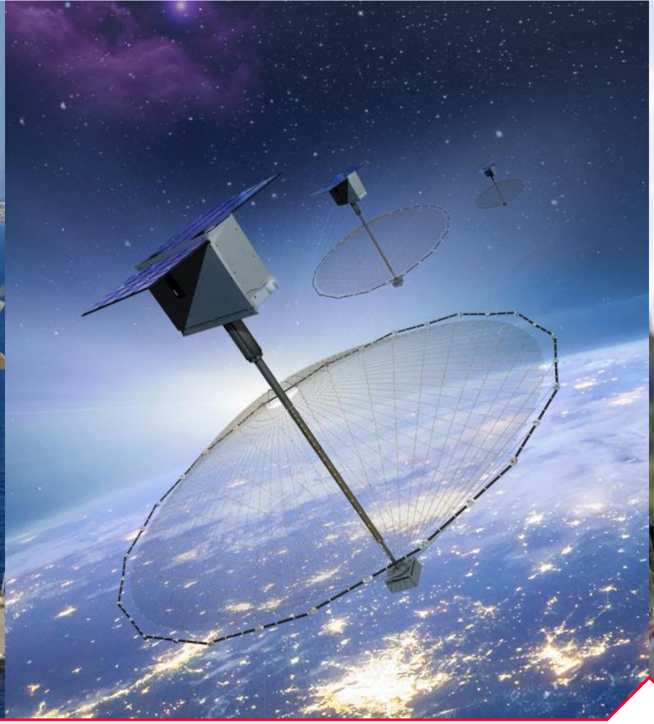



L3HARRIS™

THE CHALLENGES OF AUTONOMOUS PLATFORMS IN THE MARITIME DOMAIN

MASRWG Conference: MASS Regulation | Unlocking the Future of MASS

Tuesday 19th January

Danielle Berenbaum BEng(Hons)
Dr Giles Howard BSc(Hons) PhD MSaRS MIET

Introduction

Historically, Naval vessel power, propulsion and warfare was executed via a multitude of hydraulic, mechanical and electrical systems which were all locally controlled by operators. Overarching control of the vessel as a platform was through the arrangement of operators into hierarchical control structures.

Advances in technology has enabled vessels to be highly *automated* through solutions such as Integrated Bridge & Navigation Systems (IBNS), Integrated Platform Management Systems (IPMS) and Combat Management Systems.

These solutions provide a unified control interface to a multitude of systems, enabling the following benefits to be realized:

1. Sensor fusion
2. Lean manning
3. Automatic responses & behaviours

The next step is for vessels to transition from being automated to being autonomous. This is a significant step-change as the platform's own decision-making authority is increased, and the direct involvement of operators is reduced proportionally.

The aim of this presentation is to examine the development of autonomy frameworks & standards within the maritime industry and consider the challenges faced in achieving a common language to define maritime autonomy.

Assurance concerns for autonomous vessels

The increase in autonomous platforms poses several key assurance challenges, both to operators and regulators within the maritime domain:

How do we assure the safety of autonomous platforms?

→ This requires a paradigm shift as we care about safety in the presence of failures, as in traditional functional safety, but also ***safety in the absence of failure*****.** This is not well-covered by existing standards and techniques and is a novel issue for autonomous platforms.

How can we be confident in the cyber security of autonomous platforms?

→ This also requires a paradigm shift: autonomous platforms will make use of a variety of sensors and data sources; compromise of this data can cause accidents **as well as enable the autonomous platform to serve as a launchpad for further attacks.** Autonomous platforms therefore represent a more attractive target for an attacker to compromise and undermine.

How can we manage the interplay between security and safety on autonomous platforms?

→ Answering this question requires expertise from both the safety & security domains to come together on paradigms to ensure that both properties are meaningfully managed and conflicts resolved in a mutually beneficial way.

Autonomous platforms demand greater consideration to successfully manage safety & security

Addressing assurance challenges

The assurance challenges presented on the previous slide are complex and require a great deal of thought by stakeholders across the domain if they are to be overcome and facilitate rather than hinder progress.

One option to reduce or rationalise this level of effort is to look at trends from other domains, as they move to autonomous platforms. This allows us to identify key activities in the move to autonomy, such as:

- Is there a process that other domains have followed, with key milestones and outputs to define, classify and assure autonomy?
- Is that process potentially adaptable for use in maritime autonomy?
- Could an awareness of this process focus efforts and enable frameworks & standards to be achieved more rapidly?

We can look to other domains to make the autonomy journey more straightforward

Learning lessons from other domains

There are a number of domains, additional to maritime, where autonomous platforms are being increasingly deployed, including:

1. Aerospace
2. Rail
3. Automotive
4. Space

For the purpose of this presentation, **automotive** has been selected as the domain of choice due the following reasons:

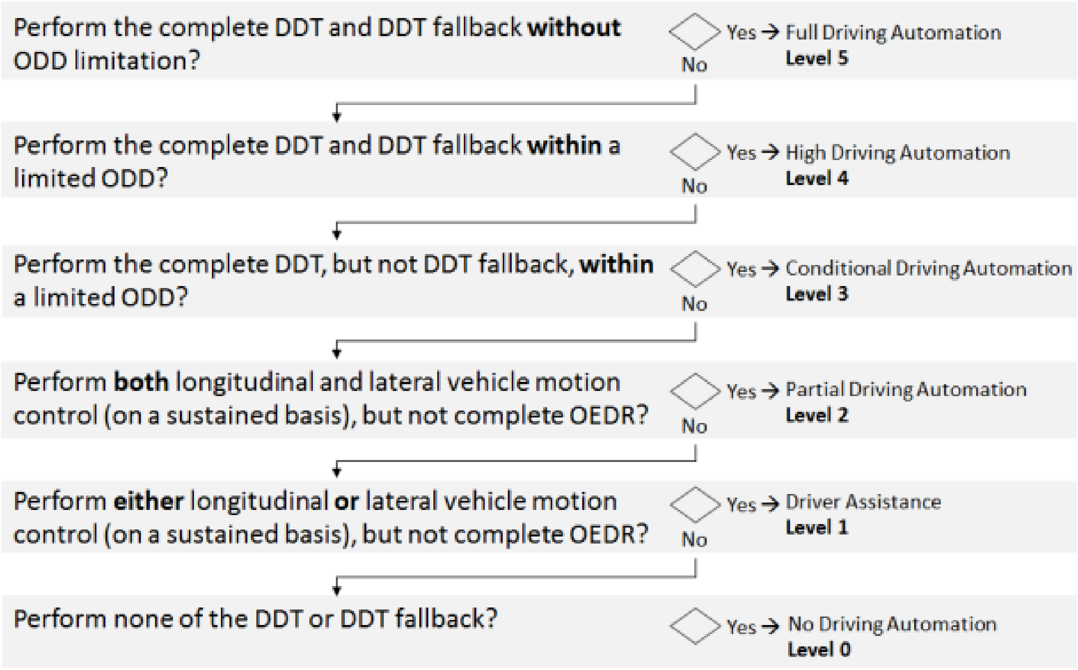
- The relative maturity of autonomy frameworks in the automotive domain, which enable platforms to be categorised and described in **a common language**.
- The failures of correct autonomous behaviour have similar consequences (e.g. collisions, loss of life).
- The increasing maturity of assurance standards in the automotive domain.

Automotive has been selected due to the advancements being made in autonomy

Autonomous automotive – a common language

The automotive domain has some key autonomy features which make it desirable for viewing it as a roadmap for classifying and assuring autonomy:

- A **single terminology** to define, describe and exchange information on levels of autonomy:
  - (e.g.) Operational Design Domain (ODD), Object Event Detection & Response (OEDR)
- An **algorithm** for classifying autonomous platforms into one of five levels of autonomy.
- **Assurance standards** have been developed to address autonomy that exists here-and-now, as well as future autonomy that is under development.
  - (e.g.) BSI/PAS 21448 and UL 4600 for safety.



This represents a *common language* which all stakeholders can use in developing, describing and assuring autonomous automotive platforms. This is embodied in the widely accepted SAE J3016 framework, which is used by OEMs, regulators and other stakeholders

Agreement on a common language has enabled the automotive domain to rise to the challenge of autonomy

Autonomous automotive – measuring success & safety

One significant area of research and practice within the developing field of autonomous automotive systems concerns **metrics.**

There are a set of metrics (RAND 2018) which are often considered in relation to any new automotive platform with autonomy features, such as:

1. **Miles per disengagement** (e.g. the operator overrides the autonomous system or the autonomous system cannot parse a situation and defensively hands back control to the operator).
2. **Cumulative mileage** under autonomous operation.
3. **Infractions** (i.e. failure to follow the rules of the road)
4. **Roadmanship** (the perception of the system being ‘a good driver’ and not creating hazards through sudden actions).

There has even been the suggestion that these metrics could culminate in a **‘driving test’ for autonomous platforms** prior to any system being certified for use on public roads.

In maritime, adoption of similar and domain-appropriate metrics could enable autonomous systems in maritime to get a ‘head start’ on any future regulatory or certification regime. This would also aid in providing that autonomous products & platforms are at least as safe as professional crew, who are subject to much more scrutiny and regulation that drivers of automotive platforms.

Robust metrics are essential to prove safety & suitability of autonomous platforms

Fraade-Blanar, Laura, Marjory S. Blumenthal, James M. Anderson, and Nidhi Kalra, Measuring Automated Vehicle Safety: Forging a Framework. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR2662.html. Also available in print form.

Learning lessons from automotive in maritime (1)

The IMO have developed a framework for MASS that defines four degrees of autonomy, with the lowest representing vessels with automated processes and decision support, and the highest involving fully autonomous vessels which require no human input or supervision (International Maritime Organization, 2020).

Table 1-2: Degrees of Autonomy (IMO)	
1	**Ship with automated processes and decision support.** Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated and at times be unsupervised but with seafarers on board ready to take control.
2	**Remotely controlled ship with seafarers on board.** The ship is controlled and operated from another location. Seafarers are available on board to take control and to operate the shipboard systems and functions.
3	**Remotely controlled ship without seafarers on board.** The ship is controlled and operated from another location. There are no seafarers on board.
4	**Fully autonomous ship.** The operating system of the ship is able to make decisions and determine actions by itself.

Competing frameworks are to be expected in the early phases of autonomous systems becoming a serious consideration however the lack of alignment and consistency between the frameworks within the maritime domain may act as a barrier to broader acceptance of autonomous vessels.

Table 1-4: Level of Control Definitions

Level	Name	Description
0	Crewed	MASS is controlled by operators aboard
1	Operated	Under Operated control all cognitive functionality is within the human operator. The operator has direct contact with the MASS over e.g., continuous radio (R/C) and/or cable (e.g., tethered UUVs and ROVs). The operator makes all decisions, directs and controls all vehicle and mission functions.
2	Directed	Under Directed control some degree of reasoning and ability to respond is implemented into the MASS. It may sense the environment, report its state and suggest one or several actions. It may also suggest possible actions to the operator, such as e.g. prompting the operator for information or decisions. However, the authority to make decisions is with the operator. The MASS will act only if commanded and/or permitted to do so.
3	Delegated	The MASS is now authorised to execute some functions. It may sense environment, report its state and define actions and report its intention. The operator has the option to object to (veto) intentions declared by the MASS during a certain time, after which the MASS will act. The initiative emanates from the MASS and decision-making is shared between the operator and the MASS.
4	Monitored	The MASS will sense environment and report its state. The MASS defines actions, decides, acts and reports its action. The operator may monitor the events.
5	Autonomous	The MASS will sense environment, define possible actions, decide and act. The Crewless Vessel is afforded a maximum degree of independence and self-determination within the context of the system capabilities and limitations. Autonomous functions are invoked by the on-board systems at occasions decided by the same, without notifying any external units or operators.

Consistent definition of the degrees of autonomy could encourage acceptance

Learning lessons from automotive in maritime (2)

On the topic of **assurance standards** within the automotive domain**,** standards have been developed along the following directions:

1. Standards to address contemporary autonomy, such as BSI/PAS 21448, enable OEMs and regulators to assure ‘current generation’ autonomy systems.
2. Standards to address holistic whole-platform autonomy, such as UL 4600, are much more rigorous than BSI/PAS 21448 and are intended to evolve as the domain learns more from the development of autonomous systems.

This is in contrast to maritime, where the currently available Codes of Practice and frameworks detail a minimum set of obligations involved in the development and use of maritime autonomous platforms.

While the existing codes of practice and frameworks will work for development of small autonomous platforms and test-beds, it creates challenges as autonomous platforms increase in size and complexity:

1. The level of engineering rigour required is undefined, which can risk substantial rework and delays.
2. A lack of formal standards with which to comply can complicate acceptance / sign-off of autonomous platforms.
3. Safety & security arguments essentially become highly bespoke.

These challenges will become more prominent as innovators seek to scale autonomous vessels in size, capability and complexity.

Maritime needs to focus on developing comprehensive assurance standards

Technology implications

Autonomous platforms in the maritime domain also generate a number of technology implications, **when contrasted with the automotive domain**:

1. Autonomous vessels lack high-bandwidth connectivity while away from shore and ports. This means they cannot depend on a reliable stream of information, and will require considerably more on-board intelligence to cope with low bandwidth / connection outages.
2. The response time of an autonomous vessel differs substantially to that of a modern connected car. The prime movers involved in control of a larger vessel may take on the order of seconds to respond to a change in demand, and may take minutes to actually meet the required demand. To this end, an autonomous vessel will need to predict the behaviour of other nearby vessels over a longer duration than is required of autonomous automobiles.
3. The reliability of an autonomous vessel, particularly one intended to be away from port for significant periods, will need to be considerably higher than is expected of automotive platforms. This is due to the fact that fault-free operation on the order of days and weeks is far in excess of what is expected of an automobile.

Maritime autonomy presents its own unique challenges

Conclusions

From comparing and contrasting the automotive and maritime domain on the topic of autonomous platforms, the following key points can be taken away:

1. The proliferation of maritime autonomy frameworks and Codes of Practice frustrate the ability of stakeholders to discuss, develop and classify autonomous maritime systems in a common language and from a single point of reference.
2. Through not having an agreed common language of autonomy, it is difficult to author standards which enable autonomous platforms to be assured and argued as safe & secure.
3. The technology implications for autonomous maritime platforms are clearly different in many regards to those of autonomous automotive platforms.

It is therefore suggested that the following steps are taken within the maritime domain to help enable the use of autonomous platforms:

1. The agreement between all stakeholders on a single framework which enables **meaningful description** of autonomous platforms, an accessible method to **classify autonomous platforms** as well as an agreed set of autonomy levels, both in terms of operator and autonomous decision-making involvement.
2. The development of standards and metrics to cover the safety and security of current-generation autonomous platforms, to ensure these can be safely and securely deployed.
3. The parallel development of horizon-scanning standards and metrics for assuring future (i.e. experimental) autonomous platforms.

L3HARRIS™