Unmanned and autonomous maritime – the challenges of assurance

Giles Howard*^ BSc(Hons) PhD MIET
Joe Chilcott* BEng(Hons) MSc CEng
Emma Parkin MEng (Hons)

** L3 MAPPS Limited, Bristol, UK. Subsidiary of L3Harris.*
^ Corresponding Author. Email: giles.howard@l3harris.com

Synopsis

The development of autonomous platforms in the maritime domain poses significant assurance challenges. While maritime as a domain has some unique facets, it can be helpful to consider and draw lessons from other domains where autonomy is better established and assurance approaches are more significantly developed. This paper first explores the development of the prominent autonomy frameworks and assurance standards in the automotive domain. This paper then identifies the commonalities and differences between the maritime and automotive domain. Finally, the paper reviews the current status of autonomy frameworks and standards in maritime autonomy and concludes that there is a need for a single, unified autonomy framework for the maritime domain, which will then enable assurance approaches and standards to be more meaningfully developed and achieved.

Keywords: Autonomy frameworks; safety; security; assurance; maritime autonomy

1. Introduction and context: Increasing automation of maritime platforms

Historically, naval vessels contained a multitude of distinct mechanical, electrical and hydraulic systems, which were controlled and managed through local control panels and positions, while overall coordination and control of the vessel was achieved through the communication between personnel in hierarchical command structures.

As technology has advanced, a number of products have been introduced to the market which enable control of multiple ship systems to be unified through a single control & monitoring interface. This includes products such as Integrated Platform Management Systems (IPMS), Integrated Bridge and Navigation Systems (IBNS) and Combat Management Systems. These systems can be generally titled as *automated systems*, as they permit repeatable tasks to be achieved through rulesets, thus reducing the task load on ships' personnel (Parkin & Chilcott, 2019).

The unification of control and monitoring functionality from a multitude of different *controlled systems* into a single *automated* system realises a number of advantages:

1. Sensor *fusion* can take place, where multiple, related information feeds originating from different systems can be pooled together, improving the situational awareness of the crew.
2. Lean manning can be realised, enabling ships to be crewed more lightly due to personnel not being required at local control interfaces at all times.
3. Automatic responses can be achieved, when the controlled systems are detected to have entered potentially hazardous states, thus improving vessel and personnel safety.
4. Multiple operator positions with access to the automated system can be provided, enabling reversionary control in the event of damage as well as facilitating further distribution of workload between personnel.

In addition to *automated* vessels, there has been an explosion in the number of *autonomous* vessels such as those demonstrated in Unmanned Warrior 2016 and Autonomous Warrior 2018, which do not possess human crews, but are platforms utilising sensors, coupled to a limited degree of artificial intelligence, to achieve operator-defined tasks and missions. It is therefore clear that the movement in the maritime domain is towards highly *automated* as well as *autonomous* platforms, and this introduces significant complexity in assuring these platforms from a transverse engineering perspective. This is best embodied in the Royal Navy's Digital and Data Plan, which

---

Authors' Biography

Giles Howard BSc(Hons) PhD; L3 MAPPS Limited – Following completion of his PhD, with a thesis focusing on blending formal methods with security & safety analysis techniques, Giles works as a Senior Safety Engineer and provides software safety expertise to IPMS solutions and projects.

Joe Chilcott BEng(Hons) MSc CEng; L3 MAPPS Limited – Whilst working for L3 MAPPS Limited over the past 8 years, Joe has had a number of Engineering Roles, starting as a Software Engineer, moving through to an integration specialist role and Principal System Design Engineer. He is currently the Design and Technology Manager for L3 MAPPS Limited working on solutions for the business development team and is fulfilling the Delegated Design Authority role for T31e IPMS.

Emma Parkin MEng (Hons); - Emma has previously been a technical sales engineer at L3Harris for 2 years. During this time, Emma has been seconded to the Royal Navy, DE&S and CMRE working on a range of maritime autonomy projects. She has a Master's degree in Chemical Engineering from the University of Sheffield.

 https://doi.org/10.24868/issn.2515-818X.2020.013

outlines a high-level strategy for increasingly autonomous and interoperable platforms and products (Royal Navy, 2019).

1.1. Taking inspiration from the automotive domain

As truly autonomous systems and vessels in the maritime domain are a rapidly evolving and relatively-nascent discipline, it is useful to draw upon the lessons learned from other domains where the movement towards highly-autonomous systems and platforms is more substantially underway. This paper has selected the automotive domain, for the following reasons:

1. The design and assurance scope for platforms in both domains involve continuous control, over a number of degrees of freedom, in order to successfully navigate from one location to another successfully.
2. Successful autonomous navigation of a platform is highly dependent on sensor fusion from a number of data sources to form a complete situational awareness of the environment, which is then the basis of all autonomous decision-making.
3. The consequences of failing to maintain adequate situational awareness, or taking incorrect action in response to correct situational awareness, are broadly comparable between the two domains, resulting in the potential for collisions with other platforms or the broader environment, and ultimately the loss of the platform itself.
4. The rapid development and deployment of these autonomous platforms mean that the presence of an experienced operator who can override incorrect behaviour of the autonomous decision-making cannot always be counted on.
5. The lack of an operator presence also has impacts on assumptions regarding maintenance and recovery in the event of partial or even total system failures.
6. The automotive domain has developed a number of autonomy-focused standards, which can provide inspiration to the development of similar standards in the maritime domain.

As can be seen, there are some commonalities which have driven the selection of automotive rather than other domains such as aerospace. The selection of another domain as a reference point enables the following activities to take place:

1. Similarities between domains can enable the identification of common expectations or requirements around autonomous systems, and therefore existing standards / regulations which address these expectations / requirements in one domain can potentially be applied to anther domain.
2. Differences between domains can highlight where additional assurance is likely to be necessary. As an example, an autonomous automotive platform may have a reasonable expectation of usage not exceeding 10 hours a day, while a vessel at sea may be depended upon for continuous availability of weeks at a time with no interruptions.
3. Differences between domains can also highlight where lesser assurance or argumentation may be warranted. For instance, the threat model for a seagoing vessel while at sea insofar as cyber security threats is likely to be perceived as lesser when contrasted with an autonomous automotive platform operating in a highly-connected environment, and so lesser assurance in this area may be tolerable.

2. Autonomy and assurance in the automotive domain

Autonomy in the automotive domain has been a highly contentious topic, with supporters of increased autonomy advocating for the economic, social and environmental benefits that can be realised through the automation of the humble car. Equally, critics of increased automation in the automotive domain point to the relative immaturity of the underlying technologies, as well as the ethical concerns associated with vehicles capable of advanced decision-making, as evidence that the path to autonomous cars and other vehicles should be highly scrutinised and carefully managed by regulators, manufacturers and other stakeholders.

While automotive is not a perfect parallel to the maritime domain, it is clear that a great deal of thought and understanding has gone into both defining autonomy and generating solutions to the assurance challenges posed by autonomous vehicles. This represents a rich body of work from which lessons can be drawn for maritime autonomy and caveated by the differences between the two domains.

This section therefore aims to:

1. Provide an overview of the benefits of autonomy frameworks to autonomous system stakeholders.
2. Provide a summary of the widely-adopted SAE J3016 Framework for understanding automotive autonomy.
3. Outline the challenges and solutions associated with assuring autonomous automotive platforms.

 https://doi.org/10.24868/issn.2515-818X.2020.013

4. Compare the automotive domain with the maritime domain, in order to identify commonalities and differences between the two.

2.1. Autonomy frameworks

When attempting to understand complex systems within a domain, it can be helpful to have a common reference point, which all parties and stakeholders can utilise to ensure that there is a shared understanding of the systems in question. This is best embodied in a framework, which defines key autonomy elements such as:

- The terminology associated with autonomous platforms in the domain.
- A process to enable the classification of autonomous systems into various levels or categories.
- A definition of the general capabilities and limitations of autonomous systems at each level.

Autonomy frameworks, such as those that exist within both the maritime and automotive domains, can serve as the foundation for more complex discussions that are required around autonomous systems, especially when these frameworks are widely adopted by stakeholders. These include:

1. Assurance expectations (in terms of safety, security, etc.) can be articulated on the basis of *level of autonomy* and provide manufacturers and regulators with clear guidance on what is acceptable.
2. Levels of autonomy can clearly define expectations in terms of both the *operational domain* and *fallback behaviours* of the autonomous solution and the involvement of operators.
3. By categorising autonomous systems into levels of autonomy, operators will develop an understanding of the capabilities and limitations of systems falling into a given level of autonomy.

There are significant challenges in achieving widespread acceptance of a given autonomy framework within a domain however, as the framework must be acceptable to all stakeholders, especially OEMs and regulators. Additionally, autonomous frameworks must be applicable to both current and next generation systems, or there is a risk that the framework will be left behind as systems advance in complexity or technology.

2.2. The SAE J3016 Framework for automotive autonomy

The dominant framework for autonomy within the automotive sector is produced by SAE and defines a progressive framework for classifying and understanding automotive autonomy; this is entitled *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* (SAE International, 2018). This taxonomy defines a number of key terms / concepts, which are key to understanding automotive autonomy; several major ones have been selected and are provided below:

- **Operational Design Domain (ODD):** The environmental and other operational conditions that an autonomy system has been designed to operate within, such as driving on a motorway or performing hands-off parking in a car park.
- **Dynamic Driving Task (DDT):** All real-time operational and tactical functions required to *operate a vehicle* in on-road traffic, excluding strategic functions such as trip scheduling and selection of destinations and waypoints.
- **Dynamic Driving Task fallback (DDT fallback):** The actions or activities that occur in the event of the system exiting the ODD or experiencing a performance-degrading failure. The DDT fallback may involve the user or autonomous system taking control and continuing the DDT or alternative placing the vehicle into a Minimal Risk Condition.
- **Object and Event Detection and Response (OEDR):** The activity of monitoring the environment of the autonomous vehicle (including both objects and events) and executing appropriate responses to objects and events as required.

The taxonomy provided in SAE J3016 utilises these key terms to construct 6 (six) levels of autonomy which are expected to exist within the automotive domain, based primarily on the relative contributions of the *driving automation system* and the *user*. A flowchart for the classification of a *driving automation system* is repeated as Figure 1.

 https://doi.org/10.24868/issn.2515-818X.2020.013

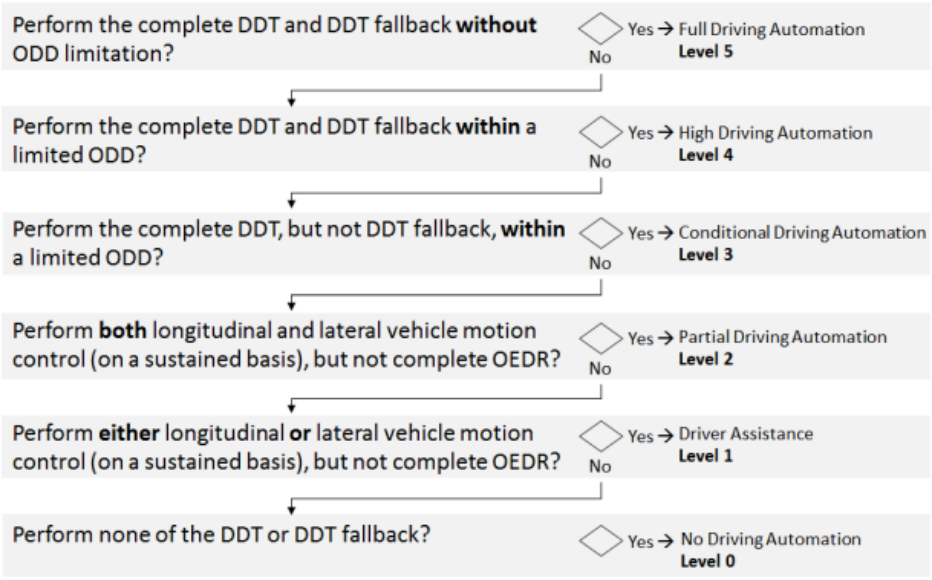

Figure 1: Decision criteria for classifying features of an autonomous automotive platform (SAE International, 2018)

It is clear from this flowchart that the greater the involvement of the driving automation system across the operational design domain (ODD), including the ability to perform DDT fallback successfully, the higher the level of autonomy that can be attributed to the driving automation system in question. An alternative way to view this flowchart is that increased levels of potential user intervention result in a system possessing a lower autonomy level.

The SAE J3016 taxonomy for characterising and understanding automotive levels of autonomy has achieved broad acceptance in the automotive domain, with key stakeholders such as the National Transportation Safety Board (NTSB) utilising it in accident reports (National Transportation Safety Board, 2017) and by OEMs such as Daimler (Daimler AG, 2019) and Siemens (Siemens PLM Inc, 2018).

2.3. Challenges and solutions in assurance of automotive autonomy

The automation of the automobile creates a number of regulatory and transverse engineering challenges, of which safety and security are jointly first amongst equals. To address these challenges, there has been significant effort dedicated to the development of safety and security standards for automotive autonomy, and this section dedicates some

 https://doi.org/10.24868/issn.2515-818X.2020.013

2.3.1. ***Safety***

Autonomous automotive systems present a new safety assurance challenge: ensuring that the system is safe in the *absence of a failure* and where continued safety of a platform requires accurate, precise and continuous situational awareness. This runs contrary to conventional functional safety engineering which concerns itself primarily with ensuring safe operation in the event of a failure. The majority of safety standards are therefore are designed to reduce the impact of both systematic and random faults and failures on the ability to achieve the intended safety behaviours of a safety-related or safety-critical system, and this is the problem that standards such as IEC 61508 or ISO 13849 were developed to address.

One standard which has been developed explicitly to deal with automotive autonomy assurance is Safety of the Intended Function (SOTIF) and has been codified in ISO/PAS 21448 (International Organization for Standardization (ISO), 2019). This standard provides measures and techniques, which can be applied to the design, verification and validation phases of an automation system lifecycle to account for the limitations of current technologies utilised to enable automation of automotive platforms (Schnellbach & Griessnig, 2019). This includes:

- Identification and evaluation of hazards caused by the Intended Functionality.
- Identification and evaluation of so-called Triggering Events, which are pre-events that lead into a hazard.
- Identification and evaluation of so-called Countermeasures, which are any choices taken in order to reduce risk, such as improving performance of key components (such as sensors) or limiting functionality to situations where performance of key components is sufficient.
- Ensuring that verification occurs against high-fidelity, realistic scenarios within and on the edges of the ODD, including varying elements such as weather and other environmental conditions, taking into account previously-identified hazards and triggering events.

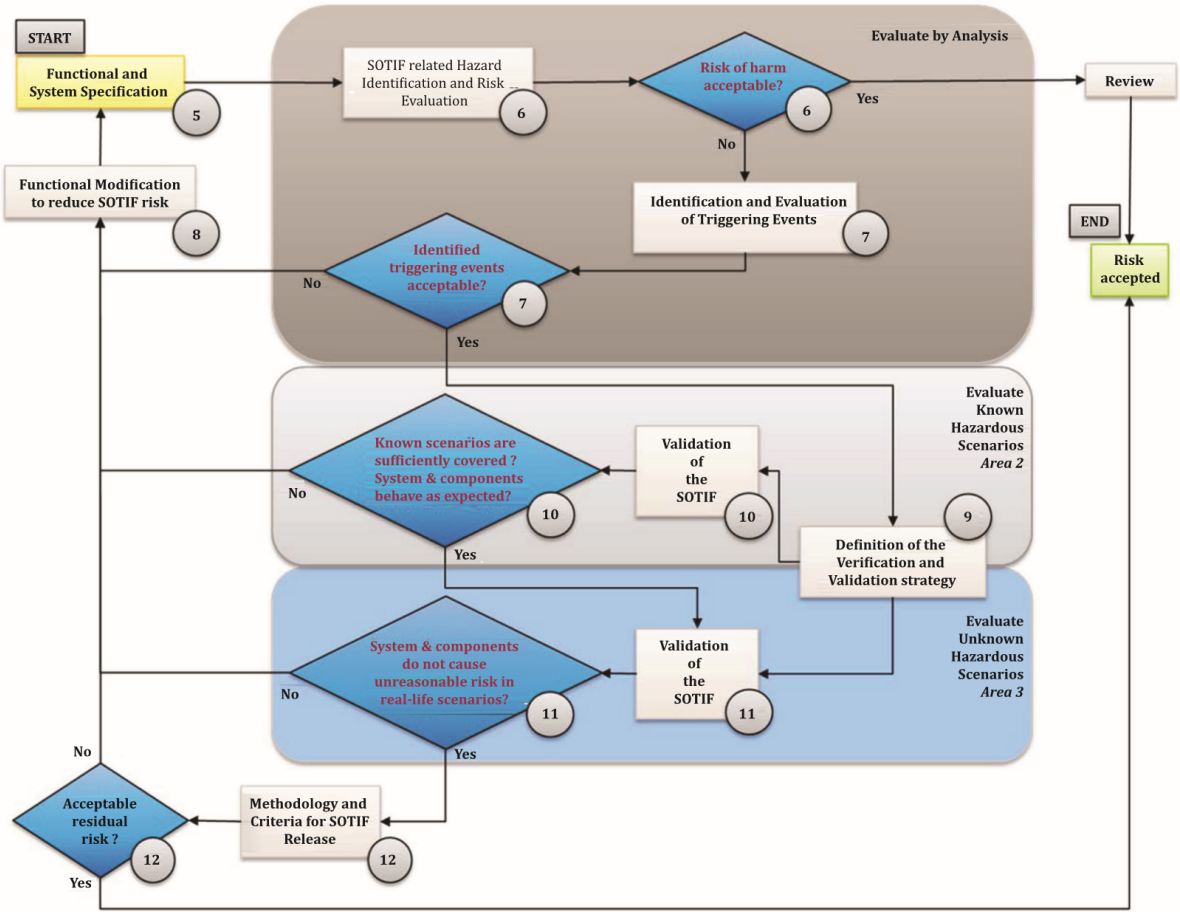

Figure 2: Activity flow from ISO/PAS 21448 (International Organization for Standardization (ISO), 2019)

 https://doi.org/10.24868/issn.2515-818X.2020.013

One major characteristic of ISO/PAS 21448 is that it is explicitly intended for use in assurance of Level 1 and Level 2 systems on the SAE J3016 autonomy scale. It therefore only applies to systems for which there is still a receptive, alert driver who can override the behaviour of any driving automation system and/or take control of the vehicle at short notice. This is likely due the significant amount of development of Level 1 and Level 2 systems that is currently taking place by manufacturers in the automotive domain and so the standard sought to provide a clear articulation of assurance measures that can be taken to assure these systems.

A further recent standard in the automotive domain is that of UL 4600 (UL, 2020) which, instead of seeking to bolster the V-lifecycle associated with autonomous automotive platforms, targets the safety cases associated with these platforms and provides a comprehensive and systematic set of rules and requirements that these safety cases must meet, such as:

- Requiring that the safety argument includes a comprehensive fault model, capturing the credible failure modes of all safety-related items, components, features or other aspects that make up the autonomous platform.
- Requiring that initial risk and risk criticality levels are recorded for each hazard in a Hazard Log.
- Requiring that safety-related communication features that are relevant to humans are identified, in both active and passive forms.

UL 4600 aims to remain technology-neutral, and therefore be as broadly applicable to as many autonomous automotive platforms as possible. UL 4600 emphasises the use of independent assessors in judging the effectiveness of a safety case and it is intended that this use of independent assessors will inform subsequent editions of the standard as they can define further rules and requirements to address common pitfalls in extant safety cases. Through imposing a comprehensive ruleset upon safety case authors, based on lessons learned from both successful and unsuccessful autonomous automotive platforms, UL 4600 seeks to provide a robust framework for the development of autonomous automotive platforms (Koopman, et al., 2019).

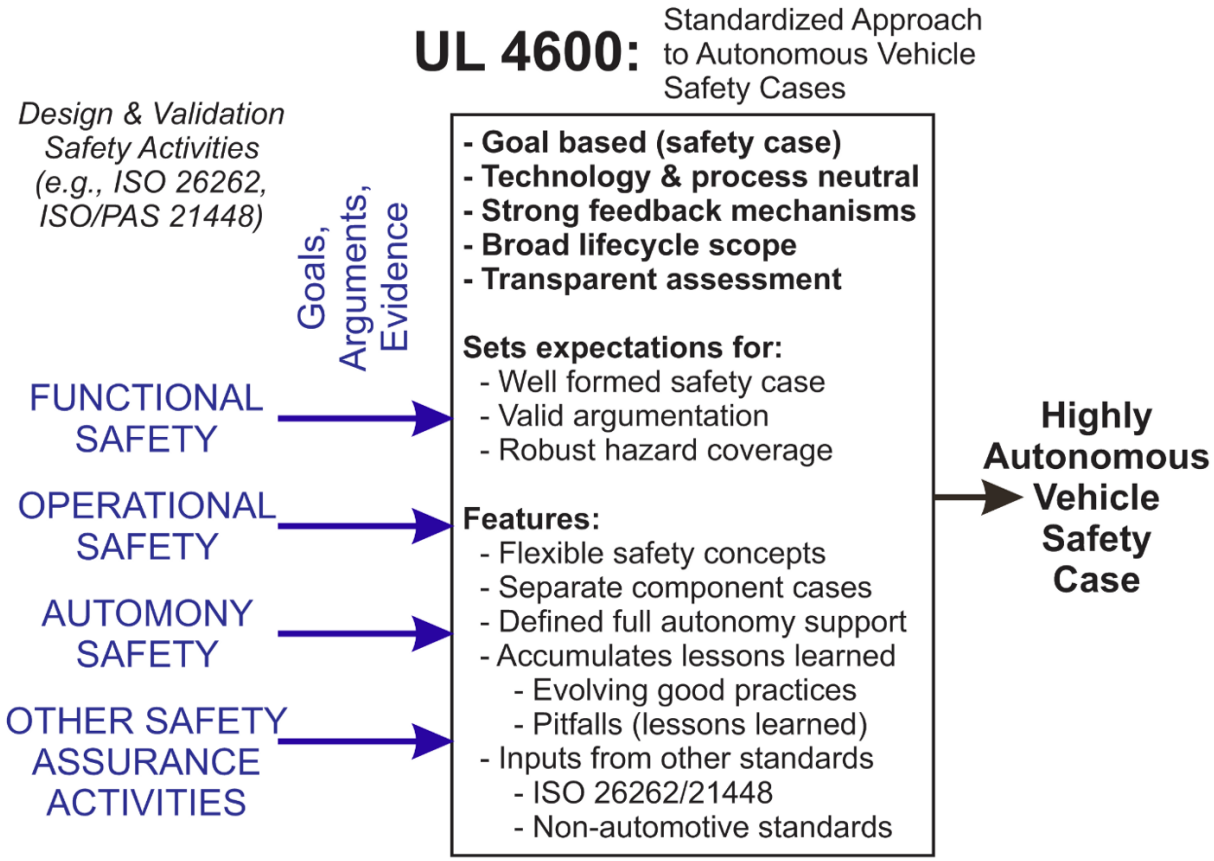

Figure 3: UL 4600 approach to delivering a robust, systematic safety argument for autonomous vehicles (Edge Case Research, 2019)

The limitation of UL 4600 is that the significant body of rules and recommendations are likely to be viewed as excessive for the development of systems falling on the lower end of the J3016 autonomy levels, and in these circumstances, it is likely that the application of ISO/PASS 21448 would be viewed more favourably by

 https://doi.org/10.24868/issn.2515-818X.2020.013

manufacturers. This will likely limit UL 4600 to the development of higher-autonomy systems such as Level 3 systems and above, where the reduced role of the human driver will require a rigorous and substantial safety case to justify.

As has been shown, there are two major standards used for safety assurance of autonomous automotive systems, with each having a clear niche as to which levels of autonomy they are intended to address. ISO/PAS 21448 covers the immediate issues of regulators and manufacturers when it comes to automotive platforms making use of Level 1 and Level 2 autonomy systems, while UL 4600 takes a systematic and holistic approach to assurance of autonomous systems at Level 3 and beyond.

While this provides coverage of all autonomy levels within the automotive domain, this approach does mean that stakeholders are required to be familiar with two separate standards and the natural progression from one level of autonomy to another may involve suddenly having to utilise a brand new and more-complex standard. This is less than ideal so a single autonomy standard with a dynamic set of rules that are required or not required based on the system's autonomy level may be more effective and enable broader adoption of the standards in question.

2.3.2. ***Security***

Security in automotive autonomous platforms will require an extra degree of assurance beyond that of the current cybersecurity standards, due to the consequences that a security breach may have on the continued, safe functioning of an automotive platform. More concerning still, an automotive platform infected with malware becomes a useful, dynamic asset to an attacker as it could be used to spread malware further to other autonomous platforms. This is due to the high degree of connectivity that modern automobiles possess, such as remote updates and mobile applications, which enable functions of the car to be controlled by the owner.

This section will focus on the two major standards in automotive cybersecurity: BSI PAS 1885 and ISO/SAE 21434. The purpose of these standards is to provide a systematic approach to security engineering of automotive platforms, rather than viewing cybersecurity as a bolt-on, and are not exclusive to autonomous automotive platforms. Nonetheless, these standards represent the state-of-the-art in terms of cybersecurity standards, which can be utilised for all automotive platforms, including autonomous ones.

BSI PAS 1885 is a published standard, entitled '*The fundamental principles of automotive cyber security',* which provides a high-level set of definitions and concepts that are key when approaching cybersecurity from an automotive perspective. It additionally articulates requirements for each lifecycle stage as to what activities should be undertaken in addition to what evidence should be captured associated with these activities.

ISO/SAE 21434 is currently under development and aims to provide a whole-lifecycle approach to cybersecurity, including undertaking threat analysis and risk assessment to derive security requirements (Schmittner & Macher, 2019). The major contributions of draft versions of this standard (Schmittner, et al., 2018) can be summarised as follows:

1. The definition of an iterative, whole-of-system-life risk management process for identifying, assessing, mitigating and monitoring cybersecurity risks associated with a platform or product.
2. The definition of a V-model lifecycle, based on ISO 26262, that takes into account cybersecurity activities which should be undertaken in each phase of the lifecycle of a system.
3. An articulation of how cybersecurity management should be undertaken within manufacturers, providing guidance on how OEMs should structure themselves to ensure good cybersecurity practice and oversight at all levels.

While both of these standards are useful, they are not specific to autonomous platforms and therefore lack an additional dimension of assurance necessary for these platforms. This is because an autonomous platform will possess a variety of sensors and other information feeds in order to derive situational awareness. It is this situational awareness that is required for effective decision making. The security of these information feeds is therefore critical to maintain the integrity and correct behaviour of autonomous platforms.

To address this shortfall, the government-funded 5StarS consortium consisting of members such as MIRA, Ricardo, Roke and Thatcham Research are in the process of developing an assurance framework building upon existing standards efforts such as ISO/SAE 21434 to enable the security assessment and assurance of highly-connected automotive vehicle platforms with the aim of building customer trust in these platforms (5StarS Consortium, 2019). As connected vehicles are a precursor technology to highly-automated vehicles, it is clear that this represents a significant starting point on security assurance of autonomous automotive platforms.

 https://doi.org/10.24868/issn.2515-818X.2020.013

2.4. Commonalities and differences to maritime autonomy

A comparison between maritime and automotive autonomy can be made on the basis of four of the autonomy characteristics as defined in SAE J3016:

1. The Operational Design Domain (ODD)
2. The Dynamic Driving Task (DDT)
3. The Dynamic Driving Task fallback (DDT fallback)
4. The Object and Event Detection and Response (OEDR).

This section will aim to outline the commonalities and differences between these four major facets of autonomous platforms in both the maritime and automotive domain in order to highlight where technological and assurance challenges may exist.

2.4.1. The Operational Design Domain (ODD)

The Operational Design Domain refers to the *environmental* conditions that an autonomous platform is developed to be able to perform its decision-making authority and responsibilities. For both maritime and automotive domains, autonomous platforms have the following considerations for their operational design domains:

1. Weather conditions, which can degrade the performance of sensors, as well as affecting the underlying performance of the platform's propulsive components.
2. The availability of an environmental profile such that the autonomous platform knows what the expected environmental conditions should be, and can therefore take mitigating decisions if the environment is in a worse state than expected.

There are also some nuances between the automotive and maritime domains in terms of environment:

1. The maritime environment has to contend with obstacles on the sea bed which can be moved by currents and tides. Automotive platforms do not have to contend with obstacles of this type in the same way, as any significant obstacles on the road are removed quickly by the appropriate agency.
2. The presence of currents and tides means that the environment in terms of the waterways are not as consistent and therefore can vary significantly depending on the time of day. The closest parallel for this in the automotive domain is the degradation of road surface, however, this occurs over a significantly longer period of time.

None of these considerations are entirely novel, as existing technologies handle these aspects on existing manned vessels with minimal operator input. It does highlight that autonomous vessels will need to be capable of handling more significant variations in the environment that can perhaps be expected on roadways.

2.4.2. The Dynamic Driving Task (DDT)

The Dynamic Driving Task (DDT) refers to the total set of actions required to be taken by the autonomous platform to get from a starting position to a defined end position. This includes corrections required due to impassable obstacles, redirections due to traffic, management of propulsion, etc. For both maritime and automotive domains, autonomous platforms have the following considerations for their dynamic driving task:

1. Autonomous platforms need to continually review the current navigation path, and take into account any corrections required in terms of e.g. propulsive power and braking so they remain under control and are safe at all times.
2. Autonomous platforms need to apply steering adjustments sufficient that they maintain their navigational path without exiting the intended transit ways (waterways or roads) that make up the intended route.
3. Autonomous platforms also need to ensure they have sufficient endurance (in terms of fuel and other consumables) over the duration of the navigation or the platform risks being stranded and dependant on external assistance to continue.

There are once again some nuances between the automotive and maritime domains in terms of the DDT:

1. The degrees of movement usually considered in the automotive domain are longitudinal and lateral movements, however, maritime vessels have more degrees of freedom than automotive vessels and so an autonomous maritime platform needs to be capable of controlling movement across more total axes. This is not a significant issue as modern dynamic positioning systems in the maritime domain are capable of compensating for vessel movements in all axes.
2. Automotive platforms are generally required to undertake the DDT in bursts of several hours, while an unmanned cargo vessel or similar may need to have a DDT that spans multiple days or weeks of

 https://doi.org/10.24868/issn.2515-818X.2020.013

continuous operation. This places a higher reliability burden on the autonomous maritime system, as uninterrupted performance of the DDT, without crew being available to service/maintain the system, will be required.

3. The tolerance for momentary errors or uncertainties is higher in maritime than in the automotive domain. An autonomous automotive platform which hesitates on a busy motorway at high speed for several seconds risks a collision with another automobile. An equivalent hesitation of several seconds is unlikely to make a significant impact on autonomous vessels, particularly when for significant periods of the voyage, a vessel will have significant separation from all other vessels.

2.4.3. The Dynamic Driving Task fallback (DDT fallback)

The Dynamic Driving Task fallback is the fallback behaviour in the event of a performance-degrading failure in the autonomous platform. Equally, the DDT fallback can occur when an autonomous platform enters a scenario outside of its Operational Design Domain. The DDT fallback may result in an operator being required to take control of the platform or a lower autonomous capability to continue to execute. For both maritime and automotive platforms, the following considerations exist for fallback behaviours:

1. In high-traffic areas, an autonomous platform which is no longer capable of fully featured autonomous operation will need to fallback to some mode of operation where it does not put any other platforms at risk. This may involve operating more slowly, deferring to other platforms more frequently, and generally placing itself out of any challenging or complex situations.
2. Where skilled operators can be depended on to respond to a fallback control request on short notice, the autonomous platform will need some method to alert and confirm with the operator that they are in a position to take meaningful and complete control of the platform before the autonomous decision-making ceases operation.
3. Where skilled operators are not available to take control of the autonomous platform, the platform may need to cease operation entirely, in which case the autonomous decision-making will need to identify a suitable, safe location in which to stop on relatively short notice until repairs can occur or operators are available to take control.

There are some material differences between the maritime and automotive domain on the issue of DDT fallback:

1. Existing behaviours such as dynamic positioning currently exist for maritime platforms and are capable of keeping a vessel in a fixed position with minimal operator input for long durations. This means that the DDT fallback for a maritime platform could be to engage a dynamic positioning system until an operator was available. For contemporary automotive platforms, fully featured self-driving capability is not possible, and so modern automotive platforms are guaranteed to have an operator behind the wheel.
2. Waterways are considerably larger and less congested than roadways, and so the response time required before an operator must take control of an autonomous maritime platform could be considerably longer (i.e. on the order of minutes rather than seconds) compared to automotive.

2.4.4. The Object and Event Detection and Response (OEDR)

Object and Event Detection and Response (OEDR) is an umbrella term for all activities which are required to detect, classify and respond to the presence of objects and events during autonomous operation. For both maritime and automotive platforms, the following considerations exist for OEDR:

1. Autonomous platforms will need to correctly identify other vehicles and objects in their path in sufficient time to either take evasive action or to adjust their current propulsion to ensure collisions do not occur.
2. Autonomous platforms will need to anticipate the behaviour of previously-identified vehicles and objects in order to ensure they do not become hazardous in the near future. This will involve tracking and predicting the behaviour of objects for an appropriate length of time.
3. Autonomous platforms will need to be capable of undertaking OEDR across the entire environmental conditions specified in their Operational Design Domain. This will likely require a number of sensor technologies working in concert, so that a change in the environment which degrades one type of sensor technology does not prevent the platform detecting and responding appropriately to objects and events.

There are some material differences between the maritime and automotive domain on the issue of OEDR:

 https://doi.org/10.24868/issn.2515-818X.2020.013

1. The ability of an automotive platform to stop, even at high speeds, can be measured in seconds during good weather conditions (i.e. dry surface with responsive brakes). For a maritime platform, however, this response may be measured more appropriately in the order of minutes. This means that the 'response' portion of OEDR for a maritime vessel is unlikely to include stopping, and will instead need to involve more complex evasion or avoidance behaviours.
2. Likewise, the ability of the autonomous decision-making in a maritime platform to predict the behaviour of nearby vessels will need to be projecting movement of the vessel further into the future to determine if collisions are probable and therefore take evasive manoeuvres. For an automotive platform, this is not practical given how rapidly cars can change direction compared to maritime platforms, where decision-making is measured in milliseconds. This being said, smaller maritime vessels are likely to require faster decision-making than larger vessels such as tankers.
3. Finally, sensor technologies for autonomous cars tend to focus on radar and LIDAR as major technologies. Maritime vessels will need to fuse a number of data sources, including AIS and ECDIS and radar - as well as potentially more complex technologies such as sonar – to form a full picture of the environment in order to respond appropriately to events and objects in proximity to the vessel.

2.4.5. Technology implications

The implications of much of the preceding section for naval technologies are that an autonomous vessel will need to be able to fuse a larger number of data sources than current automotive platforms are required to. This is not a novel challenge in the maritime domain, with systems such as dynamic positioning already pulling together a number of measurement systems and using this to inform a network of propulsive elements to maintain a fixed position or course. It does however represent a net increase to the amount of interfacing and data interchange which is currently required of automotive vessels. Furthermore, modern technologies have safety cases that are dependent on the presence and expertise of human operators, which is no longer a certainty when dealing with autonomous vessels.

It is also clear that the response time required of automotive platforms, necessitating a significant amount of parallelised processing power, is much faster than what is required in maritime vessels in order to truly achieve autonomy. However, this is traded off against the need for autonomous vessels to operate error-free over longer durations, potentially without crew, and so will likely necessitate a higher degree of redundancy and diversity to ensure that the autonomous vessel is not disabled by the failure of a single processing node.

Connectivity is also a greater challenge at sea than it is on land. While satellite systems are widely used in the maritime domain, these are more expensive to maintain and utilise to receive real-time data exchanges, and so an autonomous vessel will need an order of magnitude more stored data available when compared to automotive platforms. An autonomous car will be able to utilise technologies such as 5G to constantly request data as it operates, and so localised data storage demands are significantly less.

Finally, the underlying data model of the autonomous automotive platform is considerably simpler than that of a modern maritime vessel. A modern car may contain on the order of 100 control units, all with a distinct responsibility, but the digital representation of a modern vessel possesses more degrees of freedom and vastly more signals from plant equipment and sensors. This may result in a higher processing burden to continually refresh and maintain this model than is currently required by modern automobiles, with the natural trade-off that these updates can be less frequent due to the lower response time requirements of a vessel at sea.

3. Autonomy and assurance of maritime platforms

This paper has dedicated a significant discussion to automotive autonomy, the autonomy frameworks and assurance standards, which exist to support this emerging set of technologies and approaches. The intent of this focus was to highlight the strides that have been taken in developing a body of knowledge to enable automotive autonomy to not only be realised successfully, but also to be realised in a way that is both safe and secure.

Turning now to the topic of maritime autonomy, it becomes possible to identify the steps that have already been taken by key stakeholders in the domain. Additionally, it becomes possible to identify the lessons learned from automotive autonomy and how these can provide a 'roadmap' of the remaining work still required within the maritime domain, in order to ensure that autonomy is realised effectively and in a manner that can be successfully assured.

 https://doi.org/10.24868/issn.2515-818X.2020.013

3.1. Frameworks for maritime autonomy

One of the most comprehensive frameworks for maritime design is the Lloyd's Register ShipRight procedures. These procedures provide guidance and articulate a basic standard for all manner of vessels to ensure that all transverse engineering considerations are included and achieved throughout the life of the vessel (Lloyd's Register, 2007).

Within the ShipRight procedures are two autonomous frameworks which can be applied to maritime autonomy as outlined in this paper:

1. The *Design Code for Unmanned Marine Systems* outlines seven potential levels of autonomy which range from AL0 (no autonomy) to AL6 (fully autonomous). This framework is explicitly intended for systems that operate without any personnel on board during normal operations (Lloyd's Register, 2017).
2. The *Procedure for assignment of digital descriptive notes for autonomous and remote access ships* outlines six potential levels of autonomy which range from AL0 (no autonomy) to AL5 (maximum autonomy). This framework is intended for 'digital ships' and is therefore intended to cover highly-connected as well as autonomous ships (Lloyd's Register, 2019). This framework also explicitly includes vessels which are manned.

Both frameworks provide a general set of expectations and steps which will be carried out by Lloyd's in assessing autonomous vessels, based on a risk-based assessment of the functionality. These represent an equivalence to the SAE J3016 framework in the automotive domain, and due to originating from Lloyd's Register, have a similar prominence within the domain.

Additionally, the IMO are developing a framework for Maritime Autonomous Surface Ships (MASS) that will define 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). This work is in the 'scoping' phase, with the IMO producing an interim set of guidelines for trials of MASS platforms (International Maritime Organization, 2019).

It is clear that there has been a proliferation of competing frameworks for framing and understanding the varying levels of autonomy in the maritime domain. While this is to be expected in the early phases of autonomous systems becoming a serious consideration in a domain, the lack of alignment and consistency between the frameworks within the maritime domain may act as a barrier to broader acceptance of autonomous vessels.

OEMs, regulators and other stakeholders require a single, broadly-accepted framework through which they can classify and understand autonomy, as well as the assurance expectations that are associated with the varying levels of autonomy. Once this has been achieved, as is seen with the SAE J3016 automotive framework, the focus of the conversation can switch away from the classes of autonomy and towards developing assurance approaches for satisfying safety, security and other regulatory obligations.

3.2. Safety and Security

The current status of safety in maritime autonomy is that OEMs are utilising conventional functional safety standards, such as IEC 61508 and ISO 13849, as part of developing autonomous systems. Cybersecurity can be considered to be a developing area of focus for maritime stakeholders, with bodies such as the IMO producing broad guidelines which recommend the usage of standards such as ISO 27001 or the NIST framework for all vessels, regardless of autonomy level (International Maritime Organization, 2017).

Additionally, frameworks for autonomous systems such as the interim guidance published by the IMO and the Lloyd's Register ShipRight series have articulated expectations that risk management, safety analysis and cybersecurity assessment are proactively addressed when developing and deploying autonomous maritime platforms.

While this represents a useful initial position, the lessons learned from automotive autonomy indicate that a major dependency for developing safety and security standards is the agreement of a single, all-encompassing autonomy framework. From this point, several activities will naturally occur:

1. Standards that cover the state-of-the-art, both in terms of technologies and use-cases, will be developed. These will cover the "lower" levels of a standardised autonomy framework, and will aim to provide guidance and requirements that address the immediate problems of assuring autonomy for

 https://doi.org/10.24868/issn.2515-818X.2020.013

technologies being rapidly adopted and pressed into service. This is best exemplified through the development of ISO/PAS 21448 in the automotive domain, which addresses the immediate issue of assuring Level 1 and Level 2 automotive autonomy technologies, such as lane-keeping, city braking, etc.

2. Standards that are forward-looking and aim to be applicable to future technologies and use-cases will also be developed. These will aim to address the "unknown unknowns" through articulation of a thorough, systematic assurance argument for more-advanced, higher-level autonomy platforms and vessels. These standards will endeavour to be technology-agnostic, to enable the greatest level of innovation and the broadest applicability to future systems. This is best exemplified in the development of UL 4600 in the automotive domain, which aims to provide a comprehensive set of rules and requirements that will be primarily utilised for platforms at Level 3 and beyond on the J3016 autonomy scale.

The parallel activities of generating these two classes of standards will enable a roadmap of increasingly complex and progressively autonomous platforms to be conceptualised, developed, and delivered to the marketplace in a safe and secure manner.

4. Conclusions

This paper has explored the challenges facing the development and adoption of autonomy in the maritime domain, as well as the lessons that should be learned from automotive domain where autonomous systems are more well-established and better-defined. A significant milestone for automotive autonomy was the widespread adoption of the SAE J3016 taxonomy. Following the development of this framework, a number of standards have been developed to define assurance approaches for both low and high degrees of autonomy. It is therefore recommended that effort is expended in the maritime domain to ensure that a single framework is developed which can bring together all stakeholders (including OEMs and regulators) and reach a common understanding of maritime autonomy. From this point, the development of assurance routes and standards will naturally follow and these will become streamlined through adoption of a detailed framework for maritime autonomy.

This paper has also identified a number of commonalities and differences between the maritime and automotive domains in terms of the expectations on autonomous decision-making. This has highlighted technology implications, such as the need for larger volumes of stored data maritime autonomous platforms will require in order to meaningfully progress further into the world of full autonomy.

Acknowledgements

The authors are grateful to all parties involved in the review and editing of this paper.

References

5StarS Consortium, 2019. *A Roadmap to Resilience,* s.l.: 5StarS Consortium.

Daimler AG, 2019. *Safety First for Automated Driving (SaFAD),* Stuttgart, Germany: Daimler AG.

Edge Case Research, 2019. *An Overview of Draft UL 4600: "Standard for Safety for the Evaluation of Autonomous Products".* [Online] Available at: https://medium.com/@pr_97195/an-overview-of-draft-ul-4600-standard-for-safety-for-the-evaluation-of-autonomous-products-a50083762591 [Accessed 01 February 2020].

International Maritime Organization, 2017. *Guidelines on Maritime Cyber Risk Management,* London: International Maritime Organization.

International Maritime Organization, 2019. *Interim Guidelines for MASS Trials,* London: International Maritime Organization.

International Maritime Organization, 2020. *Autonomous shipping - in focus.* [Online] Available at: http://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx [Accessed 1 March 2020].

International Organization for Standardization (ISO), 2019. *PAS 21448 - Road Vehicles - Safety of the Intended Functionality,* Geneva: International Organization for Standardization (ISO).

Koopman, P., Ferrel, U., Fratrik, F. & Wagner, M., 2019. *A Safety Standard Approach for Fully Autonomous Vehicles.* Cham, Springer International Publishing.

Lloyd's Register, 2007. *ShipRight Overview,* London: Lloyd's Register Marine Business Stream.

Lloyd's Register, 2017. *Design Code for Unmanned Marine Systems,* London: Lloyd's Register Group Limited.

 https://doi.org/10.24868/issn.2515-818X.2020.013

Lloyd's Register, 2019. *Procedure for assignment of digital descriptive notes for autonomous and remote access ships,* London: Lloyd's Register Group Limited.

National Transportation Safety Board, 2017. *Collision Between a Car Operating With Automated Vehicle Control Systems and a Tractor-Semitrailer Truck Near Williston, Florida, May 7, 2016 - Accident Report,* Washington D.C.: National Transportation Safety Board.

Parkin, E. & Chilcott, J., 2019. *Integrating Autonomy - Maintain, Launch, Execute.* s.l., Zenodo.

Rødseth, Ø. J., Nordahl, H. & Hoem, Å., 2018. *Characterization of Autonomy in Merchant Ships.* Kobe, Japan, IEEE.

Royal Navy, 2019. *Digital and data plan,* London: Defence & Security International.

SAE International, 2018. *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles,* Warrendale, Pennsylvania: SAE International.

Schmittner, C., Griessnig, G. & Ma, Z., 2018. *Status of the development of ISO/SAE 21434.* Bilbao, Spain, Springer International Publishing.

Schmittner, C. & Macher, G., 2019. *Automotive Cybersecurity Standards - Relation and Overview.* Cham, Springer International Publishing.

Schnellbach, A. & Griessnig, G., 2019. *Development of the ISO 21448.* Cham, Springer International Publishing, pp. 585-593.

Siemens PLM Inc, 2018. *The future car, Driving a lifestyle revolution,* Plano, Texas: Siemens PLM Software Inc.

UL, 2020. *UL 4600 - Standard for Evaluation of Autonomous Products,* Northbrook: UL.

 https://doi.org/10.24868/issn.2515-818X.2020.013