Lloyd's Register Foundation

UNIVERSITY of York

Safety Assurance for Highly Automated Vehicles

PROFESSOR JOHN MCDERMID, OBE FRENG

22ND MAY 2018

Lloyd's Register Foundation

UNIVERSITY of York

Safety Issues

- Highly automated road vehicles
  - Work in a (heterogeneous) System of Systems (SoS)
- Safety Engineering includes
  - Hazard analysis for the SoS
  - Safety of intended function (SOTIF)
- Safety Assurance includes
  - Validation of algorithms and learning
    - What are useful measures of "environment coverage"?

Lloyd's Register Foundation

UNIVERSITY of York

Assuring Autonomy BoK

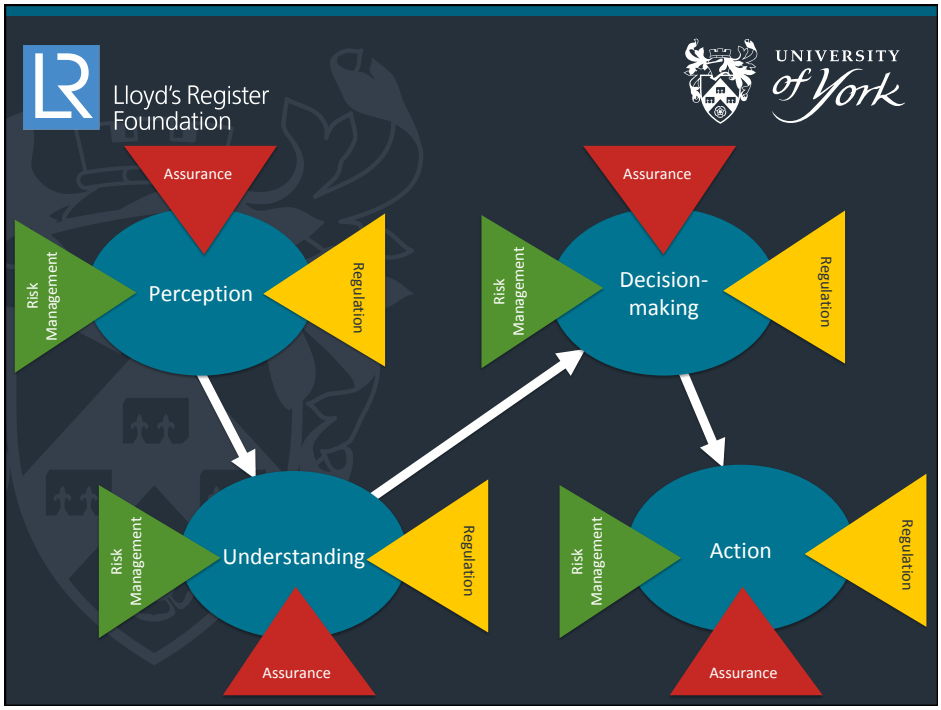
- The Assuring Autonomy International Programme (AAIP) will produce a Body of Knowledge (BoK)
  - Problems, principles, product & technology, processes
- Product by abstract operations PUDA/OODA/MAKE
  - Perception (Observe)
  - Understanding (Orient)
  - Decision-making (Decide)
  - Action (Act)

Lloyd's Register Foundation

UNIVERSITY of York

Design, Assurance & Regulation

- Risk management considers how the risks associated with hazards are managed to an acceptable level (and what is acceptable)
- Assurance considers how the required level of confidence is demonstrated (and what level is required)
- Regulation considers what is necessary in order to comply with the relevant legislation


Lloyd's Register Foundation
UNIVERSITY of York
Assurance
Risk Management
Perception
Regulation
Assurance
Risk Management
Decision-making
Regulation
Risk Management
Understanding
Regulation
Assurance
Risk Management
Action
Regulation
Assurance


Lloyd's Register Foundation
UNIVERSITY of York
Simple Example: Lane-Keeping
SCHOOL

Lloyd's Register Foundation

UNIVERSITY of York

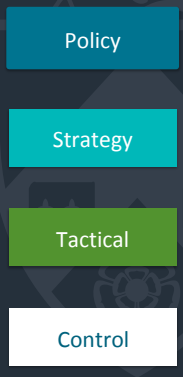
Simple Example: Lane-Keeping

- Risk Management
  - Design so vehicle keeps to lane, takes curves at safe speed (depends on road, weather, load/mass, etc.)
- Assurance (Act is standard)
  - Perception/understanding – e.g. accurate lane models
  - Decision-making – e.g. predictive so can make smooth turns, always safe speed, etc.
- Regulations
  - Consistency between manufacturer's designs?

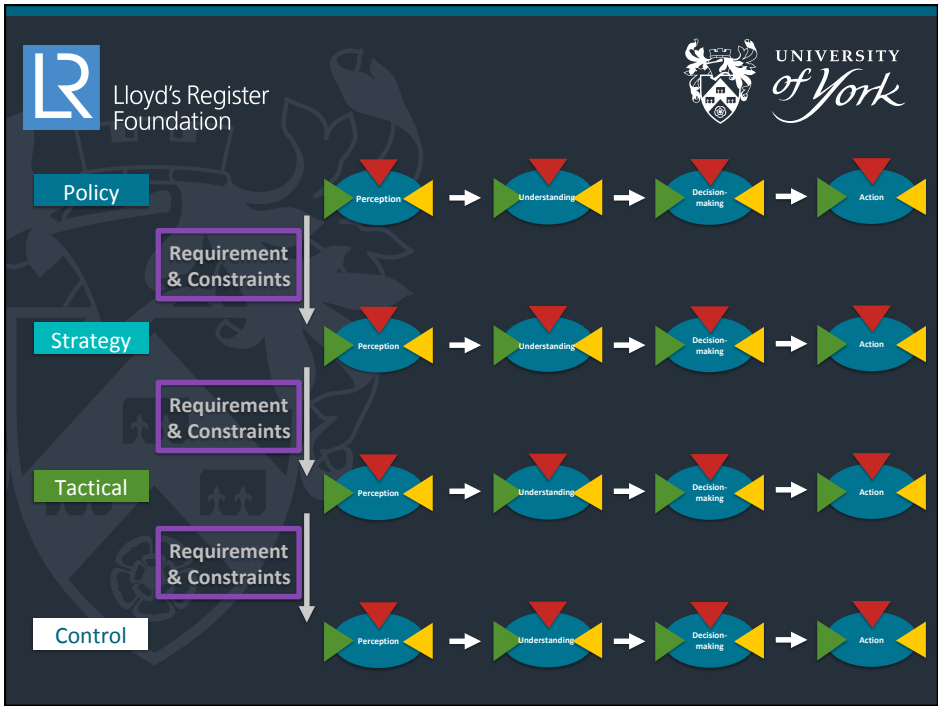
Lloyd's Register Foundation

UNIVERSITY of York

Layering



- Policy: control (of goals) of multiple interacting systems over long time-spans.
- Strategy: how a single system can achieve its goals. Typical timescale – hours/minutes.
- Tactical: how the strategy can be met under current conditions. Typical timescale – secs.
- Control: direct control of system to implement defined behaviour. Typical timescale <sec (may bypass U & D)



Lloyd's Register Foundation

UNIVERSITY of York

Simple Example: Lane-Keeping

- Policy (or high-level strategy)
  - Performance envelope – road curvature, weather, (load/mass,) … to steering angle ($^{dSA}/_{dt}$) bounds
- Strategy (see earlier example slide)
- Tactics
  - Normal – e.g. use steering to centre in lane
  - Abnormal – e.g. indicate and change lane and/or speed
- Control (classical closed-loop control – hysteresis?)

Lloyd's Register Foundation

UNIVERSITY of York

Safety Engineering Revisited

- PUDA (OODA) an abstract architecture (may need a "whole system" model/architecture as well)
  - Risk management – includes design patterns
  - Assurance – how specific functions are assessed
  - Regulation – what needs to be consistent in an SoS
- Need to do safety process at each "level"
  - The wrong policy might be unsafe
  - Need to consider SOTIF and failure conditions

Lloyd's Register Foundation

UNIVERSITY of York

A Safety Case (1)

- Evidence needs to address PUDA, and the layers of the model (policy to control); example at tactical level:
  - Perception/understanding
    - Identify narrowing/closing of lane (yellow barrier)
    - Maximum intrusion of barrier and angle
  - Decision-making
    - Steering angle to avoid barrier, trajectory to avoid other vehicles, and indicating to change lanes

Lloyd's Register Foundation

UNIVERSITY of York

A Safety Case (2)

- For perception/understanding assurance evidence
  - Need generic solution for "lane narrowing"
    - Prediction sufficiently good for avoidance
    - Ability to deal with occlusion (by other vehicles)
    - Ability to estimate intrusion angle
    - Capability limit to warn driver to take control
  - Assuming learnt behaviour, evidence from learning focused on "worst case" scenarios

Lloyd's Register Foundation

UNIVERSITY of York

A Safety Case (3)

- At the policy level
  - Risk management
    - Driver always in control and has situational awareness
  - Assurance evidence (from a simulator?)
    - Warning of reaching capability limits early enough
    - Tests that demonstrate the abiltiy of a human to maintain attention and regain control

Lloyd's Register Foundation

UNIVERSITY of York

Lloyd's Register Foundation

UNIVERSITY of York

Accident Data

- Courts will focus on the specific, not the general
  - What did the car do in the circumstances?
  - Prosecution lawyers will try to "prove" that there was a "weakness" in the algorithms/design
- Evidence needed that the system
  - Behaved as intended (i.e. safely)
  - Did provide a *credible* warning (within reasonable expectations of the driver)

Lloyd's Register Foundation

UNIVERSITY of York

Observations

- BoK (as it evolves) may (is intended to) help
  - Structure arguments
  - Set expectations as to appropriate (means of producing) safety/assurance evidence
- The system design needs to support accident and incident analysis
  - Need some form of "black box", capable of dealing with operational learning, if that can occur