AUTONOMOUS VEHICLE CERTIFICATION: EATING THE ELEPHANT

Abstract: Autonomous vehicles are one of the most anticipated and exciting innovations in the world today. The 'mobility as a service' promise will revolutionise transport design, availability, density, and safety. As autonomous vehicle technology advances, how can we be confident that manufacturers are creating a product that is safe and that their emergence can be controlled without significant disruption to the existing environment? One answer is centralised performance-based regulation similar to what is defined for the aviation industry.

This submission presents a top-down framework to illustrate the perspectives of aviation stakeholders, describes their relationships as functions of integrity, and defines the current regulatory approach. When the aviation flavours are removed and replaced with autonomous vehicles, agnostic of land, sea or air, insights are gained into where updates to regulations could be considered. These include:

- An understanding of how aviation environmental integrity elements can be applied to autonomous vehicles.
- Perspective on the autonomous vehicle 'system of systems', presenting a possible framework for the grouping and validation of regulations.
- An understanding of how integrity transfers between stakeholders as the level of autonomy rises.

Authors:

Karl Morris
BSc (Mathematics, Computer Science), DipAeroEngMgmt
Associate – Systems Engineering
Beca Applied Technologies
karl.morris@beca.com

Kelly Loving
MEng (Systems Engineering)
Systems Engineer
Beca Applied Technologies
kelly.loving@beca.com

Jessica Tucker
MSc (Physics)
Senior Associate – Systems Engineering
Beca Applied Technologies
jessica.tucker@beca.com

Presenter: Jessica Tucker

INTRODUCTION

Autonomous vehicles are one of the most anticipated and exciting innovations in the world today. The 'mobility as a service' promise will revolutionise transport design, availability, density, and safety. As autonomous vehicle technology advances, safety considerations and appropriate regulation must evolve simultaneously to be confident that products are safe and that their emergence can be controlled without significant disruption to the existing environment.

In this paper we present a basis for an autonomous vehicles certification framework. This basis certification framework leverages existing concepts, structures, and functions from New Zealand aviation regulations. Aviation regulations have evolved over time in response to lessons hard-learned and are recognised as being responsible for enabling the conduct of safe and efficient air operations in New Zealand. The aviation regulations are therefore a suitable foundation for the development of an integrity and assurance framework for autonomous vehicles. The presented general autonomous vehicle certification framework is then applied to the specific case of an autonomous bus.

In the context of this paper, the term "integrity"[1] is used to indicate that a system can be relied upon to work correctly and safely. Regulations and certifications are often employed to achieve integrity in systems operating in the public space. Additionally, the term "assurance"[2] is used to express the planned and systematic actions necessary to establish confidence and evidence that a product and/or process satisfies requirements or regulations.

AVIATION INTEGRITY FRAMEWORK

Safety of life is paramount in aviation and consequently the roles and relationships between stakeholders have evolved accordingly. Early aviation was without regulation and as a consequence followed a "fly-fix-fly" path. [2] Here designs and operations were improved only after real-world failure regularly resulting in the loss of life. Over time, as lessons were learned and adopted, regulations and design controls were established to enable assurance by compliance for future products and operations. Modern techniques now use predictive analysis to show changes to aviation products and services do not adversely affect the integrity of the aviation systems operating in New Zealand.

The integrity in an aviation system of systems can be generalised into three elements: (1) aircraft, (2) operational, and (3) environmental. Integrity is achieved in the system through regulations imposed on Aircraft Manufacturers and Air Transport Operators and controlling the operational environment. Figure 1 represents how integrity exists in the context of an air transport service in New Zealand and how this is delegated to, and implemented by, stakeholders.

---

[1] Integrity [1]: Qualitative or quantitative attribute of a system or an item indicating that it can be relied upon to work correctly. It is sometimes expressed in terms of the probability of not meeting the work correctly criteria

[2] Assurance [1]: The planned and systematic actions necessary to provide adequate confidence and evidence that a product or process satisfies given requirements.

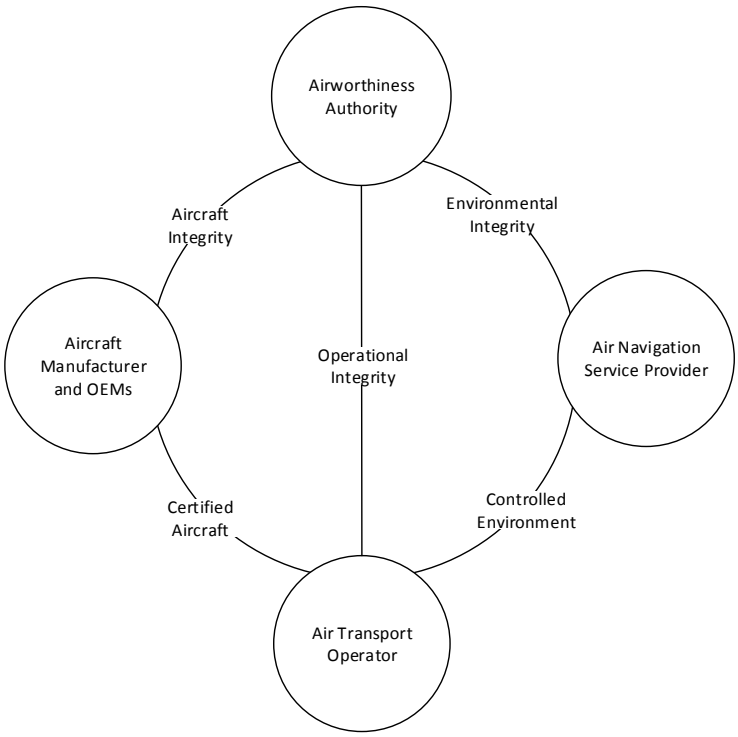

Figure 1: Aviation Integrity Framework

Airworthiness Authority

The Airworthiness Authority is accountable to the public and the New Zealand government for the safe and efficient implementation of an air transport services. The Airworthiness Authority defines integrity through the issue of regulations, and assurance is provided through engagement and audit of relevant stakeholders. The Airworthiness Authority framework is structured in the form of binding regulations, guidance material, and industry standards recognised as meeting both regulation and guidance material.

Aircraft Manufacturer and Original Equipment Manufacturer

The Aircraft Manufacturer and Original Equipment Manufacturer (OEM) design and manufacture aviation products that conform to the regulatory requirements. This conformity is achieved at all levels of product abstraction and across the development lifecycle, including type certification of the aircraft design, specification of materials, and control of aircraft manufacturing.

For example, a transport aircraft would be developed to 14 Code of Federal Regulations (CFR) Part 25, which defines requirements for the performance requirements of the final product and the design processes requirements. Product requirements define characteristics that the aircraft must exhibit. An example of a design process requirement in CFR 14 Part 25, there is an obligation to conduct a system safety assessment, where specific functions of the aircraft are developed to a level corresponding to the risk they present to operation of the vehicle and occupants. Similar regulatory requirements exist for aircraft manufacture to ensure that each aircraft is produced in accordance with the approved type design by an approved manufacturing organisation.

Air Navigation Service Provider

An Air Navigation Service Provider (ANSP) is responsible for the infrastructure and provision of

services to maintain environmental integrity. Environmental integrity is established through the provision of the following sub-functions: navigation, communications, surveillance, and air traffic management. Each of these subservices have specific regulatory requirements imposed by the Airworthiness Authority.

A Navigation Service entails the provision of fixed navigation aid infrastructure and service in order for an aircraft to determine position and routing information in all conditions. In the aviation system, this is implemented through use of ground-based navigation aids that provide a fixed reference of position as well as global navigation satellite systems (e.g. Global Positioning System).

A Communications Service enables two-way communication between aircraft or between aircraft and air traffic control. Regulations from the Airworthiness Authority prescribe operating and technical standards for communications services and associated infrastructure, including standardised RF frequencies, messages and message sets, and communication security.

A Surveillance Service provides situational awareness to air traffic control of the aircraft's position, speed, and heading. Traditionally, this was achieved through radar and transponders fitted to aircraft which communicated with ground-based receivers. The New Southern Sky program, which is currently being implemented in New Zealand, decentralises surveillance where all aircraft automatically self-reports position, speed, and heading information to air traffic control and other local aircraft.

An Air Traffic Management Service has two major sub-functions: separation provisioning and airspace traffic flow management. Separation provisioning ensures that aircraft within local airspace maintain safe operating distances from each other and other hazards. This is achieved through information obtained from filed flight plans and the surveillance service, and en route communications. Airspace traffic flow ensures efficient use of airspace capacity by directing local aircraft speed and heading. Both sub-functions interface with the aircraft via air traffic control.

Air Transport Operator

The Air Transport Operator provides a commercial service using the certified aircraft from Aircraft Manufactures within a controlled operating environment provided by the ANSP. The Airworthiness Authority imposes requirements on the individuals within the operator's organisation and on the organisation and its processes as a whole. The regulations ultimately ensure that appropriately qualified and experience people use the aircraft safety within the controlled environment and maintain it to preserve aircraft integrity.

GENERIC AUTONOMUS VEHICLE INTEGRITY FRAMEWORK

The aviation integrity framework described above contains all the elements needed for the emerging autonomous vehicles. The aviation framework is suitable as a baseline because it provides integrity over similar functions, is scalable, and has demonstrated effectiveness in the real world. A general integrity framework based on the aviation model accelerates the emergence of safe autonomous vehicle operations by leveraging accepted and standardized concepts and taxonomy. Adopting this model bypasses the expensive and hazardous "fly-fix-fly" development approach used out of necessity by early aviation regulators. Figure 2 tailors the aviation integrity framework to a Generalized Autonomous Vehicle Integrity Framework.

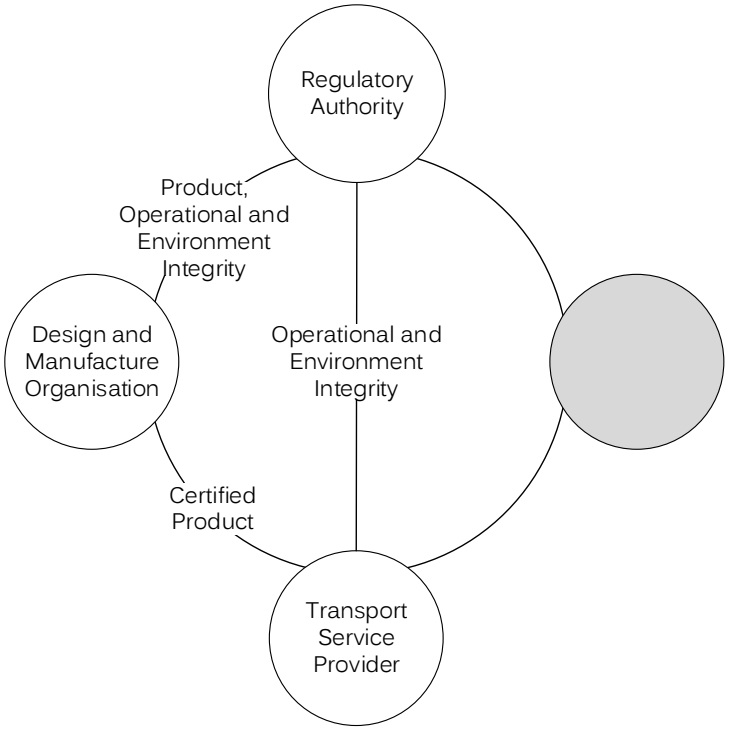

Figure 2: Generalized Autonomous Vehicle Integrity Framework

As shown, while much can be leveraged directly from the aviation regulatory model, some changes and adaptations are necessary to accommodate the unique characteristics of a general autonomous transport environment. The most significant difference between the aviation and autonomous vehicle framework is the removal of a centralised body that manages the environmental integrity. In other words, there is no role analogous to the ANSP in the new autonomous vehicle framework and associated responsibilities shift to the Design and Manufacture Organisations and Transport Service Providers.

Regulatory Authority

The Regulatory Authority will perform a role similar to the Airworthiness Authority for the operational domains (i.e. ground, maritime, air) for autonomous vehicles. Formally establishing a central Regulatory Authority body for each domain ensures control of the emergence of all aspects of autonomous vehicle products, services, and environment. This stakeholder will be accountable to the public and the government of New Zealand for the safe and efficient implementation of overall autonomous vehicle integrity within their domain. The Regulatory Authority will assure integrity through engagement, auditing, and monitoring of other stakeholders.

Autonomous Vehicle Design and Manufacture Organisations (DMO)

Similar to the Aviation Model, the DMOs for autonomous vehicles will be responsible for the integrity of the design and manufacturing of the products they deliver. Such products and constituent components will need to be certified by the Regulatory Authority as meeting regulatory requirements.

The role of the DMOs is expanded, however, to include responsibilities for ensuring environmental integrity of communication, navigation, and surveillance services, as well as separation provisioning. This shift is necessary because there is no role analogous to the ANSP in the general

autonomous vehicle integrity framework. Additionally, because a driver is no longer present in autonomous operations, responsibility for primary control of the vehicle shifts to the DMOs to implement a similar function in their product. In domain dependent situations the integrity sub-function of traffic flow management would be managed collaboratively by Transport Service Provider, or in decentralised cases, to the DMOs.

Transport Service Provider (TSP)

In the generic autonomous vehicle framework, the role of the TSP is diminished compared to the previously discussed role of an Air Transport Operator. This is primarily due to the integrity requirements of primary vehicle control are passed to the DMOs. The TSP would remain responsible for maintenance of the vehicle to ensure that vehicle integrity is maintained throughout its service life and for those support operations such as fuelling and passenger control. Again, in domain dependent situations, the integrity sub-function of traffic flow management would be managed collaboratively by Transport Service Provider, or in decentralised cases to the DMOs.

Responsibility Transfer Summary

Table 1 summarises each integrity sub-function and which stakeholder responsibility under both the aviation and autonomous vehicle integrity frameworks.

Integrity Sub-function	Aviation	Autonomous Vehicle
Primary Control	ATO	DMO
Maintenance	ATO	TSP
Service Operation	ATO	TSP
Design	Manufacturer	DMO
Manufacturing	Manufacturer	DMO
Communication	ANSP	DMO
Navigation	ANSP	DMO
Surveillance	ANSP	DMO
Separation Provisioning	ANSP	DMO
Traffic Flow Management	ANSP	Domain and architecture dependent

Table 1: Responsibility Transfer Summary

APPLICATION OF INTEGRITY FRAMEWORK TO AUTONOMOUS BUS

In this section, we are applying the generalised model to a specific example: an autonomous bus used in public transit. We will describe the stakeholders and how the integrity of the framework is applied.

Stakeholders

The Ministry of Transport would establish and delegate the role of Regulatory Authority. This Regulatory Authority and would establish the regulations and guidance used to establish product integrity, operational integrity, and environmental integrity, with input from both DMOs and

Transport Service Providers. This Regulatory Authority would be responsible for certifying products and service providers as suitable for operation in public spaces. DMOs and TSP would develop products and services in accordance with these governing regulation and would compile evidence and artefacts to enable certification by the Regulatory Authority.

Integrity

Regulations already exist governing the conventional aspects of bus design and certification. New regulations are required to address the autonomous aspects introduced with the removal of human driver controls. For example, with the removal of a human driver to control a vehicle (Primary Control) while navigating along a service route (Navigation), making route adjustments for traffic flow (Traffic Flow Management), and maintaining a safe distance from other vehicles (Separation Provisioning), the autonomous vehicle design must employ mechanisms to provide these sub-functions to ensure safe operation in a public space. Figure 3 describes how integrity sub-functions in Table 2 would be introduced to design regulations and relationships between regulation domains to address the new regulations.

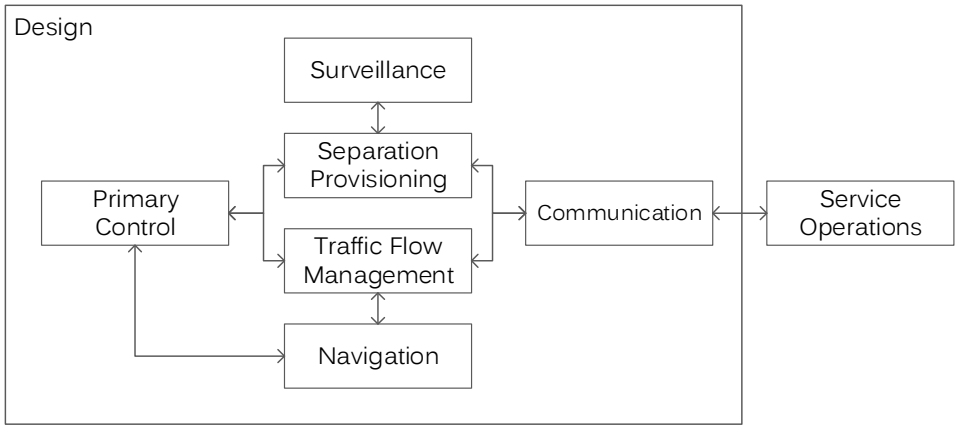

Figure 3: Autonomous Vehicle Sub-Function Block Diagram

Table 2 provides a notional regulatory requirement for each integrity sub-function and identifies a possible stakeholder who would be responsible for demonstrating conformance to regulation.

Integrity Sub-Function	Notional Regulation Description for Autonomous Bus	Stakeholder
Primary Control	Regulations to ensure that design of systems and equipment implementing primary control of the vehicle during operation will not result in an unsafe act or violation of road code.	DMO
Maintenance	Regulations to ensure that vehicle remains roadworthy over operational lifetime	TSP
Service Operation	Regulations for safety of occupants and to prevent interference with primary control	TSP

Integrity Sub-Function	Notional Regulation Description for Autonomous Bus	Stakeholder
Design	Regulations to establish roadworthiness requirements for a bus and for the organisations conducting vehicle design. These regulations are extant for elements of conventional bus design.	DMO
Manufacturing	Regulations to establish that all buses produced implement the certified design and for organisations	DMO
Communication	Regulations for secure communication with the TSP and between autonomous vehicles operating in a local area	DMO
Navigation	Regulations to establish sensory input requirements for the bus to determine its position, speed, and heading	DMO
Surveillance	Regulations to establish sensory input requirements for bus situational awareness of objects in its vicinity	DMO
Separation Provisioning	Regulations to standardize and control distance between the bus and potential hazards	DMO
Traffic Flow Management	Regulations governing how buses make routing decisions based on traffic flows and city planning considerations	DMO

Table 2: Overview of Integrity Sub-functions and Notional Regulations for an Autonomous Bus

CONCLUSIONS AND RECOMMENDATIONS

We have presented a generalized regulatory model for autonomous vehicles drawn from the existing aviation regulation framework in place today. Further, we have summarized the types of regulations required and identified responsible stakeholders for the specific case of an autonomous bus. We recommend that this new generalized autonomous vehicle regulation framework be applied to near-term emerging deployment of autonomous vehicles. Careful analysis of extant regulations for aviation and automotive integrity, drawn from lessons hard-learned in these domains, will accelerate fielding of autonomous vehicles in New Zealand.

REFERENCES

1. SAE Aerospace, December 2010, *Aerospace Recommended Practice SAE/ARP 4754-A Guidelines for the Development of Civil Aircraft and Systems*, SAE Aerospace

2. ROLAND, H.E and MORIARTY, B. (1990). *System Safety Engineering and Management, Second Edition*, Wiley, USA