Welcome!

Collaborative Discussion of Risk Controls in AV Safety Risk Assessment

Virtual Mini-Forum: Part 2

Upon entering the session:

1. Find yourself in the participant list and click on your name.

2. Click the dropdown next to your name and select “Rename”.

3. Add your company next to your name (ex: Becca Lehner – MITRE)

4. Respond to the following question in the chat box:

If you could take a road trip around the United States where is the #1 place you’d go?

MITRE

Session Objectives & Agenda

Session Objective: Engage in an interactive analysis of risk controls using specific examples of AV hazardous scenarios

Agenda:

12:00 – 12:10: Welcome + Introduction

12:10 – 12:20: Review of SRA and Risk Controls Identified in Session 1

12:20 – 1:20: Analysis of Risk Controls in AV Hazardous Scenarios

1:20 – 1:30: Closing

AV SMS Forum Ground Rules

Collaborating across the ADS community to implement SMS by sharing promising practices

Participants are encouraged to share process-related (non-proprietary) safety-related knowledge and practices relevant to others to achieve our collective goal of safe deployment of ADS vehicles.

Participation is welcome from leaders who are actively working to implement SMS in their organizations.

To create a safe space for candid discussion:

1. **Chatham House Rule:** We agree to the Chatham House Rule, in that ***we can use the information received***, but we will not reveal the identity nor the affiliation of the speaker(s) or other participants.
2. **Recording:** We agree not to record (audio or video) or photograph information without prior approval.
3. **Social Media:** We agree to solely use social media for event promotion and not for sharing information or content from the sessions.
4. **Anti-Trust:** We will not discuss the following during any session: i) prices, changes in pricing, or price forecasting; ii) competitive pricing strategy; iii) terms or conditions of sales, or supplier terms and conditions; iv) credit terms, profits, profit margins, or costs; v) selection, rejection, or termination of suppliers or customers; vi) market share or sales territories; or vii) competitive bids or bidding strategy.
5. **Respect:** We commit to listen well, participate fully, be constructive, and acknowledge alternate viewpoints.

Committee Vision

AV SMS Forum

Vision: ADS community is recognized as a leader in organizational safety and SMS

We exist to:

- **Provide information, guidance, and justification to support the advancement of SMS** within organizations in tangible and actionable ways (e.g., guides, templates)
- **Hold rich discussions on problems and solutions** to difficult topics *(with agreements in place to support candid discussion)*
- **Help organizations to learn from each others' experiences** *(non-intellectual property and non-competitive advantage)*

We strive to:

- **Grow into an SMS industry forum** with sustained connectivity and communication around SMS resources

How we will achieve this vision:

- **Collaborative development of resources/artifacts** (e.g., create and share a resource 1-2x per year and incorporate discussion of the resource into a broader workshop or small group forum)
- **Hold a workshop 1x per year for the community of stakeholders** with interest in SMS focused on exploring a resource or topic of universal interest with limited sensitivity—T*his will also serve to identify additional participants for smaller group forums*
- **Hold small group forums 2x/year to explore a targeted problem space and discuss solutions in a safe environment** with ADS organizations that have signed on to an agreement to participate in this exploration together (e.g., team of 2 from the Committee will plan the problem to discuss, lead the discussion, and identify the associated resource(s) to share)

Value this group/forum brings:

- **Experience and practical insights** on methods for implementing and growing SMS
- **A pragmatic, solutions-based approach** for how to put safety into action
- **A place to think and learn about SMS** outside of a direct company's practices and policies
- **People who are excited to collaborate!**

Special thank you to the Forum Committee Members!

Opportunities for Future Discussion

Future discussion topics identified by the Committee and Mini-Forum participants include:

1. Fostering a Safety Culture
2. Relating SMS to a Safety Case Framework
3. Communicating SRAs and Generating Buy-In for Action
4. Safety Reporting Framework and Targets
5. Integrating Quality Management and SMS
   - Inspection and Compliance Frameworks
6. Integrating Software Safety Assurance and SMS
7. Integrating Field Safety Monitoring and Software Safety Assurance

Prior forum topics have included:

- **Introduction to SMS and ADS (April 2021)**
- **Where to Start and How to Evolve Your SMS (October 2021)**
- **Getting Started With Organizational Safety Performance Indicators (October 2021)**

For additional resources and executive level summaries of prior events, visit adssafety.org

MITRE

Common Risk Controls in AV Industry

Risk controls will be applied across different types of hazards. Testing, for example, may be used to determine AV performance in different settings as a control, or the testing process types may be applied as controls when the hazard being assessed is an ineffective process.

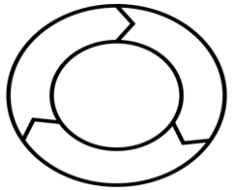
AV Performance
- Performance from on road
- Closed course testing performance
- Sim testing performance
- EURO/NCAP testing performance
- Fallback functionality

Other Road Users
- Reaction time to evade collision
- Federal, state and local laws

Safety Drivers
- Collision evasion
- Time to take control of vehicle
- Takeover intervention guidance
- Driver monitoring/fatigue management

Other
- Non-collision hazard controls
- Perception
- OSHA controls
- Tech stack

Training
- Classroom
- In vehicle
- On the job/ shadowing
- Interactive
- Self-guided
- Specialized certifications
- Technical Training



Processes/ Procedures
- Formally documented
- Checklists
- SOPs
- Tribal knowledge
- Development lifecycle for AV behaviors
- Maintenance QA
- Technician Certifications
- Calibration checks
- Operational Safety and integrity checks
- Auditing safety driver performance
- Process audit

Redundancy
(in sensors and processes)
- ASIL ratings
- Redundant electrical systems
- Dual compute
- Multiple sensor types

ODD Limitations
ODD Infrastructure
- Lighting
- Time of day
- Geofence
- Road configuration
- Traffic lights and signs
- Road conditions
- Rural/city
- Weather conditions
- Speed limits
- Visibility conditions
- Avoidance areas
- Operational time windows

Testing
- Simulation process
- Road testing (with drivers) process
- Closed course process
- EURO/ NCAP process

Vehicle Infrastructure
- Brakes
- Collision Avoidance
- Lane detection
- Base vehicle safety functions
- Degraded states

MITRE

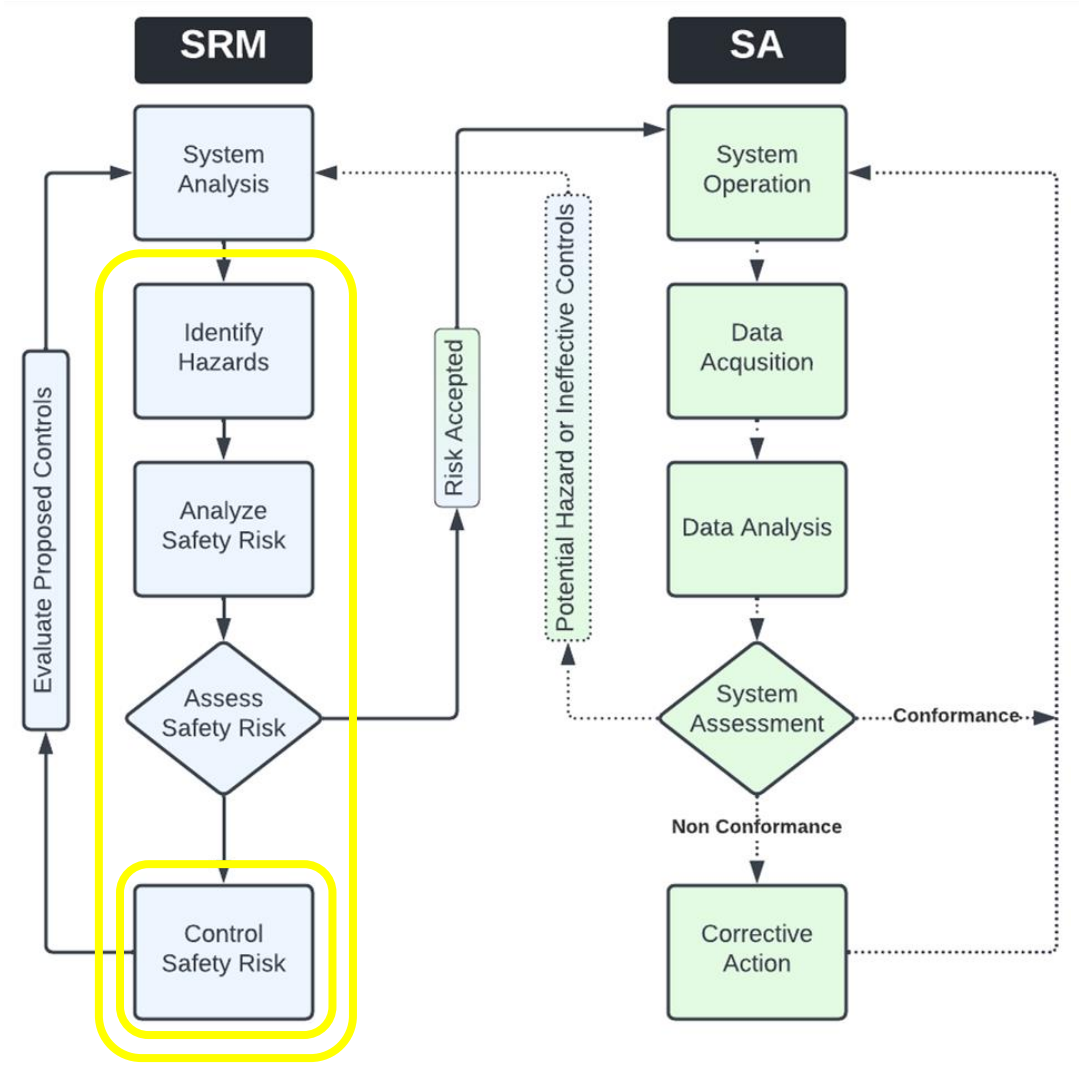
Analysis of Risk Controls in AV Hazardous Scenarios

Our analysis will necessarily be simplified

to focus on the yellow box and especially

to focus on safety risk controls that can

address hazards of AV system scenarios.



From Business Situations to Hazardous Scenarios

A poll of group interests identified **Business Situations** that involve SRA

From these, we identified **Hazardous Scenarios** that might fall within the scope of SRAs

- The scenarios are simplified and intended to support the objective of this session:
- To generate group discussion around specific AV examples of Risk Controls in SRA

Business Situation Examples

- *Should a planned demo/deadline be delayed because of known sensor issue*
- *Expansion from day to night, new territory, poor weather, etc.*
- *How to deal with lack of data for edge cases like offroad, GPS denied, etc.*
- *What barriers can catch if new code affects performance of a maneuver*
- *Lithium battery shipping/logistics, and relation between SRA and EHS*

Poll - Select the top 2 hazardous scenarios you'd like to explore together today

Hazard Scenario 1

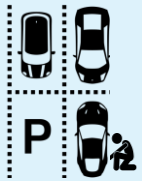
AV approaches a pedestrian crosswalk at night

Received 5/10 votes

Hazard Scenario 2

AV travels around a curve on an icy highway

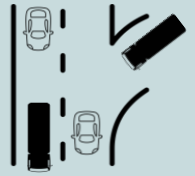
Received 2/10 votes



Hazard Scenario 3

AV is sabotaged by nefarious actor in parking lot

Received 4/10 votes



Hazard Scenario 4

AV merges onto highway in initial demonstration of capability

Received 5/10 votes

Hazard Scenario 5

Lithium battery overheats during operation of AV at intersection

Received 4/10 votes

★ Received top votes for discussion

Definitions

To focus discussion of each hazardous scenario

Hazard

A condition with the potential to cause harm or loss

Risk

A measure of potential (likelihood) for harm or loss (severity) resulting from the propagation of a hazard

Credible and Safety-Critical

A hazard that propagates to pose a risk with likelihood and severity each exceeding a threshold of concern

Questions

To focus discussion of each hazardous scenario

Q1: Hazard

What is one hazard that poses a credible and safety-critical risk?

Q2: Controls

What are some controls that can reduce the risk associated with this hazard?

Q3: Impacts

How would you quantify or qualify each control's impact on risk (via likelihood or severity)?

Q4: Sources

How would you justify each control's impact on risk (via data, models, judgments or other sources)?

Selected Scenario 1

Hazard Scenario 1

AV approaches a pedestrian crosswalk at night

Hazard *What is one hazard that poses a credible, safety-critical risk?*	**Controls** *What are controls that can reduce risk of this hazard?*	**Impacts** *How would you quantify or qualify each control's impact on risk (in terms of severity or likelihood)?*	**Sources** *How would you justify each control's impact on risk (using data, models, judgments, or other source)?*

• Vehicle does not detect pedestrian (e.g., pedestrian wearing dark clothes at night – vehicle stops, then proceeds)
  • Collision is the outcome/risk
	1. Vehicle platform controls are triggered (e.g., stock AEB, collision mitigation)
	  • vehicle visibility (e.g., headlights)
	2. Multi-sensor fusion in the autonomy
	3. Sim testing results (e.g., probability of system performance)
	4. Safety operator
	5. Pedestrian avoids car (e.g., does not step into road)
		Use risk matrix.
		Severity
		1 Catastrophic
		2
		3
		4 Negligible
		• Consider worst credible outcome for "initial" risk.
		• Leverage subject matter expertise.
		• Assume all controls are in place and functioning properly (unless SA program says otherwise based on organizational feedback (e.g., safety culture, submitted safety reports)).
		• Assess 'residual' risk. Do not double dip!
		• Explore how to connect safety methodologies – SMS, systems engineering, quality management – to iterate SRA.
		
		Systemic safety culture management as an area for exploration in AV industry - non-competitive, potential to leapfrog in safety performance.
		
		1) Vehicle platform controls: Leverage OEM test results of vehicle platform controls.
			• Consider orientation of pedestrian, angle of impact (e.g., sideways, facing vehicle).
			• Draw on scenario families from ODD (e.g., higher speed trucking, lower speed taxi).
			• Capture context in notes!

MITRE

Selected Scenario 2

Hazard Scenario 4

AV merges onto highway in initial demonstration of capability

Hazard *What is one hazard that poses a credible, safety-critical risk?*	**Controls** *What are controls that can reduce risk of this hazard?*	**Impacts** *How would you quantify or qualify each control's impact on risk (in terms of severity or likelihood)?*	**Sources** *How would you justify each control's impact on risk (using data, models, judgments, or other source)?*

• Vehicle gets into unsafe state (e.g., too close to another vehicle).
• Assume: Bust safety envelope in front of vehicle – front-end collision for AV.
  • Assume new code on the road.
  • Worst-case credible outcome is a collision.
 	
ISO 26262
• Does not consider autonomous controllability; autonomous system cannot take credit for controllability (?). (e.g., How well can human driver avoid catastrophic loss?).
• Component level standard applies to electronic components; does not apply to entire vehicle.
• Can be used to certify reliability of a component, not to certify AV behavior. Could inform estimate about whether a human operator could take over for automation.
	1. Rules of the road. Other drivers will merge predictably. Through traffic does not change speed to allow merging.
	2. Vehicle platform controls (e.g., forward collision warning/AEB)
	3. Safety operator – careful not to double dip for credit as existing control and mitigation (e.g., part of system state)
	4. Testing process (e.g., closed course testing, sim testing). How many runs, times passed? Pass criteria?
	
	Idea for future discussion:
	Development testing.
		1) Rules of the road compliance:
		Inform confidence that you put in control effectiveness:
		ODD characterization about typical behavior on this state/roadway.
		Crash statistics (at state level).
		
		2) vehicle platform controls
		Similar to hazard 1. Account for different criteria (e.g., humans, technology) to inform failure rates.
		Consider capability effectiveness based on speed.
		
		3) Safety operator
		Weight effectiveness as 0.5 for initial control and as 0.1 incremental mitigation from control.
			• Did you meet requirements during testing?
			• Regression analysis on testing. Analysis of anomalies. Repeat anomalies/repeat root causes.
			• Does test procedure assess the requirement correctly?

MITRE

Thank you!

We will follow up with session resources and a brief survey

For additional resources and executive level summaries of prior events, visit adssafety.org