energies

MDPI

Review

Recent Advancements in Automated Vehicle Certification: How the Experience from the Nuclear Sector Contributed to Making Them a Reality

Riccardo Donà [1], Biagio Ciuffo [2], Anastasios Tsakalidis [2], Lorenzo Di Cesare [2], Calogero Sollima [2], Marco Sangiorgi [2] and Maria Cristina Galassi [2,*]

[1] Uni Systems Italy, Via Michelangelo Buonarroti 39, 20145 Milan, Italy
[2] European Commission, Joint Research Centre (JRC), 21027 Ispra, Italy
* Correspondence: maria-cristina.galassi@ec.europa.eu

Abstract: The current paper discusses the most recent advancements in automated vehicle (AV) certification and how existing regulations/best practices from the nuclear field helped make AVs a reality. In particular, three main pillars differentiate the newly devised certification frameworks from previous automotive regulations: the introduction of a *safety management system*, the adoption of *in-service monitoring and reporting* data logging systems, and the use of *virtual testing* to demonstrate the safety of the AV; a set of pillars that are also found in the nuclear practice. The argumentation is informed by relevant literature and shared experiences from the nuclear power plant and transportation fields where there are established safety practices to manage safety-critical cyber-physical systems. Although the nuclear and transportation fields might seem unrelated, strong synergies were found, including risk management approaches and operational data collection procedures, which supported the timely drafting of the new regulation for AVs. Nonetheless, some open challenges remain due to peculiar aspects of AVs that will need to be addressed in the near future. Namely, practical methodologies for the residual-risk calculation for the various Operational Design Domains (ODDs), the design of scalable monitoring techniques, and the definition of detailed procedures for the virtual testing tool qualification.

Keywords: automated driving; monitoring; reporting; investigation; operational data; safety; virtual testing

Citation: Donà, R.; Ciuffo, B.; Tsakalidis, A.; Di Cesare, L.; Sollima, C.; Sangiorgi, M.; Galassi, M.C. Recent Advancements in Automated Vehicle Certification: How the Experience from the Nuclear Sector Contributed to Making Them a Reality. *Energies* **2022**, *15*, 7704. https://doi.org/10.3390/en15207704

Academic Editor: Mario Marchesoni

Received: 30 September 2022
Accepted: 17 October 2022
Published: 18 October 2022

1. Introduction

The field of road transport is witnessing a Copernican revolution as vehicles have started being equipped with automated driving systems (ADSs) that allow the driver to be freed from the driving task and not be legally responsible while the vehicle is operated by the ADS. Such technologies have dramatic potential to increase safety, reduce fuel and energy consumption, and increase accessibility to transportation services [1,2]. Nonetheless, effective certification procedures are needed to translate the beneficial potential into concrete real-world achievements.

The type-approval process of conventionally-driven vehicles typically relies on sets of well-defined tests to be carried out in a controlled environment (proving ground or laboratories) by specialized personnel. That is, in contrast with how vehicles actually operate in the real-world once they are allowed to circulate on public roads. Such a mismatch between the traditional physical testing/certification and the in-service operation is particularly emphasized as the degree of complexity of the system under test is increased due to technological advancements as we highlighted in [3]. Considering, for instance, the field of automated vehicles (AVs), a widely recognized work has demonstrated how obtaining sufficient statistical evidence that an AV is as safe as the average driver would require several millions of miles to be driven [4].

Under this premise, the United Nations Economic Commission for Europe (UNECE) WP.29 Working Party on Automated/Autonomous and Connected Vehicles (GRVA) has developed the New Assessment/Test Methods (NATM) Master Document [5], where a novel multi-pillar approach is envisaged, as shown in Figure 1. The newly conceived certification aims at addressing the aforementioned gap between the certification pre-market deployment and the in-service operation by complementing physical testing with additional pillars that are new within the field of road transport.

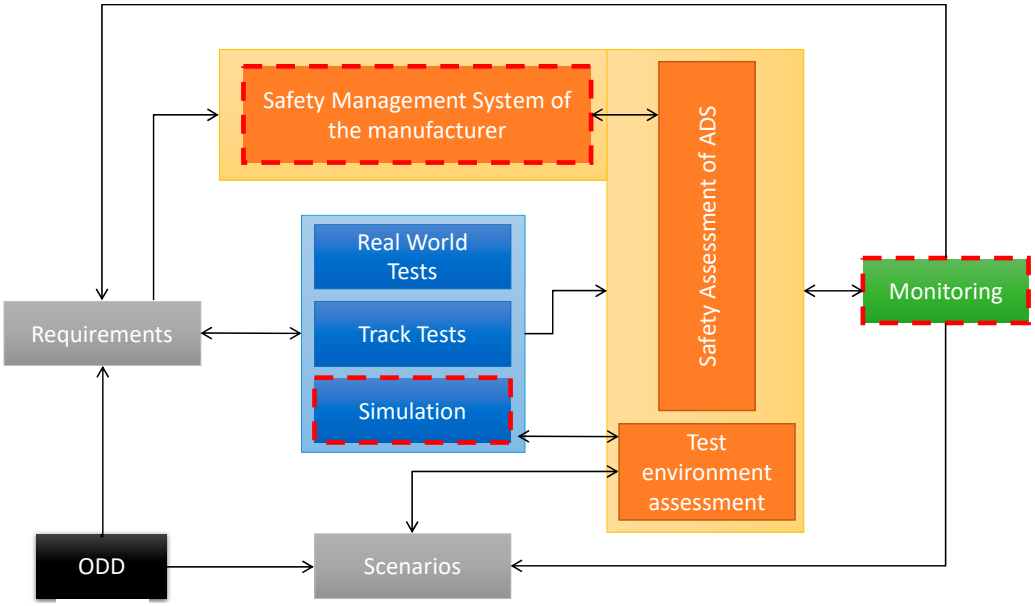


Figure 1. The multi-pillar approach. Authors' own elaboration based on the NATM guideline document [6]. Surrounded by red-dotted line blocks are the novelty aspects of the newly conceived certification framework. The light-blue background encompasses the "testing" pillars (i.e., real-world, track-test, and simulation). The light orange L-shaped box is instead representative of provisions to be fulfilled via an Audit phase (i.e., the manufacturer's SMS, the Safety Assessment of the ADS, and the assessment of the test environment).

Specifically, in parallel to the traditionally-performed proving ground and real-world tests, the multi-pillar approach features novel aspects such as the simulation/virtual testing pillar [7,8] and includes the investigation of the post-certification ADS behavior thanks to the "In-Service Monitoring and Reporting" (ISMR) pillar. Albeit in several fields, monitoring and reporting are widely established ingredients of the system operation, the introduction of ISMR for ADSs represents the first known application within the automotive industry. A similar consideration applies to the "Simulation" pillar. Indeed, simulation was already an accepted means to demonstrate some roadworthiness criteria [9]. However, prior to the NATM, the tool was only accepted to replace very specific tests via a prescriptive approach. Eventually, these two phases are complemented by a preliminary analytical phase ("audit pillar"), where the maturity of the manufacturer's company in terms of safety culture is verified through an audit of its Safety Management System (SMS), and the "safety concept" implemented in the ADS design is also assessed through the evaluation of a documentation package prepared by the manufacturer. In addition, this analytical phase represents an innovative aspect of the newly designed ADS safety validation framework.

This paper discusses the synergies that were found in the definition of the novelty pillars of the ADS certification approach from other fields, namely, nuclear energy production and other transportation sectors where safety-critical automation technology has been effectively adopted. The paper is structured as a review manuscript and constitutes a follow-up of our previous works [3,10], where we shared our initial view concerning how different fields might contribute to the overall certification of AVs. In the present

manuscript, we take a step forward by demonstrating how existing regulations and best practices have supported the formulation of requirements for the SMS, the adoption of virtual testing, and the introduction of an ISMR for ADS.

Firstly, we give details concerning the state-of-the-art regulatory background on ADS certification at both European Union (EU) and UNECE level. Then, we discuss how the challenges related to ADS certification were tackled by taking advantage of the lessons learned in various fields. Finally, a discussion focuses on the remaining gaps in the field, followed by conclusions.

2. Automated Driving Regulatory Background and Recent Outcomes

The development of AVs has undertaken a remarkable step forward in the last two years with the introduction of a set of regulations enabling higher automation levels on public roads. In fact, until the very beginning of 2021, the maximum SAE J3016 [11] (Figure 2) automation level allowed on the market was Level 2. More specifically, an SAE Level 2 vehicle is featured with Advanced Driver Assistance Systems (ADAS) that fully automate the car provided that a specific Operational Design Domain (ODD) is met. However, the human driver must always supervise the vehicle under any circumstance and remains legally liable during the entire operation. An example of an SAE Level 2 vehicle is a car equipped with Adaptive Cruise Control (ACC) coupled with a lane-centering ADAS.

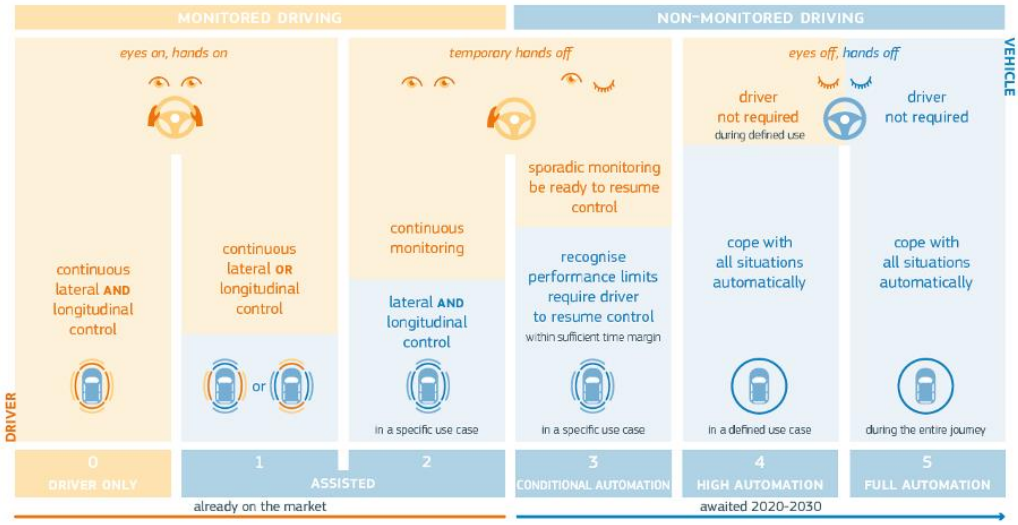


Figure 2. SAE J3016 automation levels [3].

Nonetheless, proper Automated Driving (AD) is defined for SAE Level 3 and above, where the driving system is legally responsible for the Dynamic Driving Task (DDT) in its ODD and the human driver is not required to pay attention to the road when the ADS is active. In particular, according to the SAE Level 3 specifications, the human driver is allowed to carry out non-driving-related activities when the ADS is activated; nonetheless, in case the system issues a take-over request, they shall take the control of the vehicle. On the contrary, according to the SAE Level 4, the system is capable of performing a Minimum Risk Maneuver (MRM) to reach a Minimum Risk Condition (MRC) in case of a system failure or any other critical condition arising which necessitates the ADS disengagement. SAE Level 4 vehicles might not even necessitate the presence of a human driver on board, thus enabling driver-less vehicle configurations. Eventually, the SAE Level 5 removes any limitation concerning the ODD where the ADS can operate hence enabling AD under any circumstance.

In this section, we give an overview of the regulatory frameworks for AD at both EU and UNECE level, taking advantage of the very latest developments within the field.

2.1. UNECE Regulation 157

A major milestone for AD took place in January 2021, with the first release of UNECE Regulation 157 (UN R157) [12], which established provisions for the type-approval of the firstly regulated SAE Level 3 system: the Automated Lane Keeping System (ALKS). The ALKS is an automation system that can control the speed and lane-keeping on motorways where pedestrians and cyclists are forbidden and with physical separation between opposite driving lanes. Originally, the ALKS was restricted to a maximum operational speed of 60 km/h and with no possibility of automated lane-changes. Such an initial realization of the ALKS was also known as "Traffic Jam Assist". In the last year, however, UN R157 has been amended to enhance the competencies of the ALKS while maintaining the same ODD. The revised ALKS features automatic operation up to 130 km/h and is allowed to carry out automated lane-changes [13]. Thus, the augmented ALKS is also known as the "Highway Chauffeur". The increased speed and behavioral competencies are backed by a revision of the original testing provisions with now two dedicated Annexes for proving ground and real-world testing and performance models for the safety benchmark [14].

A fundamental aspect of UNECE Reg. 157 is related to the introduction of an audit phase where the manufacturer is required to demonstrate to the authority that processes have been put in place to ensure that the ALKS is free from unreasonable risks for the occupants and other road users during the ALKS lifetime. The type-approval authority shall also be informed of the design principles behind the ALKS functioning in an attempt to create stronger synergy between authorities and manufacturers.

Moreover, UNECE Reg. 157 mandates the introduction of the Data Storage System for Automated Driving (DSSAD). The DSSAD is a tool that monitors the status of the (human) driver vs. the ADS, recording, among the others, the system activation, deactivation, manual override, and transition demand requests issued by the ALKS. The main aim of DSSAD is to establish the liability during an occurrence since, with SAE Level 3, the legally responsible driver might be either the human or the ADS and without a logging tool it would be impossible to reconstruct who was in charge of the driving task at the time of the event. Coupled with the Event Data Recorder (EDR), mandated according to UNECE regulation Reg. 160 [15], the EDR/DSSAD duo enables accident reconstruction and liability assignment. Critical accidents during engaged ALKS operation shall be reported by the manufacturer and, in case a safety-relevant threat is identified, the manufacturer is required to provide suitable corrective actions.

Eventually, the regulation does allow the manufacturer to supply the type-approval authority with supporting evidence for its safety case based on simulation data, provided that the scope of the simulation and the validation of the virtual testing tool is performed beforehand.

2.2. EU ADS C(2022)5402

The recently adopted EU ADS implementing act [16] moves a step towards higher automation levels by regulating the type-approval of a variety of SAE Level 4 systems in small production series. The regulation allows the market introduction of fully automated systems capable of performing "hub-to-hub" applications, "automated valet parking", and serving as robo-taxis or urban shuttles. While the UN R157 incorporated the NATM principles only to some extent, the EU ADS Regulation represents de-facto the first practical application of the multi-pillar approach as described in the NATM master document [5].

The Audit pillar is indeed also included in the EU ADS implementing act. In particular, the type-approval authority shall be informed about the ADS' layout, control strategies, and safety concept to ensure that the residual risk is sufficiently low for market introduction. In particular, a complementary acceptability criterion for safety as a global threshold is introduced and must be demonstrated at type approval, before market introduction. Such a transition from a prescriptive to a performance/risk-based approach is documented to be a better fit for complex cyber-physical systems, which are evolving at a faster rate than regulation can follow [17,18].

Similarly to UN R157, EU ADS C(2022)5402 also mandates the collection of onboard generated data. Nonetheless, the scope is not limited to accident reconstruction and consequent blame assignment. Instead, the data collection is part of an overarching *reporting* exercise that aims at sharing scenarios and lessons learned among regulators and original equipment manufacturers (OEMs). The in-service reporting distinguishes between "critical occurrences" (i.e., safety-related events), that shall be notified within one month and "non-critical occurrences" (i.e., events where an operational disruption occurred but that did not result in an accident or serious incident). In addition, every year the manufacturer is expected to issue a report, which confirms the safety performances claimed for the systems at the type-approval. The regulation's Annex 3 [19] also provides the manufacturer with a list of occurrences.

Moreover, the EU ADS Act also regulates the usage of virtual testing to demonstrate the safety of the ADS. A key aspect differentiating EU ADS C(2022)5402 from UNECE Reg. 157 is the approach toward virtual testing. While in UNECE Reg. 157 simulation can be used to support the safety concept provided that correlation analysis against real-world data is supplied, in the EU ADS act, a simulation *credibility* framework is provided. The credibility concept goes beyond data correlation between simulation and real-world (validation). Instead, credibility covers all aspects related to the management of Modeling and Simulation (M&S) toolchain including the *verification* of simulation models and the training of the personnel who designed and operated the M&S toolchain as shown in Figure 3.

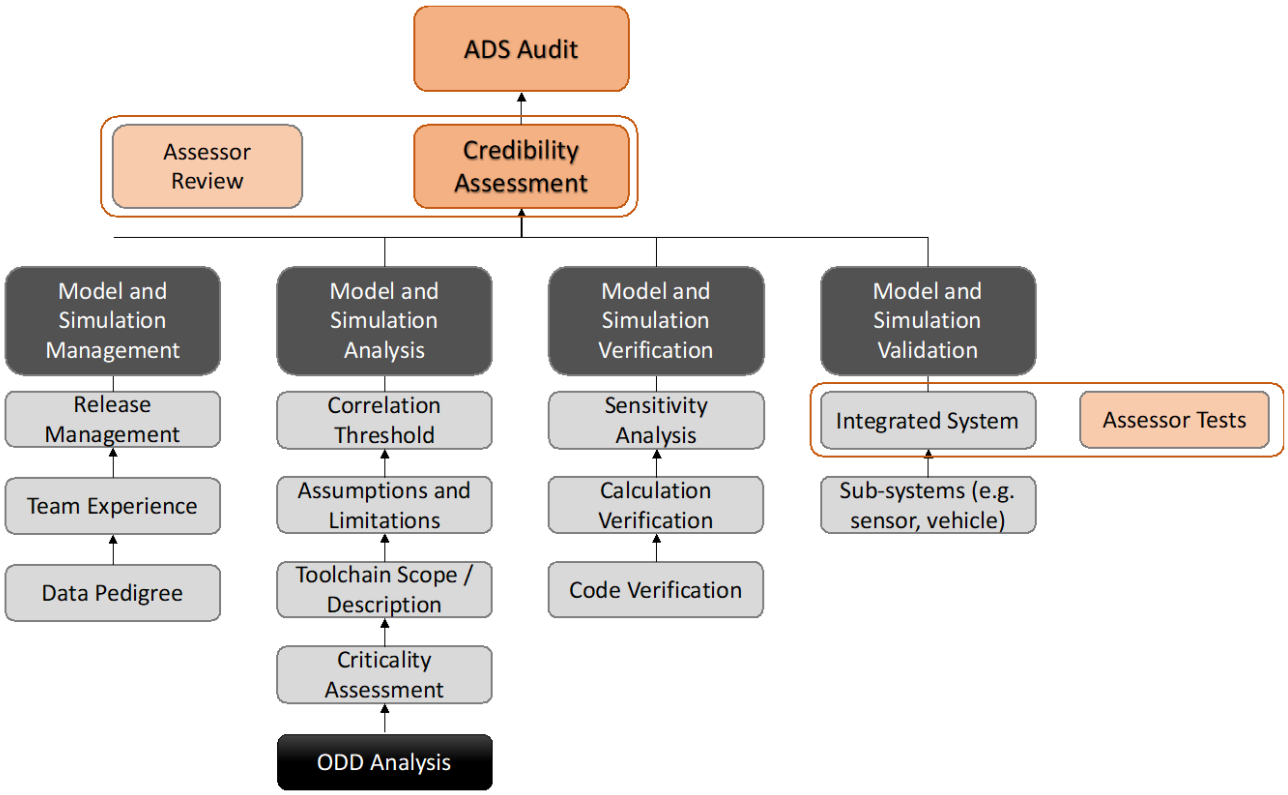


Figure 3. Authors' own elaboration based on the Simulation Credibility framework [19].

2.3. NATM Guidelines

Following up on the NATM Master Document [5], the UNECE-developed NATM Guidelines [6] were mainly developed as a versatile tool to support upcoming detailed regulations for ADS. Indeed, as mentioned above, the NATM Master Document fueled the drafting of EU ADS C(2022)5402. However, some interesting concepts further developed into the most recent version of the NATM Guidelines (successive to the adoption of the

EU ADS Act) which are mainly related to the ISMR, are not yet applied. In particular, the NATM guidelines foresee the introduction of a *monitoring* mechanism, in addition to the reporting already enforced in ADS C(2022)5402, as a way to achieve a proactive ADS safety performance confirmation. The monitoring exercise is concerned with elaborating vehicle collected data to identify dangerous trends (e.g., degrading braking capabilities), unusual driving scenarios, and effective crash avoidance strategies performed by the ADS for positive lessons sharing.

The guidelines give additional details concerning the data reporting flow of information as shown in Figure 4. Firstly, data are collected at Member State (MS) level by the responsible type-approval authority. The databases are then streamlined into a central repository, which allows the safety authority to have a complete overview of the type-approved ADS functioning and to issue safety recommendations.

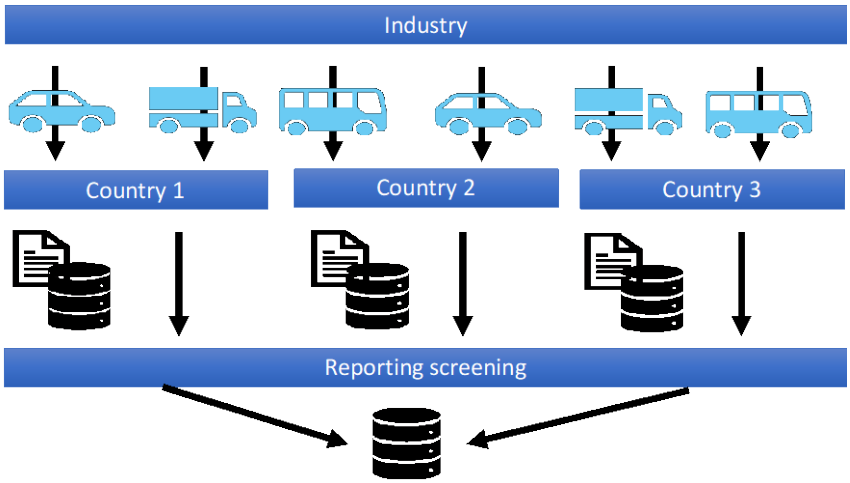


Figure 4. Reporting Mechanism, authors' own elaboration based on [6].

Finally, the latest NATM Guidelines also provide advice for the setting up of an investigation mechanism within the ISMR pillar by ensuring that critical occurrences are comprehensively analyzed, with the scope of deriving safety recommendations.

The three components of the ISMR pillar are graphically summarized in Figure 5 in terms of the degree of anticipation versus the severity level that the tool is concerned with. Monitoring is the most anticipative tool as it covers the ordinary operation of the vehicle while the ADS is activated. On the other side, the investigation is only required for critical occurrences after they have happened, thus being the least anticipative.

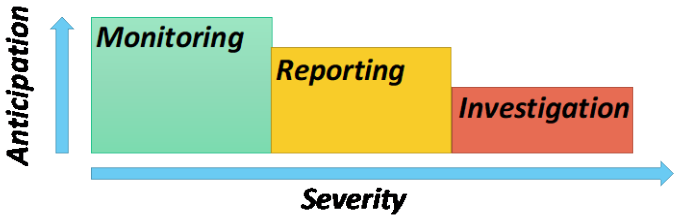


Figure 5. Relationship among monitoring, reporting, and investigation. Authors' own elaboration based on [6].

Similarly, the SMS audit section also features a more detailed description. The SMS as foreseen by the NATM guidelines covers three components:

- *human component*, which deals with the skills and training of the personnel involved in the ADS lifecycle;
- *organizational component*, that is concerned with the methods to manage the identified risks;

- *technical component*, that covers the appropriateness of the tools used.

The three aspects combined make up the so-called "HOT" structure within the SMS framework that are also present in other fields, as argued in the next section.

Undoubtedly, the work being carried out in the UNECE working groups will provide useful input in the next years to further develop the ADS approval framework also in the EU.

3. Lessons Learned Concerning the Safety Assessment/Management System

As we discussed in the introduction, the safety assessment of an ADS is an extremely complex task that demands testing solutions that go beyond real-world tests on a track or on the public roads. One of the methods to support the safety argument is to investigate the manufacturer's safety awareness and its capability to manage the identified safety hazards. Such a concern is typically accomplished by means of a Safety Management System, a collection of activities aimed at proving that the product was designed having safety in mind and that the developer has sufficient capabilities to ensure the safety of the product throughout the whole lifecycle.

The definition of an SMS is not a peculiar feature of the recent regulations concerning ADS. Instead, the lessons learned from the energy sector (in particular from Nuclear Reactor Safety) and transportation safety cultures played a major role in the definition of the requirements for the ADS manufacturer's SMS.

3.1. Nuclear Power Plant

Although the nuclear reactors might seem disconnected from automated driving, the nuclear field has a strong history of effective SMS solutions [20], which also include innovative risk assessments procedures (e.g., the Probabilistic Safety Assessment (PSA) [21,22] and the iterative approach for reporting and licensing).

Even though the development of an effective SMS was not achieved without any safety violations that resulted in fatalities, which started as early as in 1945 during the Los Alamos experiments [23], the nuclear community managed to make effective use of the experience gained. For instance, the 1979 Three Mile Island accident highlighted a series of inadequate management practices that could not counteract the otherwise solvable technological failure causing the accident [24]. Following an extensive analysis of the event, corrective action was taken by the International Atomic Energy Agency (IAEA) concerning measures for operator training and monitoring instrumentation [25]. Similarly, the ineffective and untrustworthy human operation that led to the Chernobyl disaster [26] was investigated and corrective actions was taken by the IAEA [27]. More recently, after the Fukushima-Daiichi accident, an EU-coordinated initiative, assessed the robustness of the European installed reactors against potential hazardous events by means of a "stress test", aiming at increasing their safety level via a set of commonly recognized practical actions [28].

Currently, the SMS devised by the International Nuclear Safety Advisory Group (INSAG) gives a clear picture [20] of the challenges behind ensuring the safety of a nuclear reactor. These challenges go beyond the pure system engineering but include operational and cultural issues that might well contribute to catastrophic accidents if not properly accounted for, as thought for the Chernobyl disaster [26]. Moreover, the report stresses the role of lesson learned among different plants operated worldwide. Safety is indeed not a local concern, and a catastrophic event might negatively influence the overall public acceptance of a potentially life improving technology. Such a scenario is also very worrisome for AVs [29]. Ultimately, the main message conveyed is the importance to promote a suitable "safety culture" within all the personnel involved in the system operation throughout the whole system lifecycle.

Another line of similarities is found in the licensing procedures. In fact, the two-step licensing approach adopted within the nuclear field (construction permit and operation) [30], is also found in the EU ADS C2022(5402). Specifically, the type-approval (first step) is

carried out at EU level whereas the licensing (second step) takes place at local level by the Member States.

Concerning the risk-management procedures, the PSA leverages on probability to analyze the effect on safety of uncommon situations. Indeed, edge cases dramatically affect the world of AVs to the point where a certain level of residual risk will have to be accepted. With this regard, the EU ADS C20222(5402) provides a first attempt, inspired by PSA, to discard scenarios that show an exposure significatively lower than the global safety threshold.

3.2. Transportation

The systematic approach toward safety management has been recognized as one of the processes that contributed the most to the increased security of many transportation fields [31]. Indeed, many transportation fields, such as aviation, railway, and maritime can rely on the support of safety agencies providing technical guidance on the SMS. For instance, in Europe, the European Aviation Safety Agency (EASA) is a specialized agency devoted to the type certification, monitoring, and investigation of aircraft. Similarly, the European Maritime Safety Agency (EMSA) and European Railway Agency (ERA) are in charge of ensuring the highest common level of safety within the maritime and railway fields, respectively.

3.2.1. Aviation

Despite the engineering challenge in maintaining a machine weighing several tons airborne, in 2022, EASA reported no fatalities involving large aircraft. Moreover, such a safety achievement holds true since 2017 [32], suggesting a clear evidence of a successful application of the safety culture principles within the aviation industry.

Practical guidance on the SMS fulfillment is provided by the Agency [33]. In particular, a set of activities that should be carried out by the manufacturer/operator and that are also relevant for the current discussion are listed:

- hazard identification;
- occurrence reporting;
- risk-management;
- The identification of hazards is the starting point of many SMS and is also an ingredient of all the ADS regulations summarized in Section 2. In particular, the hazard analysis is at the core of the "knowledge-based" approach to the definition of testing scenarios within the EU ADS implementing act;
- EASA provides several tools for risk-assessment, which include bottom-up approaches such as Failure Mode and Effect Analysis (FMEA) and top-down methodologies as the Systems Theoretic Accident Modelling and Process (STAMP) [34]. The two aforementioned tools are also listed among the suggested approaches in the UNECE Reg. 157 and EU ADS Act for the SMS fulfilment.

3.2.2. Railway

Similarly, the field of railway is supported by corresponding relevant guidelines for the SMS compliance [35]. The SMS, in addition to the vehicles and vehicles' operators, encompasses the infrastructure: a vital piece of the railway operation, which is not currently addressed in the ADS regulations (Figure 6). As such, explicit methodologies are defined to handle the complexities of the multi-actors train operating environment. The "HOT" components' list is also found in the ERA guidelines similar to the NATM guidelines.

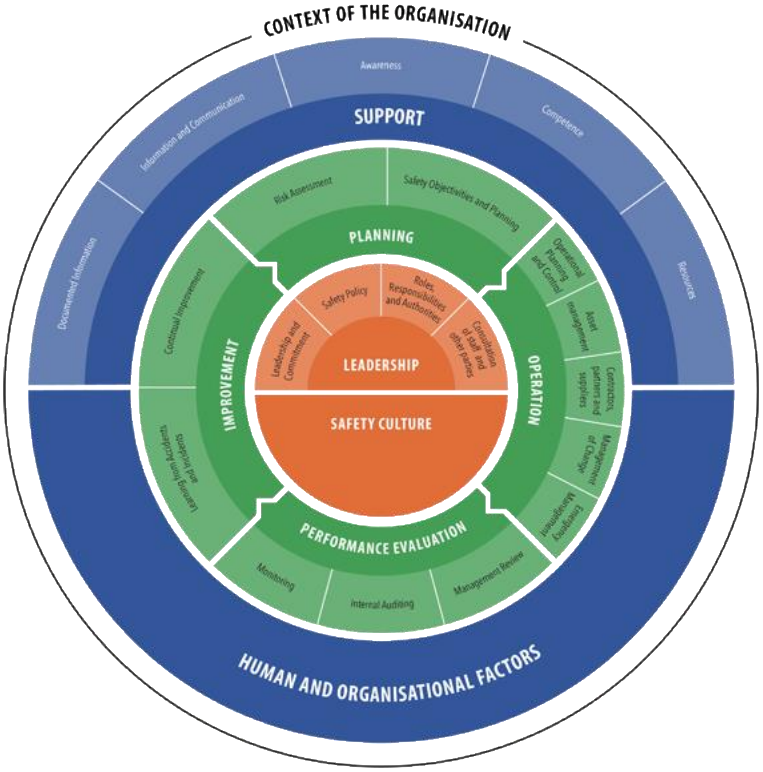


Figure 6. Safety Management Systems as of ERA [35].

The extensive collaboration between the representatives of ERA and the authors culminated in a joint workshop where similarities and gaps were acknowledged [10]. More specifically, the need to create a strong link between the vehicle and the infrastructure to allow for automation was recognized, a link which underlies the ODD analysis (i.e., the input block for the multi-pillar approach as seen in Figure 1). Moreover, the maintenance of vehicles to ensure safe automated operation was included in the SMS requirements to be reported by the ADS based on the discussions.

The development of future SMS solutions is also a topic of particular relevance within the research community dealing with new risk assessment techniques. For instance, in [36], the authors suggest the use of network thinking methodologies for a more effective risk assessment procedure.

4. Lessons Learned Concerning the Use of Operational Data

Obtaining objective feedback regarding the actual performance of a system during the real-world service via collecting operational data is extremely valuable information and also constitutes one of the main principles of any SMS analyzed. The collection of data mandated by the California Department of Motor Vehicle (CA DMW) has already been demonstrated to provide useful information to California authorities [37]. With the introduction of a standardized EDR/DSSAD and reporting obligations for ADSs, we can expect a major benefit also for European road authorities not only for manufacturers and insurance companies [38].

Another key aspect of operational data analysis is the capability to proactively anticipate critical events via the analysis of near misses [39,40] (i.e., events that did not result in damages or injuries but had the potential to do so). Near misses are reported to be between several hundred and a few thousand times the number of actual critical scenarios as reported in many safety pyramids, an example of which is given in Figure 7. Currently, the exact ratio between near misses and critical occurrences remains unknown due to the unavailability of recorded data. Nonetheless, ADS collected data might contribute to

building additional awareness for effective anticipative corrective actions, so that major events could be prevented and avoided.

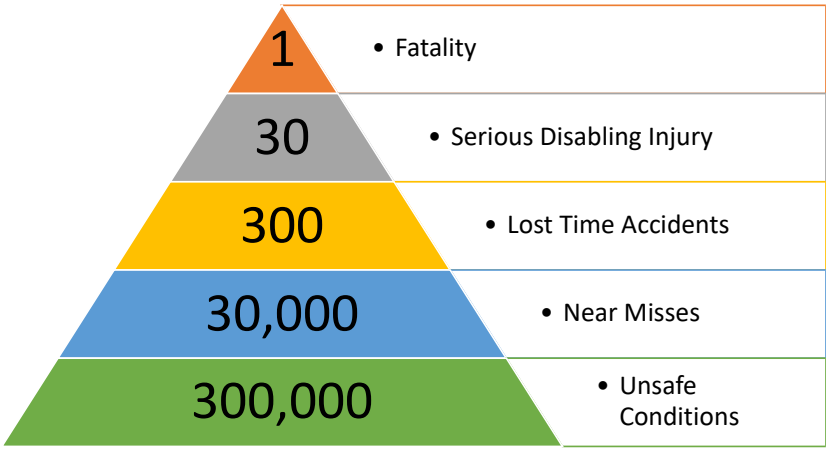


Figure 7. Safety Pyramid, authors' own elaboration based on [41].

4.1. Nuclear Power Plant

Monitoring tools are an integral part of the nuclear reactors' SMS [42,43]. The IAEA provides the nuclear power plant operators with best practices in collecting and distributing data [44], which also includes a list of practical examples and highlights roles and responsibilities within the management. In particular, safety-related events shall be analyzed, and the corresponding lessons learned shall be made available to other operators and authorities. Moreover, following the appropriate screening, the relevant event will undergo an investigation phase (Figure 8).

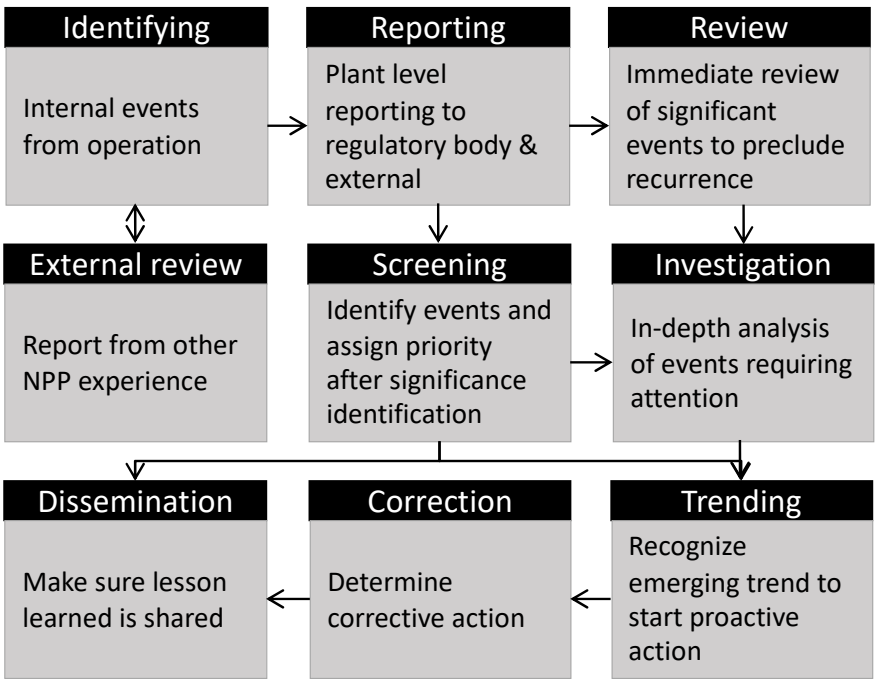


Figure 8. NPP monitoring and screening mechanism, own elaboration based on [44].

Even though the nuclear field is based on a different set of data-elements and occurrences to be reported, due to the different nature of the phenomena with respect to AVs, the overall NATM ISMR mechanism was heavily inspired by the nuclear sector experience. The nuclear sector approach constitutes a reporting mechanism that foresees

immediate notification of the responsible authority in case of a significant event. That is indeed very similar to the ISMR, which provides notice including a list of well-defined safety-related occurrences to the type-approval authority within 24 h. Then, thorough reporting should follow the initial analysis. Finally, an investigation will take place if deemed necessary. Such an investigation mechanism for safety-critical occurrences was also adopted in the NATM ISMR, given that it provides the authority with the possibility of "closing the loop" by linking operational data to safety recommendations to be shared with all relevant stakeholders.

Nonetheless, the best practices provide extensive details on the practical implementation of the reporting mechanism, which are currently not yet available in the NATM guidelines.

As an example of practical implementation, evidence collected through monitoring tools has contributed to amending the SMS as of the Fukushima accident in 2011 [43]. That was possible thanks to the information collected by IAEA and resulted in the safety recommendations issued to plants' operators to prevent similar phenomena from happening in the future.

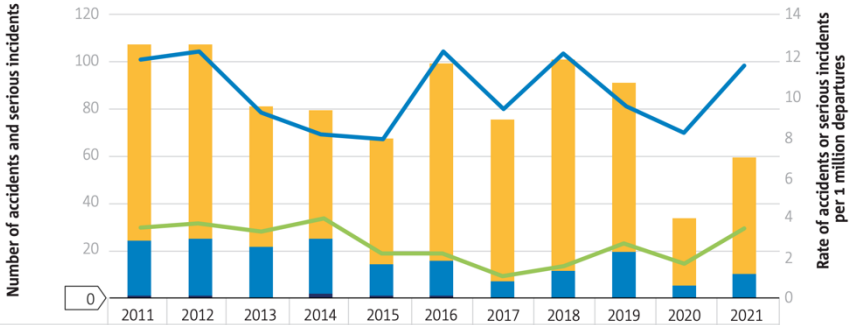
4.2. Transportation

Several transportation fields can rely on robust and well-established monitoring and reporting systems. In particular, the aviation, railway, and maritime transportation sectors can leverage on the European Coordination Center for Accident and Incident Reporting Systems (ECCAIRS) database [45]. ECCAIRS provides the users with a predefined taxonomy that supports safety-related events, which did not necessarily result in fatalities. The database has been developed since 1974, initially for the aviation field only. Overall, more the 4500 safety recommendations were issued based on the collected occurrences for the aviation sector only [46].

Conversely, road transport's related occurrences, which involved injuries or fatalities can be reported to the CARE [47] database in the EU by the Member States. The road transport reporting mechanism is thus inherently more limited than the other transportation reporting tools since occurrences where police investigation was not required (e.g., damage-only accidents and minor incidents are not reported). Moreover, harmonization issues affected the CARE database, which were ultimately solved only using the more recent Common Accident Data Set (CADaS) [48] approach that provides a minimum set of elements to be reported.

4.2.1. Aviation

Concerning aviation, the data procedures enable the safety agency to carry out statistical analysis and monitor the evolution of safety. For instance, EASA every year issues an "Annual Safety Review" where safety-related events are reported as in Figure 9. The report contains extremely valuable information since the authority can have the complete picture of the safety level achieved by the aircraft operators. Moreover, based on the information collected, the agency can issue safety recommendations as in the 2022 Annual Safety Recommendation Review [49].



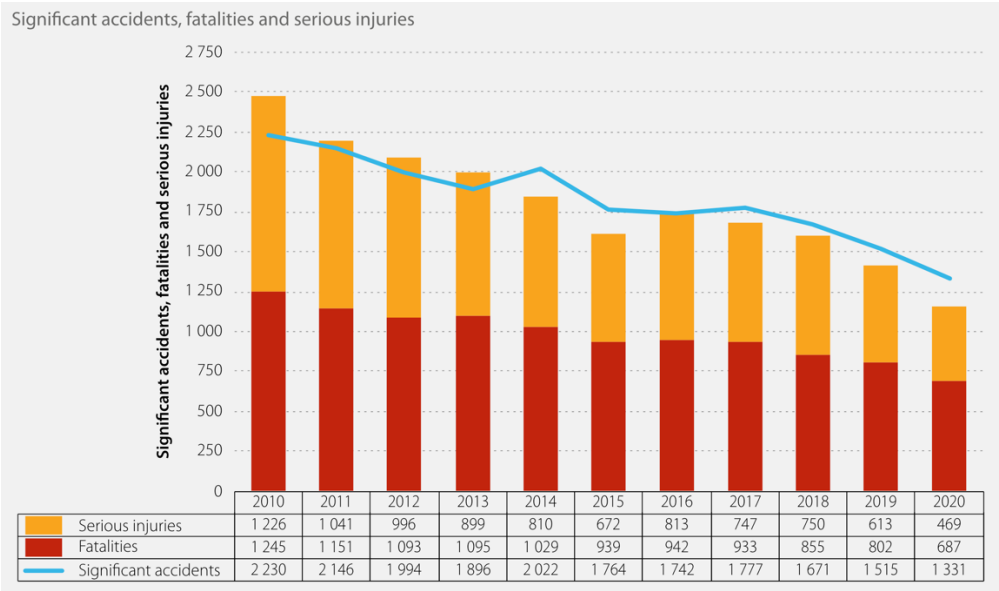
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Serious incidents	83	83	60	54	53	84	68	90	72	28	48
Non-fatal accidents	24	24	22	24	14	15	8	12	20	6	12
Fatal accidents	1	1	0	2	1	1	0	0	0	0	0
Serious incident rate	11.9	12.3	9.2	8.2	7.9	12.1	9.5	12.2	9.6	8.2	11.3
Accident rate	3.6	3.7	3.4	3.9	2.2	2.3	1.1	1.6	2.7	1.8	2.8

Figure 9. EASA 2022 Annual Safety Review [32], large airplane accidents.

Eventually, the recent introduction of a standardized risk classification system, the European Risk Classification Scheme (ERCS) [50], supports the effectiveness of the data collection by providing a set of severity indexes for a list of critical events and associated probabilities.

4.2.2. Railway

Similarly to EASA, the European Railway Agency (ERA) issues safety reports, such as the Report on Railway Safety and Interoperability [51], where safety-related occurrences are reported (Figure 10). Overall, a positive increasing safety trend can be observed for the railway sector.



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Serious injuries	1 226	1 041	996	899	810	672	813	747	750	613	469
Fatalities	1 245	1 151	1 093	1 095	1 029	939	942	933	855	802	687
Significant accidents	2 230	2 146	1 994	1 896	2 022	1 764	1 742	1 777	1 671	1 515	1 331

Figure 10. ERA 2022 Report on Safety and Interoperability [51].

5. Lessons Learned Concerning the Use of Virtual Testing

Virtual testing is a fundamental tool in the design phase of many safety-critical systems due to the lower testing costs, inherent safety, and repeatable executions. However, virtual testing needs to be *qualified* in order for the simulation-generated data to be accepted at the type certification phase. In particular, the qualification procedure aims at establishing the domain where simulation is a suitable substitute for the physical tests by means of

a *validation* exercise. Moreover, simulation management factors such as the personnel expertise and the simulation models' traceability together with the validation originate an overarching *credibility* framework for the virtual tool. The literature analyzed hereafter gives insights concerning how the qualification of the virtual tool is carried out in the fields that supported the definition of ADS regulation's credibility framework.

5.1. Nuclear Power Plant

The nuclear power plant field pioneered the use of simulation as early as the 1970s, mainly for operators' training [52]. A particular instance of these simulators are the Full Scope Simulators (FFS) used to train personnel in virtual replicas of the nuclear power plant. The qualification of such simulation tools has been supported by the American National Standards Institute (ANSI) since 1985, thanks to the ANSI-3.5 standard [53]. A similar validation approach underpins the ANSI-3.5 and the NATM/EU ADS simulation credibility framework, and that is related to the validation of the individual simulation models to be carried out in parallel to the simulation toolchain validation. Such a validation effort was deemed necessary given the complex physics and strong interactions existing among simulation models for both nuclear power plant and ADS simulation, which makes the individual simulation models' validation insufficient per se. Nonetheless, ANSI-3.5 moves a step further with respect to the NATM/EU ADS act by suggesting a list of relevant Key Performance Indicators (KPIs) and acceptance thresholds.

5.2. Transportation

The use of simulation in transportation fields is widespread, both as a tool to certify some of the system's requirements and as a testing environment to license pilots similarly to the application discussed within the nuclear power plant practice. Nonetheless, open gaps are reported both on the technical level (i.e., the development of established Verification and Validation (V&V) methodologies) and on the non-technical level (i.e., harmonization procedures to ensure reliability and acceptance across different simulation domains) [54]. Thus, cooperation among stakeholders dealing with qualification procedures for virtual testing is advocated to promptly bridge the gaps.

5.2.1. Aviation

Aviation regulations allow, in principle, for certain airworthiness criteria to be demonstrated via simulation. Simulation is indeed recognized as a valuable tool to avoid risky and costly type certification testing. However, no standardization effort has been successfully accomplished yet in terms of modeling practices and simulation qualification methodologies [55]. Thus, the appropriateness of the simulation toolchain adoption for the certification purpose is still guided by individual cooperation between manufacturers and the safety agency. Nonetheless, experience from the aviation sector played a major role in the drafting of the NATM simulation credibility framework, which was also the starting point for the EU ADS implementing act. In particular, the EASA CM-S-014 [56], which in turn is influenced by NASA-STD-7009A [57], proved to be a valuable inspirational source. EASA CM-S-014 provides guidance on all the aspects related to the credibility assessment of a simulation toolchain, which includes the V&V methodologies, uncertainty estimation methods, simulation management, and personnel experience and expertise (E&E).

Another widely established application of simulation is the pilot licensing via Flight Simulator (FS) training sessions. EASA has developed certification schemes for such systems (i.e., CS-FSTD) [58] and provides a classification of those systems, ranging from basic instrumentation training devices to full flight simulators. Despite our effort concerning the formulation of a credibility framework for virtual testing covered only the simulation tools related to the ADS testing, in the future the role played by driving simulators for the training of ADS safety drivers or remote operators might become relevant. Thus, the EASA CS-FSTD may turn out to be a precious tool to support upcoming research and regulatory activities.

5.2.2. Railway

Similarly to the aviation sector, the railway licensing process foresees the use of simulation-generated data at the certification level. For instance, aerodynamics compliance might be proven using numerical simulation in line with the specifications detailed in EN14067 [59], while crashworthiness might be virtually assessed according to EN15227 via Finite Elements Method (FEM). The intensification of the simulation usage as a certification tool is, nonetheless, a topic of research that is investigated, among others, by the European Joint Undertaking Shitf2Rail. In particular, the Shift2Rail deliverable D4.1 [54] gives extensive details on V&V approaches and acceptance criteria. An important aspect investigated in D4.1 is the need to move beyond the pure V&V to derive instead a credibility framework for simulations. One of the methods surveyed is derived from NASA-STD-7009A [57], the "Credibility Assessment Scale" (CAS), whereas the Predictive Capability Maturity Model (PCMM) is a new contribution. PCMM is built upon six points, four of which (i.e., code verification, solution verification, model validation, and uncertainty quantification) are also part of the EU ADS/NATM credibility framework.

6. Discussion

The radical change that is affecting the motor vehicle market with the introduction of AVs was backed by a vigorous regulatory effort in the last years. The regulators' work could benefit from existing best practices and lessons learned on certification specifications coming from fields where safety-critical technology is already an essential ingredient of the corresponding system's operation.

For instance, the SMS audit and the product safety assessment are an integral part of many transportation and energy production fields and its timely application to the AVs sector was possible thanks to the large experience accumulated in the mentioned literature. Such a newly introduced pillar enables moving a first step in the direction of a risk-based approach instead of purely prescriptive formulations, which the relevant literature and experience suggests is inadequate for ADS certification.

Operational data collection procedures have been introduced by means of reporting tools in the latest ADS regulations. Countless publications have shown the added value of collecting operational data, especially within the framework of risk-based certification schemes, as a feedback-loop for safety improvement.

Eventually, a simulation credibility framework underpins the state-of-the-art regulations for ADS, which strongly relies on the widely-established certification practices in aviation and railway industries.

Still, more work is needed in order to maximize the regulations' implementation effectiveness. For instance, practical guidelines to support type-approval authorities in analyzing the SMS are being developed. Monitoring is yet to be implemented in regulations to cover the anticipative factors and a scalable solution capable to handle the huge amount of data generated by the vehicle is to be envisaged. Effective techniques to qualify virtual testing will play a key role in enabling credible safety argument cases demonstration.

Moreover, regulators are necessarily shifting towards a top-down and open regulatory approach, that on one side allows more flexibility in adapting to the upcoming technological development, but on the other side requires an additional effort to achieve a single regulatory and certification process among Member States. Hence, strong collaboration and coordination among regulators, authorities, and manufacturers is deemed necessary in the upcoming years.

7. Conclusions

The present paper reviewed relevant literature that supported the drafting of the most recent EU and UNECE regulations concerning the type-approval of vehicles equipped with ADS. The work has discussed both international standards/regulations and state-of-the-art scientific contributions.

Three main components of the multi-pillar approach to ADS safety validation were discussed throughout the work: the SMS audit, the monitoring and reporting, and the virtual testing. Our effort encompassed inputs coming from several fields of the energy and transport sectors and their contribution to drafting the described regulation. The manuscript was inspired by the long-lasting safety cultures in nuclear power plants and other transport fields that are backed by factual safety records. Ultimately, the experience maturated in the nuclear energy production and transport sectors proved to be a useful basis within the AV field which allowed regulators to timely respond to the market demand.

Indeed, in the past years, the regulatory effort for driving automation has advanced substantially, as nowadays we witness an extended UNECE regulation for the approval of highway chauffeur and an EU Act for the approval of driverless vehicles. In particular, the EU regulation enforces the most innovative approach deriving from the continuous work being carried out at global level in the framework of UNECE working groups.

Still, open gaps remain to be explored. Namely, suitable guidelines and interpretation documents should be developed to balance the open-regulation approach adopted and support the harmonization of the type-approval processes across Member States. Moreover, strong collaboration among ADS manufacturers and regulators, but also among experts from other fields, is deemed necessary to evaluate the effectiveness of the certification processes put in place and improve where needed, in order for regulations not to inhibit but to foster a safe technological development.

Author Contributions: Conceptualization, M.C.G., B.C., L.D.C., C.S., M.S., A.T. and R.D.; methodology, M.C.G. and R.D.; writing—original draft preparation, R.D.; writing—review and editing, M.C.G. and A.T.; supervision, M.C.G.; project administration, M.C.G.; funding acquisition, M.C.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Directorate General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW) and the Joint Research Centre (DG JRC) of the European Commission.

Acknowledgments: The authors would like to acknowledge the EU institutional funding for the possibility to establish the presented research activities and for the resources made available.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alonso Raposo, M.; Ciuffo, B.; Alves Dias, P.; Ardente, F.; Aurambout, J.P.; Baldini, G.; Baranzelli, C.; Blagoeva, D.; Bobba, S.; Braun, R.; et al. *The Future of Road Transport: Implications of Automated, Connected, Low-Carbon and Shared Mobility*; Publications Office of the European Union: Luxembourg, 2019; ISBN 978-92-76-14318-5. [CrossRef]
2. NHTSA. *Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey*; National Highway Traffic Safety Administration (NHTSA): Washington, DC, USA, 2018.
3. Galassi, M.C.; Ciuffo, B.; Tsakalidis, A.; Di Cesare, L.; Sollima, C.; Sangiorgi, M.; Lagrange, A. New Approaches for Autonomous Vehicles Certification: Learning Best Practices from Nuclear Reactor Safety. Using knowledge to manage risks and threats: Practices and challenges. In Proceedings of the 58th ESReDA Seminar Hosted Online by the European Commission, Joint Research Centre, Alkmaar, The Netherlands, 15–16 June 2021; Publications Office of the European Union: Luxembourg, 2021. ISBN 978-92-76-42383-6. [CrossRef]
4. Kalra, N.; Paddock, S.M. Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability? *Transp. Res. Part A Policy Pract.* **2016**, *94*, 182–193. [CrossRef]
5. UNECE. *New Assessment/Test Method for Automated Driving (NATM)-Master Document*; UNECE: Geneva, Switzerland, 2021; p. 37.
6. UNECE. *New Assessment/Test Method for Automated Driving (NATM) Guidelines for Validating Automated Driving System (ADS)*; UNECE: Geneva, Switzerland, 2022; p. 68.
7. Donà, R.; Ciuffo, B. Virtual Testing of Automated Driving Systems. A Survey on Validation Methods. *IEEE Access* **2022**, *10*, 24349–24367. [CrossRef]
8. Donà, R.; Vass, S.; Mattas, K.; Galassi, M.C.; Ciuffo, B. Virtual Testing in Automated Driving Systems Certification. A Longitudinal Dynamics Validation Example. *IEEE Access* **2022**, *10*, 47661–47672. [CrossRef]
9. UNECE. *Uniform Provisions Concerning the Approval of Passenger Cars with Regard to Electronic Stability Control (ESC) Systems*; UNECE: Geneva, Switzerland, 2017; p. 26.

10. Galassi, M.C.; Lagrange, A.; Guido, P.; Mele, R.; Ciuffo, B.; Piron, O.; Malfait, W. *ERA–JRC Workshop on Safety Certification and Approval of Automated Driving Functions: Analogies and Exchange of Best Practices between Railway and Automotive Transport Sectors*; Publications Office of the European Union: Luxembourg, 2021; ISBN 978-92-76-28947-0. [CrossRef]
11. SAE International. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_202104. Available online: https://www.sae.org/standards/content/j3016_202104/ (accessed on 16 October 2022).
12. UNECE. *Uniform Provisions Concerning the Approval of Vehicles with Regard to Automated Lane Keeping Systems*; UNECE: Geneva, Switzerland, 2021; p. 64.
13. UNECE. *Proposal for the 01 Series of Amendments to UN Regulation No. 157 (Automated Lane Keeping Systems)*; UNECE: Geneva, Switzerland, 2022; p. 100.
14. Mattas, K.; Albano, G.; Donà, R.; Galassi, M.C.; Suarez-Bertoa, R.; Vass, S.; Ciuffo, B. Driver Models for the Definition of Safety Requirements of Automated Vehicles in International Regulations. Application to Motorway Driving Conditions. *Accid. Anal. Prev.* **2022**, *174*, 106743. [CrossRef] [PubMed]
15. UNECE. *Uniform Provisions Concerning the Approval of Motor Vehicles with Regard to the Event Data Recorder*; UNECE: Geneva, Switzerland, 2021; p. 21.
16. European Commission. *EU ADS Implementing Act*; European Commission: Brussels, Belgium, 2022.
17. Sgobba, T. B-737 MAX and the Crash of the Regulatory System. *J. Space Saf. Eng.* **2019**, *6*, 299–303. [CrossRef]
18. FAA. Type Certification for UAS—Back to the Future. Available online: https://www.faa.gov/uas/resources/events_calendar/archive/2019_uas_symposium/media/Type_Certification_for_UAS-Back_to_the_Future.pdf (accessed on 10 October 2022).
19. European Commission. *EU ADS Implementing Act Annex*; European Commission: Brussels, Belgium, 2022.
20. IAEA. *Management of Operational Safety in Nuclear Power Plants: A Report by the International Nuclear Safety Advisory Group*; International Nuclear Safety Advisory Group, Ed.; INSAG; International Atomic Energy Agency: Vienna, Austria, 1999; ISBN 978-92-0-102899-0.
21. Aldemir, T. A Survey of Dynamic Methodologies for Probabilistic Safety Assessment of Nuclear Power Plants. *Ann. Nucl. Energy* **2013**, *52*, 113–124. [CrossRef]
22. IAEA. *Probabilistic Safety Assessment*; International Nuclear Safety Advisory Group, International Atomic Energy Agency (IAEA): Vienna, Austria, 1992; p. 36.
23. A Criticality Study on the LA-1 Accident Using Monte Carlo Methods | Elsevier Enhanced Reader. Available online: https://reader.elsevier.com/reader/sd/pii/S0029549319304984?token=7C0DE725C0A3BEA697F2092DE56B7D8767945AB185B2A39ABA3E3006B625D7C46CE36C9CBC232E142649B91C3918BBE6&originRegion=eu-west-1&originCreation=20221010080409 (accessed on 10 October 2022).
24. Hopkins, A. Was Three Mile Island a 'Normal Accident'? *J. Conting. Crisis Manag.* **2001**, *9*, 65–72. [CrossRef]
25. IAEA. *International Experience in the Implementation of Lessons Learned from the Three Mile Island Incident*; TECDOC Series; International Atomic Energy Agency (IAEA): Vienna, Austria, 1983.
26. Salge, M.; Milling, P.M. Who Is to Blame, the Operator or the Designer? Two Stages of Human Failure in the Chernobyl Accident. *Syst. Dyn. Rev.* **2006**, *22*, 89–112. [CrossRef]
27. *The Chernobyl Accident: Updating of INSAG-1*; INSAG Series; International Atomic Energy Agency: Vienna, Austria, 1992; ISBN 92-0-104692-8.
28. ENSREG. *Stress Tests Performed on European Nuclear Power Plants*; European Nuclear Safety Regulators Group: Brussels, Belgium, 2012; p. 53.
29. Duboz, A.; Mourtzouchou, A.; Grosso, M.; Kolarova, V.; Cordera, R.; Nägele, S.; Alonso Raposo, M.; Krause, J.; Garus, A.; Eisenmann, C.; et al. Exploring the Acceptance of Connected and Automated Vehicles: Focus Group Discussions with Experts and Non-Experts in Transport. *Transp. Res. Part F Traffic Psychol. Behav.* **2022**, *89*, 200–221. [CrossRef]
30. U.S. Nuclear Regulatory Commission. *Nuclear Power Plant Licensing Process*; Office of Public Affairs, U.S. Nuclear Regulatory Commission: Washington, DC, USA, 2004; p. 20.
31. Maurino, D. Why SMS: An Introduction and Overview of Safety Management Systems. Available online: https://www.itf-oecd.org/sites/default/files/why-sms.pdf (accessed on 10 October 2022).
32. EASA. *Annual Safety Review*; European Aviation Safety Agency (EASA): Cologne, Germany, 2022; p. 174.
33. SM ISG. 10 Things You Should Know about Safety Management Systems (SMS). Available online: https://www.icao.int/NACC/Documents/Meetings/2017/ANSATS/ReferencesResources-10ThingsYouShouldKnowAboutSMS.pdf (accessed on 10 October 2022).
34. EASA. *Methodology to Assess Future Risks*; European Aviation Safety Agency (EASA): Cologne, Germany, 2021.
35. European Union Agency for Railways. *Safety Management System Requirements for Safety Certification or Safety Authorisation*; Publications Office of the European Union: Luxembourg, 2022.
36. Bekisz, A.; Kowacka, M.; Kruszyński, M.; Dudziak-Gajowiak, D.; Debita, G. Risk Management Using Network Thinking Methodology on the Example of Rail Transport. *Energies* **2022**, *15*, 5100. [CrossRef]
37. Favarò, F.M.; Nader, N.; Eurich, S.O.; Tripp, M.; Varadaraju, N. Examining Accident Reports Involving Autonomous Vehicles in California. *PLoS ONE* **2017**, *12*, e0184952. [CrossRef] [PubMed]
38. Baecke, P.; Bocca, L. The Value of Vehicle Telematics Data in Insurance Risk Selection Processes. *Decis. Support Syst.* **2017**, *98*, 69–79. [CrossRef]

39. Gnoni, M.G.; Saleh, J.H. Near-Miss Management Systems and Observability-in-Depth: Handling Safety Incidents and Accident Precursors in Light of Safety Principles. *Saf. Sci.* **2017**, *91*, 154–167. [CrossRef]
40. Hayward, J.C. Near-Miss Determination Through Use of a Scale of Danger. *Highw. Res. Rec.* **1972**, *384*, 25–34.
41. Heinrich, H.W. *Industrial Accident Prevention: A Scientific Approach*; McGraw-Hill book Company, Incorporated: New York, NY, USA; London, UK, 1931.
42. IAEA. Monitoring and Diagnosis Systems to Improve Nuclear Power Plant Reliability and Safety. In Proceedings of the Specialists Meeting, Gloucester, UK, 14–17 May 1996; p. 249.
43. IAEA. *Accident Monitoring Systems for Nuclear Power Plants*; International Atomic Energy Agency: Vienna, Austria, 2015; ISBN 978-92-0-110414-4.
44. Perramon, F. *Best Practices in Identifying, Reporting and Screening Operating Experience at Nuclear Power Plants*; International Atomic Energy Agency: Vienna, Austria, 2008; ISBN 978-92-0-111507-2.
45. ECCAIRS. 2 Central Hub | Home. Available online: https://aviationreporting.eu/en (accessed on 7 September 2022).
46. SRIS2. Available online: https://sris.aviationreporting.eu/safety-recommendations (accessed on 21 September 2022).
47. Report of the Working Party on Transport Statistics on its sixty-second session ECE-TRANS-WP6-2011. Available online: https://unece.org/DAM/trans/doc/2011/wp6/ECE-TRANS-WP6-161e.pdf (accessed on 16 October 2022).
48. Yannis, G.; Evgenikos, P.; Chaziris, A. CADaS-A Common Road Accident Data Framework in Europe. In Proceedings of the IRTAD Conference, Seoul, Korea, 16–17 September 2009; pp. 89–98.
49. EASA. *Annual Safety Recommendations Review*; European Aviation Safety Agency (EASA): Cologne, Germany, 2022; p. 42.
50. European Commission. *European Risk Classification Scheme*; European Commission: Brussels, Belgium, 2021.
51. European Railway Agency. Report on Railway Safety and Interoperability in the EU-2022. Available online: https://www.era.europa.eu/sites/default/files/library/docs/report_on_railway_safety_and_interoperability_eu_2022_en.pdf (accessed on 16 October 2022).
52. Miettinen, J. Nuclear Power Plant Simulators: Goals and Evolution. Available online: https://inis.iaea.org/collection/NCLCollectionStore/_Public/42/101/42101979.pdf (accessed on 16 October 2022).
53. Elliott, N.S.; Wanner, G.H. *ANSI/ANS 35 Standard for Nuclear Power Plant Simulators*; IAEA Symposium on the Training of Nuclear Facility Personnel: Nashville, TN, USA, 1985; p. 3.
54. Juris, M. Virtual Certification: State of the Art, Gap Analysis and Barriers Identification, Benefits for the Rail Industry. Available online: https://projects.shift2rail.org/download.aspx?id=e5be23b4-3990-426d-86b1-631e9034a881 (accessed on 16 October 2022).
55. Lu, L.; Padfield, G.; Podzus, P.; White, M.; Quaranta, G. Preliminary Guidelines for a Requirements-Based Approach to Certification by Simulation for Rotorcraft. Available online: https://dspace.lib.cranfield.ac.uk/bitstream/handle/1826/18454/certification_by_simulation_for_rotorcraft-2022.pdf?sequence=1&isAllowed=y (accessed on 16 October 2022).
56. EASA. *EASA CM-S-014*; European Aviation Safety Agency (EASA): Cologne, Germany, 2020; p. 55.
57. NASA. *Standard for Models and Simulations*; National Aeronautics and Space Administration: Washington, DC, USA, 2016.
58. EASA. *Certification Specifications for Aeroplane Flight Simulation Training Devices*; European Aviation Safety Agency (EASA): Cologne, Germany, 2018; p. 184.
59. *EN 14067-6:2018*; Railway Applications-Aerodynamics-Part 6: Requirements and Test Procedures for Cross Wind Assessment. Available online: https://standards.iteh.ai/catalog/standards/cen/a9acedac-3968-4b8c-a6cc-5a035c91e9b3/en-14067-6-2018 (accessed on 21 September 2022).