UL 4600

STANDARD FOR SAFETY

Evaluation of Autonomous Products

UL Standard for Safety for Evaluation of Autonomous Products, UL 4600

First Edition, Dated April 1, 2020

Summary of Topics

This is the First edition of ANSI/UL 4600, Standard for Safety for Evaluation of Autonomous Products.

The new requirements are substantially in accordance with Proposal(s) on this subject dated December 13, 2019 and February 14, 2020.

No Text on This Page

UL 4600

Standard for Evaluation of Autonomous Products

First Edition

April 1, 2020

This ANSI/UL Standard for Safety consists of the First Edition.

The most recent designation of ANSI/UL 4600 as an American National Standard (ANSI) occurred on April 1, 2020. ANSI approval for a standard does not include the Cover Page, Transmittal Pages, and Title Page.

Comments or proposals for revisions on any part of the Standard may be submitted to UL at any time. Proposals should be submitted via a Proposal Request in UL's On-Line Collaborative Standards Development System (CSDS) at https://csds.ul.com.

CONTENTS

1 Preface (Informative)

1.1 Goal

1.1.1 This standard is intended to help ensure that an acceptably thorough consideration of safety for an autonomous product has been performed during the design process and will continue to be done throughout the system lifecycle. It does so by emphasizing repeatable assessment of the thoroughness of a safety case.

1.1.2 Conformance with this standard is not a guarantee of a safe automated vehicle. However, conformance with this standard promotes more rigorous engineering in support of a safe automated vehicle. It is also recognized that a safety case is just one of many important parts to a complete safety assurance framework for automated vehicles, and it is expected that this standard will be used in conjunction with other standards and test methodologies defined by standards organizations and regulators.

1.2 Scope

1.2.1 The scope of this standard is a generalized autonomous system standard framework using light autonomous road vehicles as a concrete example. To that end, this version of the standard includes extensive prompt lists applicable to light autonomous road vehicles (both passenger and cargo vehicles). Many of the prompts will apply to other autonomous ground vehicles and even other types of autonomous systems, but no specific attempt has been made to include extensive prompts for other applications, nor to segregate road vehicle prompts from more general prompts.

1.2.2 The approach taken in this standard (UL 4600) is to require a claim-based safety case that encompasses essentially the entirety of the material necessary for safety assurance. The safety case includes a structured set of claims, argument, and evidence supporting the proposition that an item (a vehicle plus all other support contributing to safety) is acceptably safe for deployment. In support of that goal, UL 4600 assessments emphasize ensuring that the safety case is reasonably complete and well formed. In particular, UL 4600 provides guidance to improve consistency and completeness of the safety case. To this end, some best-practice process activities and granular work products are specifically required (e.g., creation of a hazard log). However, no specific overall design process is mandated, nor are there mandates for specific methods used to create the majority of work products (e.g., a V-style development process is not required; any reasonable approach used to create a list of hazards can be acceptable).

1.2.3 This standard does NOT define a process, but rather puts forth assessment criteria to determine the acceptability of a safety case. As such, the ordering of sections, clauses, and prompt elements does NOT imply temporal ordering or other process path dependencies.

1.3 Use of this standard with other standards

1.3.1 This standard is intended to work with existing standards to provide the additional elements necessary to assure that safety aspects of fully autonomous item operation have been considered in a comprehensive manner when creating a safety case.

1.3.2 To the maximum extent practicable, it is intended that developers can take advantage of effort expended and assessment credit gained for conformance to other existing standards. Developers may incorporate materials into their safety case generated as a result of executing processes and generating work products required by other standards.

1.3.3 It is the intent of this standard to be compatible with existing relevant safety standards to the maximum extent practicable, and in particular avoid prohibiting any activity or approach that is required by those standards. In particular, compatibility with ISO 26262:2018 and ISO/PAS 21448:2019 has been considered. Annex A discusses a mapping of some clauses of this standard onto ISO 26262:2018 and ISO/PAS 21448:2019. Other safety standards such as IEC 61508 are relevant and expected to be generally compatible, but detailed analysis of IEC 61508 and other functional safety standards is out of scope for this version of UL 4600.

1.3.4 Two areas out of scope for this standard are setting acceptable risk levels and setting forth requirements for ethical product release decisions and any ethical aspects of product behavior. For both topics the developer records what decisions have been made, but this standard does not establish acceptance criteria beyond that they have been recorded. Other standards such as the IEEE P7000 series provide guidance on those topics.

2 Scope

2.1 Scope summary

2.1.1 This standard covers the safety principles, risk mitigation, tools, techniques, and lifecycle processes for building and evaluating a safety argument for vehicles that can operate in an autonomous mode.

2.1.2 Operation is assumed to occur without human supervision and without expectation of human intervention in performing and supervising the dynamic driving task and other normal system operations based upon the current item state and ability to sense and otherwise interpret the operating environment. Human contributions to safety in other than normal operation are considered (e.g., maintenance), as are interactions with humans who are not operating the item (e.g., pedestrians).

2.1.3 This standard generally uses the term “item” rather than “system” or “product” when referring to the scope of the safety case as well as the operation of the item. This approach is in recognition of the possibility that the safety of the item might rely upon infrastructure, services, support processes, and other factors that might not normally be considered part of a system such as a vehicle per se, but which materially affect its safety and therefore are all considered within the scope of the item being assessed for conformance.

2.1.4 This standard assumes that the item autonomously operates starting at some well-defined initial state to some other well-defined end state without human intervention. Human input might influence the selection of desirable states (e.g., via an occupant requesting a destination). However, the extent to which human operators mitigate or introduce risk by performing or supervising a dynamic control task (e.g., by driving or taking responsibility for monitoring system operation) is outside the scope of the standard. Similarly, the extent to which human operator performance or non-performance is involved in risks related to transferring human driver control to or from the item is also outside the scope of the standard. However, ensuring that the item itself properly performs any change of control functions if and when it is supposed to is generally within the scope of the standard since it can adversely affect operation in fully autonomous mode as well. Thus, while portions of this standard might be helpful for addressing less than fully autonomous vehicles, issues involving human driver responsibilities, vigilance, and ability to properly accept responsibility for vehicle control are out of scope for this standard.

2.1.5 While information security is an essential topic, the details of that area are out of scope for this standard beyond a general requirement for a Security Plan and prompt elements that are possibly unique to autonomous vehicle operation in comparison to other vehicular security requirements. Reasonably foreseeable misuse and abuse as well as physical attacks (e.g., physical sensor damage) are in scope.

2.1.6 The requirements of this standard are considered to be at a necessary, but possibly not sufficient, level of completeness and rigor to create an acceptably well-formed and acceptably complete item safety case. In particular, prompt element lists are considered non-exhaustive, with an expectation that design teams will include additional items as relevant to the item and its operational design domain.

2.2 Elements in scope

2.2.1 Specific aspects of item operation and safety related issues which are explicitly intended to be in scope for this standard include:

a) Operation of autonomous items in potentially unstructured environments

EXAMPLE: A vehicle is the first vehicle directed into an open farm field containing a mixture of viable and non-viable areas for traversal and parking as part of an ad hoc overflow event parking process. There are no lane markings and no positioning beacons. Moreover, there are cows and hay bales randomly placed in the field. There are no humans assisting with organizing vehicle parking positions. This situation is in scope for the standard.

EXAMPLE: A crowd has spilled into the street at a fire scene. Emergency response equipment, response personnel, victims, and casual observers are moving without regard to normal road use patterns. Fire hoses, falling pieces of burning debris, small explosions, traffic signal power outages, damaged pavement, and other disruptions to normal infrastructure expectations exist. Multiple injured people at building exits are calling for pickup by autonomous vehicle ride hail services to be transported to urgent care medical facilities. This situation is in scope for the standard.

NOTE: A particular item's safety case might require a structured environment for safe operation as specified by an ODD description. However, structure is not assumed to be present by default. Therefore, operation in unstructured environments must be specifically disclaimed by the safety case if applicable.

b) Operation with potentially inaccurate, incorrect, incomplete, or misleading data provided by sensors

c) The effects of potentially inaccurate, incorrect, incomplete, or biased data, including test data, field report data, other validation data and machine learning training data.

d) The effects of potentially imprecise, inaccurate, or incomplete simulation models.

e) Potential defects and failures of hardware and/or software in the item, data collection functions, data processing functions, communications, engineering support systems, tools, and infrastructure support.

f) Human contributions to potential risk, including occupants, pedestrians, other road users, non-road users, cargo handlers, maintainers and inspectors. This includes acts of omission and commission; accidental and malicious physical acts; and human roles in creating as well as mitigating risk.

g) Lifecycle considerations, including design data collection, engineering data management, tool qualification, design, implementation, testing, other validation, field data collection, operations, maintenance, updates, upgrades, and retirement. Lifecycle considerations also encompass potential changes to the environment which may affect ODDs, changes in object types, changes in behaviors, etc..

h) Inclusion of risk mitigation and other aspects of contributions to the safety case made by conformance with other standards, and in particular both ISO 26262 and ISO/PAS 21448 standards for products within scope for those standards.

i) Ability to use a heterogeneous approach to arguments, including use of diverse standards to support safety (e.g., use of different but acceptable functional safety standards for different item subsystems).

2.2.2 None of the described in-scope topics is intended to require that the item successfully delivers full service in all situations described. Rather, the requirement is to consider all prompt elements and argue that risk is acceptable despite these factors. In many cases that will involve crafting an ODD that excludes problematic prompt elements. However, excluding a prompt element from the ODD (or similar approach) creates an obligation to argue that the exclusion does not itself result in unacceptable risk.

EXAMPLE: Unpaved roads without lane markings are excluded from the ODD. The safety case generally argues that geo-fencing and map creation will exclude all unpaved roads. It is further argued that this exclusion encompasses quickly identifying roads undergoing repaving projects that are temporarily unmarked but still carrying traffic.

EXAMPLE: Snow is excluded from the ODD. Snow is still part of the safety case to cover un-forecast snow that occurs during an operational mission. The safety case generally argues that it can successfully terminate a mission via in-lane stop despite snow. It further argues (with evidence) that snow will happen so infrequently in the deployment location that the elevated product risk presented by occasional in-lane stops is acceptable.