CARS
CONFERENCE ON ASIA ROAD SAFETY 2024
“ Safer Journey, Sustainable Future ”
2-4 SEPTEMBER 2024 | PUTRAJAYA INTERNATIONAL CONVENTION CENTRE (PICC), PUTRAJAYA

Main Challenges in Deploying Autonomous Fleets

Niels de Boer

Snr Programme, Director
Centre of Excellence for Testing & Research of Autonomous Vehicles
Nanyang Technological University

POWERED BY

MIROS
MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH
ASEAN ROAD SAFETY CENTRE

PERKESO

PLUS
A member of UEM

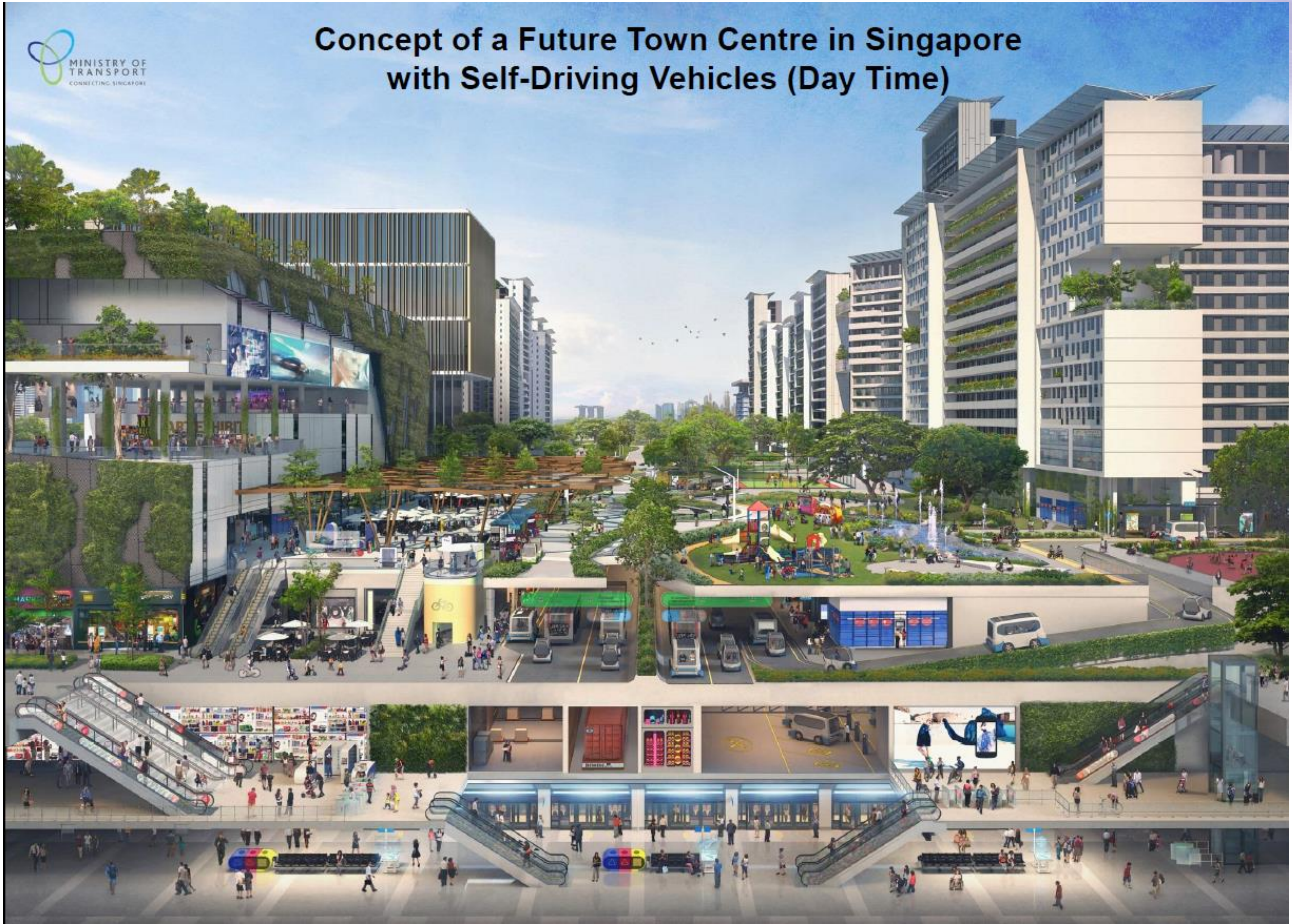
Supported by:

RSF
UN ROAD SAFETY FUND

VISION ZERO
Safety.Health.Wellbeing.

Car Lite Estates

Concept of a Future Town Centre in Singapore with Self-Driving Vehicles (Day Time)



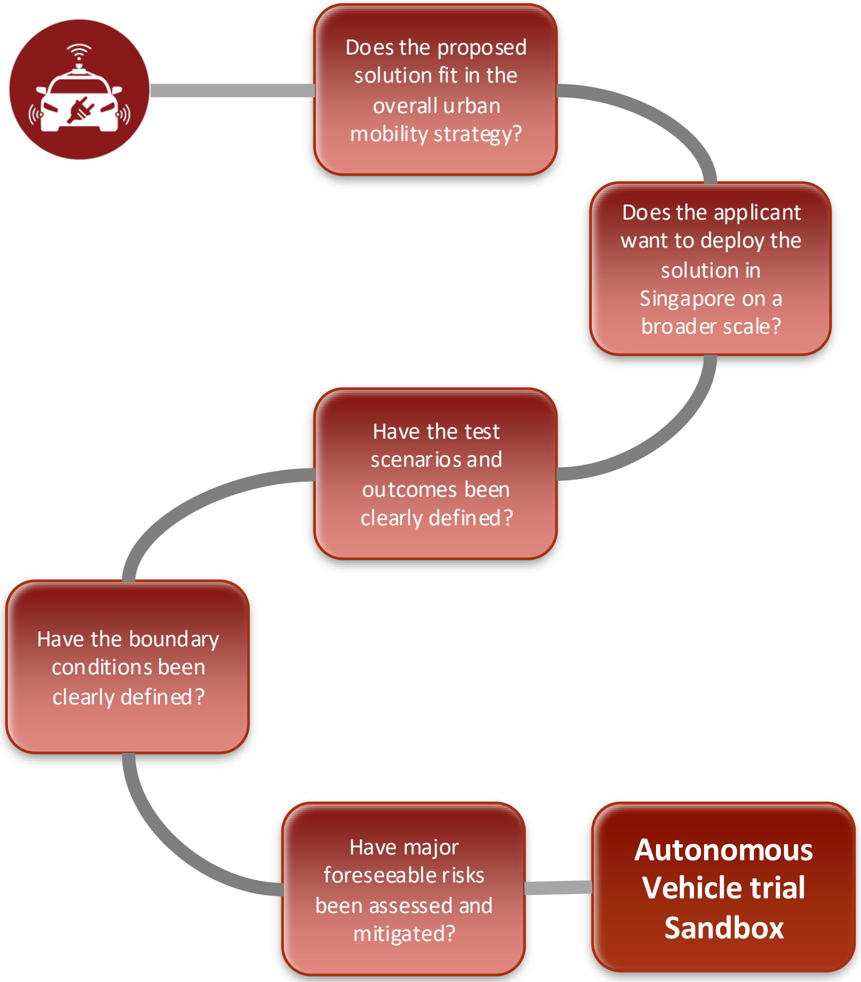
CETRAN Centre of Excellence for Testing & Research of AVs – NTU

- **Centre of Excellence to support Singapore AV community**
  - Standards development
    - Developing AV testing procedures
    - Perform AV testing on behalf of LTA to support issue of AV Authorization
    - Technical lead in development of AV Technical Reference
  - Operator of CETRAN AV Test Centre
  - Linking with other countries to align on standards and testing
  - Supporting skills development for Industry
  - AV Developer support

Centre of Excellence for Testing and Research of Autonomous Vehicles – NTU (CETRAN)

Regulatory Sandbox

- Autonomous Vehicle regulatory sandbox has the same structure as other regulatory sandboxes deployed in Singapore (e.g. FinTech)
  - A regulatory sandbox has been implemented and could be extended at the end of 5 years, before enacting more permanent legislation
  - Caters for trials without safety driver on public roads – if the risks have been mitigated
  - Advantage of the sandbox is Threefold:
    - Development of legislation without having to go to parliament for every incremental change
    - Be able to tailor requirements to a specific solution if required
    - Being able to trial regulations before rolling them out as law



Does the proposed solution fit in the overall urban mobility strategy?

Does the applicant want to deploy the solution in Singapore on a broader scale?

Have the test scenarios and outcomes been clearly defined?

Have the boundary conditions been clearly defined?

Have major foreseeable risks been assessed and mitigated?

Autonomous Vehicle trial Sandbox

Milestone Framework

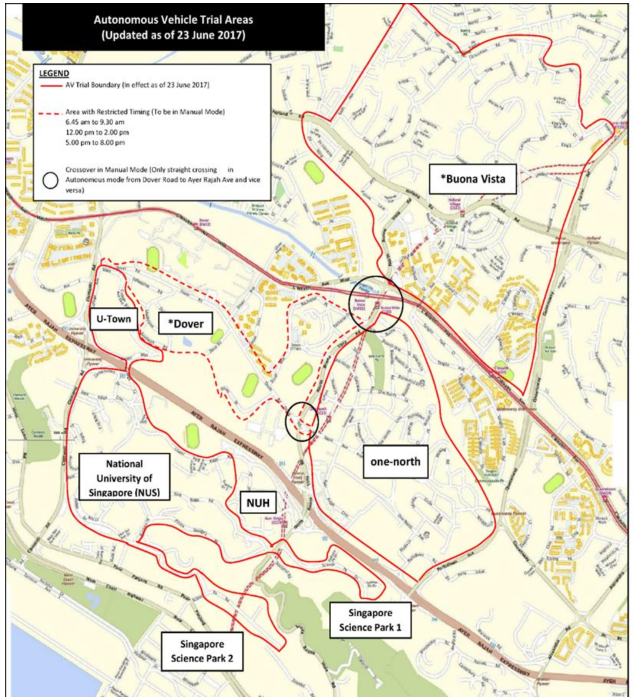
- Assumption:
  - Vehicles are SAE Level 4 in automation
  - Will have an increase in technical maturity as trials progress

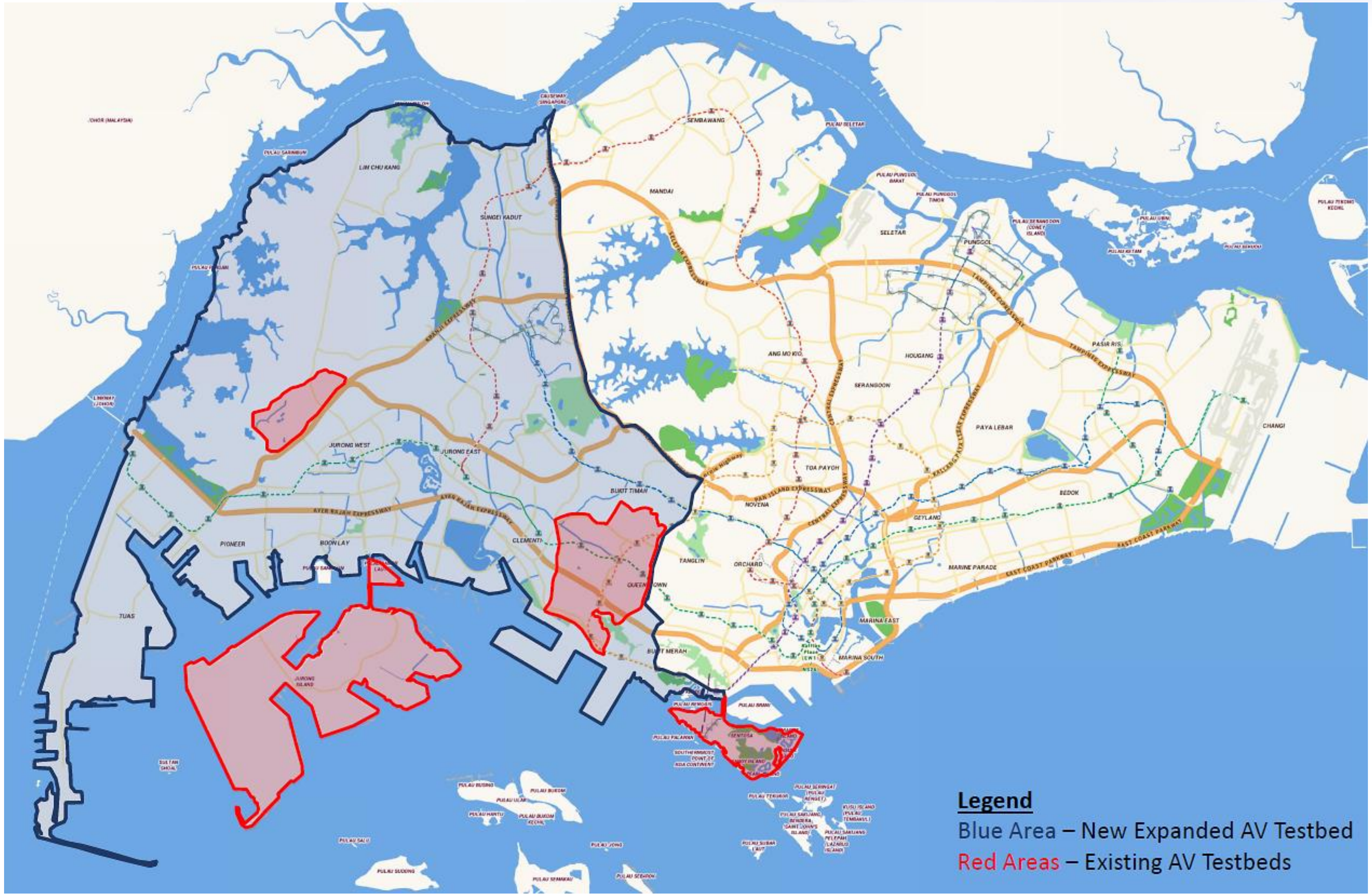
- Effectively a Stage-Gate R&D process applied to AV trials
  - Stages are trials with increasing levels of complexity and increasing levels of risk
  - Gates are readiness assessments to determine
    - The level of maturity has sufficiently increased that the risk is acceptable for trial in an increased complexity environment
    - The vehicle has developed sufficient maturity that an increase in complexity of the environment is justified

- Question going forward:
  - Past vehicles were locally developed: How doe we manage vehicles which have been proven in other overseas environments

AV Trial Testbed

- Test bed at One North as a future proof concept for AV testing
  - Infrastructure to support trials
  - Closed Circuit CCTV

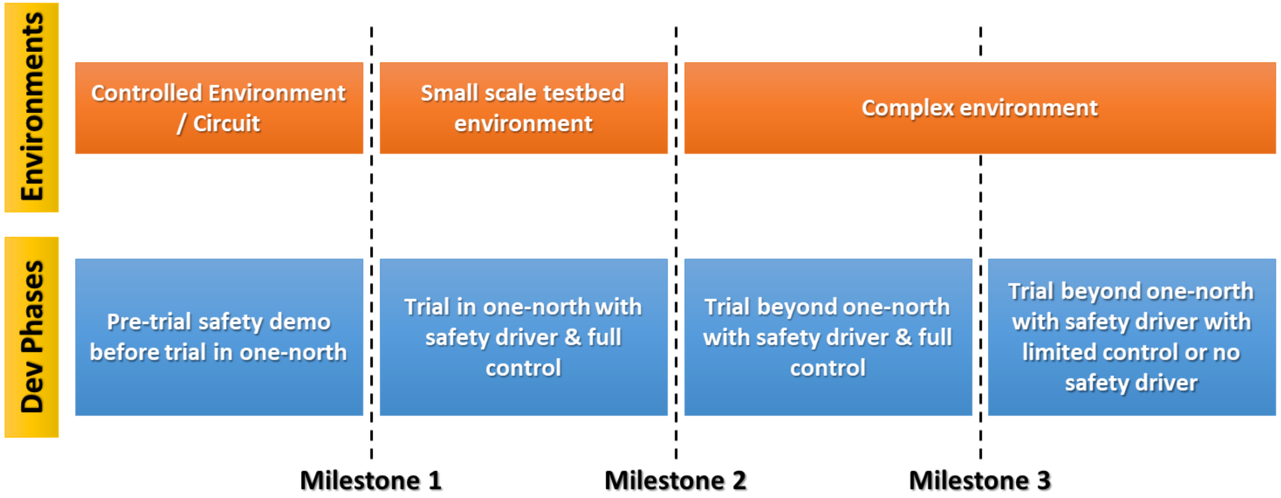

Autonomous Vehicle Trial Areas
(Updated as of 23 June 2017)
LEGEND
AV Trial Boundary (In effect as of 23 June 2017)
Area with Restricted Timing (To be in Manual Mode)
6.45 am to 9.30 am
12.00 pm to 2.00 pm
5.00 pm to 8.00 pm
Crossover in Manual Mode (Only straight crossing in Autonomous mode from Dover Road to Ayer Rajah Ave and vice versa)
*Buona Vista
U-Town
*Dover
one-north
National University of Singapore (NUS)
NUH
Singapore Science Park 1
Singapore Science Park 2



Milestones for AV Trials

Milestones are used to assess AVs before they are allowed to proceed to their next phase of trial

- Each milestone test will produce a test report with recommendation which is used by the Land Transport Authority as one of the decision criteria to “pass” the AVs



Environments
Controlled Environment / Circuit
Small scale testbed environment
Complex environment
Dev Phases
Pre-trial safety demo before trial in one-north
Trial in one-north with safety driver & full control
Trial beyond one-north with safety driver & full control
Trial beyond one-north with safety driver with limited control or no safety driver
Milestone 1
Milestone 2
Milestone 3

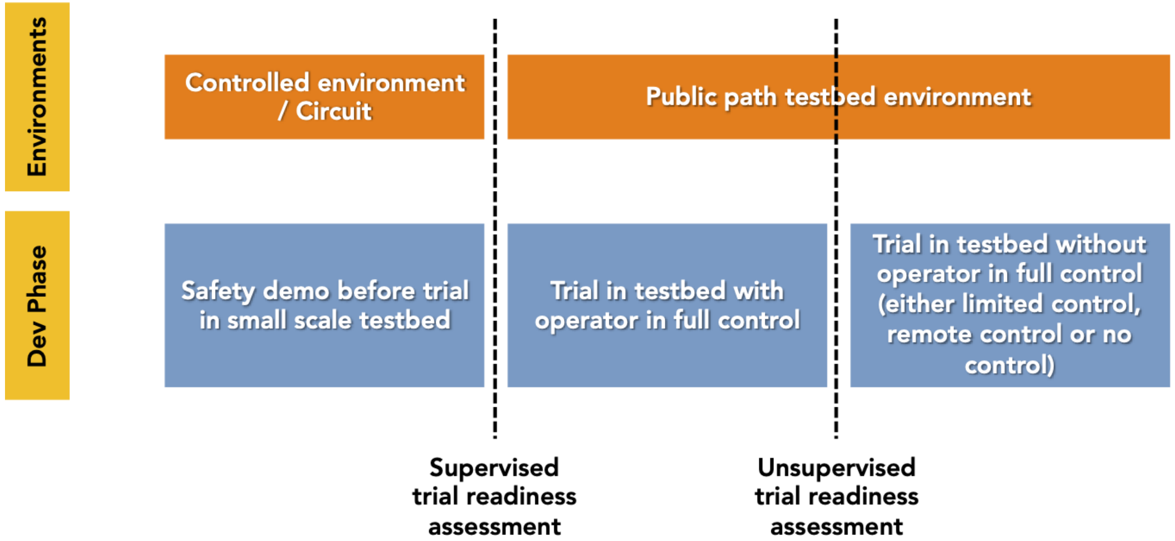
- **Milestone 1**
  - Ability to safely conduct testing of autonomous vehicles with safety driver in a small scale testbed.
- **Milestone 2**
  - Ability to safely conduct testing of autonomous vehicles with safety driver in a complex environment.
- **Milestone 3**
  - Ability to safely conduct testing of autonomous vehicles without or with a safety driver (with limited control) in a complex environment. This implies high technical maturity.

Extension to AMR

Milestones for AV Trials on Public Paths

Adaption of Public Road Milestone Framework to facilitate trails on public paths:

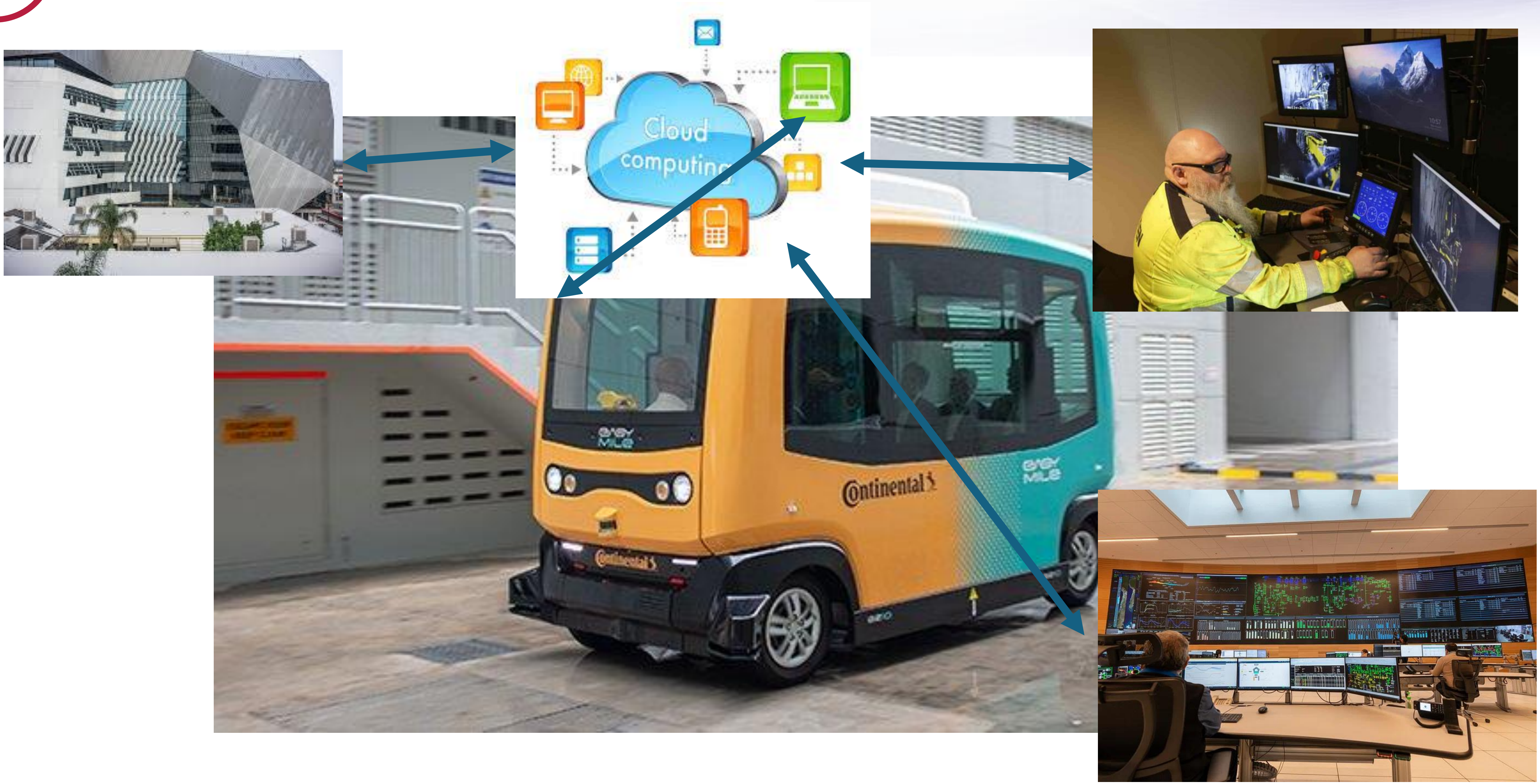
- 3 categories of vehicle defined:
  - Cat-A1: Vehicles not carrying passengers with a width of less than 70cm.
  - Cat-A2: Vehicles not carrying passengers with a width of less than 70cm.
  - Cat-B1: Vehicles not carrying passengers with a width of more than 70cm.
  - Cat-B2: Vehicles carrying passengers with a width of more than 70cm.


Environments
Dev Phase
Controlled environment / Circuit
Public path testbed environment
Safety demo before trial in small scale testbed
Trial in testbed with operator in full control
Trial in testbed without operator in full control (either limited control, remote control or no control)
Supervised trial readiness assessment
Unsupervised trial readiness assessment

- **Supervised trial readiness assessment (T1)**
  - Derived from Milestone 1
  - Changes in safety operator requirements and safety controls
  - Test routes adapted to reflect trial environments

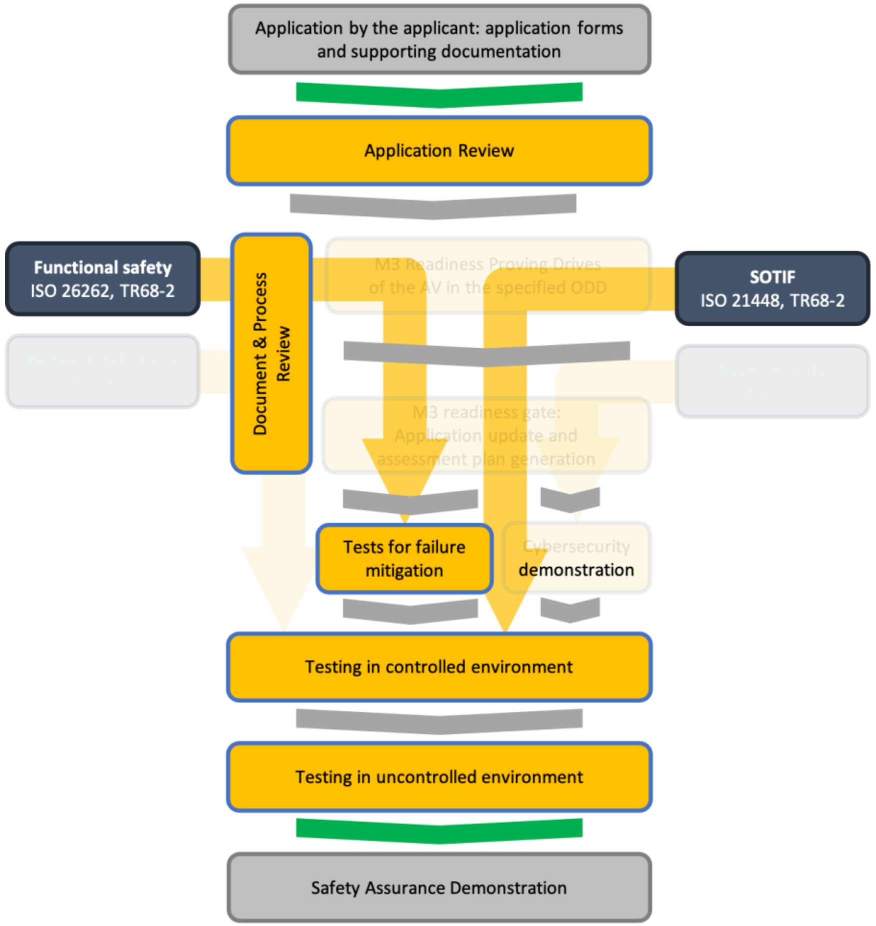
- **Unsupervised trial readiness assessment (T2)**
  - To be derived from Milestone 3
  - Available mid 2024

Transition from vehicle centric to system centric assurance



How to ensure integrity?

- Traditional verification



Application by the applicant: application forms and supporting documentation

Application Review

Functional safety
ISO 26262, TR68-2

Behavioural safety
TR68-2

Document & Process Review

M3 Readiness Proving Drives of the AV in the specified ODD

SOTIF
ISO 21448, TR68-2

Cybersecurity
TR68-2

M3 readiness gate: Application update and assessment plan generation

Tests for failure mitigation

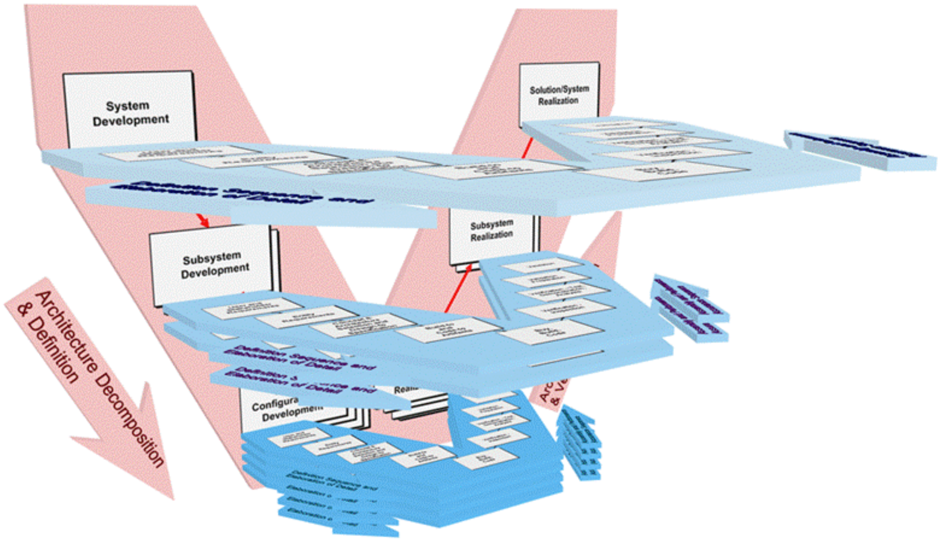
Cybersecurity demonstration

Testing in controlled environment

Testing in uncontrolled environment

Safety Assurance Demonstration

Data and process verification


System Development
Solution/System Realization
Subsystem Realization
Subsystem Development
Architecture Decomposition & Definition
Configura Development
Definition Sequence and Elaboration of Detail

As the system becomes more complex and acting as a 3rd party verifier, data and process verification becomes unavoidable

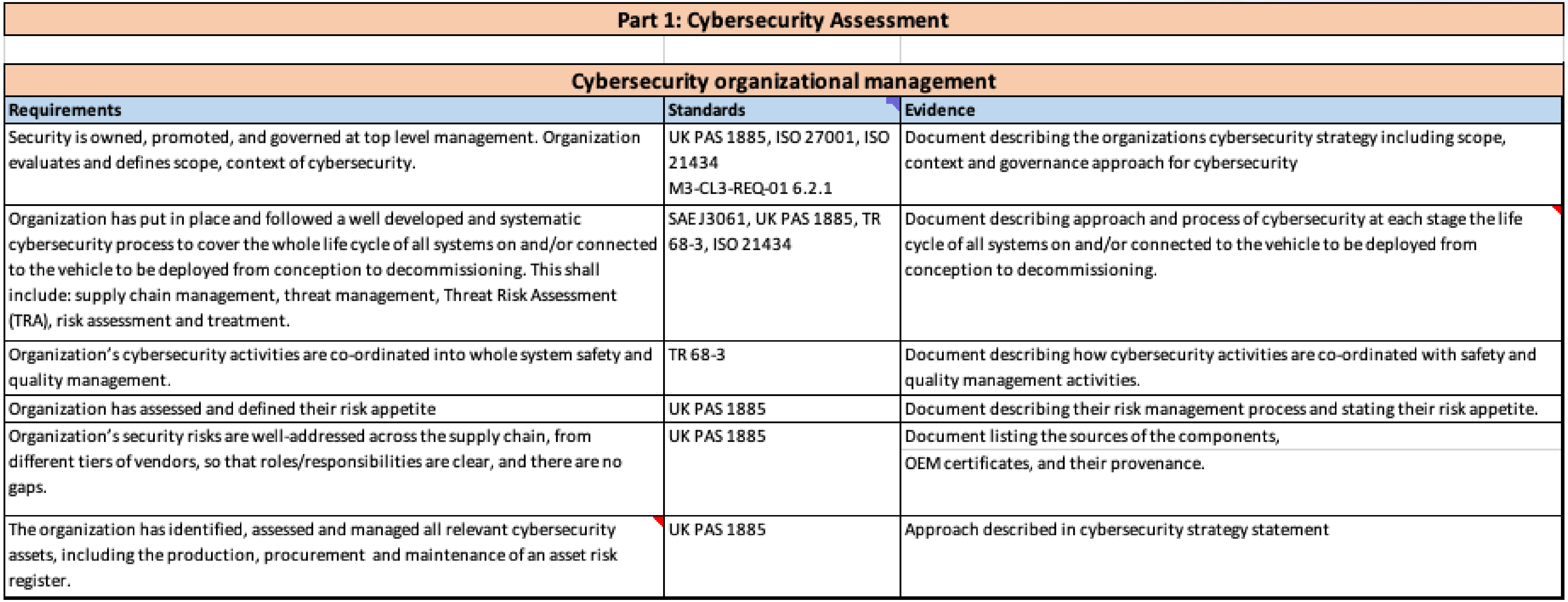
3 examples samples

1. Cybersecurity
    - It is extremely complex to perform independent physical verification as a 3rd party
        - Direct internal knowledge of the system details is required.

2. Assurance of Machine Learning
    - Machine Learning can not be verified using traditional automotive techniques

3. Vehicle behaviour
    - Traffic behaviour is too complex to describe for most conditions
        - If you try to use mathematics to describe all traffic behaviour, you will fail

Cybersecurity – Organizational management

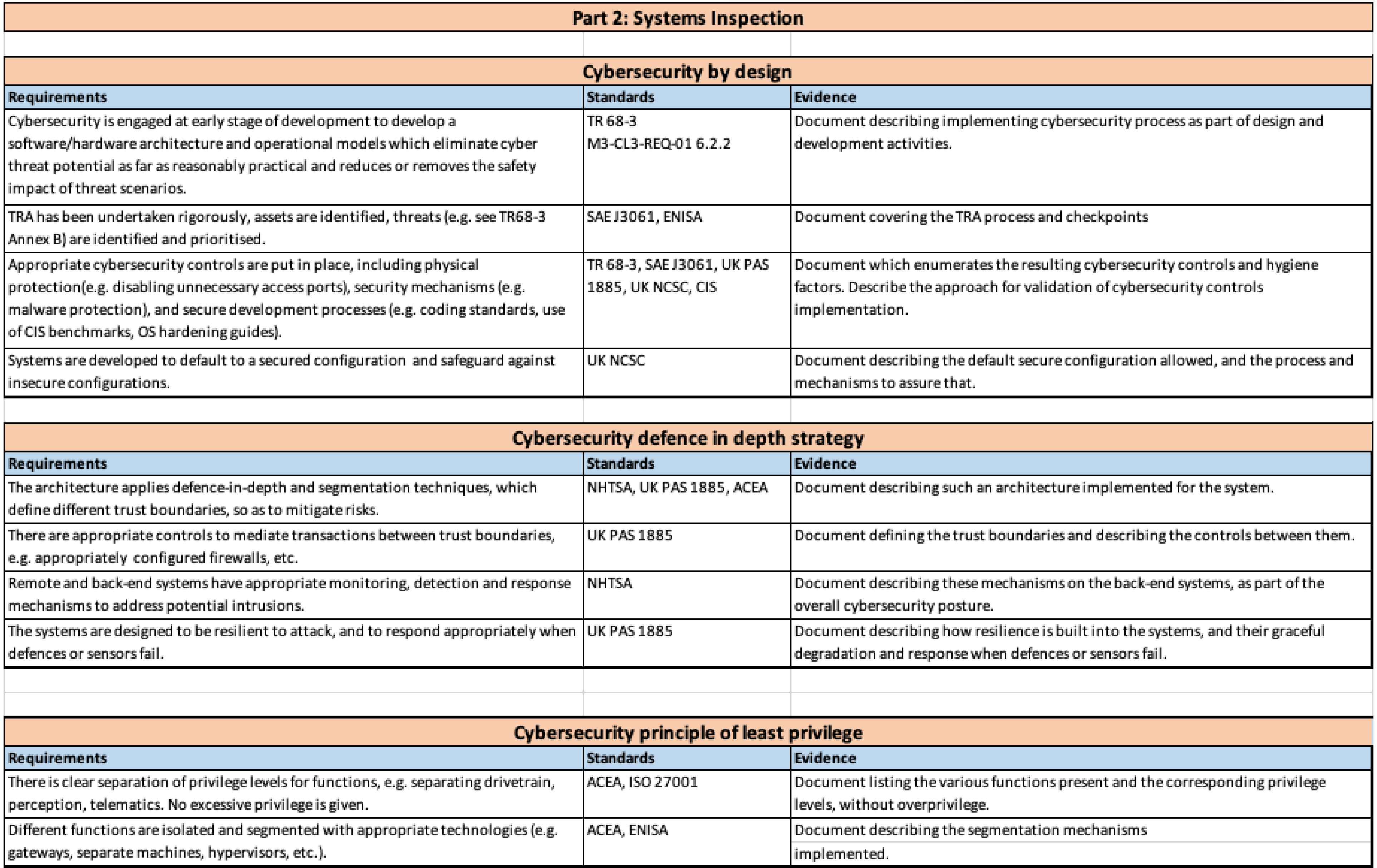


Part 1: Cybersecurity Assessment

Cybersecurity organizational management

Requirements	Standards	Evidence
Security is owned, promoted, and governed at top level management. Organization evaluates and defines scope, context of cybersecurity.	UK PAS 1885, ISO 27001, ISO 21434 M3-CL3-REQ-01 6.2.1	Document describing the organizations cybersecurity strategy including scope, context and governance approach for cybersecurity
Organization has put in place and followed a well developed and systematic cybersecurity process to cover the whole life cycle of all systems on and/or connected to the vehicle to be deployed from conception to decommissioning. This shall include: supply chain management, threat management, Threat Risk Assessment (TRA), risk assessment and treatment.	SAE J3061, UK PAS 1885, TR 68-3, ISO 21434	Document describing approach and process of cybersecurity at each stage the life cycle of all systems on and/or connected to the vehicle to be deployed from conception to decommissioning.
Organization's cybersecurity activities are co-ordinated into whole system safety and quality management.	TR 68-3	Document describing how cybersecurity activities are co-ordinated with safety and quality management activities.
Organization has assessed and defined their risk appetite	UK PAS 1885	Document describing their risk management process and stating their risk appetite.
Organization's security risks are well-addressed across the supply chain, from different tiers of vendors, so that roles/responsibilities are clear, and there are no gaps.	UK PAS 1885	Document listing the sources of the components, OEM certificates, and their provenance.
The organization has identified, assessed and managed all relevant cybersecurity assets, including the production, procurement and maintenance of an asset risk register.	UK PAS 1885	Approach described in cybersecurity strategy statement

Cybersecurity – Systems Inspection



Part 2: Systems Inspection

Cybersecurity by design

Requirements	Standards	Evidence
Cybersecurity is engaged at early stage of development to develop a software/hardware architecture and operational models which eliminate cyber threat potential as far as reasonably practical and reduces or removes the safety impact of threat scenarios.	TR 68-3 M3-CL3-REQ-01 6.2.2	Document describing implementing cybersecurity process as part of design and development activities.
TRA has been undertaken rigorously, assets are identified, threats (e.g. see TR68-3 Annex B) are identified and prioritised.	SAE J3061, ENISA	Document covering the TRA process and checkpoints
Appropriate cybersecurity controls are put in place, including physical protection(e.g. disabling unnecessary access ports), security mechanisms (e.g. malware protection), and secure development processes (e.g. coding standards, use of CIS benchmarks, OS hardening guides).	TR 68-3, SAE J3061, UK PAS 1885, UK NCSC, CIS	Document which enumerates the resulting cybersecurity controls and hygiene factors. Describe the approach for validation of cybersecurity controls implementation.
Systems are developed to default to a secured configuration and safeguard against insecure configurations.	UK NCSC	Document describing the default secure configuration allowed, and the process and mechanisms to assure that.

Cybersecurity defence in depth strategy

Requirements	Standards	Evidence
The architecture applies defence-in-depth and segmentation techniques, which define different trust boundaries, so as to mitigate risks.	NHTSA, UK PAS 1885, ACEA	Document describing such an architecture implemented for the system.
There are appropriate controls to mediate transactions between trust boundaries, e.g. appropriately configured firewalls, etc.	UK PAS 1885	Document defining the trust boundaries and describing the controls between them.
Remote and back-end systems have appropriate monitoring, detection and response mechanisms to address potential intrusions.	NHTSA	Document describing these mechanisms on the back-end systems, as part of the overall cybersecurity posture.
The systems are designed to be resilient to attack, and to respond appropriately when defences or sensors fail.	UK PAS 1885	Document describing how resilience is built into the systems, and their graceful degradation and response when defences or sensors fail.

Cybersecurity principle of least privilege

Requirements	Standards	Evidence
There is clear separation of privilege levels for functions, e.g. separating drivetrain, perception, telematics. No excessive privilege is given.	ACEA, ISO 27001	Document listing the various functions present and the corresponding privilege levels, without overprivilege.
Different functions are isolated and segmented with appropriate technologies (e.g. gateways, separate machines, hypervisors, etc.).	ACEA, ENISA	Document describing the segmentation mechanisms implemented.

Cybersecurity – Systems Inspection

Cybersecurity prioritise protection of safety-critical components and interfaces

Requirements	Standards	Evidence
Attack surfaces are identified as part of TRA, and controls are implemented to minimise the attack surfaces, based on appropriate prioritisation.	SAE J3061, TR 68-3	Document listing the attack surfaces and the corresponding control measures.
There is good resilience to component or system outage, so that safety is not compromised.	UK PAS 1885	Document describing the resilience built into the system, so that it is clear that safety is not affected.
The operational and degraded states of operation which may be engaged during deployment are completely and clearly defined.	ENISA	Document clearly defining the different states involved.

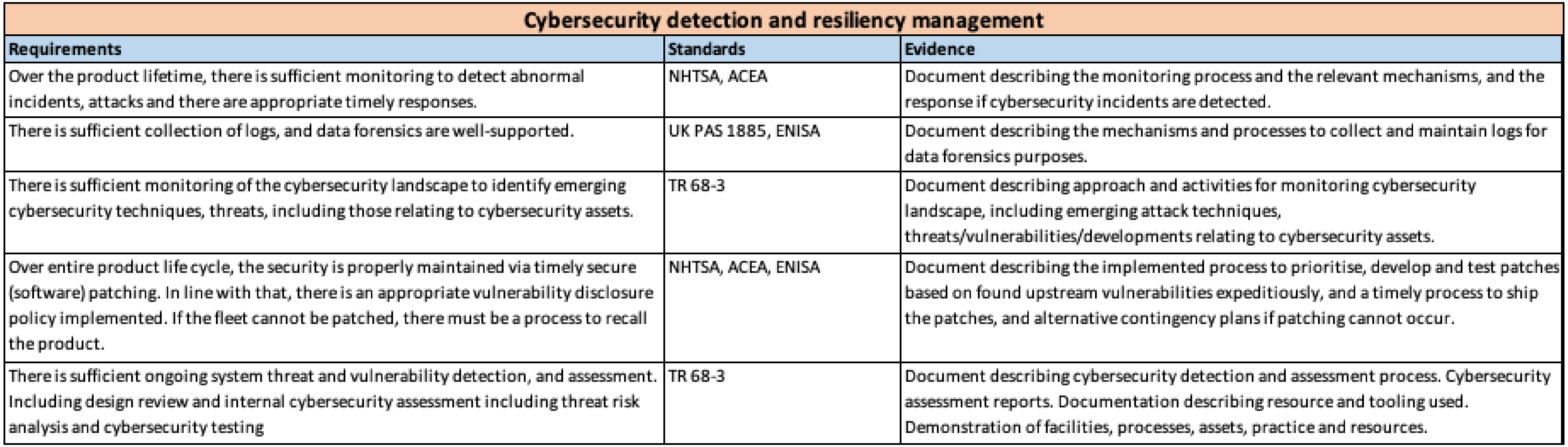
Cybersecurity access and authorisation controls

Requirements	Standards	Evidence
Entities requesting use of resources are authenticated, and must be authorised and on the access control list, before being allowed to access the requested resources. Appropriate authentication mechanisms are used.	UK NCSC	Document listing the types of resources available, and the access control, authorisation, and authentication means.
Appropriate processes in place for managing service procedures and other physical access	TR 68-3	Document describing physical access controls. Demonstration of service procedure and controls.

Cybersecurity encryption of sensitive data

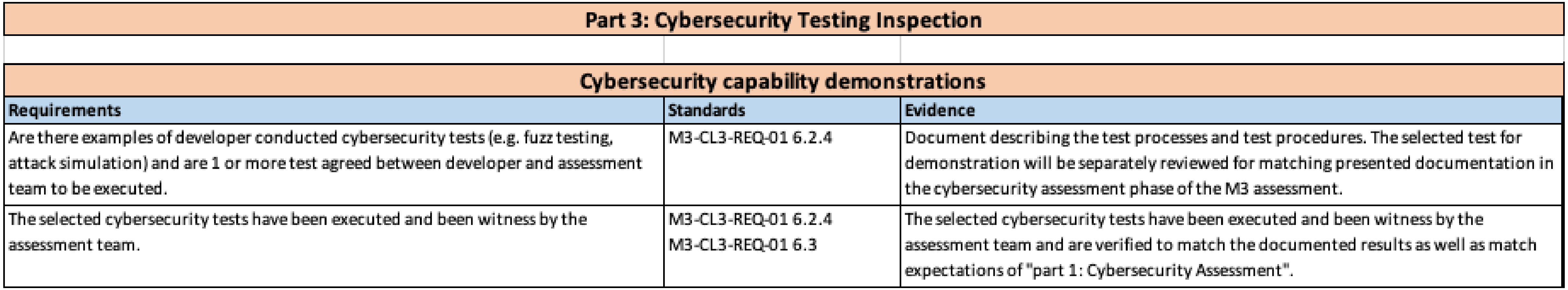
Requirements	Standards	Evidence
Assets must be identified through the TRA, and appropriate protection mechanisms implemented.	SAE J3061, ENISA, TR 68-3	Document listing the assets and their control means, as part of TRA.
Only appropriate approved algorithms (for hashing, signature, MAC, symmetric and asymmetric encryption) are used. Likewise, only approved security protocols are used.	ISO standards (ISO 10118, 11770, 13888, 14888, 15946, 18014, 18033, 9797, 9798, etc.)	Document describing such cryptographic protocols and algorithms used.
Communications outside of the vehicle are secured with appropriate confidentiality and integrity algorithms and schemes.	ACEA, ENISA	Document describing external communications and such security mechanisms in place.
Intra-vehicular traffic is secured with appropriate confidentiality and integrity algorit	NHTSA, ACEA	Document describing internal communications and such security mechanisms in place.
Software and image integrity for computing elements is assured by appropriate security mechanisms, such as platform root-of-trust and secure-boot.	NHTSA	Document describing the platform security mechanisms.
In particular, sensitive materials such as secret keys, passwords, private key certificates, etc., are subjected to high degree of protections. Materials such as private keys should be generated securely. Such materials must not be extractable from the system.	ISO 13491-1, NIST SP 800-57	Document listing the protection mechanisms, and/or OEM certificates (e.g. FIPS 140-2 certificate)

Cybersecurity – Systems Inspection



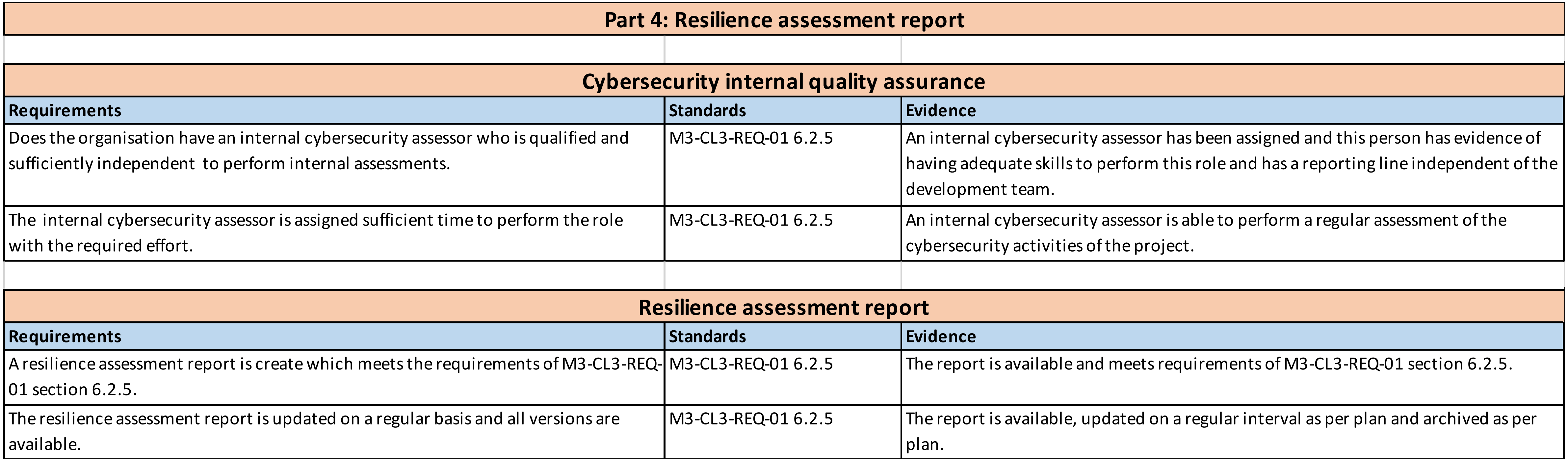
Cybersecurity detection and resiliency management		
Requirements	**Standards**	**Evidence**
Over the product lifetime, there is sufficient monitoring to detect abnormal incidents, attacks and there are appropriate timely responses.	NHTSA, ACEA	Document describing the monitoring process and the relevant mechanisms, and the response if cybersecurity incidents are detected.
There is sufficient collection of logs, and data forensics are well-supported.	UK PAS 1885, ENISA	Document describing the mechanisms and processes to collect and maintain logs for data forensics purposes.
There is sufficient monitoring of the cybersecurity landscape to identify emerging cybersecurity techniques, threats, including those relating to cybersecurity assets.	TR 68-3	Document describing approach and activities for monitoring cybersecurity landscape, including emerging attack techniques, threats/vulnerabilities/developments relating to cybersecurity assets.
Over entire product life cycle, the security is properly maintained via timely secure (software) patching. In line with that, there is an appropriate vulnerability disclosure policy implemented. If the fleet cannot be patched, there must be a process to recall the product.	NHTSA, ACEA, ENISA	Document describing the implemented process to prioritise, develop and test patches based on found upstream vulnerabilities expeditiously, and a timely process to ship the patches, and alternative contingency plans if patching cannot occur.
There is sufficient ongoing system threat and vulnerability detection, and assessment. Including design review and internal cybersecurity assessment including threat risk analysis and cybersecurity testing	TR 68-3	Document describing cybersecurity detection and assessment process. Cybersecurity assessment reports. Documentation describing resource and tooling used. Demonstration of facilities, processes, assets, practice and resources.

Cybersecurity – Testing Inspection



Part 3: Cybersecurity Testing Inspection		
Cybersecurity capability demonstrations		
Requirements	**Standards**	**Evidence**
Are there examples of developer conducted cybersecurity tests (e.g. fuzz testing, attack simulation) and are 1 or more test agreed between developer and assessment team to be executed.	M3-CL3-REQ-01 6.2.4	Document describing the test processes and test procedures. The selected test for demonstration will be separately reviewed for matching presented documentation in the cybersecurity assessment phase of the M3 assessment.
The selected cybersecurity tests have been executed and been witness by the assessment team.	M3-CL3-REQ-01 6.2.4 M3-CL3-REQ-01 6.3	The selected cybersecurity tests have been executed and been witness by the assessment team and are verified to match the documented results as well as match expectations of "part 1: Cybersecurity Assessment".

Cybersecurity – Resilience Assessment



Part 4: Resilience assessment report

Cybersecurity internal quality assurance

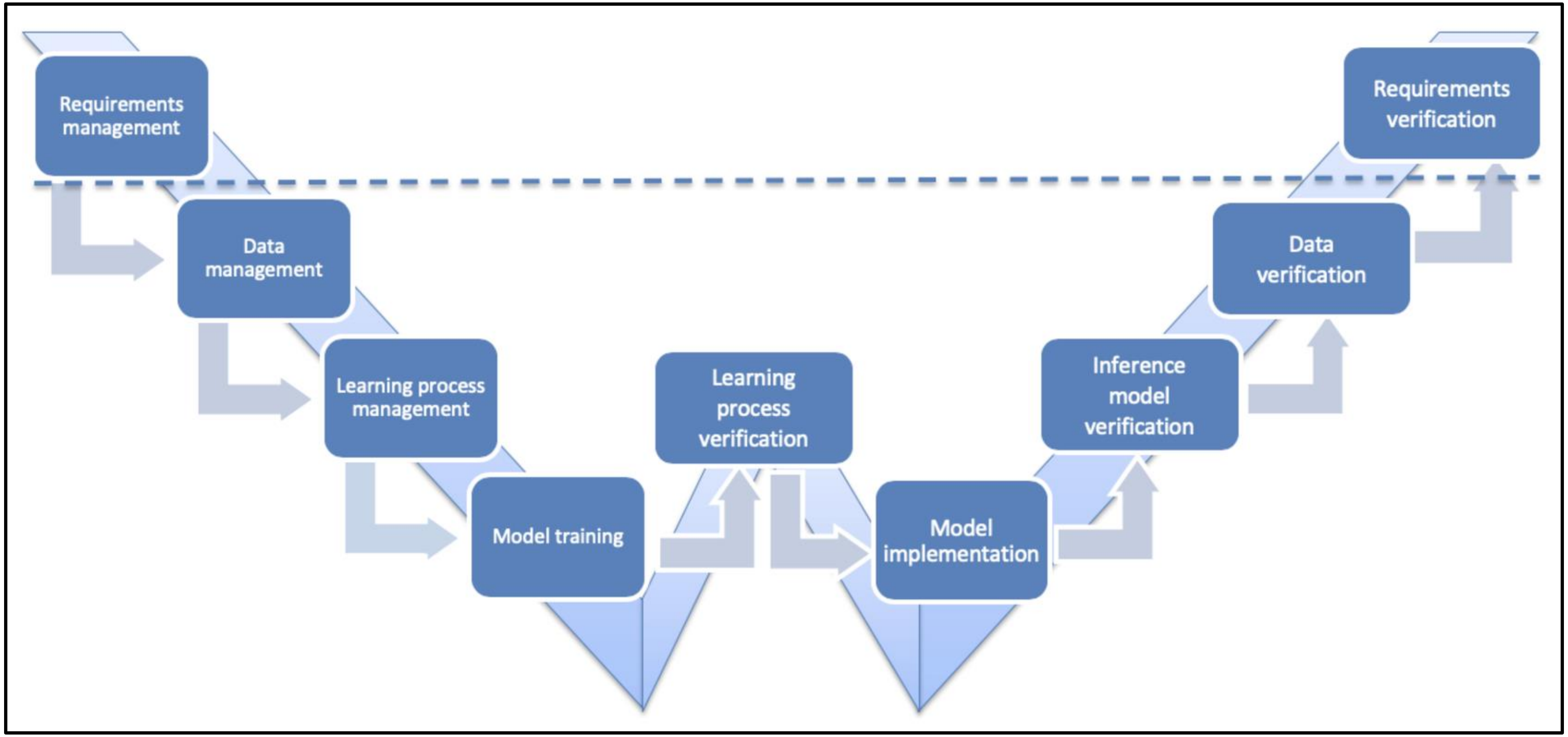
Requirements	Standards	Evidence
Does the organisation have an internal cybersecurity assessor who is qualified and sufficiently independent to perform internal assessments.	M3-CL3-REQ-01 6.2.5	An internal cybersecurity assessor has been assigned and this person has evidence of having adequate skills to perform this role and has a reporting line independent of the development team.
The internal cybersecurity assessor is assigned sufficient time to perform the role with the required effort.	M3-CL3-REQ-01 6.2.5	An internal cybersecurity assessor is able to perform a regular assessment of the cybersecurity activities of the project.

Resilience assessment report

Requirements	Standards	Evidence
A resilience assessment report is create which meets the requirements of M3-CL3-REQ-01 section 6.2.5.	M3-CL3-REQ-01 6.2.5	The report is available and meets requirements of M3-CL3-REQ-01 section 6.2.5.
The resilience assessment report is updated on a regular basis and all versions are available.	M3-CL3-REQ-01 6.2.5	The report is available, updated on a regular interval as per plan and archived as per plan.

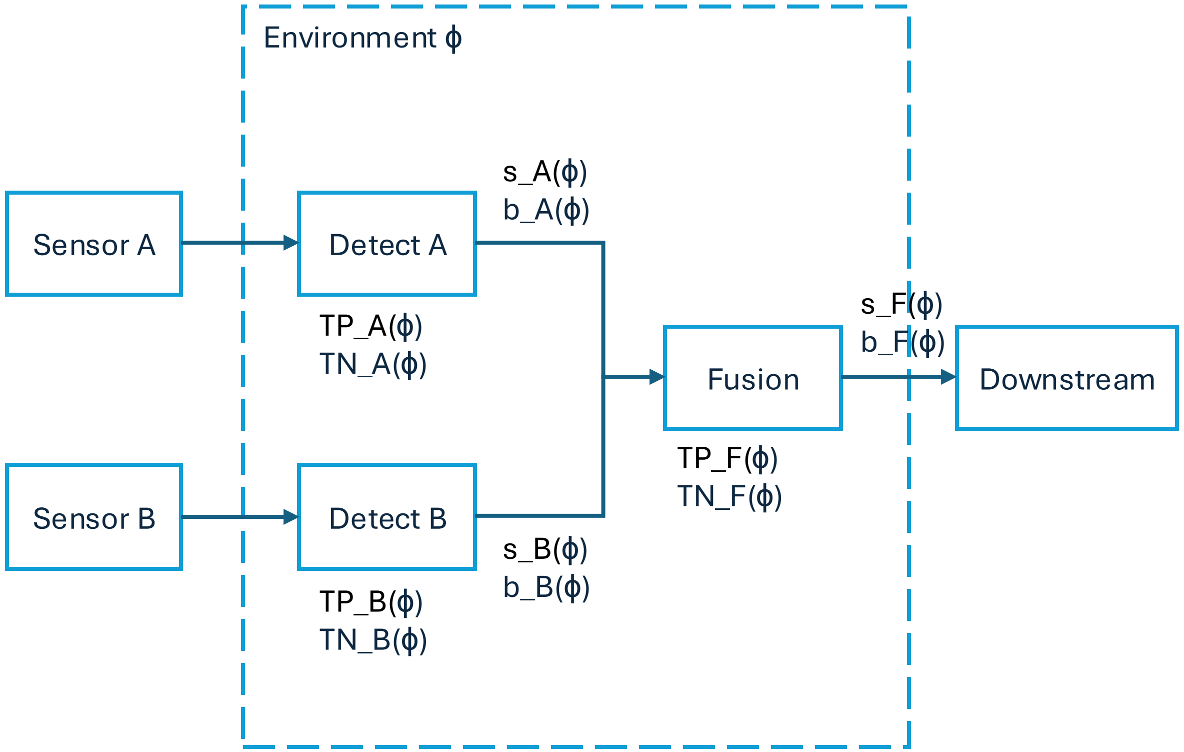
W-Shaped Machine Learning Assurance

- New area: Assurance of Machine Learning derived functionality.


Requirements management
Data management
Learning process management
Model training
Learning process verification
Model implementation
Inference model verification
Data verification
Requirements verification

Source: Concepts of Design Assurance for Neural Networks (CoDANN), EASA & Daedalean, 2021

Compositional performance and belief propagation : training & deployment environment specific

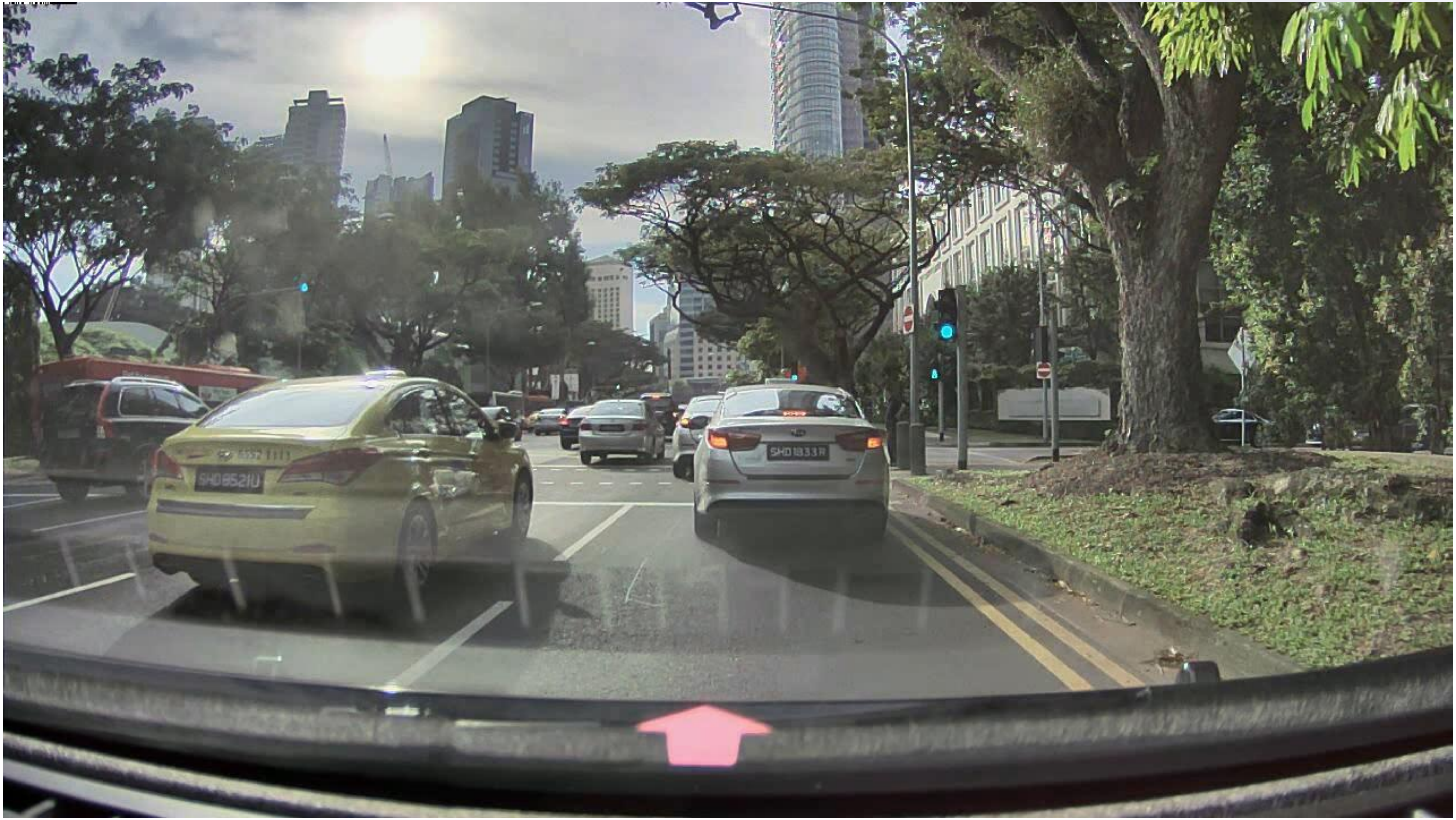


Challenge

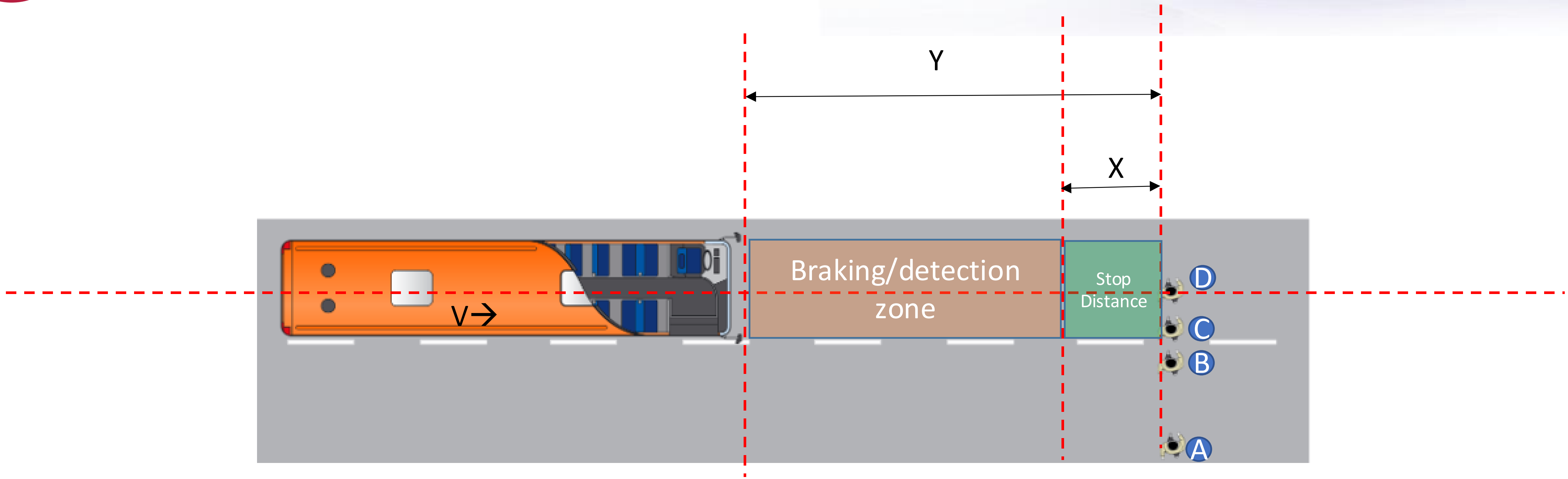
- Given:
  - Modules for Detect A, Detect B providing states s and beliefs / probabilities / confidences b
  - Detect B could be ML based
  - Environment ϕ
  - (Empirical Validation) Performance True Positive, True Negatives in Environment ϕ
- Question:
  - How to model statistical quantities propagating downstream?
    - Design-time: ROC parameters TP, TN -> verify quantitative safety goals
    - Run-time: s, b -> report detected obstacle
    - ..
  - Does any of this give us principled instructions on the design of Fusion?
  - How to model Environment ϕ changes
- Remark: Illustrated here for perception, but to be generalizable across architecture

Source: Claus Bahlmann, Dagstuhl Seminar 11.04.2024

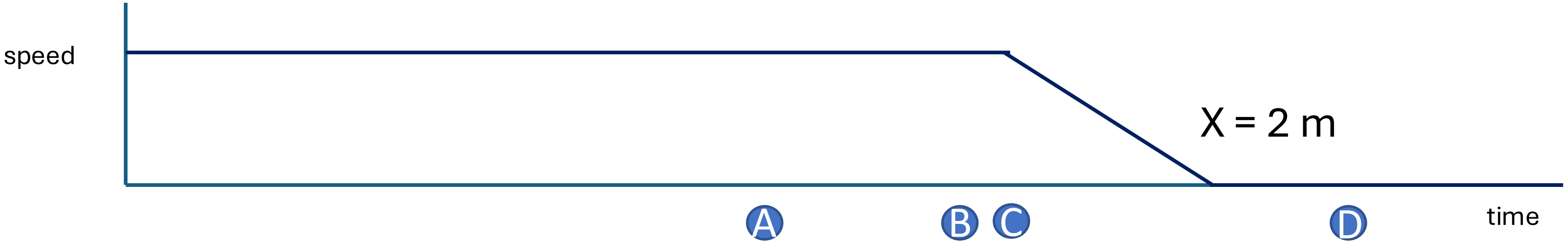
Challenge: complex traffic scenarios



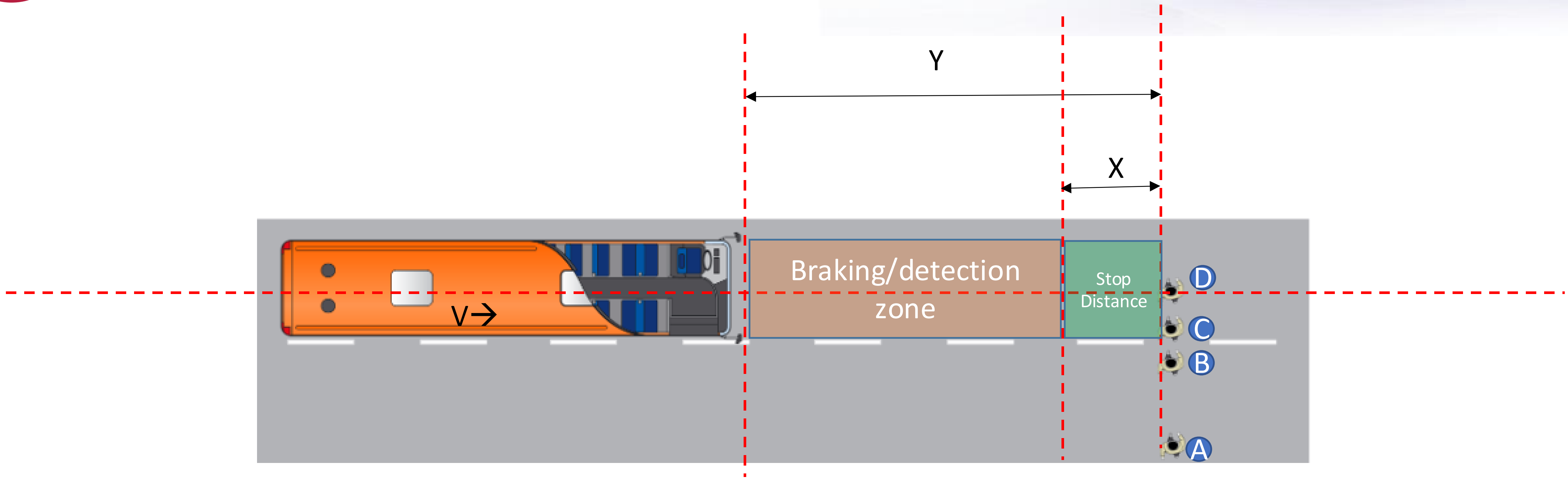
Challenges: what is the desired behaviour?



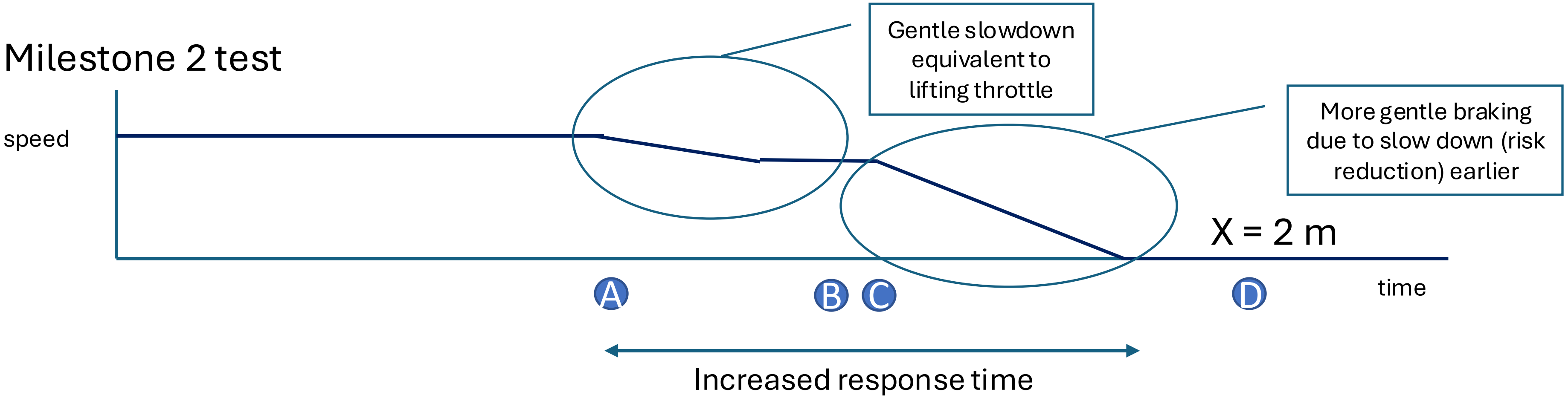
Milestone 1 test



Challenges: what is the desired behaviour?



Milestone 2 test



Gentle slowdown equivalent to lifting throttle

More gentle braking due to slow down (risk reduction) earlier

Future research

- How do we assess the performance of autonomous vehicles?
  - There is lots of data available, but how do we condense it in a relatively simple set of metrics which can give sufficient confidence to allow for complete driverless operation?

Thank You