Dedicated to innovation in aerospace

NLR-CR-2017-461 | December 2017

Introducing automation in aviation

Lessons learned for self-driving vehicles

CUSTOMER: Ministry of Infrastructure and Water Management

NLR – Netherlands Aerospace Centre

Netherlands Aerospace Centre

NLR is a leading international research centre for aerospace. Bolstered by its multidisciplinary expertise and unrivalled research facilities, NLR provides innovative and integral solutions for the complex challenges in the aerospace sector.

NLR's activities span the full spectrum of Research Development Test & Evaluation (RDT & E). Given NLR's specialist knowledge and facilities, companies turn to NLR for validation, verification, qualification, simulation and evaluation. NLR thereby bridges the gap between research and practical applications, while working for both government and industry at home and abroad.

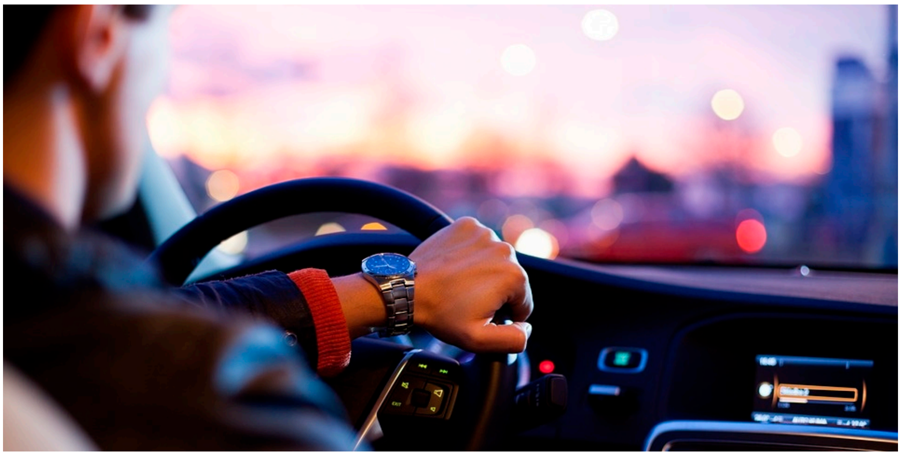
NLR stands for practical and innovative solutions, technical expertise and a long-term design vision. This allows NLR's cutting edge technology to find its way into successful aerospace programs of OEMs, including Airbus, Embraer and Pilatus. NLR contributes to (military) programs, such as ESA's IXV re-entry vehicle, the F-35, the Apache helicopter, and European programs, including SESAR and Clean Sky 2.

Founded in 1919, and employing some 650 people, NLR achieved a turnover of 71 million euros in 2016, of which three-quarters derived from contract research, and the remaining from government funds.

For more information visit: **www.nlr.nl**

Introducing automation in aviation

Lessons learned for self-driving vehicles



REPORT NUMBER
NLR-CR-2017-461

AUTHOR(S)
R.J. Roosien
T.M. van Birgelen

REPORT CLASSIFICATION
UNCLASSIFIED

DATE
December 2017

KNOWLEDGE AREA(S)
Safety

DESCRIPTOR(S)
Self-Driving
Automated Transport
Safety Methods
Safety Regulation

Problem area

Current compliance-based regulations for road vehicles are based around the core assumption of a human driver controlling the vehicle. Self-driving vehicles challenge this core assumption. Existing rules and regulations were not designed for this new type of vehicles and are therefore not a good fit. This gap may slow down the development of innovative and commercially viable products and services in The Netherlands and in Europe.

Description of work

The Self-Driving Vehicles group (*projectgroep zelf-rijdende auto*, ZRA) of the Ministry of Infrastructure and Water Management assigned the Netherlands Aerospace Centre NLR to transfer the lessons learned in dealing with automation in aerospace to stakeholders in the road transport system.

For this NLR organised an interactive work session on October 11th 2017 for 10 different stakeholders. The lessons focussed on how to view the total transport system as a whole, how to collaborate with stakeholders and how to set joint goals that will lead to an overall safe system.

Results and conclusions

Aviation has seen a steady flow of new automation from the outset. Its history provides valuable lessons on how (not) to handle new automation.

The work session identified a need for a performance-based safety assessment methodology for self-driving vehicles. The *Total System Model* as used in the work session provides a template that can be used to develop performance based methodology for automated vehicles up to SAE level 4 in a relatively short amount of time. More information on the autonomy levels as defined by the Society of Automotive Engineers (SAE) can be found in Appendix B.1.

In order to develop the safety case for an operation including automated vehicles up to level 4, the Total System Model can (a.) assess the safety of self-driving vehicles within its operational context and (b.) provide a platform that allows stakeholders to develop new operational use cases together. This would allow for the development of use cases that actually create value to stakeholders.

Applicability

The findings of this project are applicable to the safety assessment, certification and regulatory framework of self-driving vehicles up to and including SAE level 4.

Dedicated to innovation in aerospace

NLR-CR-2017-461 | December 2017

Introducing automation in aviation

Lessons learned for self-driving vehicles

CUSTOMER: Ministry of Infrastructure and Water Management

AUTHOR(S):

R.J. Roosien	NLR
T.M. van Birgelen	NLR

NLR - Netherlands Aerospace Centre

No part of this report may be reproduced and/or disclosed, in any form or by any means without the prior written permission of the owner.

CUSTOMER	**Ministry of Infrastructure and Water Management**
CONTRACT NUMBER	**1156113**
OWNER	**Ministry of Infrastructure and Water Management**
DIVISION NLR	**Aerospace Operations**
DISTRIBUTION	**Limited**
CLASSIFICATION OF TITLE	**UNCLASSIFIED**

APPROVED BY :		
AUTHOR	**REVIEWER**	**MANAGING DEPARTMENT**
R.J. Roosien	H. van Dijk	A. Rutten
DATE 1 8 1 2 1 7	DATE 1 8 1 2 1 7	DATE 1 8 1 2 1 7

Contents

E19 E25
Ring Rotterdam (noord)
Den Haag
Hoek van Holland
Havens 200-1000
A20
7
70
70
E19
Ring Rotterdam (oost)
Dordrecht
Breda
Andere Havens
A16
6
90
90
50

Abbreviations

ACRONYM	DESCRIPTION
CBR	Centraal Bureau voor de Rijvaardigheid
EASA	European Aviation Safety Agency
ICAO	International Civil Aviation Organisation
IenW	Ministry of Infrastructure and Water Management
NLR	Netherlands Aerospace Centre
RDW	Rijksdienst Wegverkeer
RWS	Rijkswaterstaat
SAE	Society of Automotive Engineers
ZRA	(Projectgroep) Zelf-Rijdende Auto

This page is intentionally left blank.

1 Introduction

To all who participated in this morning's rush hour, rejoice. Driving as we know it is about to change. Self-driving cars are the talk of town and their promise is mind blowing. Automated driving promises greater productivity for the driver, increased safety, higher traffic capacity, greener transportation and social inclusion of persons with reduced mobility. No wonder everybody is excited! Today the manufacturer that is NOT involved with automated driving systems is the exception to the rule: everybody is doing it. The sector is developing sophisticated automated driving aids, testing features that will let you let go of the wheel entirely, and wetting the consumer's appetite for the things to come.

How to proceed? Self-driving vehicles need roads and rules to function. At the moment there are no rules that are fit for these new vehicles, nor are there methods to adequately assess the advanced automation in self-driving vehicles. Road authorities and regulators prepare for these new vehicles. But how do you prepare for a change that is so fundamental?

The Self-Driving Vehicles group (*projectgroep zelf-rijdende auto*, ZRA) is a task force of the Dutch Ministry of Infrastructure and Water Management (*Ministerie van Infrastructuur en Waterstaat*, IenW) and includes members of the ministry, the Netherlands Vehicle Authority (*Rijksdienst Wegverkeer*, RDW), and Rijkswaterstaat (RWS). Together, the group is building a knowledgebase for the Dutch government to safely introduce self-driving vehicles on the Dutch roads. All knowledge is then compiled in the so-called *Knowledge Agenda Automated Driving*[1]. ZRA assigned the Netherlands Aerospace Centre NLR to transfer the lessons learned in dealing with automation in aerospace to stakeholders in the road transport system. For this NLR organised an interactive work session on October 11th 2017 for 10 different stakeholders. The lessons focussed on how to view the total transport system as a whole, how to collaborate with stakeholders and how to set joint goals that will lead to an overall safe system. The goal was not to copy from aviation, but to get inspired by the methodologies used.

This document both captures and elaborates on the work session. Section 2 kicks off with a description of the approach to this project and the set-up of the work session. The remainder of the document illustrates the results of this work session. Section 3 provides an overview of the introduction of automation in aviation. Section 4 introduces a fundamental concept to deal with (automation) disruption via an actual case. Section 5 applies the concept introduced in the previous section to a fictive highway cruise scenario. Section 6 concludes on the lessons learned from the work session.

[1] http://knowledgeagenda.connekt.nl/engels/

2 Approach

From the outset, aviation has seen a gradual transfer of control from human operator to automated systems. Moreover, it managed to perform this transformation while improving the levels of safety. The main objective of this project was to transfer the lessons learned to stakeholders that are relevant to the safety of self-driving vehicles. Given the complexity of the problem and the vast pool of available experience, we wanted to involve road transport stakeholders to determine what elements are most relevant. For this, NLR organised a full day workshop with stakeholders on October 11th 2017 at NLR in Amsterdam.

2.1 Attendees

Road transport is a complex system consisting of many parts. The safety of the system is only guaranteed because all parts fit together. If you make a change to the system as fundamental as automating human driving tasks, many stakeholders will be affected. To cover the full spectrum, we invited representatives of rule makers, oversight authorities and users & industry that are involved with the driver, vehicle, and infrastructure. The table below shows the parties involved. Parties within brackets were involved, but could not attend the session. The list of attendees can be found in Appendix A.2.

Table 1: involved stakeholders for work session

	Rule Maker	Oversight	Users & Industry	Other stakeholders
Driver	Ministry of IenW	CBR	ANWB	SWOV, Provincie Noord-Holland, 380 on behalf of Noord Nederland
Vehicle	Ministry of IenW	RDW	(2Getthere)	
Infrastructure	Ministry of IenW	RWS	CROW, Dura Vermeer, (RHK-DHV)	

2.2 Set-up

Prior to the work session, NLR sent out an online questionnaire (Appendix A.1) to adjust the scope of the work session. The questionnaire confirmed that self-driving vehicles were relevant to all invited stakeholders. 'Safety' and 'collaboration' were mentioned most as being the most important factors to discuss. Based on discussion with the Ministry and the results of the questionnaire, the scope of the session was limited to the operational safety of self-driving vehicles with emphasis on (1) the interaction between control, vehicle and infrastructure and (2) collaboration between stakeholders.

The work session was divided into two parts. In the morning, we explained how automation is introduced in aviation and what lessons can be learned. Furthermore we discussed the differences between compliance-based regulation and performance-based regulation. Using the example of a recent research project, the *Total System* design method was introduced as a tool to address the safety and operational design domain of a new, disruptive operation.

The afternoon session was devoted to applying the Total System design method to a fictive highway-cruise scenario. The goal was to drive from the The Hague to Schiphol via the *A4 highway* with uninterrupted automated driving after transition of control until the highway exit.

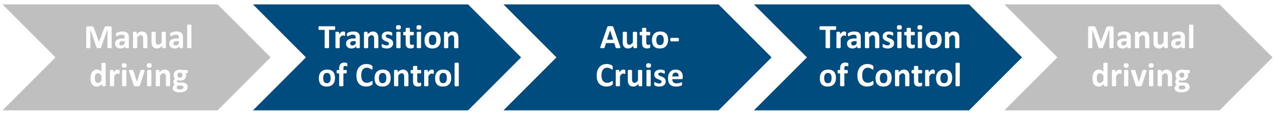


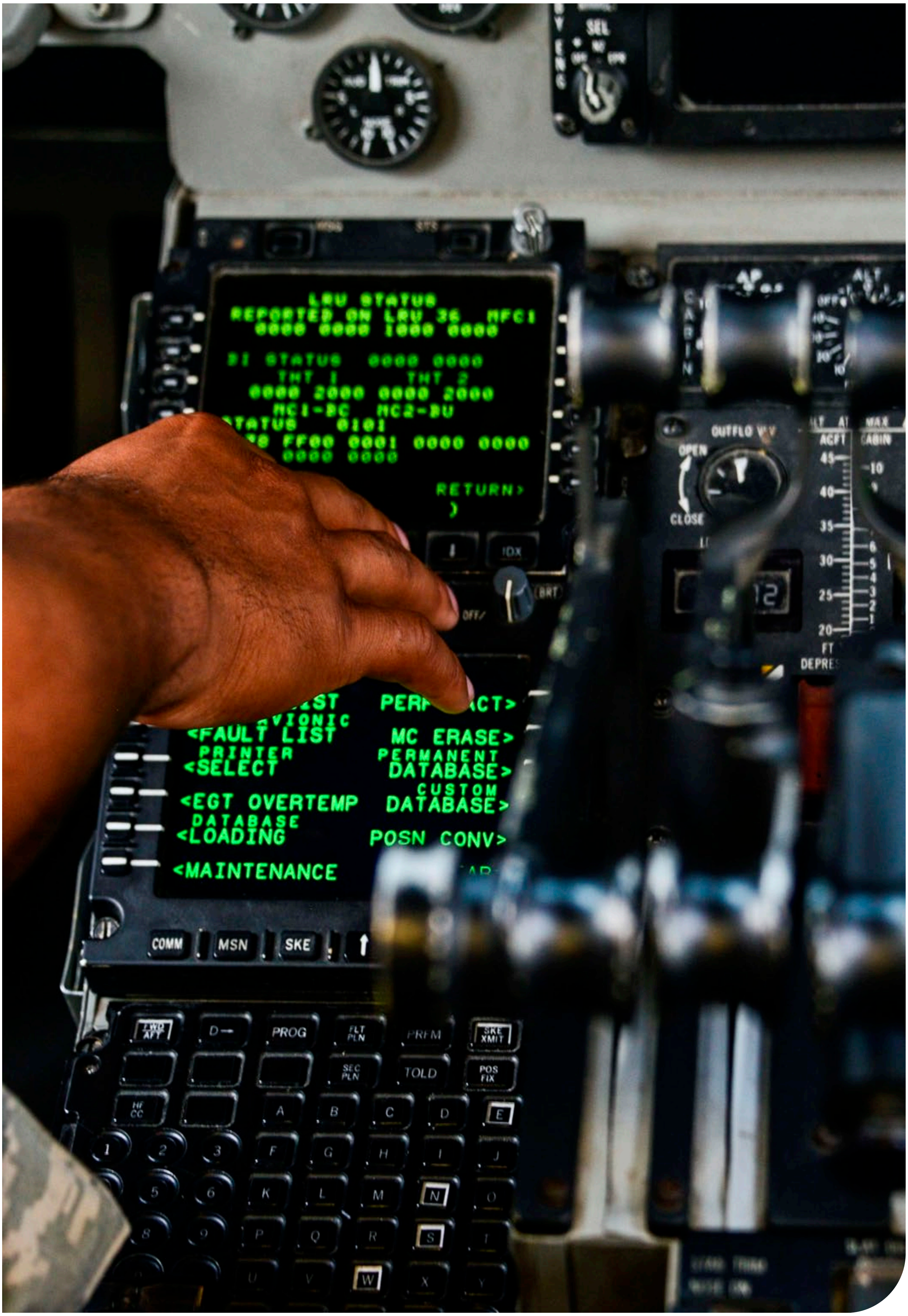
Figure 1: blue indicates the driving phases within scope of the case study

2.3 Results

All attendees to the work session agree that exploitation of self-driving vehicles is still in its infancy. In order to develop the safety case for an operation including automated vehicles up to level 4, the Total System design method can (a.) assess the safety of self-driving vehicles within its operational context and (b.) provide a platform that allows stakeholders to develop new operational use cases together. This would allow for the development of use cases that actually create value to stakeholders.

All slides of the presentation including comments and observations can be found in Appendix A.2.

Figure 2: Impression of October 11


LRU STATUS
REPORTED ON LRU 36 MFC1
0000 0000 1000 0000
BI STATUS 0000 0000
THT 1 THT 2
0000 2000 0000 2000
MC1-PC MC2-BU
RETURN>
<FAULT LIST
PRINTER
<SELECT
MC ERASE>
PERMANENT
DATABASE>
CUSTOM
DATABASE>
<EGT OVERTEMP
DATABASE
<LOADING
POSN CONV>
<MAINTENANCE
COMM
MSN
SKE
PROG
TOLD
OUTFLO V/V
OPEN
CLOSE

3 Introducing automation in aircraft

This section provides a very short historic overview of the introduction of automation in aviation. For a more complete overview of automation in aviation, please refer to the previous publication *Human Factors in de luchtvaart* by De Reus, Vermaat and Van Dijk (NLR-CR-2016-263) (zie knowledge agenda + link). The section puts special emphasis on the safety issues that emerged and how they were handled by legislation. The section closes off with an outlook on future automation.

3.1 Historic overview

From the first auto-pilot in the thirties to fully automated drones the present, aviation has seen new automation from the outset to (1) widen the *performance envelope* or *operational design domain*, (2) reduce the likelihood of errors, (3) reduce the number of operators.

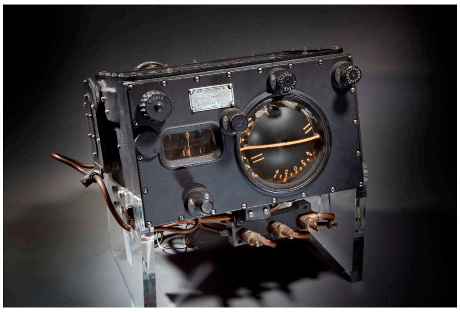


Figure 3: Sperry auto-pilot

Pioneering days
In the early days of aviation, flying was a manual affair. The pilot was using visual landmarks to navigate while controlling heading, speed and altitude. Especially during cross-country flights this was very tiresome. The Sperry Corporation developed the first gyroscopic auto-pilot in 1912, two years prior to the start of the Great War. It was the military's need to prevent fatigue of fighter pilots during their bombing runs that spurred the development of *auto-straight-and-level*. By the 1930's this developed into an auto-pilot that automatically maintained the heading and altitude of the aircraft. Today, most auto-pilots still have an *altitude-hold* mode.

The jet age
Again, a military development found a civilian application in *auto-land*. In the 1960s, Europe's airports were severely constrained by poor visibility conditions. Fog or smog could close down an airport completely. Auto-land could automatically position the aircraft on its glide path towards the runway with high accuracy irrespective of weather conditions. Thus auto-land reduced pilot workload and greatly improved the availability of airports.

Figure 4: Poor visibility conditions during landing

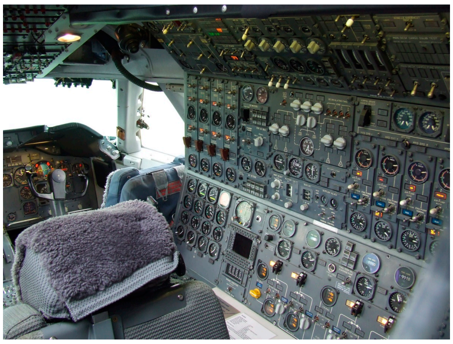


Figure 5: Working position of the on-board engineer in a Boeing 747-200

Seventies system management
The seventies brought system management to on-board systems such as engine control. This had such a positive effect on the work load of the flight crew that the on-board engineer became redundant.

Digital eighties fly-by-wire
In the eighties, replacing analogue mechanical flight controls with digital fiberglass (*fly-by-wire*) not only reduced weight, but also proved to be more reliable. It also allowed flight computers to alter the flight behaviour of the aircraft. Thus an aircraft company could let all their aircraft be flown in the same manner reducing the cost for pilot training.

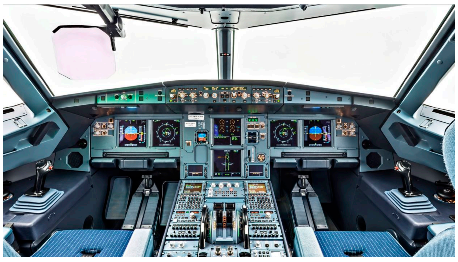


Figure 6: Cockpit of an Airbus A320

Figure 7: Level-of-sight operation of a drone

2000 to present day
Navigation relied for a large part on ground-based radio beacons and on-board receivers. Detailed specification requirements and standards guaranteed a desired level of accuracy. Given this level of accuracy, minimum separation standards between aircraft ensured a desirable level of safety. GPS navigation theoretically allowed the aircraft to navigate without the need for expensive ground-based beacons. However, its accuracy is a lot less predictable. At first this made GPS extremely difficult to certify in aviation. Only after it became possible to automatically monitor the performance of the positioning system and adjust separation accordingly (*Required Navigation Performance*, RNAV) did it became feasible to safely rely on GPS for navigation.

Although last century saw automated how pilots fly the aircraft, how they navigate and how they operate on-board systems, pilots always remained ultimately responsible. Pilots are always *in the loop*. Decision making for flight planning is not automated either, but computers do help optimise routes. Modern airliners are operated by two piloted who act in unison. Each pilot has specific tasks such as flying the aircraft or operating the communication radio. During critical flight phases, pilots can check and correct each other, decreasing the likelihood of errors.

The current maximum level of automation in aviation, including drones, is comparable to level 3 as defined by the Society of Automotive Engineers (SAE). Functions are automated, but the human operator remains the back-up in case of automation failure. If you are unfamiliar with the SAE autonomy levels, please refer to Appendix B.1.

3.2 Safety

Aviation takes a careful, conservative approach towards new systems. Due to the nature of flight, unforeseen failures can have a catastrophic outcome. One cannot simply pull-over and stop in the air. Before a new system can be used in operation a manufacturer faces a lengthy certification process in which the system is extensively tested. Even then, new automation will give rise to new, unexpected failures. Perhaps surprisingly, not all have to do with technical failure.

Automation can work differently as intended and fail:

- Cause confusion about the intention of the automation to the monitoring pilot. For example: the pilot expects auto-pilot behaviour that belongs to a different auto-pilot mode (mode confusion) or is unsure about systems settings with non-moving throttles and non-moving sidesticks.
- Unexpected behaviour when the system encounters conditions not foreseen in the design of the system.
- Different flight behaviour after a technical failure, for instance in case of fly-by-wire

There are also cases in which the automation works as intended, but still fails:

- Automation can make the job of operators less demanding in ways that it undermines professionalism.

Automation transfers tasks from humans to automation, yet Human Factors issues are still causing automation failure. Currently there is no universal method to design interfaces that guarantee safe human-machine interaction. Instead, manufactures need to demonstrate their operating logic as part of the certification process. For this reason the aviation regulator EASA (European Aviation Safety Agency) prefers small steps over radical change when certifying new automation in order to control the risk of automation failure.

3.3 Certification and regulation

Aviation regulation covers the entire air transport systems. The table below gives an overview. In aviation, the International Civil Aviation Organisation (ICAO) and EASA ensure the cohesion and consistency of this framework. Above regulation is almost universally adopted. This ensures that an aircraft certified in the US, flying with an Asian crew should have little difficulty landing in Europe.

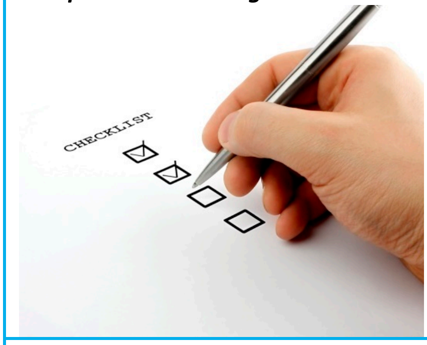
Component	**Regulation**
Airworthiness of the aircraft	EASA Certification Specifications
Aircraft maintenance	EASA Continuing Airworthiness
Aircraft operations	EASA Air Operations Regulations
Pilot training	EASA Flight Crew Licensing
Routes and traffic rules	ICAO PANS ATM, doc 4444, Annex 2
Air traffic control	ICAO Annex 11
Navigation	ICAO Annex 11
Airports	ICAO Annex 14

In general there are two sets of regulation.

Compliance-based regulations prescribe (part of) a solution. A significant part of this type of regulations is based on learning from accidents. To accommodate new developments with different solutions, this type of regulations must be adapted. This is a lengthy process as it requires adaptation of the law. This limits the innovations pace.

Performance-based regulations do not prescribe solutions, but requires a certain performance from a solution. To accommodate new developments, this type of regulations does not need to be adapted. For certification developers need to demonstrate that their ‘system’ (in the broadest sense) is safe and in this process can set their own pace. Performance-based regulations are available for smaller categories of aircraft, in order to stimulate innovation in this segment of the market.

Table 2: Compliance-based regulation versus performance-based regulation

	Pro	**Con**
Compliance based regulation 	Easy to enforce, predictable	Prescribes technical solution, not applicable to unforeseen solutions
Performance based regulation MODE SPLIT RESET START STOP ACCUSPLIT 10:5323 MIN. SEC. 1/100 PRO SURVIVOR 601X 3V.1	Output driven, allows for different technical solutions and means of compliance	Requires fundamental insight in technical system, more difficult to set-up

3.4 Future developments

As stated above, aviation takes a careful approach towards introducing new automation especially for manned flight. With unmanned flight (drones), developments move at a faster pace. Here we will see unmanned operation in a predictable domain (equivalent to SAE level 4). First this will be automated operations beyond line of sight with small drones used for surveillance and transporting small payloads. In a next stage, cargo aircraft might be converted into unmanned cargo drones. Only after manufacturers and regulators gain experience with these aircraft and the general public becomes familiar with unmanned flight, will fully automated passenger aircraft be considered.

In parallel unmanned military drones will make a transition to a non-predictable operational domain (equivalent to SAE level 5) using Machine Learning Artificial Intelligence. This requires adaptation of the current regulations.

ROCKWELL FIELD
ARMY AIR SERVICE

4 Total System

The current (high) level of safety on the road and in the air is built upon a complex set of standards, rules and institutions that have been built and improved over more than a hundred years. And all these years all rules, regulations, road safety standards and oversight bodies were designed around the assumption that there is a human operator controlling the vehicle. What will happen if the first generation of highly automated vehicles will lead to an unexpected increase in fatalities and a decrease in capacity? Replacing the human operator by an automated system is a paradigm shift that requires re-evaluation of all components of the transportation system. This is difficult as you can no longer rely on previous experience.

The *Total System* design methodology is a design method developed in aviation that can (a.) assess the safety of a vehicle within its operational context and (b.) provide a platform to develop the operational design domain. It provides a systematic tool to define fundamental aspects as: ‘what will you do?’, ‘under what conditions will you operate?’, ‘what will you use?’, and ‘how will you control the system?’.

For this, the methodology progresses through a number of steps:

1. Set the objective of the operation
2. Define the scope and content of the technical system
3. Determine the required (technical) functions of the system
4. Describe the operational environment
5. Describe the operational concept
6. Describe how the system will be monitored and controlled
7. Define the transition at the beginning and endpoint of the operation

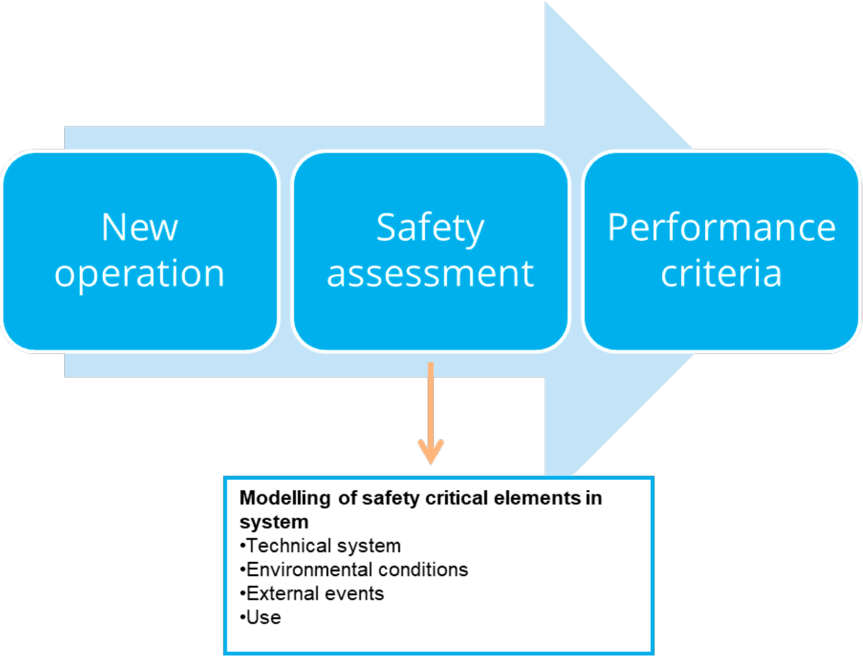


Figure 8: Total System design methodology as part of the safety assessment

Let’s use an example of recent research project that NLR participated in to illustrate the use of the methodology.

4.1 An example operation

Operational margins in aviation are notoriously slim. Therefore airlines want aircraft to be as light as possible in order to minimise cost. As a result aircraft are refuelled with a carefully calculated amount of fuel before each departure. Air-to-air refuelling has been used in the air force to extend the endurance of military aircraft. If this could be applied to civilian aircraft it would require airliners to carry less fuel and could lead to a significant reduction of CO_2 emissions. In this section it is described how this new type of (automated) operation can be developed and how it could be certified using the Total System methodology.

Figure 9: Air-to-air refuelling as case to demonstrate the Total System design method

For air-to-air refuelling the aircraft in need of fuel makes contact with the refuelling boom of the tanker aircraft and gets refuelled. The procedure follows a predefined pattern. However, it is a potentially very dangerous operation because disturbances such as technical failures, environmental conditions and external events can all lead to collisions. In order to increase the safety of air-to-air refuelling, the process could be automatic.

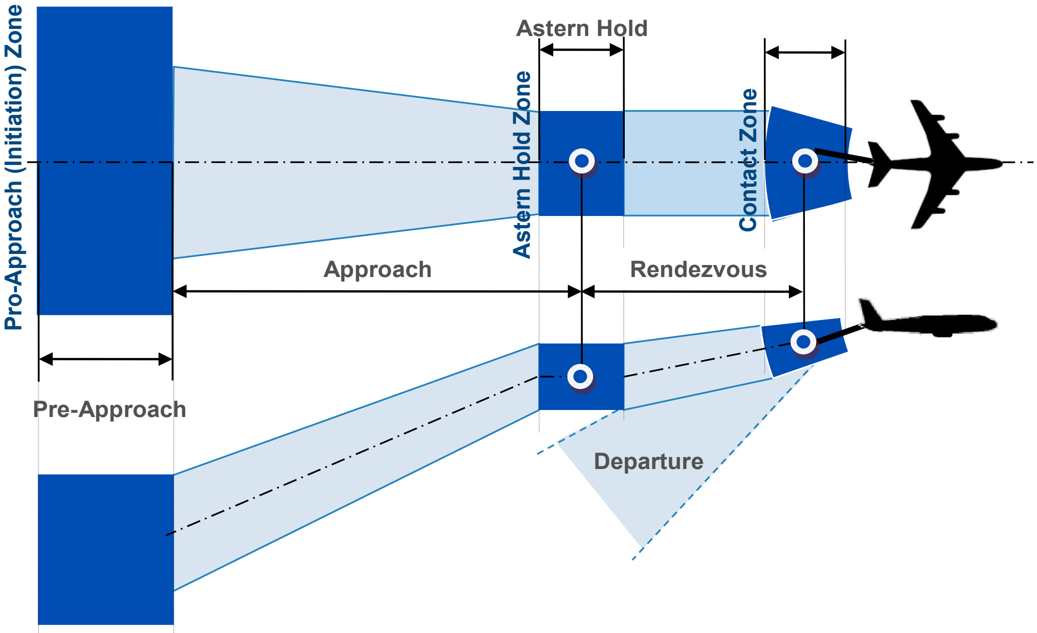


Figure 10: Approach pattern of to-be-refuelled airliner towards tanker aircraft

4.2 Applying the methodology

Air-to-air refuelling of airliners is a new type of operation with new technical systems and new functions. Potentially the procedure is very dangerous. The Total System design method identifies the required functions of the technical systems and their performance and safety requirements. In addition, it helps develop procedures to deal with disturbances. The method covers the operation, the technical systems required to perform the operation, and the decisions to be taken to perform the operation, in all foreseen circumstances. For all the above, it must be demonstrated that these are complete and correct.

Technical system and functions

The method starts with the performance of the functions of technical systems that are required to perform the nominal operation in certain environmental conditions. A function can be anything that the system needs to be capable of to fulfil its objective, e.g. locate the refuelling boom. Subsequently additional functions and their performance that are necessary to cope with technical failures, extreme environmental conditions and external events, are identified.

Requirements

It should be noted that the feasible operations are determined by the available performance of the functions. Vice versa, the required functions and their performance are determined by the desired operations. In combination with a required safety level, the definition of the desired operations leads to the safety requirements of the functions. This is usually described in terms of availability and integrity. In this way the safety and performance requirements of the functions of the technical systems are determined. Although the approach is systematic, hazard identification and risk tolerability remains a subjective task that relies on the judgement of specialist.

As illustration, let’s look at the safety and performance requirements for a relative-position determination system of an air-to-air refuelling system.

Requirement	Criteria
Performance requirement	The probability of a collision because of insufficient relative position determination accuracy, when the turbulence level is within certain limits, must be **smaller than 10^{-9} per flight hour**.
Safety requirement	The minimum allowed relative position between the two aircraft must be achieved with a probability of **at least 1 - 10^{-9} per flight hour**.

Human Factors

The identified functions and their safety and performance requirements form the starting point for the technical developers. When all circumstances that can occur are known beforehand, the use of the functions for the nominal operation as well as in case of technical failures, extreme environmental conditions and external events, can be exactly specified by a model of the operation. The model of the operations forms the specification of the software. Note that when not all conditions can be known beforehand, a pilot must remain in the loop to take decisions during unforeseen circumstances. The Human Machine Interface that this involvement requires must be assessed by human factors experts and test pilots. In such an assessment the main criteria are usually adequate ‘situational awareness’ and ‘acceptable workload’ for a given amount of pilot training.

4.3 Regulations and certification

The conventional procedure to certify a system or operation is that the designers must demonstrate compliance to a *certification basis*. This certification basis can be the applicable regulations as agreed with the certification authority. A certification basis always consists of two parts: (1) a set of performance criteria and (2) *means of compliance* (methods to demonstrate that the criteria have been met).

To define a certification basis for air-to-air refuelling would require a large amount of adaptations and extensions of the current compliance-based regulations and would require at least:

- CS-25 Airworthiness regulations
- CS AWO All Weather Operations
- Air Operations Regulations
- Flight Crew Licensing

When performance-based regulations would be available, the developers could set their own pace in the certification process. With the Total System design methodology, the system model used in the design of the operation could be part of the to-be-developed performance-based regulation itself.

5 CASE: L4 highway cruise

In this section an automated transport case is worked out using the design method from the previous chapter. Performance and safety requirements of the required functions of the technical systems will be determined, and it will be shown how the correctness and completeness of the software specification can be assessed. Also it will be shown how regulations can be developed that ensures safety while leaving developers free design their own technical solutions.

5.1 Case – automatic driving on A4 highway

The automated transport case considers driving with SAE automation level 4 over the A4 highway from Schiphol to The Hague. The driver starts with conventional, manual driving. On the on-ramp to the highway, the driver can turn on the automation to transfer control to the vehicle. Until the vehicle nears the off-ramp near the destination, the driver does not have to monitor or control the vehicle. Here, the vehicle transfers control back to the driver.

Figure 11: Hands-off automated driving

Level 4 has been selected for the case based on the following arguments.

Level 2 and 3 offer mostly comfort functions. *Automated emergency braking* being a notable exception. In addition, these systems are already available under existing regulation. Level 4 is technically speaking relatively easy to realise provided the operational domain has been made predictable (no unpredictable behaviour of other road users and no occurrence of unforeseen external events). Yet, level 4 has the potential of significant efficiency enhancements in the economy. Finally, level 5 is only achievable at long term using Machine Learning, due to the unpredictability of the behaviour of other road users and the possible occurrence of unforeseen external events.

5.2 Applying the methodology

In this section the aviation design method sketched in section 4, is applied to a SAE level 4 automated passenger vehicle. The section below gives an overview of all elements identified during the work session.

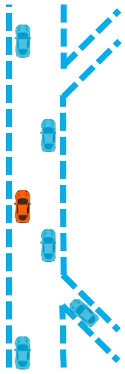
Technical system and functions

The road

- Obstacle-free surface with low roll friction

The car

- Changing direction
- Changing speed
- Determine location on the road
- Determine location of other vehicles on the road



The nominal operation – use of the functions

With a selected speed (between the minimum and maximum allowed speeds) automatic driving on the highway, without colliding to other vehicles. This implies staying in the lane, changing lanes when there is sufficient space and the selected speed justifies a lane change, and keeping distance to the vehicle in front.

This means that the four main functions of the car must have a high availability (e.g. probability of non-availability less than 1 per billion driving hours, depending on the desired safety level). In case of non-availability of a function access to automated driving functionality is denied.

Non-nominal operation

Technical failures	Response
Hole in the road surface	Register the hole (requires an additional function) and drive around it or stop the vehicle on in the driving lane. Or prevent holes by frequent road inspections.
Blowout tyre	Register the blowout (required an additional function), prevent the car from spinning and steer the car towards the emergency lane and bring it to a stop. If this is not possible stop the vehicle on the driving lane.
Fire (on-board)	Register the fire (requires an additional function) and steer the car towards the emergency lane and bring it to a stop
Engine failure	Register the engine failure (requires an additional function) and steer the car towards the emergency lane and bring it to a stop. If this is not possible stop the vehicle on the driving lane.

Extreme weather	Response
Fog	No adaptations necessary
Thunderstorm	No adaptations necessary
Rain	Register the rain (requires an additional function) and adapt the maximum speed
Snow	Register the rain (requires an additional function) and adapt the maximum speed
Black ice	Register the black ice (requires an additional function) and adapt the maximum speed
Wind	Register the wind (requires an additional function) and adapt the maximum speed

External events	Response
Object on the road	Register the object (requires an additional function) and drive around it or stop the vehicle in the driving lane.
Animal crossing the road	Animals have unpredictable behaviour that cannot be modelled. Therefore this event needs to be prevented by instalment of fences along the sides of the road.

Modelling the operation for all circumstances

- Model the operation as described above as chains of events leading to certain outcomes.
- From these chain of events, the safety (availability and integrity) and performance requirements of the functions follow.
- The functions and their safety and performance requirements do not prescribe technical solutions but leave technical developers free to design their own solutions.
- The model of the operations forms the specification of the software.

Transition of control

When exiting the highway, the driver must take control of the technical systems that implement all functions mentioned above. Limiting ourselves to the four main functions this implies:

Function	Driver action
Changing direction	Control the steering wheel (= HMI)
Changing speed	Control the accelerator pedal and brake pedal (= HMI)
Determine location on the road	Look through the window (= HMI)
Determine location of other vehicles on the road	Look through the window and into rear-view device (=HMI)

Visibility can be a problem due to a misted windshield, ice-covered windshield, snow-covered windshield or fog, all of which can have arisen during the automatic driving period.

Prior to transition of control it must be ensured that the windshield is clean. Considering already existing functions in a vehicle, this implies that an additional function that can detect fog is required. In case of fog, the vehicle must be slowed down to a safe speed, prior to transition of control.

5.3 Regulations and certification

Regulations

The method used in section 4.2 and sketched in section 3.2 could be the basis for performance-based regulations for autonomous transport. Performance-based regulations have the advantage over compliance-based regulations that it does not prescribe technical solutions and allows developers to set their own pace in the certification process. Compliance-based regulation is only practical after technical solutions have converged to common solutions.

Certification

For certification the following would have to be demonstrated:

- The model of the operation is complete and correct.
- The software implementation corresponds 1-1 with the model of the operation.
- The technical systems provide the required functions, performance, availability and integrity.
- The Human Machine Interface required for ‘transition of control’ provides an adequate situational awareness and acceptable workload. The training of the driver is adequate, given the Human Machine Interface.

MODE
SPLIT RESET
START STOP
ACCUSPLIT
STOPWATCH
A
10:5323
C
MIN. SEC. 1/100
PRO SURVIVOR
601X
3V.1

6 Conclusions

Road transport is regulated by rules and standards that specify aspects such as the design of vehicles, roads and infrastructure, the rules of the road, and how drivers are trained. To ensure the safety of the road transport system, regulatory authorities check if all stakeholders comply with rules and standards. How to adapt regulations to automated vehicles was one core challenges presented to the attendees of the work session.

Because compliance-based regulation and certification prescribes how to do things, it is both easy to govern and easy to adhere to. The downside is that it is restrictive in how to meet a goal. This dismisses solutions that are different from those foreseen when drafting the regulations. The assumption of a human driver is at the core of current compliance-based regulations, yet evidently this assumption does not apply to increased automation levels. Existing regulation does not allow for this change nor can it guarantee the safety of a driverless operation. One could draft new compliance-based regulations that would apply to self-driving vehicles but the lack of experience with these vehicles would make this either a very long process or very restrictive. Both outcomes stifle innovation.

Performance-based regulation is the way forward for regulating self-driving vehicles.

Performance-based regulations provide an alternative to compliance-based regulations. Instead of checking for compliance with standards, regulatory authorities set minimum performance requirements. How you meet those requirements and how you prove it, is up to the manufacturer or operator. Over time, accepted means of compliance will develop. If a manufacturer or operator follows this procedure and meets the requirements, the regulator will approve of the operation. Nevertheless, alternatives will remain possible. The downside of this approach is that it requires a fundamental understanding by the regulatory authority of the system that it regulates, including all underlying complexities. This can be challenging, especially if the system is new and complex. Still, all stakeholders present at the work session agreed that performance-based regulation is the way forward for self-driving vehicles.

Currently there is no unified way of assessing the safety of automated driving use cases. This gap makes it more difficult for the attendees to innovate with these vehicles. The *Total System* design methodology as used in the work session provides a promising alternative. The methodology should be able to develop performance based regulation for self-driving vehicles up to SAE level 4 in a relatively short amount of time. This would help remove a major hurdle in the way of improving safety, mobility, comfort and productivity in road transport by means of automated driving.

We can conclude from the work session that exploitation of self-driving vehicles is still in its infancy. In order to develop the safety case for an operation including self-driving vehicles up to level 4, the Total System design method can (a.) assess the safety of self-driving vehicles within its operational context and (b.) provide a platform that allows stakeholders to develop new operational use cases together. This would allow for the development of use cases that actually create value to stakeholders.

7 References

Table 3: Picture acknowledgements

PAGE	CAPTION	SOURCE
Cover	-	‘DS355’ via Flickr.com
Executive summary	-	‘why kei’ via unsplash.com
3	-	Beterbenutten.nl
9	Figure 2: impression of October 11	NLR
10	-	Janelle Patiño, US airforce
11	Figure 3: Sperry auto-pilot	Eric Long, National Air and Space Museum, Smithsonian Institution
12	Figure 5: working position of the on-board engineer in a Boeing 747-200	Wikimedia Commons
12	Figure 6: cockpit of an Airbus A320	Geek.com
12	Figure 7: level of sight operation of a drone	NLR
15	-	Wikimedia Commons
20	-	Costabrava.com.br
21	Figure 11: hands-off automated driving	David Paul Morris, Bloomberg
25		Swimoutlet.com
29		SAE International

Appendix A Work Session

Appendix A.1 Online questionnaire

The following questionnaire was sent to all invitees to the work session. It was replied to 7 times.

Question	Options	Response
Do you expect to encounter (partially) self-driving vehicles in your profession within the next 5 years?	Yes No Maybe	Response is attached in separate document.
How will (partially) automated vehicles affect your job?	Open	
I know what expect from ... in the context of (partially) automated vehicles.	Vehicle Infrastructure Driver Regulation	
What are your biggest challenges?	Public acceptance Regulation Engineering Safety Collaboration Other...	
What would like to know from other stakeholders?	Open	
When do you consider a collaborative workshop with stakeholders to be successful?	Open	

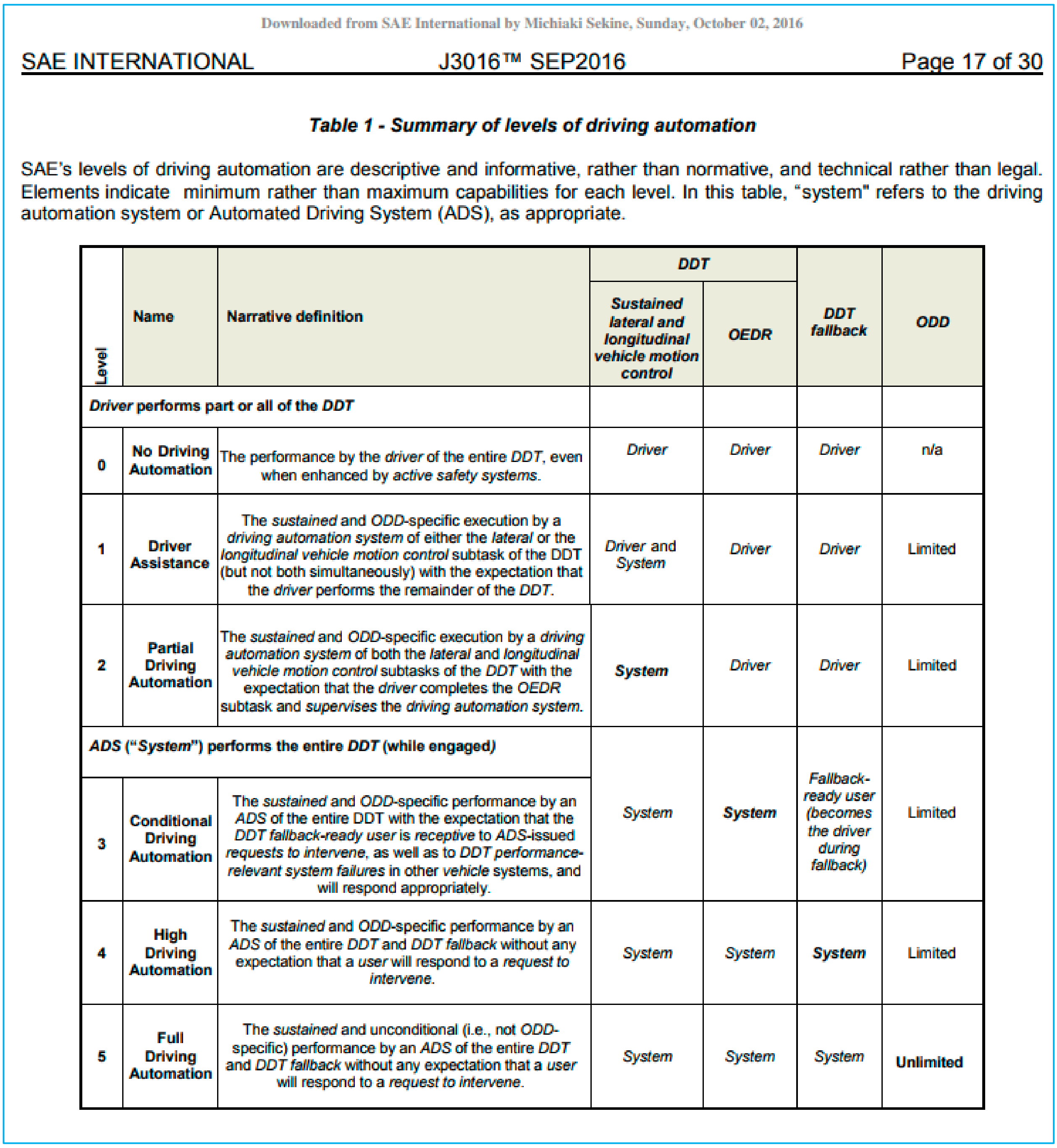
Appendix A.2 Slides and notes

Slides are provided in a separate document.

Appendix B Additional material

Appendix B.1 SAE autonomy levels

The Society of Automotive Engineers (SAE) defines 5 levels of autonomy to describe the automation of driving tasks.



Downloaded from SAE International by Michiaki Sekine, Sunday, October 02, 2016

SAE INTERNATIONAL J3016™ SEP2016 Page 17 of 30

Table 1 - Summary of levels of driving automation

SAE's levels of driving automation are descriptive and informative, rather than normative, and technical rather than legal. Elements indicate minimum rather than maximum capabilities for each level. In this table, "system" refers to the driving automation system or Automated Driving System (ADS), as appropriate.

Level	Name	Narrative definition	*DDT*		*DDT fallback*	*ODD*
			Sustained lateral and longitudinal vehicle motion control	***OEDR***		
Driver* performs part or all of the *DDT						
0	**No Driving Automation**	The performance by the *driver* of the entire *DDT*, even when enhanced by *active safety systems*.	*Driver*	*Driver*	*Driver*	n/a
1	**Driver Assistance**	The *sustained* and *ODD*-specific execution by a *driving automation system* of either the *lateral* or the *longitudinal vehicle motion control* subtask of the DDT (but not both simultaneously) with the expectation that the *driver* performs the remainder of the *DDT*.	*Driver and System*	*Driver*	*Driver*	Limited
2	**Partial Driving Automation**	The *sustained* and *ODD*-specific execution by a *driving automation system* of both the *lateral* and *longitudinal vehicle motion control* subtasks of the *DDT* with the expectation that the *driver* completes the *OEDR* subtask and *supervises* the *driving automation system*.	***System***	*Driver*	*Driver*	Limited
***ADS* ("*System*") performs the entire *DDT* (while engaged)**			*System*	***System***	*Fallback-ready user (becomes the driver during fallback)*	Limited
3	**Conditional Driving Automation**	The *sustained* and *ODD*-specific performance by an *ADS* of the entire DDT with the expectation that the *DDT fallback-ready user* is *receptive* to *ADS*-issued *requests to intervene*, as well as to *DDT performance-relevant system failures* in other *vehicle* systems, and will respond appropriately.				
4	**High Driving Automation**	The *sustained* and *ODD*-specific performance by an *ADS* of the entire *DDT* and *DDT fallback* without any expectation that a *user* will respond to a *request to intervene*.	*System*	*System*	***System***	Limited
5	**Full Driving Automation**	The *sustained* and unconditional (i.e., not *ODD*-specific) performance by an *ADS* of the entire *DDT* and *DDT fallback* without any expectation that a *user* will respond to a *request to intervene*.	*System*	*System*	*System*	**Unlimited**

This page is intentionally left blank.

NLR

Anthony Fokkerweg 2
1059 CM Amsterdam, The Netherlands
p) +31 88 511 3113 f) +31 88 511 3210
e) info@nlr.nl i) www.nlr.nl