A systematic approach to certification of complex control systems

C R Hawthorn* MEng MIET

* *Frazer-Nash Consultancy, UK*
* Corresponding Author. Email: c.hawthorn@fnc.co.uk

Synopsis

As commercial and naval ships push to reduce manning requirements, the complexity of the platform management and control systems is increasing.
The current route to compliance relies heavily on audits of the detailed design during the design/commissioning of the ship. Having it so late in the lifecycle adds risk of rework to the Shipbuilder and system supplier. As the complexity of control increases both the probability that changes will be required in response to identified safety issues, and the cost of making these changes will rise significantly.
For systems that have safety significance, and will be expected to comply with IEC 61508, this poses even more of a challenge as the level of evidence needed to support the functional safety argument will be almost impenetrable if viewed in the form of a single audit.
This paper proposes a staged approach to compliance, which will build confidence in the control and management system during the development lifecycle. It incorporates practices from other industries, such as aerospace, where complex control and safety systems have been in use for some time. Using a gated approach, loosely based on a tailored ARP 4754A model, Shipbuilders can mitigate much of the risk, and prevent cost overruns.
This systematic approach to progressively accumulating and signing off evidence increases auditor involvement, and keeps them much more informed throughout the design. This will allow the auditor to have more confidence in the suitability of complex control and protection systems, and being assured of the safe running of the ship.
This model has been common practice in aerospace for a number of years, and has supported advances in automation beyond the accepted norms of the marine industry.
This paper provides an overview of the risks presented by the current Certification mechanisms, and discusses possible solutions presented by ARP 4754A.

Keywords: Functional Safety; IEC61508; Systems engineering

1. Scope

The paper discusses the development model presented by the aerospace recommended practices ARP 4754A[1], and ARP 4761 [2], referred to as 'the ARPs'. The intent of this paper is not to go through the ARP 4754A/ARP 4761 approach in detail. It presents some specific cases, where the lifecycles, and principles presented by the ARPs could help improve safety, and alleviate some current issues with certification and assurance of complex control systems on naval surface ships.

The work presented should not be considered a conclusive or complete solution. Instead, it captures a proposition for a concept that, once matured, will help to address them. It is hoped that the outputs from this work will initiate further discussion and development to ultimately influence the certification of ship certification.

This paper is primarily be focussed on Naval Marine, but many of the topics and solutions discussed will be of interest to Commercial Marine, especially complex/high risk ships such as passenger ships and gas carriers

2. Introduction: The History of certification, and the challenges it faces

Initially Classification Societies, such as Lloyds Register (LR), classed merchant ships purely for assessing the risk for insurers. There were no build requirements, but a surveyor would do a survey and assign a rating for the hull and the equipment. (for Lloyds Register it was a vowel for the hull, A, E, I, O or U and a number for the equipment 1, 2 or 3, so A1 was top class while U3 was as bad as you could get and still be afloat).

During the 19th Century rules for the construction of the ships were developed by the Classification Societies and the ships were required to meet the minimum acceptable standard of A1 (later briefly for iron ships 99A1 then for steel ships 100A1). In the latter part of the 19th Century, partly due to campaigning by Samuel Plimsoll, the

Author Biography
Callum Hawthorn is a Senior Engineer at Frazer-Nash Consultancy in Bristol, UK. A Control and Instrumentation engineer, working primarily within the Civil Nuclear and Defence sectors.

 http://doi.org/10.24868/issn.2515-8198.2019.008

Government got involved in shipping legislation and had the authority to stop ships from sailing when they were overloaded. The British Government led with shipping legislation, partly because the British merchant fleet was the largest in the world.

Following the loss of the Titanic, it was agreed to have an international forum to develop shipping requirements. This resulted in the 1919 meeting of IMCO (International Maritime Consultative Organization) which developed the first international requirements and provided for governments to issue Certification for ships (primarily at first for life saving arrangements). Over the decades, IMCO developed and produced requirements that are more detailed, and after the formation of the UN in the years following WW2 was subsumed as a UN body becoming IMO.

The ships certification regime developed so that the Governments issue the statutory certification (i.e. that required by the Statutes of the Government, which are the adopted IMO legislation) while the Classification Societies issue the Classification Certificates. Initially these were ensuring separate issues – the Statutory Certification was concerned with the safety of life, pollution, etc. while the Classification Certificate was more concerned with the seaworthiness of the ship and the safety of operation.

Over the years the separation of these two has become somewhat fuzzy and the IMO legislation has incorporated Classification issues (and to a slight degree, vice versa). The overlap and the fact that Classification Societies have worldwide coverage often means that the Classification Society has a presence at the shipyard where the ship is built but the Flag Administration (the government body responsible for Certification) does not, so they delegate the authority for the Statutory Certification to the Classification Society. There is now also a requirement in the IMO legislation that states that Certification is dependent on the ship being classed (and a similar statement in the Class Rules that the ship must have the appropriate Statutory Certification in order to be accepted into Class – a bit of a chicken and egg situation).

The process for acceptance is dependent on three stages – design review, inspection and testing/trials. This is tried and tested as far as the ship structure and the machinery is concerned, though perhaps less so for modern control systems.

The design review will involve an assessment of the design drawings against defined requirements – so for hull the strength, stability etc. For the machinery, it is more concerned with the performance, strength, safety etc. For electrical systems the requirements are more closely aligned with functionality, particularly resilience to faults and redundancy.

The inspection/survey involves firstly whether the design has been followed, particularly any required changes that have been identified. It also involves a visual inspection of the build quality etc. to ensure that appropriate standards are being maintained.

The testing trials involves verification of the operation of the system/equipment and may be at the Factory (Factory Acceptance Test), on board during build (Harbour Acceptance Test) or Sea Trials, or any combination of these.

The early control systems took land based industrial control systems and put them on ships, with predictably poor results. Not many land-based systems undergo severe vibration or roll from side to side. This led to the development of Type Approval by the Classification Societies where the equipment underwent environmental testing to ensure it was suitable for the marine environment.

Apart from checking suitability for marine use, control systems approval differed little from the above process, with design reviews, inspection and testing. The big change came in when programmable systems started to appear. The initial reaction was to ensure that programmable systems were not the sole control for critical systems, a similar approach taken by civil nuclear. This involved arrangements such as hard-wired back-ups, or secondary control systems. However as programmable systems became both cheaper and more powerful this became harder to ensure and there was a move to systems assurance rather than solely equipment approval. This involved assessment of the QA scheme under which the software was developed rather than just a test of the software. The degree of assurance was dependent on the safety criticality of the system.

For safety related/safety critical systems a more rigorous process was brought in which involved auditing of the software production to ensure the QA procedures were being followed, somewhat akin to TickIT.

The latest move is for more an even more rigorous assessment of the software to be undertaken, presenting its own challenges to overcome.

 http://doi.org/10.24868/issn.2515-8198.2019.008

3. ARP 4754A overview

ARP 4754A is an aerospace systems engineering guidance note and it was created to be read alongside ARP 4761 and the air systems standards DO-178 & DO-254. As such, it does not include specific coverage of detailed software or electronic hardware development, safety assessment processes, in service safety activities, structural development.

It was initially developed to address the issue of increasing system complexity and with the knowledge that testing of PE (Programmable Electronics) is unlikely to expose all faults in that may have been introduced during the development of that function. This document was originally developed in response to a request from the Federal Aviation Administration (FAA) to the SAE International (SAE)[1]. The FAA requested that SAE define the appropriate nature and scope of system-level information for demonstrating regulatory compliance for highly integrated or complex systems. The Systems Integration Requirements Task group (SIRT) was formed to develop an ARP that would address this need.

At its core, the ARPs follow a classic systems engineering lifecycle. The overall development lifecycle proposed by ARP 4754A maps onto the V-Lifecycle as shown in Figure 1.

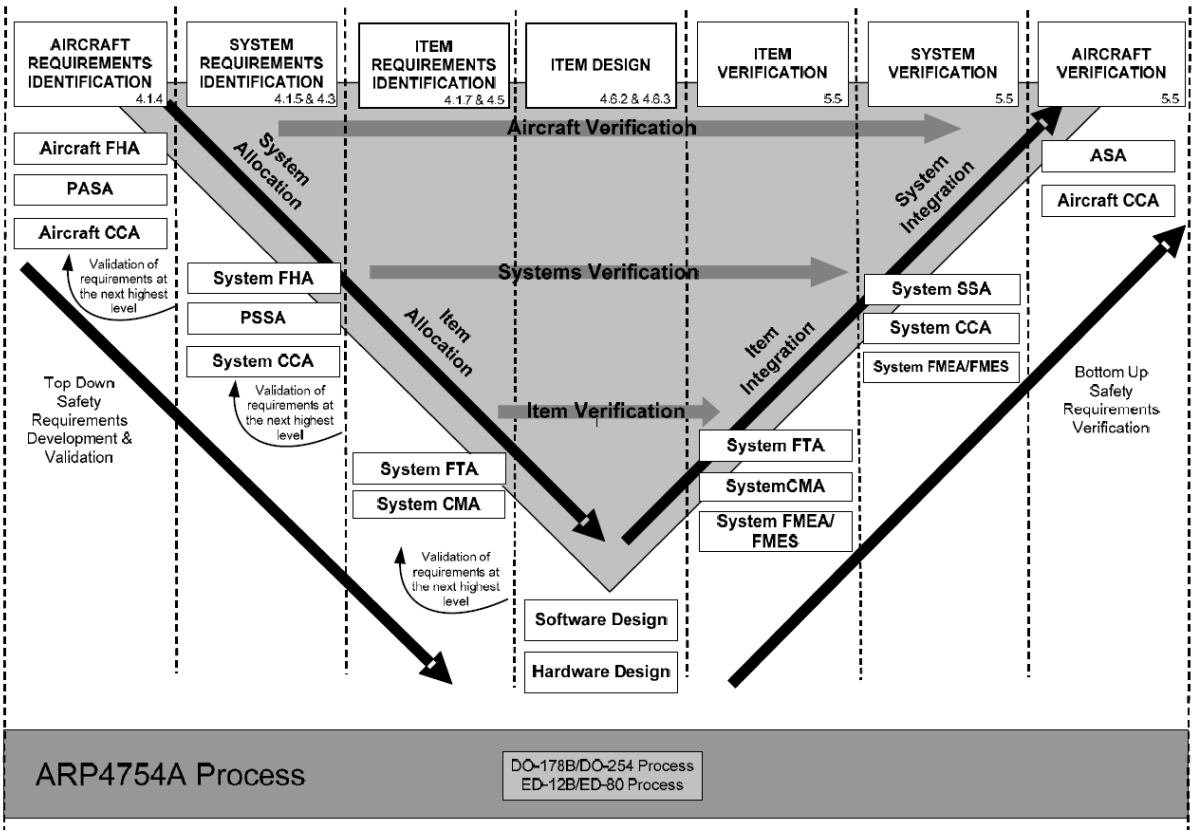

Figure 1 - ARP 4754A V-Lifecycle (ARP 4754A, 2010)

ARP 4754A differs from other systems engineering lifecycles (such as the lifecycle presented in IEC 61508), which address specific ‘systems’, and instead focuses on ‘functions’ important to safety, before then allocating each function to a system. It is only at this stage that the architecture is defined, before allocating any required assurance levels to specific equipment items. The processes of decomposing the concept design down to items is shown in Figure 2, where the’ aircraft’ in this case can be replaced with ‘ship’.

Fundamental to the process is the implementation of Preliminary Aircraft Safety Assessments (PASA) and Preliminary System Safety Assessments (PSSA). The PASA process, assess the aircraft architectures and develops safety requirements so that aircraft and individual systems development can proceed with reduced rsik. The PSSA then examines the proposed system architecture, failure conditions and associated safety objectives identified by the allocated from the PASA. These activities are supported with Functional Hazard Assessments (FHA), and Common Cause Analyses (CCA).

 http://doi.org/10.24868/issn.2515-8198.2019.008

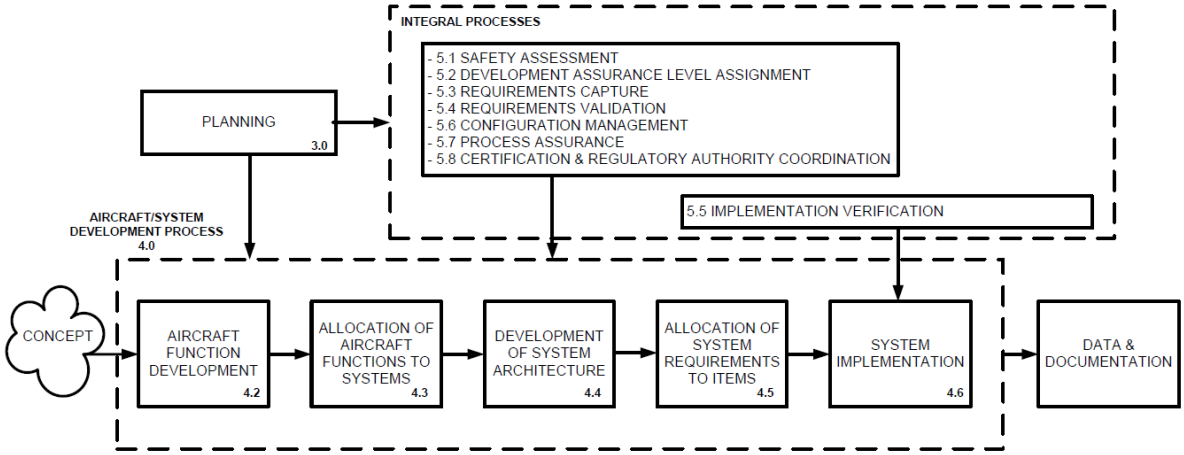

Figure 2 - ARP 4754A system development process model (ARP 4754A, 2010)

4. What can we learn from this certification approach?

4.1. Addressing the increased risk of development error

Complex systems and integrated ship level functions present greater risk of development error (requirements determination and design errors) and undesirable, unintended effects. At the same time it is generally not practical (and may not even be possible) to develop a finite test suite for highly-integrated and complex systems which conclusively demonstrates that there are no residual development errors. Since these errors are generally not deterministic and suitable numerical methods for characterizing them are not available, other qualitative means should be used to establish that the system can satisfy safety objectives.

The lifecycle presented by ARP 4754A instead shifts some of the focus from looking at the end product, to assessing the development process itself. This is with the aim to provide assurance that the development has been completed in a sufficiently disciplined manner to limit the likelihood of development errors that impact vehicle safety.

In IEC 61508 terms, this means shifting the focus towards evidence of production excellence. This is most applicable to the development of safety critical software, as generally the software is developed specifically for ship in question. This means the Certification Authority, and Shipbuilder can have more involvement in defining required certification activities, and assurance.

For COTS, or configurable equipment stricter through life assurance evidence could potentially to offset the high integrity requirements that usually result in the use of a separate hardwired protection system. This approach common to the Civil Nuclear domain, puts smart devices through a rigorous EMPHASIS assessment [3] to qualify the product for use in a high integrity safety system.

4.2. Cross system functional allocation

A great strength of the ARP is that it starts with top-level functions (whole aircraft which maps to whole ship). It is clear that the current Shipbuilder approach is to start at system or product level, and to try to “balance SILs, etc”. between system elements.

This will become a particular problem as control complexity drives the design to implement functions crossing system boundaries. The ARP was developed explicitly because of problems with the system-focused approach that has emerged, as aircraft systems became more complex and highly integrated. Thus the ARP has been designed to address a problem that still faces the Shipbuilder.

This paper is not advocating for the complete adoption of this function centric approach, or the incumbent systems development. There is value however, in including a review that identifies the safety functions in the same manner as presented in the ARPs, as a means of performing a gap analysis. This will aid in the design of the

 http://doi.org/10.24868/issn.2515-8198.2019.008

system architecture, and highlight areas where functions are served by multiple systems, potentially simplifying the design, or allowing a relevant mitigation strategy to be put in place.

4.3. Early buy in and continual involvement from certification authority

The current certification approach has an independent audit late in the design lifecycle. This will introduce an increasingly likely risk of rework, or design changes because of the certification audit. The commercial and programme implications of this risk will also increase as control systems become more complex, and the effort required to correct any shortfalls becomes more substantial.

Alongside this is the possibility that the auditor/regulator may not be able to award the certification due to concerns stemming from being unable to form a complete understanding of the complex system, and the design decisions taken in the development of the system.

'The certification authority determines the adequacy of the data for showing regulatory compliance. The applicant should develop a certification summary to describe how it was determined that the system, as installed on the aircraft, or the aircraft itself (as appropriate) complies with the agreed certification plan.

The certification summary / compliance report should provide an outline of the results of the activities established in the certification plan. Any deviation from the agreed plan should be described together with rationale to substantiate the deviation. In addition to addressing the content of the certification plan, the certification summary should include:

a. A statement of compliance to the airworthiness requirements.

b. An outline of any open problem reports that impact functionality or safety.'

Extract from ARP 4754A, 2010, p.77

The above extract form ARP 4754A describes one of the key interactions with the certification authority that act as a mitigation against the risk of rework, or design changes resultant from the certification audit. A certification and assurance strategy could be agreed with the Certification Authority (for surface ships this would likely be the Naval Authority Group) early in the development lifecycle. They would then periodically review the development process, ensuring that the Shipbuilder is carrying out the strategy, and approving any deviations as they surface. By having continual engagement throughout the lifecycle, the regulator is aware of the design decisions, and builds an understanding of the system as it develops. This also has a benefit for the Shipbuilder as it de-risk the likelihood of late design rework due to the certification, as the certification approach is approved at each stage of the design.

One of the important features that would need to be addressed is the identification of points in the development where a *'meaningful review'* could be completed. This would vary from ship to ship, and would have to be agreed with the Certification Authority in advance.

The selection of the Certification Authority, and delegation of responsibility is non-trivial, and discussed in Section 4.5

4.4. Physical division of hardware

This issue is not addressed specifically in the ARPs, but functional approach to managing safety enables opportunities that are not usually considered in the architecture and system design of systems.

As safety requirements are only allocated to specific equipment items, this means that given a demonstrable segregation, a single system could be split to provide different integrity function within a single system. This has advantages in reducing costs in development as only those functions that require higher integrity are developed to that standard. In practice this can be difficult, as showing satisfactory segregation can be difficult, but in many cases the cost saving of going through that process are significant. Figure 3 shows a basic breakdown of how this would look in hardware, with specific emphasis places on the uni-directional communication between higher and lower SIL hardware.

 http://doi.org/10.24868/issn.2515-8198.2019.008

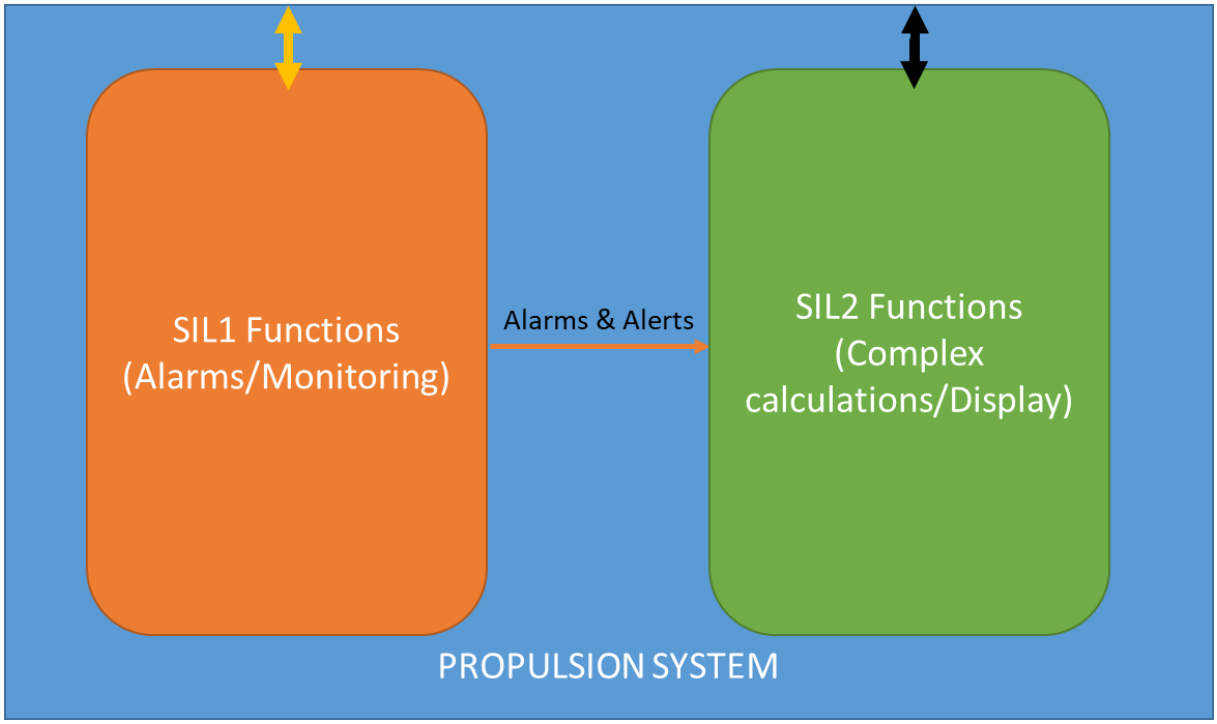

Figure 3 - Example of physical division of hardware

3. Challenges of applying the key principles

4.5. Certification Authority

One of the key issues when adopting the principles of ARP 4754A is likely to be the identification of the Certification Authority. Currently the Certification Authority is the Naval Authority Group (NAG), who in turn delegate this role to the auditor, while maintaining some level of responsibility.

4.5.1. Independence vs Experience

The workload is expected to increase if continuous involvement is expected, and the view is that the NAG do not, as currently resourced, have the capability to discharge this duty. Finding an independent with the available resource, broad experience, and independence to discharge this duty is a near impossible task, so other solutions should be considered.

These options include delegating the role of Certification Authority to the engineering management function, referred to in ARP 4754A as the Designated Engineering Representative (DER), as they have the system knowledge to understand the implications of design changes, and the suitability of assurance activities. They would sit embedded within the development, but would act independently of them. They would sign off the certification strategy, and sit in on design reviews to ensure they meet the required standards.

The problem with this approach would become evident when attempting to demonstrate that there is suitable independence in the DER, and that programme concerns do not interfere with an otherwise diligent certification strategy. Additional confidence in the independence of the decision making could be added by utilising independent 3rd parties to support the assurance activities, proving an independent view where needed. This would need to be detailed in the certification strategy, and agreed with the regulator. With this configuration the DER could potentially still overrule the independent party, to avoid this protection needs to be put in place so that the DER must have agreement from the independent 3rd parties before they are able to dismiss concerns.

Another option may be to select an Independent Safety Auditor (ISA), this may be more in keeping with a DEF-STAN-00-56 development as it is considered likely that a more appropriate skill set may be available than that available from the commercial aviation DER approach.

An ISA could be a lead individual supported as required by other SQEP individuals in the disciplines required (Software Intensive Safety Critical Systems development and certification, Hardware engineering, Complex Electronic Hardware development, Software development, Submarine systems and Submarine operation) but

 http://doi.org/10.24868/issn.2515-8198.2019.008

possessing the degree of independence required to satisfy the certification authority. They would perform a similar function to that of the DER, but would not require the same level of system specific knowledge, meaning there is a larger pool of experts from which a candidate could be selected.

4.6. DAL to SIL conversion

One of the core difficulties when trying to incorporate techniques used in the ARPs is that risk is categorised differently that in IEC 61508. The ARPs deal with Development Assurance Levels (DALs), which is in essence the level of developmental scrutiny that is required based on the function-associated hazards. These hazards are identified as part of the Functional Hazard Assessments (FHAs).

This approach is fundamentally different from the system integrity approach using Safety Integrity Levels (SILs), which are allocated to systems in the ship. As a result, the mapping from DALs to SILs is not simple to achieve, and in-fact DEFSTAN-00-55 specifically discusses the implication of using DO-178/DO-254 for this specific reason.

A large portion of the difficulty is derived from taking qualitative development assurance evidence, produced as part of the ARP process, and converting this to a justification of a probabilistic failure rate. ARP 4761 has a table mapping DALs to a maximum probability of failure, but it unclear if this, alongside assurance evidence, would be sufficient to support an IEC 61508 SIL claim.

It is therefore theoretically possible to convert DALs to SILs, but it requires close consideration, and agreement from the Certification Authority to show that they are equivalent.

For this reason, the author recommends only the adoption of the key principles of the ARPs discussed in this paper for use on Naval Ships.

5. Conclusions

The complexity of control systems has been progressively increasing, to a point where the prevalence of Programmable Electronics (PE) is challenging the suitability and capability of the current certification approach in surface ships.

Learning from other industries standards, and adopting a staged approach to certification and assurance, with continual involvement of the Certification Authority may build confidence in the development of these control systems and reduce the risk of expensive rework towards the end of the design lifecycle.

Adding an additional safety function assessment may also enable the designer to make informed choices that can both improve the safety of the ship by identifying functions that require multi-system input, but also highlight areas where a system can be split at a hardware level into different integrity level, saving the project money and requiring a less rigorous approach.

These changes will require close consideration if they are to be implemented as the implications of a failure to properly apply the safety principles could result in increased risk to crew. However, if they are considered and implemented properly, it will allow save money, and provide additional confidence in the complex control systems that will be needed to reduce manning on surface ships.

References

1. SAE Aerospace, 2010: “ARP 4754A -Guidelines for Development of Civil Aircraft and Systems”
2. SAE Aerospace, 1996, “ARP 4761 - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment”
3. R. Stockham, 2009, “Emphasis on Safety”, IET Magazine, Issue 02 2009

 http://doi.org/10.24868/issn.2515-8198.2019.008