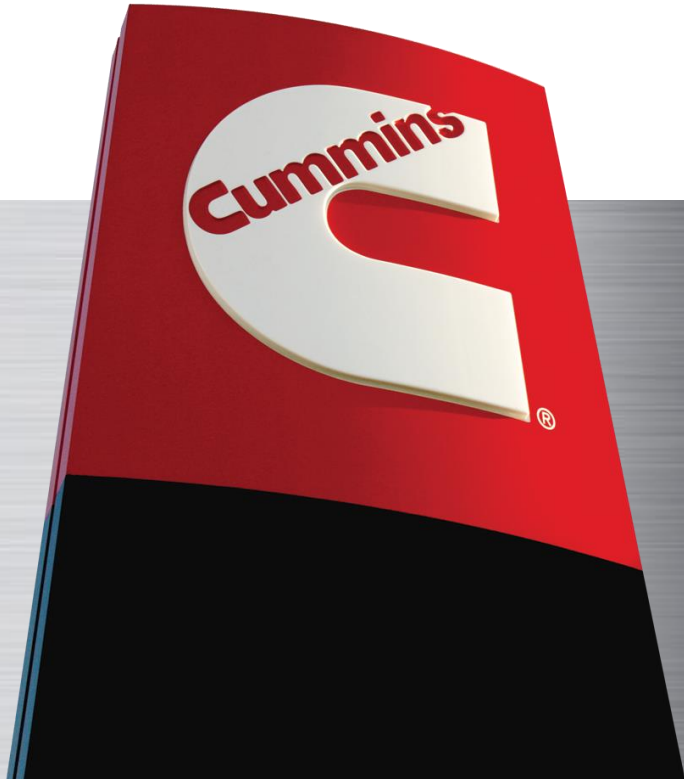
Product CyberSecurity: A Challenge for the Automotive Industry

Larry Hilkene

Oct 2016

Public



Agenda

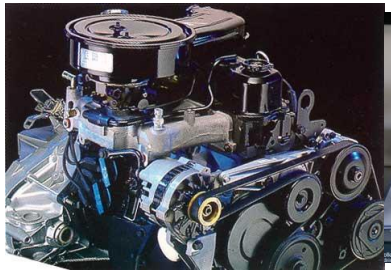
Auto Cyber – Yesterday, Today & Tomorrow

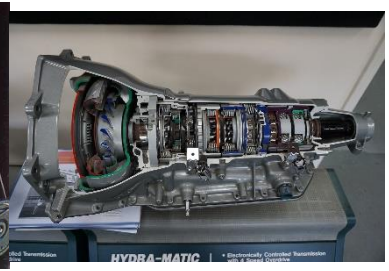
- A Bit of History – how did we get to today?
- Today - Current State
- Tomorrow - ??
- Opportunities/Challenges

Yesterday – how did we get here?

- Why electronic controls?
  - Fuel Efficiency
  - Emissions
  - Faster, more precise control
- Other Requirements
  - Reliability
  - Speed of response
  - Minimal cost

Boundary Diagram - Yesterday

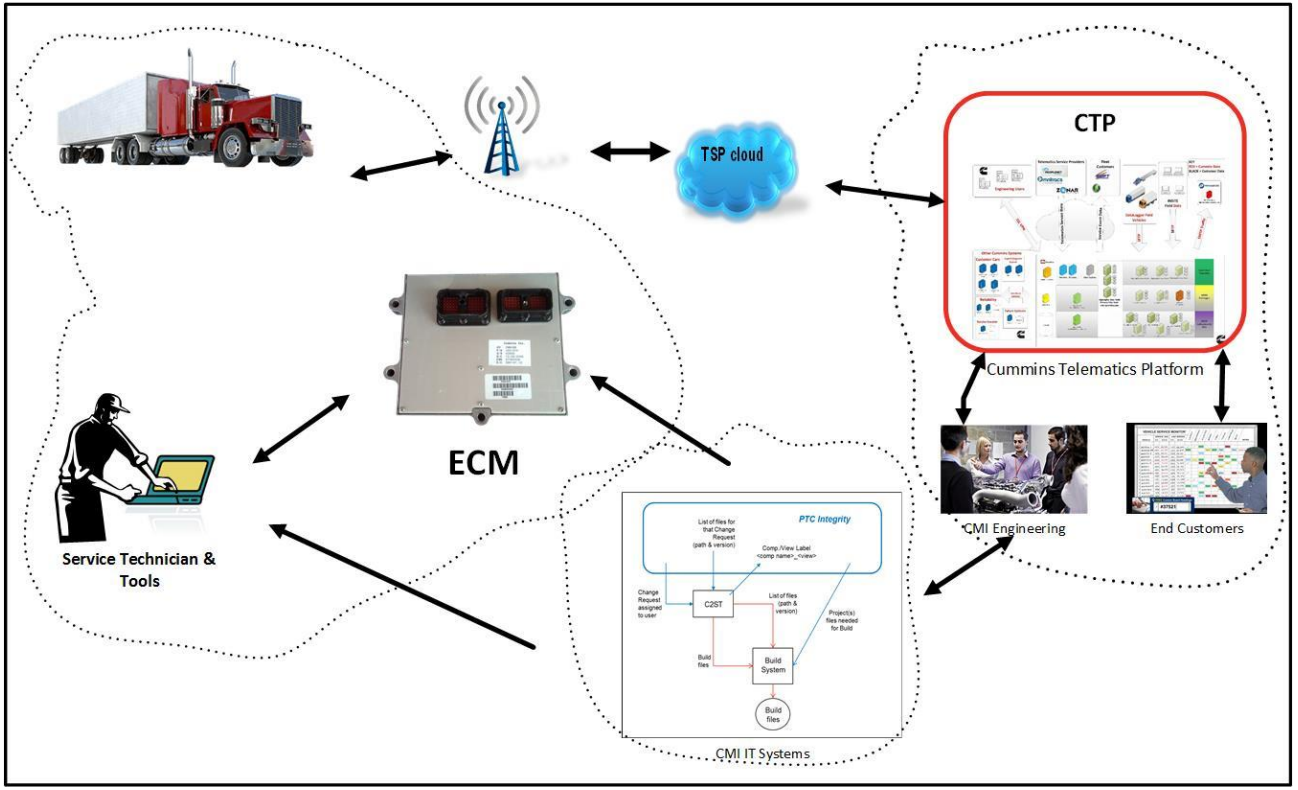




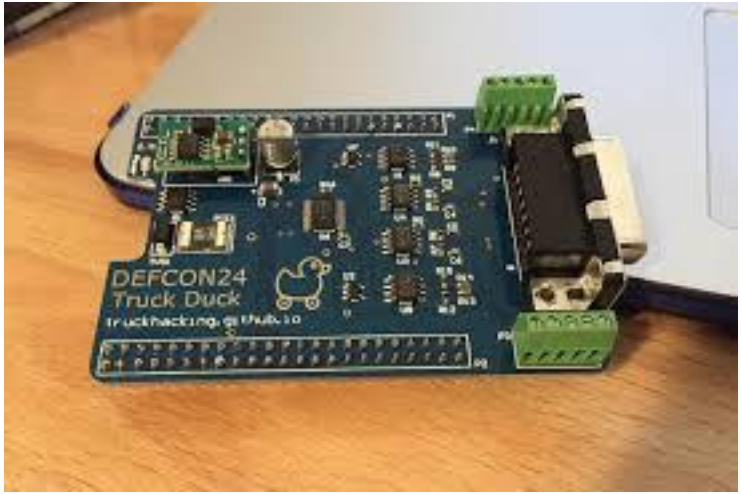
Today – Where are we?

- Developments:
  - Many more ECUs per vehicle
  - Electronic Tools now required – Right to Repair
  - OnBoard Diagnostics
- Connectivity
  - Becoming more common
  - Different ways (Infotainment, Bluetooth, Telematics)
- Promise for Next

Boundary Diagram - Today



Hacking has begun



Today - Government Actions

- NHTSA Enforcement Guidance Bulletin
  - Acknowledges lack of standards
  - Intentionally expanding scope and reach of regulations
- Product Cybersecurity leader recommendation
- Request from House Cmte re: OBD practices
- Upcoming additional guidance regarding security frameworks and practices

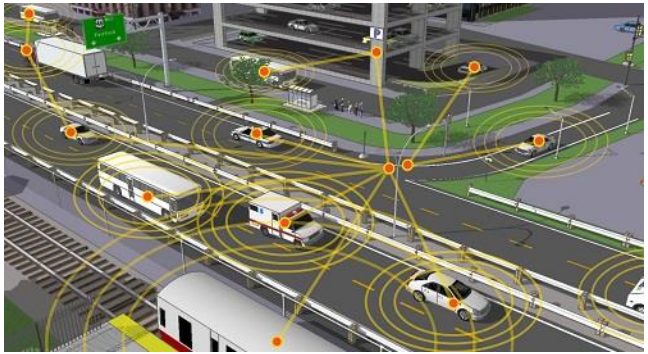
Trade/Industry Activities

- Develop new standards
  - Securing Protocols
  - Data types/formats
- Educate workforce
  - Develop training
  - Develop processes & practices
- Work with Governments
- Share Information

Tomorrow – What will it be?

- Vehicles connected to X
  - Other vehicles
  - Homes/businesses
  - Infrastructure
- Data possibilities
  - Vehicle performance/service
  - Services tailored to the customer
-

Tomorrow – Boundary Diagram?



Opportunities & Challenges

- Changing Marketplace
  - Connecting vehicles to services
  - Making the vehicle more personal
- Preventing Unwanted Access
  - Hacking the vehicle
  - Access to data
- Systems Pressures
  - Development
  - Test
  - Updates

Questions?