

Software Certification Consortium

medical devices
automotive

22ND SOFTWARE CERTIFICATION CONSORTIUM MEETING

MAY 9-10, 2024

Co-located with High Confidence Software and Systems 2024 - Annapolis

THEME: *SAFE & SECURE REMOTE OPERATION OF SAFETY-CRITICAL SYSTEMS*



Status and Challenges of Remote Operation of Motor Vehicles

Dr. Joseph D'Ambrosio, Dr. Ramesh S.
General Motors R&D

joseph.dambrosio@gm.com

ramesh.s@gm.com

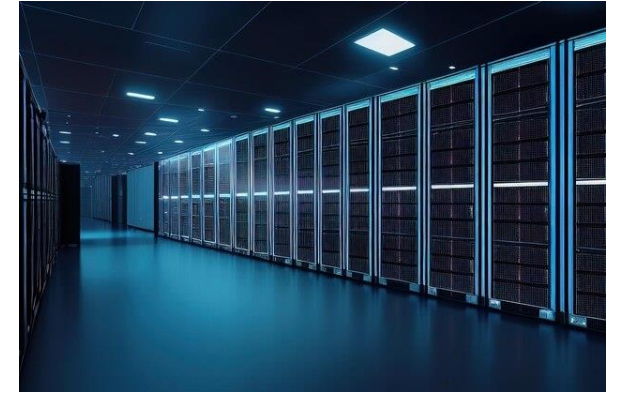


Overview

- Vehicle Remote Operation Enablers
- Relevant Automotive Trends
- Automotive Safety Standards
- Automotive Remote Operation Examples
- Summary

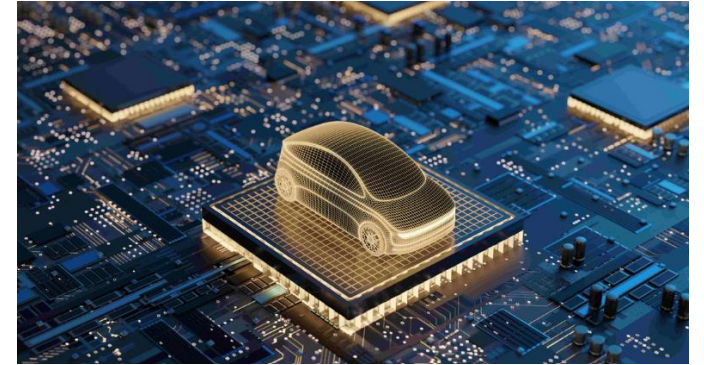
Remote Operation Enablers

- Secure connected vehicle
 - Cellular, Wifi, BTLE, or UWB
 - Cloud Services / Back Office
 - APIs providing access to:
 - Vehicle state information / diagnostics
 - Reprogramming
 - Sufficient QoS
- Electronically controlled actuators w/ control SW APIs
 - Steering
 - Braking
 - Propulsion / throttle
 - Transmission
 - Park brake
- Remote Interface Support
 - Monitoring devices
 - Vehicle state information
 - Situational awareness of external environment
 - Camera, GPS, ...
 - Remote input/ command devices
 - Automated (e.g., continuous deployment)
 - Driving command capture

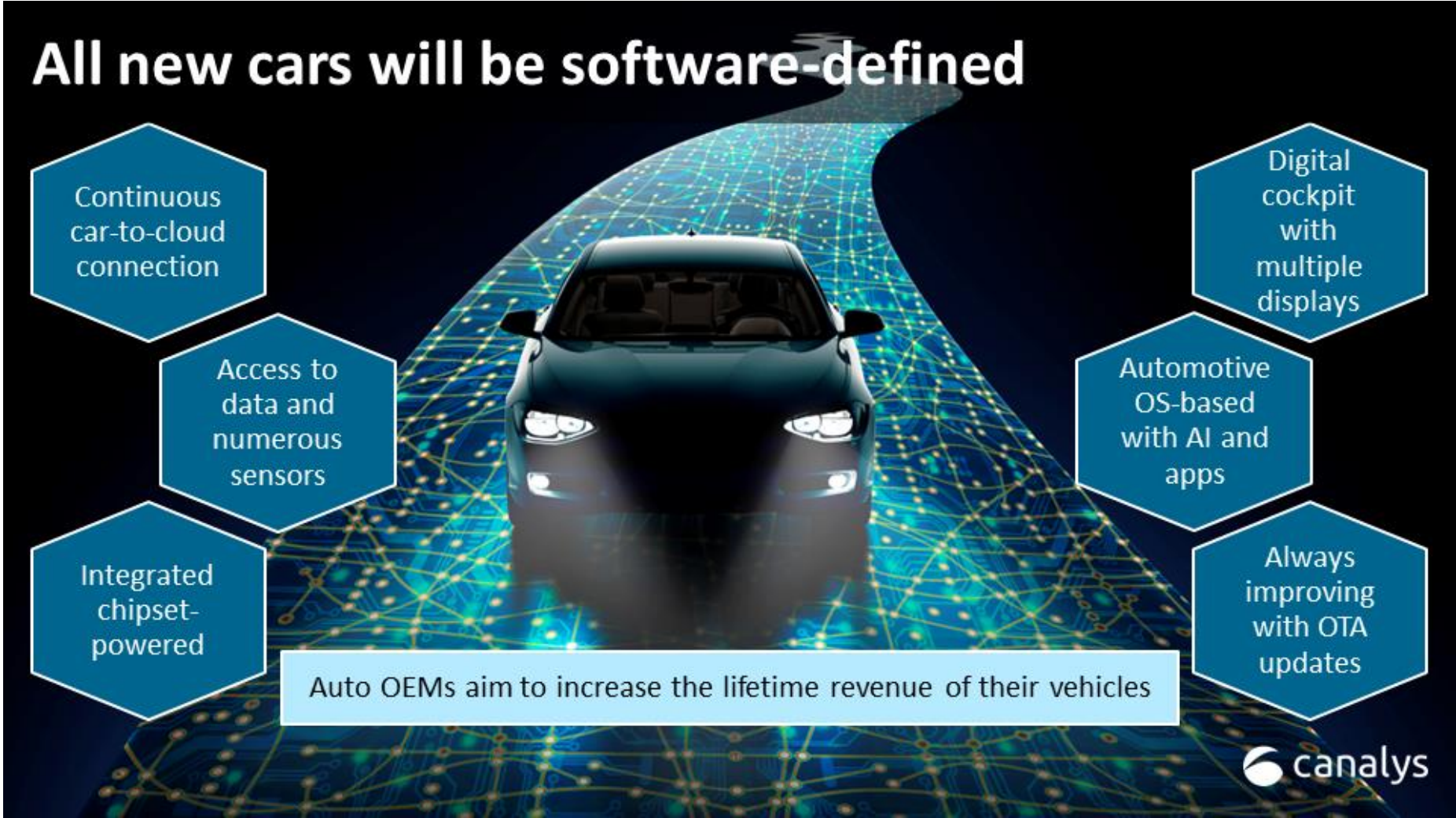


Overview

- Vehicle Remote Operation Enablers
- Relevant Automotive Trends
 - SDV
 - Connected Vehicle
 - ADAS & AV
 - Connected ADAS & Autonomy
- Automotive Safety Standards
- Automotive Remote Operation Examples
- Summary

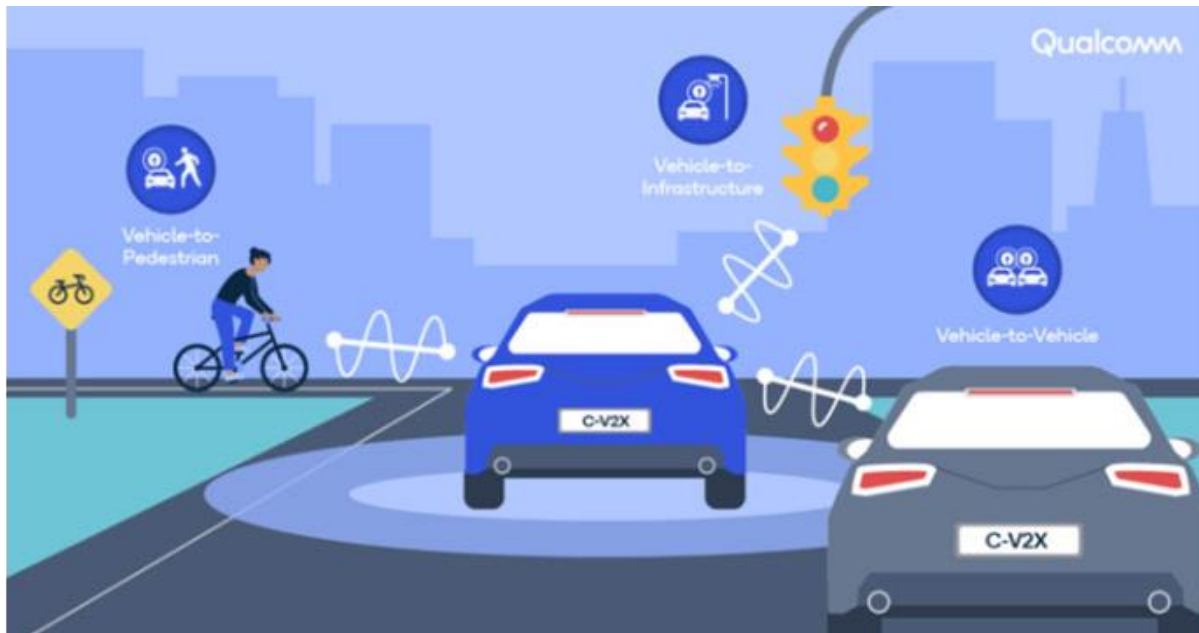


Software Define Vehicle

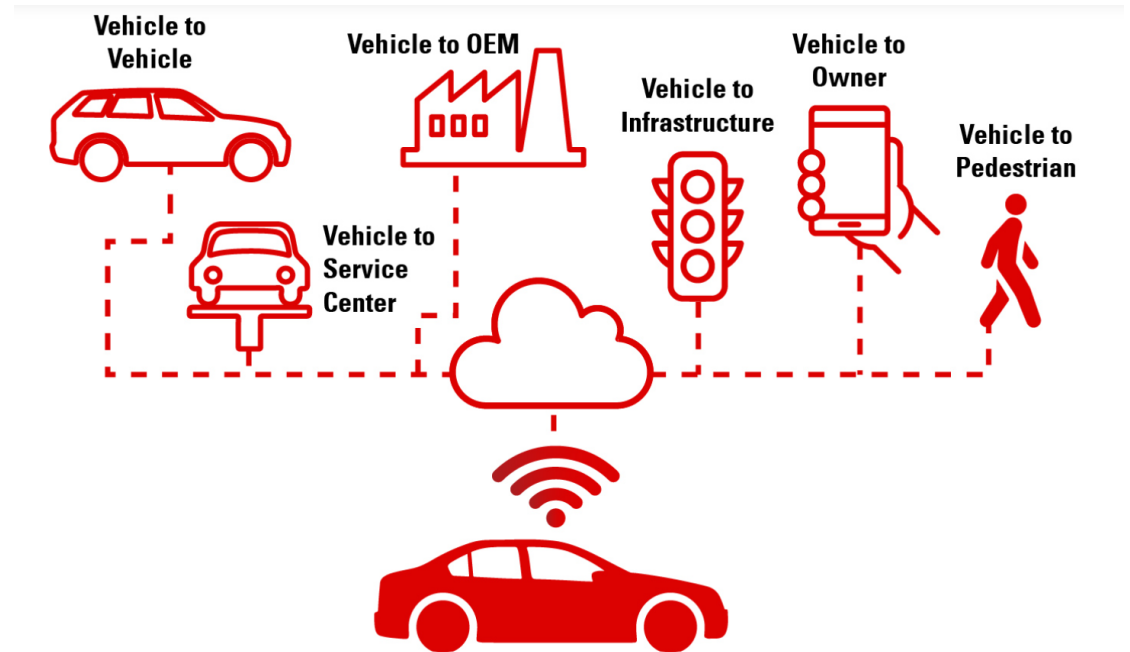


REF <https://www.canalys.com/insights/automotive-industry-future>

Connected Vehicles & Smart Cities



REF <https://www.qualcomm.com/news/onq/2020/11/c-v2x-delivers-outstanding-performance-automotive-safety>



REF: <https://www.nexteer.com/blog/software-defined-vehicles-where-we-are-and-where-were-heading/>

ADAS and Automated Driving



REF <https://www.ansys.com/blog/linking-safety-management-software-simplifies-ad-as-autonomous-car-design>



SAE J3016™ LEVELS OF DRIVING AUTOMATION

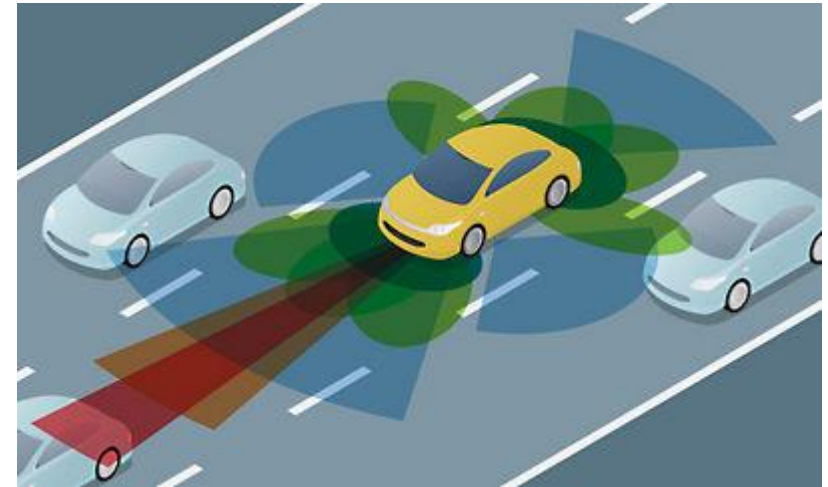
	SAE LEVEL 0	SAE LEVEL 1	SAE LEVEL 2	SAE LEVEL 3	SAE LEVEL 4	SAE LEVEL 5
What does the human in the driver's seat have to do?	You <u>are</u> driving whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			You <u>are not</u> driving when these automated driving features are engaged – even if you are seated in “the driver’s seat”		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	
What do these features do?	These are driver support features			These are automated driving features		
	These features are limited to providing warnings and momentary assistance	These features provide steering OR brake/acceleration support to the driver	These features provide steering AND brake/acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met	This feature can drive the vehicle under all conditions	
Example Features	<ul style="list-style-type: none"> • automatic emergency braking • blind spot warning • lane departure warning 	<ul style="list-style-type: none"> • lane centering OR • adaptive cruise control 	<ul style="list-style-type: none"> • lane centering AND • adaptive cruise control at the same time 	<ul style="list-style-type: none"> • traffic jam chauffeur 	<ul style="list-style-type: none"> • local driverless taxi • pedals/steering wheel may or may not be installed 	<ul style="list-style-type: none"> • same as level 4, but feature can drive everywhere in all conditions

Connected Autonomy

- Goes beyond vehicle receiving an autonomous driving mission
- Examples:
 - External “data” directly influences ADAS or Autonomous Features
 - Feature capability partially resides off the vehicle
 - Autonomy as a service



+



Overview

- Vehicle Remote Operation Enablers
- Relevant Automotive Trends
- Automotive Safety Standards
 - ISO 26262
 - ISO TS 5083
 - ISO PAS 8800
 - Others
- Automotive Remote Operation Examples
- Summary

1. Vocabulary		
2. Management of functional safety		
2.5 Overall safety management	2.6 Safety management during the concept phase and the product development	2.7 Safety management after the item's release for production
3. Concept phase		
3.5 Item definition	4. Product development at the system level	
3.6 Initiation of the safety lifecycle	4.5 Initiation of product development at the system level	4.11 Release for production
3.7 Hazard analysis and risk assessment	4.6 Specification of the technical safety requirements	4.10 Functional safety assessment
3.8 Functional safety concept	4.7 System design	4.9 Safety validation
	4.8 Item integration and testing	
	5. Product development at the hardware level	
	5.5 Initiation of product development at the hardware level	6. Product development at the software level
	5.6 Specification of hardware safety requirements	6.5 Initiation of product development at the software level
	5.7 Hardware design	6.7 Software architectural design
	5.8 Evaluation of the hardware architectural metrics	6.8 Software unit design and implementation
	5.9 Evaluation of the safety goal violations for the product hardware	6.9 Software unit testing
	5.10 Hardware integration and testing	6.10 Software integration and testing
		6.11 Verification of software safety requirements
7. Production and operation		
7.6 Production		
7.8 Operation, service (maintenance and repair), and decommissioning		
8. Supporting processes		
8.5 Interfaces with distributed developments	8.10 Documentation	
8.6 Specification and management of safety requirements	8.11 Confidence in the use of software tools	
8.7 Configuration management	8.12 Qualification of software components	
8.8 Change management	8.13 Qualification of hardware components	
8.9 Verification	8.14 Process to use argument	
9. ASIL-oriented and safety-oriented analysis		
9.5 Requirements decomposition with respect to ASIL labelling	9.7 Analysis of dependent failures	
9.8 Criteria for coexistence of elements	9.8 Safety analysis	
10. Guideline on ISO 26262		



Safety Standards: ISO 26262 Road Vehicles – Functional Safety

- Functional Safety of EE Systems installed in production vehicles
 - Vehicle safety life cycle requirements
- Item – what is being developed
- Item Context:
 - Item contained within single vehicle
 - Vehicle has full authority and full responsibility for the item's operation / function
- Not sufficient for remote operations safety

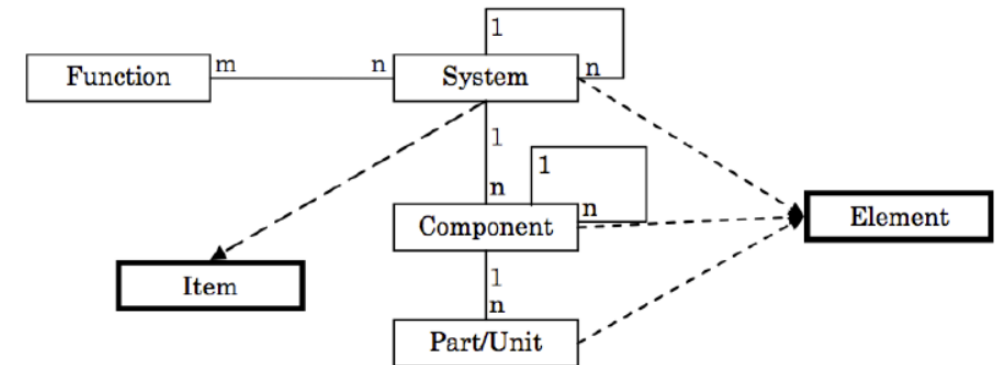
ISO 26262-1:2018

Road vehicles

Functional safety

Part 1: Vocabulary

Status : **Published**



Safety Standards: ISO TS 5083

- Scope / Focus
 - Overarching standard linking others with a specialized focus
 - Adopts SAE J3016 Definitions
 - Primarily targeting SAE Levels 3 & 4
 - Risk acceptance criteria
 - Cybersecurity considerations
- Consideration of the following
 - Remote assistance
 - Modify goals / constraints,
 - Does not include “teleoperations”
- Concept of data safety
 - Data properties
 - Confidence in source provider
 - Refinement of confidence
 - Environment and command data

ISO/CD TS 5083

Road vehicles

Safety for automated driving systems


Design, verification and validation

Status : **Under development**

CURRENT **REVISED** 2021-04-30

Taxonomy and Definitions for Terms
Related to Driving Automation Systems
for On-Road Motor Vehicles

[J3016_202104](#)



LEVEL 3	LEVEL 4	LEVEL 5
Conditional Automation	High Automation	Autonomous
System drives the car; drivers are expected to respond when requested	Vehicle performs all driving functions under limited conditions	Vehicle performs all driving functions

AUTOMATED Driving Features

Remote Updates for AI Based Systems Continuous Assurance

- ISO PAS 8800 is an emerging standard for AI based components and subsystems
- Remote Monitoring and Updates necessary elements in next gen ADS systems with the use of AI components
- Data Distribution Shift monitoring is an important aspect
- Any shift impacting the safety addressed with remote update of AI parameters
- Continuous assurance, an important requirement
- Data Collection for potential trigger conditions and edge cases in AI based systems

ISO/CD PAS 8800

Road Vehicles

Safety and artificial intelligence

Status : [Under development](#)

Safety Standards: Others

- ISO 4272:2022
 - Definitions, Platooning Control System (PCS) Modes
 - Joining & leaving platoons
 - Longitudinal and lateral control
 - V2V & optional V2I messages

ISO 4272:2022

Intelligent transport systems

Truck platooning systems (TPS)

Functional and operational requirements

Status : **Published**

Emerging Safety Case Approach for ADS w/ External Elements

- For safe operation of ADS, several external elements may be relied upon for safe operation
 - Will be comprehended by ISO TS 5083
 - Examples: Remote assistance to ensure safety, centralized vehicle management, Map updates, Weather and road condition updates
- Safety requirements allocated to both ADS and External elements
- Safety case may make assumptions of external elements

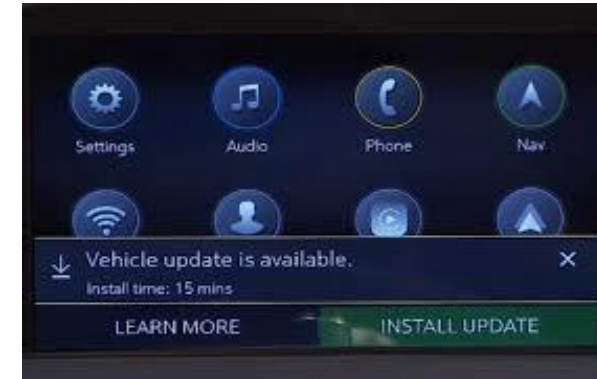
Overview

- Vehicle Remote Operation Enablers
- Relevant Automotive Trends
- Automotive Safety Standards
- **Automotive Remote Operation Examples**
- Summary



Over the SW air updates

- Key aspects
 - Secure reprogramming
 - Confirmation of update process
 - Tracking of software versions
- How to validate update across vehicle variants?



Stolen Vehicle Assistance: Remote Slowdown

- Stolen Vehicle Slowdown Protocol
 - Owner reports vehicle stolen
 - Remote identification of vehicle location identified using connected vehicle GPS
 - Police locate vehicle
 - Remote engagement of vehicle flashers
 - Police confirm flashers on
 - Remote ramp down of vehicle speed to idle.



ADS Remote Assistance for Edge Cases

- Autonomous driving systems “phones a friend”
- Remote operator assesses situation
- ADS goals / task modifications
- Benefit of human in the loop for edge cases



REF <https://nyc.streetsblog.org/2020/02/07/new-city-rule-tells-truckers-dont-even-think-of-double-parking-here>

Human in the Loop Autonomy



- Proactive human remote control for challenging situations
- Benefits
 - Enhanced safety case vs. autonomous only control
 - Improved quality of life for drivers



Remote Driving: Fleet Operations

- Vehicle control
 - Drive by wire vehicles
 - Low speed operation
- Target operation areas
 - Parking lots and garages
 - Vehicle manufacturing plants
 - Loading / unloading for long haul transportation



BMW CES 2024 Remote Driving Demo

REF <https://arstechnica.com/cars/2024/01/bmw-adds-a-human-touch-to-driverless-parking-at-ces-2024/2/>

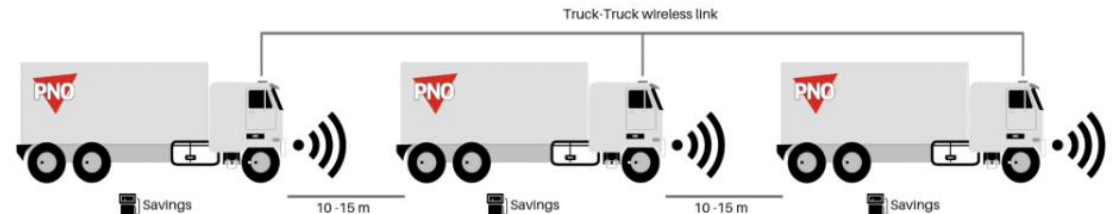
Vehicle Platooning

Cooperative Braking

- Leader / follower operation a vehicle convoy
- Technologies
 - By-wire driving
 - Connectivity
- Benefits:
 - Improved fuel economy
 - Reduce congestion
 - Safer operation of large vehicles
- Challenges:
 - Forming / dissolving platoon
 - Vary performance
 - Loss of communications
 - Non platoon vehicle cut ins
 - Handling emergency situations



REF <https://pnorental.com/truck-platooning-the-future-of-road-transport/>



DoD / US Army Unmanned Ground Vehicles

- UGV capability Classes:
 - Leader / Follower
 - Teleoperation
 - Platform autonomous operation
 - Network autonomous operation
- US Army Robotic Combat Vehicle (RCV)
 - Defense Innovation Unit – teleoperation of unmanned vehicles
- Challenges
 - Potentially only passive sensing
 - Hazards obscured by vegetation, water, ...

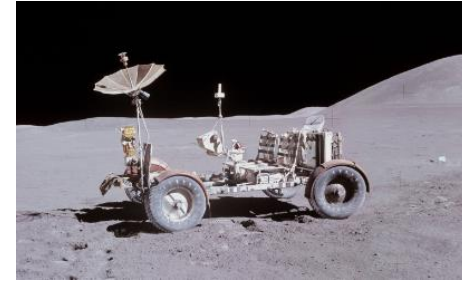


<https://breakingdefense.com/2023/06/army-closing-down-leader-follower-robotic-truck-development-eyeing-commercial-solutions/>

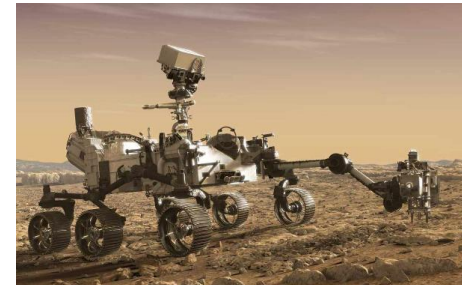


Space Mobility: NASA Artemis Lunar Terrain Vehicle

- 2029 ARTEMIS 5 Mission
- Manual & remote operation
- Challenges include:
 - Poor vehicle handling
 - Communications
 - 2-8 second delays
 - Areas with no communications
 - Sun Light
 - Sun light just above horizon
 - Large dark shadowed regions
 - Permanent dark areas
 - Low resolution terrain maps
 - Uncertainty of GPS availability
 - Regolith dust



Apollo Lunar Rover
BEV, 13 kph



Perseverance Rover
0.16 kph
Autonomous /
Remote Control



Artemis LTV
BEV, Solar Panels
15 kph
Autonomous /
Remote Control

Summary

- Growing demand for vehicle remote operation
- Newer vehicles have necessary enablers for remote operation
- Published safety standards not sufficient
- Emerging ISO standards may help address some gaps
- Teleoperation / human remote real time performance of dynamic driving task not a current focus

Factors for Developing Remote Operation Safety Case

- Impact of Role of Remote Operator on Safety Case
- Human in the loop autonomous
 - Remote operator attentiveness
 - Remote operator override
 - Situational Awareness
 - Loss of communication
- Teleoperation
 - Situational awareness
 - Communication delays / loss
- Operational Environment
 - Static vs. dynamic
 - Controlled vs. uncontrolled
- Operating speed
- Environment sensing
 - Vehicle sensor vs. external sensors
- Loss of communications
 - Transition to safe state vs. continue operation