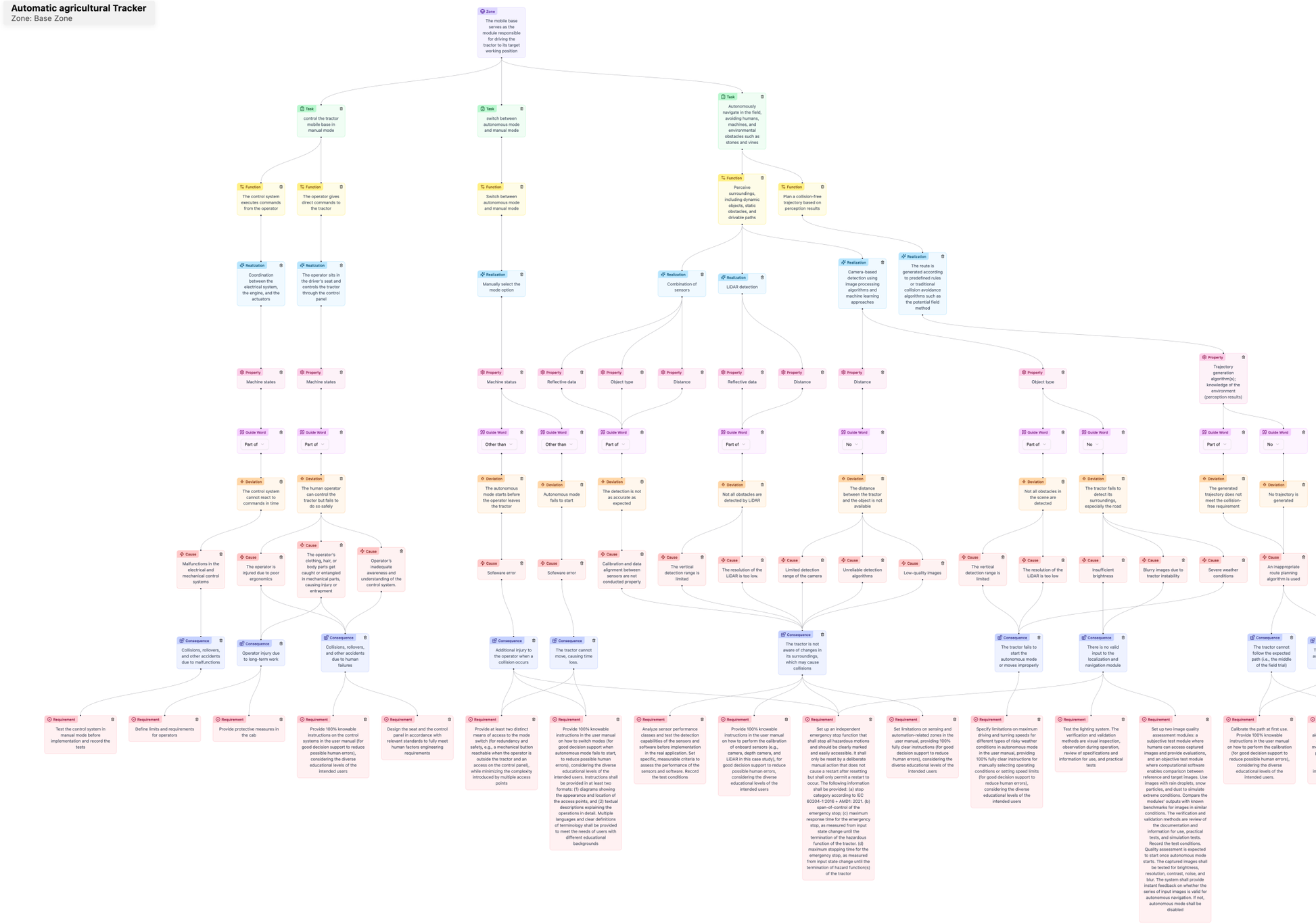
Project Report

12/6/2025, 3:26:41 PM

Project: Automatic agricultural Tracker • Zone: Base Zone



Function-Centric Hazard Identification

Hazard Zone: Base Zone

The mobile base serves as the module responsible for driving the tractor to its target working position

Task	Function	Realization	Property	Guide Word	Deviations	Causes	Consequences	Requirements	ISO Standard
switch between autonomous mode and manual mode	Switch between autonomous mode and manual mode	Manually select the mode option	1. Machine status	Other than	1. Autonomous mode fails to start	1. Sofeware error	1. The tractor cannot move, causing time loss.	1. Provide at least two distinct means of access to the mode switch (for redundancy and safety, e.g., a mechanical button reachable when the operator is outside the tractor and an access on the control panel), while minimizing the complexity introduced by multiple access points 2. Provide 100% knowable instructions in the user manual on how to switch modes (for good decision support when autonomous mode fails to start, to reduce possible human errors), considering the diverse educational levels of the intended users. Instructions shall be provided in at least two formats: (1) diagrams showing the appearance and location of the access points, and (2) textual descriptions explaining the operations in detail. Multiple languages and clear definitions of terminology shall be provided to meet the needs of users with different educational backgrounds	ISO 25119-1:2018, IEC 62061:2021+AMD1:2024 CSV, ISO 12100:2010, ISO 20607:2019, ISO 7010:2019, ISO 13849-1:2023
				Other than	1. The autonomous mode starts before the operator leaves the tractor	1. Sofeware error	1. Additional injury to the operator when a collision occurs	1. Set up an independent emergency stop function that shall stop all hazardous motions and should be clearly marked and easily accessible. It shall only be reset by a deliberate manual action that does not cause a restart after resetting but shall only permit a restart to occur. The following information shall be provided: (a) stop category according to IEC 60204-1:2016 + AMD1: 2021. (b) span-of-control of the emergency stop; (c) maximum response time for the emergency stop, as measured from input state change until the termination of the hazardous function of the tractor. (d) maximum stopping time for the emergency stop, as measured from input state change until the termination of hazard function(s) of the tractor 2. Provide 100% knowable instructions in the user manual on how to switch modes (for good decision support when autonomous mode fails to start, to reduce possible human errors), considering the diverse educational levels of the intended users. Instructions shall be provided in at least two formats: (1) diagrams showing the appearance and location of the access points, and (2) textual descriptions explaining the operations in detail. Multiple languages and clear definitions of terminology shall be provided to meet the needs of users with different educational backgrounds 3. Provide at least two distinct means of access to the mode switch (for redundancy and safety, e.g., a mechanical button reachable when the operator is outside the tractor and an access on the control panel), while minimizing the complexity introduced by multiple access points	IEC 60204-1:2016/AMD1:2021, ISO 13850:2015, IEC 62061:2021, ISO 13849-1:2023, ISO 25119-1:2018, IEC/IEEE 82079-1:2019, ISO 7010:2019, ISO 14119:2024
Autonomously navigate in the field, avoiding humans, machines, and environmental obstacles such as stones and vines	Perceive surroundings, including dynamic objects, static obstacles, and drivable paths	Camera-based detection using image processing algorithms and machine learning approaches	1. Object type	No	1. The tractor fails to detect its surroundings, especially the road	1. Blurry images due to tractor instability 2. Severe weather conditions 3. Insufficient brightness	1. There is no valid input to the localization and navigation module 2. The tractor fails to start the autonomous mode or moves improperly	1. Set up two image quality assessment modules: a subjective test module where humans can access captured images and provide evaluations, and an objective test module where computational software enables comparison between reference and target images. Use images with rain droplets, snow particles, and dust to simulate extreme conditions. Compare the modules' outputs with known benchmarks for images in similar conditions. The verification and validation methods are review of the documentation and information for use, practical tests, and simulation tests. Record the test conditions. Quality assessment is expected to start once autonomous mode starts. The captured images shall be tested for brightness, resolution, contrast, noise, and blur. The system shall provide instant feedback on whether the series of input images is valid for autonomous navigation. If not, autonomous mode shall be disabled 2. Set up an independent emergency stop function that shall stop all hazardous motions and should be clearly marked and easily accessible. It shall only be reset by a deliberate manual action that does not cause a restart after resetting but shall only permit a restart to occur. The following information shall be provided: (a) stop category according to IEC 60204-1:2016 + AMD1: 2021. (b) span-of-control of the emergency stop; (c) maximum response time for the emergency stop, as measured from input state change until the termination of the hazardous function of the tractor. (d) maximum stopping time for the emergency stop, as measured from input state change until the termination of hazard function(s) of the tractor 3. Test the lighting system. The verification and validation methods are visual inspection, observation during operation, review of specifications and information for use, and practical tests 4. Specify limitations on maximum driving and turning speeds for different types of risky weather conditions in autonomous mode in the user manual, providing 100% fully clear instructions for manually selecting operating conditions or setting speed limits (for good	ISO 21448:2022, ISO 25119-2:2019, ISO 25119-3:2018, ISO 25119-4:2018, IEC 60204-1:2016+AMD1:2021 CSV, ISO 13850:2015, IEC 60598-1:2020, ISO 12233:2024, ISO 15739:2023, ISO 19056-1:2015

Task	Function	Realization	Property	Guide Word	Deviations	Causes	Consequences	Requirements	ISO Standard
								decision support to reduce human errors), considering the diverse educational levels of the intended users	
				Part of	1. Not all obstacles in the scene are detected	1. The resolution of the LiDAR is too low 2. The vertical detection range is limited	1. The tractor fails to start the autonomous mode or moves improperly	1. Specify limitations on maximum driving and turning speeds for different types of risky weather conditions in autonomous mode in the user manual, providing 100% fully clear instructions for manually selecting operating conditions or setting speed limits (for good decision support to reduce human errors), considering the diverse educational levels of the intended users	ISO 21448:2022, ISO 26262-6:2018, ISO 26262-5:2018, ISO 26262-7:2018, ISO 25119-1:2018, ISO 13849-1:2023, ISO 9241-11:2018, ISO 9241-210:2019
			1. Distance	No	1. The distance between the tractor and the object is not available	1. Limited detection range of the camera 2. Low-quality images 3. Unreliable detection algorithms	1. The tractor is not aware of changes in its surroundings, which may cause collisions	1. Set limitations on sensing and automation-related zones in the user manual, providing 100% fully clear instructions (for good decision support to reduce human errors), considering the diverse educational levels of the intended users 2. Analyze sensor performance classes and test the detection capabilities of the sensors and software before implementation in the real application. Set specific, measurable criteria to assess the performance of the sensors and software. Record the test conditions 3. Set up an independent emergency stop function that shall stop all hazardous motions and should be clearly marked and easily accessible. It shall only be reset by a deliberate manual action that does not cause a restart after resetting but shall only permit a restart to occur. The following information shall be provided: (a) stop category according to IEC 60204-1:2016 + AMD1: 2021. (b) span-of-control of the emergency stop; (c) maximum response time for the emergency stop, as measured from input state change until the termination of the hazardous function of the tractor. (d) maximum stopping time for the emergency stop, as measured from input state change until the termination of hazard function(s) of the tractor 4. Provide 100% knowable instructions in the user manual on how to perform the calibration of onboard sensors (e.g., camera, depth camera, and LiDAR in this case study), for good decision support to reduce possible human errors, considering the diverse educational levels of the intended users	ISO 13855:2024, ISO 13849-1:2023, IEC 60204-1:2016+ AMD1:2021 CSV, ISO 12100:2010
	LiDAR detection	1. Distance 2. Reflective data	Part of	1. Not all obstacles are detected by LiDAR	1. The resolution of the LiDAR is too low. 2. The vertical detection range is limited	1. The tractor is not aware of changes in its surroundings, which may cause collisions	1. Set limitations on sensing and automation-related zones in the user manual, providing 100% fully clear instructions (for good decision support to reduce human errors), considering the diverse educational levels of the intended users 2. Analyze sensor performance classes and test the detection capabilities of the sensors and software before implementation in the real application. Set specific, measurable criteria to assess the performance of the sensors and software. Record the test conditions 3. Set up an independent emergency stop function that shall stop all hazardous motions and should be clearly marked and easily accessible. It shall only be reset by a deliberate manual action that does not cause a restart after resetting but shall only permit a restart to occur. The following information shall be provided: (a) stop category according to IEC 60204-1:2016 + AMD1: 2021. (b) span-of-control of the emergency stop; (c) maximum response time for the emergency stop, as measured from input state change until the termination of the hazardous function of the tractor. (d) maximum stopping time for the emergency stop, as measured from input state change until the termination of hazard function(s) of the tractor 4. Provide 100% knowable instructions in the user manual on how to perform the calibration of onboard sensors (e.g., camera, depth camera, and LiDAR in this case study), for good decision support to reduce possible human errors, considering the diverse educational levels of the intended users	ISO 13855:2024, ISO 13849-1:2023, IEC 60204-1:2016+ AMD1:2021 CSV, ISO 12100:2010
	Combination of sensors	1. Reflective data 2. Distance 3. Object type	Part of	1. The detection is not as accurate as expected	1. Calibration and data alignment between sensors are not conducted properly	1. The tractor is not aware of changes in its surroundings, which may cause collisions	1. Set limitations on sensing and automation-related zones in the user manual, providing 100% fully clear instructions (for good decision support to reduce human errors), considering the diverse educational levels of the intended users 2. Analyze sensor performance classes and test the detection capabilities of the sensors and software before implementation in the real application. Set specific, measurable criteria to assess the performance of the sensors and software. Record the test conditions 3. Set up an independent emergency stop function that shall stop all hazardous motions and should be clearly marked and easily accessible. It shall only be reset by a deliberate manual action that does not cause a restart after resetting but shall only permit a restart to occur. The following information shall be provided: (a) stop category according to IEC 60204-1:2016 + AMD1: 2021. (b) span-of-control of the emergency stop; (c) maximum response time for the emergency stop, as measured from input state change until the	ISO 13855:2024, ISO 13849-1:2023, IEC 60204-1:2016+ AMD1:2021 CSV, ISO 12100:2010

Task	Function	Realization	Property	Guide Word	Deviations	Causes	Consequences	Requirements	ISO Standard
								termination of the hazardous function of the tractor. (d) maximum stopping time for the emergency stop, as measured from input state change until the termination of hazard function(s) of the tractor 4. Provide 100% knowable instructions in the user manual on how to perform the calibration of onboard sensors (e.g., camera, depth camera, and LiDAR in this case study), for good decision support to reduce possible human errors, considering the diverse educational levels of the intended users	
	Plan a collision-free trajectory based on perception results	The route is generated according to predefined rules or traditional collision avoidance algorithms such as the potential field method	1. Trajectory generation algorithm(s); knowledge of the environment (perception results)	No	1. No trajectory is generated	1. An inappropriate route planning algorithm is used	1. The tractor cannot avoid obstacles in a timely manner 2. The tractor cannot follow the expected path (i.e., the middle of the field trial)	1. Test the trajectory planning algorithm before implementation on the machine. Set specific, measurable criteria to assess the performance of the trajectory planning algorithm in both simulation and real implementation. Record the test conditions 2. Calibrate the path at first use. Provide 100% knowable instructions in the user manual on how to perform the calibration (for good decision support to reduce possible human errors), considering the diverse educational levels of the intended users.	IEC 62061:2021, ISO 10218-1:2025
				Part of	1. The generated trajectory does not meet the collision-free requirement	1. An inappropriate route planning algorithm is used	1. The tractor cannot avoid obstacles in a timely manner 2. The tractor cannot follow the expected path (i.e., the middle of the field trial)	1. Test the trajectory planning algorithm before implementation on the machine. Set specific, measurable criteria to assess the performance of the trajectory planning algorithm in both simulation and real implementation. Record the test conditions 2. Calibrate the path at first use. Provide 100% knowable instructions in the user manual on how to perform the calibration (for good decision support to reduce possible human errors), considering the diverse educational levels of the intended users.	ISO/IEC/IEEE 12207:2017, ISO 9283:1998, ISO 10218-2:2025, ISO 10218-1:2025, ISO/IEC 17025:2017, ISO 6385:2016, ISO 9241-210:2019, ISO 12100:2010
control the tractor mobile base in manual mode	The control system executes commands from the operator	Coordination between the electrical system, the engine, and the actuators	1. Machine states	Part of	1. The control system cannot react to commands in time	1. Malfunctions in the electrical and mechanical control systems	1. Collisions, rollovers, and other accidents due to malfunctions	1. Test the control system in manual mode before implementation and record the tests	ISO 26262-4:2018, ISO 26262-8:2018, IEC 62061:2021, ISO 13849-2:2012, ISO 13849-1:2023
	The operator gives direct commands to the tractor	The operator sits in the driver’s seat and controls the tractor through the control panel	1. Machine states	Part of	1. The human operator can control the tractor but fails to do so safely	1. The operator’s clothing, hair, or body parts get caught or entangled in mechanical parts, causing injury or entrapment 2. Operator’s inadequate awareness and understanding of the control system. 3. The operator is injured due to poor ergonomics	1. Operator injury due to long-term work 2. Collisions, rollovers, and other accidents due to human failures	1. Define limits and requirements for operators 2. Provide protective measures in the cab 3. Design the seat and the control panel in accordance with relevant standards to fully meet human factors engineering requirements 4. Provide 100% knowable instructions on the control systems in the user manual (for good decision support to reduce possible human errors), considering the diverse educational levels of the intended users	ISO 12100:2010, IEC 62061:2021+AMD1:2024 CSV, ISO 13849-1:2023, ISO 14120:2015, ISO 13857:2019, ISO 6385:2016, ISO 9241-210:2019, ISO 7250-1:2017, ISO 15535:2023, ISO 2631-1:1997, ISO/IEC/IEEE 26514:2022, ISO/IEC/IEEE 26513:2017

Function–Requirement DMM

Function \ Requirement	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16
Switch between autonomous mode and manual mode	X	X	X													
Perceive surroundings, including dynamic objects, static obstacles, and drivable paths			X	X	X	X	X	X	X							
Plan a collision-free trajectory based on perception results										X	X					
The control system executes commands from the operator												X				
The operator gives direct commands to the tractor													X	X	X	X

Key	Requirement Text
R1	Provide at least two distinct means of access to the mode switch (for redundancy and safety, e.g., a mechanical button reachable when the operator is outside the tractor and an access on the control panel), while minimizing the complexity introduced by multiple access points
R2	Provide 100% knowable instructions in the user manual on how to switch modes (for good decision support when autonomous mode fails to start, to reduce possible human errors), considering the diverse educational levels of the intended users. Instructions shall be provided in at least two formats: (1) diagrams showing the appearance and location of the access points, and (2) textual descriptions explaining the operations in detail. Multiple languages and clear definitions of terminology shall be provided to meet the needs of users with different educational backgrounds
R3	Set up an independent emergency stop function that shall stop all hazardous motions and should be clearly marked and easily accessible. It shall only be reset by a deliberate manual action that does not cause a restart after resetting but shall only permit a restart to occur. The following information shall be provided: (a) stop category according to IEC 60204-1:2016 + AMD1: 2021. (b) span-of-control of the emergency stop; (c) maximum response time for the emergency stop, as measured from input state change until the termination of the hazardous function of the tractor. (d) maximum stopping time for the emergency stop, as measured from input state change until the termination of hazard function(s) of the tractor
R4	Set up two image quality assessment modules: a subjective test module where humans can access captured images and provide evaluations, and an objective test module where computational software enables comparison between reference and target images. Use images with rain droplets, snow particles, and dust to simulate extreme conditions. Compare the modules' outputs with known benchmarks for images in similar conditions. The verification and validation methods are review of the documentation and information for use, practical tests, and simulation tests. Record the test conditions. Quality assessment is expected to start once autonomous mode starts. The captured images shall be tested for brightness, resolution, contrast, noise, and blur. The system shall provide instant feedback on whether the series of input images is valid for autonomous navigation. If not, autonomous mode shall be disabled
R5	Test the lighting system. The verification and validation methods are visual inspection, observation during operation, review of specifications and information for use, and practical tests
R6	Specify limitations on maximum driving and turning speeds for different types of risky weather conditions in autonomous mode in the user manual, providing 100% fully clear instructions for manually selecting operating conditions or setting speed limits (for good decision support to reduce human errors), considering the diverse educational levels of the intended users
R7	Set limitations on sensing and automation-related zones in the user manual, providing 100% fully clear instructions (for good decision support to reduce human errors), considering the diverse educational levels of the intended users
R8	Analyze sensor performance classes and test the detection capabilities of the sensors and software before implementation in the real application. Set specific, measurable criteria to assess the performance of the sensors and software. Record the test conditions
R9	Provide 100% knowable instructions in the user manual on how to perform the calibration of onboard sensors (e.g., camera, depth camera, and LiDAR in this case study), for good decision support to reduce possible human errors, considering the diverse educational levels of the intended users
R10	Test the trajectory planning algorithm before implementation on the machine. Set specific, measurable criteria to assess the performance of the trajectory planning algorithm in both simulation and real implementation. Record the test conditions
R11	Calibrate the path at first use. Provide 100% knowable instructions in the user manual on how to perform the calibration (for good decision support to reduce possible human errors), considering the diverse educational levels of the intended users.
R12	Test the control system in manual mode before implementation and record the tests
R13	Define limits and requirements for operators
R14	Provide protective measures in the cab
R15	Design the seat and the control panel in accordance with relevant standards to fully meet human factors engineering requirements
R16	Provide 100% knowable instructions on the control systems in the user manual (for good decision support to reduce possible human errors), considering the diverse educational levels of the intended users