UK Research and Innovation

CATAPULT High Value Manufacturing

WMG THE UNIVERSITY OF WARWICK

Cross Domain Safety Assurance Framework for Automated Transport Systems

The Motivation

Moving people and goods is worth over £100 billion to the UK economy, but it comes at a cost in terms of accidents, with over 2000 deaths and over 120,000 injuries every year.

Connected and autonomous transport has the potential to make land, air and marine journeys safer, faster and more efficient, contributing to both our national health and carbon emissions goals. Additionally, the connected and autonomous transport systems' market globally is projected to be over £700 billion by 2030, so this sector could be a major driver of economic growth in the UK.

The biggest challenge to delivering the potential of autonomous transport systems is safety and consumer acceptance. Without addressing these issues across all sectors, we will not be able to unlock the potential commercial opportunity.

To maximise the benefits will require integration and collaboration between manufacturers, infrastructure, transport service providers and regulators.

The Ambition

If, as an ecosystem of stakeholders, we are serious about the safe introduction of automated transport systems (land, air or marine), we need to focus on:

- Setting high standards for safety assurance
- Not competing on safety of automated transport systems

Both these aspects will be key to consumer acceptance and their trust in automated transport technologies.

The Framework: Building Blocks

Safety assurance of automated systems for any transport domain (land, air or marine) requires three key areas of research, standards, and regulations:

- Test scenarios
- Test environment
- Safety evidence and safety argument

Test Scenarios:

A test scenario illustrates the situations an automated transport system will experience during its deployment in the real world. Understanding of these situations is key to designing a safe automated transport system.

Test scenarios will be driven by the requirements and design of the systems. These requirements will need to include defining the operating conditions and the behaviour capabilities of the autonomous transport systems. This would entail characterising the land, air and marine operating conditions using an objective and standardised approach, adapted for each domain.

Operating conditions for land would include attributes like road type, weather type, type of actors (emergency vehicles, pedestrians) etc. (as per BSI PAS 1883). Operating conditions for sea could include attributes like current strength, wind speed and direction, salinity, water depth etc. Operating conditions for air could include attributes like wind speed and direction, air density, fog etc.

Behaviour capabilities for land transport systems could include manoeuvres like turn right/ left, lane change, cut-in etc. For marine transport systems, manoeuvres could include docking, accelerating, stopping, turning etc. For air transport systems, manoeuvres could include take off, landing, climb, turn, rolls (aileron, rudder), chandelle, trimming etc.

Test environment:

A test environment is the platform in which the autonomous transport system undergoes testing. Test environments can be a combination of hardware, software, real-world infrastructure, and data. They can be wholly computer based, or a constrained real-world setting like a test track, or in an unconstrained real-world environment.

Once the test scenarios have been identified, we need such test environments to execute the test scenarios. Due to the wide variety of test scenarios and large number of combinations of parameters within each test scenario, there could potentially be thousands, millions or even billions of combinations to test. Checking all such tests manually by driving/flying/sailing is implausible, and so we will need to utilise computer simulations in some form.

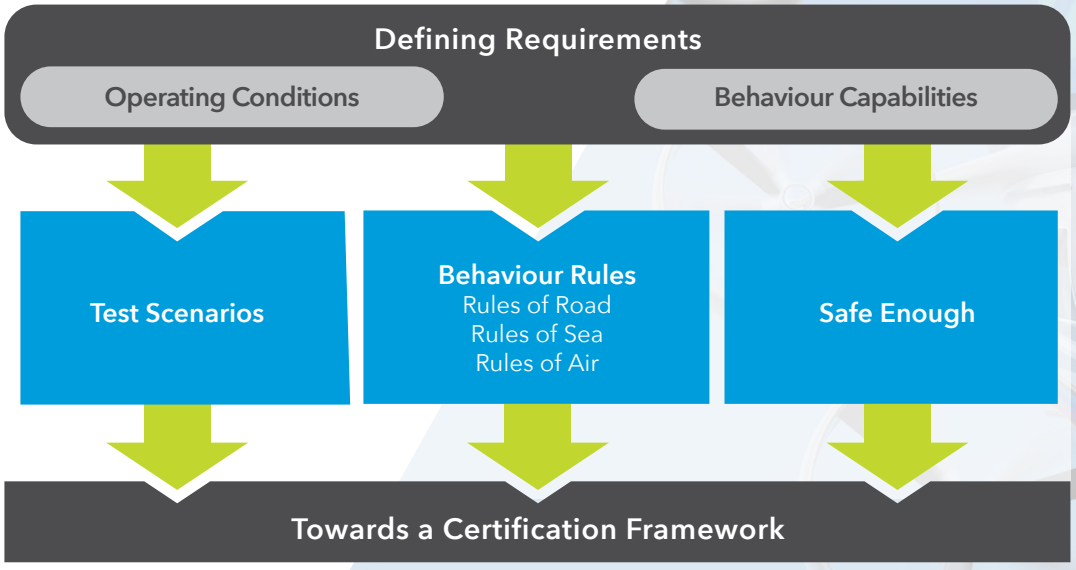
A continuum of test environments from the entirely simulated or virtual, through physical test beds, to real-world settings, will provide the range of options at a reasonable speed to ensure the safety of autonomous transport for land, air and sea. While virtual test environments offer the advantage of testing a large number of scenarios efficiently, we need to validate the virtual environment itself, i.e., ensure the virtual environment reflects the real world, to be able to trust the results of the tests within a given scenario.

Safety evidence and safety argument:

A safety argument provides the link between safety evidence and the safety claim (i.e., the system is safe to use).

Having executed the test scenarios in the test environments, we need to analyse the results and decide if they indicate that the behaviour of the system is safe. We can then use the collected evidence to create the safety argument proving that the autonomous transport system is a safe system. This will entail comparing against "defined safe behaviour" and "defined safety benchmarks". Considerable discussion around safety for automated transport systems focusses on being as good as, or better than, human driven systems on land, marine or air. Behaviour of human beings in transport systems is governed by a set of rules (e.g. rules of road (The Highway Code), rules of air (UTM/ATM) and rules of sea (COLREGs)).

However, as human beings we are exceptionally good at handling unfamiliar situations by using our intuitive pattern matching ability, which enables us to safely handle the "edge case" situations - those which bear a resemblance to situations we have experienced before, but which are not exactly the same. A computer simulation only has these links if it has been programmed to, or if it has "learnt" directly from artificial intelligence training.



The Framework: Bringing it Together

The realisation of the cross-domain safety assurance framework is underpinned by an objective characterisation of the operating conditions and the behaviour capabilities of the autonomous transport systems. Once they are defined, the relevant test scenarios for the defined operating conditions and behaviour capabilities can be identified from a centralised scenario library.

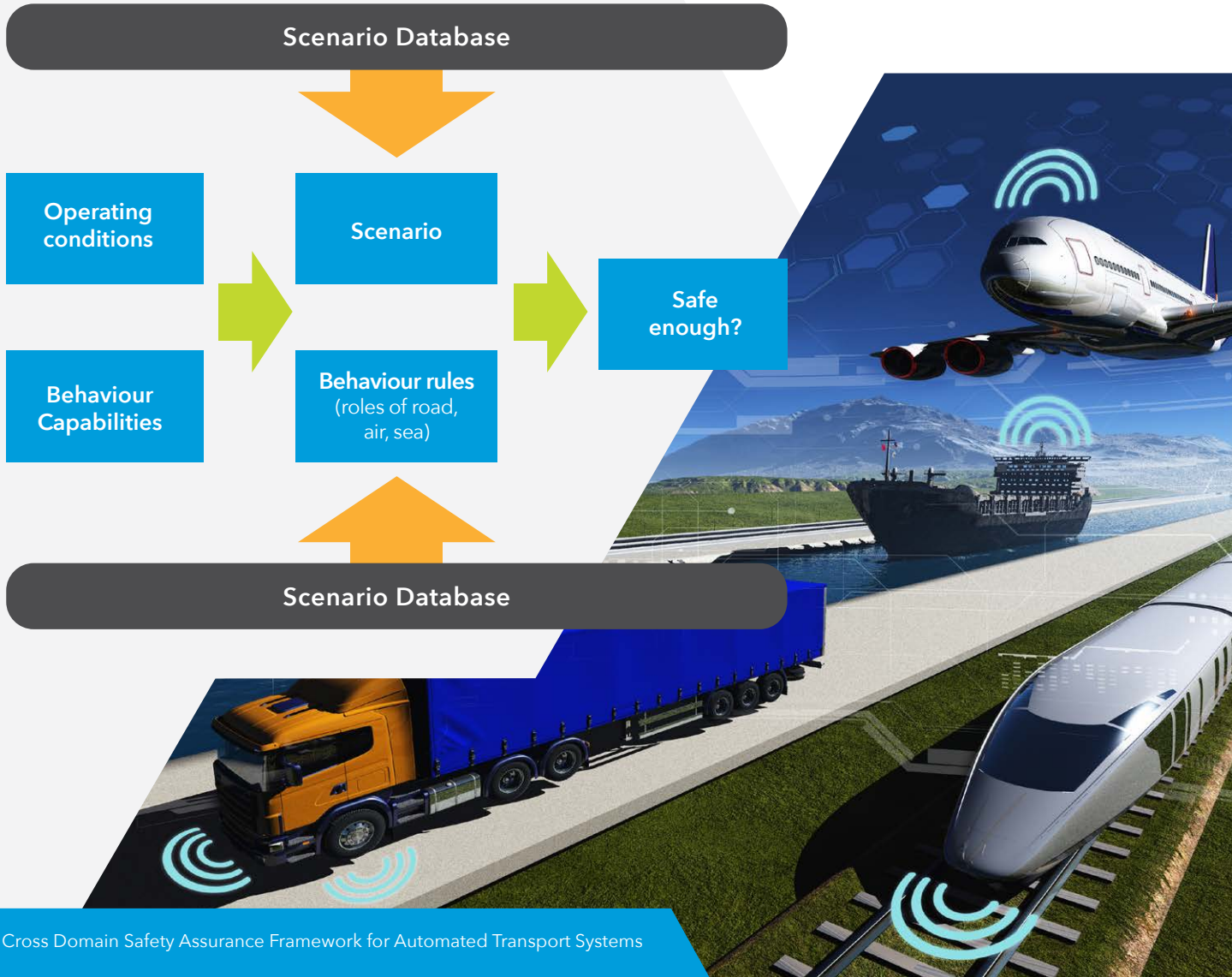
Each rule of road, air or sea will also have a relationship with the operating condition and/or behaviour capability. These rules governing our behaviour tend to prescribe us to: "do a certain behaviour *somewhere*" or to "not do a certain behaviour *somewhere*".

While the behaviour aspect of the rules has a direct relationship with the behaviour capabilities of the autonomous transport system, "*somewhere*" forms part of the operating condition for the autonomous system.

Due to this relationship between the rules of road, air and sea with operating conditions and the behaviours, we can draw a link between the identified test scenarios (from the scenario library) and the rules of land, air, and sea.

In order to make a claim for safe enough, if we can prove that for all the identified test scenarios, the autonomous transport system is compliant with the relevant rules of land, air or sea, we can make an argument for safety of the autonomous transport system.

However, taking this approach puts the onus on the coverage of test scenarios and the associated scenario library as well as the details in the rules of the road, air and sea.



The Framework: Opportunities and Benefits

Taking a cross-domain approach to safety assurance for autonomous transport systems offers various opportunities and benefits to the ecosystem. First, it enables us to learn from the strengths of individual domains. For example, the standards for defining operating conditions and behaviour competencies are relatively mature for the land domain (BSI PAS 1883, ISO 34503 etc.), as compared to those in aviation and marine.

Second, on a more practical note, the associated tools, toolchains and procedures in implementing the safety assurance framework across the land, air and marine domain could enable re-use of assets (e.g., databases, virtual test environments know-how etc.) offering value for money.

Third, it helps avoid triplication by translating learnings from one domain to another and fostering relationships across these traditionally siloed and independent domains. Thus, making research and deployment of autonomous transport systems more efficient.

Key recommendations:

The following areas of further work would support the development and adoption of a cross-domain safety assurance framework:

Accountability

- Create a government – industry body responsible for safety assurance of autonomous transport systems as a cross-domain activity

Scenarios

- Create standards and regulations on characterising the operating conditions and behaviour capabilities of the automated system
- Create a library of scenarios for use by various stakeholders including regulators

Test environment

- Enhance the National Digital Twin Programme to create a qualified Virtual Test Environment (VTE) for use by regulators in each transport domain
- Create a qualification process for VTE for use in safety assurance of automated systems

Safety evidence and argumentation

- Create a codified set of behaviour rules (rules of road, rules of sea and rules of air) to define safe and acceptable behaviour for automated transport systems
- Create a scalable safety assurance framework as a function of operating conditions and behaviour capabilities for the automated transport system

Contact:
Dr Siddartha Khastgir
Head of Verification and Validation,
Intelligent Vehicles,
WMG, University of Warwick

S.Khastgir.1@warwick.ac.uk