Managing Learning - What can shipping learn from road and air transportation for enhancing safety of MASS?

Anish Arvind Hebbar
Maritime Safety and Environmental Administration
(World Maritime University)
(Fiskehamngatan 1, 211 18 Malmö, Sweden)
{Corresponding author's email: ah@wmu.se}

"Yes, excessive automation at Tesla was a mistake... Humans are underrated."
@elonmusk on X, April 13, 2018

Abstract - Technological innovation within the maritime industry is resulting in rapid developments towards the commercial use of Maritime Autonomous Surface Ships (MASS), whether they are controlled remotely or are fully autonomous.

The International Maritime Organization (IMO) is working to ensure that the regulatory framework for MASS keeps pace with the rapidly evolving technological developments.

Within the IMO's regulatory framework, maritime safety is addressed through the SOLAS Convention and safety lessons are learnt through mandatory implementation of the Casualty Investigation Code.

Such learning and advancements in safety regulation through accident investigations is dependent on the size of dataset of marine incidents and accidents, and this methodology falls short in respect of new and emerging technologies such as MASS.

Under these circumstances, there is opportunity for maritime to learn proactively from the safety lessons in the aviation and road transportation sector so as to prevent the occurrence of similar accidents in MASS.

This paper examines select case literature on accidents involving aircraft and driverless cars in an attempt to discern way ahead on safety lessons for MASS and implications for marine accident investigation and risk management.

Keywords: autonomous ships; accident investigation; transportation safety; risk management; maritime.

INTRODUCTION

In June 2024, a goods train collided with a stationary train in India in an automated signalling territory resulting in 15 fatalities and 60 injured. [1]

In April 2024, a three-year safety investigation into Tesla's autopilot identified at least 13 fatal crashes involving autopilot [2], and as of June 21, 2024, California had recorded 721 autonomous vehicle collision reports [3].

On 11 April 2024, a Boeing 737 MAX-8 plunged inexplicably at a rate of 4,000ft a minute off the coast of Hawaii [4]. This incident is eclipsed by two air crash disasters involving the 737 MAX-8 within minutes of take-off, the first in October 2018, off Jakarta, Indonesia with loss of 189 lives and, second in March 2019 off Addis Ababa, Ethiopia with loss of 157 lives [5].

While other transportation modes grapple with accidents at various levels of automation, maritime has a series of major smart shipping projects directed towards maritime autonomous surface ships (MASS) supported by the European Union (EU), and large-scale national projects (Fig. 1).

Figure 1. Examples of projects for MASS

Project sponsor	Project examples
European Union	MUNIN, NOVIMAR, AUTOSHIP, PREPaRE SHIPS, AEGIS
Norway	NFAS
Netherlands	SMASH
Finland	One Sea
South Korea	KASS
Japan	DFFAS, MEGURI 2040

The International Maritime Organization (IMO) meanwhile conducted a Regulatory Scoping Exercise (RSE) to determine how to incorporate the safe, secure, and environmentally friendly operation of MASS into IMO instruments [6]. Results of RSE comprehensively identified the gaps in all the mandatory IMO instruments vis-à-vis MASS and made proposals for way ahead [7].

However, the RSE appears to be an inward-looking exercise focused on IMO instruments. Also, the experiences of Tesla with safety of autonomous vehicles and, Boeing with automated prevention of risk of stall in its MAX-8 series suggest that there are valuable lessons to be learnt by shipping from other autonomous transportation modes for enhancing safety of MASS. Further, several standards have been adopted by the industry in the wake of the transportation accidents which may be relevant for MASS.

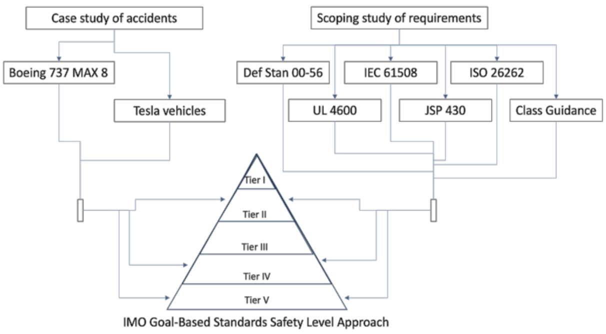
This paper, therefore, examines accidents and requirements in international instruments and standards, focusing largely on the air and road transportation sector, to derive lessons learnt for enhancing safety of MASS.

RESEARCH METHODOLOGY

The conceptual framework for the research (Fig. 2) comprised a combination of case studies of accidents and scoping study of requirements in international instruments and standards.

The case studies focused on two Boeing 737 MAX-8 air crashes and traffic accidents with autonomously driven Tesla vehicles.

Figure 2. Conceptual framework for the research



The scoping focused on requirements of Annex 13 of Chicago Convention, 1944 and, international standards Def Stan 00-56, IEC 61508, ISO 26262, UL 4600, JSP 430, and Class Guidance.

The lessons learnt were subsequently transposed to respective tiers of the IMO Goal-Based Standards Safety Level Approach (GBS-SLA) framework for enhancing safety of MASS.

RESULTS AND DISCUSSIONS

A. Case studies

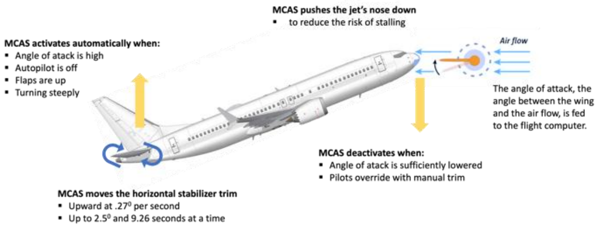
Case 1. Boeing 737 MAX-8 design safety [8][9][10]

Prima facie, the cause of the twin Boeing 737 MAX-8 crashes may be traced to continued modernization of a low-to-the-ground, legacy 737 design over fifty years up to the MAX-8 with larger engines to carry more passengers, rather than starting at some point with a clean design, presenting engineering challenges with unforeseen risks.

In order to achieve the needed 17 inches of clearance for the larger engines on the MAX-8, the pylons were extended farther forward and higher up. The change in the position of the engines increased the lift, creating a tendency for the MAX 8 nose to pitch up under certain circumstances.

The design counteraction to the nose-up tendency was the addition of the Manoeuvring Characteristics Augmentation System (MCAS), which orders the stabilizer to push down the nose if the angle of attack (AoA) got too high. For its decision-making, MCAS relies on data from two sensors which measure the AoA (Fig. 3).

Figure 3. Manoeuvring Characteristics Operating System



On the 2018 flight from Jakarta, the MCAS relied on a sensor that was erroneously reporting a high AoA when the plane was nowhere near a stall. Consequently, the MCAS software erroneously put the aircraft into a series of sharp dives. The pilots' best efforts to counteract the nose-down movements by pulling back on the yoke were of no avail. The aircraft was traveling so fast that when MCAS ordered the stabilizer to pitch the nose down it was a violent reaction that ultimately caused the jet to crash into the sea.

The sequence of events on the 2019 flight from Addis Ababa are less clear, but tracking data suggest that it also encountered sharp changes in its vertical velocity and at one point in its climb after take-off, lost 400ft of altitude. The flight dynamics of the two crashes are believed to be rather close.

Introduction of MCAS contributed to the MAX-8 crashes in several ways:

- the system acted only on the basis of AoA and does not factor-in air speed, which would better calibrate the pilots' reaction;
- the cockpit display system is not designed to identify failure of the AoA sensor which can allow the crew to abort take-off and prevent accident;
- by design, MCAS activates without pilot input to command nose-down so as to prevent risk of stalling of aircraft, and deactivates, if pilot trims aircraft manually;
- the design did not anticipate stabilizer effectiveness against MCAS higher Mach;
- MCAS was not mentioned in the flight crew operations manual (FCOM) that governs training; and
- there is no redundancy against an erratic AoA sensor. Also, there is lack of mitigation of risk of sensor malfunction.

System activation and calibration, display design, effectiveness of autonomously activated operational functions, redundancy of sensors, accuracy of operation manual, etc. are issues equally applicable to MASS.

Case 2. Tesla autonomous vehicle safety

Tesla receives real-world data from its global fleet; more than 9 billion miles of data pertains to autopilot engaged mode. Safety updates and enhancements are introduced over-the-air for cars in service. In 2023, Tesla's autopilot vehicles registered an average 5.65 million miles before a crash occurred, and between 2012-2022, approximately one Tesla vehicle fire event occurred for every 130 million vehicle miles travelled as opposed to one vehicle fire in the United States for every 18 million miles travelled. [11]

Yet, Tesla drivers died in crashes while autopilot was engaged and failed to detect obstacles in the road [12], including, police, fire and other emergency vehicles with flashing lights parked on roads. The overreliance on technology and failure of key automated function [13], applies equally to MASS in the maritime domain.

Literature [14] suggests that opacity of deep learning models impedes safety of autonomous driving systems. Challenges in deciphering autonomous software decision-making processes leads to uncertainty in predicting errors. System consistency is undermined by unpredictability due to inherent randomness. Debugging complexity inhibits prompt identification and rectification of issues. These challenges highlight the need for improved transparency and reliability in deep learning-based autonomous driving to ensure safe and effective deployment, regardless of the domain.

What lessons does Tesla autonomous vehicle case have for shipping looking to leverage artificial intelligence and automation? Humans can cope remarkably well with unforeseen situations and discrepancies between expected and actual events. On the other hand, adaptability of current advanced artificial intelligence algorithms is limited to variations within a restricted category of objects or events. Therefore, for the time being, scientists appear to be agreed on the fact that, "it is important to keep humans in the loop, …, in order to maintain an adequate level of safety in cases when the autonomous [vessel], operates outside its defined operational envelope," [15] e.g., aborting an operation.

B. Scoping of requirements

Scoping 1: Taxonomy for safety investigations

A review of taxonomy for safety investigations identified 3 “top”, 24 “medium”, and 89 “low” categories as an addition to the general traffic accident investigation items. The study proposed analytical tools and procedures that can consider all aspects of phase, target, entity, reconstruction, and task to identify systemic causes and consequences in respect of autonomous vehicles. The proposed items and system can be used to develop various autonomous driving accident scenarios. Also, based on the information, States could establish their roles and responsibilities to prepare for autonomous driving accidents. [16]

In respect of marine casualty investigation, the IMO reporting guidelines already seek more than 440 fields of data [17]. Is there still a need for a new and revised taxonomy for marine investigations? Indeed.

Firstly, continuous technological advancement of autonomous ships opens up the possibility of unexpected types of accidents, such as cyber-attacks by malware and ransomware. The existing casualty investigation system is limited in identifying the cause of these accidents.

Secondly, because of the limitations of the investigation such as a lack of sensor technology, accident investigation currently relies mainly on precrash, and in- and post-crash data are collected through accident reconstruction. However, advancement of automated detection technology and cooperative intelligent transport systems technology make it possible to systematically identify the cause of pre-, in-, and post-crash situations through various sensor technologies. Therefore, it is necessary to identify and integrate various technologies into the investigation system. There is also a need to identify additional and feasible investigation items based on various resources, including functional safety and real accident scenes.

Scoping 2: Reporting of collisions during testing

This study revealed at least one example of relevant best practice of national requirements for incident reporting during of testing of autonomous vehicles under development. California, U.S. requires manufacturers who are testing autonomous vehicles to report any collision that resulted in property damage, bodily injury, or death within 10 days of the incident. [18]

Scoping 3: Responsibility for casualty investigation

According to Annex 13 of the Chicago Convention which regulates safety investigations, the main responsibility for instituting an investigation lies with the State of occurrence. Further, the States of manufacture, design, operator, and registry should be formally notified of the accident and have each a right to appoint an accredited representative. This person has a right to follow the investigation in detail and has wide-reaching powers; such as to question witnesses and examine objects. The representative is also entitled to a draft of the final report before publication and to comment on it. If the comments are not taken into account, the investigating state has an obligation to append the comments to the final report.

All of these aspects merit consideration under the IMO Casualty Investigation Code in the context of MASS.

Scoping 4: Safety case

The requirement to present a satisfactory safety case to the industry’s regulatory body before operations can be permitted is fairly widespread across the nuclear, chemical, offshore, civil aviation and railway industries. [19][20]

In the U.K, the Defence Standard, Def Stan 00-56, is a single goal-setting for safety management across all defence activities. However, the actual safety case regime varies across operational domains, as specified in the relevant Joint Service Publication.

For e.g., Royal Navy ship safety cases are required by JSP 430 to show evidence that safety requirements have been met and that risk has been reduced to a level that is broadly acceptable or tolerable and ALARP.

For road vehicles, a safety case is required by ISO 26262:2018. U.K. has issued a “Code of practice” requiring a safety case and expects trialling organizations to develop an abridged public version of the safety case that should be freely available.

Standard UL 4600 developed by Underwriters Laboratories, addresses safety case for the safety of autonomous products. [21]

From the foregoing, there appears to be merit in requiring a safety case for the public in respect of autonomous ships to ensure awareness that safety evidence exists, and that limitations are transparent and described in an easy-to-understand way. [22]

Implementing the safety case approach may not come without challenges. While there is flexibility to set the rigour of the argument proportional to the risks involved, it can be very difficult to determine precisely what level of evidence is sufficient for a given system. It then becomes an engineering judgement that relies on the experience of those managing safety and their advisors thereby requiring a greater degree of competence from those involved in it as opposed to a prescriptive approach to safety, where managers can achieve compliance by following rules rather than making decisions.

Scoping 5: Functional safety

IEC 61508 is the mother of all international standards for functional safety (Fig. 4). IEC 61508-1 has the status of a basic safety publication according to IEC Guide 104. It covers aspects to be considered when electrical, electronic, or programmable electronic (E/E/PE) systems are used to carry out safety functions. It also enables the development of E/E/PE safety-related systems where international standards do not exist.

Figure 4. IEC 61508 application sectors

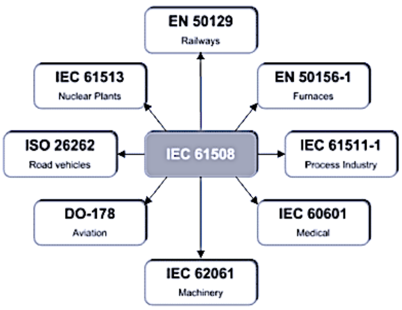


Figure 5. DO-178C Matrix of software levels [23]

Level	Failure condition	Number of objectives that must be satisfied	Number of objectives that must be satisfied with independence
A	Catastrophic	71	30
B	Hazardous	69	18
C	Major	62	5
D	Minor	26	2
E	No Safety Effect	0	0

DO-178C is the primary standard for certification authorities to approve all commercial software-based aerospace systems. It specifies the Design Assurance Level to establish the software levels (A-E), which in turn establishes the rigour necessary to demonstrate compliance [24]. Each software level requires a number of objectives to be satisfied, some with independence [25] (Fig. 5). Any software which commands, controls, and monitors safety-critical functions should achieve the highest assurance.

UL 4600, Standard for Safety for the Evaluation of Autonomous Products emphasises repeatable assessment of the thoroughness of a safety case. Its scope presents several possible takeaways for developing MASS standards including:

- extensive prompt lists;
- requirement for a goal-based safety case;
- assessments to ensure that the safety case is reasonably complete and well-formed;
- specifically requiring best-practice process activities and granular work products (e.g., hazard log); and
- compatibility with ISO 26262 and ISO 21448.

ISO 26262 addresses the need of electrical and electronic systems within road vehicles and applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic and software components.

To achieve functional safety, ISO 26262:

- supports the tailoring of the activities to be performed during the lifecycle phases, i.e., development, production, operation, service and decommissioning;
- adopts a risk-based approach to determine

Automotive Safety Integrity Levels (ASILs);
- uses ASILs to specify applicable requirements to avoid unreasonable residual risk;
- provides requirements for functional safety management, design, implementation, verification, validation and confirmation measures; and
- provides requirements for relations between customers and suppliers.

The safety integrity levels should be studied for application to MASS.

Scoping 6: Degrees of autonomy and human involvement per function

Scales developed to describe the level of autonomy for ships do not consider differences between vessel functions. For example, navigation is conventionally based on a high degree of human observations, analysis and decisions, while the machinery functions are to a high degree fully self- controlled and operating under supervision by the crew. A guideline could, therefore, use different categorizations for the degrees of automation of the navigation and engineering functions. Further, diversity of views prevails among classification societies and stakeholders, with each formulating their categorization of MASS depending on levels of automation and seafarers onboard (Fig. 6).

Figure 6. Conceptualisations of degrees of autonomy of MASS

Stakeholder	Conceptualization of MASS degrees of autonomy
DNV	multiple scales to measure navigational autonomy in ships, with five distinct levels (DNV GL, 2018)
LR	six distinct levels delineated (LR, 2016)
ABS	segmented into four tiers, depending on the extent of human-computer interaction (ABS, 2021)
BV	categorized into five levels, guided by confidence coefficient and level of autonomy in the technology used in the MASS system (BV, 2017)
KR	segmented into five levels, reflecting the data acquisition/analysis process. Decision-making, and Action (KR, 2022)
Sheridan	classified into ten distinct categories based on the ship's type, dimensions, operational zone, and state (Rolls-Royce, 2016)
IMO	RSE provides for four tiers of MASS (IMO, 2018)

There is a case for harmonization of standards across the maritime with a single global standard for MASS.

What can class rules learn from the road transportation sector? There is at least one example of technical guidance (DNV Class Guidance 0264, Sec.2.7) for marine navigation functions (in Sec.4) being based on a categorization established in the vehicle automation industry (Sec.4 [3]) with a simpler categorization for the engineering functions (Sec.5), distinguishing between systems providing automatic support and systems performing automatic operation. [26]

Scoping 7: System engineering and integration

The complexity of applying new technology for new operational concepts warrants a high focus on system engineering and integration activities (DNV Class Guidance 0264, Sec.8) [26]. The organization taking on the role as system integrator should be clearly identified in each concept qualification project. The system integrator should be responsible for the overall functional design and for verifying and validating the auto-remote functionality with focus on the operation and safety of the vessel.

CONCLUSIONS AND RECOMMENDATIONS

IMO has adopted goal-based approach to managing the safety risks for autonomous vessels. The goals and functional requirements in support of the application of GBS-SLA for MASS would be adopted via a voluntary MASS Code in the first instance. Detailed requirements are taking shape in the form of guidelines by classification societies. For verification of novel designs and applications for autonomous navigation, classification societies have adopted risk-based methods to ensure the same level of safety as traditional designs and applications.

If GBS-SLA is to be adopted and implemented, it would be critical for the functional requirements for MASS to be informed by lessons learnt from the autonomous road and air transportation sector. Tesla autopilot and Boeing MCAS serve as excellent case studies for identification of hazards that could lead some of the functional requirements on the basis of IMO’s Formal Safety

Assessment approach. The relevant risk control options could then be driven by the classification societies, national administrations and IMO.

There is yet another tier at the bottom of the GBS-SLA pyramid, Tier V, which constitutes the industry standards and best practices. This study envisages Tier V as the foundation of GBS-SLA in the absence of which the structure of GBS cannot exist. As a lesson learnt from autonomous road and air transportation sector standards ISO 26262 and DO 178, it is imperative that ISO standards are developed for the functional safety of MASS.

REFERENCES

[1] Press Trust of India, "15 dead, 60 injured as goods train rams into Kanchanjunga Express in West Bengal", 17 June 2024.

[2] The Guardian, "Tesla Autopilot feature was involved in 13 fatal crashes, US regulator says", 26 April 2024.

[3] DMV, "Autonomous vehicle collision reports", *Department of Motor Vehicles (DMV),* State of California, United States.

[4] A. Gabbat, "FAA investigates after Southwest plane drops to 'within 400ft' of Pacific Ocean", *The Guardian*, 16 June 2024.

[5] NTSB, "Investigation of Lion Air Flight 610 and Ethiopian Airlines Flight 302", *National Transportation Safety Board*, United States.

[6] IMO, "Strategic plan for the organization for the six-year period 2018 to 2023", London: *IMO,* 30th Assembly, Resolution A.1110(30), 8 December 2017.

[7] IMO, "Outcome of the Regulatory Scoping Exercise for the use of Maritime Autonomous Surface Ships (MASS)", London: *IMO*, Circular MSC.1/Circ.1638, 2021.

[8] Wikipedia, "Boeing 737 MAX groundings".

[9] J. Ostrower, "What is the Boeing 737 MAX maneuvering characteristics augmentation system?", *The Air Current,* 17 November 2018.

[10] R. Vartabedian, "How a 50-year-old design came back to haunt Boeing with its troubled 737 Max jet", California: *Los Angeles Times*, 15 March 2019.

[11] Tesla, "Tesla vehicle safety report", unpublished.

[12] N.E. Boudette, "Tesla Says Autopilot Makes Its Cars Safer. Crash Victims Say It Kills", New York: *International New York Times,* 7 July 2021.

[13] N.E. Boudette, "It happened so fast: Inside a fatal Tesla autopilot accident", New York: *International New York Times*, 19 August 2021.

[14] A. Chougule, V. Chamola, A. Sam, F. R. Yu, and B. Sikdar, "Comprehensive review on limitations of autonomous driving and its impact on accidents and collisions", *IEEE Open Journal of Vehicular Technology*, vol. 5, 2024, pp. 142-161.

[15] N.P. Ventikos, "MOSES - EU Horizon 2020 project, 3rd Autonomous Ship Reality online session", BS Group, 25 June 2024.

[16] H. Kim, H. Han, Y. You, M-J. Cho, J. Hong, and T-J, Song, "A comprehensive traffic accident investigation system for identifying causes of the accident involving events with autonomous vehicle", *Journal of Advanced Transportation*, vol. 2024, Issue 1, Article ID 9966310, 25 pp.

[17] IMO, "Revised harmonized reporting procedures – Reports required under SOLAS regulations I/21 and XI-1/6, and MARPOL, articles 8 and 12", London: *IMO,* MSC-MEPC.3/Circ.4/Rev.1, 2014.

[18] DMV, "Autonomous vehicle collision reports", *Department of Motor Vehicles (DMV),* State of California, United States.

[19] MoD, "Defence Standard 00-56 Safety Management Requirements for Defence Systems, Issue 4", 2007, Glasgow: UK Defence Standardization

[20] J. R. Inge, "The Safety Case, its Development and Use in the United Kingdom," 2007, Bristol, UK: Ministry of Defence.

[21] P. Koopman, "The UL4600 Guidebook. What to include in an Autonomous Vehicle safety Case", November 2022. Carnegie Mellon University.

[22] T. Myklebust, T. Stålhane, G. D. Jenssen and I. Wærø, "Autonomous cars, trust and safety case for the

public", 2020 Annual Reliability and Maintainability Symposium, Palm Springs, CA, USA, 2020, pp. 1-6.

[23] RTCA, "DO-178C Software Considerations in Airborne Systems and Equipment Certification", Annex A, *Radio Technical Commission for Aeronautics*, 2011.

[24] RTCA, "DO-178C Software Considerations in Airborne Systems and Equipment Certification, p. 116, *Radio Technical Commission for Aeronautics*, 2011.

[25] RTCA/DO-178C, "Software Considerations in Airborne Systems and Equipment Certification", p. 41, *Radio Technical Commission for Aeronautics*, 2011.

[26] DNV, "Autonomous and remotely operated ships", DNV Class Guideline DNV-CG-0264, Edition September 2021, pp. 20-21.