Welcome!

Adapting Current Safety Risk Management (SRM) Practices with AV Testing to Address Safety Concerns

Virtual Mini-Forum: Part 1

Reminder: The 2nd part of this session is
Monday, March 28, 12:00pm-1:30pm ET

Upon entering the session:

1. Find yourself in the participant list

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:

What’s one thing you wish you had in your car right now?

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.

Housekeeping

Meeting Notes: MITRE to share non-attributed, summary-level notes that do not disclose participating organizations.

Transparency About Who's In this Virtual Room: All participants are to be registered and present on Zoom as themselves.

Agenda

12:00 – 12:10: Welcome and Housekeeping

12:10 – 12:45: SMS & Safety Risk Management
Safety Risk Assessment Deep Dive
Traditional SRM SRA Pros & Cons
Barrier-Based Methodology for SRAs

12:45 – 1:25: Discussion: Common Risk Controls to Address Safety Risk Challenges of the AV Industry

1:25 – 1:30: Setting the Stage for Part 2 and Closing

Reflection “Prompter” Questions

Consider the following questions as we move through today’s content…

- What’s your current experience with Safety Risk Management?
- What information would you consider when thinking about safety risk?
- What value do Safety Risk Assessments add?

SMS and Safety Risk Management

What is Safety Risk Management?

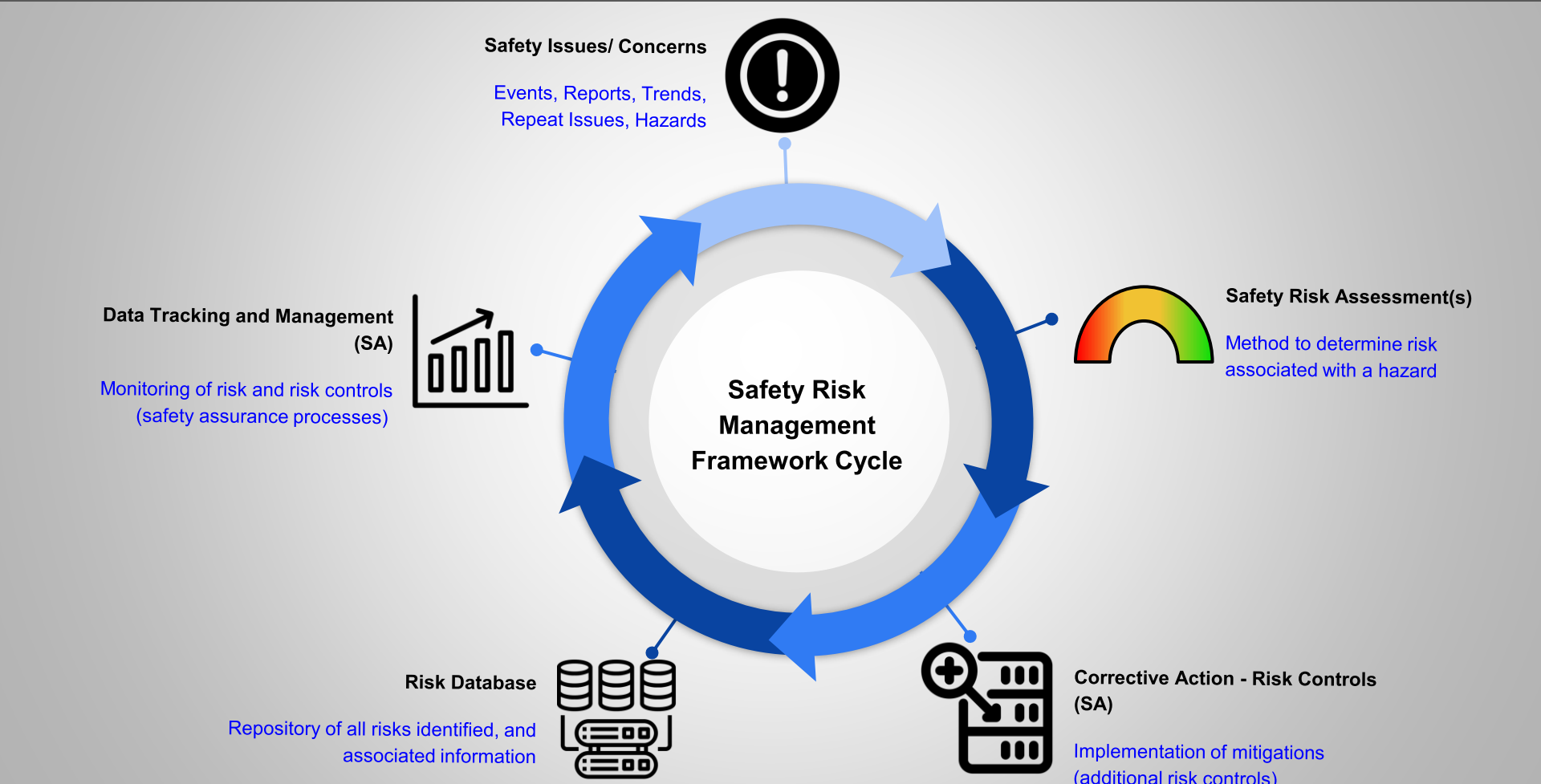
Framework with processes by which a hazard is identified, assessed, controlled and tracked throughout time.

SRM Common Definitions….

- The identification, analysis and elimination or mitigation of hazards and their associated risk
- A systemic, explicit, and comprehensive analytical approach for managing safety risk at all levels, and throughout the entire scope and lifecycle of an operation
- A disciplined assessment and management of safety risk

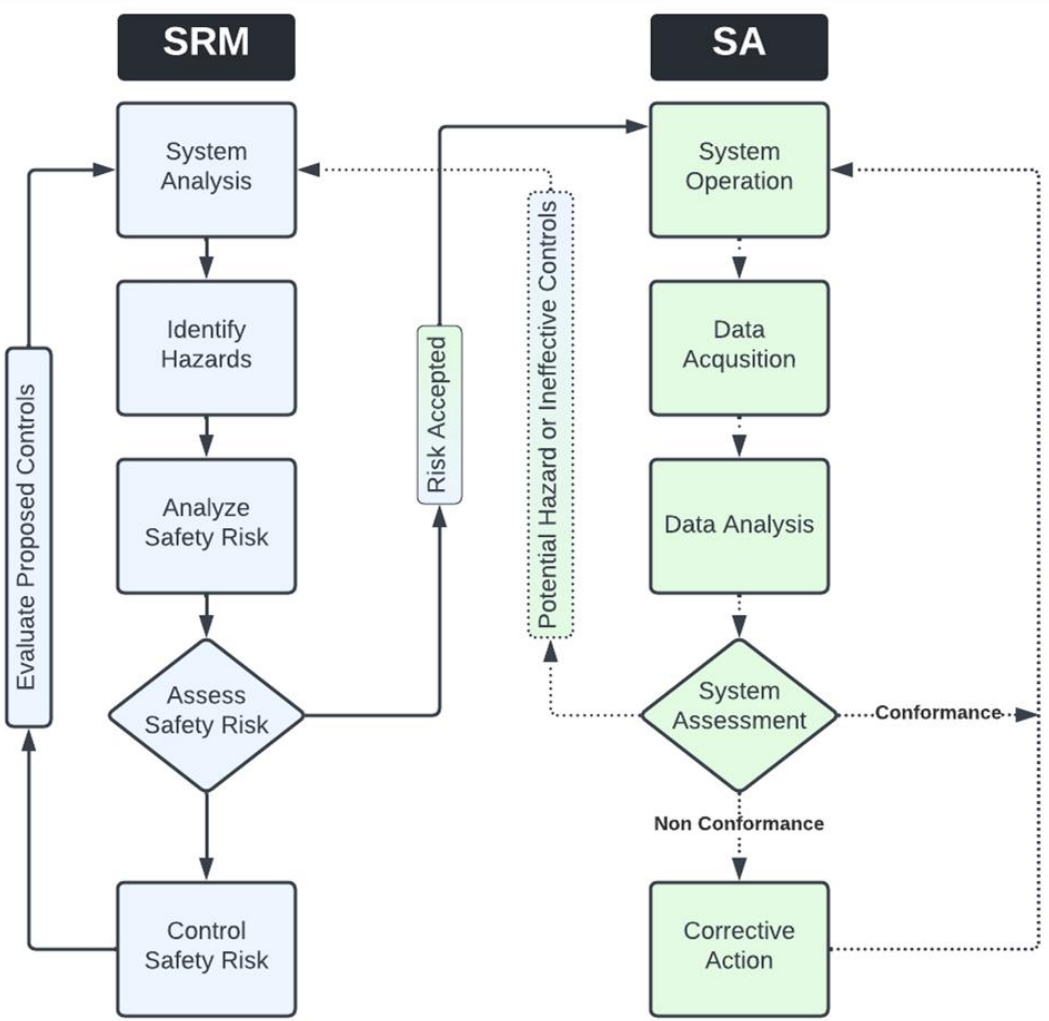
But what does that actually look like in practice?

SMS Safety Risk Management Framework Cycle



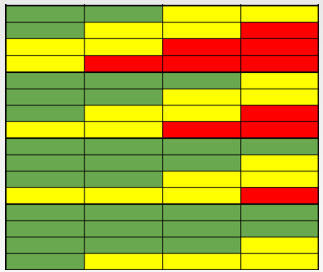
Safety Risk Management and Safety Assurance Interfaces

There is a cyclical relationship between SRM and SA



Risk Ownership in SRM

Risk Ownership
Authority and resources to mitigate risk, accountability for the risk of safety issues and corrective/ mitigation plans.



Safety Risk Assessment

Risk assessment complete and risk level surfaced.

Risk Level	Authority Position
	AE
	VP/ Director
	Manager

Authority Levels for Risk Ownership

Risk level determines role in organization with authority to make a decision about the risk.

Decision
Accept
Mitigate
Stop

Decision Options

Various decisions available for the risk owner to make.

Awareness Briefing and Risk Entry

Following decision, awareness of risk is provided to higher level safety boards/ committees (part of Safety Promotion). Risk is entered on the Safety Risk Registry.

Safety Risk Assessment Deep Dive

Value Added by SRAs

What value does completing SRAs provide to an organization?

- **Decision making tool - enable leaders to make decisions at the right time with the right information**
- Provide the organization with the ability to temporarily halt operations and contain risk
- Provide a piece of information necessary for enterprise risk management
- Provide a baseline of risk for management into the future. Future risk can be compared to baseline (continuous monitoring).

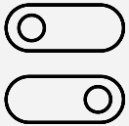
Considerations for Building an SRA Tool

What type of criteria are considered when completing an SRA?

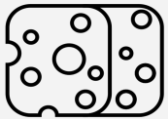
Severity

Likelihood/ Probability

Exposure



Controllability



Effectiveness of Controls

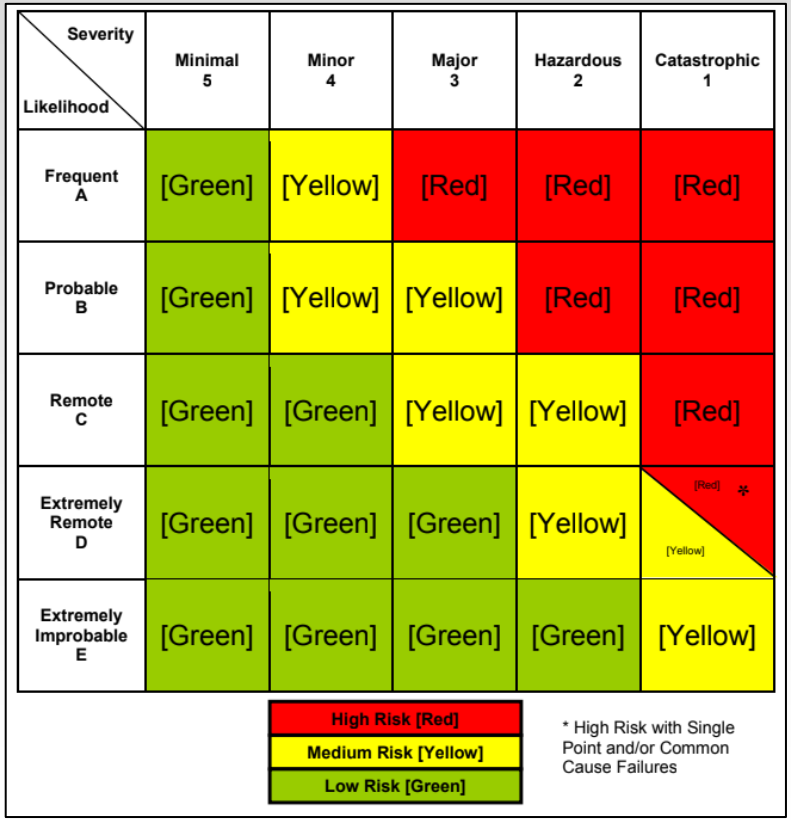
Traditional SRM SRA Pros and Cons

What is a Traditional SRA

The safety risk of a hazard is the function of the severity and likelihood of the hazard's potential outcomes. The safety risk associated with the hazard must be determined and documented in terms of severity and likelihood.

Severity is the potential consequence or impact of a hazard in terms of degree of loss or harm. It is a prediction of how bad the outcome of a hazard can be. There may be many outcomes associated with a given hazard, and the severity should be determined for each outcome.

Likelihood is the estimated probability or frequency, in quantitative or qualitative terms, of the outcome(s) associated with a hazard. It is an expression of how often an outcome of a hazard is predicted to occur in the future. When sufficient empirical data exists, statistical probabilities should be used.



Traditional SRA Pros and Cons

Pro's

- Traditional SRM via Severity and Likelihood are easy to teach the overall concept of Risk Assessment.
- Easy to compare risk from different sources or different analyses
- Easy to see the risk on a chart or matrix
- Can have quantitative data for both severity and likelihood as well as qualitative data
- Can allow for a very quick SRM analysis to get an immediate understanding of a given hazard. (i.e., Real time analysis V.S. planning (deliberate) analysis)

Con's

- Doesn't allow you to take in account for controllability, or say recognition that add to a more complex risk picture
- For multiple complex systems its harder to understand your overall risk vs. component or subsystem risk
- A quick SRM analysis may not show you all the risk that you could be exposed to

Traditional SRA Cons Scenario

Scenario

AV yielding to a jaywalking pedestrian (with safety drivers)

Hazard – AV not yielding to jaywalking pedestrian

Most likely outcome – collision with pedestrian

Severity – Depends on speed – need severity table that is informed by speed and geometry of vehicle collisions

Likelihood -
Likelihood of jaywalking pedestrian exposure?
Likelihood of AV not yielding?
Likelihood of Safety driver evading collision?

Inability to effectively root cause hazard after risk assessment due to inability to incorporate exposure and failure dimensions into a single likelihood dimension.

	Qualitative	Quantitative – Time/Calendar-based Occurrences Domain-wide/System-wide
Frequent A	Expected to occur routinely	Expected to occur more than 100 times per year (or more than approximately 10 times a month)
Probable B	Expected to occur often	Expected to occur between 10 and 100 times per year (or approximately 1-10 times a month)
Remote C	Expected to occur infrequently	Expected to occur one time every 1 month to 1 year
Extremely Remote D	Expected to occur rarely	Expected to occur one time every 1 to 10 years
Extremely Improbable E	Unlikely to occur, but not impossible	Expected to occur less than one time every 10 years

Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Negligible safety effect	– Physical discomfort to persons – Slight damage to aircraft/vehicle	– Physical distress or injuries to persons – Substantial damage to aircraft/vehicle	Multiple serious injuries; fatal injury to a relatively small number of persons (one or two); or a hull loss without fatalities	Multiple fatalities (or fatality to all on board) usually with the loss of aircraft/ vehicle

Barrier Based Methodology for SRAs

Barrier Based Thinking

Hazard
System, component, condition or concern with potential to cause harm to people or damage to resources.
A hazard is a condition that might cause (is a prerequisite to) an accident or incident.

Barrier/ Risk Control
Specific activities, systems, tools or procedures that are taken to prevent the risk associated with a hazard. This may include reducing the probability of an undesired outcome, reduction in exposure or reduction in severity.

Triggering Event
Event or condition that progresses the hazard to the undesired outcome

Recovery Barrier/ Risk Control
Specific activities, systems, tools or procedures that are taken to mitigate the risk associated with a hazard. This may include reducing the probability of an undesired outcome, reduction in exposure or reduction in severity.

Undesired Outcome
The consequence and its severity of harm or damage

Risk
Measure of potential for undesired outcome resulting from the propagation of a hazard.

Barrier Based SRA Pros and Cons

Pro's

- Allows you to take in account for controllability, and directly measure impact of risk controls in the risk assessment.
- Enables comparison of risk from different sources or different analyses
- Enables view of risk on a chart or matrix
- Can support qualitative and quantitative assessments (based on criteria tables).
- Enables the assessment to break down "likelihood" and measure hazard exposure, triggering event frequency, and risk control effectiveness.

Con's

- Identification of barriers that need to be taken into consideration, as they impact risk.
- Additive and non-additive barriers.
- Initial lift to develop criteria tables (for each dimension included in the risk assessment).
- Newer concept that takes more effort to educate others.
- Can be quickly over complicated

Common Example Risk Controls in AV Industry

AV Performance

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

Training

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

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

Other Road Users

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

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

Safety Drivers

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

Testing

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

Other

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

Redundancy

(in sensors and processes)

- ASIL ratings
- Redundant electrical systems
- Dual compute
- Multiple sensor types

Vehicle Infrastructure

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

*Blue font are additions made by the group during a discussion exercise.

Join us for Session 2!

Collaborative Application and Evolution of a Barrier-Based Tool Using Hazard Scenarios

- Workshop multiple scenarios to determine which risk controls from Session 1 apply to each
- Conduct light SRAs on the barrier-based tool for each scenario, with the incorporation of risk controls
- Review example criteria tables, and discuss how these can be taken to our respective organizations and revised to include specifics for our own organizations

Thank you!

See you next week!

Virtual Mini-Forum: Part 2
Monday, March 28, 12:00pm-1:30pm ET