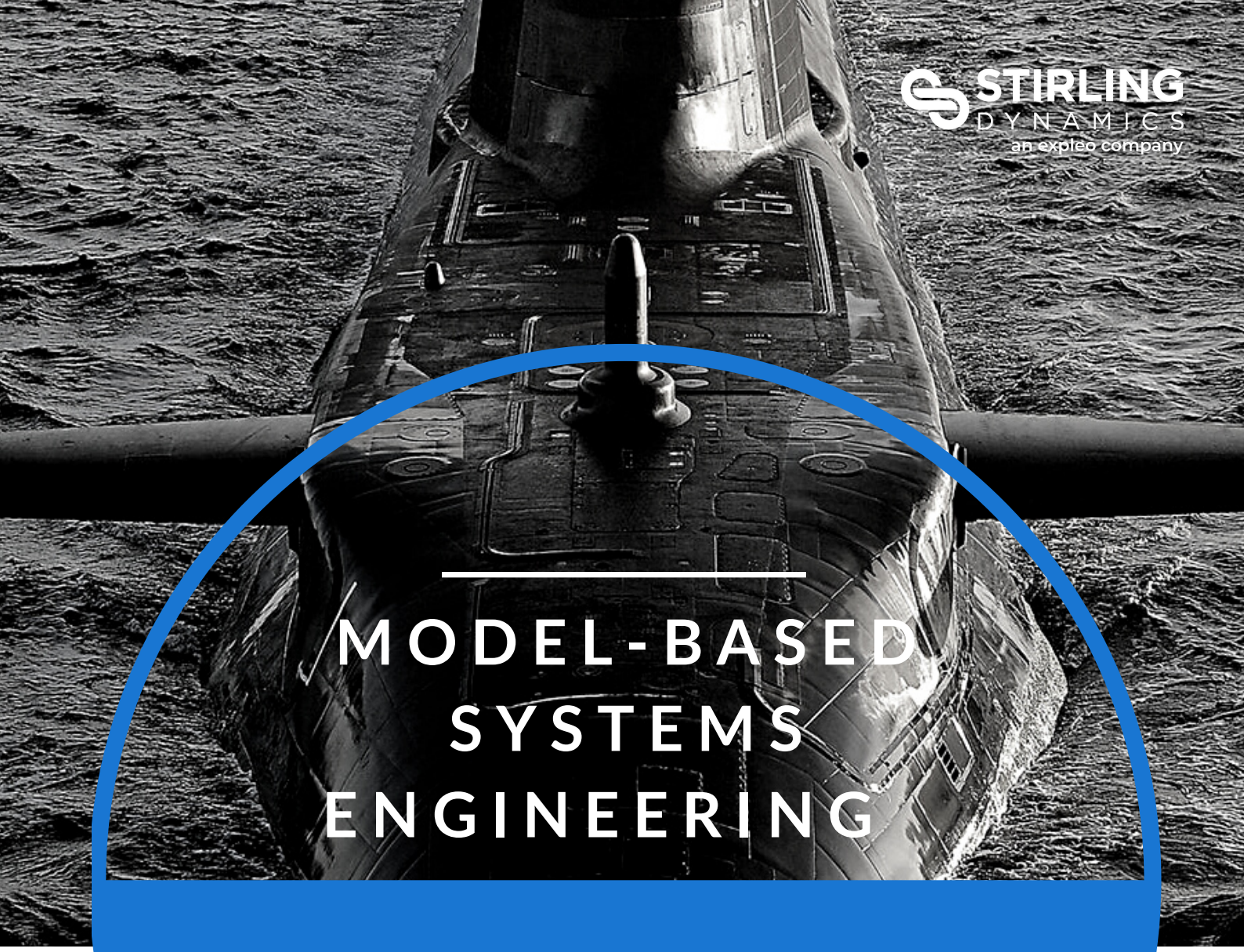


STIRLING DYNAMICS
an expleo company

MODEL-BASED SYSTEMS ENGINEERING

UTILISING MBSE FOR SAFETY-CRITICAL SOFTWARE

PREPARED BY
CHRIS HARRIS, STIRLING DYNAMICS

WWW.STIRLING-DYNAMICS.COM

INTRODUCTION

INFORMING BETTER DECISIONS

Systems have become increasingly complex over recent years, particularly within the military domain. Many of the systems have safety-critical elements, redundancy, and an increasingly high level of interaction. It is becoming more difficult to specify and corroborate these systems' requirements and further validate the proposed technical solutions, particularly when the systems may be developed by multiple different suppliers.

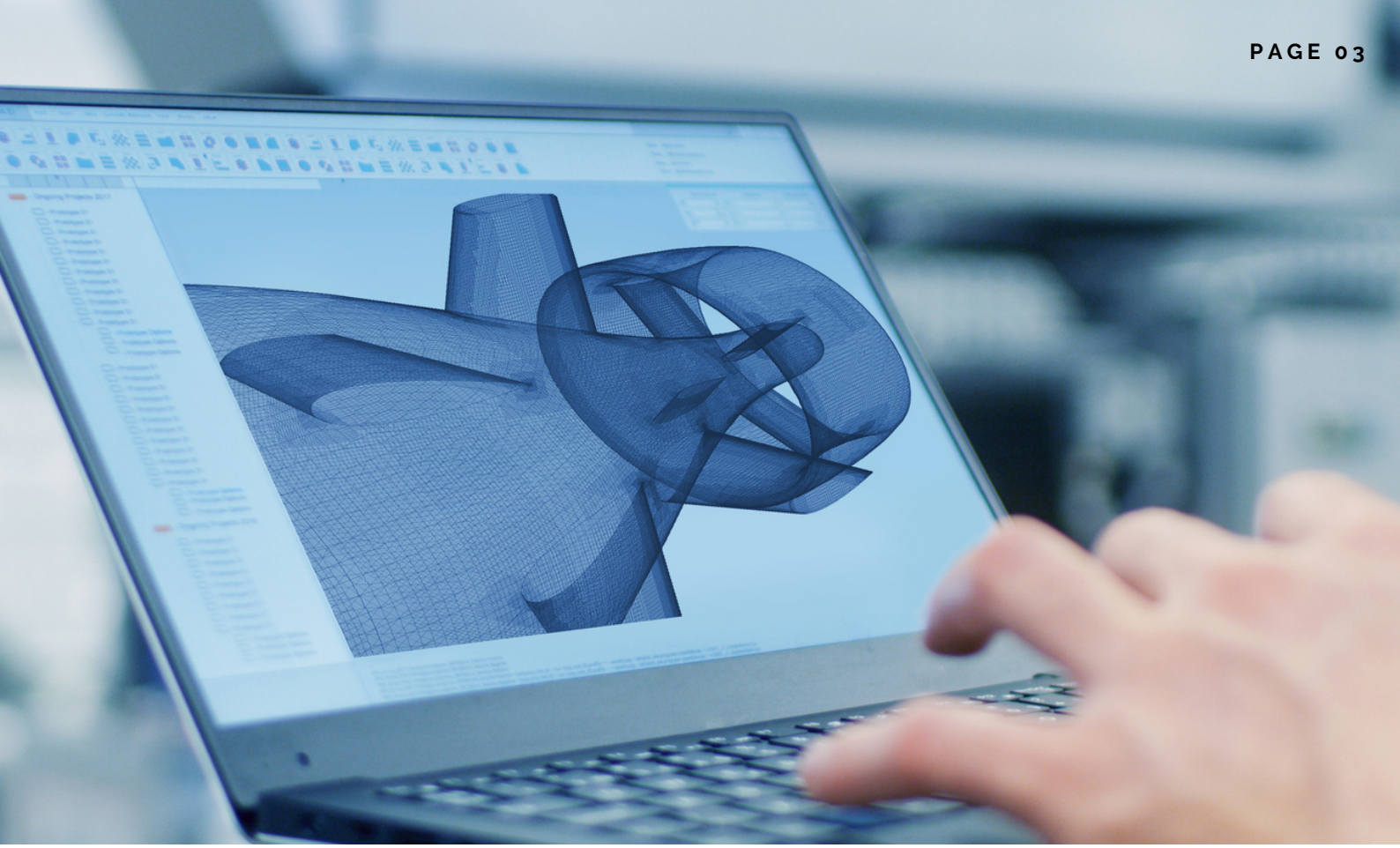
Such systems can include boat control systems, power generation and distribution systems, weapons systems, fuel systems, engine systems and propulsion systems.

Conventional system design approaches require the capture of requirements, validation of these requirements and specification of the system through a series of interconnected textual documents. It can be difficult for a complex system to trace these dependencies, with design updates being manually propagated through related documents and prone to error.

Furthermore, text-based requirements can be ambiguous leading to misinterpretation and a challlenging format for use in a formal verification and testing process. Adopting Model-Based Design processes and associated methods can help address many of these issues as part of the system development process.

WHAT IS MODEL-BASED SYSTEMS ENGINEERING?

Model-based systems engineering (MBSE) is a systems engineering methodology that focuses on utilising a set of interconnected models and exploiting these as the primary means of information exchange between engineers, and within the supply chain. The benefits of MBSE include increased clarity in requirements and communication, reduced development risk, improved quality, and increased integration within the design life cycle.



MBSE IN THE MARINE SECTOR

We have seen MBSE used successfully in the aerospace sector. Aircraft are highly complex with many conflicting requirements. With the continued push for better performance, cost-effectiveness, safety, reliability, maintainability, it is very challenging to design these multi-system interfacing platforms without undergoing detailed analyses. Furthermore, the sooner these analyses take place, the quicker potential problems can be found, leading to more straightforward solutions. Through MBSE, analysis is continually being performed, assessing the design, running concept trade-offs and optimisations. Any problems identified are significantly quicker and cost-effective to solve at this stage.

Within aerospace, Stirling Dynamics recently worked on a regional jet project where we developed models for all aircraft systems. This meant that each system could be analysed individually to verify that the design meets the performance and safety requirements. However, the real power of this approach was to integrate the system models together.

When doing this, the interactions between the systems can be assessed, in unusual scenarios such as failure cases. This shows how one failure in one system could have a detrimental effect on another system. Once these unwanted interactions were found, the models were used to study different design concepts to rectify the issues.

At Stirling Dynamics, we have utilised the lessons learnt and best practices within the aerospace sector to improve the development and delivery of safety-critical software in the Marine Sector. Given the nature of the work Stirling Dynamics has undertaken using MBSE, it was unable to be deployed within its purest sense, however, significant gains and efficiencies have been made in using parts of it to help deliver safety-critical software to safety integrity level 2. The following case study highlights the way Stirling Dynamics has utilised best practices and tailored them to improve the delivery of safety-critical software into the Marine Sector.

EXAMPLES AND CASE STUDIES

To illustrate the concepts discussed in this paper, we have provided a case study of a recent project undertaken by Stirling Dynamics that used MBSE for verification and validation purposes.

Stirling Dynamics developed the central computer software for a Royal Navy submarine. This software included, for example:

- Course and depth autopilot
- Hover control algorithm
- Safe manoeuvre envelope
- Depth measurement system
- Warning and alarms system
- Joystick input handling
- Monitoring and backup systems

These elements act as complex interconnected systems, making a traditional document-based engineering approach difficult for assessing the overall system behaviour. Therefore, system models have been designed to not only represent the deliverable software elements, but also to simulate the wider platform management system, submarine sub-systems, and the overall vessel dynamics.

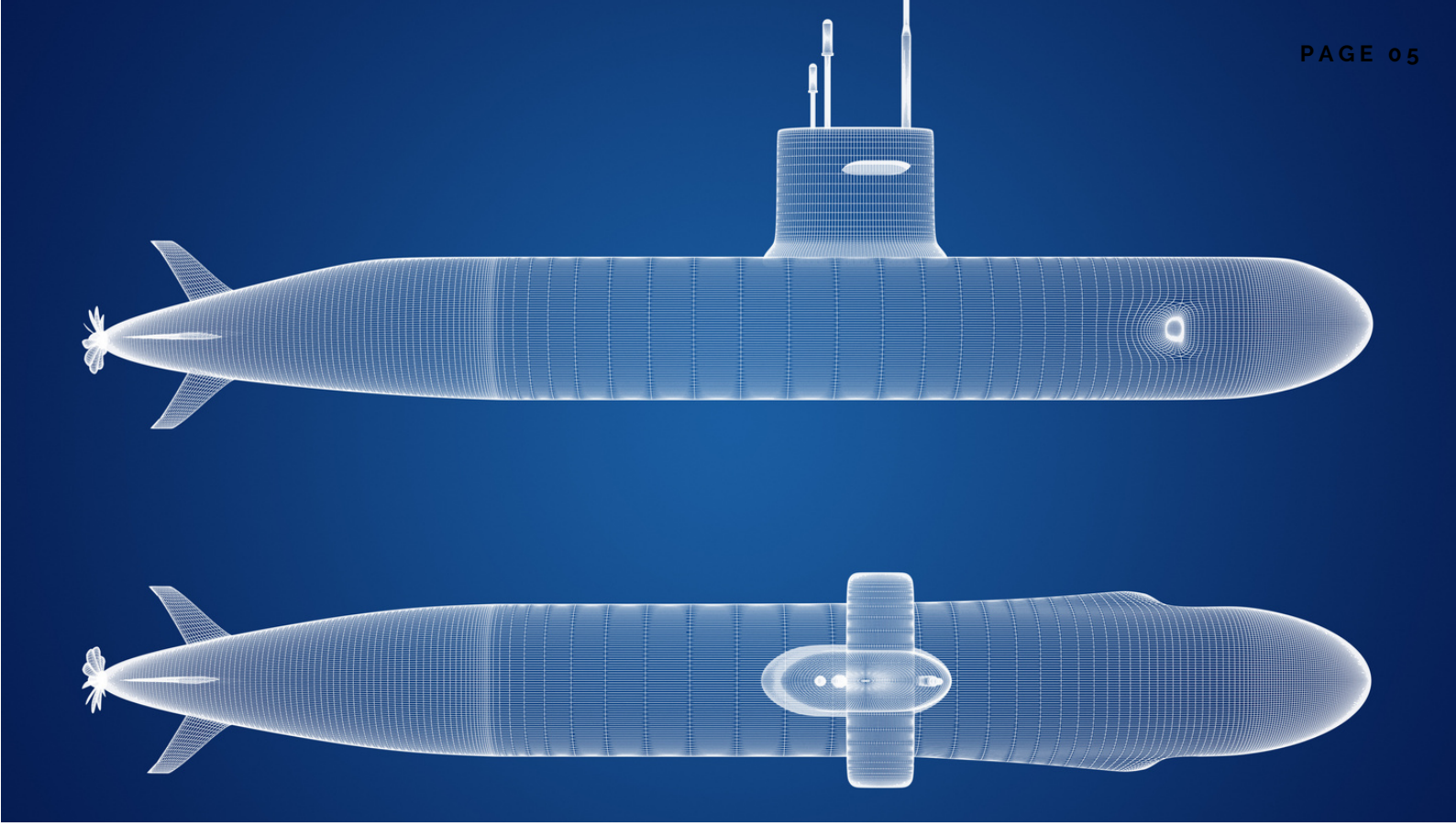
This has allowed several complex analyses and trade studies to be performed:

- **Autopilot and hover control system interactions**
  Performance requirements are defined for both the autopilot system, and the hover control system, and these are individually assessed. Combining these two elements into a full system model, however, has allowed the performance to be assessed for both systems operating in tandem. This assessment has given confidence to the crew to enable them to perform a seamless transition from hover control (low speed) to autopilot control (high speed), with both systems operational across the transition speed.

- **Impact latency on system performance**
  Simulation models of the PMS network architecture and associated hardware have allowed the autopilot system to be assessed against possible system latency. This allowed the theoretical phase margins of the autopilot to be fully assessed and help form predictions for how the system would behave under worse-case latency scenarios, and if these worse case predictions could be handled by the system.

- **Hover system failure**
  Having the ability to simulate the full submarine trim and compensation system allows interactive tests of the hover control algorithm to be undertaken. This helps identify any potential problems with the system at an early stage, which can inform the overall submarine safety case, and form part of the operator training. The ability to perform realistic complex operating scenarios allows the system to be fully evaluated prior to commissioning.

- **Rapid prototyping**
  The existence of a full system model allows rapid prototyping of production code, as any changes can be assessed against the system model. This full system model allows a large amount of integration testing to be performed in a fully simulated environment, prior to the software being incorporated into a fully-fledged integration rig. This approach has proven to provide significant timesaving and allow a more compressed development lifecycle.



SUMMARY

In this whitepaper, we have considered how MBSE can be a tool to help improve the speed, development and accuracy of safety-critical software requirements where multiple systems interact and the complexity justifies a move away from textual requirement validation. At Stirling Dynamics, we constantly strive to drive efficiencies and improve deliveries to our customers. We are passionate about learning lessons across the different sectors and utilising them in the most efficient way to drive great outcomes. We appreciate the value of the process and tools and have employed them so to maximise their benefit in an intelligent way.

Through utilising these MBSE methods, we have successfully delivered Safety Critical software to the Royal Navy Submarine fleet for several years and continue to do so. Our Autopilot algorithm sits on a wide range of boats around the world and for each solution we tailor our approach to best fit the project/programme we are working on. MBSE, whilst a very useful tool, does not solve all the challenges with delivering onto a highly complex marine environment, however, we hope in this whitepaper we have touched on how it can be utilised to drive efficiencies in certain areas.

In the future, there is no doubt that the complexity of systems and the interactions between multiple systems will require the capabilities of model-based systems engineering to support their development. Combine this with digital twin innovations and the future development concept may be feasible completely in a virtual environment. There are exciting powerful opportunities ahead that, with the innovative application for the benefit of systems development, could bring step changes to development time and solution robustness.

In the meantime, Stirling Dynamics continues to develop a broader capability across domains, bringing cross-fertilisation to its marine and aerospace activities, and working with the industry to develop future concepts.

ABOUT THE AUTHOR

Chris Harris
PRINCIPAL ENGINEER
SIMULATION AND CONTROL

Chris is a principal engineer within Stirling Dynamics' Marine & Industrial Systems group. His key skills and expertise lie in the areas of autopilot design, control and simulation, data analysis, and model development. During his time at Stirling Dynamics, he has worked on a wide range of marine and aerospace projects, including multiple submarine autopilot design and development projects, sea trials support and analysis, aircraft pitch control algorithm development, design of submarine simulation software, test rig commissioning activities, and investigation into the use of Kalman filtering to reduce flight control system and structural mode iterations for a modern combat aircraft application.

ABOUT STIRLING DYNAMICS

Stirling Dynamics is an advanced engineering company that provides high-end engineering and consultancy services to support programmes in the aerospace and marine industries – including those with demanding safety-critical requirements. The company's strength is in providing world-leading technical expertise and the ability to work collaboratively with customers to build strong relationships with a focus on open communication and transparency. Trading since 1987, Stirling Dynamics has accumulated a wealth of knowledge on over 70 different aircraft types and 11 naval platforms around the globe, covering both civil and military programmes, ranging from conceptual design through to in-service support.

CONTACT US

TELEPHONE: +44 (0)117 9152 500
EMAIL: ENQUIRIES@STIRLING-DYNAMICS.COM
WEBSITE: WWW.STIRLING-DYNAMICS.COM

STIRLING DYNAMICS
an expleo company