AV Safety Standards Frameworks: How UL 4600, ISO 21448 (SOTIF) and ISO 26262 can work together to build a safety case

March 24, 2021 | Nicholas Alexiades
Who we are

Since 1894, UL has employed scientific processes and the highest ethical principles to help create a safer world.

UL’s functional safety team is located globally in eight countries and is made up of a diverse team with experiences in various industries including automotive, robotics, machinery, process industry, among others.

UL’s Mission: Working for a safer world

UL is passionate in helping customers navigate the complex technical challenges of today’s functional safety landscape, while working for a safer world. With our extensive safety expertise and customer centric approach, we help improve the safety of products and the systems containing those products.
Our services

- Component **assessments**
- Hardware and software **assessments**
- Complete **end product** (vehicle) **assessments**
- Functional safety and **autonomy safety assessments**
- Organization-wide process **audits**
- Cyclic project process **audits**
- Independent **reviews** (safety analysis, safety requirements, etc.)
- Personnel certification - UL-CFSP (**Certified Functional Safety Professional**) **training** and UL-CFSX (**eXpert**) **training**
- Software **tool qualifications**
Electronics and safety

- All electronics
- All electronics requiring product/electrical safety
- All electronics requiring functional safety
- All electronics requiring autonomy safety
ISO 26262 standard for functional safety

Functional safety\(^1\) = “absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E (Electrical and Electronic) systems”

“malfunctioning behavior” is caused by random and systematic faults…

…in electronic hardware, in software, and in systems

\(^1\) definition per ISO 26262:2018
The U.S. Department of Transportation (DOT) uses SAE J3016’s six levels of driving automation for on-road motor vehicles in its “Federal Automated Vehicles Policy”.

This is a de facto global standard to define autonomy levels implemented by the automotive industry.
Functional safety versus SOTIF

Functional Safety (‘FuSa’)

- Diligent engineering to rigorously contain or counteract ‘faults’ within electronic systems
- Addresses “faults” as traditionally defined, e.g., as “bugs”, “glitches”, etc.
- Answers the question “Is the system safe when a fault/glitch/bug occurs?”

Safety of the Intended Functionality (SOTIF)

- Diligent engineering to assure the safety of systems operating without “faults” as traditionally defined
- Addresses system-level misbehavior due to performance gaps (in sensor sets, algorithms, AI and training data, etc.)
- Answers the question “Is the system safe when operating as intended?”

Autonomous vehicles and other industrial systems require FuSa AND SOTIF to build a complete safety case.
Three major standards in ADAS/AV safety

- ISO 21448
  - Well established/widely used
  - Restricted in scope to traditional malfunction
  - A basis for all low-level E/E faults and data errors
  - Not a complete pathway to full ADAS or AV assurance

- UL 4600
  - Newly developed (released in 2020)
  - Scope is only for full autonomy (L4/L5)
  - Guidance for many hazardous behaviors including field operation, AI/ML, data pipeline, etc.
  - Often requires arguments that can be made using ISO 26262/ISO 21448 frameworks

- ISO 26262
  - Under development (DIS published)
  - Addresses ADAS for products at L2/L3 and can be extended for L4/L5 architectures
  - Well-matched to terminology of ISO 26262
  - Wide-scale automotive industry buy-in
SOTIF: ‘Safety of the Intended Functionality’

‘Safety of the Intended Functionality’ – absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality

- SOTIF addresses hazards caused by limitations in the intended function in a system that is free from faults as defined in ISO 26262.

- Safety problems with the intended function may be related to:

  Performance limitations
  Complex environments
  Human-machine interactions
The four-quadrant scenario framework

Scenarios can be categorized as follows:

Area 1: **Maximize or maintain area**, while minimizing areas 2 and 3. This retains or improves safe functionality.

Area 2: **Minimize area** with technical measures to an acceptable level; evaluate the potential risk; and, if necessary, shift hazardous scenarios to area 1 by improving the function or by restricting the use/performance.

Area 3: **Minimize area** (the risk of the unknown) as much as possible with an accepted level of effort (every detected hazardous scenario will be shifted to area 2).
Summary of SOTIF activities from ISO 21448

'Left Side' of V-model / Analysis-Oriented

5 Specification and Design

6 ID & evaluate hazards caused by intended function

8 Functional modification to reduce SOTIF risk

9 Definition of the V&V Strategy

10 Evaluate known hazardous scenarios (area 2)

11 Evaluate unknown hazardous scenarios (area 3)

12 Criteria for SOTIF Release

13 Operating phase activities

'Right Side' of V-model

- If SOTIF release fails
- If verification fails
- If validation fails

Risk Accepted

- if SOTIF risk is acceptable -

- if acceptable -

- if SOTIF release passes

- if SOTIF risk is unacceptable -
Overlap of activity timelines between ISO 26262 and ISO 21448

**Contrast to ISO 26262:** Levels of hierarchy, while they may be present in SOTIF, are not enforced or maintained in ISO 21448

Note: Cybersecurity is out of scope of ISO 21448 (addressed in ISO 21434)
Partner with UL for autonomy safety assessments

The world’s complex with many intricate solutions.

1. We partner with our customers to identify the best solution to help ensure a safe product and to provide third-party reviews.

2. There is not always a one best solution approach; therefore, UL works together with our customers to find the best specific approach.
The future of automotive safety

- Safe vehicles require a complete safety case
  - Based on **functional safety**; AND
  - Based on **SOTIF**; AND
  - Based on **other techniques** and frameworks, e.g., UL 4600
- For complex products, safety itself is complex.
- Integrators must **confirm** the **safety arguments** of suppliers.
- An **independent third-party** is a highly recommended element for safety.
Current safety standards provide essential guidance for designing safe vehicles. However, existing standards, such as ISO 26262 (Functional Safety) and ISO 21448 (SOTIF – Safety of the Intended Function), were envisioned for vehicles that ultimately have a human driver responsible for safe operation of the vehicle.

With existing standards, safety is typically achieved via following a specified design process, together with the imposition of specific technical requirements and validation methods.

Higher degrees of risk result in more rigorous engineering requirements to ensure appropriate risk mitigation.
Goal based and technology-agnostic means UL 4600 requires explaining why the self-driving car is safe without requiring the use of any specific design approach or specific technology use.

- For example, using LIDAR is not required. Rather, the safety case has to credibly argue that relevant objects will be successfully detected and classified with whatever sensors are installed within the limits of the intended operational design domain.

- Similarly, there is no fixed limit on the number of road-testing miles that must be accumulated before deployment.

Rather, the safety case must argue that an acceptably robust combination of analysis, simulation, closed course testing, and safe public road testing have been performed to ensure an appropriate level of system safety for the initial vehicle and each software update.
UL 4600: Standard for Safety of Autonomous Products

‘Autonomous’ system – a system that operates in a generally unstructured operational environment without human oversight or supervision

UL 4600 addresses potential safety issues such as:

- Machine learning and AI
- Data pipeline
- Operational feedback

…in addition to topics addressed within ISO 26262 and ISO 21448
## UL 4600 overview

### Clauses

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Preface</td>
</tr>
<tr>
<td>2.</td>
<td>Scope</td>
</tr>
<tr>
<td>3.</td>
<td>Referenced Publications</td>
</tr>
<tr>
<td>4.</td>
<td>Terms, Definitions and Document Usage</td>
</tr>
<tr>
<td>5.</td>
<td>Safety Case and Arguments</td>
</tr>
<tr>
<td>6.</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>7.</td>
<td>Interactions with Humans and Road Users</td>
</tr>
<tr>
<td>8.</td>
<td>Autonomy Functions and Support</td>
</tr>
<tr>
<td>9.</td>
<td>Software and System Engineering Process</td>
</tr>
<tr>
<td>10.</td>
<td>Dependability</td>
</tr>
<tr>
<td>11.</td>
<td>Data and Networking</td>
</tr>
<tr>
<td>12.</td>
<td>Verification Validation and Test</td>
</tr>
<tr>
<td>13.</td>
<td>Tool Qualification, COTS and Legacy Components</td>
</tr>
<tr>
<td>14.</td>
<td>Lifecycle Concerns</td>
</tr>
<tr>
<td>15.</td>
<td>Maintenance</td>
</tr>
<tr>
<td>16.</td>
<td>Metrics and Safety Performance Indicators (SPIs)</td>
</tr>
<tr>
<td>17.</td>
<td>Assessment</td>
</tr>
</tbody>
</table>
ISO 26262 and UL 4600

What is the relationship between UL 4600 and other standards, such as ISO 26262 and ISO 21448 (SOTIF)?

• The UL 4600 Standard focuses on ensuring that a comprehensive safety case is in place including safety claims, argumentation, and evidence. It is intended to cover computer-based system aspects of autonomous operation.

• UL 4600 is specifically designed to build upon the strengths of existing standards such as ISO 26262, and evolving standards such as ISO 21448-SOTIF.

• UL 4600 is not a competing standard to other standards being developed. UL 4600 permits claiming appropriate credit for conforming to those standards while ensuring autonomy-specific gaps are filled.
UL 4600 and other standards

- **Red:** UL 4600
- **Blue:** ISO 21448 (SOTIF)
- **Green:** ISO 26262 (FuSa)

Legend:
- Red: UL 4600
- Blue: ISO 21448 (SOTIF)
- Green: ISO 26262 (FuSa)
Relationship: UL 4600 and other standards

Red: UL 4600
Clause 5
Clause 6
Clause 7
Clause 8
Clause 9
Clause 10
Clause 11
Clause 12
Clause 13
Clause 14
Clause 15
Clause 16
Clause 17

Blue: ISO 21448
various
clause 6
clause 5
clauses 5, 8
-
various
various
clauses 9, 10, 11
-
-
-
clauses 5, 11
clause 12

Green: ISO 26262
part 2, sub-clause 6.4.8
part 3, clause 5
-
-
part 4 and Part 6
part 4, part 5
part 4, part 6
parts 4, 5, 6
Part 8
parts 27
part 7
part 5, clause 89
part 2, sub-clause 6.4.9

Light color: ISO covers a small part of the UL4600

Dark color: ISO covers a large part of the UL4600
For most of UL 4600, a large part of the UL 4600 requirements are covered by ISO 26262 or ISO 21448.
For some of UL 4600, only a small part of the UL 4600 requirements are covered by ISO 26262 or ISO 21448.

- **Safety Case Framework**
  - Mentioned in ISO 26262, but UL 4600 is more specific
    - Part 2 sub-clause 6.4.8

- **Interaction w Others and Autonomy Functions**
  - These are addressed in ISO 21448, but there are more specific requirements in UL 4600
    - Clause 5
    - Clauses 5, 8

- **Lifecycle and Maintenance**
  - These are addressed in ISO 26262, but there are more specific requirements in UL 4600
    - Clause 14
    - Clause 15
    - Parts 2.7
    - Part 7
UL 4600 versus SOTIF

What are the UL 4600 areas of focus?

• Areas of specific emphasis include safety practices for machine learning based approaches, functionality for which complete requirements are not available, addressing “unknown unknowns” in safety argumentation, and helps ensure that adequate fault mitigation capabilities are present in systems that do not have human driver oversight.

• We anticipate that many users of the Standard will, in fact, build upon existing ISO 26262 and newly created ISO 21448 (SOTIF) conformance strategies, and we believe these standards are complementary to UL 4600.
How we evaluate UL 4600: Starting with a gap analysis

Assessment of the safety case for conformance examples:
  • Conformance plan
  • Objective versus subjective assessment
  • Assessment package
  • Self-audit

Independent assessment is required by qualified personnel.

Conformance monitoring must be included in the safety case.

What does this all mean? Much like ISO 21448, we partner with our customers to identify gaps between their current processes and techniques in comparison to UL 4600.
For ISO 26262, autonomy and other safety related topics reach out:

Contact today’s presenter, Nicholas Alexiades, UL engineering manager at:

- Nicholas.Alexiades@ul.com
- +1-847-664-8244

Global.functionalsafety@ul.com

KVAUSA.com/training

UL.com/FunctionalSafety
Thank you!