Important to know when a self-driving car design is acceptably safe

- What do we measure?

Safety case ties together:

- Standards-based engineering
- Knowing what to measure
- Showing that system is acceptably safe
Standards-Based Engineering Approach

<table>
<thead>
<tr>
<th>SYSTEM SAFETY</th>
<th>UL 4600</th>
<th>Safety Beyond Dynamic Driving</th>
</tr>
</thead>
<tbody>
<tr>
<td>DYNAMIC DRIVING FUNCTION</td>
<td>ISO/PAS 21448</td>
<td>SaFAD/ISO TR 4804</td>
</tr>
<tr>
<td>FUNCTIONAL SAFETY</td>
<td>ISO 26262</td>
<td></td>
</tr>
<tr>
<td>CYBER-SECURITY</td>
<td>SAE J3061</td>
<td>SAE 21434</td>
</tr>
<tr>
<td>VEHICLE SAFETY</td>
<td>FMVSS</td>
<td>NCAP</td>
</tr>
</tbody>
</table>
Explaining Via A Safety Case

Safety Case:
A structured written argument, supported by evidence, justifying system is acceptably safe for intended use.

Answers questions:
- What do you mean by “safe” (claim)
- Explain why you think you’re safe (argument)
- Show data to support your explanation (evidence)
From Safety Case To Dashboard

Safety Performance Indicators (SPIs) for safety case claims

- **Standards**: Cover relevant standards, best practices
- **Validation**: Safety metrics from testing predict acceptable risk
- **Process**: Engineering rigor and process quality metrics
- **Feedback**: Field feedback data shows risk prediction is accurate
- **Safety Culture**: Metrics indicate a healthy safety culture

Dashboard:

- **Deploy when SPIs show your claims are supported by data**