Safety Argument Framework for Vehicle Autonomy

John Birch
Chief Engineer
Functional Safety

May 17

Agenda

- Safety challenges with autonomy
- Value of an explicit safety argument
- MISRA safety argument model
- Safety argument framework
- Concluding remarks

Safety Challenges with Autonomy

Safety Challenges with Autonomy (SAE Level 3+)

- Safety of the Intended Functionality (SOTIF)
  - Hazardous behaviour not only caused by malfunction
  - Not always clear how system should behave in order to be ‘safe’
  - May be required to trade off one form of hazardous behaviour for another
  - Safety challenge is not just technical but also philosophical and ethical

- No clear definition of acceptable risk
  - Even with ongoing exercise to develop the SOTIF PAS (ISO/PAS 21448) in line with ISO 26262 edition 2

- Required technology at odds with existing standards
  - ‘Non-deterministic’ software

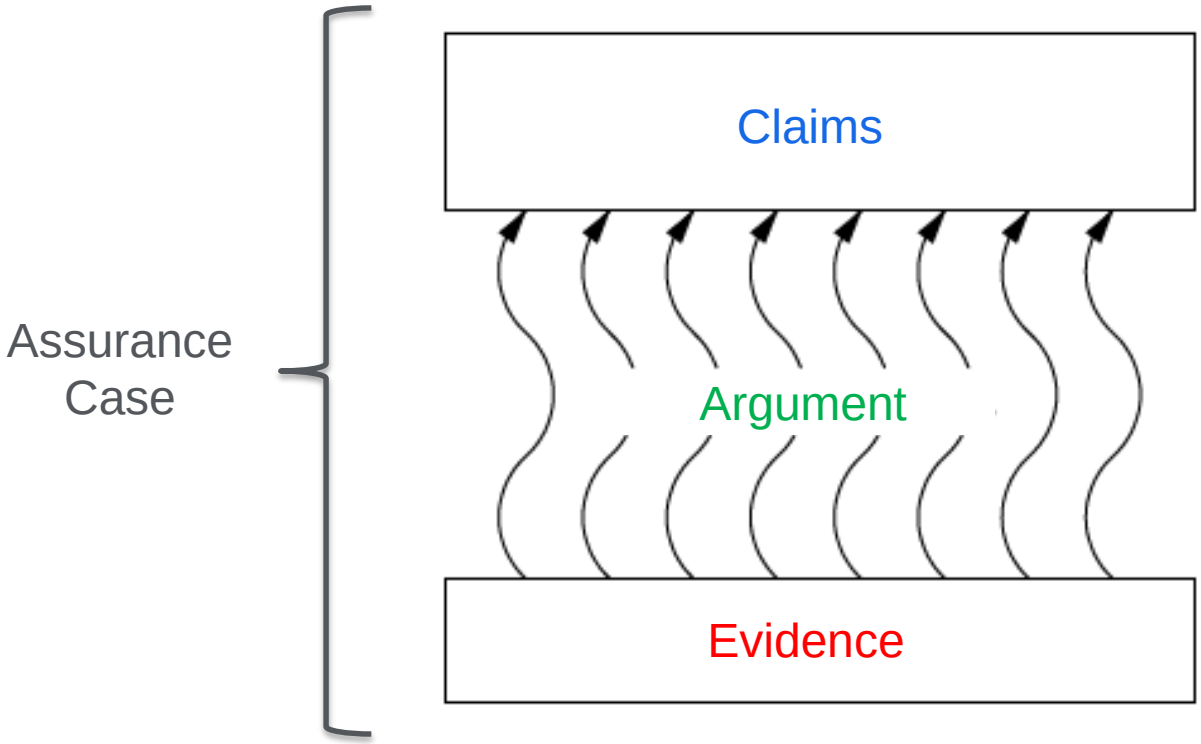
Safety Challenges with Autonomy (SAE Level 3+)

- Safety of the Intended Functionality (SOTIF)
  - Hazardous behaviour not only caused by malfunctio
  - Not always clear how system should behave i
  - May be required to trade off one form … another
  - Safety challenge is not just tec… al and ethical
- No clear definition …
  - Even wi… elop the SOTIF PAS (ISO/PAS 21448) in lin…
- P… gy at odds with existing standards
  - …eterministic' software

Whatever the safety argument is, it needs to be written down!

Value of an Explicit Safety Argument

Value of an Explicit Safety Argument



Adaption of figure from:
Kelly, T. P., Arguing Safety – A Systematic Approach to Safety Case Management, DPhil Thesis, Department of Computer Science, University of York, UK, 1998

Value of an Explicit Safety Argument

Claims

The autonomous vehicle is acceptably safe for use on pubic roads

Argument

Evidence

Value of an Explicit Safety Argument

Claims

The autonomous vehicle is acceptably safe for use on pubic roads

Argument

Evidence

Test result showing three million miles of incident-free autonomous driving

Successful audit against the requirements of standard x

Value of an Explicit Safety Argument

Claims

The autonomous vehicle is acceptably safe for use on pubic roads

Argument

???

Evidence

Test result showing three million miles of incident-free autonomous driving

Successful audit against the requirements of standard x

Value of an Explicit Safety Argument

Claims

The autonomous vehicle is acceptably safe f… …abic roads

…??

Evidence

T… …owing three million miles of incident-free autonomous driving

Successful audit against the requirements of standard x

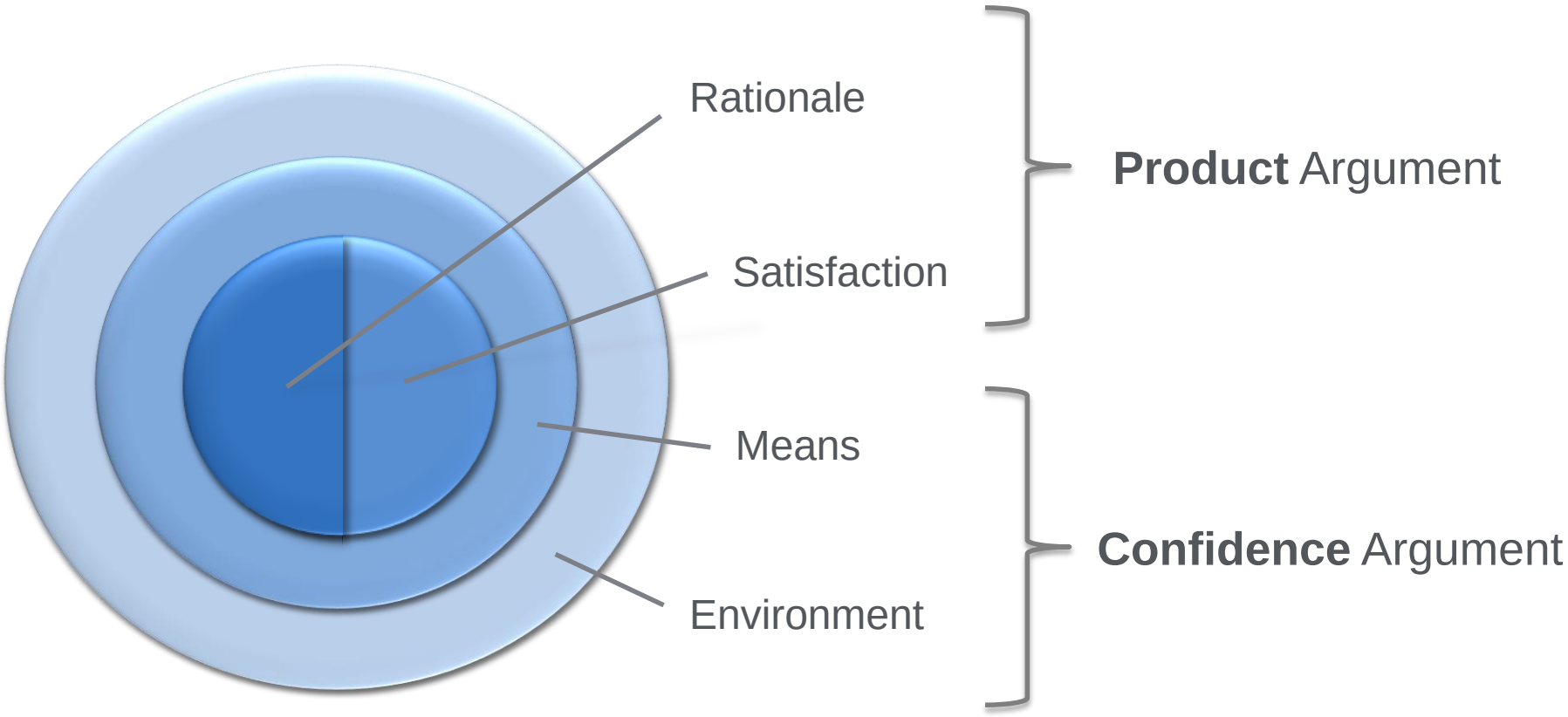
Evidence without argument is unexplained

MISRA Safety Case Guidelines: Argument Model

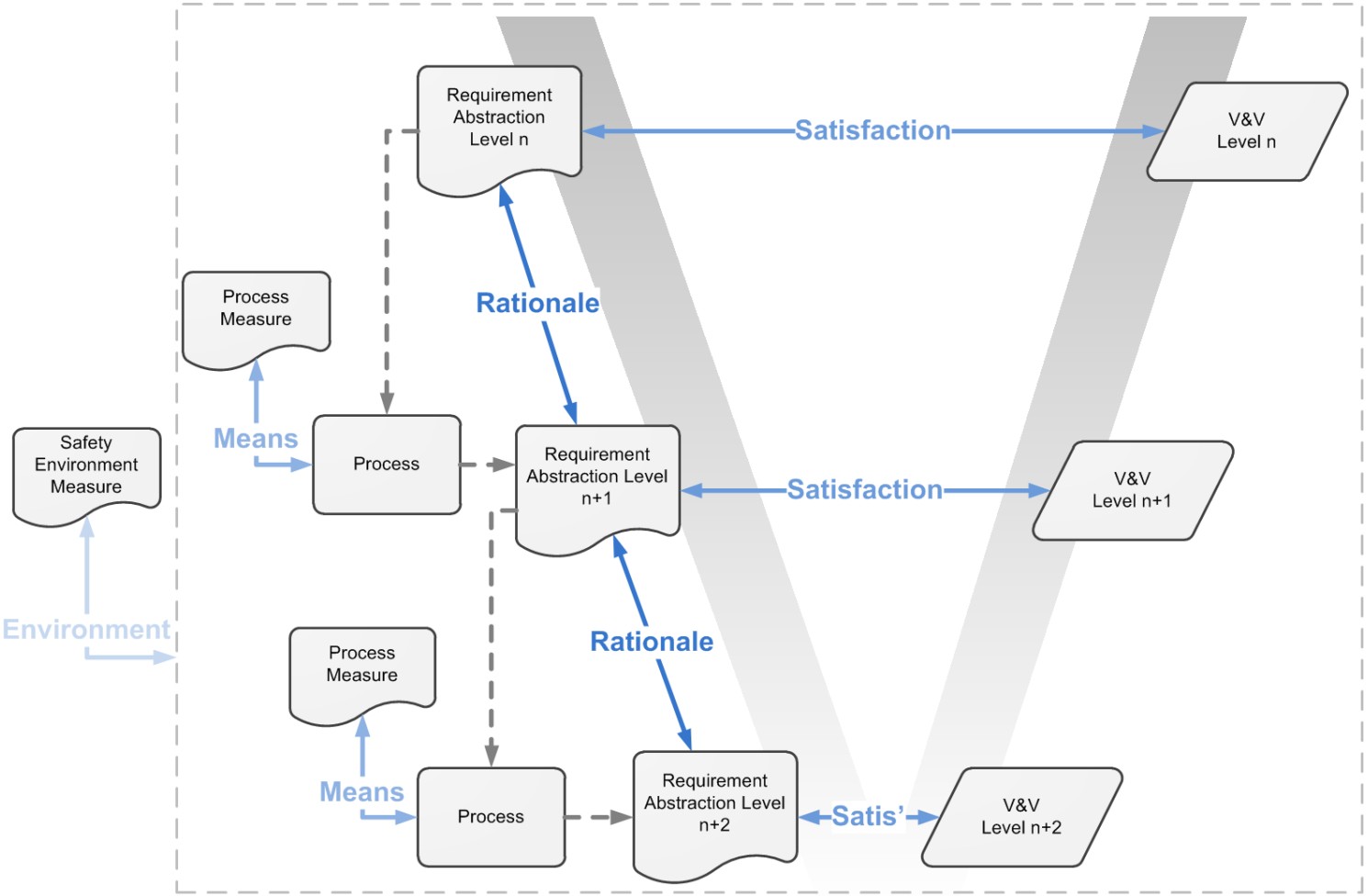
MISRA Safety Case Guidelines

- MISRA (Motor Industry Software Reliability Association) producing a set of guidelines on automotive safety case development
  - Due for publication late 2017
  - Initial scope aligned with ISO 26262 Edition 1
  - Collaborative activity:

MISRA Safety Case Guidelines
Argument Model

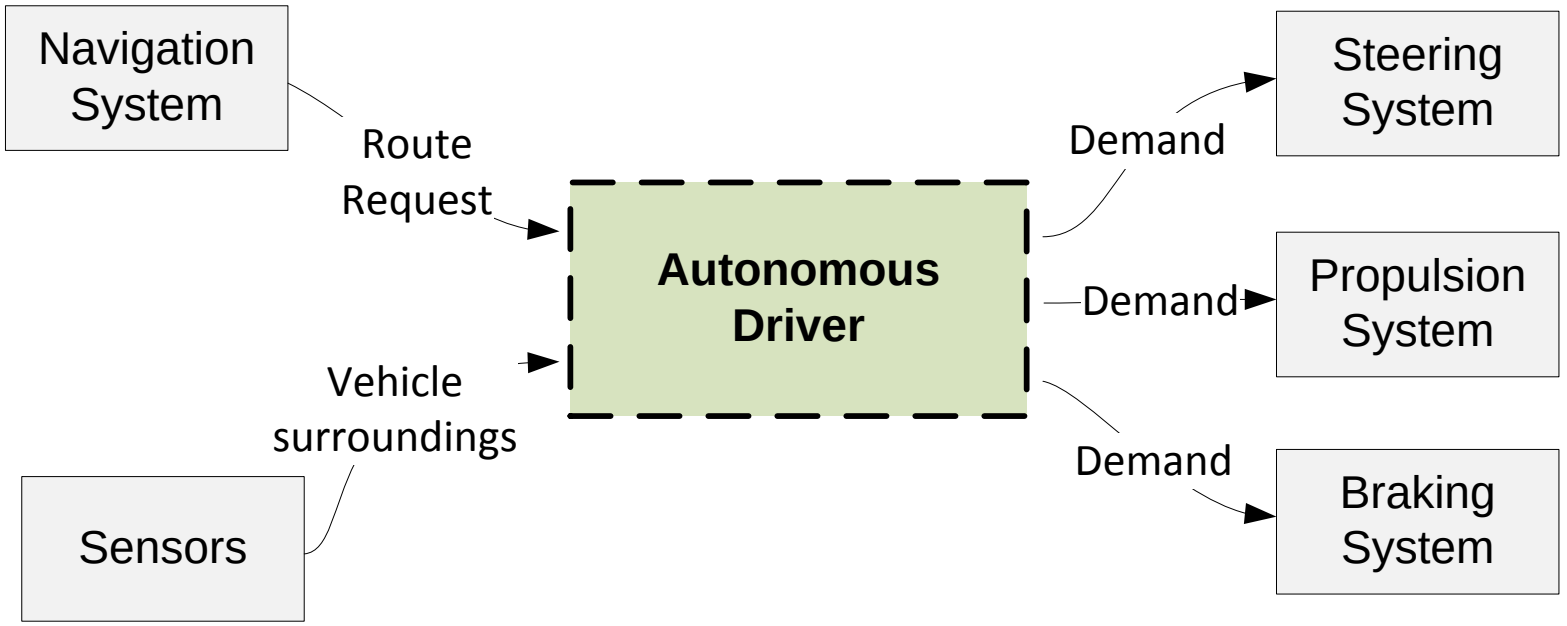


MISRA Safety Case Guidelines
Argument Model

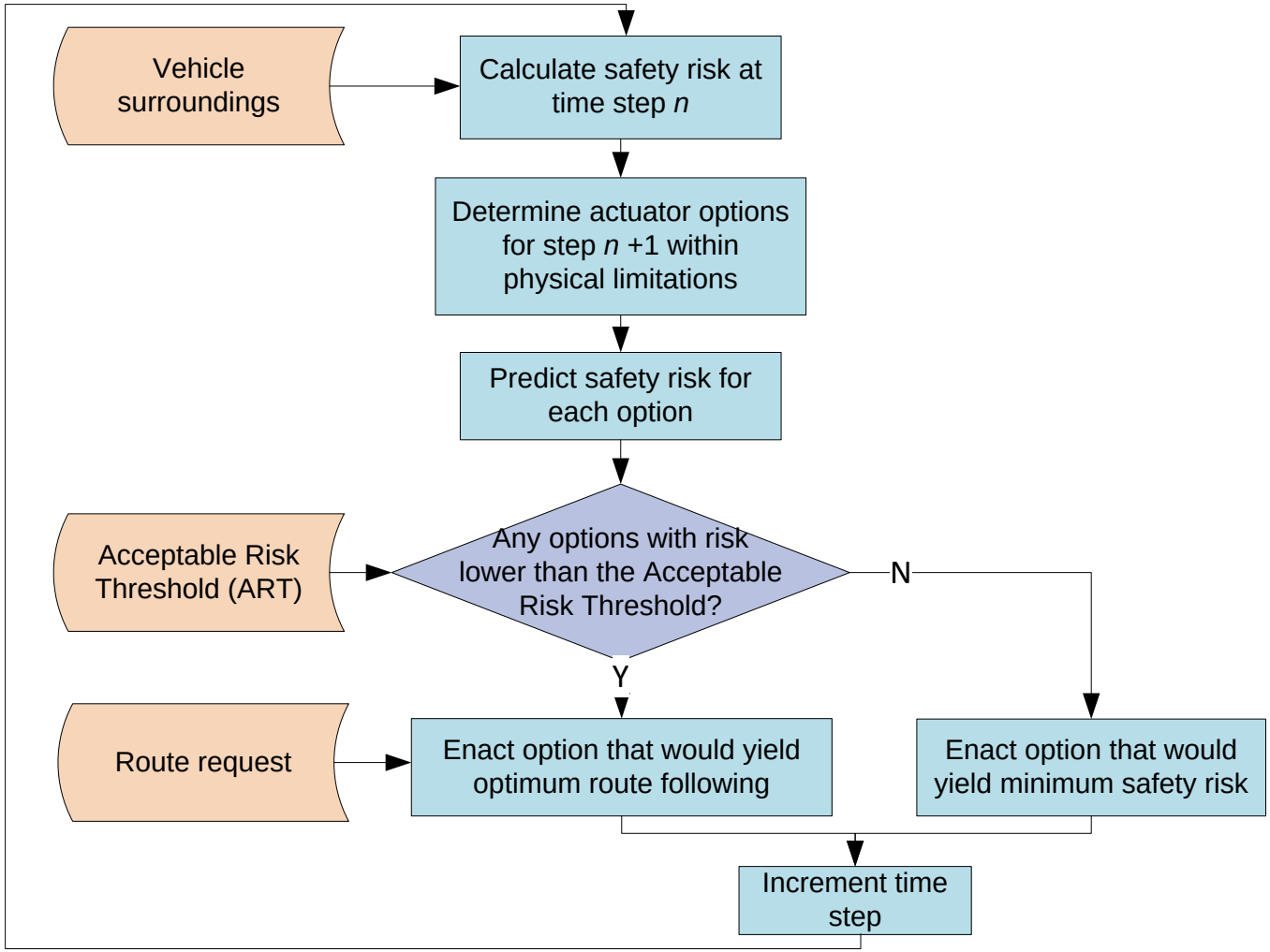


Assurance Argument Framework

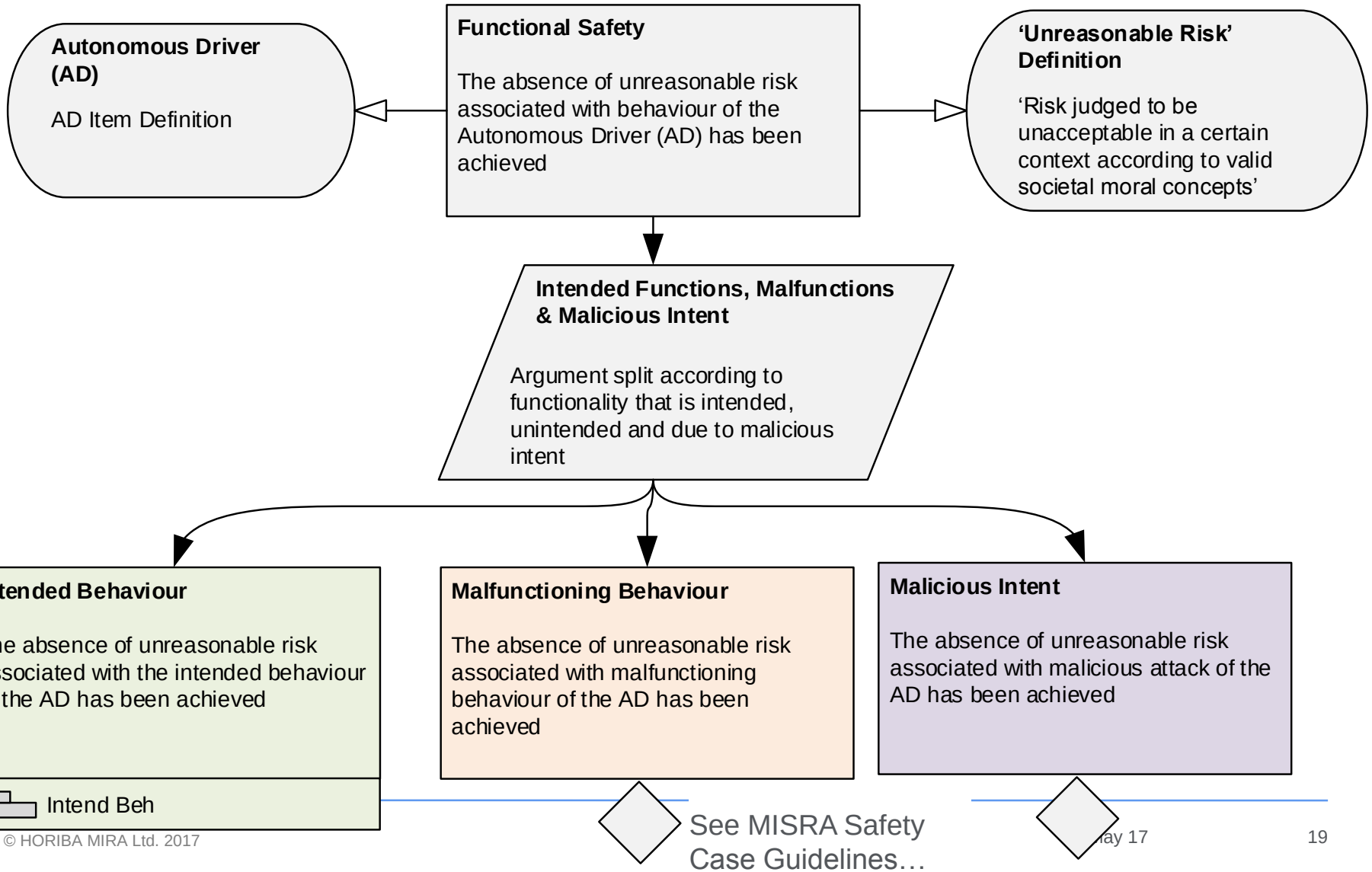
Assurance Argument Framework
Item Definition – Autonomous Driver



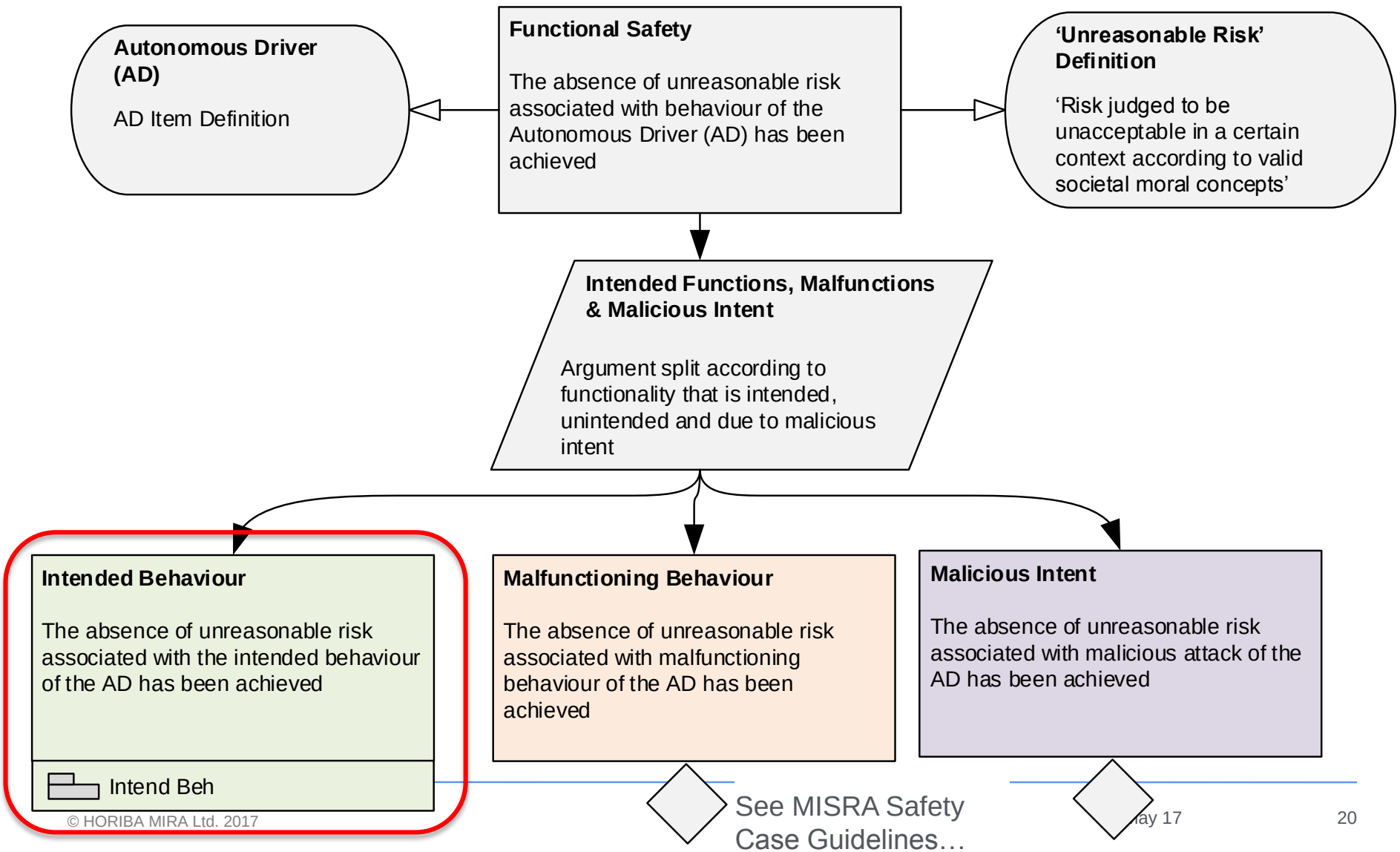
Assurance Argument Framework
Item Definition – Autonomous Driver



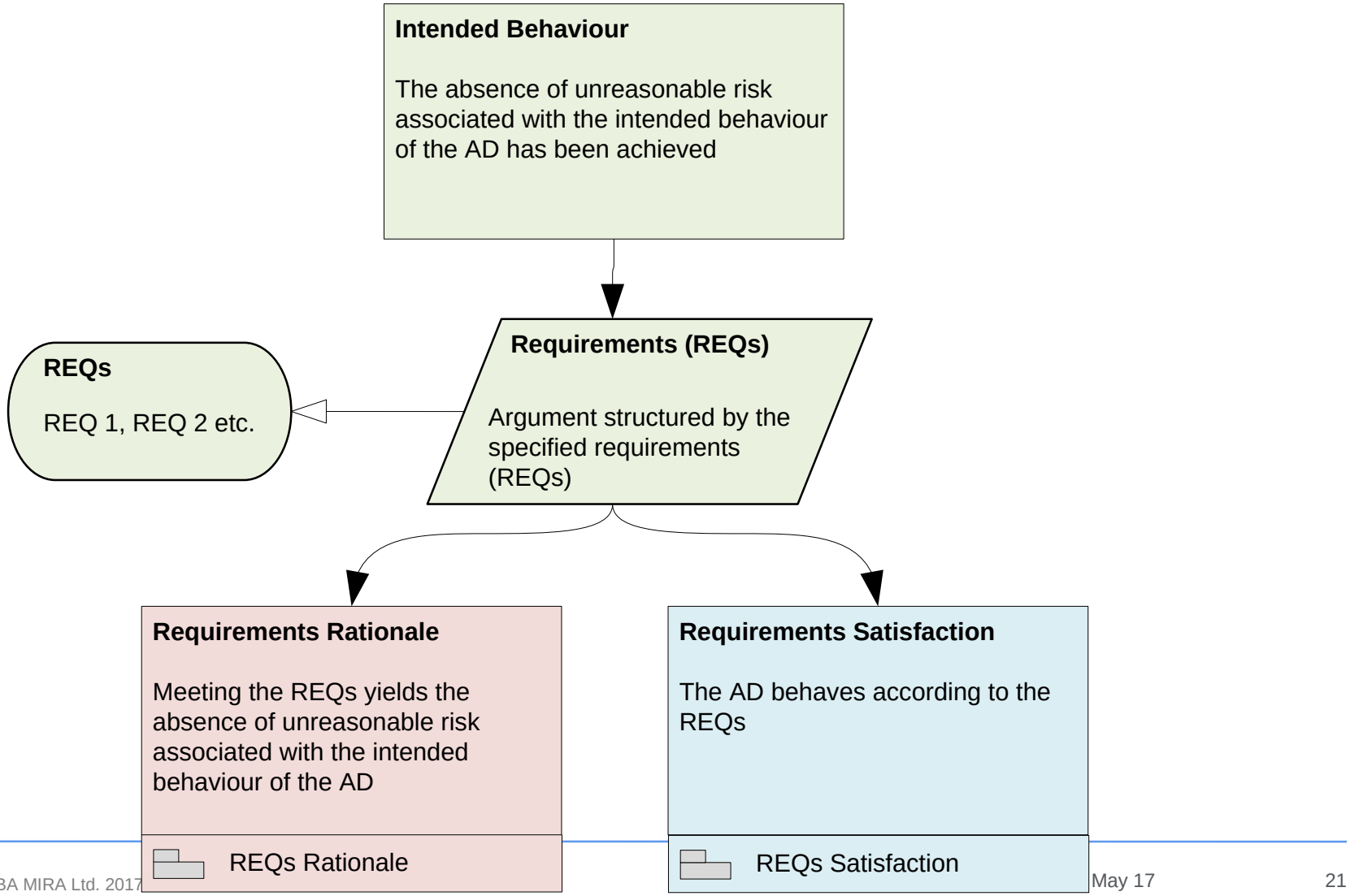
Assurance Argument Framework
Functional Safety



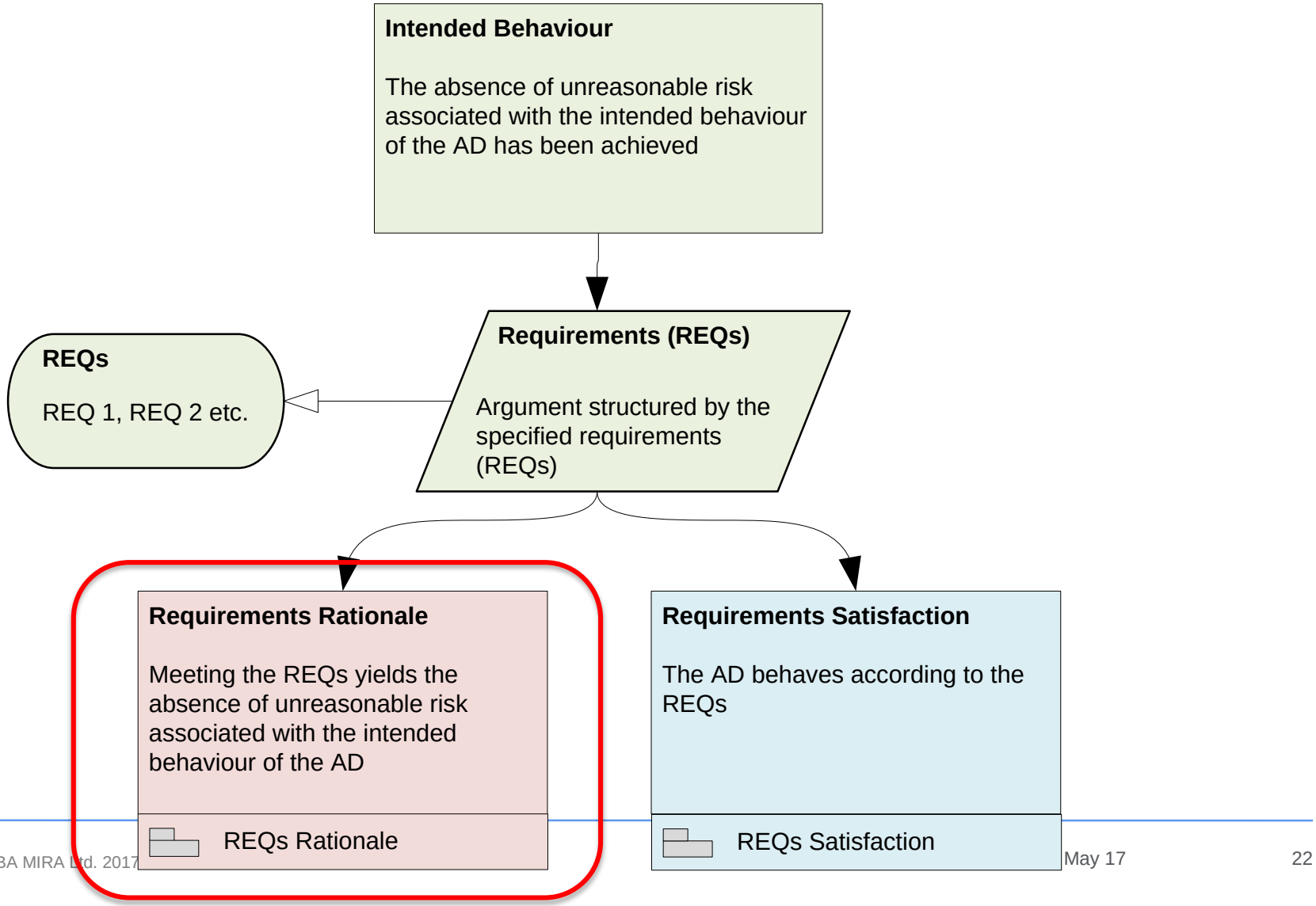
Assurance Argument Framework
Functional Safety



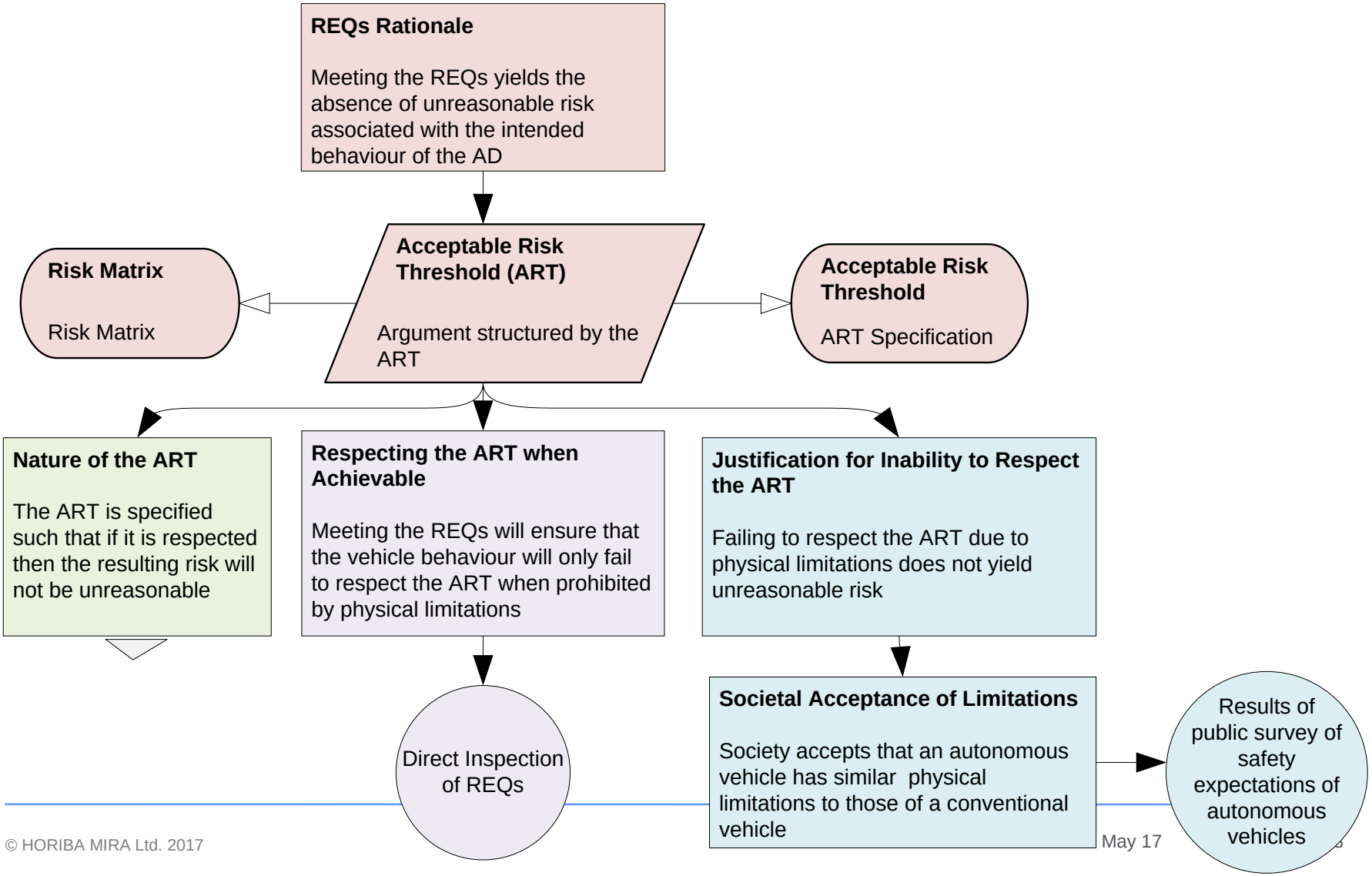
Assurance Argument Framework
Functional Safety – Intended Behaviour



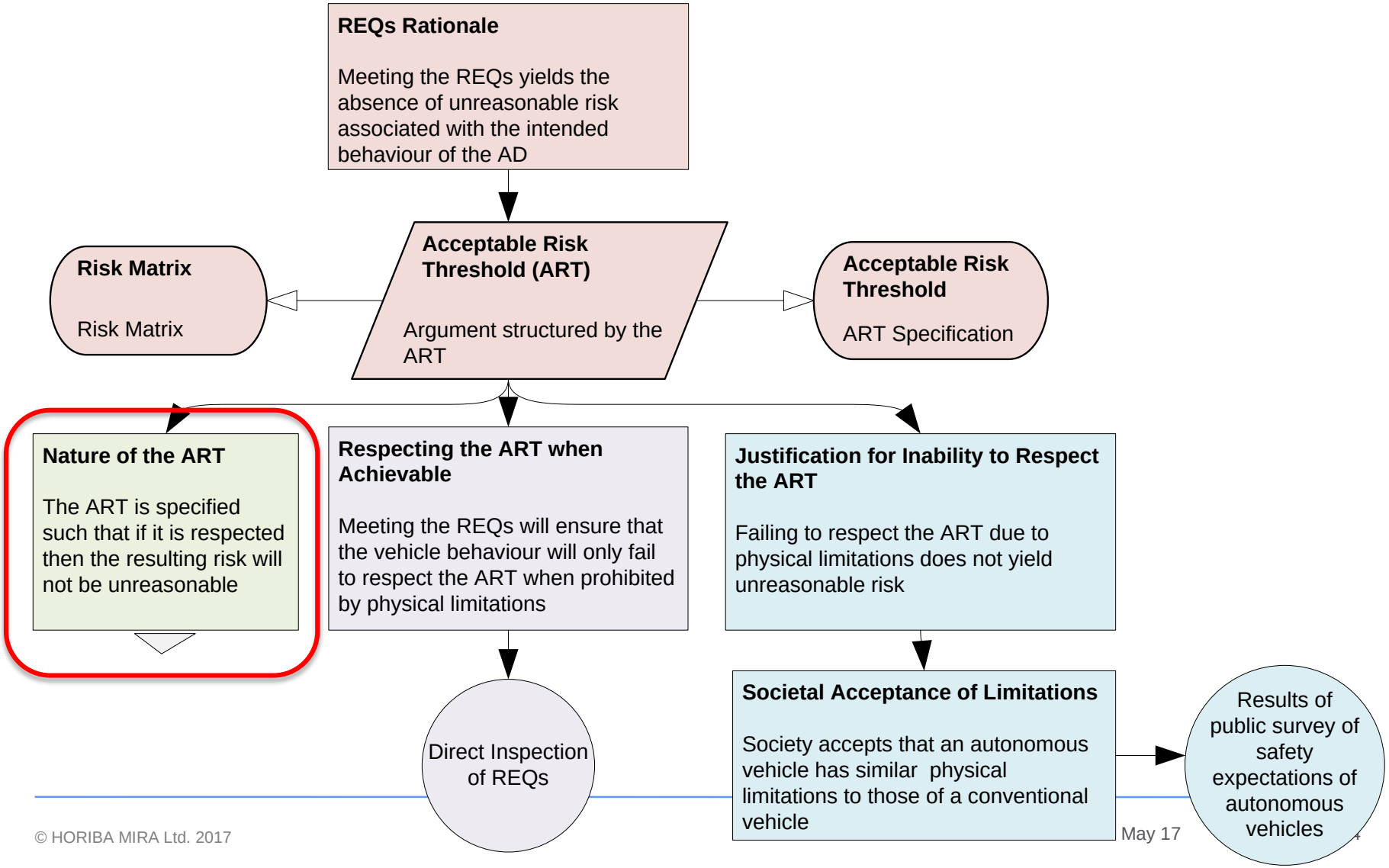
Assurance Argument Framework
Functional Safety – Intended Behaviour



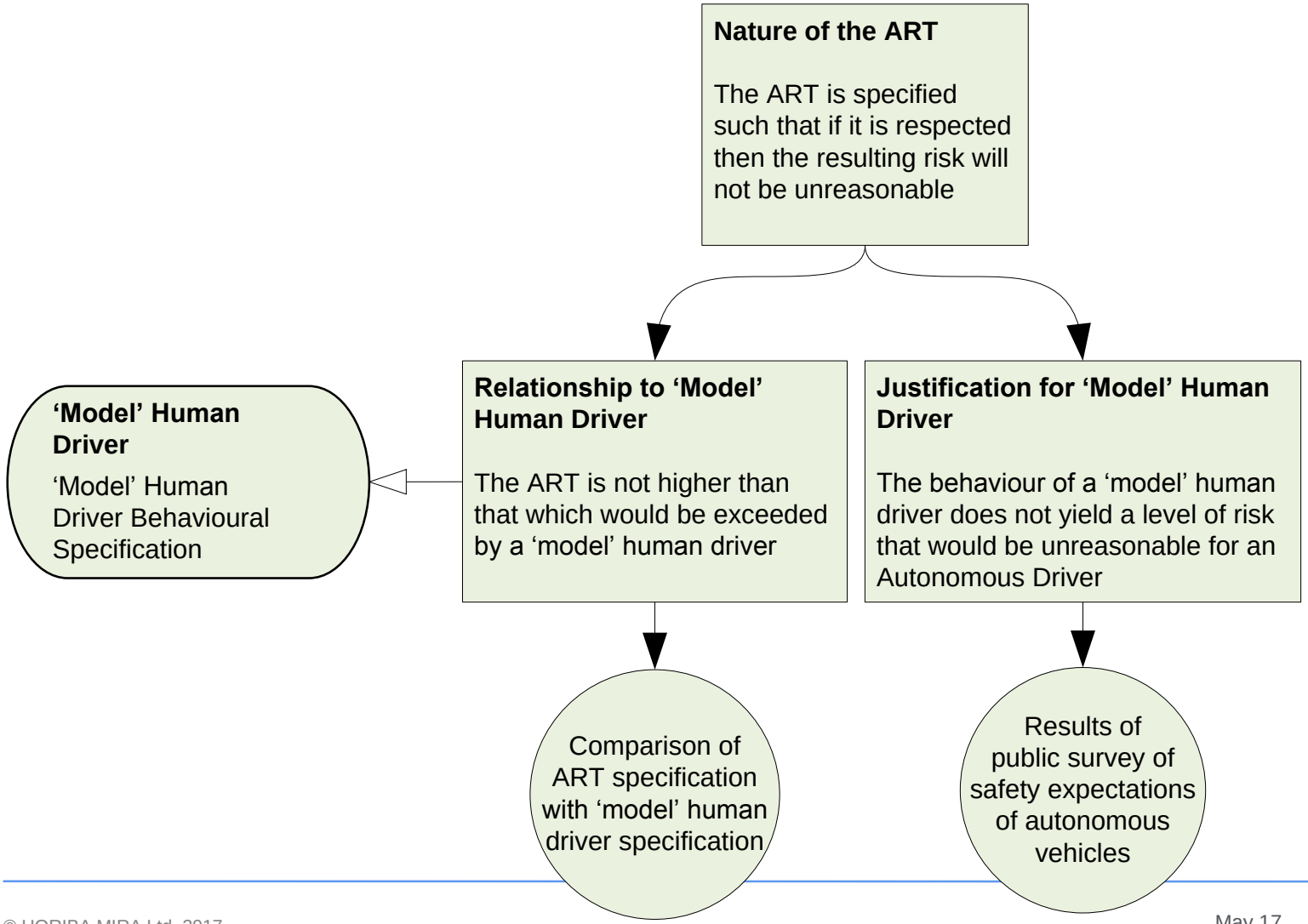
Assurance Argument Framework
Functional Safety – Intended Behaviour Rationale



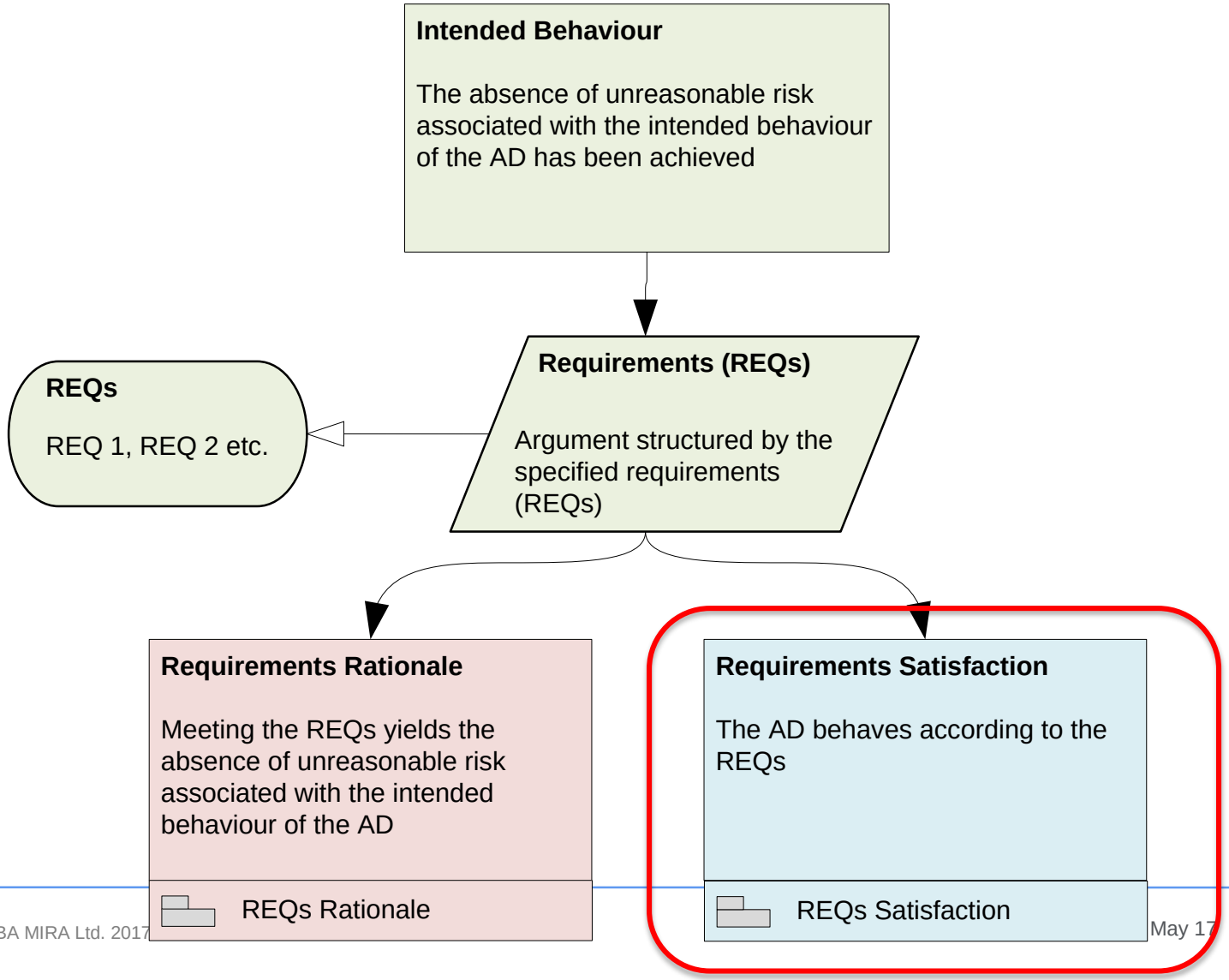
Assurance Argument Framework
Functional Safety – Intended Behaviour Rationale



Assurance Argument Framework
Functional Safety – Intended Behaviour Rationale

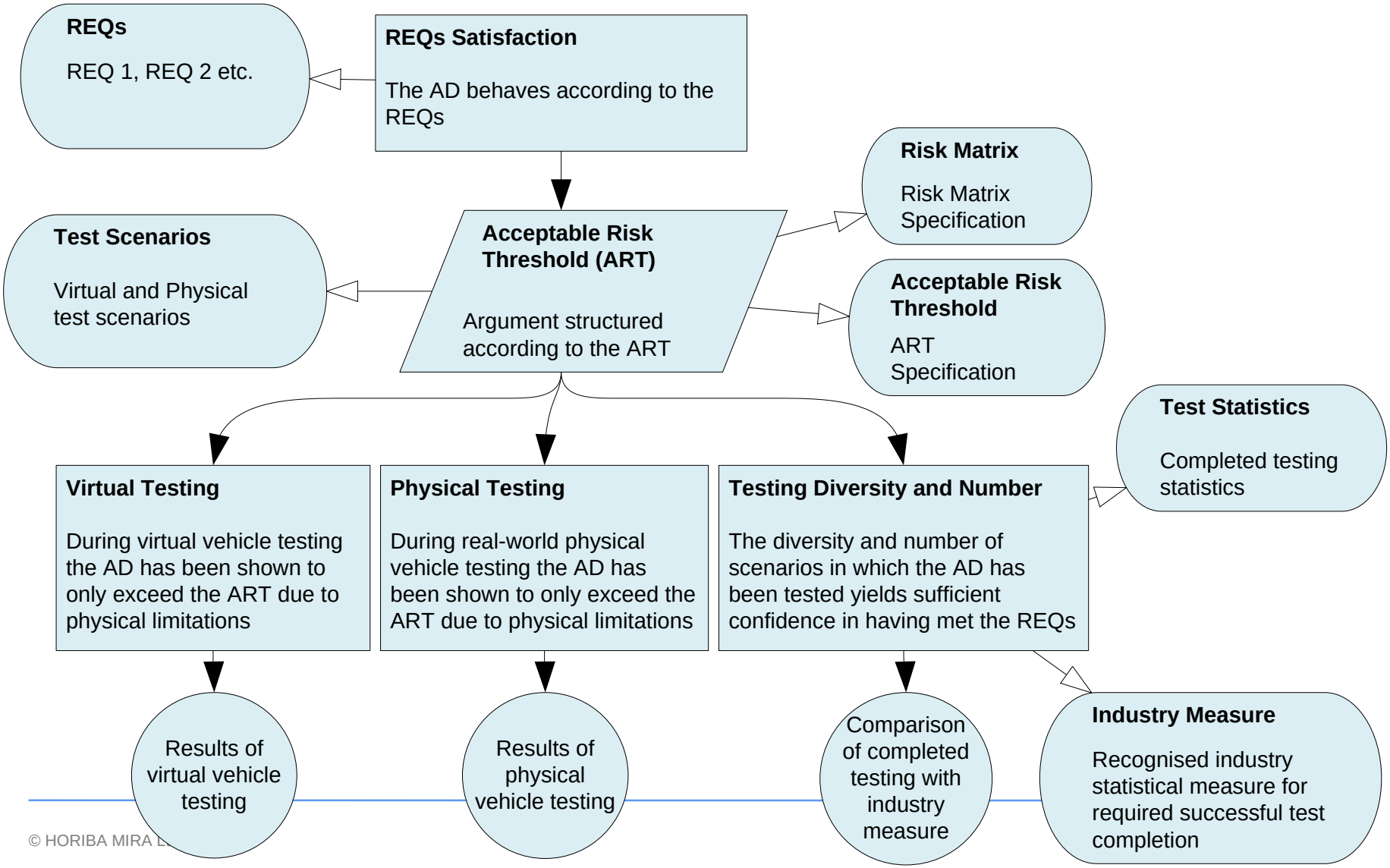


Assurance Argument Framework
Functional Safety – Intended Behaviour



Assurance Argument Framework

Functional Safety – Intended Behaviour Satisfaction



Concluding Remarks

Concluding Remarks

- Safety for autonomy is multi-faceted and challenging
- Important to be able to show structured, explicit reasoning for achievement of safety, particularly to justify residual risk
- Argument may need to be pitched at a higher level of abstraction than would be the case for a ‘conventional system’
- Dynamic safety cases may be required, but automation should not preclude thought!
- Argument likely to require philosophical and ethical reasoning as well as technical
- The devil is in the detail
- Complex problem – not claiming to have the final answer!

Contact details

John Birch
MEng CEng MIMechE

Chief Engineer, Functional Safety

Direct T: +44 (0)2476 355 415
Mobile: +44 (0)7834 158049
Email: John.Birch@horiba-mira.com

HORIBA MIRA Ltd
Watling Street,
Nuneaton, Warwickshire,
CV10 0TU, UK

T: +44 (0)24 7635 5000
F: +44 (0)24 7635 8000

www.horiba-mira.com