity, it can be concluded that person detection capability is demonstrated for a reduced maximum WMDS speed of up to 7 m/s, for which all cylinder test results are beyond the critical distance limit. However, this only applies to the first occurrence of the emergency brake flag. If the system is released for the consistent detection limit only, the maximum speed of the WMDS would have to be limited to 5.5 m/s.[114] Both are below the intended maximum speed of 10 m/s, for which the system was actually designed. While the detection capabilities towards minimum object widths comply with the theoretical estimations, the objects of minimum height are detected in only smaller distances than expected and therefore are the limiting factor. This is due to the large ground filter threshold and disturbances caused by unevenness. Thus, a limitation of the WMDS' ODD is required. This ODD constraint can be either the maximum WMDS speed or a specific workspace underground condition at which lower vehicle inclinations and buildup rates take place. However, to which degree of WMDS inclination or buildup rates the system is usable at the maximum WMDS speed cannot be determined within the scope of the conducted experiments. The results only allow the conclusion that the detection capabilities increase towards greater distances when there is less influence of the ground unevenness. First, because the ground inlier threshold can be set smaller. Second, because the vertical cluster size can potentially be decreased to 1. Third, because less disturbance by vibrations and inclinations are expected. In the future, the parameter calibration and the tests should be repeated for more even surfaces, and also without the pushing vehicle, in order to identify this.

To further increase the object detection distances despite the present ground conditions, a higher sensor resolution is a possibility, as this increases the number of detections on the objects. The comparison from standing and lying cylinder shows that for an application up to a WMDS speed of 10 m/s, the resolution must be increased only in elevation, since the tests are passed for the standing cylinder with critical width. If the WMDS is used with its maximum speed of 15 m/s, the resolution must be increased in both elevation and azimuth. Estimations of the required sensor resolutions for a full range object detection are elaborated in Annex F and apply to approximately

[114] The minimum distance of the consistent emergency brake flag for a horizontal cylinder is 8 m, as shown in Fig. 8-8. The maximum tolerable speed in this case can be read from Fig. 8-7.

0.17° for azimuth and elevation when used on even grounds. When the WMDS is further used on an uneven ground such as the present workspace, the elevation resolution requirement is estimated to 0.1° for the full scale detection range. In addition, a suspension system, as planned for the full scaled WMDS MORPHEUS 2.0, may allow to lower the ground inlier threshold and thus improve the detectability of small objects. To further improve the existing set-up, approaches to finer ground segmentation shall be investigated, which also facilitate smaller ground inlier thresholds.

The ball proved to be a particular challenge for the object detection function. Since the critical object sizes in isolation resulted in significantly larger detection distances, this must be a consequence of the spherical surface or a lower reflectivity. However, the ball represents a more critical object size than would humans, so that no further limitations for the detection of persons are concluded from this. Small objects, such as a toolbox or a large stone, are more likely to fall into this category. Since such objects do not suddenly approach the WMDS during operation, the workspace can also be cleared from them during an initial walk-through by the operators prior to operation.

Validity of Experiments

The validity of the experiments requires that the most critical conditions that can occur in reality have been tested. The use of black objects as test objects for laser-based personal protection systems is also prescribed by the standard for driverless transportation systems (cf. Chapter 2.3), as they have a low reflectivity and are therefore a challenge for the measurement principle. However, actual object reflectivity limits were not investigated, e.g. for different shades of black or different materials. It was further assumed that objects which possibly appear on the workspace are not purely specular or transparent, which would further challenge the lidar sensors. For humans, this is considered a valid assumption. For vehicles, the areas of the windows would possibly not be detected, which is acceptable since major parts of regular vehicles consist of non transparent parts. In addition, only full bodies were considered, so e.g. a mesh box might not be detectable, depending on the mesh width. This can also apply for bicycles. Here, however, the human on or next to the bicycle would fulfill the conditions investigated. Since the WMDS will always be operated within a controllable environment and the workspace can be cleared from objects prior to each operation, the detection of human during operation (with or without vehicles) is considered the most important task. In this case, the object size and reflectivity used are regarded as valid worst cases. Especially a lying person is a conservative worst case with a low probability of occurrence.

The speeds driven with the WMDS were below the intended maximum speed. Consequently, the tests would have to be repeated for these. However, the results do not show a clear influence of the WMDS speeds towards the maximum distance of object detection, so that it is considered that the tests will show similar results when the WMDS drives at higher speeds during the experiments. A further limitation of the experiments is that it was not possible to test under critical weather conditions. An outlook on this can be found in Chapter 8.3.

A simplification that was basically assumed in the design of the object detection is that the collision objects do not have an ego speed. This is assumed because the WMDS is not applied in moving traffic, contrary to a road vehicle. Instead, it has its own operating area and it is assumed that other objects stop as soon as the WMDS approaches them.[115] The ego speed of objects could be considered with an additional safety factor in the PZ design. This increases the required object detection distance, and an alignment with the radial speed limits is no longer given.

8.3. Outlook on the influence of Rain and Sun Light

In fact, the experiments described above should have been carried out under the most adverse weather conditions as part of the ODD. After excluding fog and all kinds of heavy precipitation, these are strong, low sunlight and light rain. Since the prototype WMDS is not waterproof, rain had to be omitted in the experiments. The limited availability of the WMDS also did not allow explicit tests under clear skies and low sun. Nevertheless, the work of Linnhoff et. al.[116] enables an assumption about the influence of rain and sunlight on the safety functions of this work.

In this publication, the influence of weather conditions, containing rain, fog, snow and sun light, on different lidar sensors is investigated with a static measurement setup. Among the lidar sensors investigated is the Ouster OS1-32 Gen2 used in this work. In Fig. 8-10, the relative number of detections on three targets with 50 % reflectivity in a distance of 50 m, 58 m and 66 m in relation to the measured precipitation rate is shown. The number of detections is scaled to the respective maximum detection count on the targets in clear conditions to obtain a probability value that a laser beam reaches a target instead of being reflected by the rain. It is observable that the detection probability remains close to 1 for rain rates of up to 10 mm/h for all three targets. The German metheorological service describes rain rates of below 10 mm/h as moderate, while light rain is only below 2.5 mm/h.[117]

Concluding, the detection probability is only slighly decreased in these experiments. However, the results are only valid for targets with a minimum of 50% reflectivity and a maximum distance of 66 m. Since the sensor outputs the strongest return, less reflective objects, as the black objects used in this work, are potentially detected with lower probability. Nevertheless, the maximum distance for the object detection is below $20\,\mathrm{m}$ for the limited WMDS speed, which possibly compensates a lower object reflectivity. Nevertheless, since individual detections can be lost due to rain, an application under light rain also argues for the use of a higher-resolution sensor in elevation and azimuth. The LLLPS, due to the highly reflective landmarks and the fact that their

[115] This is in line with the standards for collision protection systems for driverless transportation systems, as explained in Chapter 2.3.

[116] Linnhoff, C. et al.: Environmental Influence on Automotive Lidar Sensors (2022).

[117] Deutscher Wetterdienst: Glossar - Niederschlagsintensität (2022).

dimensioning allows single detection losses, is considered unsensitive towards rain, also with the currently chosen sensor.

Concerning sun light, the influence of ambient brightness on the intensity of detections as well as the influence of sun light pointing directly in the sensor are investigated by Linnhoff et al. For the latter, the occurrence of atmospheric detections in the direction of the sun light were investigated for different angles of sun radiation during sun rise and sun set. While lidar sensors of other manufacturers (Blickfeld Cube 1 and Velodyne VLP-16), detections above ground in direction of the sunlight are observed, for the Ouster OS1 Gen2 lidar sensor, no influence in both cases was measurable by Linnhoff et. al. Therefore, no effect on the object detection and LLLPS function of sun light is considered for the sensor system chosen for the WMDS.[116]

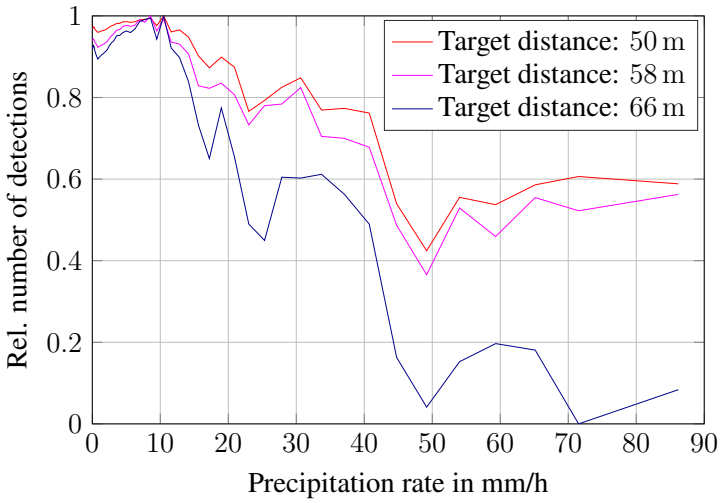


Figure 8-10.: Relative number of detections of the Ouster OS1-32 lidar sensor on three 50 % targets depending on the rain rate. Figure taken from Linnhoff et. al.[116]

9. Final Conclusion and Outlook

The main objective of the present work was to investigate the feasibility of an active safety system for WMDS. This aimed to address previous weaknesses in the their safety architecture by providing a *collision avoidance function* and a *workspace compliance function* to safeguard the WMDS within the workspace without physical barriers. The framework condition was that the system should not hinder the mobile and flexible use of a WMDS. According to the requirements placed on safety related functions by the state of the art in machine safety, the following sub research hypotheses were investigated within the feasibility analysis:

- RH1.1: The safety functions reduce the estimated risk of all identified hazards to an acceptable level.
- RH1.2: The safety functions are able to perform their intended function under all conditions as specified within the ODD of the WMDS, while not unacceptably disturbing the WMDS operation in situations uncritical to safety.
- RH1.3: The safety functions are intrinsically safe by detecting unsafe deviations from the target conditions causing failure of the functions.

The first research objective was to deduce the minimum requirements for both functions in terms of measurement variables and decision logics for a safe and usable solution. The solutions developed extend the WMDS architecture by a total of three measurement quantities (object distance, WMDS position, WMDS speed) and two logic units with a safety integrity requirement, in addition to the external emergency braking system. Thereby, a reduction of safety-relevant components was achieved in comparison to previously derived safety requirements for WMDS. In addition, through the active collision avoidance, the intervention of operators towards potential collisions is no longer required, which reduces the risk that the use of an unbound WMDS involves. Thus, a valuable addition to the WMDS architecture and its functional specification was generated in this work. Applying state of the art methods for risk evaluations of machines, a sufficient risk reduction was demonstrated. Therewith, the possibility of risk reduction of the unbound WMDS motion with an active safety system is supported (RH1.1).

The second research objective of the work was to demonstrate the feasibility of the developed concept in terms of suitable measurement systems and software components that can fulfill the previously defined requirements. The choice fell on the application of vehicle-bound environment sensor technology, which shall fulfill the object detection as well as the position and speed measurement function through the set up of artificial workspace landmarks. Among generally conceivable sensor technologies, in this work only the application of lidar sensors was investigated, as these seemed most promising due to their ability of high resolution environment scanning.

However, the actual suitability of lidar sensor technology was unknown to this state and therefore to be evaluated within the work. For the assessment, only a scaled prototype of the WMDS was available. Furthermore, the available test field posed challenges by an uneven ground.

For the *lidar and landmark based positioning system (LLLPS)*, the sensor technology as well as presented software algorithms proved to be suitable, as the identified position measurement error was below a set target and no availability drawbacks were observed even under worst case vehicle motion states and external disturbance factors. Therefore, the applied sensor hardware and software already proves to be sufficient to meet the target measurement performance and can be adopted for future applications. However, potential is seen to decrease the measurement error even more, if less reflective landmarks with a lower detection scattering are used. Concerning the speed determination, potential to reduce the measurement error through further elaboration of suitable data filters was shown. Both is to be investigated in future work. Basically, a worthful result of this work is the conclusion that an LLLPS is suitable for the application in WMDS as a system to observe the compliance with position dependent speed limitations within the *workspace compliance* function. It is further known which building blocks are needed to make this robust against safety risks. The safe fulfilment of the intended task within all conceivable situations and without undesired disturbance under situations uncritical to safety (RH1.2) is considered corroborated with the obtained results. The basic feasibility of fault detection within the LLLPS was exemplary shown, while suitable threshold values are suggested to be verified more thoroughly in the future, when a higher amount of representative data is available. Since the level of fault detection is on the processed data output, the fault detection coverage is high. Thereby, the LLLPS is considered as intrinsically safe (RH1.3).

For the *collision avoidance* function, software algorithms were found that allow identification of objects under discrimination of ground reflections or other atmospheric detections. Thus, no availability drawbacks were observed in representative maneuvers. However, for light rain, this functionality still needs to be investigated in the future. It was further shown in the experiments that even small objects with low reflectivity and cylindrical surface are generally detectable by the lidar sensors. Especially for the protection of persons from collisions, the system is considered suitable. However, the maximum detection distances are smaller than expected due to limitations in the ground detection filter caused by ground unevenness on the workspace. Thus, with the current sensor setup, the WMDS would only be allowed to operate at a limited speed, which would require further down scaling of the demanded accelerations in a driving simulation. Otherwise, a limitation for the workspace surface quality must be set, which is also in favor for a high quality driving simulation. A concrete specification of permitted unevenness, in which the present system still functions for the desired ranges, is to be investigated in the future. Else, an improvement can be expected with further software adaptions and when the WMDS is applied with the additional suspension system. Furthermore, the used sensors with 32 layers are not yet at the limit of the maximum resolution of lidar sensors. A higher resolution lidar will compensate detection losses on objects and therefore increase the object detection distance towards the required distances,

which is to be further investigated in future work. Thus, despite the observed insufficiencies of the current system, the safe fulfilment of the intended task within all conceivable operative conditions (RH1.2) is still considered feasible with the application of lidar sensors. With regard to the detection of fault conditions, measures investigating the incoming point data are required. Approaches were presented that intend to detect occlusions or misplacement of the sensor via the reference of the ground detections. The procedure for occlusion detection contains the limitation that not all sensor layers can be checked during an ongoing operation, but only those that are aligned to the ground and not additionally affected by disturbance through unevenness. Thus, the detectability of faults impeding the object detection function would also profit from a more even workspace surface. In the future, further experiments will be needed to determine the extent to which observation of the layers directed at the ground is sufficient to detect small partial occlusions on the sensor. Until then, a detectability of fault conditions for the object detection can only be confirmed to a limited extent (RH1.3).

In conclusion, the feasibility of an active safety system for WMDS using lidar sensors is not considered neglected with this work. Approaches for the collision avoidance as well as the workspace compliance function were demonstrated in their basic functionality. The position and speed determination could already fulfill all requirements with the proposed hard- and software and therefore represents a promising extension of the WMDS safety architecture. For the object detection function, the necessary software modules have been identified and proven to be fundamentally suitable, while identified limitations can potentially be solved with a higher resolution sensor and more even workspace undergrounds. The requirements for both safety functions have been precised by this work and can be considered in future designs. In addition, it is now known that an uneven workspace surface is not only disturbing for a realistic driving simulation, but also affects the collision avoidance and fault detection functions when using lidar sensors.

The results are an essential step towards safe real world experiments with WMDS and therefore further promote the applicability of the novel DS concept in the future.

A. Hazard and Risk Assessment

Table A-1.: HARA performed on behavioural level according to ISO 12100. Each hazard has a risk index larger than 1, which requires risk mitigation measures.

Identification of hazardous event			Classification of hazardous event								Safety Goal
Hazardous Event			S		F		A		O		Risk level	
Failure	Consequence	Situation		Justification		Justification		Justification		Justification		
Person / object enters WMDS workspace	Collision between WMDS and person / object	Driving simulation with test person, close to boundary, high velocity	2	Serious injury or death to at least one person	2	Driving simulation is regular application, maneuvers close to boundary appear often	2	Workspace overview might not be sufficient to detect approaching object, evasion of object hardly possible for unpredictable WMDS motion	2	Seldom occurence expected, but compliance with instructions necessary	5	The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided. The WMDS shall be stoppable at any time.
WMDS leaves its designated workspace	Collision between WMDS and person / object	Driving simulation with test person, high velocity, third persons and infrastructure outside the workspace	2	Serious injury or death to at least one person	2	Driving simulation is regular application, maneuvers close to boundary appear often	2	Workspace overview might not be sufficient to detect exceeding borders, evasion of objects hardly possible, underground condition outside might not be sufficient to brake before harm occurs	3	A single fault within any hardware or software component within the motion control and motion execution can cause the WMDS to leave its workspace	6	The WMDS shall detect failure that causes leaving its predefined workspace and initiate a braking maneuver so that the workspace limits are not exceeded. The WMDS shall be stoodable at any time
WMDS leaves its designated workspace	The WMDS turns over	Driving simulation with test person, high velocity, uneven ground / slope outside workspace	2	Serious injury or death to at least one person	2	Driving simulation is regular application, maneuvers close to boundary appear often	2	Workspace overview might not be sufficient to detect exceeding borders, evasion of objects hardly possible, underground condition outside might not be sufficient to brake before harm occurs	1	A single fault within any hardware or software component within the motion control and motion execution can cause the WMDS to leave its workspace. Nevertheless the WMDS is designed for standing stability with a safety factor, so that an actual turn over is considered not very probable	4	The WMDS shall detect failure that causes leaving its predefined workspace and initiate a braking maneuver so that the workspace limits are not exceeded. The WMDS shall be stoodable at any time

Identification of hazardous event			Classification of hazardous event												Safety Goal
Hazardous Event		Situation	S	Justification	F	Justification	A	Justification	O	Justification	Risk level	
Failure	Consequence											
Unintended start input by system operator from standstill with a following highly dynamic maneuver	Collision between WMDS and person / object	Preparation of any operational mode, persons standing in close proximity to the WMDS	2	Serious injury or death to at least one person	2	Starting of new operating modes is a regular task, preparation with persons around the vehicle are indispensable	2	Evasion of objects hardly possible	1	Operator is trained in its task	4	The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided. The WMDS shall be stoppable at any time.
Unintended operational mode: preprogrammed highly dynamic maneuver is started instead of manual drive mode	Collision between WMDS and person / object	Expected manual drive mode with persons in close proximity to WMDS	2	Serious injury or death to at least one person	2	Starting of new operating modes is a regular task, preparation with persons around the vehicle are indispensable	2	Evasion of objects hardly possible	1	Operator is trained in its task	4	The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided. The WMDS shall be stoppable at any time.
Unintended trajectory of the WMDS by functional system failure	Collision between WMDS and person	Manual drive mode with persons in proximity to the WMDS	2	Serious injury or death to at least one person	2	Manual drive mode is a frequently used task	1	Only very low speeds are driven during manual drive so that an evasion is possible under certain conditions	3	A single fault within any hardware or software component within the motion control, motion execution and external command device can cause deviating trajectories	5	The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided. The WMDS shall be stoppable at any time.
Unintended trajectory of the WMDS by erroneous inputs from the operators	Collision between WMDS and person	Manual drive mode with persons in proximity to the WMDS	2	Serious injury or death to at least one person	2	Manual drive mode is a frequently used task	1	Only very low speeds are driven during manual drive so that an evasion is possible under certain conditions	2	Operator is trained in its task but high skills and attention are required	4	The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided. The WMDS shall be stoppable at any time.

Table A-2.: HARA performed on behavioural level according to ISO 12100 with risk reevaluation after safety goals are applied. Each hazard has a risk index of 1, indicating sufficient risk mitigation.

Identification of hazardous event			Classification of hazardous event								Safety Goal
Hazardous Event		Situation	S	Justification	F	Justification	A	Justification	O	Justification	Risk level	
Failure	Consequence											
Person / object enters WMDS workspace	Collision between WMDS and person / object	Driving simulation with test person, close to boundary, high velocity	1	No or only minor injuries because of unexpected deceleration	2	Driving simulation is regular application, maneuvers close to boundary appear often	2	Workspace overview might not be sufficient to detect approaching object, evasion of object hardly possible for unpredictable WMDS motion	2	Only a fault in the detection of objects or braking can cause the WMDS to actually collide with persons	1	The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided. The WMDS shall be stoppable at any time.
WMDS leaves its designated workspace	Collision between WMDS and person / object	Driving simulation with test person, high velocity, third persons and infrastructure outside the workspace	1	No or only minor injuries because of unexpected deceleration	2	Driving simulation is regular application, maneuvers close to boundary appear often	2	Workspace overview might not be sufficient to detect exceeding borders, evasion of objects hardly possible, underground condition outside might not be sufficient to brake before harm occurs	2	Only a fault in the detection of objects or braking can cause the WMDS to actually collide with persons	1	The WMDS shall detect failure that causes leaving its predefined workspace and initiate a braking maneuver so that the workspace limits are not exceeded. The WMDS shall be stooable at any time.
WMDS leaves its designated workspace	The WMDS turns over	Driving simulation with test person, high velocity, uneven ground / slope outside workspace	1	No or only minor injuries because of unexpected deceleration	2	Driving simulation is regular application, maneuvers close to boundary appear often	2	Workspace overview might not be sufficient to detect exceeding borders, evasion of objects hardly possible, underground condition outside might not be sufficient to brake before harm occurs	2	Only a fault in the detection of objects or braking can cause the WMDS to actually collide with persons	1	The WMDS shall detect failure that causes leaving its predefined workspace and initiate a braking maneuver so that the workspace limits are not exceeded. The WMDS shall be stoppable at any time.

Identification of hazardous event			Classification of hazardous event										Safety Goal
Hazardous Event		Situation	S	Justification	F	Justification	A	Justification	O	Justification	Risk level		
Failure	Consequence												
Unintended start input by system operator from standstill with a following highly dynamic maneuver	Collision between WMDS and person / object	Preparation of any operational mode, persons standing in close proximity to the WMDS	1	No injuries	2	Starting of new operating modes is a regular task, preparation with persons around the vehicle are indispensable	2	Evasion of objects hardly possible	2	Only a fault in the detection of objects or braking can cause the WMDS to actually collide with persons	1		The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided. The WMDS shall be stoppable at any time.
Unintended operational mode: preprogrammed highly dynamic maneuver is started instead of manual drive mode	Collision between WMDS and person / object	Expected manual drive mode with persons in close proximity to WMDS	1	No injuries	2	Starting of new operating modes is a regular task, preparation with persons around the vehicle are indispensable	2	Evasion of objects hardly possible	2	Only a fault in the detection of objects or braking can cause the WMDS to actually collide with persons	1		The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided. The WMDS shall be stoppable at any time.
Unintended trajectory of the WMDS by functional system failure	Collision between WMDS and person	Manual drive mode with persons in proximity to the WMDS	1	No injuries	2	Manual drive mode is a frequently used task	1	Only very low speeds are driven during manual drive so that an evasion is possible under certain conditions	2	Only a fault in the detection of objects or braking can cause the WMDS to actually collide with persons	1		The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided. The WMDS shall be stoppable at any time.
Unintended trajectory of the WMDS by erroneous inputs from the operators	Collision between WMDS and person	Manual drive mode with persons in proximity to the WMDS	1	No injuries	2	Manual drive mode is a frequently used task	1	Only very low speeds are driven during manual drive so that an evasion is possible under certain conditions	2	Only a fault in the detection of objects or braking can cause the WMDS to actually collide with persons	1		The WMDS shall detect potential collision objects in its proximity and shall initiate a braking maneuver so that a collision is avoided. The WMDS shall be stoppable at any time.

B. Ouster Lidar Sensors

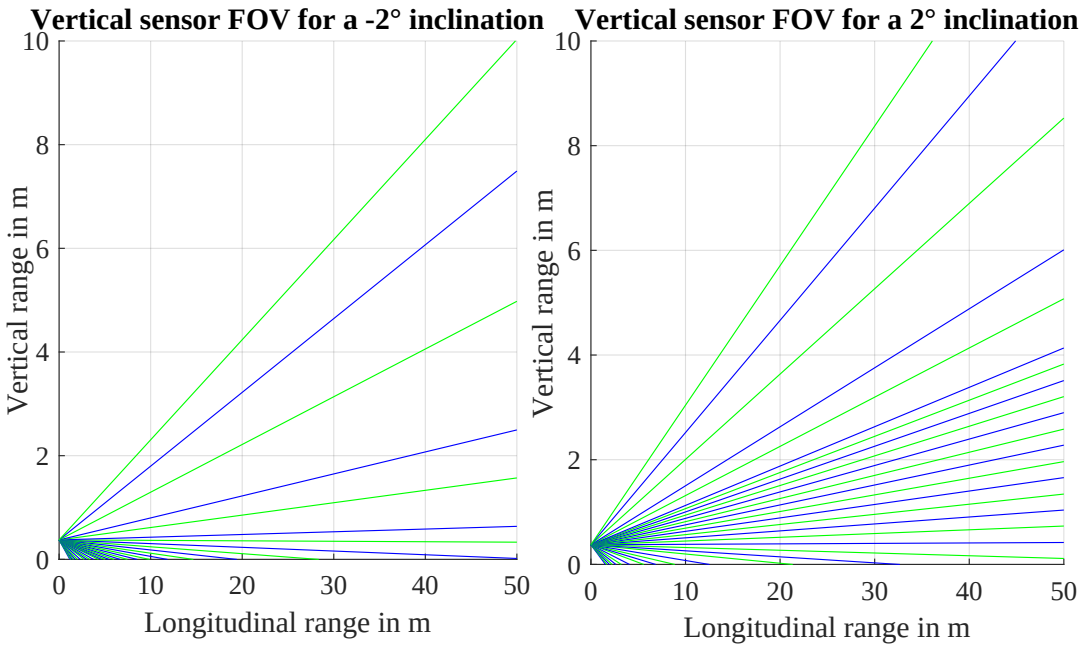


Figure B-1.: Section view of the vertical FOV of the lidar sensor for $\pm 2°$ inclination around a sensors y-axis, potentially induced by ground unevenness.

VFoV:	45	45	45	45	45	28.7	22.5	22.5	45	45	45	22.5
Description	OS1-128 Uniform	OS1-32 Uniform Column 0	OS1-32 Uniform Column 1	OS1-32 Uniform Column 2	OS1-32 Uniform Column 3	OS1-32 Gradient	OS1-32 Below Horizon Col 0,2	OS1-32 Below Horizon Col 1,3	OS1-64 Uniform Column 0,2	OS1-64 Uniform Column 1,3	OS1-64 Gradient	OS1-64 Below Horizon
+22.5	0				0					0	0	
+22.15	1			1					1			
+21.79	2		2							2		
+21.44	3	3							3			
+21.08	4				4					4		
+20.73	5			5					5			
+20.37	6		6							6		
+20.02	7	7							7			
+19.67	8				8					8	8	
+19.31	9			9					9			
+18.96	10		10							10		
+18.6	11	11							11			
+18.25	12				12					12		
+17.89	13			13					13			
+17.54	14		14							14		
+17.19	15	15							15			
+16.83	15				15					15	15	
+16.48	17			17					17			
+16.12	18		18							18		
+15.77	19	19							19			
+15.41	20				20					20		
+15.06	21			21					21			
+14.7	22		22							22		
+14.35	23	23							23			
+14	24				24					24	24	
+13.64	25			25					25			
+13.29	26		26							26		
+12.93	27	27				27			27			
+12.58	28				28					28	28	
+12.22	29			29					29			
+11.87	30		30							30		
+11.52	31	31							31			
+11.16	32				32					32	32	
+10.81	33			33					33			
+10.45	34		34							34		
+10.1	35	35				35			35			
+9.74	36				36					36	36	
+9.39	37			37					37			
+9.04	38		38							38	38	
+8.68	39	39							39			
+8.33	40				40					40	40	
+7.97	41			41					41			
+7.62	42		42							42	42	
+7.26	43	43				43			43			
+6.91	44				44					44	44	
+6.56	45			45					45			
+6.2	46		46							46	46	
+5.85	47	47							47			
+5.49	48				48					48	48	
+5.14	49			49					49			
+4.78	50		50							50	50	
+4.43	51	51				51			51			
+4.07	52				52					52	52	
+3.72	53			53					53		53	
+3.37	54		54			54				54	54	
+3.01	55	55							55		55	
+2.66	56				56					56	56	
+2.3	57			57		57			57		57	
+1.95	58		58			58				58	58	
+1.59	59	59				59			59		59	
+1.24	60				60	60				60	60	
+0.89	61			61		61			61		61	
+0.53	62		62			62				62	62	
+0.18	63	63				63			63		63	
-0.18	64				64	64		64		64	64	64
-0.53	65			65		65	65		65		65	65
-0.89	66		66			66		66		66	66	66
-1.24	67	67				67	67		67		67	67
-1.59	68				68	68		68		68	68	68
-1.95	69			69		69	69		69		69	69
-2.3	70		70			70		70		70	70	70
-2.66	71	71				71	71		71		71	71
-3.01	72				72	72		72		72	72	72
-3.37	73			73			73		73		73	73
-3.72	74		74			74		74		74	74	74
-4.07	75	75					75		75		75	75
-4.43	76				76	76		76		76	76	76
-4.78	77			77			77		77		77	77
-5.14	78		78			78		78		78	78	78
-5.49	79	79					79		79		79	79
-5.85	80				80	80		80		80	80	80
-6.2	81			81			81		81		81	81
-6.56	82		82					82		82	82	82
-6.91	83	83					83		83		83	83
-7.26	84				84	84		84		84	84	84
-7.62	85			85			85		85		85	85
-7.97	86		86					86		86	86	86
-8.33	87	87					87		87		87	87
-8.68	88				88	88		88		88	88	88
-9.04	89			89			89		89		89	89
-9.39	90		90					90		90	90	90
-9.74	91	91					91		91		91	91
-10.1	92				92	92		92		92	92	92
-10.45	93			93			93		93		93	93
-10.81	94		94					94		94	94	94
-11.16	95	95					95		95		95	95
-11.52	96				96	96		96		96	96	96
-11.87	97			97			97		97		97	97
-12.22	98		98					98		98	98	98
-12.58	99	99					99		99		99	99
-12.93	100				100	100		100		100		100
-13.29	101			101			101		101		101	101
-13.64	102		102					102		102		102
-14	103	103					103		103		103	103
-14.35	104				104	104		104		104		104
-14.7	105			105			105		105			105
-15.06	106		106					106		106		106
-15.41	107	107					107		107		107	107
-15.77	108				108	108		108		108		108
-16.12	109			109			109		109			109
-16.48	110		110					110		110		110
-16.83	111	111					111		111		111	111

Figure B-2.: Beam spacing of the lidar sensor Ouster OS1 Gen2 32 layers gradient.

C. LLLPS Development

Impact of the Motion Scan Effect

The distortion of landmark detection by translational motion only scales with the driving speed and is independent of the distance of a landmark. Assuming a maximum translational speed of $10\,\mathrm{m/s}$ of the WMDS and a scan period time of $0.05\,\mathrm{s}$ at $20\,\mathrm{Hz}$ sensor rotation rate, a worst case distortion, by means of a second detection of a landmark displaced by Δx_{LM}, amounts to:

$$\Delta x_{\mathrm{LM}} = v_{\mathrm{DS,max}} \cdot \tau_{\mathrm{scan}} = 10\,\mathrm{m/s} \cdot 0.05\,\mathrm{s} = 0.5\,\mathrm{m} \tag{C-1}$$

This is less than the diameter of a landmark and will therefore not create two separate clusters, but probably shift the estimated landmark center.

The distortion by rotational motion scales with the rotational speed and additionally linearly with the distance of a landmark towards the sensors. Assuming a worst case rotational speed of $100\,^{\circ}/\mathrm{s}$ of the WMDS and a distance towards the landmarks of $25\,\mathrm{m}$, which is the case when the WMDS is in the center position of the workspace at Griesheim Airfield. A worst case distortion by means of a second detection of a displaced landmark amounts to:

$$\Delta x_{\mathrm{LM}} = 2\ \sin(\frac{\dot{\psi}_{\mathrm{DS,max}} \tau_{\mathrm{scan}}}{2})\ d_{\mathrm{LM}} = 2\ \sin(\frac{100\,^{\circ}/\mathrm{s}\ 0.05\,\mathrm{s}}{2})\ 20\,\mathrm{m} = 2.18\,\mathrm{m} \tag{C-2}$$

This underlines the dominant influence of rotational motion of the WMDS towards the motion scan effect. When the WMDS is placed at the border of the motion space, the displacement of a landmark is even greater.

Sensor Phase Synchronization[118]

This measure aims to optimize the scan behavior by adjusting the phase offset between the lidar beams. This influences the time required for a 360° scan and the number and strength of the transition zones. Two different phase configurations were considered, shown in Fig. C-1.

In the *aligned configuration*, the beams of the three lidars rotate in parallel using a phase offset of 120° to each other. Thereby, the points in the transition areas are recorded with a minimal time offset. The advantage is that only one distinct time transition zone exists, similar to a single sensor. The disadvantage is that a potential blind spot occurs at this transition zone when the vehicle rotates against the scan direction. Also, a complete point cloud requires the full rotation time of the lidars.

[118] Lutwitzi, M. et al.: Lidar and Landmark based Positioning System for WMDS (2022).

In the *synchronized configuration*, all phase offsets are set to zero. This results in three extended time transition zones at the overlaps of the scan areas. However, the total time needed to acquire the full point cloud is halved, resulting in a reduction of the overall distortion. This configuration can benefit from the reduced scan acquisition time and has no blind spot, which is why it is implemented in the final system.

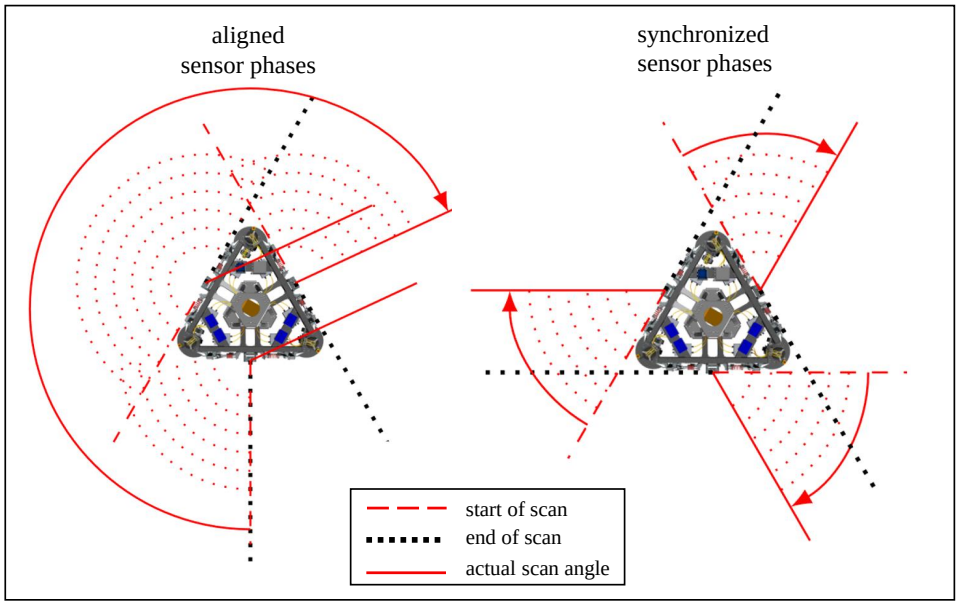
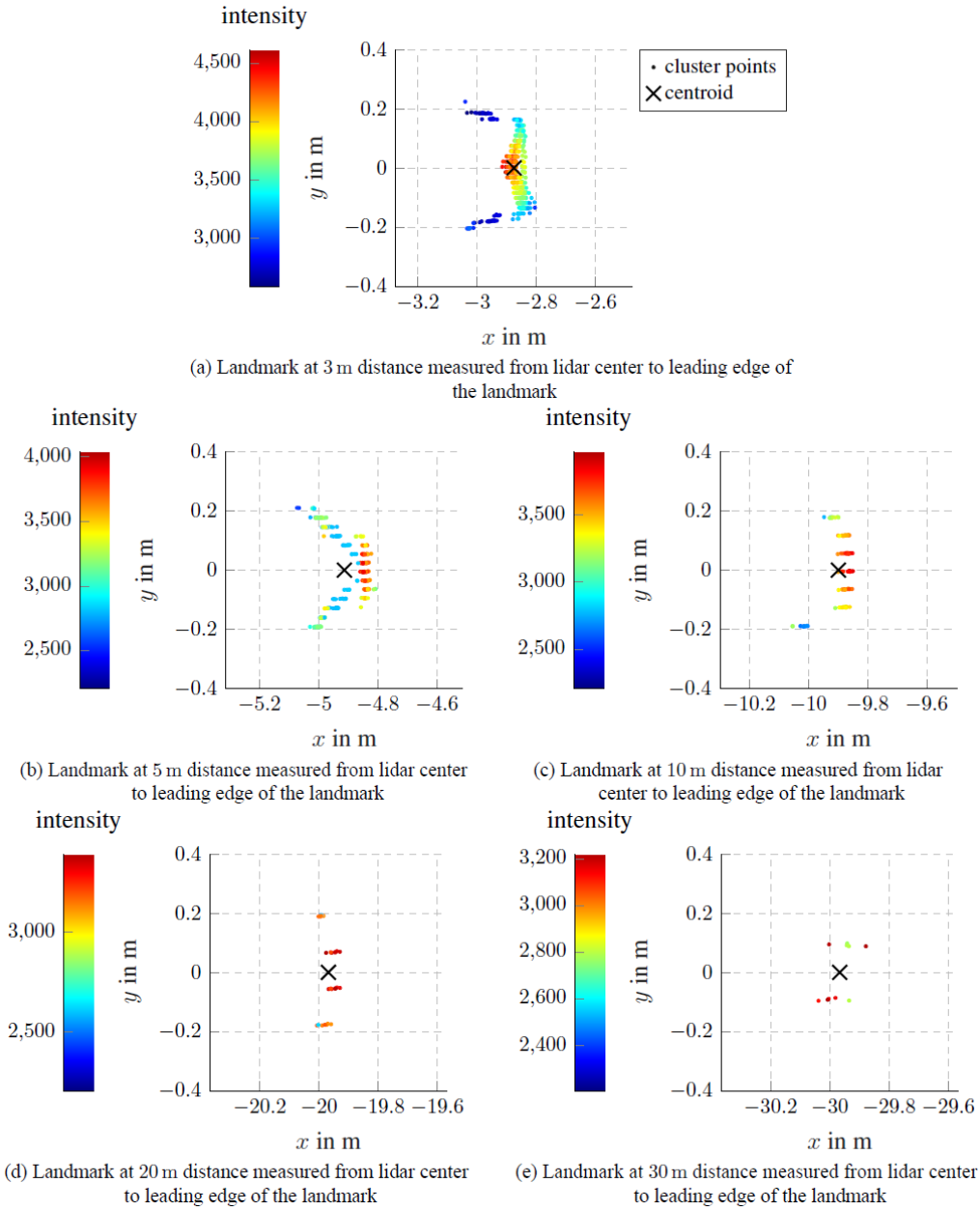


Figure C-1.: Left: Aligned sensor configuration. Right: Synchronized sensor configuration.

Cluster Centroids in Dependence of Detection Distance



(a) Landmark at 3 m distance measured from lidar center to leading edge of the landmark

(b) Landmark at 5 m distance measured from lidar center to leading edge of the landmark

(c) Landmark at 10 m distance measured from lidar center to leading edge of the landmark

(d) Landmark at 20 m distance measured from lidar center to leading edge of the landmark

(e) Landmark at 30 m distance measured from lidar center to leading edge of the landmark

Figure C-2.: Landmark cluster centroids in dependence of the distance of the sensor towards the retroreflective targets. The centroids extrude towards the cylinder surface, while the effect is stronger the closer the sensor is towards the landmark.[119]

[119] Betschinske, D.: Master Thesis, Position Determination with Lidar Sensors for WMDS (2022) p. 129.

LLLPS Timing

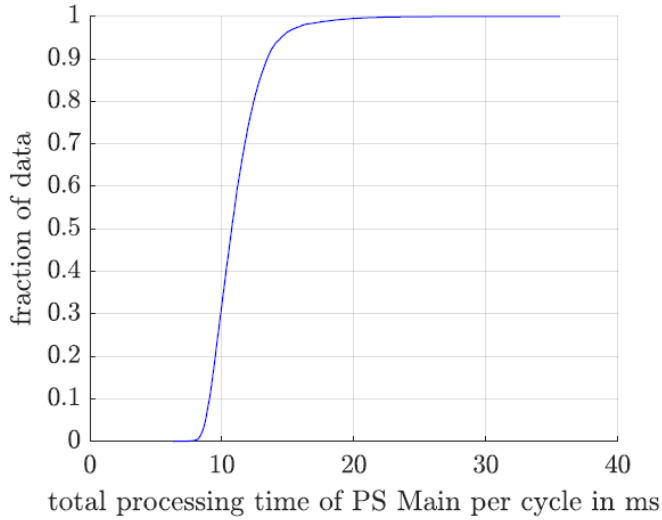


Figure C-3.: Run time of overall LLLPS algorithm during dynamic drive.[120a]

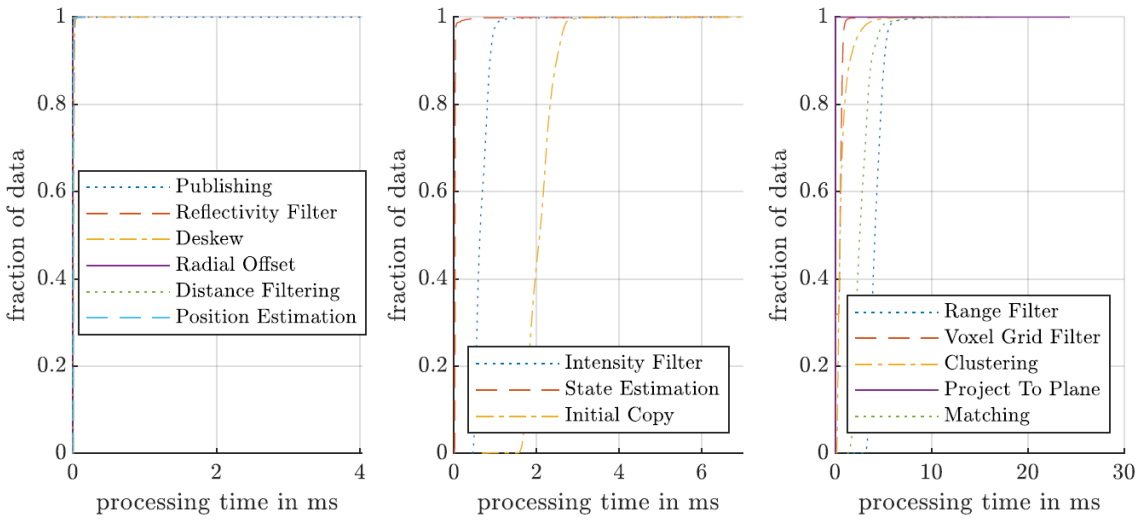


Figure C-4.: Run time of different steps in the LLLPS algorithm during the dynamic drive.[120b]

[120] Betschinske, D.: Master Thesis, Position Determination with Lidar Sensors for WMDS (2022) a: p. 96, b: 137.

Impact of Filter Application to Position and Speed Data

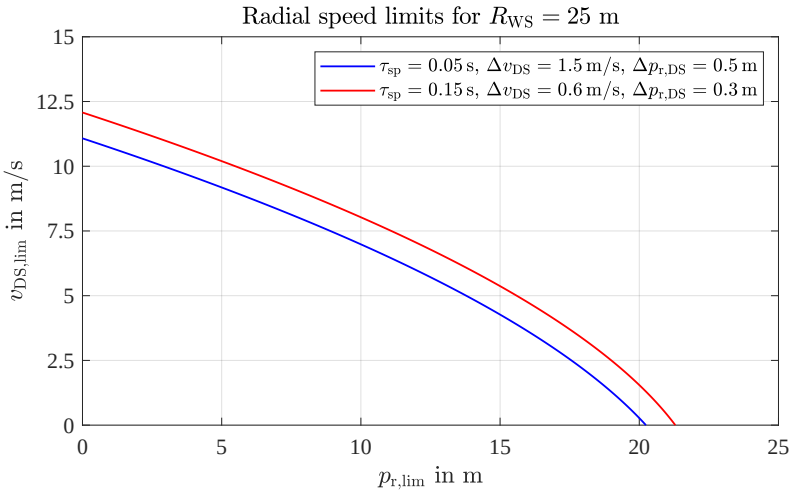


Figure C-5.: Impact of applying a moving average filter (3) to the position and speed data on the resulting radial speed limits. With the filter applied, despite the increased reaction time, the workspace usability is greater and therefore in favor.

D. Object Detection Development

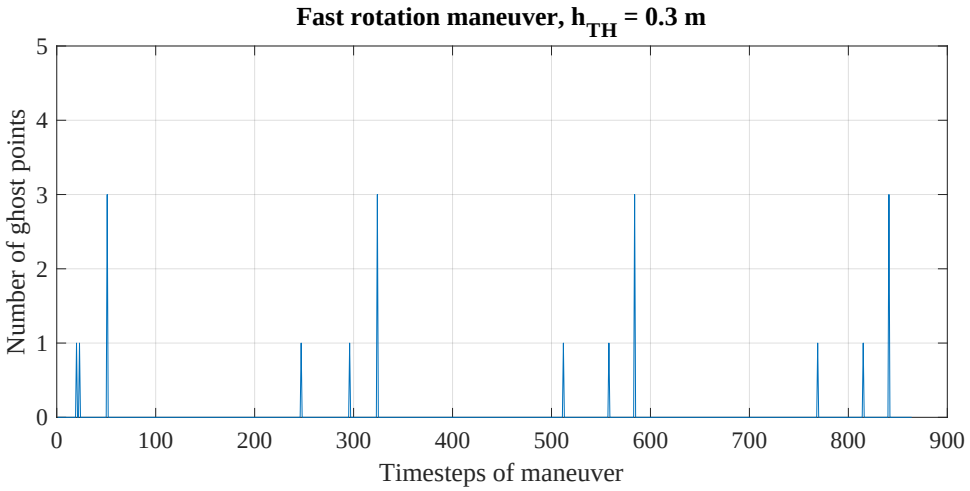


Figure D-1.: Number of points appearing in a cleared PZ during rotation after all points up to 0.3 m above the ground are filtered.

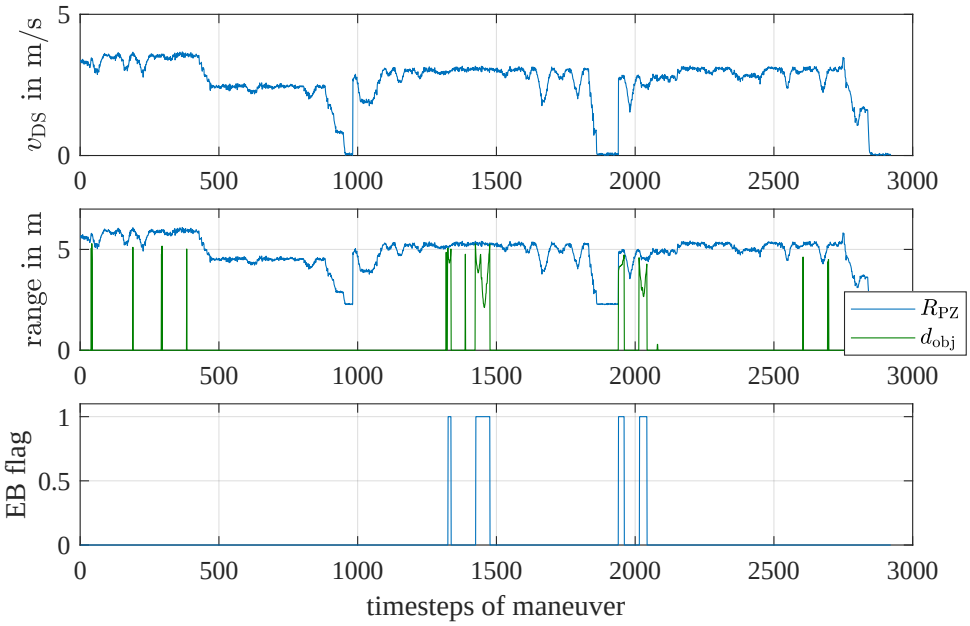


Figure D-2.: Object detection evaluation within the dynamic drive maneuver for $h_{\mathrm{TH,in}} = 0.06\,\mathrm{m}$, $n_{\mathrm{cyc,multi}} = 3$ and $n_{\mathrm{v}} = 2$. False positive object detections are visible by measured object distances appearing for single timesteps, but do not lead to an emergency brake flag.

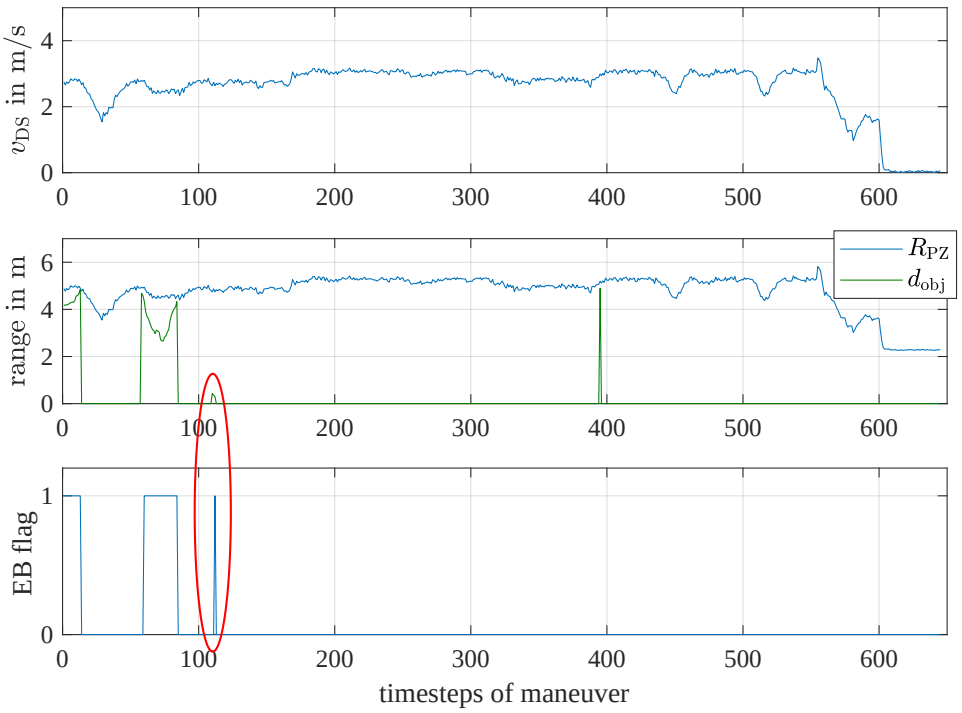


Figure D-3.: Object detection evaluation within the last third of the dynamic drive maneuver for an increased inlier threshold of $h_{\mathrm{TH,in}} = 0.12\,\mathrm{m}$, $n_{\mathrm{cyc,multi}} = 3$ and a reduced minimum cluster size of $n_{\mathrm{v}} = 1$. A false positive emergency brake trigger is set (red circle).

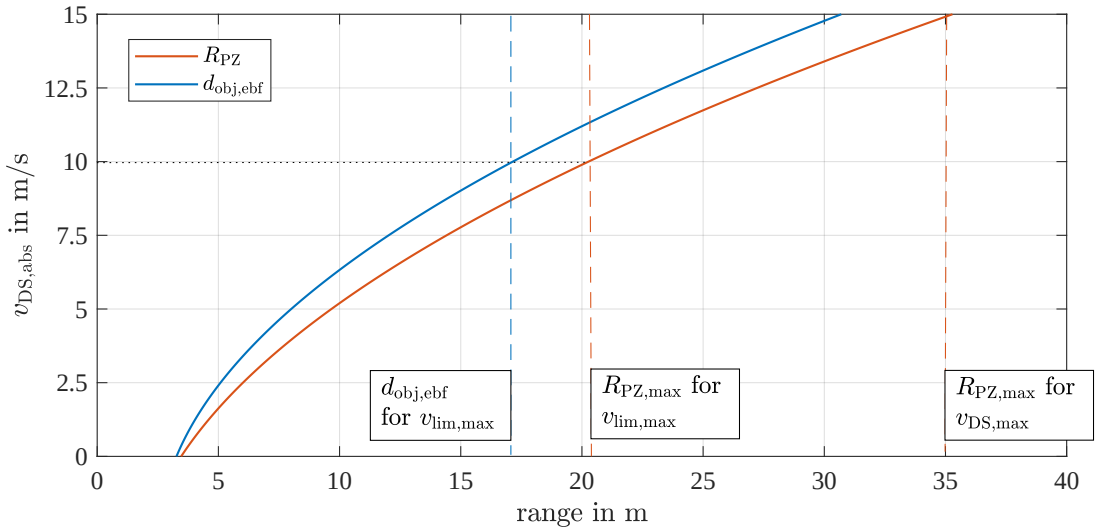


Figure D-4.: Revised PZ dimensions for the extended reaction time due to the multidetection check. Also indicated is the distance of an object, at which the emergency brake flag (ebf) must trigger at the latest to avoid a collision.

E. Fault Detection

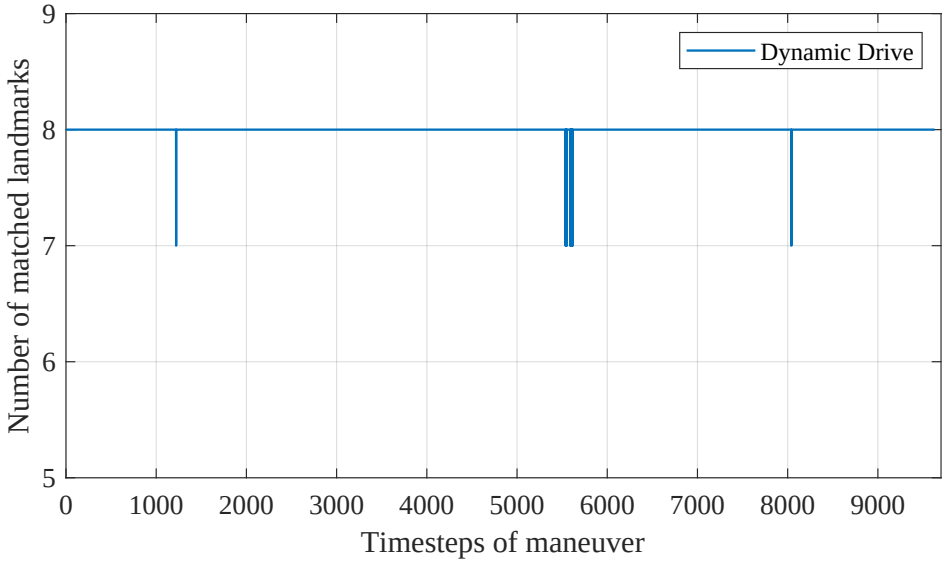


Figure E-1.: Macthed landmarks during the representative dynamic drive. Only 4 occasional losses of one landmark occur.

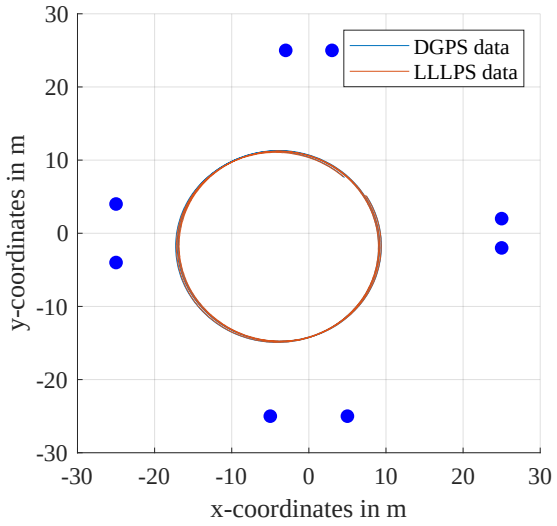


Figure E-2.: Circle drive trajectory on a non concentric workspace position. Used to evaluate the mean matching residual and position deviation in dependence on varying distances towards landmarks.

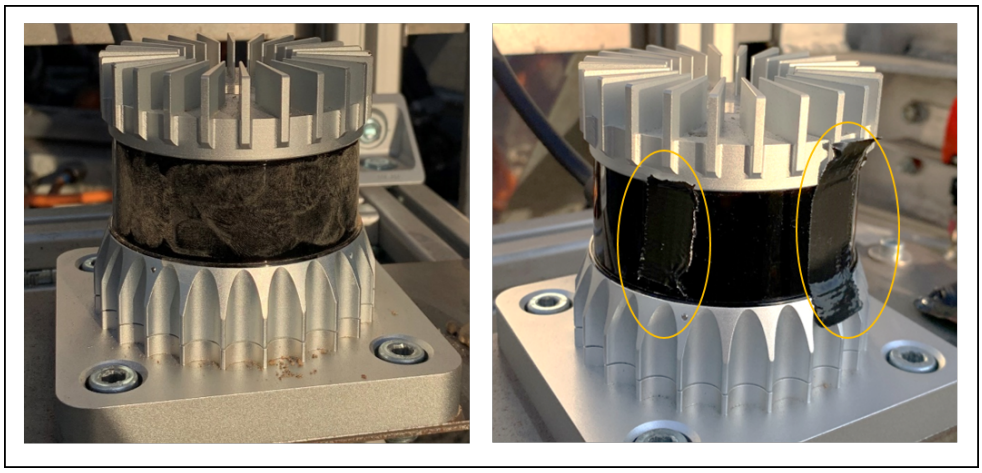


Figure E-3.: Sensor cover occlusion. Left: by dust. Right: by two stripes of tape.

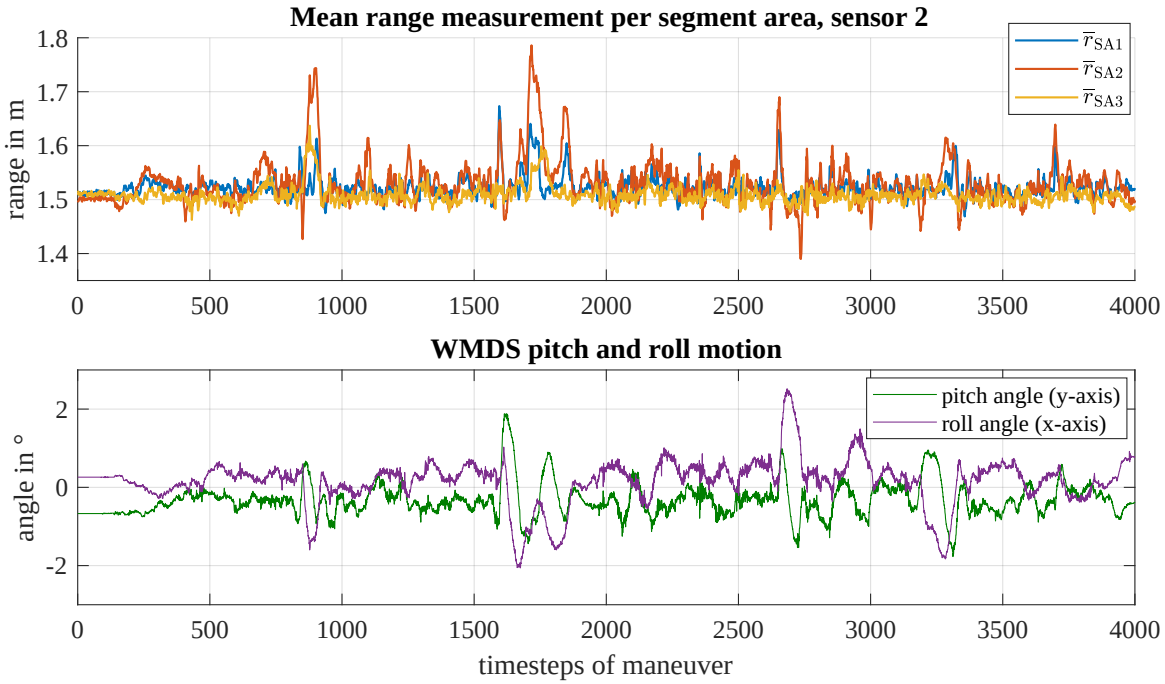


Figure E-4.: Mean range measurement per segment area during the first third of the representative dynamic drive for sensor 2. The timely correlated measurement of the WMDS' pitch and roll angle indicate that the range peaks stem from vehicle inclinations.

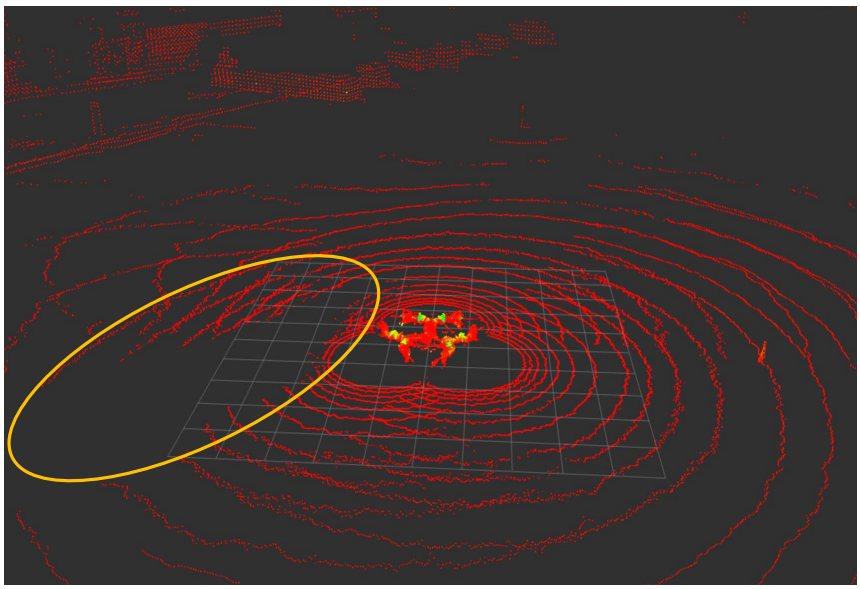


Figure E-5.: Ground detection gaps are created by water accumulations on the ground, indicated by the yellow circle.

F. Evaluation

Influence of high yaw rates on horizontal gap between two segments

For a rotation rate of 20 Hz and a segment number of 1024 per 360°, the time passed between two emitted segment beams amounts to:

$$t_{\text{seg}} = \frac{1}{20\text{Hz} \cdot 1024} = 5 \cdot 10^{-4}\text{s} \tag{F-1}$$

For a yaw rate of $\dot{\psi}_{\text{DS}} = 100$ °/s, the relative speed towards an object in a distance of $d_{\text{obj}} = 30\,\text{m}$ amounts to:

$$v_{\text{rel}} = \dot{\psi} \cdot d_{\text{obj}} \cdot 2\pi/360 = 52.36\text{m/s} \tag{F-2}$$

When the sensor rotates in the same direction as the vehicle, the gap between two segments w_{seg} is broadened by:

$$\Delta w_{\text{seg}} = v_{\text{rel}} \cdot t_{\text{seg}} = 0.0025\,\text{m} \tag{F-3}$$

Influence of Pitch and Roll Motion on Object Detection

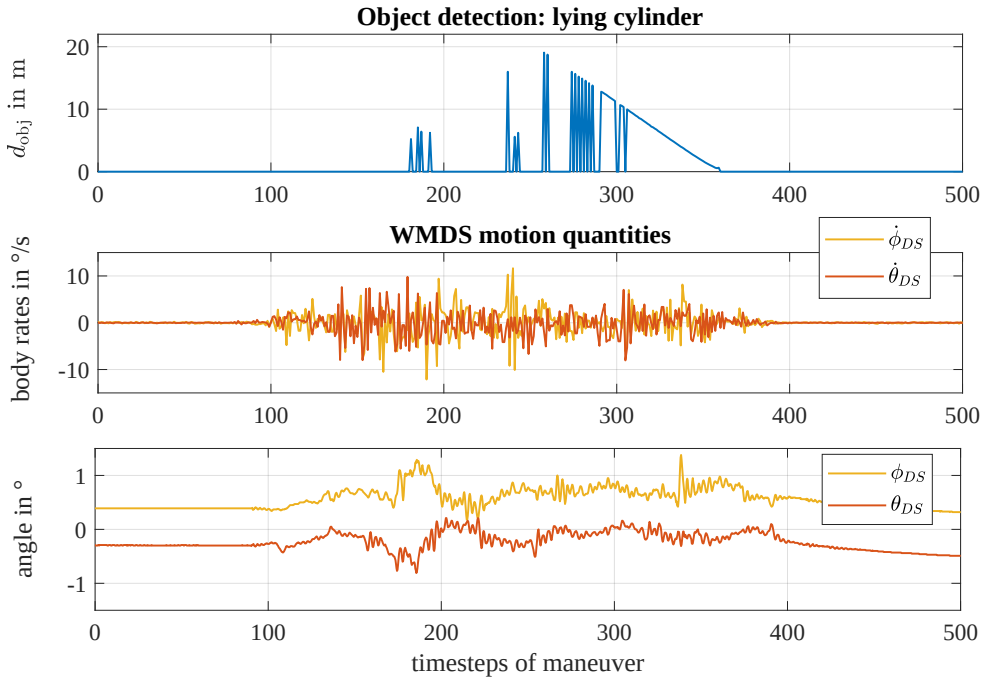


Figure F-1.: Approach of the horizontal cylinder with approx. 4 m/s. Pitch and roll rates and angles are referenced to the WMDS coordinate system, which does not correspond the sensors coordinate system. The first peaks in the object detection distance correspond to false positives, which only appear for single timesteps and therefore do not trigger the emergency brake. At the same time, peaks in pitch and roll angles and rates are visible. After 250 timesteps, the object is detected for the first time, but is lost shortly afterwards. The object losses shortly before and shortly after 300 timesteps show temporal correlating peaks in the pitch rate.

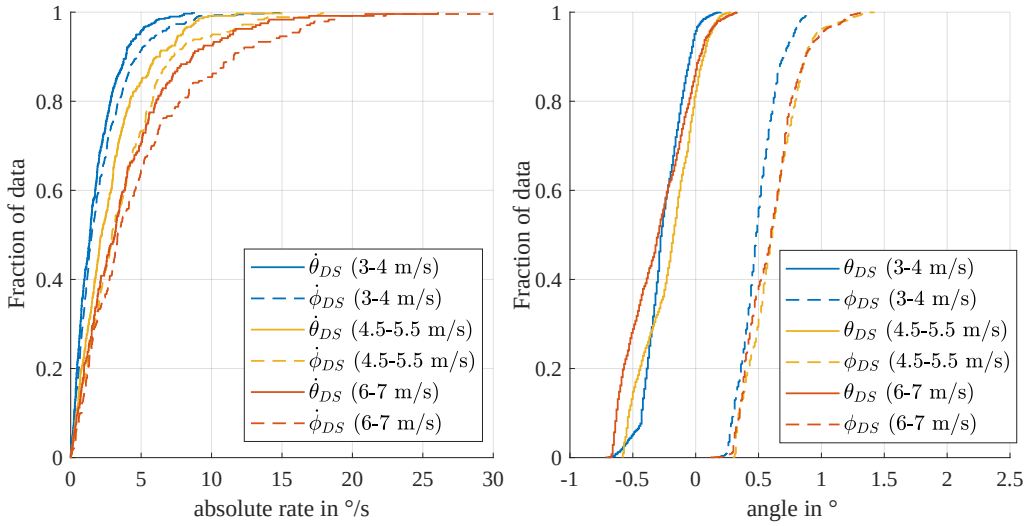


Figure F-2.: WMDS body rates and angles, referenced to the WMDS coordinate system, during object approaches.

Estimation of Required Sensor Resolution

For a full scale object detection range, complying with a WMDS speed of 15 m/s, the maximum PZ amounts to 35 m (cf. Fig. D-4). It is demanded, that at least from this distance, a consistent object detection is possible. The required resolution for the minimum object height and object width is extrapolated using the smallest distance of a consistent detection determined in the experiments for the given resolution.

An object of minimum width (standing cylinder), created a consistent ebf from a minimum distance of 16 m (cf. Fig. 8-8) with an azimuth sensor resolution of 0.35°. This means a consistent object detection started two timesteps earlier at approx. 17 m. For a detection distance of 35 m, the following azimuth resolution requirement $\Delta\Phi_\mathrm{s}$ is estimated:

$$\sin(\Delta\Phi_\mathrm{s}) = \frac{17}{35} \cdot \sin(0.35°)\Delta\Phi_\mathrm{s} = 0.17° \tag{F-4}$$

This requires a segmentation of slightly above 2048 segments per 360° scan.

The vertical beam structure also has a resolution of $0.35°$ in the area close to the ground. Without the presence of unevenness, the requirement of 0.17° also applies for the vertical resolution. However, an object of minimum height (lying cylinder), created a consistent ebf only from a minimum distance of 8 m with a vertical resolution of 0.35°. This means a consistent object detection started at approx. 9 m. Extrapolating this to a distance of 35 m requires a resolution increase by 3.8 times, meaning a vertical resolution $\Delta\theta_\mathrm{s}$ of approximately $0.1°$.

To enable a safe object detection of minimum height in the range for the limited speed of $10\,\mathrm{m/s}$, a consistent detection is required from at least 20 m. This requires a resolution increase by approximately 2.2 times, which applies to $\Delta\theta_\mathrm{s} = 0.16°$.

Fast rotation and Fast Translation

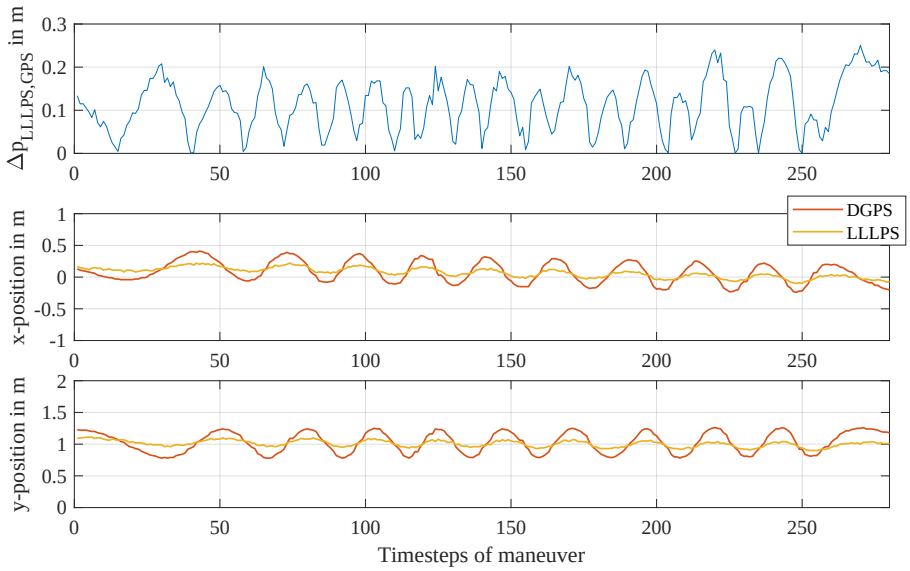


Figure F-3.: Fast rotation maneuver: The position deviation between DGPS and LLLPS reaches maximum values of approximately 0.25 m, but oscillates around 0.1 m. The GPS position measurement is not correctly referenced to the WMDS center and therefore oscillates with the vehicle rotation. Therefore, the maximum position measurement deviation between DGPS and LLLPS is considered to be smaller than the determined maximum value of 0.25 m

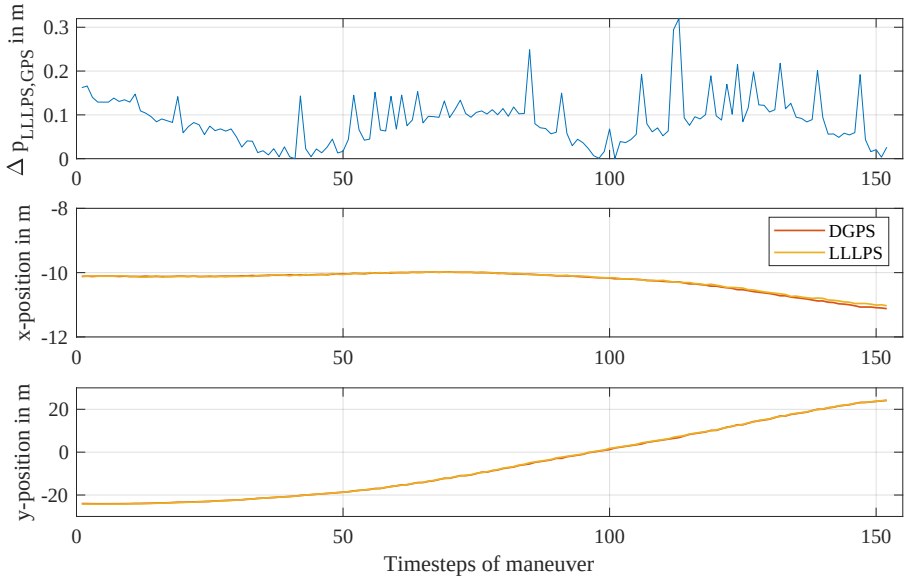


Figure F-4.: Fast translation maneuver: The position deviation between DGPS and LLLPS reaches maximum values of approximately 0.32 m.

Estimation of Possible Workspace Increase

Fig. F-5 illustrates the workspace and the most critical WMDS position for a minimum required number of 4 visible landmarks. This is the case for a position where 2 landmarks have a larger distance than the workspace radius. The maximum distance towards a landmark is indicated as $d_{\mathrm{LM,max}}$. Assuming that the maximum possible landmark distance to be detectable by the sensors is 50 m, solving for R_{WS} yields the following:

$$d_{\mathrm{LM,max}} = \sqrt{R_{\mathrm{WS}}^2 + R_{\mathrm{MS}}^2} = \sqrt{R_{\mathrm{WS}}^2 + (R_{\mathrm{WS}} - 4\,\mathrm{m})^2} = 50\,\mathrm{m} \tag{F-5}$$

$$R_{\mathrm{WS}} = 37.3\,\mathrm{m} \tag{F-6}$$

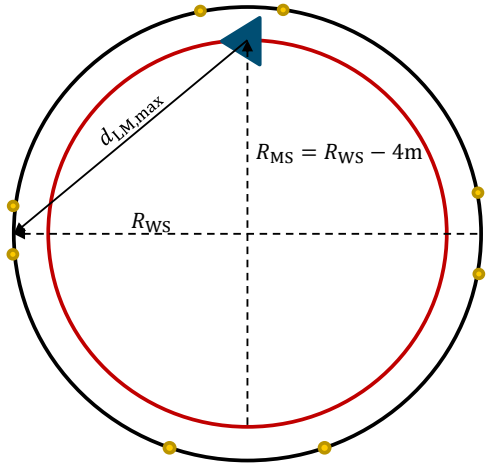


Figure F-5.: Geometric investigation of possible workspace increase: Critical workspace position for a minimum required number of 4 visible landmarks and resulting maximum landmark distance.

Additional Targets Disturbance

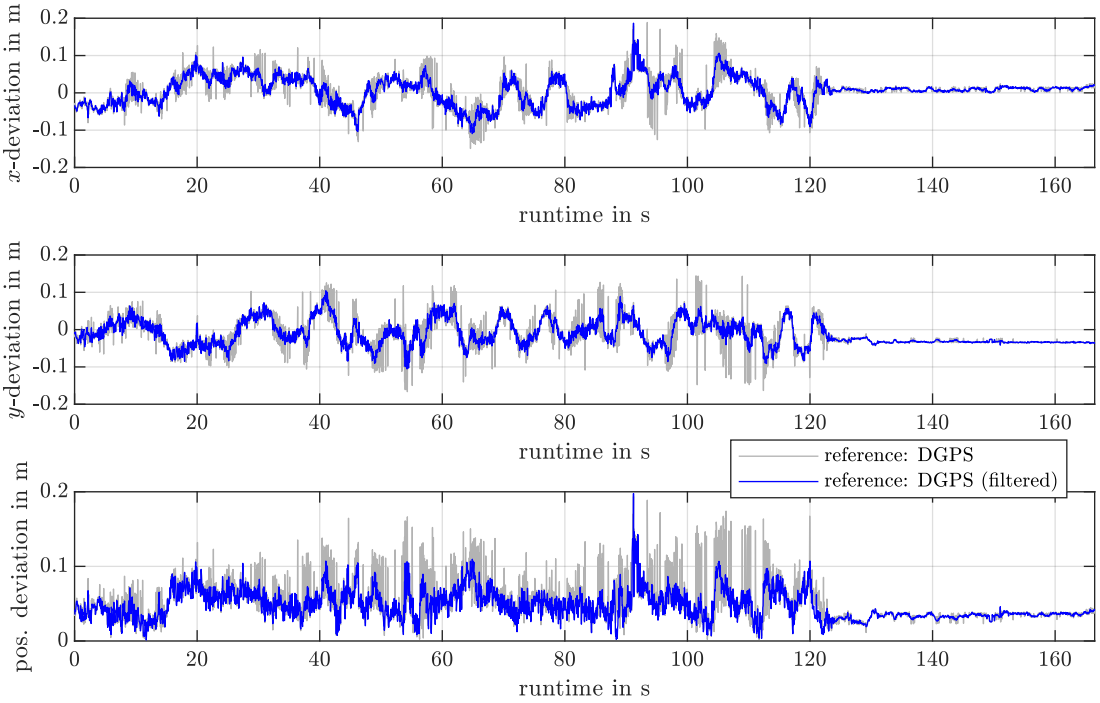


Figure F-6.: Position deviation towards DGPS for filtered and unfiltered position data during a dynamic drive with additional retroreflective targets around the workspace. A peak is visible at approx. 90 s, which is where a detected disturbance object is merged with a landmark cluster and therefore falsifies the landmark center estimation. [121]

[121] Betschinske, D.: Master Thesis, Position Determination with Lidar Sensors for WMDS (2022) p. 139.

Bibliography

2006/42/EC: Machinery Directive (2006)
2006/42/EC: Directive 2006/42/EC of the European Parliament and of the Council, 2006

Albrecht, T. et al.: Design and Challenges of WMDS (2021)
Albrecht, Torben; Ottensmeier, Meike; Chen, Xing; Plaettner, Stefan; Lutwitzi, Melina; Roßmeier, Willy; Zöller, Chris; Tüschen, Thomas; Winner, Hermann; Prokop, Günther: Rolling out a new Driving Simulator Concept - Design and Challenges of Wheeled Mobile Driving Simulators, in: Proceedings of the Driving Simulation Conference 2021 Europe VR. Munich, Germany, pp. 123–130, 2021

Berthoz, A. et al.: Motion Scaling for High-Performance Driving Simulators (2013)
Berthoz, A.; Bles, W.; Bulthoff, H. H.; Correia Gracio, B. J.; Feenstra, P.; Filliard, N.; Huhne, R.; Kemeny, A.; Mayrhofer, M.; Mulder, M.; Nusseck, H. G.; Pretto, P.; Reymond, G.; Schlusselberger, R.; Schwandtner, J.; Teufel, H.; Vailleau, B.; van Paassen, M. M.; Vidal, M.; Wentink, M.: Motion Scaling for High-Performance Driving Simulators, in: IEEE Transactions on Human-Machine Systems, Vol. 43, pp. 265–276, 2013

Betschinske, D.: Master Thesis, Master Thesis, Position Determination with Lidar Sensors for WMDS (2022)
Betschinske, Daniel: Development of a Position Determination Function for a Highly Dynamic Wheeled Driving Simulator Using Lidar Sensors, Dissertation Technical University Darmstadt, 2022

Betz, A.: Feasibility and design of WMDS (2015)
Betz, Alexander: Feasibility analysis and design of wheeled mobile driving simulators for urban traffic simulation, Fortschritt-Berichte VDI Reihe 12, Verkehrstechnik, Fahrzeugtechnik, Als Ms. gedr. Auflage, Vol. 786, VDI-Verlag, 2015

Betz, A. et al.: Development and Validation of a Safety Architecture of a WMDS (2014)
Betz, Alexander; Wagner, Paul; Albrecht, Torben; Winner, Hermann: Development and Validation of a Safety Architecture of a Wheeled Mobile Driving Simulator, in: Kemeny, Andras; Espié, Stéphane; Mérienne, Frédéric (Eds.): Proceedings of the Driving Simulation Conference Europe 2014 (DSC), 2014

BMW PressClub Global: The new BMW Driving Simulation Center (2020)
BMW PressClub Global: BMW Group sets new standards for driving simulation - NEXTGen 2020 offers exclusive insights before the new Driving Simulation Centre starts work. URL: https://www.press.bmwgroup.com/global/article/detail/T0320021EN/bmw-group-sets-new-standards-for-driving-simulation-nextgen-2020-offers-exclusive-insights-before-the-new-driving-simulation-centre-starts-work?language=en, 2020, visited on 01/04/2022

Boer, E. R.; Penna, M. D.; Utz, H.; Pedersen, L.; Siehuis, M.: The role of DS in developing AV (2015)
Boer, Erwin R.; Penna, Mauro D.; Utz, Hans; Pedersen, Liam; Siehuis, Maarten: The role of driving simulators in developing and evaluating autonomous vehicles, 2015

Borenstein, J. et al.: Mobile robot positioning: Sensors and techniques (1997)
Borenstein, J.; Everett, H. R.; Feng, L.; Wehe, D.: Mobile robot positioning: Sensors and techniques, in: Journal of Robotic Systems, Vol. 14, pp. 231–249, 1997

Coors, F. et al.: Advanced Design Project, Virtuelle Fahrszenarien für WMDS (2021)
Coors, Florian; Schellhaas, David; Beren, Katharina von; Wenzel, Lisa; Zukowski, Jan: Entwicklung von virtuellen Fahrszenarien zur Validierung eines reifengebundenen, mobilen Fahrsimulators, Advanced Design Project, Technische Universität Darmstadt, 2021

Deutscher Wetterdienst: Glossar - Niederschlagsintensität (2022)
Deutscher Wetterdienst: Wetter und Klima - Deutscher Wetterdienst - Glossar - N - Niederschlagsintensität, URL: https://www.dwd.de/DE/service/lexikon/Functions/glossar.html?nn=103346&lv2=101812&lv3=101906, 2022, visited on 06/27/2022

Donges, E.: Fahrsimulator (2001)
Donges, Edmund: Fahrsimulator, Bayrische Motoren Werke AG, Patent DE000010106150A1, Patent application number: 101 06 150.1, 2001

Ester, M. et al.: A Density-Based Algorithm for Discovering Clusters (1996)
Ester, Martin; Kriegel, Hans-Peter; Sander, Jörg; Xu, Xiaowei: A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise, in: Proceedings of the Second International Conference on Knowledge Discovery and Data Mining, pp. 226–231, 1996

Filgueira, A. et al.: Quantifying the influence of rain in LiDAR performance (2017)
Filgueira, A.; González-Jorge, H.; Lagüela, S.; Díaz-Vilariño, L.; Arias, P.: Quantifying the influence of rain in LiDAR performance, in: Measurement, Vol. 95, pp. 143–148, 2017

Fischler, M. A. et al.: Random sample consensus (1981)
Fischler, Martin A.; Bolles, Robert C.: Random sample consensus, in: Communications of the ACM, Vol. 24, pp. 381–395, 1981

GeneSys Offenburg: ADMA data sheet (2022)
GeneSys Offenburg: ADMA Automotive Dynamic Motion Analyzer with 1000 Hz Data Sheet, URL: https://genesys-offenburg.de/wp-content/uploads/2021/10/ProdDescr_ADMA_rel_09.2020.pdf, 2022, visited on 07/06/2022

Goelles, T. et al.: FDIIR Methods for Automotive Perception Sensors (2020)
Goelles, Thomas; Schlager, Birgit; Muckenhuber, Stefan: Fault Detection, Isolation, Identification and Recovery (FDIIR) Methods for Automotive Perception Sensors Including a Detailed Literature Survey for Lidar, in: Sensors, Vol. 20, 2020

Gotzig, H. et al.: Automotive LIDAR (2016)
Gotzig, Heinrich; Geduld, Georg: Automotive LIDAR, in: Winner, Hermann (Hrsg.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, 2016

Graupner, M.: Bachelor Thesis, Stadtparcours (2011)
Graupner, Maren: Entwicklung eines repräsentativen Stadtparcours mittels makroskopischer Betrachtung lokaler Verkehrsbereiche, Bachelor Thesis, Technische Universität Darmstadt, 2011

Gresek, P. M.: Bachelor Thesis, Collision Protection with Lidar for WMDS (2022)
Gresek, Philipp Michael: Further Development of a Collision Protection Function using Lidar Sensors for Wheeled Mobile Driving Simulators, Bachelor Thesis, Technical University Darmstadt Darmstadt, 2022

He, L. et al.: De-Skewing LiDAR Scan for Refinement of Local Mapping (2020)
He, Lei; Jin, Zhe; Gao, Zhenhai: De-Skewing LiDAR Scan for Refinement of Local Mapping, in: Sensors (Basel, Switzerland), Vol. 20, 2020

IEC: IEC 61025:2006 - Fault Tree Analysis (FTA) (2006)
IEC: IEC 61025:2006 - Fault Tree Analysis (FTA), 2006

IEC: IEC 61496-1:2020 - Safety of machinery - Electro-sensitive protective equipment (2020)
IEC: IEC 61496-1:2020 - Safety of machinery - Electro-sensitive protective equipment - Part 1: General requirements and tests, 2020

IEC: IEC 61508-1:2010 - Functional safety of E/E/PE systems (2010)
IEC: IEC 61508-1:2010 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General Requirements, 2010

IEC: IEC 61508-4:2010 - Functional safety of E/E/PE systems - definitions (2010)
IEC: IEC 61508-4:2010 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations, 2010

IEC: IEC 61882:2017 - HAZOP application guide (2017)
IEC: IEC 61882:2017 - Hazard and operability studies (HAZOP studies) - Application guide, 2017

IEEE 1588: Precision Clock Synchronization Protocol (2008)
IEEE 1588: IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, in: IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002), pp. 1–269, 2008

Institute of Automotive Engineering Darmstadt (FZD): Research Project: MORPHEUS (2022)
Institute of Automotive Engineering Darmstadt (FZD): Research Project MORPHEUS: Application Potential of Wheeled Mobile Driving Simulators, URL: https://www.fzd.tu-darmstadt.de/forschung/research_projects_fzd/morpheus_1/index.en.jsp, 2022, visited on 07/06/2022

Isermann, R.: Fault-diagnosis systems (2006)
Isermann, Rolf: Fault-diagnosis systems: An introduction from fault detection to fault tolerance, Springer, 2006

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

ISO: ISO 13849-1:2015 - Safety-related parts of control systems (2015)
ISO: ISO 13849-1:2015 - Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design, 2015

ISO : ISO 13849-2:2012 - Safety-related parts of control systems - Validation (2012)
ISO : ISO 13849-2:2012 - Safety of machinery - Safety-related parts of control systems - Part 2: Validation, 2012

ISO: ISO 21448:2022 - Road vehicles - SOTIF (2022)
ISO: ISO 21448:2022 - Road vehicles — Safety of the intended functionality, 2022

ISO: ISO 26262-1:2018 - Road Vehicles: Functional Safety (2018)
ISO: ISO 26262-1:2018 - Road Vehicles: Functional Safety - Part 1: Vocabulary, International Organization for Standardization (ISO), 2018

ISO: ISO 3691-4:2020 - Driverless industrial trucks (2020)
ISO: ISO 3691-4:2020 - Industrial trucks - Safety requirements and verification - Part 4: Driverless industrial trucks and their systems, 2020

ISO: ISO/TR 14121-2:2013 - Safety of machinery - Risk assessment - Practical guidance (2013)
ISO: ISO/TR 14121-2:2013 - Safety of machinery - Risk assessment - Part 2: Practical guidance and examples of methods, 2013

Jargon, E.: Bachelor Thesis, Bewegungsraumadaption des MCA für WMDS (2018)
Jargon, Elias: Entwicklung von Methoden zur Bewegungsraumadaption des Motion Cueing Algorithmus von WMDS, Bachelor Thesis, 2018

Linnhoff, C. et al.: Environmental Influence on Automotive Lidar Sensors (2022)
Linnhoff, Clemens; Hofrichter, Kristof; Elster, Lukas; Winner, Hermann: Measuring the Influence of Environmental Conditions on Automotive Lidar Sensors, in: Sensors, 2022

Lutwitzi, M.: Master Thesis, Safety Architecture for WMDS (2019)
Lutwitzi, Melina: Developtment of a Safety Architecture for a Wheeled Mobile Driving Simulator, Master Thesis, Technical University Darmstadt, 2019

Lutwitzi, M.: Bachelor Thesis, Umfelderkennung für WMDS (2016)
Lutwitzi, Melina: Entwurf eines Konzepts für eine Umfelderkennung für selbstfahrende Fahrsimulatoren, Bachelor Thesis, Technische Universität Darmstadt, 2016

Lutwitzi, M. et al.: Lidar and Landmark based Positioning System for WMDS (2022)
Lutwitzi, Melina; Betschinske, Daniel; Albrecht, Torben; Winner, Hermann: Lidar and Landmark based Positioning System for a Wheeled Mobile Driving Simulator, in: 2022 IEEE Intelligent Vehicles Symposium (IV), 2022

Marti, E. et al.: Sensor Technologies for Perception in Automated Driving (2019)
Marti, Enrique; Miguel, Miguel Angel de; Garcia, Fernando; Perez, Joshue: A Review of Sensor Technologies for Perception in Automated Driving, in: IEEE Intelligent Transportation Systems Magazine, Vol. 11, pp. 94–108, 2019

Open Source Robotics Foundation, Inc.: ROS - Robotic Operating System (2022)
Open Source Robotics Foundation, Inc.: ROS - Robotic Operating System, URL: https://www.ros.org/, 2022, visited on 07/06/2022

Ouster, Inc.: OS1 Mid-Range High-Resolution Imaging Lidar Datasheet (2022)
Ouster, Inc.: OS1 Mid-Range High-Resolution Imaging Lidar Datasheet, URL: http://data.ouster.io/downloads/datasheets/datasheet-revc-v2p3-os1.pdf, 2022, visited on 07/06/2022

Ouster, Inc.: OS2 Long-range lidar sensor for autonomous vehicles, trucking, and drones (2022)
Ouster, Inc.: OS2 Long-range lidar sensor for autonomous vehicles, trucking, and drones, URL: https://ouster.com/products/scanning-lidar/os2-sensor/, 2022, visited on 10/23/2022

Plaettner, S. et al.: Impact of Visualization System on WMDS Design (2022)
Plaettner, Stefan; Lutwitzi, Melina; Rehberg, Katharina; Chen, Xing; Tüschen, Thomas; Albrecht, Torben; Prokop, Günther; Winner, Hermann: Impact of the Visualization System Choice on Wheeled Mobile Driving Simulator Concepts, in: Proceedings of the Driving Simulation Conference 2022 Europe VR. Strasbourg, France, pp. 123–130, 2022

Point Cloud Library: Iterative Closest Point (2021)
Point Cloud Library: Iterative Closest Point: pcl::IterativeClosestPoint< PointSource, PointTarget, Scalar > Class Template Reference, URL: https://pointclouds.org/documentation/classpcl_1_1_iterative_closest_point.html, 2021, visited on 11/30/2021

Punke, M. et al.: Automotive Camera (Hardware) (2016)
Punke, Martin; Menzel, Stefan; Werthessen, Boris; Stache, Nicolaj; Höpfl, Maximilian: Automotive Camera (Hardware), in: Winner, Hermann; Hakuli, Stephan; Lotz, Felix; Singer, Christina (Hrsg.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, 2016

Rusu, R. B. et al.: 3D is here: Point Cloud Library (PCL) (2011)
Rusu, Radu Bogdan; Cousins, Steve: 3D is here: Point Cloud Library (PCL), in: IEEE International Conference on Robotics and Automation (ICRA), 2011

SAE: SAE-J3016:2021 - Taxonomy for Driving Automation Systems (2021)
SAE: SAE-J3016:2021 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, 2021

Schlager, B. et al.: Contaminations on Lidar Sensor Covers (2022)
Schlager, Birgit; Goelles, Thomas; Muckenhuber, Stefan; Watzenig, Daniel: Contaminations on Lidar Sensor Covers: Performance Degradation Including Fault Detection and Modeling as Potential Applications, in: IEEE Open Journal of Intelligent Transportation Systems, Vol. 3, pp. 738–747, 2022

Schlager, B. et al.: Effects of Lidar Sensor Cover Damages (2022)
Schlager, Birgit; Goelles, Thomas; Watzenig, Daniel: Effects of Sensor Cover Damages on Point Clouds of Automotive Lidar, 2022

Schnieder, L.; Hosse, R. S.: Leitfaden SOTIF (2019)
Schnieder, Lars; Hosse, René Sebastian: Leitfaden safety of the intended functionality: Verfeinerung der Sicherheit der Sollfunktion auf dem Weg zum autonomen Fahren, essentials, Springer Vieweg, 2019

Schöner, H.-P.: Erprobung und Absicherung im dynamischen Fahrsimulator (2014)
Schöner, Hans-Peter: Erprobung und Absicherung im dynamischen Fahrsimulator, in: (Hrsg.): SimVec - Simulation und Erprobung in der Fahrzeugentwicklung: Berechnung, Prüfstands- und Straßenversuch, VDI, Baden-Baden, 2014, 2014

Schöner, H.-P. et al.: Dynamic Driving Simulators (2016)
Schöner, Hans-Peter; Morys, Bernhard: Dynamic Driving Simulators, in: Winner, Hermann; Hakuli, Stephan; Lotz, Felix; Singer, Christina (Hrsg.): Handbook of driver assistance systems, Springer International Publishing Switzerland, 2016

SICK AG: SICK Safety laser scanners (2022)
SICK AG: SICK Safety laser scanners, URL: https://www.sick.com/at/en/safety-laser-scanners/c/g569359?q=:Def_Type:ProductFamily, 2022, visited on 11/25/2022

Slob, J. J. et al.: The wall is the limit (2009)
Slob, J. J.; Kuijpers, M. R. L.; Rosielle, P. C. J. N.; Steinbuch, M.: A New Approach to Linear Motion Technology: The Wall is the Limit, in: Proceedings of the Driving Simulation Conference Europe 2009 (DSC), INRETS, Arcueil, France, 2009, pp. 123–130, 2009

Toyota Motor Cooperation: Toyota Driving Simulator (2016)
Toyota Motor Cooperation: Toyota Driving Simulator, URL: https://global.toyota/en/download/14221274, 2016, visited on 11/04/2022

Tüschen, T.: Dissertation, Konzeptionierung eines hochimmersiven und selbstfahrenden Fahrsimulators (2019)
Tüschen, Thomas: Konzeptionierung eines hochimmersiven und selbstfahrenden Fahrsimulators, Dissertation Technische Universität Dresden, 2019

Tzafestas, S. G.: 12 - Mobile Robot Localization and Mapping (2014)
Tzafestas, Spyros G.: 12 - Mobile Robot Localization and Mapping, in: Spyros G. Tzafestas (Hrsg.): Introduction to Mobile Robot Control, Elsevier, 2014

Wagner, P.: Dissertation, Practical Feasibility and Functional Safety of WMDS (2018)
Wagner, Paul: Practical Feasibility and Functional Safety of a Wheeled Mobile Driving Simulator, Dissertation Technische Universität Darmstadt, 2018

Winner, H.: Automotive RADAR (2016)
Winner, Hermann: Automotive RADAR, in: Winner, Hermann; Hakuli, Stephan; Lotz, Felix; Singer, Christina (Hrsg.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, 2016

WIVW GmbH: Driving Simulation and SILAB (2022)
WIVW GmbH: Driving Simulation and SILAB, URL: https://wivw.de/en/silab, 2022, visited on 10/06/2022

Zermas, D. et al.: Fast segmentation of 3D point clouds (2017)
Zermas, Dimitris; Izzat, Izzat; Papanikolopoulos, Nikolaos: Fast segmentation of 3D point clouds: A paradigm on LiDAR data for autonomous vehicle applications, in: IEEE International Conference on Robotics and Automation (ICRA), pp. 5067–5073, 2017

Zöller, C. A.: Dissertation, Application of WMDS to uneven grounds (2019)
Zöller, Chris Alexander: Extension of the Application Potential of Wheeled Mobile Driving Simulators to Uneven Grounds, Dissertation Technische Universität Darmstadt, 2019

Own Publications

Zöller, C.; Wagner, P.; Lutwitzi, M.; Winner, H.: Preview of Driving Surface Unevenness in Wheeled Mobile Driving Simulators, in: IEEE (Ed.): 2018 IEEE 21th International Conference on Intelligent Transportation Systems (ITSC), November 4-7, Maui, USA, 2018

Albrecht, T.; Ottensmeier, M.; Chen, X.; Plaettner, S.; Lutwitzi, M.; Roßmeier, W.; Zöller, C.; Tüschen, T.; Winner, H.; Prokop, G.: Rolling out a new Driving Simulator Concept - Design and Challenges of Wheeled Mobile Driving Simulators, in: DSC Europe, September 2021, Munich, Germany, 2021

Lutwitzi, M.; Betschinske, D.; Albrecht, A.; Winner, H.: Lidar and Landmark based Localization System for a Wheeled Mobile Driving Simulator, in: 2022 IEEE Intelligent Vehicles Symposium (IV), June 2022, Aachen, Germany, 2022

Plaettner, S.; Lutwitzi, M.; Rehberg, K.; Chen, X.; Tüschen, T.; Albrecht, T.; Prokop, G.; Winner, H.: Impact of the visualization system choice on Wheeled Mobile Driving Simulator concepts, in DSC Europe, September 2022, Strasbourg, France, 2022

Supervised Theses

Gotta, R.: Konstruktion und Auslegung eines Fahrwerks für einen selbstfahrenden Fahrsimulator, Bachelor Thesis No. 1349/19, 2019.

Deckenbach, P.: Konstruktion und Auslegung einer elektrischen, omnidirektionalen Fahreinheit für einen selbstfahrenden Fahrsimulator, Bachelor-Thesis Nr. 1353/20, 2020.

Hohmann, A.: Gefährdungsanalyse und Sicherheitskonzept für den Betrieb von Formula Student Driverless Fahrzeugen, Bachelor Thesis No. 1354/20, 2020.

Schroeder, L.: Entwicklung eines Verwertungskonzepts für einen selbstfahrenden Fahrsimulator, Bachelor Thesis No. 1365/20, 2020.

Markard, A., Liebig, J., Vittal, D., Weimer, F.: Entwicklung einer Kollisionsschutzfunktion mittels Lidarsensorik für einen reifengebundenen, mobilen Fahrsimulator, Advanced Design Project No. 154/21, 2021.

Golla, J.: Weiterentwicklung einer Methodik zur Bewegungsraumadaption des Motion Cueing Algorithmus für einen selbstfahrenden Fahrsimulator, Bachelor Thesis No. 1379/21, 2021.

Betschinske, D.: Entwicklung einer Funktion zur Positionsbestimmung eines hochdynamischen, reifengebundenen Fahrsimulators mittels Lidarsensorik, Master Thesis No. 818/21, 2021.

Gresek, P.: Weiterentwicklung einer Kollisionsschutzfunktion mittels Lidarsensorik für einen reifengebundenen, mobilen Fahrsimulator, Bachelor Thesis No. 1391/21, 2021.

Bonfim, D.: Requirements for a Monitoring Module for the Safe Motion Control of a Wheeled Mobile Driving Simulator, Bachelor Thesis No. 1394/21, 2021.

Chai, Y., Li, D., Sun, B., Zhao, H.: Development of a Graphical User Interface for Lidar based Functions of a Wheeled Mobile Driving Simulator, Advanced Design Project No. 163/22, 2022.

Chen, C., Guo, F., Liu, J., Nie, Y., Ruan, L.: Development of Control Algorithms for the Teleoperation of an Omnidirectional Vehicle via Joystick, Advanced Design Project No. 164/22, 2022.

Bausch, J., Brückner, T., Finkeldei, F., Gotta, R., Peuker, E.: Weiterentwicklung eines Hexapod-basierten Fahrsimulators für Probandenstudien, Advanced Design Project No. 165/22, 2022.

Charleton, J., Corbelli, P., Gazura, J., Landriau, S., Wang, L.: Design of Mobile Boarding Stairs for a Wheeled Mobile Driving Simulator, Advanced Design Project No. 166/22, 2022.

Weinandi, C.: Entwicklung eines Business Case für einen selbstfahrenden Fahrsimulator, Master-Thesis, 2022.