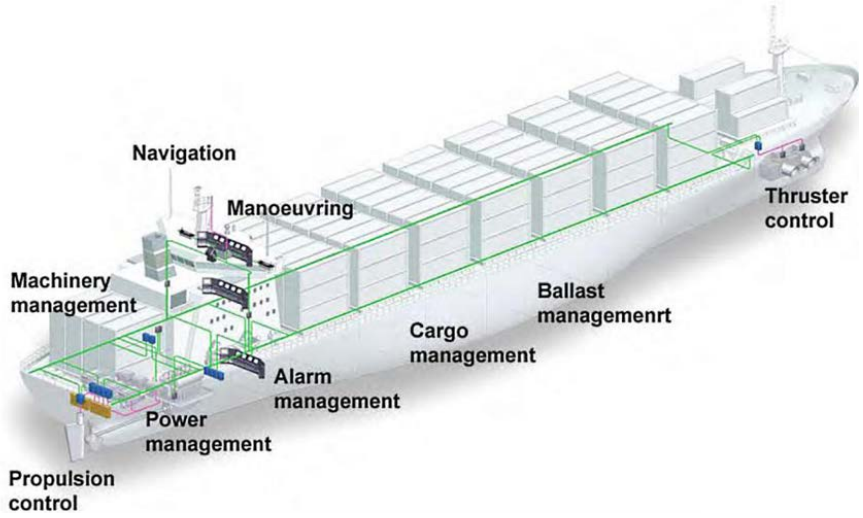
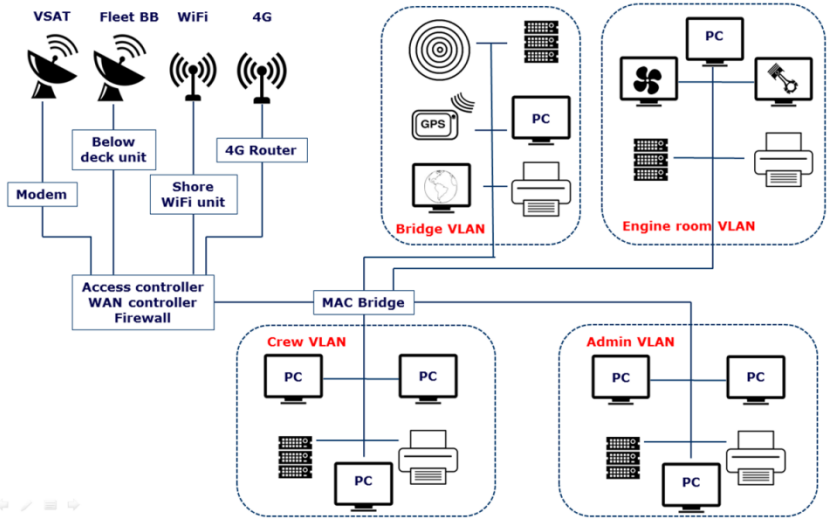
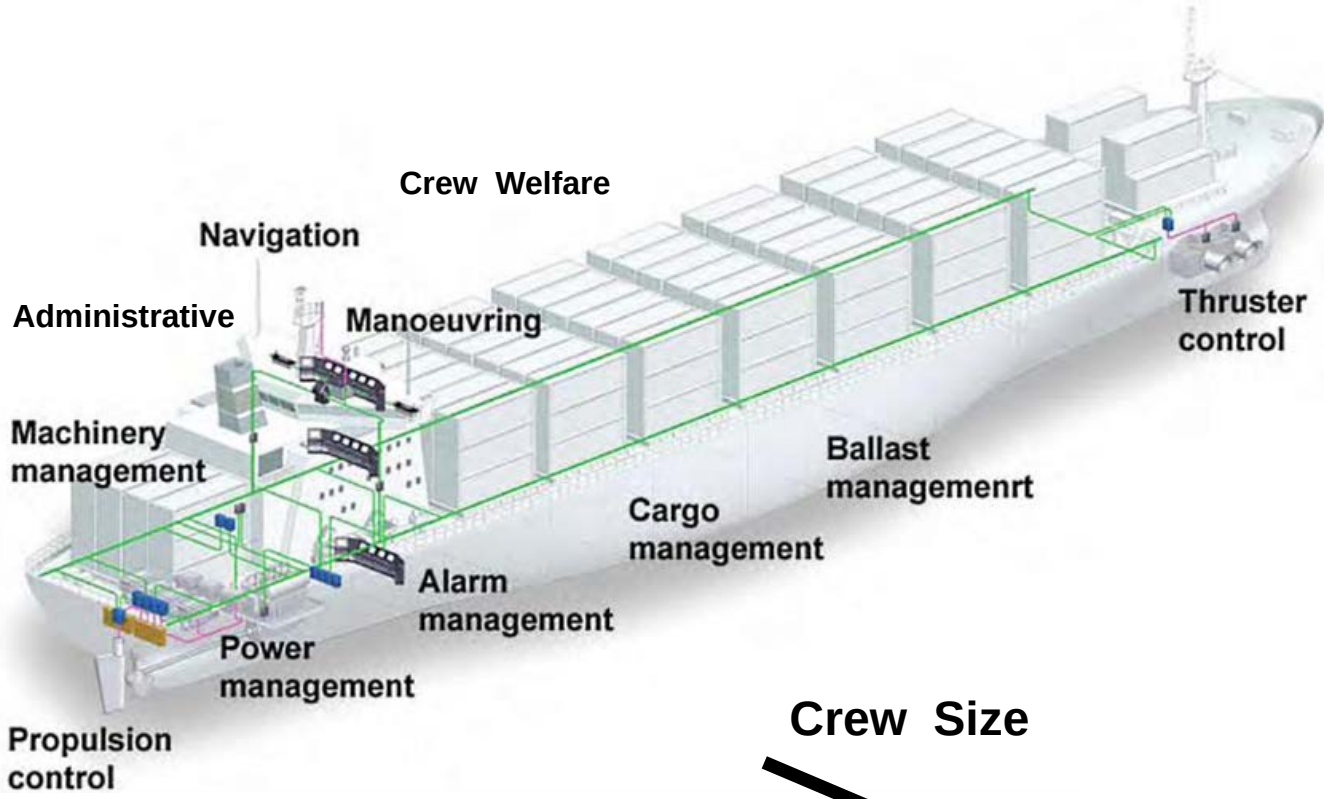




Practice of
Cyber Security Management System on Cargo Ship

October 2018

Trends



Crew Size

Management,
Decision-Assisting,
Monitor, Alarm,
Control,
Decision-Making

Automation

Interconnectivity

Ship-Shore,
Ship-Ship,
Inner

Cyber security is the premise

Administration & Industry Response

- IMO: Guidelines On Maritime Cyber Risk Management（MSC-FAL.1-Circ.3 ）

  Encourage Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021

Recommedation

⇩

KPI

- OCIMF: TMSA3, VIQ7
- RightShip: checklists

- Tanker
- Bulk Carrier

⇩

they need to be satisfied by company & ship
or ships will lose shipping qualification

de facto standard

OCIMF Requirements

- TMSA·Ch.13 Maritime Security for company including cyber security
  - ✓ establish and maintain policies and procedures
  - ✓ identify the risk – risk assessment
  - ✓ respond and mitigate the identified risk
- VIQ·Ch.7 Cyber Security for ships
  - ✓ policy & procedure: risk assessment, cyber response plan onboard
  - ✓ physical access control : USB/RJ45 ports
  - ✓ guidance on use of personal devices onboard
  - ✓ active promotion: training, instruction on safeguarding

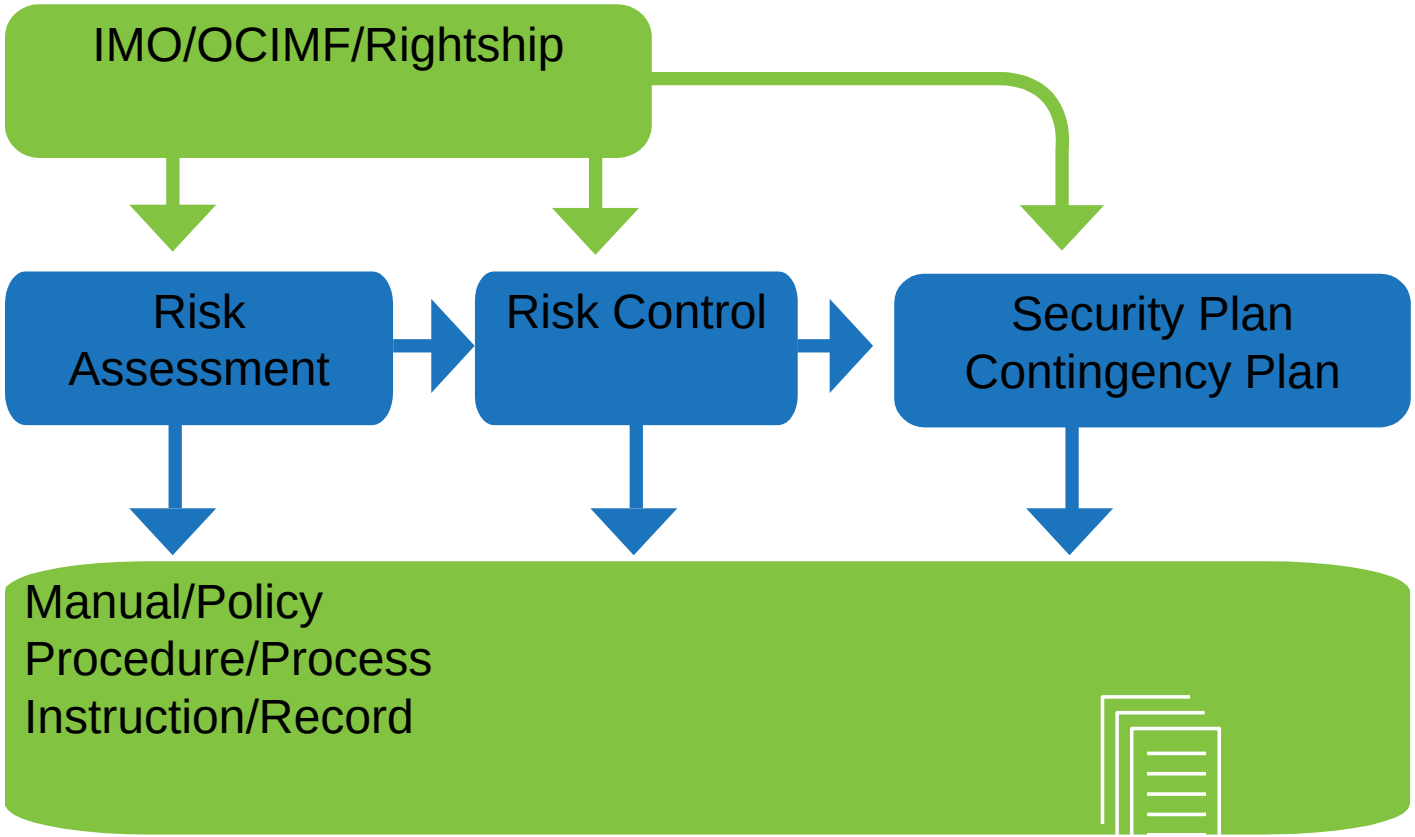
Tanker

RightShip Requirements

- ✓ documented software/firmware and hardware maintenance procedures
  - service report, available
- ✓ cyber security procedures
  - risk assessment, completed
  - response plan, available
- ✓ cyber security training

Bulk Carrier

Summary of Requirements



This is a systematic project !!!

Management, Technology, Personnel

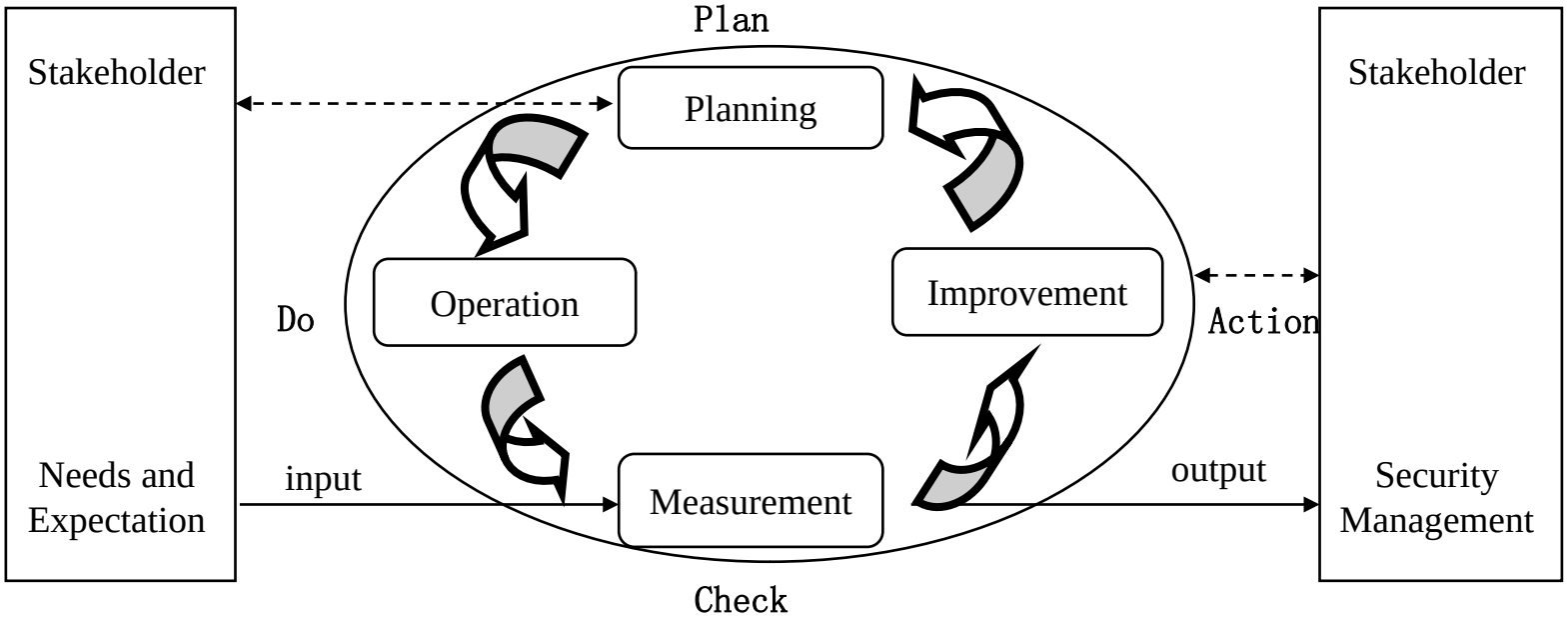
Puzzle/Difficulty of Shipping Company

- Existing safety management system is mature based on ISM rules
- But cyber security management is basically blank
- Necessary to incorporate cyber security into the existing management system
- It is a *new* issue and challenge
- Don't know how to do, too professional
- Need professional to provide guidance and supporting service

Our Practice

Cooperate with several shipping companies

- Plan and design a cybersecurity management system
- Integrate it into the existing management system



sustainable improvable management system

Development Process

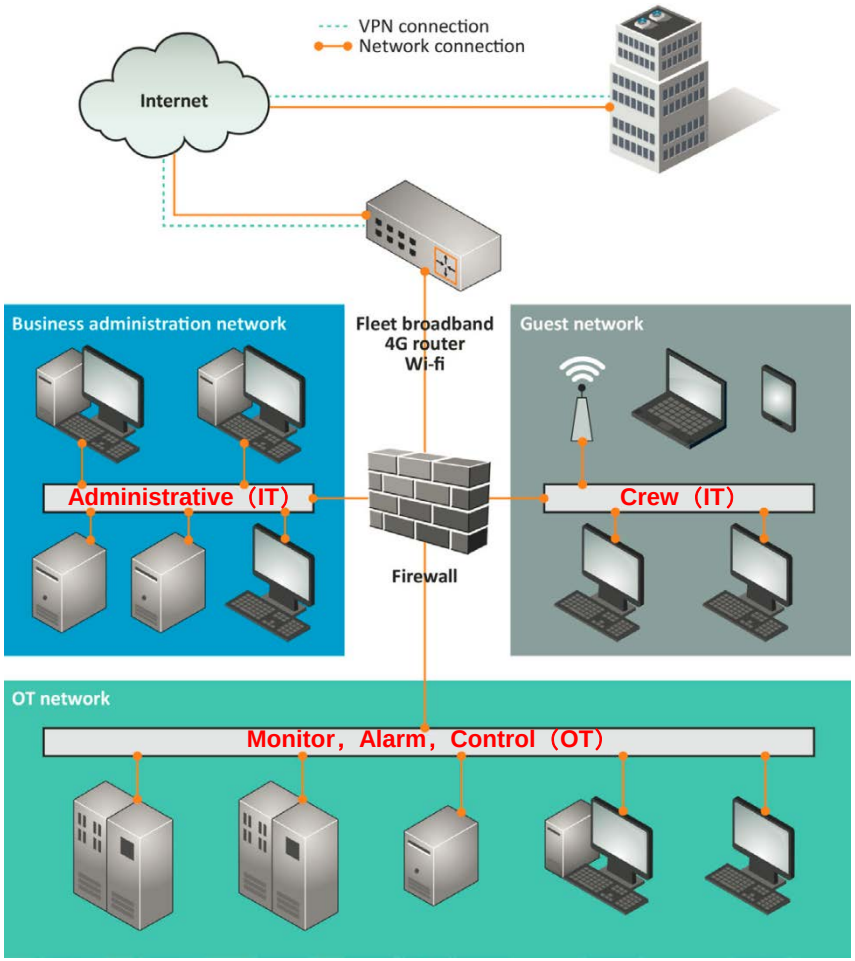
Result: Management Files

NO.	File		Description
1	Shipboard cybersecurity management manual	New	Policy, Organization, Responsibilities
2	Procedure for Shipboard cyber risk management	New	Personnel, Asset, Risk Assessment, Contingency, Measurement
3	Procedure for control of documentations	Rev.	Add content of cyber security
4	Procedure for control of records	Rev.	Add content of cyber security
5	Procedure for Information Communication	Rev.	Add content of cyber security
6	Procedure for corrective action and preventive action	Rev.	Add content of cyber security
7	Procedure for carrying out internal audits	Rev.	Add content of cyber security
8	Procedure for management review	Rev.	Add content of cyber security
9	Procedure for Change Management	Rev.	Add content of cyber security
10	Procedure for procurement, outsourcing and suppliers management	Rev.	Implement the third party access strategy
11	Instruction for shipboard cyber risk assessment	New	Assignment of asset, threat, vulnerability and risk
12	Instruction for maintenance and use of shipboard cyber asset	New	Network device, IT Computer, OT Computer, Personal device, USB port, etc.
13	Instruction for ship cyber response drill	New	Drill of shipboard only, or joint of ship-shore
14	Ship cyber response plan	New	Shipboard (each), shore-base, respective
15	Ship cybersecurity risk assessment report	New	Assessment Report (each ship)

- 1st level: Programmatic documents / manuals
- 2nd level: Procedure / Provision
- 3rd level: Instruction/Specification
- 4th level: Records, Report/Plan

4 level Management System Files

Finding 1: Network status onboard

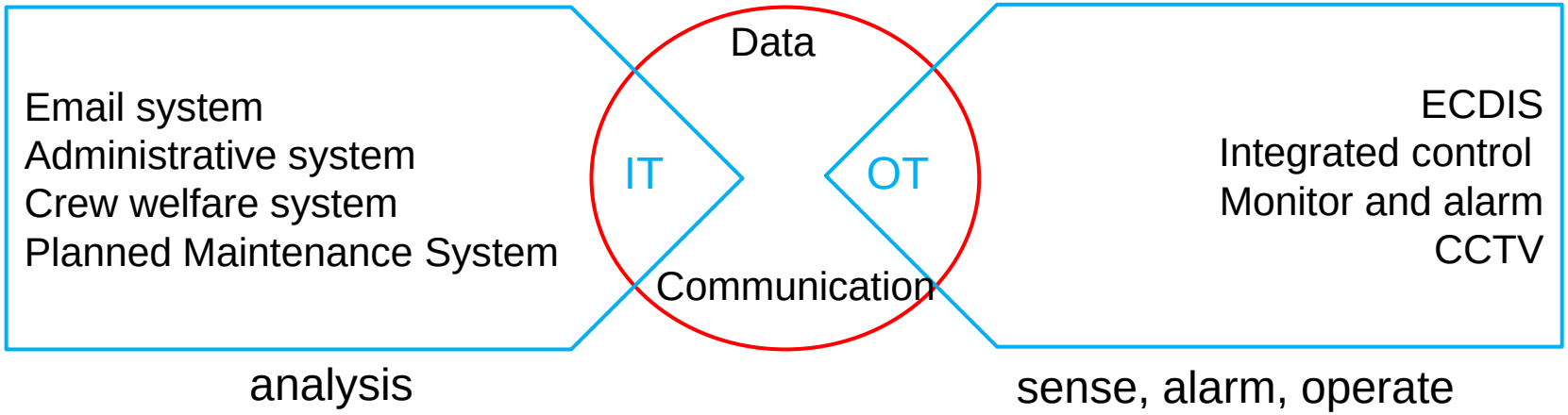


- IT and OT are not so clear
- Based on convenience, some OT system, such as ECR monitoring, will be designed to be monitored remotely from IT networks or shore-side, and the connection to shore-side will pass through IT networks.
- Some standalone OT system may also be indirectly connected via USB
- Based on cost saving, IT computers may connect directly to the Internet via a 4G network card or mobile phone during a coastal voyage or berthing.

Ideal situation

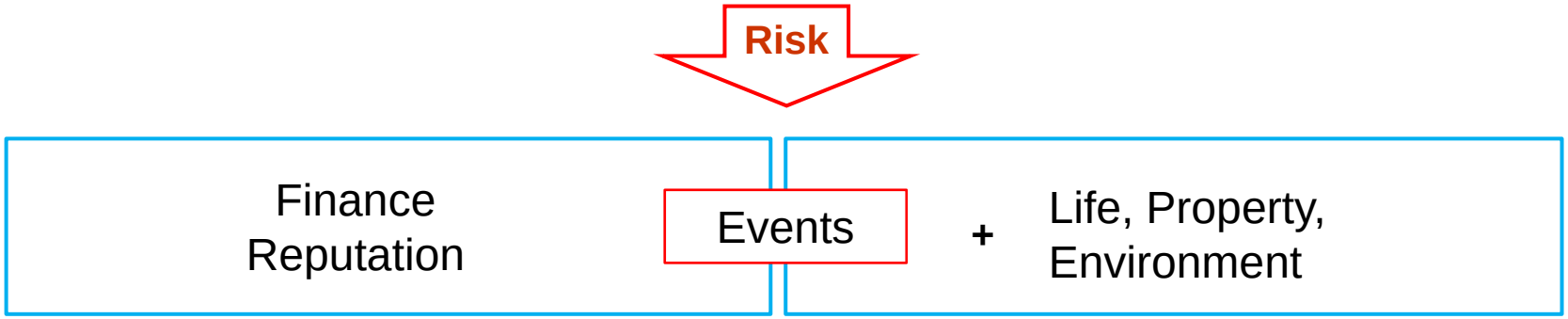
Practical situation

Finding 1: IT & OT Converge/Mingle



IT/OT Mingle

More direct , integrated , efficient



Finding 2: Management Vulnerability

General

- Cyber security management is basically blank
- Rely on established conventions and personal abilities
- Contingency is not considered

Keypoints

- No formal released cybersecurity management system
- Organizational structure not perfect and responsibilities are not clear
- Construction & delivery management not perfect
- Asset management not perfect
- No uniform operation and maintenance specification
- Security and malware prevention management is not perfect
- Change management not perfect
- Emergency preparation not perfect

Responsibilities rely on established conventions

Rely on builder & supplier

No asset inventory onboard

Rely on personal abilities of administrator

No rules for access control and upgrade maintenance

No verification of ECDIS map update

No local backup and configuration files

Finding 3: Technology Vulnerability

General

- ✓ Hardware and software, virus defense, etc. not timely updated
- ✓ Protection measures simple, security foundation weak
- ✓ IT&OT converge/mingle, expand cyber-attack-surface
- ✓ No contingency preparedness, lack of response to events, self rescue ability

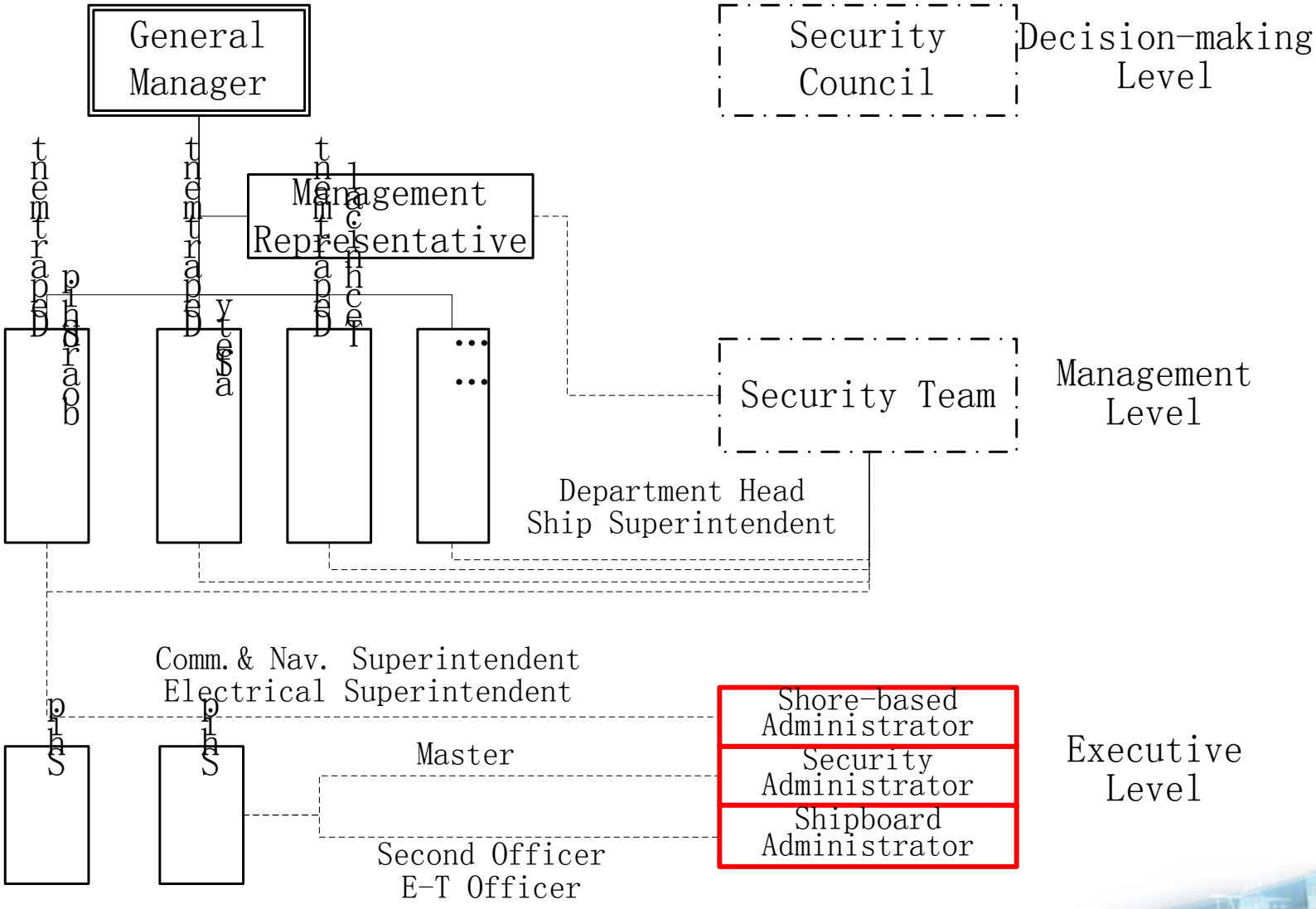
Keypoints

- ✓ OT network segment measures not perfect
- ✓ No redundancy in key equipment / function
- ✓ Lack of monitoring & checking for network configuration strategy
- ✓ Lack log of network configuration change, especially firewall & IMARSAT
- ✓ Lack external source limitation of remote access
- ✓ No limitation of personal computer access
- ✓ Weak passwords are common
- ✓ Undistinguished privileges and ordinary accounts
- ✓ Uncontrolled software installation
- ✓ System upgrade and virus database update are not in time
- ✓ Lack control of USB Ports
- ✓ OT computer lack of virus protection
- ✓ IT computer lack local backup
- ✓ No configuration file

Finding 4: Personnel Vulnerability

- General
  - ✓ Lack awareness of cyber security
  - ✓ Unfamiliar with operation, easy lead to misoperation or omission
- Keypoints
  - ✓ Responsibilities not clear, especially between shipboard and shore-side, rely on the established convenience
  - ✓ Lack of systematic training and/or guidance on cyber security, lack awareness, especially the risks posed by network threats.
  - ✓ Some business systems have no operational specification and rely on personal capabilities, easy lead to misoperation or omission
  - ✓ When leaving job, there is no specific provision for the recovery of network system resources / rights

Proposal 1：Management Organization



Proposal 2：Establish Security Policy

- General Policy: Integration of management and technology, full participation and continual improvement
- Specific Policies:

1. Information exchange
2. Information backup
3. Network monitoring
4. Information resources confidentiality
5. Change management
6. Password control
7. Email
8. Mobile code and virus prevention
9. Information security outside the site
10. Physical access
11. Access control
12. The third party access
13. Employee access
14. Clean desktop and clear screen
15. Privileged account management
16. Capacity management
17. Network configuration
18. Equipment and cable security

Proposal 3：Cyber Event Classification

- Ship Cyber Event: Emergencies involving damage to ship cyber assets (software, hardware and data), impairment of normal ship operations and even damage to ship safety
  - ✓ Accident: an event that causes damage to ship, property, life or environment
  - ✓ Major Near-Miss：an event that affects the normal operation of an OT system and may develop into an accident and require immediate measures to control, mitigate, and eliminate
  - ✓ Near-Miss：an event that affects the normal operation of the IT system, and other event besides accident and major Near-Miss.

Compatible with Event Classification of ISM

So that it can integrate with the existing security management system

Proposal 4：Risk Assessment Model

Asset Value	ID	Level	Description
1	L	Not very important	may cause a small loss after the destruction of its security properties, and the IT system will be temporarily interrupted.
2	M	More important	may cause a moderate loss after the destruction of its security properties, and the OT system is temporarily interrupted.
3	H	Very important	may cause a serious loss after the destruction of its security properties , and the network system can not be recovered.

Threat Value	ID	Level	Description
1	L	Unlikely	Once over 2 years; happen only in very rare and exceptional cases
2	M	Possible	Once per 2 years in average; or confirmed to have happened.
3	H	Likely	Once or more times per 1 year in average; or in most cases unavoidable

Vulnerability Value	ID	Level	Description
1	L	Robust	hard to be threatened
2	M	Vulnerable	difficult to be threatened
3	H	Very Vulnerable	easy to be threatened

Risk Factor = Asset * Threat * Vulnerability

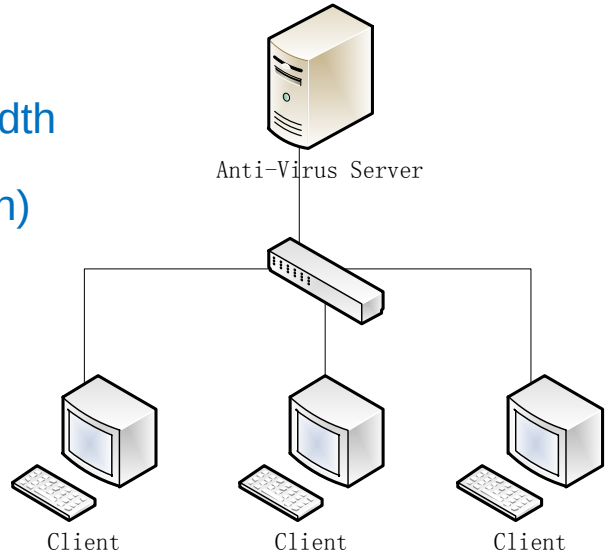
Risk Value	ID	Risk Factor	Acceptance
3	H	12<=R<=27	Control must be included in the risk treatment plan
2	M	7<=R<=11	Discuss whether to accept or not, and include unacceptable risks in risk treatment plans.
1	L	1<=R<=6	After confirmation by the person in charge, accepted without further treatment

Proposal 5：Access Control

- Physical Access
  - ✓ Setting up the cyber security area
  - ✓ Approval , check in, and accompany visitors
- Remote Access
  - ✓ Necessary to be approved
  - ✓ Restrict remote access source point
  - ✓ Mutual recognition should be made at the beginning and end
  - ✓ Appropriate monitoring during remote access to prevent unauthorized operation, best to have an action log.

Proposal 6：Anti-Virus

- Shipboard Server + Anti-Virus Clients
  - ✓ to solve the limitation of external communication bandwidth
  - ✓ server gets the update package (external communication)
  - ✓ anti-virus client is installed on the computer
  - ✓ server distributes package to anti-virus clients (inner communication)



- USB/RJ45 ports control
  - ✓ Technical measure
    - ◈ Anti-virus clients also in charge of control of physical ports such as USB.
    - ◈ Only specific devices such as mouse, keyboard, allowed to be connected;
    - ◈ Lock USB storage devices, such as U-Disk, mobile phone, so that it can not be used even if physically connected, unless authorized by administrator.
  - ✓ Physical measure

    Lock up with signature seal (dated) or physical lock

Proposal 7：Contingency Preparedness

- Asset Inventory + Responsible
  - ✓ Require builders to cooperate to develop asset inventory when delivery
  - ✓ Each asset (network equipment, IT computer, OT computer, etc.) specifies user and maintainer.
- Configuration file + Operating Specification
  - ✓ develop configuration files for network devices and IT computers, if possible, including OT computers
  - ✓ develop operating specification, deal with problems firstly according to them.
- Backup + Contingency plan
  - ✓ Cold standby or hot standby for key equipment, regularly backup for IT computers.
  - ✓ Contingency plan for each ship, different symptoms, such as software failure, hardware failure, and virus infection, are given respectively disposal plans
  - ✓ Basic strategy is to control the situation, try to restore itself, switch to emergency mode, and then request shore-based support, step by step

Proposal 8：Awareness Promotion

- Training and Drill
  - ✓ Regular cyber security knowledge training
  - ✓ Operation skills training (by supplier)
  - ✓ Regular cyber security emergency drill, shipboard only, shipboard + shore-based joint drill
- Awareness promotion materials
  - ✓ Security Manual
  - ✓ Poster (near terminals)
  - ✓ Publicity cartoon/animation/movie/film
  - ✓ Screen saver
  - ✓ …

Our Plan & Goal

Set up a cybersecurity lab, to carry out systematic research.

- Develop guidelines about cyber security, such as resilience management
  - ✓ Network architecture, redundancy and segmentation
  - ✓ Risk assessment model, classification of asset, threat, and vulnerability
  - ✓ Minimum requirements and measures of protection, detection, response and recovery
- Provide technological consulting services
  - ✓ Management: Construction consultation of cybersecurity management system
  - ✓ Technology: Harden solution of cybersecurity
    network architecture, port protection, remote access, etc.
  - ✓ Personnel: Awareness promotion by training or other materials, to train the qualified front-line manager, administrator and operator

Help shipping companies improve ship safety management system

To meet the requirements of IMO/OCIMF/RightShip and others

Create value for clients and society

This is the consistent goal of CCS.

Tel: (8610) 58112288
E-mail: ig@ccs.org.cn

Tel: (8627)85423516
E-mail: zbchen@ccs.org.cn

Welcome to contact us

Thank you for listening!