Functional Requirements for Automated Vehicles

Where to start?
Mandate

• Develop functional requirements for AV
  • In particular, combination of different functions (SAE level 2+)
  • Cover requirements for Functional Safety
• In line with following principles:
  a) System safety
  b) Failsafe response
  c) HMI/Operator information
  d) OEDR
Background Definitions

• Functional Requirements
  • Define the function of a system
  • System must do ______. (mandatory)
  • The “what?”

• Non-Functional requirements
  • Define criteria that can be used to judge the system
  • System shall do ______. (suggestion)
  • The “how?”
Where to start?

• Requirements vary based on a number of factors including:
  • General requirements
    • Ie applicable to all functions
  • Specific function(s)
    • Ie ALKS, lane change system, auto-park, full automation
  • SAE level
    • Level of reliance on driver
  • Intended use
    • Ie Driver support, driver replacement, ride-sharing
Things to consider

• Systems are heavily software based, often relying on probabilistic methods and object models
  • Nothing is 100% certain
  • “All models are wrong, but some are useful“
• It may be necessary to include requirements for degraded/temporary modes of operation
  • I.e. Temporary loss of lane markings, sensor oversaturation/interference
  • Temporary increase in risk, but may be less than overall risk of transition to driver or attempting minimal risk manoeuvre
• Humans drivers are also susceptible to the above
Possible method

• Begin with general requirements
  • Add more sophistication/complexity in layers
  • Build in some adaptability in the requirements
    • Re-use requirements across different functions

• For each function, level and intended use choose what layer (level of sophistication) is appropriate
  • Layers above could be seen as fallbacks in case of failure & have associated performance degradation/system limitations

• Keep a “database” of requirements and re-use for each function
Partial Example – Highway Chauffeur

- System must (detect/perceive/act):
  - Roadway
    - Lane
      - Lane markings
      - Centre of lane
  - Infrastructure
    - Traffic control devices
      - State of device
  - Road type
    - Road Condition
      - Adverse weather
  - Position of other road users (same lane, adjacent lane, opposite lane)
    - Velocity of other road users
      - Classify type of user
        - Indications of user intent (turn signal, location in lane, acceleration)
          - (Predict) user intended path
  - Keep a safe distance from other users
    - Accelerate/decelerate smoothly
    - Reduce likelihood of crossing intended paths
- Result: Can proceed at rated conditions (speed, lane change etc.)
Partial Example – Highway Chauffeur – (temporary) loss of a sensor

• System must (detect/perceive/act):
  • Roadway
    • Lane
      • Lane markings
      • Centre of lane
  • Infrastructure
    • Traffic control devices
      • State of device
  • Road type
    • Road Condition
      • Adverse weather
  • Position of other road users (same lane, adjacent lane, opposite lane)
    • Velocity of other road users
      • Classify type of user
      • Indications of user intent (turn signal, location in lane, acceleration)
      • (Predict) user intended path
  • Keep a safe distance from other users
    • Accelerate/decelerate smoothly
    • Reduce likelihood of crossing intended paths

• Result: Degraded mode (may need to reduce speed, cannot lane change, increase distances to other users)
Starting point

• Use some of the concepts in published guidance documents as starting point
• Build upon & categorise
• Begin with general statements, add complexity/layers when required for a technology
  • Less complex system requirements can become the degraded modes of more sophisticated systems
• Work towards specific requirements which can be testable
A few possible – “System must” from Canada’s Safety Assessment

1. ADS Level of Automation and intended use
   - Have a defined level of automation
   - Have a clear intended use
   - Be able to identify the software & hardware version

2. Operational Design Domain
   - Have a clearly defined ODD
     - Prevent system from activating if outside ODD
     - Ability to detect if OD outside ODD
     - Minimize risk if ODD exceeded
   - Maintain the safe flow of traffic
   - Comply with the traffic rules
A few possible – “System must” from Canada’s Safety Assessment

3. Object and Event Detection and Response
   - Detect & perceive other road users
   - Respond appropriately to (road infrastructure, other users, traffic control, unlawful users, animals, unclassified objects)

6. Safety Systems
   - Have redundancies
     - Monitor performance
     - Detect faults
     - Conduct hazard analyses
   - Signal malfunctions
     - Execute corrective action
   - Transition to safe fall-back
A few possible – “System must” from Canada’s Safety Assessment

• 7. Human-Machine Interface and Accessibility of Controls
  • Have intuitive controls
  • Communicate critical messages (to occupants and others)
  • Clearly communicate a take-over request
  • Allow sufficient time for a fall-back driver to respond
  • Show when the system is available, not available and operational
  • Signal intention to other road users
A few possible – “System must” from Canada’s Safety Assessment

8. Public Education and Awareness
   • Be clear to the driver when and how it performs DDT or partial DDT
     • Indicate maintenance requirements
     • Make it’s intent clear to other road users

9. User Protections during Collisions or System Failures
   • Achieve a safe state after a collision/failure
     • Communicate with passengers, first responders, emergency services
   • Conduct system tests prior to returning to circulation
A few possible – “System must” from Canada’s Safety Assessment

• 11. System Updates and After-Market Repairs/Modifications
  • Conduct system checks after update/modification/repairs
  • Be disabled if the function is no longer supported