inmarsat
The mobile satellite company

Inmarsat Research Programme

GUIDE

BEST PRACTICE INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) RECOMMENDATIONS

Presented by:
Richard B H Lim, Sector Development, Inmarsat Maritime

Best practice ICT recommendations

Contents

—
AUTHOR
Richard B H Lim,
Sector Development,
Inmarsat Maritime
—
CONTACT
Inmarsat Solutions
Singapore

richard.lim@inmarsat.com

INTRODUCTION

Ship managers are increasingly looking after vessels featuring sophisticated ICT and automated systems, which officers and crew rely on to complete their work. Gone are the days when a Master can expect a dedicated Radio Officer to send communications, or tell a Junior Officer to draft and send emails.

Crew onboard modern ships work in an environment that is similar to shore-based offices. Computers, laptops, scanners and printers are now the everyday working tools on a modern and well operated ship, and their usefulness continues to grow in an era of increased administration at sea to comply with greater regulation and stricter compliance requirements.

THE CHALLENGE

To meet economic demands and bring efficiency to a modern and well operated ship, Managers are installing computer networks of increasing scale, sophistication and complexity. These networks provide the foundation for the vessel's primary corporate email system, planned maintenance system, document management systems and crew management systems. More advanced ships will likely have one or more management functions based on the Internet of Things (IoT) which routinely send telemetry back to shore.

There are many shipboard ICT systems that have been designed, implemented and deployed by professional and cyber-savvy Ship Managers. However, there are still ships that lack infrastructure and management of onboard ICT systems.

THE RECOMMENDATION

The objective of this document is to provide the Ship Owner, Ship Manager/ Operator and the Fleet ICT Manager with a comprehensive set of best practices for the design, deployment and ongoing operational management of the ICT system on their ocean-going mobile office; their ship.

THE CUSTOMERS: THE SHIP'S CREW AND THE SHIP MANAGER

It is important to understand that users (customers) will be working out at sea and physically separated by hundreds or even thousands of miles from the usual ICT support that a shore-based customer can expect.

Key considerations:

- With the ship usually at sea, physical access to the ship's system will be difficult, while digital access will depend on connectivity.
- The ship's crews and other personnel are generally transient. They rotate and are replaced by another team every 4 to 6 months.
- Ships do NOT have dedicated ICT support staff.

WORKING WITH SHIP MANAGERS OR OWNER OPERATORS

Ship Managers are responsible for safety and managing costs of very expensive sea going vessels on behalf of ship owners.

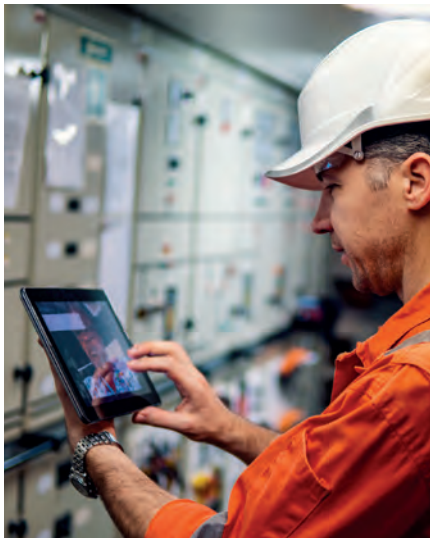
They make it their business to operate at a profit, bearing in mind requirements to achieve the safe carriage of cargo and sail the ship safely to avoid accidents,

collisions and pollution.

It is the Fleet IT Manager's responsibility to address these key concerns, while providing a suitable, reliable and effective ICT system remotely.

IT PROBLEM MANAGEMENT AT SEA

Solving IT problems is a collaborative effort. The Fleet IT Manager must have the authority to request the ship's staff execute recovery procedures on their behalf. Procedures should be kept as simple as possible. Ideally, guidance should be presented in a line-by-line format that is easy for non-experts to follow and execute. The vessel's Superintendent(s) should be kept informed to ensure compliance by the ship's staff.



CONCEPTS FOR MARINE ICT SYSTEMS

The Fleet IT Manager is responsible for designing, deploying and managing onboard ICT hardware environment that is:

- Rugged – so that it can last for 3-5 years without regular hands-on support from ICT staff.
- Easy to operate – so that it can be used and to some extent maintained by officers and other crew who do not have an IT background or intuitive understanding of computer or network operations.
- Standardized – so that crew rotating between different ships within a fleet know what to expect in terms of availability and service and can apply experience gleaned from working on other ships; maintenance and procedures can be streamlined.

PRIORITIZING SYSTEM UPTIME

An additional feature of ship IT is that all workstations should NOT be treated equally. Some machines will be more important than others.

For example, a Deck Officer's secondary working computer is NOT as important as the ship's primary radio computer or the computer used for updating nautical charts.

Priority should be accorded to systems fulfilling business and safety-critical tasks. When planning for resiliency, efforts should focus on these crucial systems.

Flexibility should be incorporated to the point where a functional but less important computer (such as that Deck Officer's extra machine) can be repurposed as a temporary stand-in for running ECDIS until a replacement machine can be obtained at the next port call.

DESIGNING A RESILIENT ONBOARD NETWORK

When designing a vessel's network, the Fleet IT Manager should deploy standard hardware so it can be used for different roles in order to improve overall availability and resilience.

- It is advisable to carry a couple of spare computers or laptops to mitigate risk.
- Alternatively, the Fleet IT Manager is advised to a set specification for all computers across the ships; in an event, this will make it easier to swap machines from low-priority applications to fulfil a critical task.

EXAMPLE 1:
Consider a ship with 9 operational computers, 3 computers dedicated to navigation and 6 running IoT systems, such as engine control and cargo handling. In the event of a failure on a critical radio communication PC, crew can be instructed to take a less important workstation (say, from the mess room) and swap out the hard-disk to restore the radio communications computer until a longer-term solution can be found.

Likewise, it is advisable to have at least

two, preferably more, network switches at the patch panel. This increases the availability of critical systems by preventing a simple power failure knocking out a single switch that might cause the ship's whole network to crash.

EXAMPLE 2:
Multiple methods should be in place to access email/other key applications. If the ship's Master uses a locally installed app version of Outlook as the primary email client for operational communications, there should be an option to switch to a web-based version in case the computer breaks down. It is possible to extend this redundancy strategy by putting in place multiple IP connections (over separate communications links) to ensure that ship's business emails still reach the charterer or cargo owners in the case of primary link failure.

This capability is built into Inmarsat's **Fleet Xpress** service, which benefits from two antennas. One operates on the Ka-band frequency, while the other uses L-band. If the link from one antenna is interrupted, the system automatically switches to the other to maintain connectivity.

ONBOARD SPARES

A shore-based IT Manager has easy access to spares to ensure efficient working of machines. If the anager doesn't have a particular spare it can be ordered for next-day (or even same-day) delivery.

On the other hand, a Fleet IT Manager does not enjoy the same luxury in supporting users, as physical access to the ship is restricted to short port calls. Even when the ship is in port, locally sourced spares may not match the specification used onboard: hardware may use a different power supply, software might default to a different language. Therefore, the most practical solution is to anticipate and provide sufficient spare parts onboard to allow a vessel's ICT system to be maintained for 3-5 years. Essential items on the spares list are replacement hard disks and boxed PCs.

POWER SUPPLY

Fleet IT Managers should ideally set-up the onboard server and critical communication equipment to tap into the ship's emergency power supply. This will ensure the ICT system keeps working in the event of a power failure, thereby providing an extra degree of redundancy.

Older ships often suffer from a lack of power outlets in the accommodation blocks. As a general rule, the Fleet ICT Manager should provide an additional power expansion strip for each PC deployed, to ensure that the ship's ICT system can be installed seamlessly.

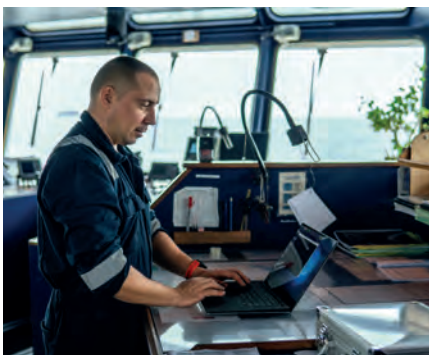
BACKUPS AND IMAGES

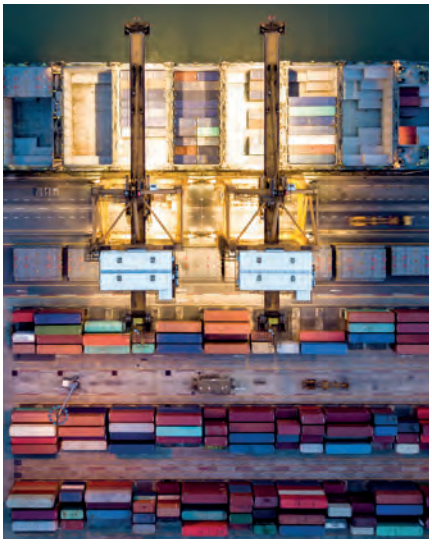
A successful onboard ICT backup strategy depends on a simple and automated process with minimal involvement of ship staff. Tape-based backups or similar solutions requiring frequent crew intervention should be avoided. Try to use interconnected Storage Access Network (SAN) or disk-based technologies, which benefit from duplication, convenience and faster recovery.

REMOTE ACCESS

Remote access is at the heart of effective Fleet ICT support. It is necessary to have the ability to connect remotely to a vessel's communications system, server, backup system and domain and user controls. Ideally the Fleet ICT Manager requires secured remote access to all machines on a ship.

For cyber-security audit purposes, all remote-controlled sessions accessing the ship's hardware should be logged, as





should sessions initiated by application or support vendors, whose application for access must be approved in advance.

STANDARDIZATION

Hardware, software and network configuration is essential when managing multiple ships and large numbers of crew. It helps to have a fixed location where workstations can be prepared before they are deployed to a vessel. Having common set-ups that can be replicated on machines destined for the bridge, the engine room, and other areas saves time and effort in IT management duties and means ship staff can expect the same IT environment when they transfer between ships.

REGULAR ICT EQUIPMENT UPGRADES

Traditionally, onboard computers were replaced only when a Master reported a 'slow' workstation. This ad-hoc approach resulted in unsystematic and unplanned replacement of hardware. This short-sightedapproach complicated the implementation of strategic workaround recovery solutions, resulting in higher support costs and more downtime.

SEGMENTATION

The Fleet Manager should design a ship's network in segments to prevent problems or security risks on one part of the network impacting the whole network. For example, the operational LAN comprising a ship's working computers must be separated from the crew LAN for wireless access points and recreational computers, and also from the IoT LAN, which comprises ECDIS, navigational and other IoT systems. This will ensure uninterrupted working of the ship's IoT system.

INTERNET PROTOCOL (IP) ADDRESS MAPPING

The Fleet IT Manager should try to assign IP addresses to workstations in a logical manner. Although this requires some effort, it is rewarded with greater segmentation and more flexibility for managing cyber-security.

Granular identification and segmentation gives the Fleet IT Manager a better view of their assets on a ship and across the whole fleet. Separating IP range on a ship also segments off LANs from virtual LANS and is more future proof in terms of bringing all ships on to a holistic fleet-wide network for the roll-out of advanced applications.

Example of IP address on page 14

Assigning IP addresses improves cyber-security by preventing crew from misusing Dynamic Host Configuration Protocol (DHCP) and simply connecting their own workstations to the vessel's operational or IoT LANs.

SOFTWARE ENVIRONMENT

Simple peer-to-peer based workgroups are easy to set up but create more work later on, for example when remote control is needed to change and manage the system. A full client/server-based domain architecture may require more effort up front but provides a degree of future proofing against many issues and comes with a suite of tools that help Fleet IT Managers administer a network and enforce cyber-security policies at a fleet-wide level.

ADUC CONTROLS

Active Directory Users and Computers (ADUC) framework makes it straightforward to set-up and manage user access rights at individual, group or global levels. It benefits from scalability and provides a comprehensive package of tools and services for performing common tasks.

Examples:

- ADUC can log and record when a USB is connected to a domain computer. This journal is especially critical to third-parties auditing and enforcing a fleet's cyber security policy.
- ADUC's Group Policy Editor can be configured to deny AutoPlay of mass storage devices, thereby preventing threats from self-running DVDs and USBs.

FLEET ICT MANAGEMENT AND PLANNING

ICT Budgeting: The Fleet IT Manager should budget and plan an upgrade schedule for the replacement of ICT equipment on each ship. This involves working in partnership with Ship Managers to approve a budget

and prepare a timetable for carrying out upgrade work every 3-5 years, in alignment with corporate level ICT equipment replacement policies and the ship's dry dock schedule. The budget process should also capture airtime and software costs that a ship may incur.

The best time to perform a system upgrade is during dry dock when the vessel is off hire. This provides sufficient time to install or replace any hardware and run tests to confirm it is fully functional and integrated before the vessel is handed back to its Master.

EDUCATION

The Fleet ICT Manager should work in partnership with the crewing department to arrange training for all sea staff on general IT topics, specific applications as well as best practice for ICT usage at sea.

All officers should be given training on cyber security and it is part of the Fleet Manager's role to guide their development and ensure training is coherent and relevant.

FLEET ICT UPDATES:

Fleet Managers must keep ship staff across the fleet regularly updated on changes and alerts related to ICT systems, via email broadcast or ISM Circulars. These should include:

1. Cyber security events
2. Application alerts
3. Scheduled service unavailability
4. Changes in procedures

RECORD OF FLEET IT POLICY

It is the responsibility of the Fleet IT Manager to formulate and document a Fleet IT policy which should at a minimum, review and include:

- Objective and scope
- Roles and responsibilities (Fleet IT, Master and Chief Engineers, Superintendent and other ship staff)
- Handover ICT-related responsibilities by the incumbent Master
- Password and access rights controls
- Authorized hardware and software usage
- Illegal download of data with intellectual property rights
- Services and operational measures of Fleet ICT department
- Ship LAN system setup and schematics showing all segments
- Cyber-security guidance
- LAN system backup and recovery procedures
- System failure support and recovery process, reporting procedures, and service level agreements
- Shipboard cyber response action plan
- Enforcement and disciplinary actions
- Appendices
  - Table itemizing equipment in all LAN Segments, produced for each individual ship
  - Approved software list (and latest version)
  - LAN system diagram with segments (for each individual ship)
  - List of approved ADUC LAN users
  - List of user access rights
  - Latest Fleet ICT support communications and standing instructions
  - Latest backup system architecture

The table below shows the comparison between domains and workgroups

	Workgroup	Domain	What this means to mariners
Network type	Peer-to-peer Windows computer network.	Client/server network.	Better command and control over remote PCs. The Peer to Peer model is not ideal and better suited to a professional operational environment.
Log in	Users have separate log-in and password at each workstation.	User can log in at any workstation via their account and access domain resources.	Officers can log-in on any PC in the domain with a universal username and password, rather than having separate credentials for each machine. Passwords can be made to comply with standards set out in maritime cyber-security audit rules.
Workstations	Maximum of 10 machines allowed on a network.	Maximum of 2000 machines allowed on a network.	This provides scalability to accommodate more machines on the network as ships are installed with more automation and IoT–based solutions in the future.
Administrator	Individual users manage the resources and security on their PC locally.	One administrator can manage the domain, its users and resources.	A domain architecture allows greater control of a ship's setup and makes it easier to comply with maritime cyber-security rules.
Computer configuration	Individual users control the settings on their own PC. No central settings.	Users can make only limited changes to a PC's settings because network administrators often want to ensure network-wide consistency.	A domain architecture allows fleet-wide configuration and remote setting of user privileges and associated permissions and restrictions.
Changes	Each computer must be changed manually or carried out daisy-chain.	Changes made to one machine are automatically rolled out to all machines.	This facilitates the fleet-wide installation of security updates in a controlled fashion.

This Policy must be reviewed yearly by the Fleet ICT Manager in partnership with the Fleet HSSE ISM Team.

SATELLITE CONNECTION

At present, satellites offer the most reliable and assured means of maintaining high-capacity ship/shore communications for ocean going ships.

Reliable ship/shore connectivity, extent and consistency of global coverage, speed and capacity should be considered when selecting the provider for a fleet.

As electronic communication is vital to modern safe vessel operation, it is also important to consider installing a back-up communications channel.

REMOTE ACCESS

Remote access to onboard systems is probably the single most important tool for managing ICT assets on a fleet operating globally.

For cyber-security reasons, extra care should be taken when granting remote access rights to external application vendors.

Tools such as TeamViewer or Bomgar are commonly used by vessel operators. When choosing a remote solution, preference should be given to those that allow session logging.

When performing tasks via remote access, a VPN should be used to ensure that the communication channel is secure.

ONBOARD COMPUTER ROOMS

Ships are mobile platforms, that often sail through rough seas. It is critical that ICT assets are designed and installed to tolerate harsh environments and not easily damaged in harsh weather.

Care should be taken to avoid packing too many high-performance server units in a traditional computer rack. Overly dense stacking of equipment can result in a 'heat island' which is detrimental to the equipment.

To avoid over-heating ensure there is adequate ventilation space between each unit. Alternatively, use tower-type units housed and appropriately secured in a tiered desk. Wherever possible, choose equipment with low heat emissions.

CYBER SECURITY

A successful malicious cyber-attack on a fleet's ICT will not only disrupt vessel information and IoT systems, but risks serious safety, environment and reputation damage.

The Fleet ICT Manager must take measures to negate – or minimize – the risk of threats impacting vessel and fleet operations.

The 'attack surface' on a ship includes:

- Vessel's ICT system – both business and crew LAN
- Vessel's IoT LAN system – including navigational chart systems and engine control systems
- Vessel's communication link to shore

CYBER EDUCATION FOR SHIP STAFF

- The Fleet IT Manager together with the Head of Crewing must work to ensure that the crew is educated and understands the importance of cyber security.
- Training, whether classroom-based or online, must be provided to educate the crew on risks such as:
  - Spear phishing
  - Malicious links in unsolicited emails
  - Social engineering
- A record of the crew's performance in these training exercises should be kept on file by the HR/Crewing department. Updates on new and emerging cyber threats should be regularly disseminated to all ships in the Fleet.
- Your seafarers can take the Fleet Secure Cyber Awareness training course and gain up-to-date cyber security knowledge. Inmarsat referral discount is available.

Strengthening onboard ICT hardware, software and user control processes:

- The Fleet ICT team should make security a priority when designing and implementing a fleet-wide network architecture. This may entail upgrading existing ICT hardware on

ships to ensure proper separation of networks. IoT system(s) are never connected to the business and separate crew welfare networks are vital for preventing malicious code crossing over and spreading between networks. Learn how Inmarsat can help separate your operational use from crew internet use with Crew Xpress.

- Fleet Email systems should have malware detection and controls installed.
- Access to ship systems should be controlled by rank based accounts managed by ADUC and crew should be allocated individual official email accounts.
- Any Wi-Fi provided for crew should be protected and require a login to access.
- The crew LAN should be separated from the ship's LAN and any IoT systems to prevent infections introduced by crew's own devices impacting ship operations.
- Crew should not be permitted USB access.
- Ship staff must guard against unauthorized access to PCs and other systems on ship. In particular, when calling at distant or seldom visited ports, they must be alert to individuals masquerading as IT technicians seeking access to the ship's network.
- Ship staff must comply with the approved application list and ensure compliance to application control process.

REDUNDANCY TO CRITICAL ICT SYSTEMS

The Fleet IT Manager needs to plan for all eventualities on the ship and implement adequate redundancies considering the criticality of systems to safe vessel operation.

Measures intended to ensure redundancy should cover hardware, software environment, and supporting communications/network infrastructure (including satellite link).

CYBER INCIDENT RESPONSE PLAN

- A Cyber Incident Response Plan must be prepared for each vessel and documented as part of its ISM policy.
- The Plan should, at minimum, include:
  - A process for initial incident triage.
  - Steps to quarantine all electronic traffic to and from ship. Procedures for alerting and requesting communication vendors to check traffic.
  - Procedures to keep corporate IT security department abreast of the situation.
  - Procedures to secure and establish a backup communications channel to affected vessel(s).
  - Steps to stabilize and isolate an infected system to guard against further spread.
  - Steps to gather intelligence and evidence from affected systems.
  - Procedures to execute recovery of critical systems remotely.
  - Arrangements to completely replace the ICT system at the next safe port after the cyber event.

CYBER DRILLS

Cyber drills must be conducted across the Fleet at least once a year to test response procedures and assess crew preparedness.

- As the plan is part of the Vessel's International Safety Management (ISM) it is important to periodically carry out drills to test and iron-out issues, train the crew, HSSE team and other stakeholders on response procedures during a cyber incident onboard.
- It is essential that the Ship Manager's Incident Commander takes charge and demonstrates effective leadership in these exercises to ensure the security of the ship, its crew and cargo, while allowing the Fleet IT team to concentrate on securing the ICT infrastructure and resolving the cyber issues.

ANTI-PHISHING CAMPAIGNS

Regular anti-phishing campaigns must be conducted to maintain high-levels of crew vigilance and test onboard systems and processes:

- Periodic anti-phishing campaigns should be implemented whereby simulated malicious emails are sent to all crew across the fleet to test their responses.
- Regular penetration testing by professional 'white-hat' hackers should be carried out to test for and

identify technical weaknesses.

- The objective of these exercises is to promote a culture of continuous improvement and preparedness.

PLANS FOR CRITICAL SYSTEMS

Workaround plans for critical systems and processes should be incorporated into the network and system design and described for Captains in a vessel's emergency manuals. These plans should include:

- Instructions and/or checklist in the event of critical system failure, due to cyber incident or unplanned system breakdown.
- Response during a system failure without a need to request and wait for help from shore office.
- Workaround plans might include:
  - Actions to restore email clients that have crashed or failed to work.
  - Actions to take when the main ship/shore communication link is degraded or has failed.
  - Usage of Citadel telephone to send telex.
  - Testing of backup email service from ship-to-shore and from shore-to-ship.
  - Actions to work around or recover failed critical PCs.

VIRTUAL SHIP INFRASTRUCTURE

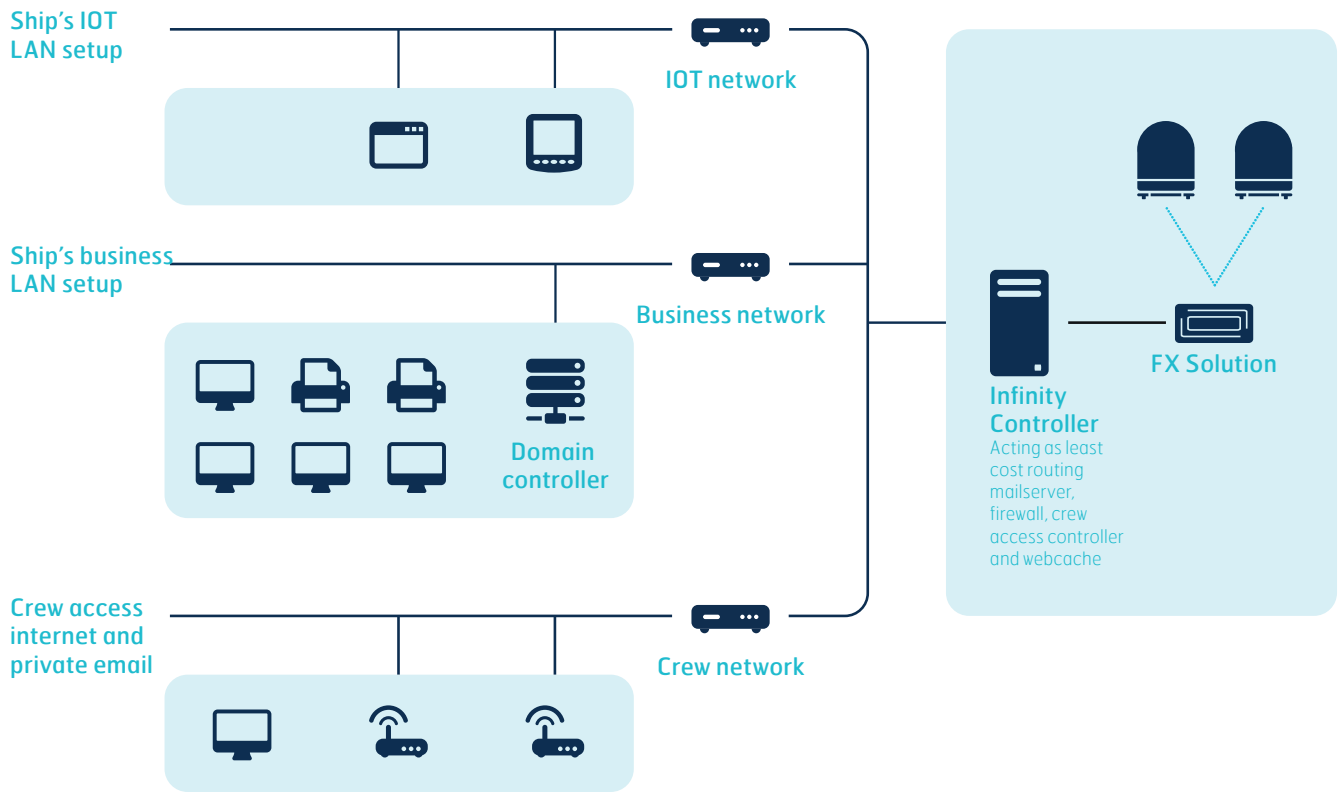
Fleet IT Managers must consider deploying virtual infrastructure on ship for servers and workstations, instead of the traditional set-up of individual workstations and servers.

The immediate benefits of a virtual infrastructure on a remote ship are:

- Fast Recovery Time: In the event of a system failure or disaster a virtual infrastructure allows faster recovery of IT resources for improved business continuity and revenue.
- Better Scalability: Virtual environments are designed to be scalable which allows for more flexibility when it comes to company growth. Instead of purchasing additional infrastructure components, new applications and upgrades can easily be implemented.
- Cost and Space Savings: Saving on the costs of IT infrastructure is a reality. Cost savings also extend to reduced energy consumption and fewer IT personnel, while reducing the amount of space that is required to house an IT environment.
- Better Return on Investment: In addition to reducing the costs of maintaining an older infrastructure, companies can increase their ROI by ensuring business continuity following a disaster and preventing revenue loss.

Example of Vessel IP Plan		
172.21.XX.1	Where XX is different for each ship	
Suggested Ship's LANs IP addressing		
172.21.XXX.YYY	172.21.XXX.YYY	Range is for Ship's IoTs
172.22.XXX.YYY	172.22.XXX.YYY	Range is for Business LAN
172.23.XXX.YYY	172.23.XXX.YYY	Range is for Crew LAN
172.24.XXX.YYY	172.24.XXX.YYY	Range is for any future LANs
17.168.XX.2	17.168.XX.9	Range is for B LAN IoTs
17.168.XX.10	17.168.XX.39	Range is for B LAN Servers
17.168.XX.40	17.168.XX.69	Range is for B LAN Workstations
17.168.XX.70	17.168.XX.79	Range is for B LAN Peripherals
17.168.XX.3	CCTV Controller	
17.168.XX.7	Ship's Business LAN Access Point	
17.168.XX.10	Server A	
17.168.XX.11	Server B	
17.168.XX.12	Seagull Training PC Server	
17.168.XX.13	Dualog PC Server	
17.168.XX.15	SAN Device A (Backup Storage)	
17.168.XX.41	Bridge PC A	
17.168.XX.42	Bridge PC B	
17.168.XX.43	Master Cabin PC	
17.168.XX.81	Chief Engineer Cabin PC	
17.168.XX.62	Chief Officer Cabin PC	
17.168.XX.63	2nd Engineer Cabin PC	
17.168.XX.65	Office PC 1	
17.168.XX.67	Office PC 2	
17.168.XX.69	ERC PC 1	
17.168.XX.71	ERC PC 2	
17.168.XX.63	Training	
17.168.XX.71	LAN Printer	
17.168.XX.72	LAN Printer	
17.168.XX.73	LAN Printer	
IoT LAN example		
18.168.XX.049	18.168.XX.149	Navigation IoTs (EDCIS, SVDR, ChartCo, DP Controllers)
18.168.XX.101	18.168.XX.149	Cargo Control Systems (Loadicators, Ballast, Stability Controllers)
18.168.XX.150	18.168.XX.199	Engine Control Systems (Main Engine, Auxiliary Control System
18.168.XX.200	18.168.XX.249	Other IoTs (Environmental)
CREW LAN (Example) (for a 24 man crew merchant Vessel)		
10.0.0.1	10.0.0.29	Crew Wireless LAN Access Points with limited range of IPs
10.0.0.50	10.0.0.52	Crew Recreational PCs

Example of segmentation of virtual LANs on a ship



inmarsat.com