T26 PMS – Real time Control of Power Generation, Propulsion & Auxiliaries

Will Miners*[1], MEng MIET, Harry Arikkat[2], MSc MEng MIET

L3 MAPPS Ltd, UK
*Corresponding Author. Email: will.miners@L3T.com

Synopsis

The Platform Management System is a key component of a lean-manned ship. Centralised remote operation removes manpower from machinery spaces, while advanced algorithms and increased integration simplify the operators' daily tasks enabling them to broaden their responsibilities. This inherently results in driving down costs and increasing efficiency. There are a great many benefits to increased automation, however a reliance on these systems means placing a greater focus on the up-front engineering effort required to make a safe and secure system which meets the needs of the user. Sometimes, however, requirements can evolve in early stages of a project, so it also needs to be able to adapt with a flexible design able to cope with inevitable change.

Strictly following a traditional V-model lifecycle can ensure compliance against customer requirements, whilst emerging requirements and user experience factors can be overlooked. A collaborative approach involving stakeholders throughout the design lifecycle helps to reduce overall programme risk by reducing change and providing progressive assurance. Through this collaboration throughout the design process and the incorporation of innovations from outside the marine industry, the T26 PMS design has evolved into a flexible, scalable and user centric solution. The innovative solution now in place can meet a plethora of challenges, incorporating safety, security and the performance required of real-time control. Safety-accredited components are used to support emergent safety requirements, while a distributed architecture both increases resilience to battle damage and scales to system load. Human factors, often placed at a lower priority than "hard and fast" requirements, have been a key design driver, with the dichotomy between safety and operability being confronted regularly throughout the design.

Following a system-of-systems approach, the development team pick a component of the PMS and take a deep-dive into the subsystem development, demonstrating the incorporation of safety, human factors and security into the design as early as possible. The paper then looks forwards to the future of the project, and the "right side of the V", showing how a proactive approach to assurance and acceptance can help reduce overall programme risk.

Keywords: Type 26; Platform Management System; Real time; Automation; Safety; IEC61508

1. Introduction

The Type 26 frigate will be one of the most advanced warfighting ships in the world, bringing a 21st Century combat capability to the Royal Navy and its allies. Supporting its combat power are the marine systems and the Marine Engineering department – the "beating heart" of a platform capable of fighting a multitude of threats.

Against the political realities of competeing spending priorities, but with increasingly complex platforms being developed, the industry – like others – has turned to automation and advanced technology to solve the problem. For the Marine Engineering department, the answer is the Platform Management System, usually referred to as the PMS or IPMS. The PMS is responsible for providing integrated control and monitoring of ship power generation, propulsion, electrical functions, auxiliaries and damage control machinery and systems. PMS is also able to support wider mission operations by facilitating information exchanges between non-marine (Combat) systems. This increased level of system integration across both the marine and non-marine systems has allowed the lean-manning of the ship, whilst simultaneously increasing the capability of the ship through automation by utilising advanced algorithms.

Like the ship itself, the T26 PMS will be cutting-edge, relying on a combination of proven and newly-developed technologies to support the increasing demands of a modern navy. Already a complex project with -thousands of hardware and software components, the modern PMS development also needs to consider the latest thinking in safety and security engineering to ensure that the system will be safe and usable many years into the future – and to ensure it still carries the functionality that is expected. The T26 PMS will be a true 21st Century

Author's Biographies
Will Miners is currently a Senior Software Engineer and the Software Lead for T26 PMS at L-3 MAPPS Ltd-UK, having worked at the company for five years. Prior to that, he attended the University of Bristol, achieving a MEng in Computer Science and Electronic Engineering.
Harry Arikkat is currently an Engineering Graduate L-3 MAPPS Ltd – UK, having held the position for one and half years. Prior to joining L-3, he worked as Research Assistant at University of the West of England. He holds an MSc in Mechanical Engineering from University of the West of England and an MEng in Integrated Mechanical and Electrical Engineering from University of Bath.

 http://doi.org/10.24868/issn.2515-818X.2018.040

PMS, with safety and security integrity requirements placed upon it from the start and considered throughout the entire engineering lifecycle . The fundamental architecture has been updated to reflect this, resulting in a system which is flexible enough to handle any safety-related functions which may be identified, while being resilient to cyber threats.

2. The Modern Platform Management System

Any opportunities to reduce manning levels must be balanced against the need to remain resilient to and recover from war-fighting damage. In a combat ship such as T26, the manpower demand is determined by the States of Readiness or action states deployed by the Royal Navy. By aligning the action states to the operational scenarios for PMS use, it is possible to reduce the manpower and thus achieve the necessary lean-manning profile for the ship. For example, Propulsion and Auxiliary Machinery equipment could be operated by minimum manning during 'Peace time Cruising', as low as one operator at the control position with a further rounds man visiting key compartments of machinery. For the action state 1 and 2 where there is an increased risk that the ship will take battle damage, this number can be increased as deemed necessary to recover capability from damage as efficiently as possible.

The PMS can provide operator-initiated automated tasks or semi-automated tasks that requires operator authentication at specified stages, for controlling and monitoring. This in turn, increases the autonomy of the system and reduces the workload on the operator considerably. An example would be the ballast transfer, where the transfer is initiated by the operator, the PMS then aligns all the necessary valves automatically and the operator can monitor and sometimes control all the necessary parameters in real-time through the display console.

The PMS provides centralised remote control of its marine functionality, allowing the operator to assume full control and monitoring of the required system or equipment from a separate location within the ship. This aids in implementing the Damage Surveillance and Control (DSAC) doctrines effectively, as all the PMS consoles are updated with automatically with damage information, which PMS automatically acquires or could be entered by an operator at any console. On top of that PMS provides the a real-time, full and up-to-date information on the damage situation of the ship, through the support of advanced alarms and warning processing techniques, kill cards and ship stability salculations.

Although the increased automation and intelligence reduces the human error and lowers the operator workload considerably, there is a great need to ensure safety and security of the remaining operators, the surrounding environments, and the system as a whole. This is achieved by placing a greater focus on the up-front engineering effort, as early as requirement capture and analysis stage with a flexibility to adapt and cope with inevitable change throughout the design and development process.

3. The Challenges

There are great many benefits to the increased level of automation, however designing and delivering these systems to the quality required by the user poses a number of challenges, each of which must be managed throughout the lifetime of the ship. A project such as the T26 GCS, which will become one of the most advanced warships in the world after commissioning, is large and complex; like any other complex project, the development can be fraught with a variety of risks, both technical and schedule-based.

As the PMS design incorporates increased levels of automation and integration between various systems on-board, one of the biggest challenges of such a project is managing schedule and cost risks, which are predominantly caused by scope creep. A number of factors could fuel this, from adding requirements at later stages of the project by the customer through to gold-plating of the system by developers. Scope creep is directly proportional to cost increases and schedule delays, which means the importance of up-front engineering of the system is higher than ever before. Changes and new functionality are inevitable however, so the system and programme must be created with adequate flexibility in the design to handle this. Hence, having a collaborative approach and communication involving all the stakeholders is paramount to define all the requirements clearly for the system at early stages of the project. Moving forwards, effective change control and configuration management need to be in place to ensure that new functionality has little impact on the existing project.

The PMS, which has already evolved into a complex integrated system, could face further challenges, incorporating safety, security and the performance required of real-time control. As described in the Platform Management Systems Paper at the INEC conference in 2016, the most visible challenge surrounding the complex integrated systems has been the issue of security, in particular the dangers of connecting systems without adequate security measures (Miners, 2016). For example, the absence of appropriate user access control permissions, would

 http://doi.org/10.24868/issn.2515-818X.2018.040

allow unauthorised and untrained users to take control and operate part or whole of the system, which could lead to potential damage or a major catastrophe.

Another design challenge for PMS is the safety aspects of the system. Running hand in hand with security, the engineers must ensure that the safety aspects not only for the whole system, but also for the remaining operators are balanced against the increased level of automation. The automated functions implemented in the system must be designed to ensure safety in event of a failure. Commercial Off the Shelf (COTS) components that are used, to assist PMS to increase automation while minimising the through-life cost, must be assured commensurate with appropriate safety standards. Safety assessment must be applied to both the hardware and the software, analysing all the hazards and applying appropriate mitigation measures, to reduce any risk to a functional entity to an "As Low As Reasonably Practicable (ALARP) level.

Human factors, often placed at lower priority then "hard and fast" requirements, plays a significant role in augmenting the safety aspects of the PMS system. The PMS system is only considered safe when the system operator can operate the system on daily basis without causing any injuries. This means appropriate ergonomic factors and anthropometric data for both male and female operators must considered while designing the operator consoles. Their proximity between the other operators, lines of sight, orientation and display feedback are also considered during the design.

Other transversals such as shock, temperature and humidity, water and particle ingress and Electro-Magnetic Compatibility (EMC), also need to be considered. Specified early as requirements, the domain specialists who design subcomponents of PMS must remember to incorporate them clearly into the design, while balancing these requirements against cost and spatial constraints to ensure that the hardware products are not over-engineered. Addressing all these challenges and achieving a balance plays a key role is making the PMS system acceptable to the customer. With the PMS being the brain of the ship and being in operation for multiple decades, it is important to enhance the autonomy and the integration by achieving the right balance in all the above mentioned challenges and risks to deliver a cost-effective PMS solution acceptable for end-user.

4. The Solution

The PMS solution is a physically distributed real-time digital control and monitoring system, which employs a combination of Commercial Off the Shelf (COTS) hardware and modified proprietary hardware and software to deliver the required systems functions. These hardware and software comprises of multifunction control consoles and distributed I/O controllers (See Figure 1), providing a degree of autonomous control and monitoring functionality to many systems throughout the ship. The distributed nature of the design means that the system is resilient to battle damage and hardware or software failure, through a combination of redundancy and fall-back modes. Even if the ships network infrastructure were to fail, PMS operators could still continue to operate from strategically placed operating positions.

 http://doi.org/10.24868/issn.2515-818X.2018.040

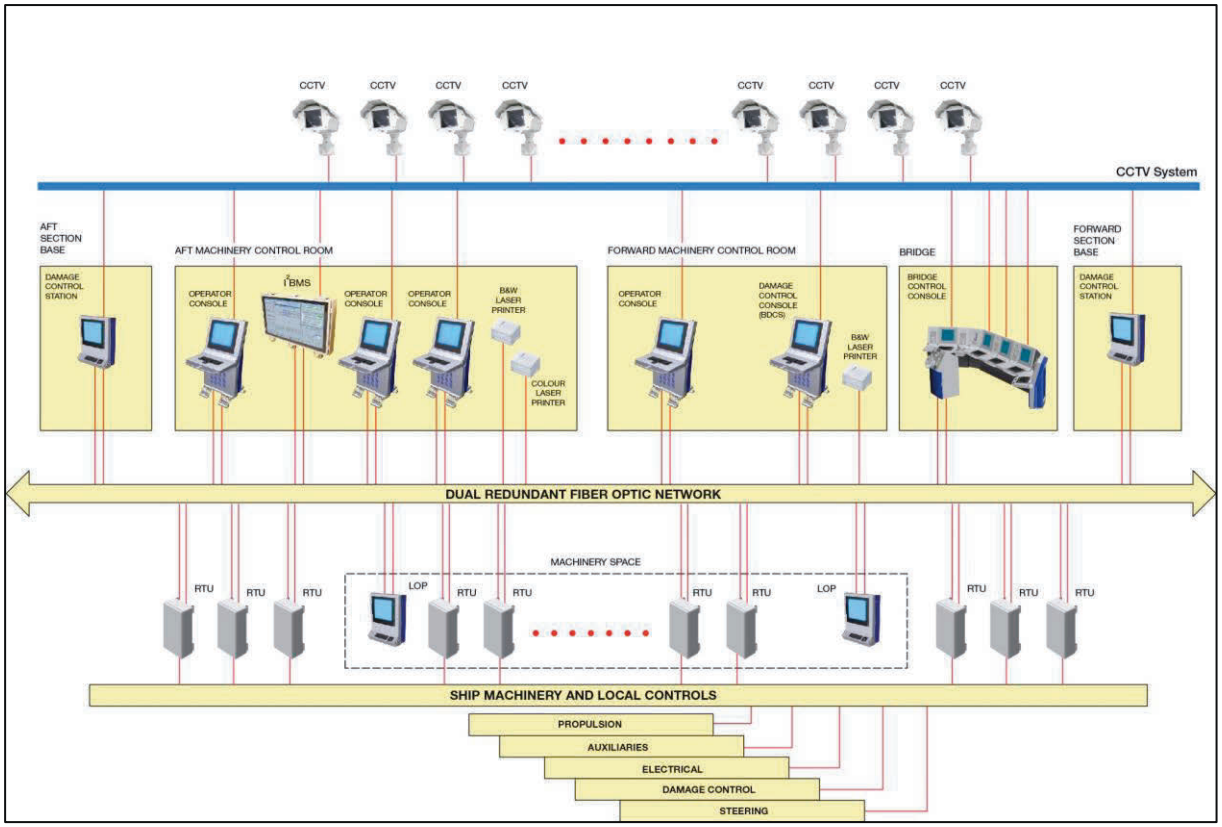

Figure 1: Typical IPMS Configuration (L3 MAPPS, 2017)

At the heart of the PMS lies the CORE software, a distributed database which provides a real-time view of all monitored signals at any PMS console on the ship. Sitting atop this is the HCI, hosting system mimic pages and providing features such as user account management, alert management, and "Station in Control". A distributed control system layer, hosted on COTS industrial logic controllers, provide data collection and simple automation. Each of these components is used in order to provide the operator with a series of "applications" – logical groupings of control functions for some platform system, such as a diesel generator or ballast system.

Some of these application functions will be considered as "safety functions" as they may contribute to a significant hazard on the platform. These functions, and the software supporting them, will be treated with a higher level of integrity than others, in accordance with the BS EN 61508 functional safety standard. It is important to separate these safety functions from any others, to avoid any interference between software components and support the system safety case. To enforce this separation, a real-time operating system (RTOS) has been selected, with a virtualisation capability to host another guest Operating System (OS). This provides the functional separation needed, so that any of the lower-integrity software – or the guest OS itself – fail, then the isolated safety functions can continue to operate as normal.

The "front-end" of the PMS – the HCI – is available to operators from a number of dedicated PMS consoles in strategically placed locations around the ship. In addition to this, operators can use any number of shared consoles to view and control PMS while also operating other software systems provided by other suppliers, such as combat and navigation systems. This flexibility further supports the lean-manning goal, and potentially opens up the future prospect of cross-functional operation between the marine and combat engineers.

5. The Lifecycle

The design of a large and complex system such as PMS must balance the need for enhancing integration and autonomy with safety, security and other transversals required for modern times, while delivering a cost-effective solution which meets the end-user needs. For T26 PMS, this is achieved by rigorous Systems Engineering approach to lifecycle management based on the standard V- model. The schema shown in Figure 2 depicts the overall approach to the system design that has been adopted. The T26 PMS comprises of many external interfaces to the ship equipment and other ship systems, hence a phased development strategy has been adopted, with each

 http://doi.org/10.24868/issn.2515-818X.2018.040

component and interface of T26 PMS due to be designed, tested and integrated over a number of incremental releases.

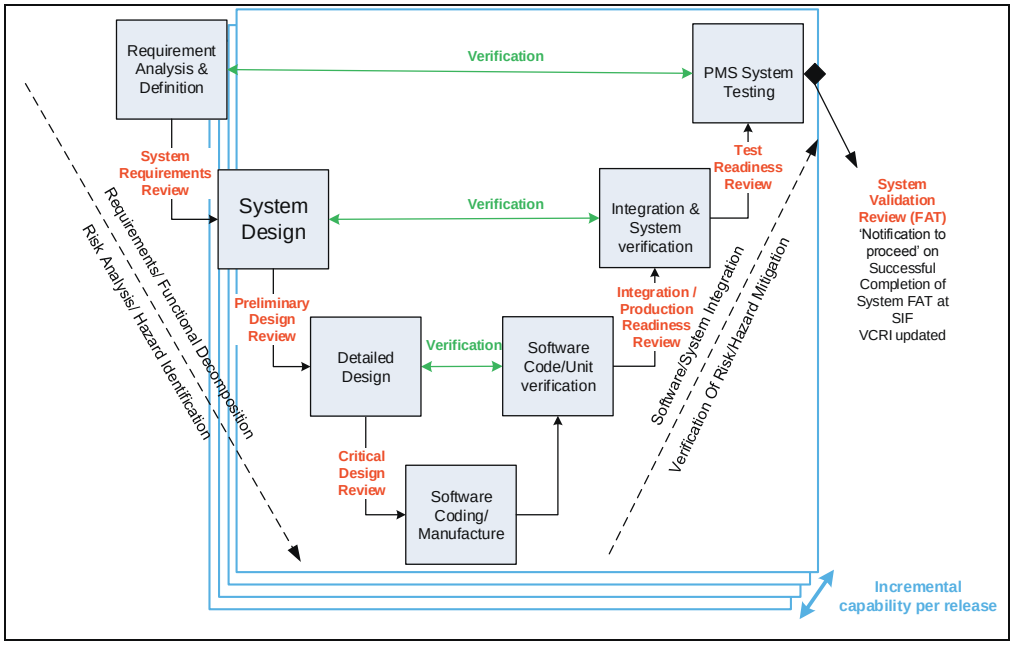

Figure 2: V-Model Development for T26 PMS

The left side of the V represents the T26 PMS design through the decomposition of Whole Ship Design (WSD) requirements into functional and physical entities that can be architected, designed, and developed. System, Performance and Transverse requirements including Security are defined and the top-level system design is formulated during the Requirement Definition and Analysis stage. Safety is incorporated from this stage itself by conducting an initial safety and environmental hazard analysis as well as Failure Mode Effects Analysis (FMEA). These will be matured as the system design progresses through the life cycle. This applies to the hardware components where the Critical Design Review (CDR) is considered as the approval for prototype manufacture and qualification testing. The right side of the V represents integration of these entities (including appropriate testing to verify that they satisfy the requirements) and their ultimate acceptance onto the T26 platform, where they will be operated and maintained.

Building on the successful approach employed the throughout the development of the PMS for the Queen Elizabeth Class (QEC) aircraft carriers (Escott & Ellision, 2012), the most practical and suitable approach to deliver T26 PMS is to adopt a phased (over several) software release model, thus allowing for data and requirement of less mature systems to catch up. This also provides an opportunity for early integration between selected interfacing systems and equipment. The phased release model allows for concurrent development of sub-system software, in which the contents of the each release is defined through advance agreement with relevant stakeholders on a risk basis with access to each development phase being controlled by the review process that act as project "gates" which control the sequencing of development activities. Each review process determines the maturity of the design being put forward whilst assessing the risk of change or design complexity. It is important to acknowledge the fact that the maturity of between interfaces may be progressing at different time scales and the anticipated rework is accommodated.

The T26 PMS system consists of individual items known as Hardware and Software Configurable Items, or HWCIs and CSCIs respectively, which are commonly known as sub-systems. Two groups; System Software, which provide the software backbone of the entire system and Application Software, which provide the software configuration for specific applications and use cases within the PMS, define the CSCIs. These are then split further down into Computer Software Items (CSC), which form the individual component of the CSCIs. By treating these individual components as mini-projects, multiple applications can be developed in parallel and brought together at the integration stage. This approach can however carry a risk of "siloing", where individual development teams are isolated and do not think of the "bigger picture". To counter this, Whole System Design Review (WDSR) is conducted once the Preliminary Design Review (PDR) of all subcomponents is complete. This review focusses on the interfaces between components and the architecture as a whole, to ensure the transverse requirements of the

 http://doi.org/10.24868/issn.2515-818X.2018.040

whole system are incorporated correctly into the design. This WSDR is conducted again during the integration process, ensuring the reliability of the whole system.

6. The Example

By way of a subsystem example, we will investigate the development of a particular PMS component – the Human-Computer Interface (HCI). Often a highly emotive topic, the design of the HCI is subject to a variety of hard and soft requirements, in addition to the design tastes and opinions of a variety of stakeholders. This is not said to discount these opinions, however it is often said that requesting feedback from 5 people on a user interface design will result in 6 different options! Further adding to this is the complexity of safety, as the HCI design must find a way to host both safety-related and non-safety-related functions at a single console, with the design intent of this split ideally appearing seamless to the operators.

The first stage of such a development involves capturing the applicable contractual requirements on the system, and then deriving them down to the subsystem. In the case of the HCI, this includes specific functionality requested by the customer, performance requirements for that component, safety requirements, and generic Human Factors requirements. In addition to this, there are number of other factors used to guide the initial design: lessons learned from previous projects, industry standard practices and operator knowledge are all used to feed into the design.

A key guiding factor throughout the design is the training burden and familiarity. At first glance, it seems as though exactly replicating the UI design from other RN platforms may be the ideal solution, as it will breed familiarity through the Service, while reducing the overall training burden when staff are moved between platforms. Familiarity, however, is not just referring to familiarity with Platform Management Systems. Younger operators are joining the Navy who have grown up using smartphones and tablets, and they have expectations as to how computer-based systems should be operated. Learning lessons from these systems and drawing on extensive R&D by other technology companies is extremely important to ensure that operators find a PMS easy to use. During early HCI design, advice and opinions were sought from various people including non-engineers, and crossing a wide range of ages. Their valuable feedback was used to guide the design, despite many of them having never operated a PMS before. The design guidelines provided by Apple and Google for application development were also consulted, enabling the PMS developers to build upon a vast wealth of research and development by these companies.

Once formal requirements have been captured and design goals set, it falls to the software engineering team to produce an initial workable design. Draft interface layouts are created, starting with pencil sketches and maturing into wireframe prototypes – examples from an early design concept are shown in Figure *3* and Figure *4*. Internal reviews are held at this stage, calling on key stakeholders to provide input and iterate the design. At this stage, four main questions are asked: Does the design meet the requirements? Does the design follow Human Factors guidelines? Does the design make sense to an (ex) operator of a PMS? Is the design safe?

 http://doi.org/10.24868/issn.2515-818X.2018.040

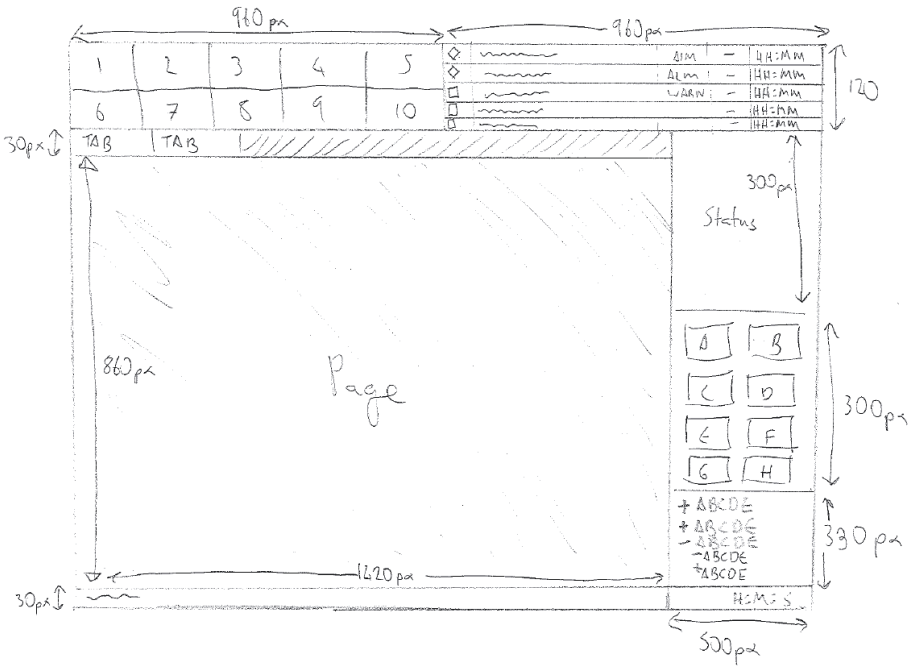

Figure 3: Initial Pencil Sketch of UI Design

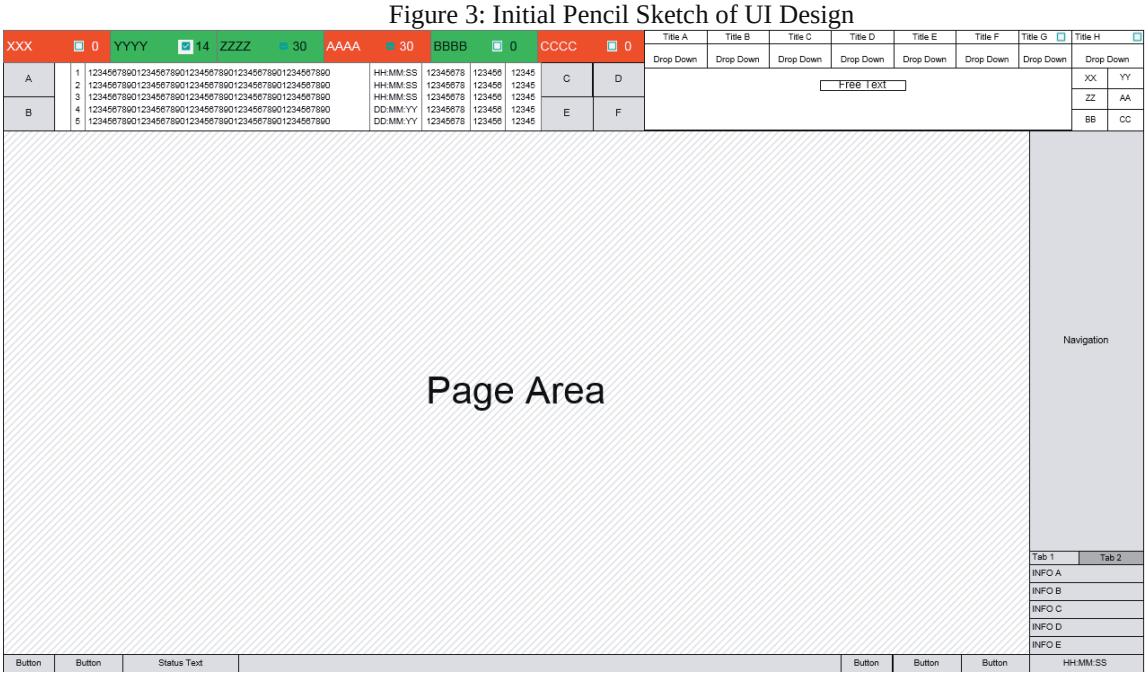

Figure 4 Wirefame Layout of UI

If these questions are satisfied, the process continues. A Style Guide is drafted, summarising the key design elements and the rules for detailed design for the software engineers to continue their work. This Style Guide, and other early prototypes provide the ideal basis for early assurance, enabling the initial design to be shared with external stakeholders before detailed design is continued. To this end, a stakeholder forum is held, with invitees from across the spectrum of end-users, customers, and human factors experts. Again, the key questions are asked, with the feedback incorporated into further iterations of the preliminary design and Style Guide. This early stakeholder feedback is an important way to de-risk the design of an area which is seen by many to be the most important component of a PMS. By ensuring this happens early in the development process, costly re-work is avoided, while ensuring the end-product meets the needs of the users.

 http://doi.org/10.24868/issn.2515-818X.2018.040

7. The End Goal

Of course, the end-goal for any subcontracted development, and a measure of success for the programme as a whole, is acceptance of the product by end-users. For such a large and complex project, it is clear that waiting until the end of development for acceptance is a risky endeavour. As seen in the HCI development process, early stakeholder involvement helps to de-risk customer acceptance, and this model can also be used for contractual acceptance. In the PMS programme, a variety of methods have been used in order to provide this assurance throughout the programme, ensuring that the overall risk is reduced throughout development.

As an example, consider the security design of the system. While there are a number of "hard" security requirements identified in the requirements set – such as to ensure system access is limited by username and password – there are often more subtle parts of the security design which must eventually be accepted by the platform accreditor. Ultimately, acceptance of the security design lies in a risk balance for the perceived security threats to the system, and presenting a final design to an accreditor sight-unseen is a poor choice. For the PMS development, security has again been incorporated early in the lifecycle. A series of regular security working groups have been held, ensuring all applicable stakeholders have been included to discuss the security aspects of the design from the earliest stages. As the design matures, findings and queries are discussed at the working group, enabling feedback to be incorporated as early as possible. As the project moves into the delivery phase, the system will eventually be subjected to a series of penetration tests by security experts. In the phased release model of the PMS software, a first test will be conducted on an early software release, ensuring that any recommendations or changes can be incorporated into a future release for the second round of testing.

The system-of-systems approach to engineering the PMS also provides a level of assurance to stakeholders that the overall system will meet the intended design and functionality, and in turn the contractual requirements. As described previously, each subcomponent is subject to a set of design reviews as the development matures. Each of these reviews is an opportunity for both internal and external stakeholders to comment on the design, providing a greater level of confidence that requirements will be met.

The phased software release model provides a further opportunity to de-risk acceptance. Key functionality and requirements with a high perceived risk will be demonstrated in earlier releases, ensuring that any required changes or fixes can be included in a future release before delivery to ship. The combination of this approach with stakeholder involvement throughout the design process means that final acceptance is greatly simplified, with less reliance on multi-day acceptance events.

8. The Future

Like the overall ship programme, the PMS programme has a great many challenges ahead. Proceeding into detailed design, the burden is now on the integrated project team to deliver a cutting-edge automation system on time, to budget, and to the quality the Royal Navy expects. By adapting a rigorous engineering approach, while still allowing flexibility where required, the PMS project is rising to the challenges and proactively managing risks. While the basic approach is tried-and-tested, the unique difficulties posed by this development have required a new look at the standard lifecycle, ensuring that all transversals can be considered and met.

In addition to this, further efficiencies are being investigated to help keep the system affordable and resilient to any incoming change. Where possible, automation is being considered for the development of the system itself. Investigations are underway to consider the automation of cable allocation, schematic drawing, and parts of the software development. If successful, this could mean that a change to ship equipment does not necessarily result in a significant update to the PMS configuration – an updated input file could be imported, and the subsequent design artefacts generated at the push of a button.

The challenge has been set. A flexible architectural design, a rigorous approach to data and requirements management, and a proactive risk management plan are all tools which will be used, and which should make the task easier. The job now lies with the delivery and engineering teams to continue the work, and ensure the success of the project.

9. Acknowledgements

The author would like to thank Liam Cody, Principal Systems Engineer at L-3 MAPPS Ltd. for his invaluable guidance that helped for the completion of this paper.

 http://doi.org/10.24868/issn.2515-818X.2018.040

10. References

Ellison P & Escott H: “Current development in the systems engineering of the IPMS for the Royal Navy’s Queen Elizabeth Class Carriers”, Proceedings of International Naval Engineering Conference 2012, Edinburgh, United Kingdom, May 15-17 2012.

L3 MAPPS: “Integrated Platform Management System”, Product datasheet, January 2017, Accessed at: http://www.mapps.l3t.com/datasheets/Marine/L3M_DS_IPMS_011117i.pdf

Miners W: “Engineering the Adaptive Platform Management System (PMS)” , Proceedings of International Naval Engineering Conference 2012, Bristol , United Kingdom, April 26-28 2016.

 http://doi.org/10.24868/issn.2515-818X.2018.040