
A worldwide team of 60 top safety specialist from 11 major companies wrote 157 pages thinking safety from the top down – from risk balance to implementation.

holistic approach for SAE L3/4 systems emphasizing the importance of safety by design and verification & validation.
### 3.4 – ISO TR 4804 – TIMELINE.

<table>
<thead>
<tr>
<th>Event</th>
<th>Start Date</th>
<th>Location</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release of White Paper “Safety First”</td>
<td>02-Jul-19</td>
<td>n/a</td>
<td>International release of White Paper as free download from all partners. Pre-work for ISO standardization</td>
</tr>
<tr>
<td>Project approval ISO TR 4804</td>
<td>30-Dec-19</td>
<td>ISO</td>
<td>ISO project formally approved to start.</td>
</tr>
<tr>
<td>Intl. kick-off meeting</td>
<td>19-Feb-20 –</td>
<td>Paris,</td>
<td>Founding of intl. expert team, alignment on strategy and commenting phase, task assignments</td>
</tr>
<tr>
<td>Project approval ISO TR 4804</td>
<td>21-Feb-20</td>
<td>BN-Auto</td>
<td></td>
</tr>
<tr>
<td>8 weeks commenting phase, national alignment meetings</td>
<td>06-Mar-20 –</td>
<td>All nations</td>
<td>Prepare formal comments on national basis Create proposals according to tasks from kick-off</td>
</tr>
<tr>
<td>Project approval ISO TR 4804</td>
<td>30-Apr-20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intl. comments resolution meeting session 1 and 2</td>
<td>5 days in May and Jun 20</td>
<td>Web meeting</td>
<td>Resolve all comments, agree and integrated proposals from tasks, prepare work on 2nd Ed.</td>
</tr>
<tr>
<td>Final editorial review by experts</td>
<td>01-Jul-20 –</td>
<td>All nations</td>
<td>Final editorial review by experts and if all agreed changes from comment sheet have been incorporated correctly.</td>
</tr>
<tr>
<td>Project approval ISO TR 4804</td>
<td>15-Jul-20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO editorial review and rephrasing</td>
<td>24-Jul-20 –</td>
<td>Genève, ISO</td>
<td>Formal review by ISO editor</td>
</tr>
<tr>
<td>Release of ISO TR 4804</td>
<td>30-Sep-20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project approval ISO TR 4804</td>
<td>07-Dec-20</td>
<td>Genève, ISO</td>
<td>ISO TR 4804 available at <a href="http://www.iso.org">www.iso.org</a></td>
</tr>
<tr>
<td>Project approval ISO TR 4804</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3.4 – ISO TR 4804 – SCOPE.

1. How safe must a Level 3/4 system be?

2. What aspects are necessary to achieve the overall safety vision?

3. What capabilities are needed to cover all the above aspects?

4. Which building blocks are necessary?

5. How to design a generic architecture out of these building blocks?

6. What verification and validation is needed?

POSITIVE RISK BALANCE AND AVOIDANCE OF UNREASONABLE RISK

PRINCIPLES OF SAFETY AND CYBERSECURITY

SAFETY BY DESIGN

VERIFICATION & VALIDATION

Overall Testing

Simulation and Field Operation

Verification & Validation of Elements

APPENDIX A

Development Examples

Generic Architecture

APPENDIX B

Deep Neural Networks

Elements

Capabilities

The ISO 26262 Digital Conference | TS 5083 – Status and Timeline | 24-Mar-2021
Based on recommendation of the German Ethics Commission in 06/2017 (BMVI):
Maximizing the evidence of a POSITIVE RISK BALANCE of automated driving solutions compared to the average human driving performance which is different
- between Europe, US and China;
- road types e.g. highway or urban road; and
- weather, age of driver

AVOIDANCE OF UNREASONABLE RISK is the second major measure to claim an acceptable level of safety. Its evidence is based on the application of a proactive and reactive driving behavior, avoidance of accidents as much as “practically possible”. These judgements are made on basis of a combination of qualitative and quantitative assessments, and also on an understanding of good engineering practice and existing standards.
Groups of principals of safety and cybersecurity

- PSC-01 Cybersecurity
- PSC-02 Data Recording
- PSC-03 Passive Safety
- PSC-04 Safety Assessment
- Automated Vehicle and Related Aspects

- Automated Driving System
  - PSC-05 Safe Operation
  - PSC-06 Safety Layer
  - PSC-07 Behaviour in Traffic
  - PSC-08 Operational Design Domain

- Human Factors
  - PSC-09 Role of User
  - PSC-10 Driver Initiated Takeover
  - PSC-11 Vehicle Initiated Takeover Request
  - PSC-12 Interdependency between Driver and Automated Driving System
3.4 – ISO TR 4804 – GENERIC ARCHITECTURE.

**Traffic Rules:** Worldwide and locally different traffic rules need to be taken into account.

**Environment Perception Sensors:** Different physical principles.

**HD maps** have to offer reliable map attributes.

**Sensor Fusion:** Combination of at least three sensor technologies (e.g. camera, lidar, radar).

**Safety measures for supervised offline trained DNNs.**

**Integrated circuits need to fulfill Functional Safety requirements.**

**Complement verification & validation approaches by field monitoring.**

**Implementation of redundant safety channel.**
Fail Safe (FS):
After failure the risk is small or covered by Fail Degraded

Fail Degraded (FD):
Provide safe system for specific time until Minimal Risk Condition (MRC) is reached
3.4 – ISO TR 4804 – DEEP NEURAL NETWORKS.

Modular-based system architecture recommends that machine learning algorithms are treated as a software component.

Development steps of deep neuronal networks

Each step should provide safety artifacts to support the safety case.

*Machine Learning
CONTINUATION IN ISO TC22/SC32/WG13
ISO TR 4804 EVOLVES INTO ISO TS 5083.

- A NWIP has been accepted by TC-22 P-members on 06-Dec-2020 to continue work as TS.
- International experts (50+) from Japan, China, Korea, Germany, France, UK, Netherlands, Sweden, Finland, Italy, Austria and USA are registered to support the project.

- SC 32 decided to found a new WG 13 in TC22 / SC 32.
  - WG 13 secretary is at VDA, Germany
  - SC32 confirmed Simon Fürst, BMW as convener of WG 13

- The TS project is intended to run in a 24 month schedule, i.e. expected release date of TS 5083 is by mid 2023
OVERVIEW ON ISO DELIVERABLES.

https://www.youtube.com/watch?v=T--RIs3E7ZE.

**Technical Report (TR)**
- Informative document, no limitation in validation, regular review of actuality without given process
- Approval by simple majority of TC/SC P-Members on existing draft (DTR), no NWIP-Procedure required
- Contain data or information about state of the art

**Publicly Available Specification (PAS)**
- Normative document, max. 6 years lifetime, then withdrawal or upgrade to TS or IS, regular revision after 3 years
- Project registration via NWIP-Ballot and approval for publication by simple majority of TC/SC-Members
- For urgent technologies not yet established well in the market

**Technical Specification (TS)**
- Normative document, max. 6 years lifetime, after that withdrawal or upgrade to IS, regular revision after 3 years
- Project registration via NWIP-Ballot and approval for publication by 2/3 majority of TC/SC-Members
- For new technologies with low experiences so that consensus is difficult to be reached

**International Standard (IS)**
- Normative document, unlimited lifetime, automatic review process all 5 years
- Registration if NWIP-Ballot approved by 2/3 majority of TC/SC-Members
- Publication if approved throughout DIS-/FDIS-Ballot by all ISO-Members; state of the art of established technologies

1st Edition in Aug-20
2nd Edition in Mid-23
3rd Edition in 2026
SAFETY AND CYBERSECURITY FOR AD SYSTEMS. STRATEGY AND OBJECTIVES.

This is regarded as a long term ISO standardization activity covering the full field of Road Vehicles – Safety and Cybersecurity for automated driving systems – Design, verification and validation.

This ISO publication shall be suitable as a basis for authorities and regulatory acts.

Standardization of the state of the art shall take place in parallel with the product development at the companies of the contributing experts.

This activity is regarded as an application-specific standardization for automated driving based on generic underlying standards like ISO 26262 (functional safety), ISO 21448 (SOTIF), ISO 21434 (automotive cybersecurity) and others, see ISO DTR 4609 (Road vehicles — Report on standardization prospective for automated vehicles (RoSPAV))

Proceed from an ISO/TR to finally release an ISO Standard.

1. ISO TR 4804, in Dec. 2020
   Target is to convert Safety First White Paper into an ISO/TR creating an early 1st edition to worldwide occupy this field by an ISO standardization activity. Avoid major changes in this step to be fast.

2. ISO TS 5083 by Mid 2023
   Go for necessary enhancements and extensions to cover scope in width and depth.

3. Continue work to proceed towards ISO IS standard afterward
   See picture on the right side for potential paths.
POTENTIAL FIELDS OF ELABORATION IN TS 5083. DECISIONS TO BE TAKEN IN UPCOMING MEETINGS OF WG13.

- Give more details and guideline on applying generic automotive standards like functional safety (ISO 26262), SOTIF (ISO 21448) and cybersecurity (ISO 21434) and other relevant standards for automated driving system (ADS).

- Add overview and linkage/ usage on standards addressing special topics of ADS.

- Interaction and correlation of applicable process / methods standards for ADS.

- Further align terminology with other relevant standards, make terms application specific whereever appropriate.

- Evolve positive risk balance and avoidance of unreasonable risk towards holistic safety approach

- Make principles more significant, enhance description, keep consistent with relevant publications.

- Define generic structure of Risk Assessment for ADS addressing FuSa, SOTIF and Cybersecurity and their balancing. E.g. assign C factor to other systems. But do not assign any ASIL to safety goals.

- Describe variants of architectures for ADS.

- Add further details on V&V methods including their interaction and relations, add statistical assessment.

- Integrate cybersecurity more detailed on level of elements and interfaces on architecture level.

- Focus on ADS specific AI/ML topics, improve usage of ML for dedicated elements.
Thank you for your attention!

Road Vehicles – Safety and cybersecurity for automated driving systems – Design, verification and validation methods