

# What Happens When Vehicle Computers Become Obsolete?

Christopher Bonati, CEO & Principal, The Baluster Group

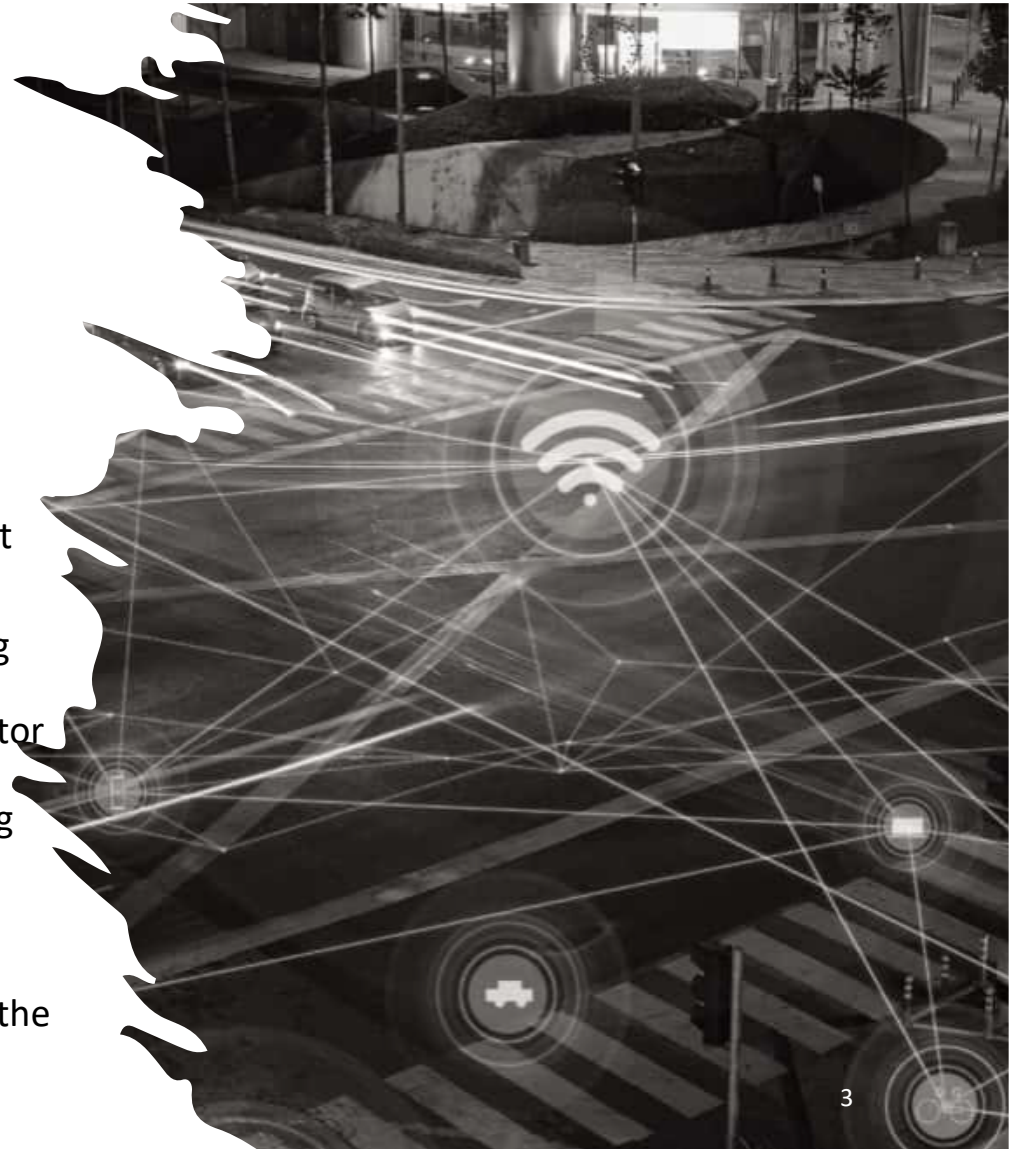


# Disclaimer

All discussion, comments, photographs, videos, etc. made during this presentation are meant for general training and educational purposes only and shall not be considered a professional opinion regarding any specific claim or legal matter.

# Qualifications & Experience to Speak to You

- Over 20 plus years of experience involved in federal investigations, regulations, compliance and oversight processes
- Investigator with NTSB, Staffer on U.S. Senate and U.S. House Committees, Chief of Staff at FRA, Director at FAA, lastly served as Associate Administrator for Rulemaking at NHTSA.
- Served as the senior executive responsible for rulemaking within the automotive and commercial vehicle industries and led the development and oversight of all Federal Motor Vehicle Safety Standards (FMVSS)—covering crashworthiness and crash avoidance matters, and testing protocols necessary to meet these standards.
- Led NHTSA's Corporate Average Fuel Efficiency (CAFE) program, the New Car Assessment Program (NCAP), the agency's vehicle theft prevention initiative, and oversaw the agency's international program.



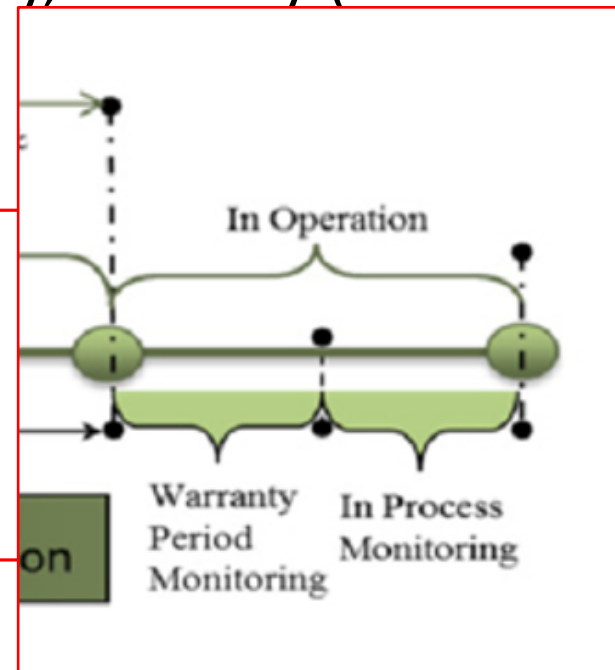
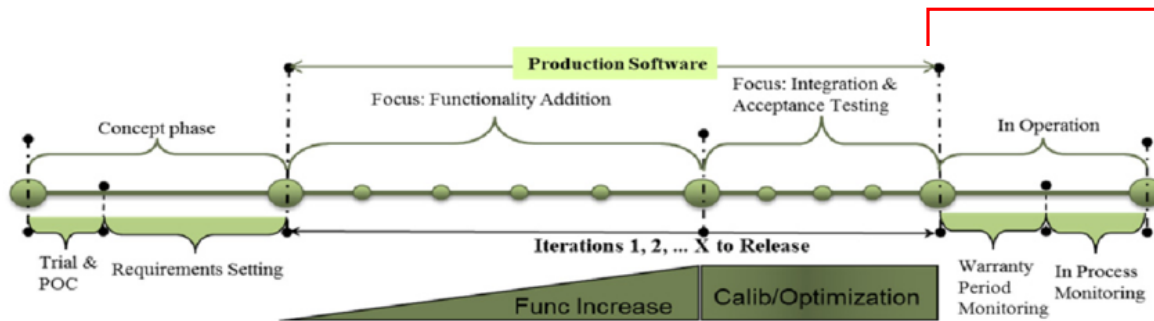
# Vehicle Computer Obsolescence & Insurance Risk

- Implications for the industry include:
  - Software Obsolescence  
Central Cause of Concern
  - Systemic risk of  
incompatible technology  
integration
  - Automotive Regulatory  
Uncertainty – Strategically  
Looking Around Corners



# Foundation of the Problem

- Vehicle lifecycle (15–25 years) vs. software lifecycle, which is supposed to be (10-15 years), but in reality, it's likely (3–7 years).
- Creates cyber-physical risk exposure



Source: Rana, R (2014), Defect Prediction over Software Life Cycle in Automotive Domain State of the Art and Road Map for Future, 2014 9th International Conference on Software Engineering and Applications (ICSOFT-EA)

# Claims Severity Inflation

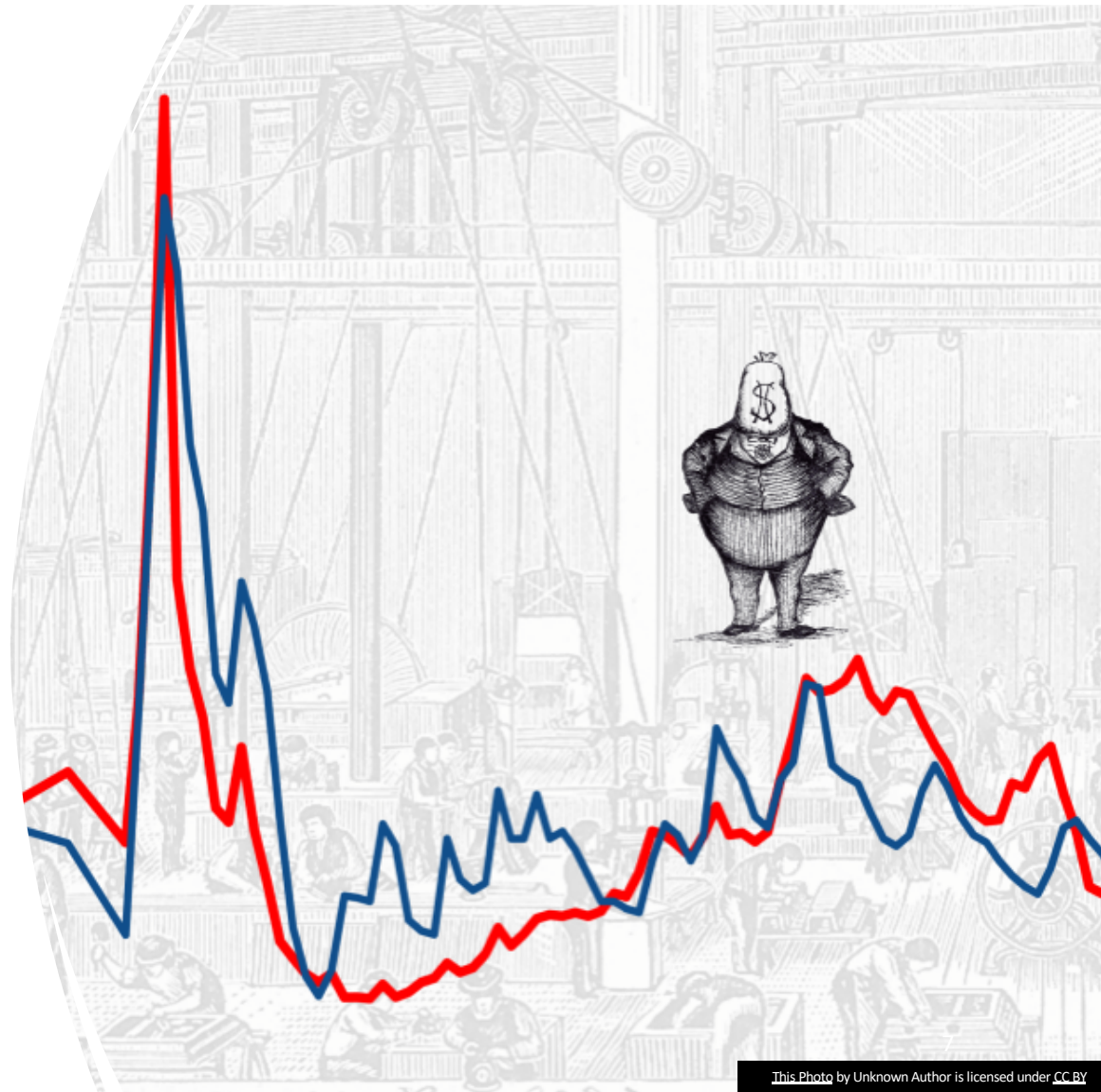
- Parts obsolescence
  - OEMs discontinue ECUs, sensors, and wiring harnesses
  - Secondary markets (salvage/rebuilt modules) introduce quality variability risk
- Software incompatibility
  - New replacement modules may not interface with legacy CAN/LIN architectures
  - Firmware no longer supported in its ability to flash or calibrate
- ADAS calibration challenges
  - Radar, LiDAR, and camera systems require post-repair calibration
  - If calibration tools/software are depreciated  vehicle is effectively non-repairable
- Higher total loss frequency



# Repair Economics

---

- ECU (electronic control unit) replacement challenges
- Limited OEM support
- Salvage market dependency
- Rising repair costs
- No Automotive industry standard for universal component connections

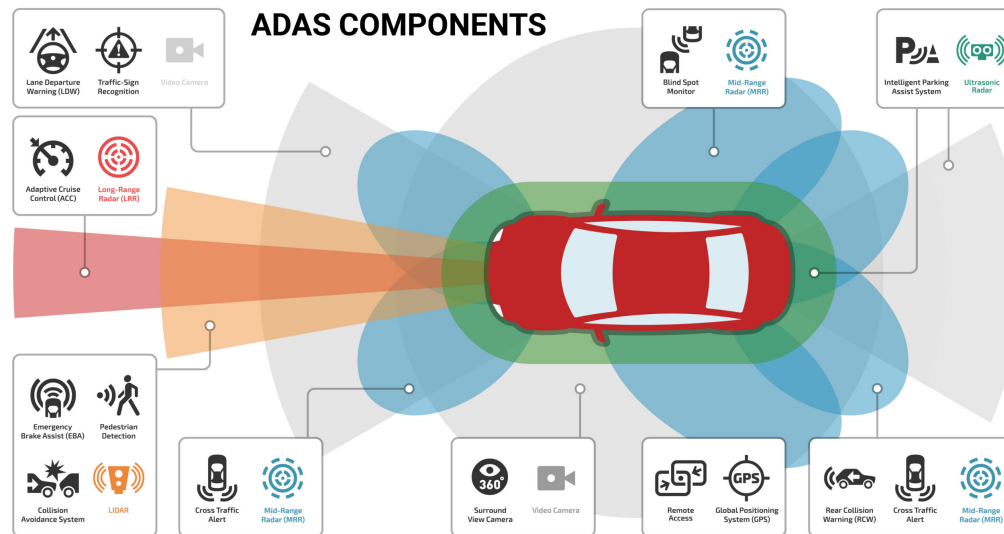


# What are the components that drive ADAS?

- AEB – Automatic Emergency Braking
  - RADAR
  - Camera
  - LiDAR, etc.
  - MCU(s) – microcontrollers
  - Main ECU
  - Harnesses to camera, radar, ECU
  - Harnesses/connection to Active Safety Module or similar
  - Telemetry to allow vehicle data analysis
  - Antennas and antenna arrays
  - Connection to brake lights (software/ECU)
  - Dashboard alerts and warnings (audible and visual)
  - Seatbelt pre-tensioners
  - Brake connection/hydraulics → pre-charge and use
  - Potentially, steering power
  - More!

# What are the components that drive ADAS?

- We've all seen diagrams like this:



What are the components that are required to make each technology work?

# Functional Safety Risk

- Degraded ADAS performance
  - Sensors drift; algorithms trained on outdated datasets
- Unsupported safety systems
  - ADAS functions (AEB, lane keeping) may silently degrade
- Software decay
  - Memory faults, timing errors, or OS-level incompatibilities
- Latent defect emergence



# Cybersecurity Exposure

- Unpatchable systems
  - Core Issue: Unsupported ECUs become unpatchable attack surfaces
- Known vulnerabilities
  - No security updates for legacy firmware
  - Known vulnerabilities remain exploitable
  - Increased connectivity (telematics, OTA history) expands attack vectors
- Cyber-physical attack risk



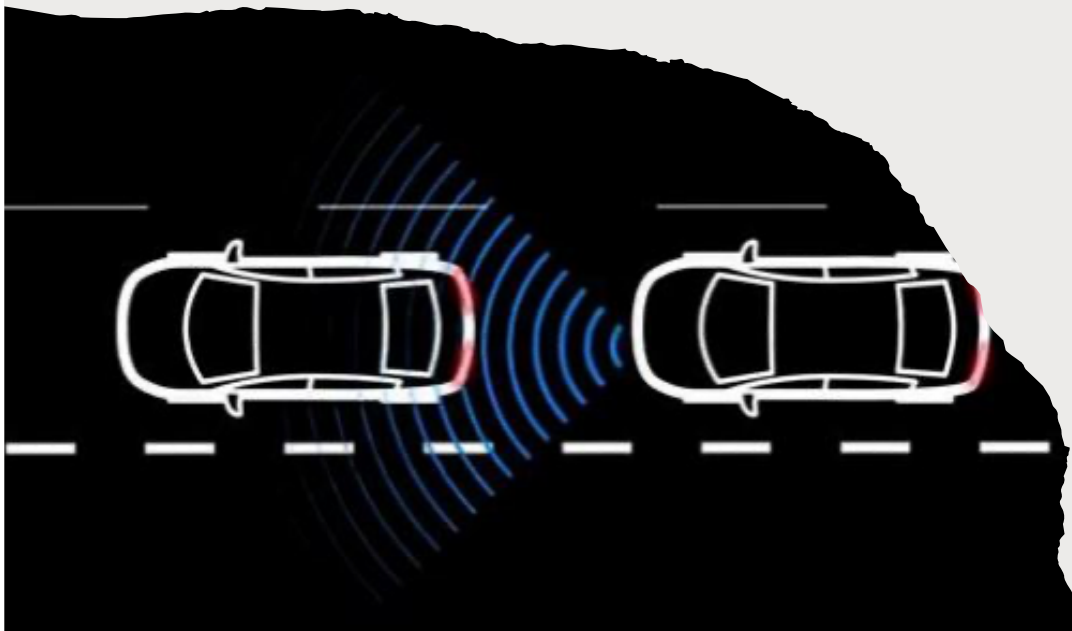
# Regulatory Risk

- Regulatory Uncertainty – Strategically looking around corners – lack of movement from regulators
- Potential non-compliance over time
- Roadworthiness disputes
- Coverage litigation risk



# FMVSS 127: A Brief Overview

- What is FMVSS 127?
  - Establishes performance requirements for AEB (Automatic Emergency Braking) for light vehicles
  - Vehicles manufactured **on or after Sept. 1, 2029**, must meet requirements
    - Applies to vehicles weighing less than 10,000 lbs.
  - Published in 2024, then delayed to March 2025
- Sets “minimal level of performance” for vehicle manufacturers to meet
  - FCW at any forward speed greater than 10 kph (6.2 mph)
  - Apply the brakes automatically at forward speeds greater than 10 kph (6.2 mph) when collision with lead vehicle (at speeds up to 90.1 mph) or pedestrian (at speeds up to 45.4 mph) is imminent
  - Prevent collisions (no contact) in all testing conditions outlined (including nighttime for pedestrian tests)
  - Provide visual notification to driver if malfunction present which would prevent proper operational performance



# Current State of Systems on Cars Today

## Before FMVSS 127

- OEM's provide speed thresholds in manuals that indicate:
  - Expected speed performance
  - Expected conditions that may cause change in system performance
  - What types of objects may be detected and avoided
- Different for every vehicle



## After FMVSS 127

- With FMVSS 127, NHTSA is establishing a “minimal level of performance” which manufacturers are expected to meet
  - FCW at any forward speed greater than 10 kph (6.2 mph)
  - Apply the brakes automatically at forward speeds greater than 10 kph (6.2 mph) when collision with lead vehicle (at speeds up to 90.1 mph) or pedestrian (at speeds up to 45.4 mph) is imminent
  - Prevent collisions (no contact) in all testing conditions outlined (including nighttime for pedestrian tests)
  - Provide visual notification to driver if malfunction present which would prevent proper operational performance

# Real World vs. FMVSS 127

- Most vehicles experience conditions outside of the parameters of FMVSS 127
  - Steering angle
  - Sun angle
  - Other vehicles, signs, conditions on road, sizes and shapes of obstacles
  - Moisture
- **Balance of FMVSS effectiveness with real-world viability will likely be a balancing act for OEMs**





## Vehicle Recalls

- Since National Traffic and Motor Vehicle Safety Act (1966) enacted, NHTSA has recalled:
  - > 935 million vehicles
  - ~ 63 million tires
  - ~ 222 million pieces of motor vehicle equipment (non-vehicle items)
  - ~62 million car seats

# Relevant Recalls in the ADAS Space

- Just a few recent recalls:
  - Rivian 2025: 24,000 vehicle – software defect in Highway Assist system
  - Tesla 2023: 2 million vehicles – Autopilot driver misuse detection
  - Mazda 2024: forward-sensing camera malfunction
  - Ford 2025: 312,000 vehicles – failure in Electronic Brake Booster
    - 88 different safety recalls between January – June 2025
- Average Cost of a Recall: \$500 - \$2,000/vehicle
- Average Cost of an OTA Software Update: \$300 - \$500/vehicle



# Defect or Not?

- 
- A long-range radar, installed on the front of the vehicle, causes the vehicle to aggressively brake when it detects a metal plate on the road surface.
  - Does this constitute a defect?  
YES or NO?



# Vehicle Non -Compliance

- If a sports car was designed to stop within distance "a" which is 100 feet less than the required distance of "b" in the FMVSS, but the vehicle's braking system is now stopping the vehicle between distance "a" and "b" - **is the vehicle in compliance with the FMVSS if the OEM provided NHTSA with the design parameters?**
- Yes or No?



# Defect or Not a Defect

- A defect must be safety related - only for safety critical functions or non-compliance with FMVSS 127.
- Other further examples and background
  - Computer algorithms
  - Braking system delayed causing the vehicle not to stop within the required regulatory requirements
  - FCW notification system delayed or emergency braking of the vehicle causes subject vehicle to impact stationary object.
  - Other safety related issues that impact the Do No Harm language found in the Motor Vehicle Safety Act.



# What are you insuring?

- What components are you insuring?
- For how long do you really need to insure these components?
- Should the insurance industry offer policies that exceed a Regulatory timeframe required by OEM?



# Recall and Notification Requirements

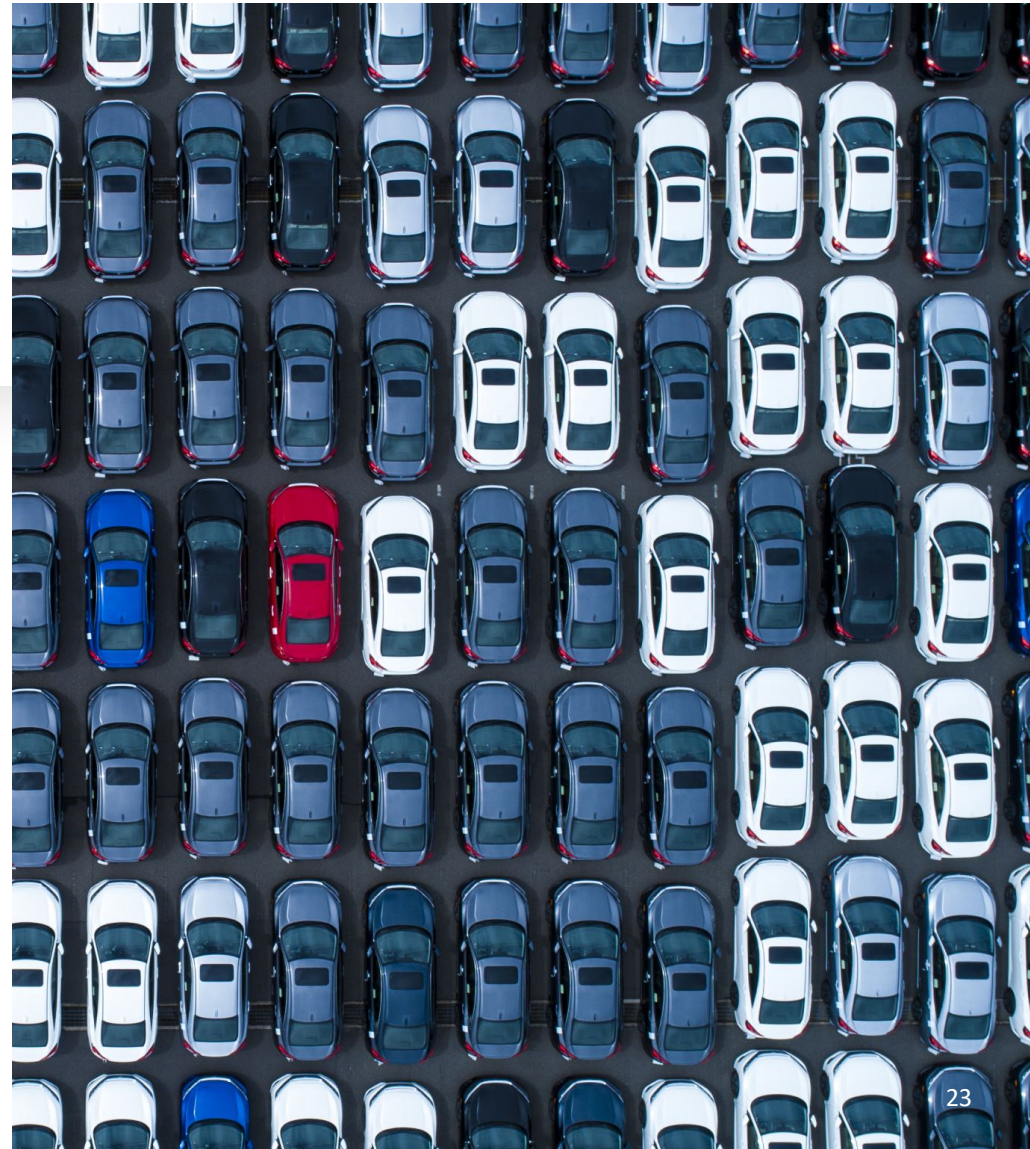
---

- How many years does NHTSA require OEMs to pay for a recall-related repair?
  - 5 years
  - 10 years
  - 15 years
  - 20 years
  - 25 years



# Recall and Notification Requirements

- OEMs must notify NHTSA within 5 days, pay for repairs for vehicles 10 years old or less
- What business practices are necessary after 10 years?
- What does NHTSA require an OEM to do if there is an issue after 10 years?
  - OEM's must still notify the registered owner of the reference vehicle, but does not need to pay for the repairs.



# Strategic Takeaway

- Shift from mechanical risk → software lifecycle risk
- Requires new actuarial and operational frameworks
- Externalities that may not have been considered in the past need to be considered in the future





THE BALUSTER GROUP

# Thank you!

Christopher J. Bonanti

*CEO & Principal*

The Baluster Group, Inc.

Office: (571) 469-9340

Mobile: (571) 334-4807

Email: [cjbonanti@thebalustergroup.com](mailto:cjbonanti@thebalustergroup.com)

Website: [www.thebalustergroup.com](http://www.thebalustergroup.com)

