Learning Lessons to de-risk future complex projects:

Design and Integration of the World's Largest Ship Platform Management System

Queen Elizabeth Class Aircraft Carriers

M Williams* B.Eng(Hons) CEng MInstMC

** Thales UK, Bristol, UK*
* Corresponding Author. Email: williamsmervyn@yahoo.co.uk

Synopsis

The Integrated Platform Management System (IPMS) on the Queen Elizabeth Class (QEC) Aircraft Carriers for the Royal Navy is the largest and most integrated ship control system ever delivered. To achieve the successful delivery of this system, with a project lifecycle of 15 years, has necessitated the need for un-paralleled alliance working between companies; the deployment of novel, agile processes; the need to produce an architecture that finds a balance between safety and operability; proactive obsolescence management; the need to trade-off customer requirements and expectations with technical and financial risk, plus the alignment of security requirements within an inherently commercial architecture.

This paper will present the major challenges faced during the lifecycle of this vast system, in particular it will examine the following areas:-

The influencers during the design stages, how they shaped the architecture (hardware and software) together with the optimal and sub-optimal outcomes in both financial and technical terms.

The alliance working between the companies involved, showing how the teams were organised in order to flexibly and efficiently match the lifecycle processes, using agile release processes in order to support commissioning, whilst allowing immature systems design to evolve, presenting the areas of good and bad practice.

The deployment of robust systems engineering processes and the analysis of their outcomes will be discussed, together with the de-risking processes including early and enhanced integration activities required to manage the 50,000 I/O spread across the 50 interfaces of various types, complexity and maturity.

The summary of this paper will present the major risk elements of the project, what the mitigation plan was and the outcomes of these risks, positive and negative. Together with the elements that provided the best cost/benefit ratio in the system delivered to the Royal Navy, it will also summarise the optimal processes and practices, plus those that could be improved upon in future projects.

Keywords: IPMS; De-risk; Lessons Learned; Integration; Control System;

1. Introduction

1.1. Scale of the task

The IPMS on the QEC Aircraft Carriers has represented a unique design, integration, commissioning and management challenge for all the many talented personnel that have been involved over the last 15 years. This uniqueness is borne from the sheer size of the ship, the resulting scale of data to be processed by IPMS, the level of integration between power and propulsion, platform and mission systems, and the desire to adopt a more commercial open architecture.

1.2. Execution

The QEC project is executed via a main alliance of the Ministry of Defence (MoD), BAE Systems, Babcock, and Thales, and a sub-alliance of Thales, GE, Rolls-Royce and L-3. Thales' main scope of supply is the Power and Propulsion solution including acting as the integrator for the partners in the sub-alliance.

http://doi.org/10.24868/issn.2515-818X.2018.070

2. Pre-contract architectural decisions

Whilst there were high level requirements flowed down from the MoD, many of the requirements were implied from the desire to reduce risk. The project can be classed as requirements light, resulting in the contracts being awarded against Ship and Equipment Specifications, with the implied requirements finding their way into the words of these specifications. The customer was keen to maximise the use of commercial hardware and software because of the expected ease of through life support from any marine control system supplier, not just the provider of the contracted control system. Perceived risk areas in procurement and through life drove the architecture captured in the specifications. Commonality of ship infrastructure where practical, was also a key consideration.

The major effects on the architecture from this approach were the following

- Commercial off the Shelf (COTS) data acquisition layer of the system – GE Fanuc I/O modules and PLCs provided and integrated by L-3
- Military off the Shelf (MOTS) Supervisory layer of the system provided and integrated by L-3
- A GE provided Electric Power Control and Monitoring System (EPCAMS), complete with data acquisition and supervisory layers, connected directly to IPMS, whilst IPMS maintained the primary operator interface. Integrated by L-3, GE and Thales
- Ship-wide shared network infrastructure. Integrated by L-3, BAE Systems and Thales.

Connection to novel and remote (particularly Mission) Systems, was desirable from a client perspective. This resulted in the connection to external interfaces outside of the normal power, propulsion and platform sphere

3. Headline Risks

3.1. Ability of the system to cope with the scale

IPMS on QEC is an order of magnitude bigger than implemented on any other Royal Navy ship, the resulting quantity of I/O resulted in 180 outstations containing the low level GE Fanuc Programmable Logic Controllers (PLCs) and Input / Output (I/O) modules. These PLCs presented a previously untested interface (Ethernet Global Data [EGD]) to the L-3 communication and Human Computer Interface (HCI) layers.

There was an initial estimate of 30,000 I/0, this increased to50,000 by the time of the preliminary design reviews and contract placement

3.2. Immature connected systems

Just as IPMS was of an order of magnitude bigger than on other ships, so were the connected systems such as Heating Ventilation and Air Conditioning (HVAC) which accounted for over 20% of the IPMS I/0. Project Management put all areas of design for ship systems under pressure to declare maturity as early as possible in order to progress the project deliverables, this presented the risk of proceeding into IPMS software development with immature data.

The risk to operability also existed for systems which were connected in order to service the Weapon Engineers who would use the system. The core skills of the IPMS design team were in the areas of Marine Engineering and Damage Control, rather than Weapon Engineering, and so the functional analysis of the Weapon Engineers tasks and roles was not fully conducted.

3.3. Safety

There was a strong desire to maintain IPMS as non-safety related (Safety Integrity Level [SIL] 0). In order to achieve this, mitigating functions were put in place on the connected systems which was deemed the most cost effective solution. This necessitated performing functional failure analysis of all systems connected to IPMS, to ensure they had no safety related functions.

3.4. 3rd party network

The ship network was provided by the BAE Mission Systems network team to ensure commonality across the platform, as well as ease of integration between disparate functional networks. This necessitated early and detailed integration of IPMS and EPCAMS to the network at the L-3 Shore Integration Facility (SIF), the GE

SIF, and at the Mission Systems SIF. This was achieved via the use of Shore Representation Units (SRU) at these faciliites.

3.5. Quantity and complexity of integration

With 50 external system interfaces to IPMS, the type and complexity were not surprisingly varied. All interfaces had to comply with a common interface specification and to be proven to be compliant via factory testing.

The EPCAMS interface provides a link between the two highly complex control systems. This solution was borne from the desire to maximise pull through from previous projects and therefore help mitigate the perceived risk of not using EPCAMS as developed for Type 45. The solution put EPCAMS at the heart of a complex 3 system stack IPMS-EPCAMS-Drives and IPMS-EPCAMS-Gas Turbine, for example

3.6. Correct connectivity to and control of remote systems

Stage 1 engineering is very much focussed on ensuring the correct interfaces are in place and that the correct control strategy is in place for the systems under control. Detailed task and role analysis is required to ensure that the architecture supports the needs of the operator. Control strategies feed the more detailed software design by the suppliers. Failure to perform this properly will result in expensive re-work during the more detailed design and software implementation stages.

3.7. Emerging Requirements

Whilst the ship specification (Aircraft Carrier Alliance [ACA] to MoD contract) and equipment specification (ACA to equipment supplier contract) were in place at contract award, they were necessarily high level to keep costs down, but inherent in this approach was the impact of emerging transverse requirements based on expectation of other stakeholders.

4. Risk Mitigation

4.1. Ship Control Centre (SCC) mock-up

This was constructed as a life size mock-up of the space including the layout of the consoles in order to verbally exercise the communication between the operators within this space, thus confirming and influencing the task and workload analysis that was in progress at the time.

4.2. Alliance Working

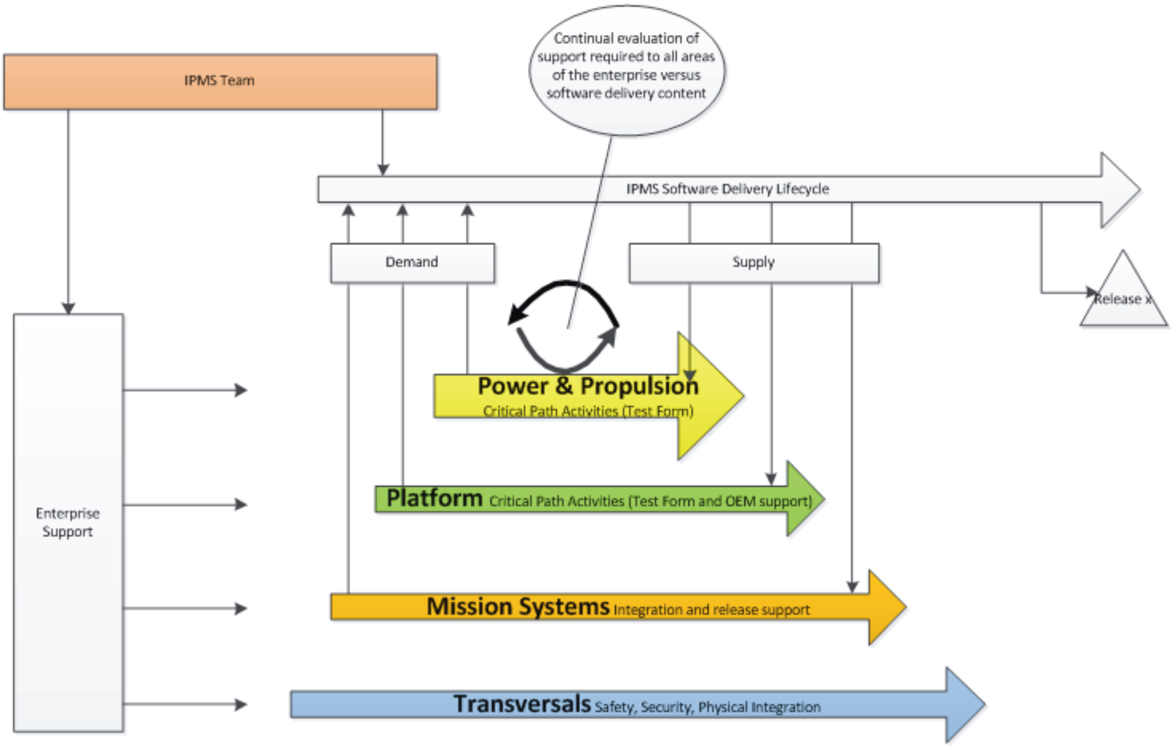

Figure 1: Alliance working – support to the enterprise

Figure 1 above shows how the IPMS team (Thales and L-3) performed together in order to support the overall needs of the enterprise. A customer / supplier relationship was never evident at a technical level – a true one-team approach was utilised to ensure the right people were doing the right job at the right time. Significant movement of personnel between the Thales and L-3 offices in order to support the priority tasks was evident at all stages of the project. This was only possible because of the construct of the formal alliances within the project, allowing risk sharing to drive the best for project behaviours.

4.3. Processes to de-risk the project

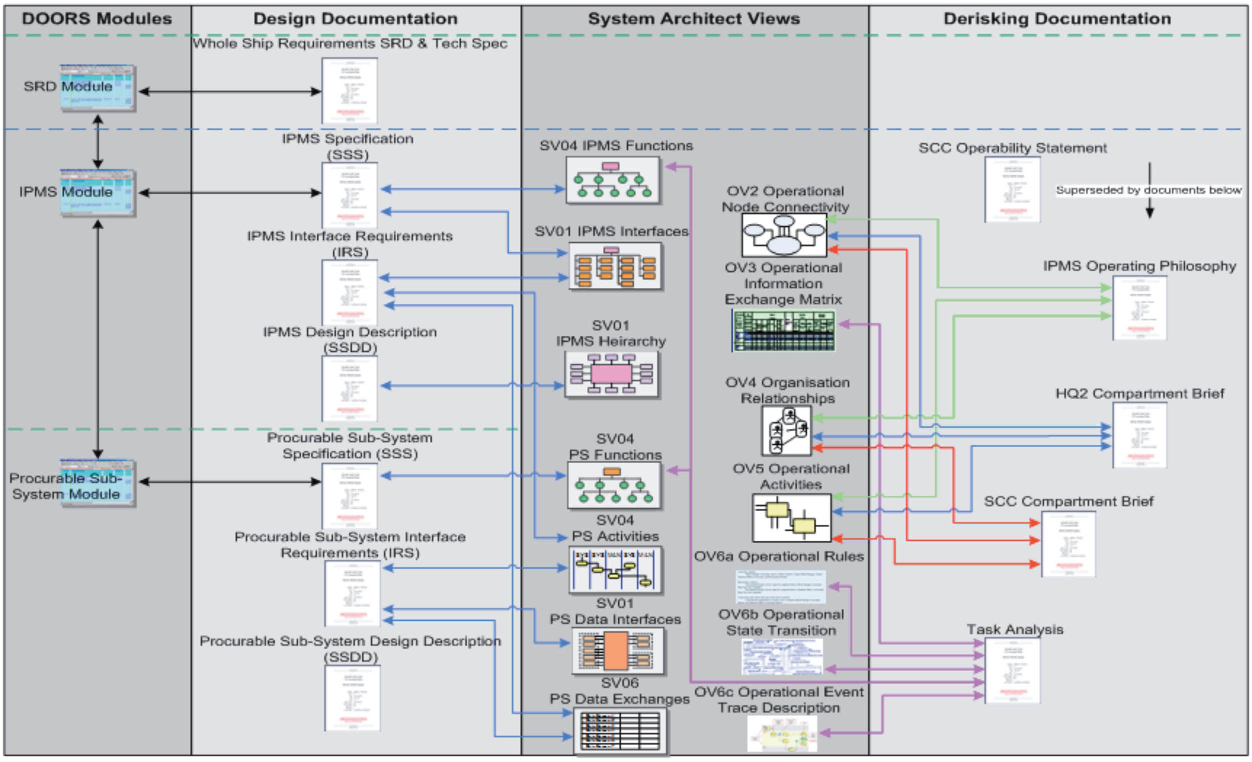

Figure 2: Use of formal toolsets

Figure 2 above shows how the project used a more Model Based Systems Engineering approach. Formal requirements (DOORS) and system architect (SA) toolsets were at the heart of developing the traceable basis for design and for generation of formal documentation. This was a significant departure from previous IPMS designs where more traditional, and less efficient, documentation based design had been evident. This allowed easier and more detailed analysis of control functions that needed further justification for the cost of automation when a trade off with cheaper manual operation was being considered. The risks identified in section 3.6 were one of the key beneficiaries from this process

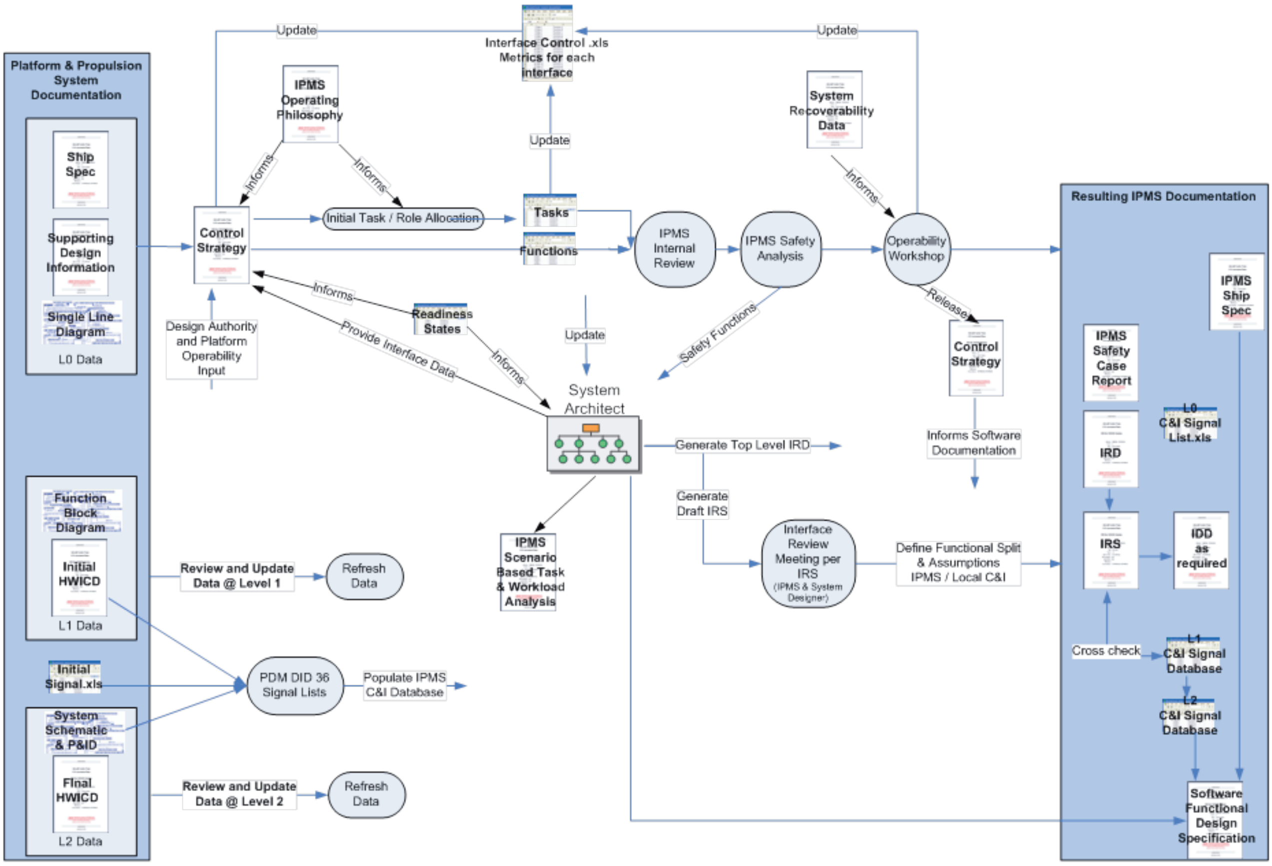

Figure 3: Stage 1 processes

Figure 3 above shows how the stage 1 processes were used to ensure that project supplied information was properly assessed and processed into complete and usable information for the suppliers' baseline documentation. Uniquely, the people who were preparing the information within these processes were often on secondment from the control system supplier, so ultimately, the data was owned by the same person, this was possible because of the sub-alliance construct of best for project resourcing.

4.4. Early and enhanced integration

Testing of the supervisory L-3 CORE software was done to ensure the scale of potential I/O was feasible. A large SIF was agreed as a way to de-risk the new commercial I/O layer together with the I/O testing before delivery to the ship. The De-risking strategy and business case did not support having a full ship set in the SIF, due to the sheer quantity and size i.e. the cost-risk benefit analysis was not met.

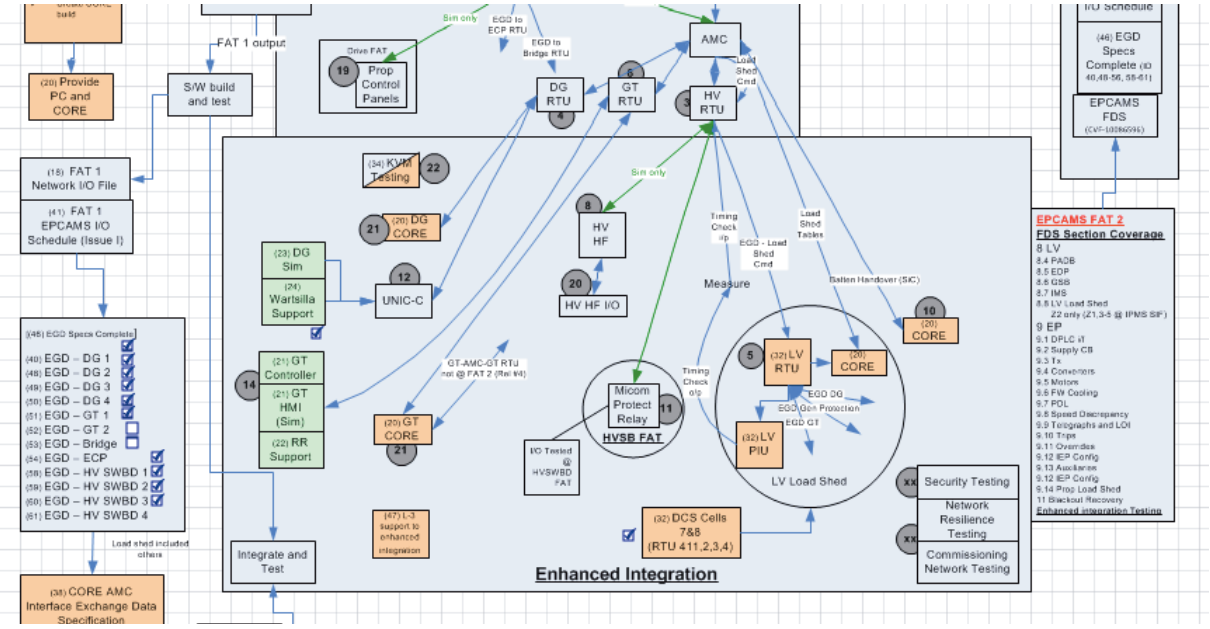

Figure 4: Complex integration to project management linkage

Figure 4 above shows part of the process that mapped the EPCAMS integration activities to the project schedules. This allowed proper agreement of the process by all parties and of project tracking in the run up to deliveries by both companies. This process thus fulfilled the needs of integration and project management. Some parts of this very complex interface were able to be progressively proven in multiple Factory Acceptance Testing (FAT) events due to early integration activities, amongst others shown in Figure 5 below.

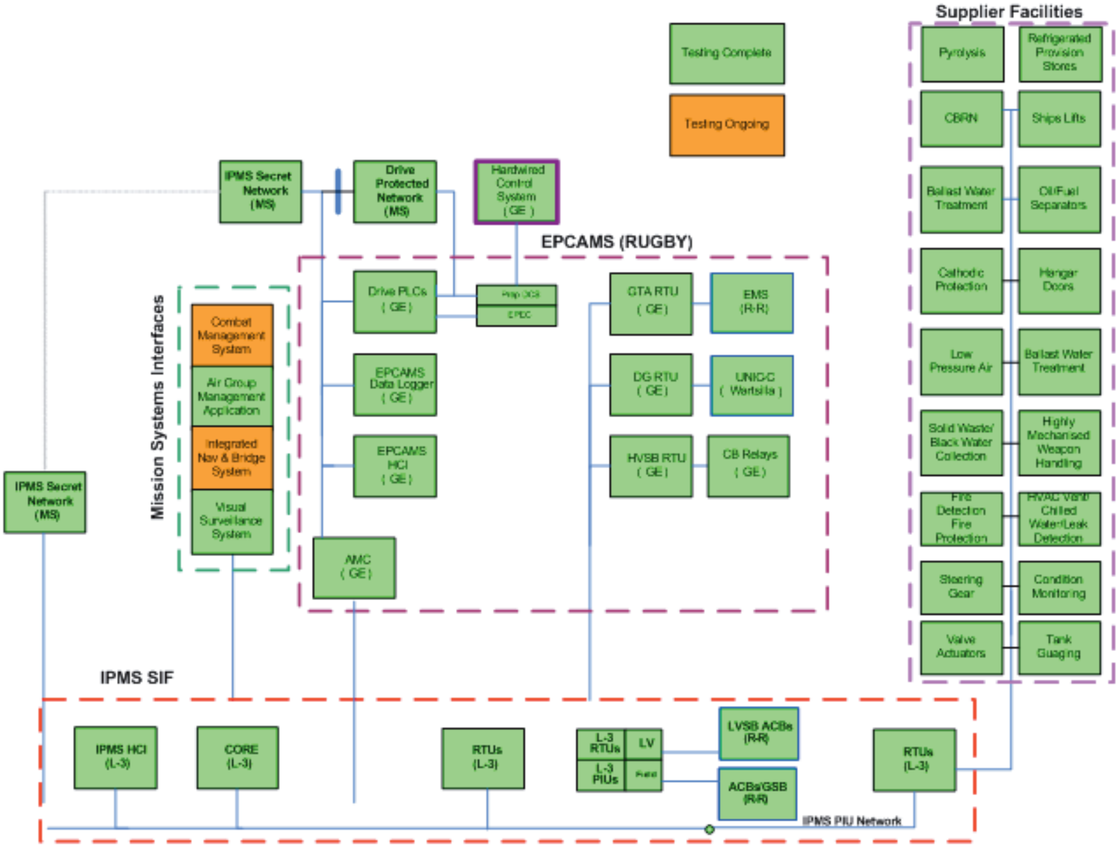

Figure 5: Enhanced integration overview

Figure 5 above shows the overall scope of enhanced integration of QEC IPMS for the interfaces that were deemed necessary for early integration testing and the best location to conduct this testing.

5. Risk Outcomes

5.1. Scale

The EGD interface between the GE Fanuc PLC and the L-3 Core software was integrated ashore to the extent possible with the hardware in the SIF. The de-risking strategy and business case did not support a full scale IPMS off ship, so as more and more systems were made live and fully connected to IPMS, data processing issues became visible. Many late changes to IPMS CORE software were required in order to cope with the eventual full scale of the operational QEC IPMS.

Recommendation 1 – A full ship set ashore is unlikely to be agreed on any project, and in any case large scale, novel integration can never be fully replicated ashore. With this limitation it is necessary to perform pro-active data measurement of PC and software performance both ashore and on the platform to capture problem areas before they start to threaten the project. Consider use of Artificial Intelligence (AI) to predict network and software loading during the design by collecting data and information early then predicting its potential growth. Allow time in the schedule to perform stress testing on the ship, possibly before the large scale, integrated machinery trials commence.

The customer drove the need to provide a COTS solution into the design of IPMS, and whilst industry might be expected to manage the risks of novel architectures, it is true that the enterprise did not fully appreciate the risks that would eventually manifest themselves. Potential suppliers are likely to carry forward software architecture risks into the product in order to try to satisfy top level customer aspirations.

Recommendation 2 – Provide a suitable qualified independent technical oversight during procurement to ensure that aspirations in one area don't result in excessive risks in another.

5.2. System immaturity

Driving the external interfaces to declare maturity early belied the amount of change that would result once the platform integration on the ship was performed. As the largest IPMS interface, HVAC is also the most prone to change from the build process. As advanced as the 3D modelling work was, there were numerous and late changes to HVAC from build which led to very expensive changes to IPMS long after the design baselines were finalised. The bespoke HVAC user interface eventually provided mitigation in this area.

The immaturity of connected systems was true for most IPMS interfaces, and resulted in the amount of software releases to the ship growing from an initial 3 at contract award to 11 major releases and a further 15 minor releases. Initial IPMS software releases were at least 18 months earlier than actually required

Recommendation 3 – Recognition at a project level that immaturity exists to avoid expensive nugatory work on tail end systems such as IPMS. Don't expect IPMS to deliver against immature data, put proper checks and balances in place to ensure the design data from the connected systems is sufficiently mature.

Recommendation 4 – Deliver software when it is really required rather than driving suppliers to inefficient early deliveries. Realistic schedules are essential otherwise early software deliveries are made and inevitably have expensive re-work.

Recommendation 5 – Identify areas of architecture that are not resilient to change and provide early mitigation via tools or software design changes.

5.3. Safety

The IPMS safety case can be regarded as a success. After an initial overly complex assessment, a more pragmatic approach was undertaken which resulted in the correct systems and functions thereof being connected to IPMS. However, duplicate work was undertaken by the ACA and L-3 due to the lack of demarcation in functional safety.

Recommendation 6 – Clear demarcation between companies particularly with regards to interface boundaries to be clearly set out at contract award to avoid expensive duplication of effort.

5.4. Network integration

Detailed network modelling was conducted to confirm that the expected loading from IPMS, EPCAMS and connected systems was compatible with the network configuration both hardware and software. Normal monetary drawdowns from risk to accommodate re-work due to physical changes on the ship were exercised. Performance testing to exercise the expected static loading was performed and confirmed the design expectations. (Notwithstanding the need for dynamic load testing as stated in **Recommendation 1**). Early commissioning networks were necessary and well utilised on both IPMS and EPCAMS sections of the network, cost savings would have been possible by relaxing the need for strong configuration management that was put in place on the EPCAMS commissioning network.

Recommendation 7 – Exercise caution for the level of engineering applied to temporary networks

5.5. Complex integration

The de-risking testing conducted on the complex network / serial interfaces at the suppliers' factories was very successful. This success can be measure by the fact that all interfaces needed software changing during the factory testing which otherwise would not have been found until set to work on the ship. The changes were required despite having agreed Interface Design Documents which were supposed to control the interface. The importance of physically checking an interface works before arriving at ship cannot be understated. Several interfaces continued to change despite the early shore based testing, this was sometimes due to lack of appropriate technical oversight so that impacts were not understood at a project level.

Recommendation 8 – Having the correct technical oversight is essential in order to understand emerging risks to the wider project. This is particularly true for sub-contracts with a mechanical bias, but with significant software content. Ensure that from the outset of the project that sufficient software oversight is in place to ensure management of standalone development and of the interfaces to the integrated control systems like IPMS.

The integration of the GE EPCAMS to the L-3 IPMS necessitated a significant and protracted integration effort which in hindsight was a poorly thought out architecture costing far more than the perceived initial benefits would justify.

Recommendation 9 – Fully qualified independent technical authority to review the complex potential solutions early in the lifecycle to make decisions in the best interests of the enterprise

Recommendation 10 – Ensure complex interfaces are fully documented not just for how data exchange takes place, but also describes in detail the operation of the control functions that exist on either side of the interface

5.6. Correct control and connectivity to remote systems

From a power, propulsion and platform perspective the operability and control design was sound and presented no major re-work during the project lifecycle. An improvement could certainly be made in the readability of the control solution documents. Functional Design Specifications (FDS) are extremely cumbersome and would be better presented as a control summary e.g. a development of early control strategies.

Recommendation 11 – Present the operators with more usable documentation to describe system operation and control

Whilst an SCC mock-up was constructed and several days of walking through normal evolutions in the SCC with the Royal Navy were conducted, more extensive formal trials were not. These could have taken the form of passive and active trials to ensure that all the system users were considered. The IPMS stage 1 design team was very focussed on ME operators and their tasks. The Weapon Engineering (WE) representative at the time was not bought into the principle of co-location in the SCC and so the WE team's roles and tasks were not properly developed, and neither were the interfaces properly matured at an early enough stage to ensure that full data exchanges were part of the design baseline. Late ad-hoc design reviews were attempted in order to try and recover these gaps in functionality, but the interfaces for the weapon repair team remains sub-optimal. Solutions such as Keyboard Video Mouse (KVM) switches to embedded laptops, web interfaces and indeed some interfaces that never materialised after the demise of DII(S), resulting in a patch-work of information that may not fully meet the needs of these operators.

Recommendation 12 – Continue operability analysis beyond the functional modelling and make greater use of physical mock-ups via tools such as passive and active trials to properly exercise the operators within their primary operating positions, ensuring all stakeholders are fully engaged.

5.7. Requirements management

Security requirements on a modern Royal Navy ship need specialist knowledge by the suppliers to avoid late changes as a result of check and penetration testing. Any desire to avoid large cost overruns would need the supplier to guarantee a product that is fully compliant with the relevant government security requirements and that they would employ qualified testers.

Recommendation 13 – Ensure suppliers have appropriate system security expertise to ensure compliant systems

6. Conclusions

6.1. Areas of greatest benefit

Main Alliance and Sub-alliance working has undoubtedly been the greatest benefit for a difficult and complex integration project. It breaks down stove pipes and supports greater integration across product streams. It has allowed more inclusive and open discussion about areas of risk and resolution. This removes the difficulties that may be more evident in a classic customer / supplier contract.

6.2. Areas of greatest manifest risk

- Influencing a suppliers' preferred architecture to meet perceived wider enterprise needs will inevitably lead to risks that are difficult to quantify at the outset. The enterprise needs to be sure the benefits outweigh the potential risks, particularly during the early stages of the project when the desire to please is greater than the desire to be risk averse.
- Equally allowing suppliers to influence architectures that are not least risk need to be carefully considered
- Immature interfaces and immature design that drive in change and cost, needs proper recognition to avoid expensive nugatory work

All of these risks could be reduced by having sufficiently empowered, properly qualified and independent technical oversight of high cost, high risk areas of the project.

7. Acknowledgements

Review and assessment of this document was carried out by Warren Mallia and within Thales UK by Jim Bennett, Graham Thomson and Stuart Jewell.

8. References

None