CONNECTED VEHICLE PILOT
Deployment Program

Preparing a Safety Management Plan for Connected Vehicle Deployments

John Harding, Intelligent Technologies Research, NHTSA

ITS Joint Program Office

TODAY'S AGENDA

- Purpose of this Technical Assistance Webinar Series
  - To assist not only the three selected sites, but also other early deployers of connected vehicle technologies to conduct Concept Development activities.

- Webinar Content
  - Connected Vehicle Pilot Deployment Program Overview
  - Safety Management Plan Development
  - Stakeholder Q&A
  - How to Stay Connected

- Webinar Protocol
  - Please mute your phone during the entire webinar
  - You are welcome to ask questions via chatbox at the Q&A Section
  - The webinar will be recorded except the Q&A Section
  - The webinar recording and the presentation material will be posted on the CV Pilots website within a week

CV Pilot Deployment Program Goals

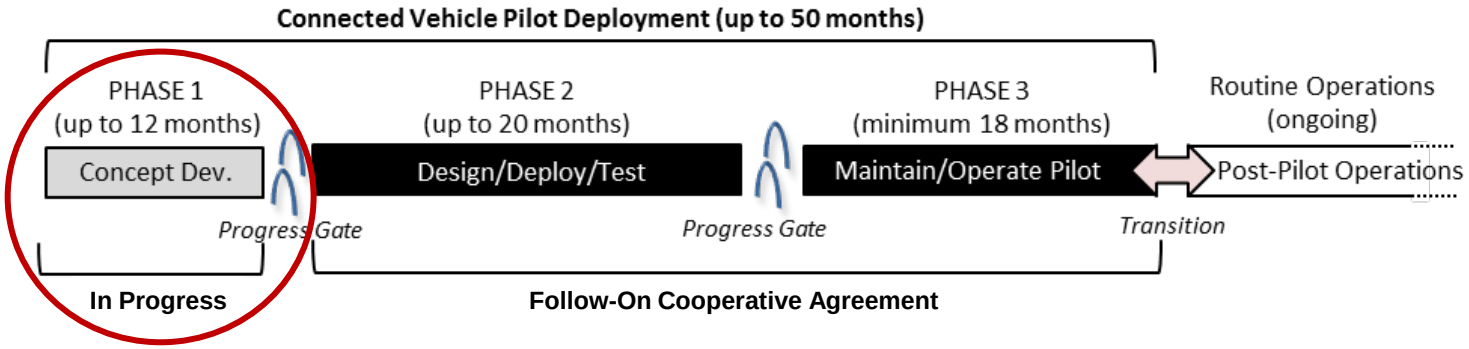
Sites Selected – 2015 Awards

- Reduce the number and severity of adverse weather-related incidents in the I-80 Corridor in order to improve safety and reduce incident-related delays.
- Focused on the needs of commercial vehicle operators in the State of Wyoming.

- Improve safety and mobility of travelers in New York City through connected vehicle technologies.
- Vehicle to vehicle (V2V) technology installed in up to 10,000 vehicles in Midtown Manhattan, and vehicle to infrastructure (V2I) technology installed along high-accident rate arterials in Manhattan and Central Brooklyn.

- Alleviate congestion and improve safety during morning commuting hours.
- Deploy a variety of connected vehicle technologies on and in the vicinity of reversible express lanes and three major arterials in downtown Tampa to solve the transportation challenges.

Deployment Schedule



- Overall Deployment Schedule
  - Phase 1: Concept Development
    - Creates the foundational plan to enable further design and deployment
  - Phase 2: Design/Deploy/Test
    - Detailed design and deployment followed by testing to ensure deployment functions as intended (both technically and institutionally)
  - Phase 3: Maintain/Operate
    - Focus is on assessing the performance of the deployed system
  - Post Pilot Operations (CV tech integrated into operational practice)
- Public webinars to share the concept development activities from the three sites
  - Concept of Operations Webinar (February – March 2016)
  - Performance Measurement Webinar (May – June 2016)
  - Deployment Plan Webinar (August 2016)

What is the Safety Management Plan?

The purpose of the Safety Management Plan is to systematically identify, assess, and minimize / mitigate safety risks associated with connected vehicle deployment.

Includes:

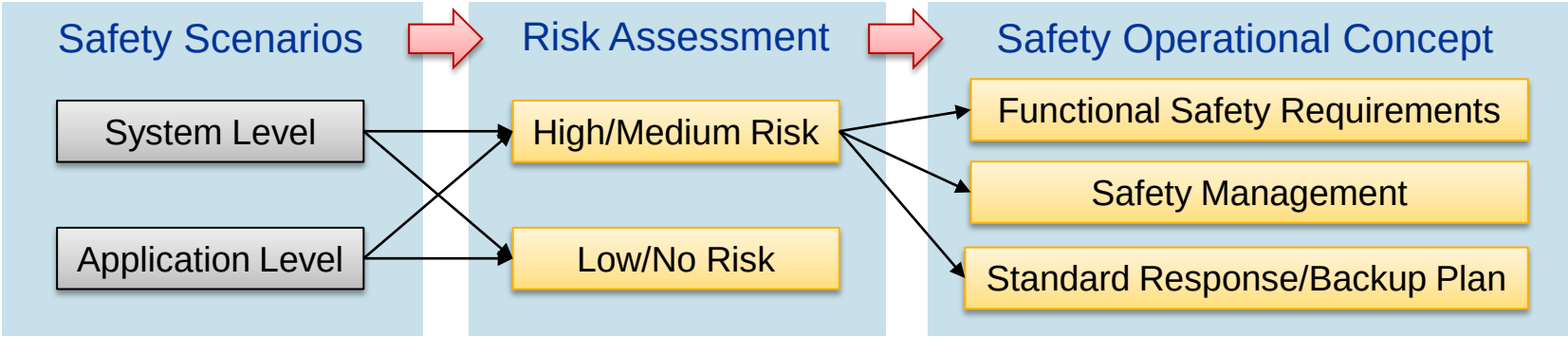
- identification and assessment of risks for *Safety Scenarios* related to the applications and technologies selected for the connected vehicle deployment
- development of a *Safety Operational Concept* that describes the actions expected to be taken within the design and deployment to reduce the likelihood and potential impact in each Safety Scenario.

Safety Management Plan is not ***Safety Evaluation***

- *Note that Safety Management planning is critical, yet different from Safety Evaluation. The purpose of Safety Evaluation is to evaluate safety impacts/benefits, while the purpose of the Safety Management Plan is to define approaches/processes for the identification and management/ minimization of the inherent safety risks associated with connected vehicle deployments.*

Safety Plan Development Process

- **Process**



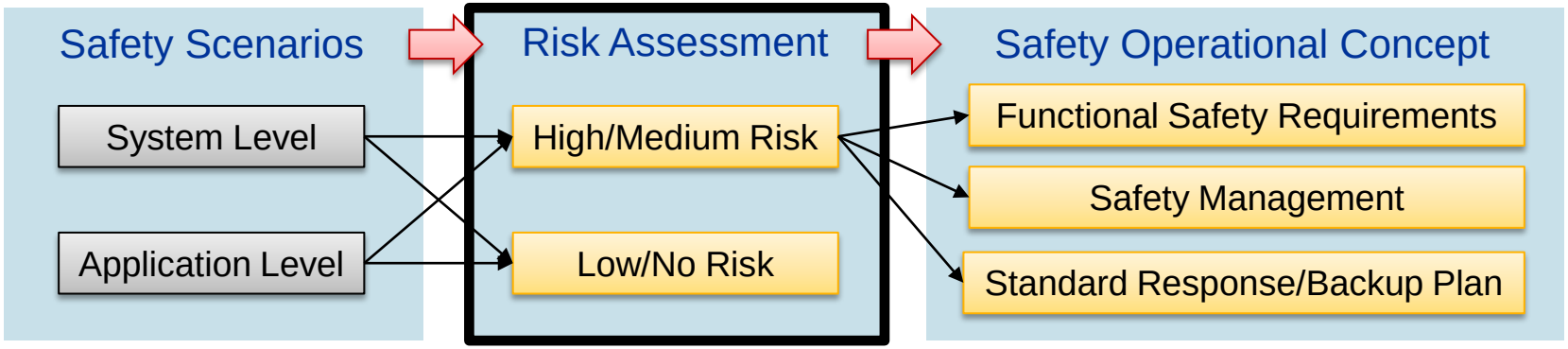
- **Examples**
  - Safety Scenario
    - System level: Power outages, communication failures, system hacks, unexpected events
    - Application Level: Hazardous product delivery, Pedestrian crossing detectors malfunction
  - Risk Assessment Approach
    - ISO 26262 ASIL (Safety Pilot) or other approaches
  - Safety Operational Concept
    - Functional Safety Requirements: Requirements to ensure safe operation of the application
    - Safety Management: Incorporation of safety from concept development to monitoring operations
    - Standard Response: Local emergency response procedure (e.g., Emergency Transportation Operations), Hazardous Materials/Dangerous Goods Regulations
    - Backup Plan: Back to pre-deployment status (shutdown deployment), a backup detection/warning system

Safety Scenarios

- System Level
  - Identify potential safety threats / risks that affect deployed CV system
  - Likely areas to examine include:
    - Communications
    - Security
    - Interfaces
    - Impacts outside CV system focus
      - Events, activities, weather
      - Awareness of other entities
        - Law enforcement
    - Consider potential safety risks beyond single application concept (collective environment)
    - Perceptions can also affect risks (behavioral changes)
    - Operational safety as well as functional

- Application Level
  - Identify ways in which application may not function as intended
    - Malfunction
    - Installation
    - Provide wrong information
      - Mobility application
  - Pay attention to interaction with non-equipped vehicles / vulnerable road users
  - Device or application issues and required updates
  - Installation that Impacts vehicle safety
    - Location of device/DVI
  - Human Factors
    - Driver Distraction – HMI/DVI

Risk Assessment Approach



- ISO 26262 one approach
  - Need to determine what approach fits situation
- ISO 26262 Overview
  - Oriented toward automotive electrical/electronic design process
  - Framework to assess and assist in preventing / mitigating safety risks
  - Automotive Safety Integrity Level (ASIL) establishes safety goal based on analysis of three dimensions:
    - Exposure
    - Severity
    - Controllability

ASIL – Three Dimensions

- Exposure – Probability of Exposure to situation (time/location) associated with Safety Risk
  - E1: Extremely low probability
  - E2: Low probability
  - E3: Medium probability
  - E4: High probability
- Severity – Direct harm to persons as a result of hazard
  - S0: No injuries
  - S1: Light and moderate injuries
  - S2: Severe and life-threatening injuries – survival probable
  - S3: Life-threatening injuries – survival uncertain
- Controllability – Ability to control scenario once exposed to hazard
  - C1: Simply controllable
  - C2: Normally controllable
  - C3: Difficult to control or uncontrollable

ASIL Level Determination

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

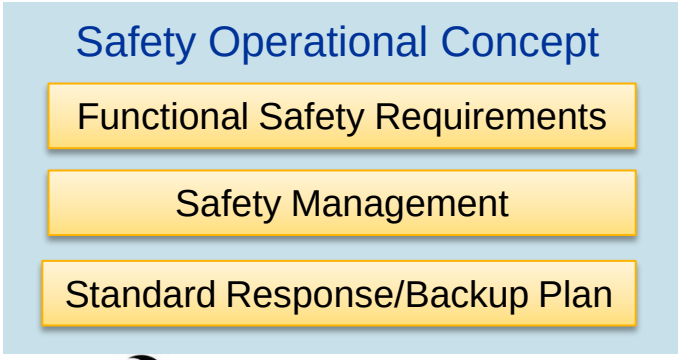
S=Severity, E=Exposure, C=Controllability

Example Risk Assessment

ID No.	Risk Register Reference	Category	Description	Impacts	Risk Response Plan	E	S	C	ASIL
4	54	Fleet Builds	Improper installation causes a device to misbehave	Safety of the participant. In this case, there is no increase to the potential injuries. Therefore, we designate the potential severity as SO. Since these are warning systems, the driver is still in control of the vehicle and will need to assess the situation and determine how to react. UMTRI can show with data collected on previous programs, such as IVBSS, that false warnings do not pose a hazard.	Include lessons learned and best practices from IVBSS and RDCW incorporated by UMTRI in the installation design. -Conduct design review of installation interface. -Verify installation before deployment (institute specific end-of-line testing and checklist procedures).	1	0	1	QM

Safety Operational Concept

- Implementing Safety Operational Concept
  - Identify Functional Safety Requirements for system, devices, applications
    - Collaboration with Suppliers and other related entities
    - Design and conduct supportive testing as needed
  - Develop response, action, and backup plans
    - Incorporate in design, operations, and training
  - Designate Safety Manager
    - Ongoing Safety Management
      - Incorporate safety into design/deployment, and Operational phases
      - Testing and Installation
      - Change and Configuration Management
      - Operational Safety and Monitoring
      - Documentation and Training
      - Maintenance and updates
      - Coordination with other entities



Safety Challenges

- Risk Assessment
  - Issue: Overestimate/underestimate the risk
  - Possible Strategy: Identify different level of risk using risk assessment approach
- Site-Specific Safety Plan
  - Issue: Safety scenarios vary depending on deployment sites/applications selected
  - Possible Strategy: Develop a site-specific safety plan
- Local Support
  - Issue: Coordinate with various local emergency response agencies
  - Possible Strategy: A safety manager coordinating and executing the procedure
- Reaction of Participants
  - Issue: Participants are not aware of the safety scenarios and the corresponding responses
  - Possible Strategy: Include in the training plan

Useful References

- NHTSA, Integrated Vehicle-Based Safety Systems Preliminary Field Operational Test Plan, http://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2008/811010.pdf
- NHTSA, Road Departure Crash Warning System Field Operational Test: Methodology and Results, http://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2006/RDCW-Final-Report-Vol-1_JUNE.pdf
- NHTSA, Vehicle Safety Communications – Applications Final Report, http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2011/811492A.pdf
- NHTSA, Safety Pilot Model Deployment: Test Conductor Team Report, http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2015/812171-SafetyPilotModelDeployDelTestCondrTmRep.pdf
- International Organization for Standardization, *ISO 26262 Road Vehicles - Functional Safety* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43464
- USDOD, Department of Defense Standard Practice – System Safety (MIL-STD-882E), http://www.system-safety.org/Documents/MIL-STD-882E.pdf
- Federal Emergency Management Agency, Operational Lessons Learned in Disaster Response, http://www.usfa.fema.gov/downloads/pdf/publications/operational_lessons_learned_in_disaster_response.pdf
- Pipeline and Hazardous Materials Safety Administration, 2012 Emergency Response Guidebook, *http://phmsa.dot.gov/pv_obj_cache/pv_obj_id_7410989F4294AE44A2EBF6A80ADB640BCA8E4200/filename/ERG2012.pdf*

Stakeholder Q&A

- Please keep your phone muted
- Please use chatbox to ask questions
- Questions will be answered in the order in which they were received
- This Q&A section will not be recorded, nor posted to the website

STAY CONNECTED

Join us for the *Getting Ready for Deployment* Series

- Discover more about the Wave 1 CV Pilot Sites
- Learn the Essential Steps to CV Deployment
- Engage in Technical Discussion

Website: http://www.its.dot.gov/pilots

Twitter: @ITSJPODirector

Facebook: https://www.facebook.com/DOTRITA

Contact for CV Pilots Program:

Kate Hartman, Program Manager

Kate.hartman@dot.gov

December 2015 Technical Assistance Webinars:

- 12/7/2015, 2:00 – 3:30 pm EST
  Preparing a Safety Management Plan for Connected Vehicle Deployments
- 12/9/2015, 1:30 – 3:00 pm EST
  Preparing a Security Concept for Connected Vehicle Deployments
- 12/10/2015, 12:30 – 2:00 pm EST
  Preparing Institutional/Business Models and Financial Sustainability for Connected Vehicle Deployments

Please visit the CV pilots website for the recording and the briefing material of the previous webinars.