2018-09-26

A Virtual Teams Model for Supporting Maritime Technology Management

G Berner University of Tasmania, AUS
R Hopcraft Royal Holloway, University of London, UK
J Scanlan University of Tasmania, AUS
M Lutzhoft, Western Norway University of Applied Sciences, Norway
J Earthy Lloyd's Register, UK

SUMMARY

Computer and networking technology on board ships is increasing in complexity as the levels of automation and monitoring at sea evolve. Ships are acknowledged to be a System of systems, including both IT (Information Technology) and OT (Operational technology). A virtual team that includes members of the various on-board departments, shore based technical support staff and vendors perform management of technical equipment, largely in isolation. It is possible to conclude that the technology installation is one of the only operational aspects of a vessel, where no one has the full picture and could drive a coordinated response to a major technology issue. This paper will propose a best practice framework for governance of technology on board ships. This framework will serve as an input to the process of including cyber security in the ISM Safety Management Manual for the 2021 deadline.

1 INTRODUCTION

The increasing growth of Information Technology (IT) and Operational technology (OT) on board sea going vessels is a response to the environment of increasing competition and regulation in combination with a reduced complement of seafarers. This has resulted in a developing reliance on integrated technology systems for day-to-day ship board operations [11]. The use of technology also supports the expansion of shore based monitoring and control [15]. The use of shore based personnel to perform support functions for ship based technology is a growing trend in maritime technology management where the responsibility of operating and maintaining maritime systems resides with a ”virtual team” including members of the vessels crew, shore based operators and technology vendor staff. Achieving the goal of reliable technology in any field of endeavour requires well-designed solutions that are maintained according to good engineering practice with appropriate governance systems overseeing their operation. In many cases the management of technology on board ships could currently be characterised as being ad-hoc. The technical capability can be represented as a collection of islands of expertise/practice with little standardisation, making them worthwhile candidates for maturity uplift through the implementation of IT Service Management (ITSM) [5]. IT Service Management has been identified by [5] as a method for providing stronger alignment between technology and its consumers, improved service delivery and utilization of resources.

Robust IT governance systems have demonstrated that it is possible to reduce the potential for operational failures in critical systems [7]. A failure of critical technology can endanger life, property and the environment. An example highlighted by [16] demonstrates a lack of cohesiveness between a virtual technology support team and consumers of the technology service placed a vessel at risk. In this case, a software patch was installed remotely by a service engineer who was unaware of the operational context of the vessel at that time. The vessel was the process of berthing and the install resulted in a system reboot that stopped the engine room ventilation system, and subsequently left the vessel without propulsion at a critical time while it was manoeuvring.

Since the 1990s technology organisations have been using governance frameworks such as the IT Infrastructure Library (ITIL) [7] to provide significant benefits to their respective organisations through rigorous control of testing and system changes, resulting in more predictable infrastructure, reduced faults and consistent handling of technology incidents. Organisations who have adopted these technology service management frameworks enjoy cost effective services, reduced downtime, improved security and higher customer satisfaction [5]. This paper will discuss the potential for increasing the maturity of technology service provision on sea going vessels through the use of an IT governance framework.

2 MARITIME TECHNOLOGY SYSTEMS MANAGEMENT AND ITS CHALLENGES

While there are currently many technology companies providing shipboard solutions to the maritime industry, historically the industry has lagged behind other shore based industries in adoption and governance of new technologies. The global focus on cyber security over the last few years has led to activity in the development of guidance and regulation. This includes the IMO releasing requirements for management of cyber risk [9], and various other maritime organisations releasing technical papers and guidelines - [3], LR [14], DNV [6]. There are also a number of standards being developed that address maritime technology, The International Standards Organisation is currently drafting ISO-19847 and ISO-19848, specifying minimum standards for on-board computing and communications. Despite these recent efforts, the overall current maturity of IT service provision is low, and time and commitment are required

from stakeholders to reach a suitable level. The following sections discuss some of the challenges ahead.

Technology management on sea going vessels can be described as having a relatively low level of maturity. Two well-known aspects of this are software quality [2] and cyber security [9]. These challenges are symptoms of a unique and complex operating environment that often features different stakeholders managing parts of the technology infrastructure in isolation. Company technologists, seafarers and vendors all participate in supporting and operating the specialised equipment that is installed on-board. There are however few, if any, processes around over-arching technology governance.

A new vessel entering service is designed for an operational lifespan of 25 years [8]. Technology systems, both hardware and software are supported by their respective vendors for only short period of time relative to the lifespan of a ship. Once hardware and software reaches it's 'end of support' date, software and firmware upgrades are no longer provided reducing the reliability of the technology. Many vessels in the worldwide merchant fleet rely upon legacy hardware and software that is no longer supported by vendors, placing them at increased risk of technology failure.

With respect to configuration management the nature of the technology installation is such that changes to installed software, hardware or configuration are typically made directly into the 'production' system, as there is often no test network available that would allow for full validation of the change prior to implementation. This is a significant deviation from best practices used ashore when making changes to production [12].

2.1 COMMUNICATIONS

Vessels travel around the globe and are often reachable only via low bandwidth / high cost satellite communications, limiting the opportunity for remote shore based technical support. Due to the limited physical access to systems the downloading of updates and patches increasingly needs to be performed remotely via a limited bandwidth connection [14]. The size and release frequency of software patches for operating systems alone may challenge the total bandwidth available to the vessel, resulting in patches not being installed when required.

2.2 OPERATIONAL CONSIDERATIONS

The role of seafarers has changed significantly in recent decades, with automation playing an ever-increasing role in day-to-day operations. While this has increased efficiency, offering a steady reduction in the number of people required to operate a vessel, there are other trade-offs that need to be considered, particularly in the context of a geographically distributed virtual team. The current generation of ships are inadvertently provided with remote team members performing tasks such as system monitoring, performance optimisation, software patch installs and in some cases system control [16].

Physical maintenance of technology systems is often performed in port by technicians that may not understand the history of the vessels systems and who will be operating under the vessels tight schedule, leaving limited time for testing and fine tuning of systems.

Controlling and authorising changes made to technology either as configuration changes or software updates are critical to the reliability of the systems. Supporting this and equally important is the capability for centralised management of problems and incidents [5]. While developing these processes and artefacts may be seen as a significant outlay in time and resources, there are opportunities for return on investment where system downtime can be reduced or removed as a result.

2.3 TEAMWORK

Every team requires a number of elements to make it effective - a clearly understood shared purpose, leadership and defined roles for team members. [15] has identified that challenges currently exist within the virtual team due to the lack of a central point of oversight. Off-ship support staff may also be impacted by time zone differences. The effectiveness of a fragmented workforce must also be considered in maintenance / breakdown repair activities and most critically in response to an emergency situation. Where somewhat tenuous communications links are relied upon for team coordination, consideration must be given to process that defines actions that are taken in the event of loss of team communications.

2.4 MANNING

The manning levels needed to operate a vessel safely are defined through a process known as MSM (Minimum Safe Manning). This process requires consideration of risks associated with the sudden failure of critical equipment [15]. When consideration is given to the reduction of crew, the use of shore based resources as part of a virtual team and the increasing role of automation, it is necessary to ask whether it is realistic to revert to manual methods in the event of a broad failure of on-board technology. A scenario such as the Slammer Worm, that was released in 2003 has the potential to simultaneously impact multiple critical systems, as happened in the case of the Davis-Besse power plant in Oak Harbour, Ohio [4]. In the case of a virtual team, relying upon digital communications to collaborate, a broad technology failure may disrupt communications, resulting in additional challenges in resolving such an incident.

2.5 SAFETY, SKILLS & TRAINING

The use of remote support by vendors delivers significant benefits, as they are able to provide highly specialised

skills and utilise them across multiple vessels. The skills and training that exists within a team clearly impacts the ability of that team to work effectively. In the case of maritime technology systems, the strategies of relocation of skills to shore and the outsourcing of capabilities to external companies that provide the service remotely need to be monitored to ensure that the necessary skills are maintained within the broader team in a sustainable manner that transcends staff turnovers within service provider companies [16]. It is also necessary to determine how accountabilities that would have traditionally resided with licensed officers can be allocated to shore based organisations [15]. The resultant de-skilling of team members also needs to be considered. Automation has the potential to impact the ability for team members to perform effective problem solving when the automation fails. This is particularly problematic during emergency situations where manual tasks that would normally be performed by automation must be re-configured and shared across team members [15].

3 DISCUSSION

The use of computing technology on ships has changed dramatically in recent years. There has been a transition from proprietary electronics to the use of general purpose computing infrastructure [10]. These systems have significantly different requirements for maintenance and governance. The following sections will discuss the desired changes to increase the maturity of technology governance.

3.1 CHANGE OF PHILOSOPHY FOR TECHNOLOGY ON SHIPS

Keeping technology systems operational includes ensuring that problems and incidents receive appropriate responses; user accounts and access permissions are managed; any changes to configuration or software upgrades are tested and authorised before being applied to the production systems; systems have sufficient capacity and are secured against cyber attack. Planning must also be performed to allow for continuity of operations in the event of a system failure that cannot immediately be resolved. This level of robust management of systems should be initiated at the start of a vessels life and be a constant until it is decommissioned. It may be necessary for the systems and processes to transition through a number of owners and management arrangements during that time so that the necessary technology governance can be maintained.

To reach the target state of maturity and robustness, it is necessary to change the current philosophy of design and operation. Equivalent rigour should be applied to the technology infrastructure, as is found in other aspects of vessel operations. Examples include: the requirement for a ’technology log book’ that records significant events that are applicable to the technology systems, as has been required for deck and engine room operations throughout the history of shipping; applying a permit to work scheme for technology changes, requiring vessels to undergo periodic technology surveys and inclusion of technology systems in the planned maintenance schedule.

3.2 FUTURE DESIGN CONSIDERATIONS

System design plays a key part of any robust technological system. When considering that the overall ship IT system must be operated and maintained by a virtual team, this requirement must be considered up front to ensure that appropriate collaboration and governance can occur throughout the full life-cycle of the systems from vessel concept to decommissioning [14]. The design of vessel systems must satisfy the needs for dependability and reliability and enable both onboard and remote operators to work safely, securely and collaborate effectively [15]. Also of critical importance is the requirement for fast recovery of a failed system to restore safety critical operations [11, p.9]. Any design (or modification) of a vessel’s technology during its service life needs to consider the full set of operational constraints of the technology services that are provided [13]. This may be documented as a set of ’use cases’ that detail the functional tasks that the system provides and shows which ’actors’ within the virtual team perform which tasks and any collaboration that is necessary between the actors should be specified. This philosophy may require modification to current practices of developing design specifications and commercial contracts [16].

3.3 THE FUTURE OF TECHNOLOGY GOVERNANCE AND REGULATION

As the policy maker for the maritime industry, the IMO has identified, through the release of their cyber risk management guidelines [9], that risk management for technology systems is fundamental to safe and secure shipping. By 2021 all vessels must include cyber risk management within their safety certificates. There is also an opportunity within the ISPS Code for future inclusion of digital systems and infrastructure within its safety management practices [1]. Lloyds Register has published a ShipRight procedure [14], endorsing a total system approach including consideration of the ship, communications links and off-ship facilities and services that could potentially compromise the safety or the capability of the vessel. This shows an increasing awareness and commitment from key industry organisation that needs to be broadened and translated into operational maturity and governance.

The remediation plans outlined within the ISM and ISPS Codes are required to be reviewed annually, following an incident or after any changes to infrastructure. This ensures that the plans take into consideration the rapidly changing technological solutions offered to the industry. It also enforces the adaptability of these assessments, as a company must prove post-incident that risks are being mitigated.

The approach to providing a more robust technology environment which has been adopted in shore based industries is to implement enterprise capabilities that support the primary mission oriented systems. This approach works well within large enterprises, as it provides consistency and economies of scale such that specialist staff can be employed to provide these services. Using the example of software asset management [15], a large enterprise may deploy a dedicated system that monitors all other infrastructure and periodically gathers data on installed software packages and versions. This is a powerful tool, as it allows for centralised analytics, reporting and identification of non-compliant, vulnerable software. While this approach works well in this type of organisation, enterprise solutions typically require their own specialist resources, infrastructure and connectivity to the supported systems. Enterprise solutions also typically provide services such as identity and access management, configuration management, asset management and centralised management of a Standard Operating Environment (SOE) for desktops and Servers [4]. Maritime based technology operates on a mobile platform with limited connectivity and these arrangements may be challenging to implement in this context.

IT Service Management has been identified by Cater-Steel, Toleman and Tan [5] as a method for providing additional rigour around IT services and reducing the level of ad-hoc operations. An IT Service Management framework such as the IT Infrastructure Library (ITIL) could be applied to the technology services that support operations on sea going vessels. At the tactical level, clear definitions of the various services being provided by technology and their criticality would provide a valuable starting point to stakeholders to understand the technology landscape and the roles that various team members perform in providing those services. An understanding of the current and projected capacities of the infrastructure and realistic plans for maintaining availability / service continuity would complement the service definitions, providing a governance view of the technology as a whole.

3.4 THE VIRTUAL TEAM

The challenge for the virtual team in maintaining sea going technology has many aspects. It includes collaborating with other team members across organisations and geographies, traversing diverse written and spoken languages to support technology infrastructure that is mobile, adding also the difficulties of uncertain connectivity, bandwidth and skills on-board and ashore. It is important to define how much technology work can be managed shore side and what will be done by seafarers, defining boundaries of responsibilities/ dynamics / communications between ship and shore. This is critical to ensure that trust is established between on ship and off ship team members to ensure that the needs of all the team members are being considered [16]. Moving to more robustly governed technology requires the establishment of system boundaries and clear roles / accountabilities (including for any systems hosted or managed ashore). These established boundaries will clearly define any remote connections from ship to shore. There is a need to evolve current management practices to include testing and authorisation of any changes to software or configuration, with roll-back capability in the event of failed changes [14].

4 CONCLUSIONS

Technology has inevitably found its way onto sea going vessels in increasing ways. However, the importance of technology to the operation of the vessel is not represented in the culture of shipping at present. Accountability and ownership for technology is not clearly defined on board. Other critical operations on-board such as navigation and propulsion have formal processes supporting them such as defined roles, accountabilities and the use of logbooks for recording events, the onboard technology is not operated with the same rigour. Similarly, the vessels maintenance program does not typically include details of technology hardware or software patches or software version updates that are required.

Current practices employed for management of technology on sea going vessels has been described as ad-hoc, largely due to the inherent constraints of the operating environment. In addition to this, there is often a lack of technology governance or formally defined IT Service management applied to shipboard technology. Observations of the current industry technology strategy suggest that the levels of automation and the use of ’virtual teams’ to support ship based technology will continue to grow. Ship based technology needs to be managed throughout the life-cycle of the vessel and therefore must be considered from the development of the concept, through signing of contracts, build and operation. As the industry moves toward remote operated systems and further reduction of crews, the governance of technology systems will become more critical, as there will be less opportunity for human intervention in the event of a failure of technology at sea.

While there are significant upsides in providing shore based skills to support seafarers (such as sharing extremely specialised skills across a broad range of vessels) there are risks that need to be managed, including de-skilling of seafarers, and lack of ship to shore connectivity during an emergency making shore based support unavailable. The use of virtual teams also presents an organisational and management challenge due to the fact that the members may operate in different geographies, time-zones and organisations. To be successful any well organised team must have a structure, reporting lines and the necessary collaboration tools to ensure that they can achieve their common purpose of supporting the on-board technology systems.

The principles of good governance require that any changes made to technology should be authorised by an allocated system owner, who is accountable for the system and its reliable operation.

The lifecycle of technology is much shorter than that of mechanically engineered systems such as a ship. While ships' main and auxiliary systems may be expected to last (with necessary maintenance) for the life of the vessel, technology system lifecycles are much shorter that other equipment on board. Technology requires not only regular maintenance but will also become redundant within a shorter timeframe, requiring technology refit to maintain reliable service. System design is critical when delivering technology systems that must be relied upon. Design does not simply refer to the technology. When considering the entirety of a ship based technology system and the virtual team supporting it the system boundary includes the team members that operate the system and all the enabling processes that occur to support the technology.

Taking the opportunity to adopt a formal ITSM framework such as ITIL to provide governance over the critical technology service on vessels would lift the maturity of the technology services, providing accountability and a reduction in unplanned technology failures.

5 ACKNOWLEDGEMENTS

Rory Hopcraft receives funding from the EPSRC.

6 REFERENCES

[1] A G Bermejo. Maritime Cybersecurity Using ISPS and ISM Codes, 2015.

[2] AMMITEC. Maritime Software Quality Guidelines. 2017.

[3] BIMCO. The guidelines on cybersecurity onboard ships. 2016.

[4] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry. Challenges for securing cyber physical systems. In *Workshop on future directions in cyber-physical systems security*, volume 5, 2009.

[5] A. Cater-Steel, M. Toleman, and W.-G. Tan. Transforming it service management-the ITIL impact. *ACIS 2006 Proceedings*, page 81, 2006.

[6] DNV-GL. Recommended practice dnvgl-rp-0496: Cyber security resilience management for ships and mobile offshore units in operation, 2016.

[7] H.B. Esmailia, H. Gardesh, S.S. Sikari. Validating ITIL Maturity to Strategic Business-IT Alignment. *In Proceedings of the2nd International Conference on Computer Technology and Development*, pages 556-561. IEEE, 2010.

[8] IMO. Report of the Maritime Safety Committee on its Eightieth Session MSC 80/24, 2005.

[9] IMO. Guidelines on Maritime Cyber Risk Management MSC-FAL.1/Circ.3, 2017.

[10] C. W. Johnson. Why we cannot (yet) ensure the cybersecurity of safety-critical systems. 2016.

[11] K. D. Jones, K. Tam, and M. Papadaki. Threats and impacts in maritime cyber security. 2016.

[12] S. K. Katsikas. Cyber security of the autonomous ship. In *Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security*, pages 55–56. ACM, 2017.

[13] A. Kott and I. Linkov. Cyber resilience of systems and networks, 2018.

[14] Lloyds Register. Cyber-enabled ships: Deploying information and communications technology in shipping, Lloyds Register's approach to assurance. 2016.

[15] H. A. Oltedal and M. Lützhöft. *Managing Maritime Safety*. Routledge, 2018.

[16] B. Twomey. The cyber-enabled ship what are the risks and what are the mitigations? *Encyclopedia of Maritime and Offshore Engineering*, pages 1–17, 2017.

7 AUTHORS BIOGRAPHY

Gerd Berner is a PhD Researcher from University of Tasmania (AMC). His research is focused on cyber security resilience of maritime technology.

Rory Hopcraft is a PhD Researcher from Royal Holloway University of London. His research is focused on regulatory aspects of maritime cyber security.

Joel Scanlan is a lecturer in ICT at the University of Tasmania. His research background and primary teaching area are in Cyber Security.

Margareta Lutzhoft is a Professor in the MarSafe group at the Western Norway University of Applied Sciences. Her research interests include human-centered design and the effects of new technology.

Jonathan Earthy is a Principal Human Factors Specialist for Lloyd's Register Marine and Offshore. He coordinates standards, research and assessment activities and products. His specialist area is assurance of the quality of Human Factors work, in particular for complex IT systems.