Custom-made Maritime
Cyber Security Management Systems

eDOT Solutions

ClassNK Certificate of MET

BIMCO MEMBER

ISO/IEC 27001:2013 | ISO 9001:2015 Certified | ISO 21001:2018

Risk assessment of OT systems

(CTS – Critical Technical Systems)

Whitepaper

Capt. Ruchin C Dayal

CEO, eDOT Marine, India

Master Mariner (MMI) | FIIMS (UK) | AMS - SAMS (USA)
MAIMS (Australia) | AFNI (London) | ISA

www.edot-solutions.com

contact@edot-solutions.com
ruchin@edot-solution.com

Table of Contents

1. Foreword 2
2. What are Critical Technical Systems? 3
3. IT & OT 4
4. What is the best practice for RART of OT systems? 6
5. Role of OEM's? Which OT systems require this input, as there are so many in the OT inventory? 8
6. What is the other information required for OT RART & whose responsibility is it for collating the same? 11
7. Examples 13
8. Quick Reference 16
9. Conclusions 17

1. Foreword

It has been over 4 years since work commenced on developing a practical, sustainable & a technically sound Cyber Security Management System (CSMS), for the Merchant cargo ships; and for 4 years, the risk assessment & treatment of OT systems has been the elephant in the room. From recommendations of the IMO Res 428/MSC FAL.1 Circ.3, to Class requirements, from Industry expectations (BIMCO), to views of the technical managers, the understanding and approach is phenomenally subjective & diverse.

Furthermore, with the economic demands of the trade thru the years, much of the ship-building activity takes place in the east, where cultural and lingual differences, especially in trying to communicate with integrators of a multivendor automation system, can be a challenging experience; specially so when the vessel gets older, say 10-15 years old. With multiple technical managers thru the years, with varying work cultures, DD's & modifications, the manuals and network & line diagrams tend to become obsolete. Hence, obtaining the much-needed relevant data from makers and integrators turns into a very sluggish process.

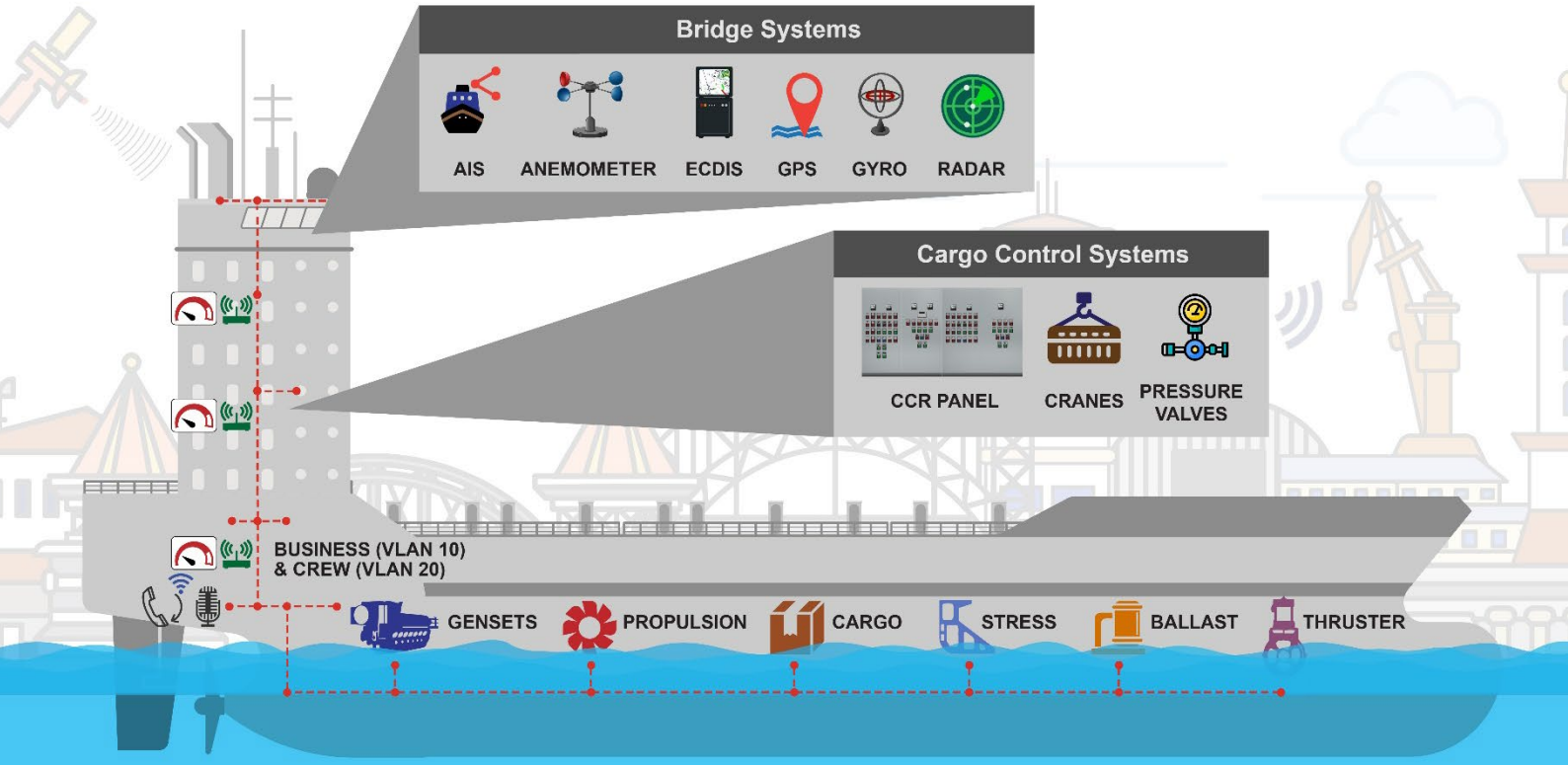
While many Classification Societies have developed guidelines for equipment manufacturers and yard integrators, it will take time to bear fruit. This is only the beginning & the road is long, but the destination is well established – a mature and robust Cyber Security Management System.

This paper has been written with the objective of providing answers to frequent questions from Ship Managers and technical Superintendents. It considers the spirit of the resolution, the industry expectations, as well the nuances of the maritime trade, together with the day-to-day onboard routines of Seafarers. I hope that it will be useful to anybody concerned with Merchant Marine Cyber Security.

2. What are Critical Technical Systems?

Commonly called as OT systems (operational technology), these are critical to the operations & safety of the ship, crew & cargo.

Some common onboard examples include Main Eng. Control systems, Power management systems in the engine room & the ECDIS on the Bridge.



3. IT & OT

IT Systems	OT Systems
Software & hardware, where the designed output is communication, is termed as IT (information technology)	Software & hardware, where the designed output is action, is termed as OT (operational technology)
Usually pertains to typical computing systems (networked or stand-alone) & their related peripherals, like switches, printers, etc.	Often pertaining to SCADA (supervisory control & data acquisition systems) systems, such as the power management system of the ship.
Non-critical & offline systems. Can be rebooted without affecting vessels operational levels.	Critical & online systems. Cannot be rebooted as will directly affect vessels operational levels.
IT systems have a COMMON output. Each system may run different OS, different versions of office, different anti-virus software, but will have a common output – communication. Can be in the form of accounting/inventory data, email, verbal speech, etc.	Each OT system will have a UNIQUE output – physical change. From closing of valves to starting of motors, from opening drains to dispensing of material, etc. Each OT system usually has its own unique firmware. This may have an ability to use HMI (human-machine interface) using a standard windows operating system.
IT systems are usually standardised – using generic hardware and software, like MS windows, intel motherboards, etc. These are designed to be patched and maintained by inhouse IT teams or outsourced IT maintenance contracts.	OT systems use customised hardware and proprietary software, which can be patched and maintained only by the makers or their authorised and trained service contractors.

Early signs of malfunction or infection are relatively easy to detect – sluggish speed of the PC, unwarranted pop-ups, or the usual hanging of the machine. Most times, just a simple reboot and running the antivirus scan may resolve the issue.	Most times, infection of an OT system may only be detected when a malfunction affecting the operational integrity of the vessel takes place – power shutdown, non-responsive engines, failure of ECDIS, etc. Rebooting of these systems is not an option.
Risk assessment & treatment of IT systems is based on standard parameters – OS, AV, software LICs, etc. – Each system/machine will be assessed individually for the status of their standard defined parameters, based on the deliverability of the common output – communication.	The output of OT systems is unique to each system and contributes towards fulfilling diverse onboard operational requirements. Hence, the risk assessment is based on the impact the OT system may have on a particular onboard activity, such as Navigation, propulsion, etc.
Makers/OEM inputs are usually not required for RART.	Crucial inputs from makers or integrators or specialist technical service contractors are required for RART.
Integrity & Confidentiality are important. Usually has no bearing on immediate operational safety. IT systems can be considered as off-line.	Integrity & Availability are important. Has an immediate and direct bearing on operational safety. OT systems are on-line systems.

4. What is the best practice for RART of OT systems?

An Asset (system) & Activity centric practice.

The following OT risk assessment is based on recommendations of MSC-FAL.1/Circ.3, BIMCO & ISO 27001. The eDOT CSMS is based on Class NK CSMS – Ref is made to Class NK Cyber Security Management System for Ships (First Edition).

As discussed earlier in this document, the output of each OT system is a unique physical action element, which contributes to operational demands of the vessel. Hence, while a system-by-system assessment approach needs to be adopted, it is of paramount importance to consider the impact of failure of any of these systems, on the operational integrity of the activity with which they be directly or indirectly associated.

To start with, the vessels operations must be broken up into main activities such as:

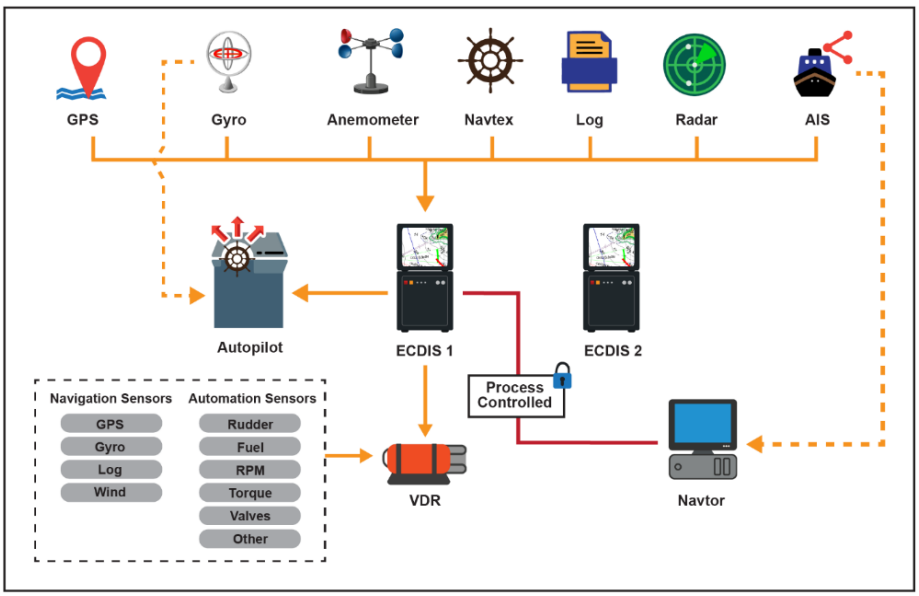
- Bridge systems
- Cargo handling and management systems
- Propulsion and machinery management and power control systems
- Access control systems
- Administrative and crew welfare systems
- Communication systems.

The main activity must then be further broken down into sub-activities.

Bridge systems has been considered as an example for the purpose of this document.

a) Bridge systems – Navigation (main activity) with the following sub-activities (non-exhaustive):
   I. Passage planning
   II. Position fixing
   III. ROR
   IV. Steering/Autopilot
   V. Weather recording/Nav-Warnings/SafetyNet
   VI. Reporting & Identity (AIS Ops)
   VII. VDR functions
   VIII. BNWAS – Alarm systems
   IX. Remote Engine Controls

Each of these sub-activities are executed using a set of OT systems redundancy(assets). The risk assessment must be focused on each sub-activity, asset-wise (system by system), where each sub-activity must be handled separately. While assessment for "vulnerability" & to some extent "threat", may be OT system specific, the impact considerations are to be made considering the vessels activity. For example, the "vulnerability" of ECDIS revolves around the methodology adopted for ENC correction, which is system specific. This "vulnerability" may be exploited as a "threat" of infection from virus, malware. However, malfunction/failure of the ECDIS may



render the vessel without a working chart, which surely will "impact" the vessels' ability to navigate, which may further result in disastrous consequences for the ship manager.

It has to be appreciated that the practical aspects of threat and impact of an activity is well understood by the seafarer and may even be within the purview of an auditor or a third-party management system integrator, however, the technical intricacies of OT systems must be collaborated upon with respective OEM's or relevant authorised technical service providers.

A brief example of the proposed system-by-system, activity centric risk assessment is produced in the later sections of this paper.

Chapter 6.2 of BIMCO Guidelines V4 states very aptly
"The risk assessment relies on knowledge of the functionality of the systems, data flows to and from the system, and precisely how each system is connected to other systems either by cable or wireless connection. For the same reason, the risk assessment will most likely require input from a broad range of company staff, equipment makers and external cyber security experts, when appropriate."

Role of OEM's? Which OT systems require this input, as there are so many in the OT inventory?

Do not mix up "Inventory" with RART (Risk Assessment & Risk Treatment). The RART will be based on ships main-activities, sub-activities & the systems (assets) associated with them.

Determine the list of OT systems associated with these activities, which directly impact operational integrity of the vessel; These listed OT systems, (in the prescribed RART form) MUST be focused on first.

Other OT systems, which may not be impacting critical operations of the vessel may be attended to in a phased manner once the company's CSMS (Cyber Security Management System) matures.

New buildings must use every opportunity to comply with cyber security requirements concerning all relevant OT systems. Makers (OEM's) are aware of Class & industry guidelines, and Class representatives themselves will ensure adherence.

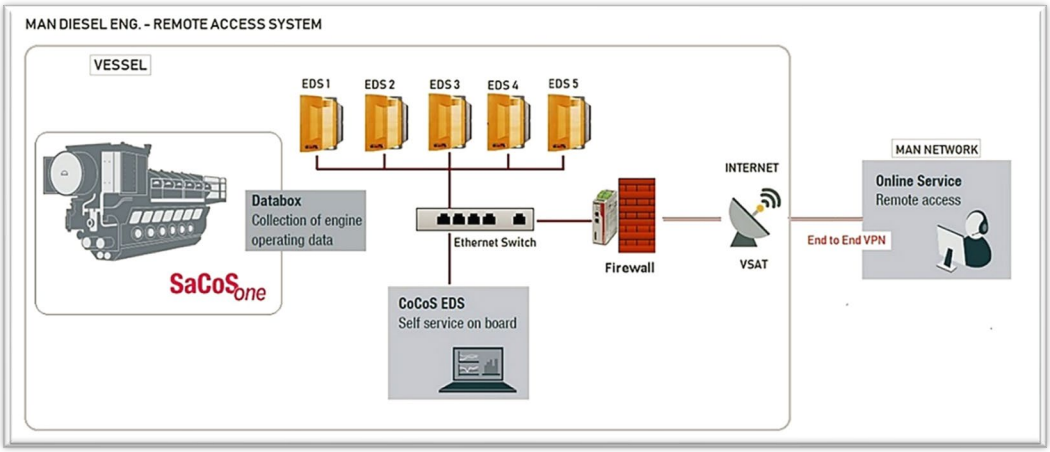
Existing ships, especially those which are a decade or more old, may find the exercise (of collating system data from OEM's) more challenging. However, if the proposed practice of RART is adapted organically into the culture of the management, the assessment will become more detailed and relevant over time. Contribution from technical superintendents, ships engineers, service contractors, as well as professional third-party consultants, together with whatever possible consultation with OEM's, will improve the over-all process. It is relevant that records of collective efforts towards this practice are maintained, if only to determine a tangible & objective evidence of the improvement in the quality of RART & the availability of data for FDD's. For example, email records of meetings organized, technical papers on OT systems, introduction of third-party suggestions, etc.

The FDD (functional descriptive diagram)

What information may be required in an FDD?

Much will depend on the system itself, however, other factors such as the expected competencies of the end-users, will also determine the form an FDD must take. For example, consider the GPS, where the device

simply receives satellite positions & feeds information to the other systems related to navigation; the end user of the GPS is a navigation officer, with limited engineering knowledge; hence, the FDD must be simple block diagram with input and output connections, the redundancy provided, simple instructions and easy contact details of the help at hand. However, the FDD of a SCADA system in the engine-room will be more detailed, where the inter-connectivity is more complex, however, a qualified marine engineer will be expected to understand the intricacies involved.



In general, it is proposed that a FDD must contain the following information. ***For new buildings - a MUST || existing ships – develop in a phased manner.***

- A block diagram/schematic, showing the various components & interconnectivity of the system
- Dependencies – input information – output information
- Input ports – output ports – connected & open – location of these ports
- Communication protocols/ports & services in use – encrypted or not
- Embedded OS/firmware version – update/backup/patch plan & process
- System requirements for internet/VSAT connectivity
- Established vulnerabilities / recovery procedure
- Inbuilt cyber security measures / tamper proof mechanisms
- Single point contact (OEM) – name / number / email

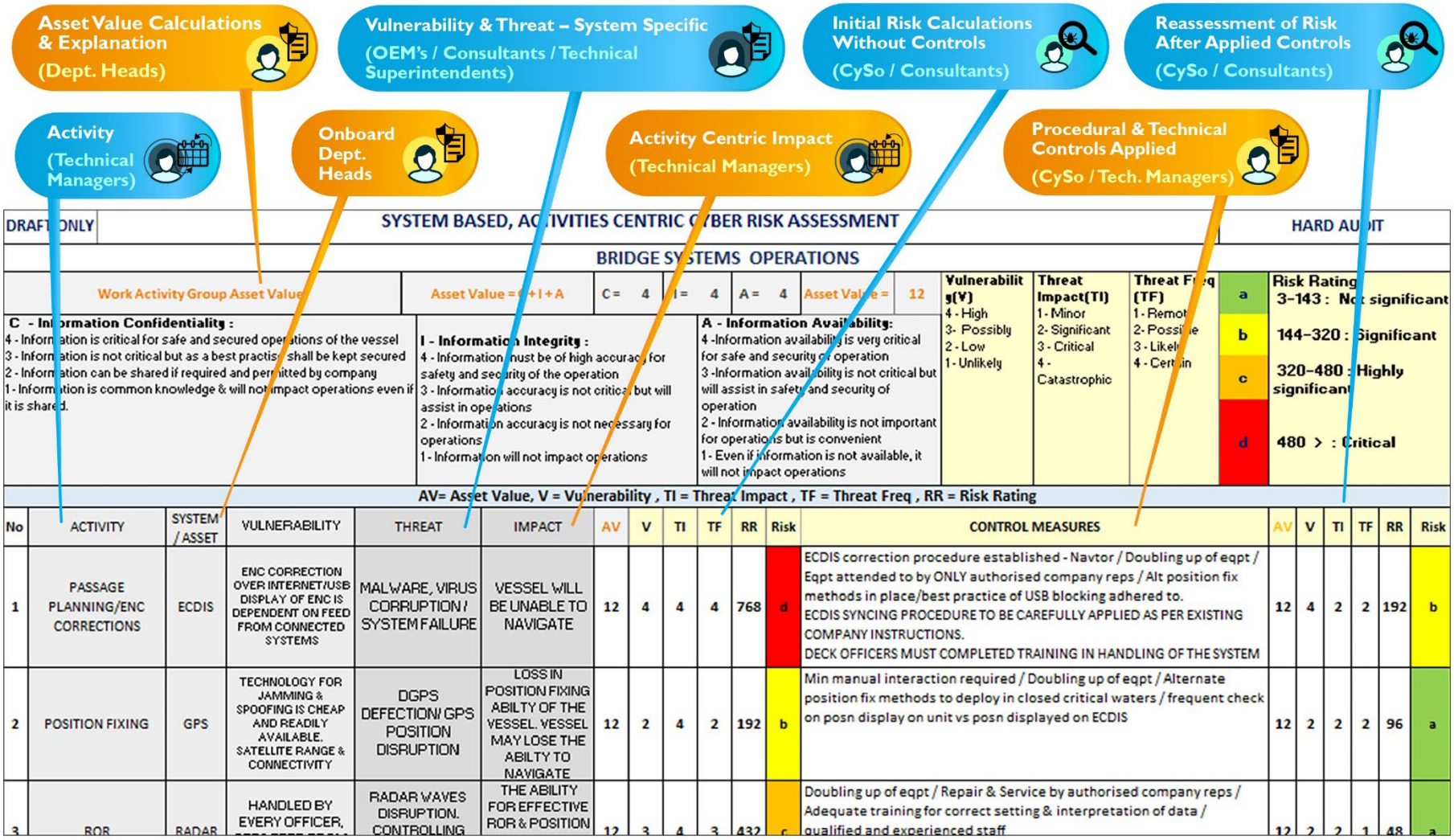
5. What is the other information required for OT RART & whose responsibility is it for collating the same?

ELEMENTS OF MANAGING RISK	FUNCTIONS	RESPONSIBILITY	REMARKS
IDENTIFY	List main activities & sub-activities	Ship managers/Master/Dept heads	Much of this work can be carried out in consultation with a third party professional cyber security expert.
	List down related equipment	Vessel Dept heads	
	Determine CIA score	SCyO/CySO (ship & Company cyber officer)	
	Establish initial risk rating with no controls	SCyO/CySO	
PROTECT	Provide technical details of equipment as an FDD	TSI(technical suptds)/OEM	FDD must be furnished by OEM TSI inputs are paramount. Professional guidance is available TSI must liaise with OEM for the same.
	List control measures & comments	OEM/TSI	
	Recalculate risk rating after control measures	SCyO/CySO	
	Communicate with TSI/OEM for risk concerns	SCyO/CySO	
	Implement necessary processes/devices to mitigate risk	TSI/OEM/technical service contractors	

DETECT	Establish drills & routines to check control measures efficacy	SCyO/CySO	Training Manual must be placed onboard/Drill calendar to be established.
	Recognise symptoms to identify potential problems	OEM must provide a guide / training doc	
	Implement best practices	Ship managers/Master/Dept heads	
RESPOND	Ref is made to the Cyber response plan (CSMS)	Dept heads	Response must be in conjunction with single point contact of the OEM
	Ref must be made with the FDD	TSI/OEM/technical service contractors	
RECOVER	Ref must be made with the FDD & backup & restore instructions of the OEM	TSI/OEM/technical service contractors	Recovery must be in conjunction with single point contact of the OEM

Risk assessment of OT systems (CTS – Critical Technical Systems)

6. Example



DRAFT ONLY — SYSTEM BASED, ACTIVITIES CENTRIC CYBER RISK ASSESSMENT — HARD AUDIT

BRIDGE SYSTEMS OPERATIONS

Work Activity Group Asset Value	Asset Value = C+I+A	C = 4	I = 4	A = 4	Asset Value = 12

C - Information Confidentiality :
4 - Information is critical for safe and secured operations of the vessel
3 - Information is not critical but as a best practise shall be kept secured
2 - Information can be shared if required and permitted by company
1 - Information is common knowledge & will not impact operations even if it is shared.

I - Information Integrity :
4 - Information must be of high accuracy for safety and security of the operation
3 - Information accuracy is not critical but will assist in operations
2 - Information accuracy is not necessary for operations
1 - Information will not impact operations

A - Information Availability:
4 -Information availability is very critical for safe and security of operation
3 -Information availability is not critical but will assist in safety and security of operation
2 - Information availability is not important for operations but is convenient
1 - Even if information is not available, it will not impact operations

Vulnerability(V)
4 - High
3- Possibly
2 - Low
1 - Unlikely

Threat Impact(TI)
1 - Minor
2- Significant
3 - Critical
4 - Catastrophic

Threat Freq (TF)
1 - Remote
2- Possible
3 - Likely
4 - Certain

a	Risk Rating 3-143 : Not significant
b	144-320 : Significant
c	320-480 : Highly significant
d	480 > : Critical

AV= Asset Value, V = Vulnerability , TI = Threat Impact , TF = Threat Freq , RR = Risk Rating

No	ACTIVITY	SYSTEM / ASSET	VULNERABILITY	THREAT	IMPACT	AV	V	TI	TF	RR	Risk	CONTROL MEASURES	AV	V	TI	TF	RR	Risk
1	PASSAGE PLANNING/ENC CORRECTIONS	ECDIS	ENC CORRECTION OVER INTERNET/USB DISPLAY OF ENC IS DEPENDENT ON FEED FROM CONNECTED SYSTEMS	MALWARE, VIRUS CORRUPTION / SYSTEM FAILURE	VESSEL WILL BE UNABLE TO NAVIGATE	12	4	4	4	768	d	ECDIS correction procedure established - Navtor / Doubling up of eqpt / Eqpt attended to by ONLY authorised company reps / Alt position fix methods in place/best practice of USB blocking adhered to. ECDIS SYNCING PROCEDURE TO BE CAREFULLY APPLIED AS PER EXISTING COMPANY INSTRUCTIONS. DECK OFFICERS MUST COMPLETED TRAINING IN HANDLING OF THE SYSTEM	12	4	2	2	192	b
2	POSITION FIXING	GPS	TECHNOLOGY FOR JAMMING & SPOOFING IS CHEAP AND READILY AVAILABLE. SATELLITE RANGE & CONNECTIVITY	DGPS DEFECTION/ GPS POSITION DISRUPTION	LOSS IN POSITION FIXING ABILTY OF THE VESSEL. VESSEL MAY LOSE THE ABILTY TO NAVIGATE	12	2	4	2	192	b	Min manual interaction required / Doubling up of eqpt / Alternate position fix methods to deploy in closed critical waters / frequent check on posn display on unit vs posn displayed on ECDIS	12	2	2	2	96	a
3	ROR	RADAR	HANDLED BY EVERY OFFICER,	RADAR WAVES DISRUPTION. CONTROLLING	THE ABILITY FOR EFFECTIVE ROR & POSITION	12	3	4	3	432	c	Doubling up of eqpt / Repair & Service by authorised company reps / Adequate training for correct setting & interpretation of data / qualified and experienced staff	12	2	2	1	48	a

In a nutshell the value (VA) of an asset (equipment) is directly proportional to the C (confidentiality), I (integrity), A (availability) rating of the information generated by the equipment. The seafarer is equipped to determine the values for the information generated by the equipment, albeit with a little basic training. For example, the position from the GPS, the targets on the radar, position, and chart display on the ECDIS – the critical value of information, how these equipment are interdependent and how dependent is the bridge team on this information – this is well understood by the seafarer.

Asset Value (AV)

This can be easily determine by onboard officers & engineers – basic training is sufficient, if at all required – based on system specific generated information.

Vulnerability

This is the natural weakness of the system because of the very nature of the job it is designed for- "helplessness" may be a good word. This is seldom understood or appreciated by the seafarer. This is system specific; an adequate FDD and sufficient training material for creating awareness about equipment vulnerability amongst the seafarers will help. Armed with training and knowledge, the shipboard cyber officer can easily determine the vulnerability score.

Threat

System vulnerabilities may be exploited in realization of technical threats. OEM guidance in this regard, if available, should be used. The impact of threats, on main operations of the vessel is well understood by the seafarer. Training in threat anticipation and their impact may be required. Third-party professional may be considered for consultation.

Risk (without controls)

Simple mathematical formula will provide a score of risk.

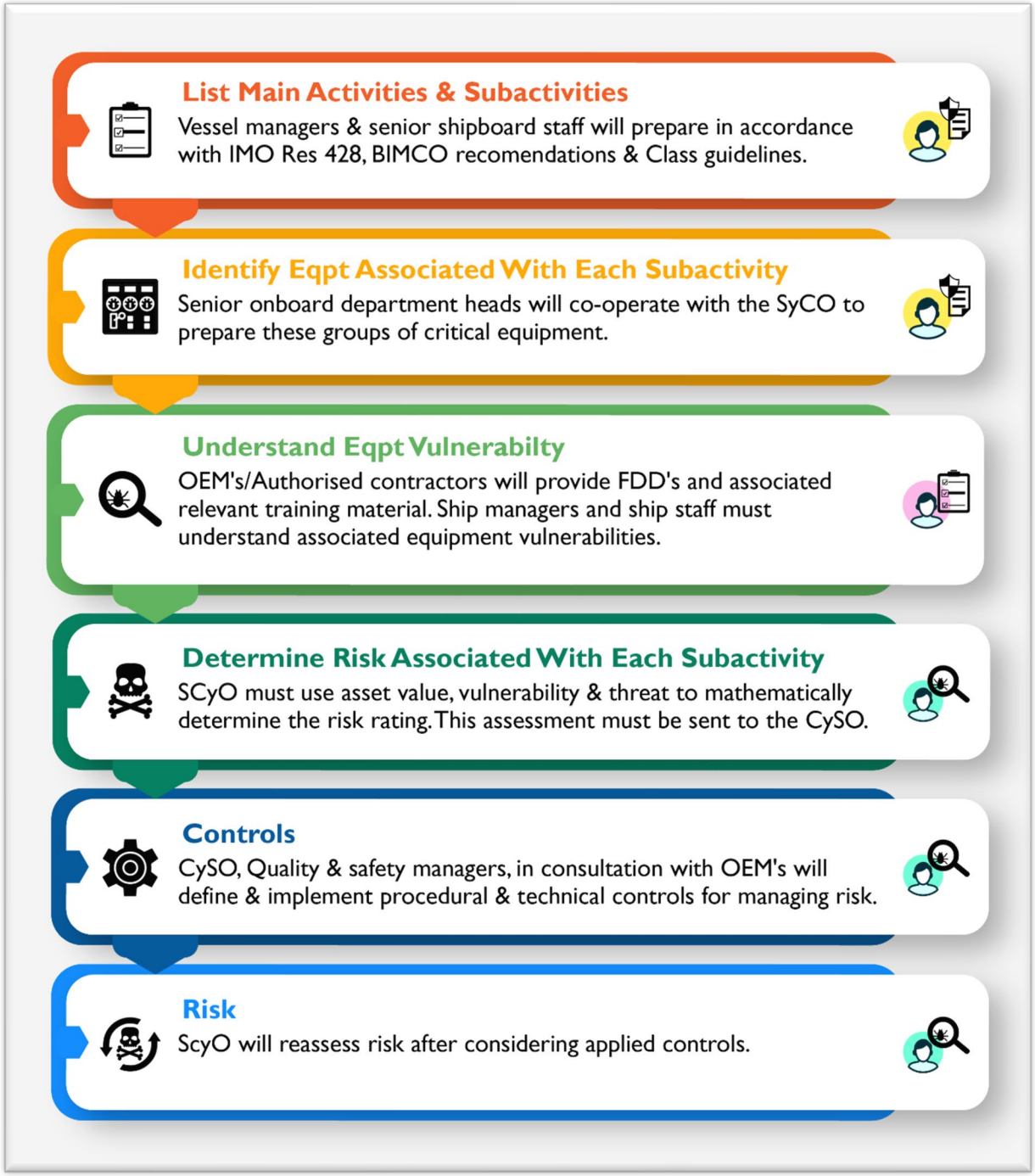
Controls

The Company Cyber Officer, senior safety and quality management, technical superintendents, third-party consultants will determine adequate controls to be implemented for mitigation of risk, where warranted. These may consist of procedural or technical solutions, often in conjunction with the manufacturers and integrators of equipment.

Risk rating with controls

Fresh scores for V, TI, TF will be determined considering the controls in place. While the score of 'V' usually must remain unaltered, the scores for TI & TF will be affected, with redundancy, broker services or stringent procedures of operation, backup & restore. This is preferably carried out by Company's cyber officer in liaison with the ships cyber officer. It is also a good practice to involve an objective third party expert.

7. Quick Reference



8. Conclusions

OT risk assessment & treatment may come across as a complicated process, however, it can be a fairly straight forward & a relatively simple exercise, if the following is considered & understood:

The objective of this exercise is to ideally prevent, but always be prepared for any contingency or emergency resulting from a cyber-attack on critical OT systems, which are integral to the safety of the vessel, crew, and environment.

The shipboard staff, especially senior members, Master, Ch Off, Ch Eng, as well as ship managers, who most times have been sailing until recently, understand the nuances of daily shipboard operations, onboard their vessels, better than anybody else. They are sufficiently experienced to identify critical activities and the associated equipment, as well as the critical nature of the information generated by these equipment. They are also well aware about situations which may develop as a result of compromise or failure of these critical equipment. Hence, the impact of an eventuality is well understood & recognised within a company – The “what” will happen is clear. However, most times, “how”, “why” and “when” an equipment may fail is beyond the comprehension of the seafarer, especially in regard to cyber related problems. This is where the roles of the OEM’s, Integrators, authorised servicemen, becomes critical.

A FDD must be provided (or developed), by or thru the makers (OEM’s), as described earlier in this document. This will help the seafarers to understand the vulnerabilities of the equipment and plan sufficient controls to mitigate risk. The FDD also provides confidence to the ship-staff, as well as the office team, that if a cyber related incident does take place, a dedicated phone number/email is at hand for immediate help from the OEM’s.

Custom-made Maritime Cyber Security Management Systems

eDOT Solutions

Email: contact@edot-solutions.com
Website: edot-solutions.com

India. Singapore. Texas. Philadelphia

ClassNK Certificate of MET

BIMCO MEMBER

ISO/IEC 27001:2013 | ISO 9001:2015 Certified | ISO 21001:2018

GOA (INDIA)

FO/2, 4th Floor, Rukmini Towers,Near Tilak Maidan, F.L. Gomes Road, Vasco-Da-Gama, Goa – 403802.

+91 832 2501715

contact@edot-solutions.com

SINGAPORE

10, Raeburn Park, #02-15E, Singapore-088702

TEXAS

7618 Westmoreland Drive, Sugar Land, TX 77479

PHILADELPHIA

Yorktown CT, Malvern, PA 19355, U.S.A.

QUALIFIED • ACCREDITED • EXPERIENCED