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

Near Miss

Shipboard Cyber Security – Operational technology

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

The seafarer has been reporting near-misses since the advent of the ISM code, for more than two decades, and as such, is tempted to ask – "what's the big deal?". However, identifying or recognizing a "near-miss" in the context of cyber security, is not only different, but also requires basic training; specially to be able to relate to potential cyber threats which are not sufficiently discussed nor documented yet.

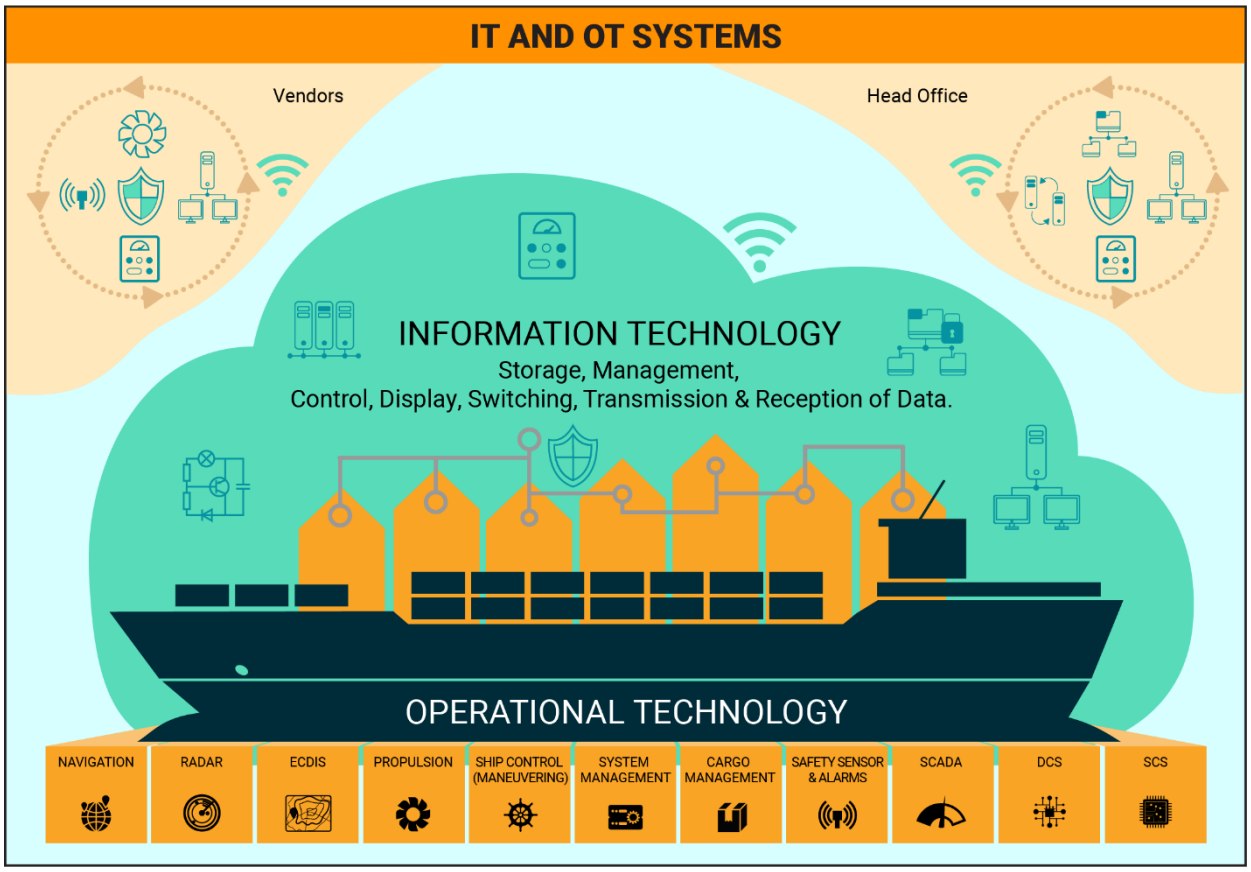
Furthermore, it is relevant to note that understanding the concept of "operational technology – (OT)", and its differences from 'information technology (IT)", is essential for estimating potential impact to operations and safety of the vessel. These concepts are explained in my papers published earlier. Readers may email me directly for these papers or for any clarification which they may require on the subject.

OT Risk Assessment
Whitepaper

Near Miss - IT
Whitepaper

Cyber Security & Ships
Published Article

In recent times, the approach of the industry has been very subjective and diverse about OT near-miss reporting. This paper attempts to create a focused line of thought in identifying & reporting of Cyber Security related OT near-misses. In a small way, I hope it will help ship managers, as well as the sailing staff, in getting familiarized with the requirements of a Cyber Security Management System.



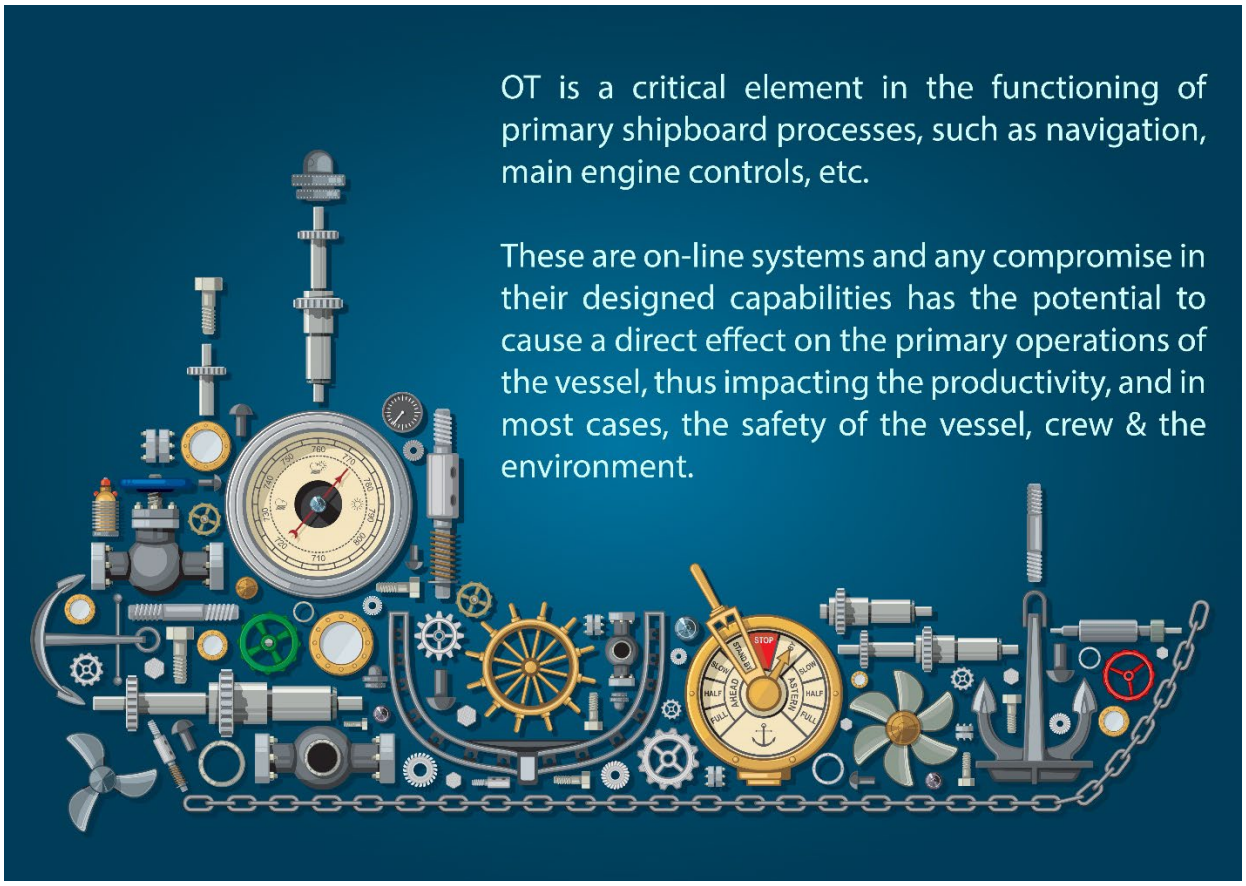
2. Near-Miss

"Near Miss" in layman terms is a "Close Shave" or "Close call" or even a "lucky escape". In the maritime world, it is quite common to be simply defined as follows:

I. When a potential risk is identified, and due to corrective action taken in time, an Incident is avoided. Usually by due diligence. OR
II. When a potential risk is not identified, and hence no corrective action is taken, however, an incident is still avoided. Usually by sheer luck.

OT Near-Miss

Hardware & software, where the designed output is physical change or action, is termed as Operational technology (OT).



OT equipment consists of hardware, as well as software-especially the controlling arm of the automation. While hardware inspection regimes, preventive & predictive maintenance schedules are well developed over time, software regimes – preventive & predictive, upgrades, compatibility, cache clean ups, efficiency and

other related maintenance tasks criteria are still at a nascent stage. This is no mean a task as several OEM's (original equipment manufacturers), with a range of different machinery/equipment, are connected by common protocols, albeit each with unique outputs and varying vulnerabilities, to arrive at an integrated onboard system. While each OEM is concerned with the performance of its supplied equipment, the vessels operations are dependent on the information generated by integrating several equipment together. For example, the process of position fixing, a sub-activity of navigation, requires the GPS, ECDIS, RADAR, GYRO, etc. Similarly, the onboard power management system may be a SCADA system with several independent components.

Post IMO Res 428, most of the classification societies as well as BIMCO have issued guidelines to the ship-staff, managers, as well as equipment manufacturers, detailing the requirements for safeguarding against software corruption and the associated controls which must be exercised as best practices. While the process will mature with time, it is essential that training of shipboard personnel is proactively approached & pursued, making them more resilient in recognizing signs of cyber related potential threats. Near Miss reporting, thus becomes an essential part of the exercise.

Recognizing & recording near-misses for OT contribute immensely to experiential learning, as well as development of the schedules for preventive/predictive maintenance & providing valuable technical data to the makers for improving and modifying equipment & controls.

3. OT Cyber Related Corruption

For recognizing or identifying a cyber related OT near-miss, it is necessary to understand, how an OT system is affected in the first place. A "cyber related event" refers mainly to corruption of the controlling software of the equipment in question, or corruption of the software controlling the entire shipboard activity. Hence, it is the corruption of the software element of the OT system.

A cyber related control software corruption can take place in 4 main forms:

1. **Direct Corruption**

This is relevant for online systems, connected via VSat/Inmarsat/others, to either makers, managers, service contractors or the internet. Some common examples include propulsion controlling systems, power management systems, which send data for analysis to dedicated servers, proactively using the vessels internet, or the ECDIS, which is dependent on connectivity for ENC corrections. These systems are vulnerable to direct corruption of their software via the internet. In the merchant cargo ships, present day context suggests that most times, this is inadvertently introduced. Willful compromise for illicit gains is presently rare. This is mainly due to the very low bandwidth made available onboard. However, as the onboard internet speeds increase to 100 Mbps or more, highly targeted hacking and tracking will become more common in the merchant marine. Until then, we have an opportunity to prepare and increase the resilience of shipboard staff & systems.

2. **In-direct Corruption**

This is relevant to all onboard systems which are driven by a controlling software. It refers to corruption arising from attendance of service engineers with their own HMI's (human machine interface – can be a simple laptop), which may be corrupted by malware unknown to them, which then gets introduced into shipboard systems in the process.

3. **Natural Corruption**

Many controlling software's use a standard operating platform. Can be a server, database, or can be that the code has been written in a certain version of a language. With the passage of time, the system resources (the hardware running the software) tend to get sluggish; either with temporary files or with a growing database cache, or simply because the operating systems and software versions get outdated, many times unsupported. A frequent observation in these systems is that they tend to "hang". Best practices for regular maintenance of the associated software are seldom followed by seafarers, who are hesitant (many times, rightfully so) to touch controlling software for critical systems. These legacy systems are especially vulnerable when attended to by external vendors, whose laptops are loaded with contemporary software; ref is made to point no 2.

4. **Un-natural Corruption**

This refers to "misuse" of the system with the controlling software. Many times, the HMI may be a regular computer or even a laptop. Poorly trained and undisciplined personnel use these systems with their personal storage devices and tend to infect them with the existing malware and other kinds of trash. There have been reports of personnel using these critical systems to watch movies during their watch-keeping. This should be considered as a severe dereliction of duty and the personnel in question must be brought to task in a very stringent manner.

It is relevant to mention that any corruption of data or introduction of malware, may go undetected for months together, coming to light only when an abnormality is noticed in the operation of the hardware. Most times, the investigation is focused on mechanical defects, failures, or related causes. Makers or service engineers are brought into the picture only after efforts of shipboard engineers and technical superintendents are exhausted, many times after changing spares,

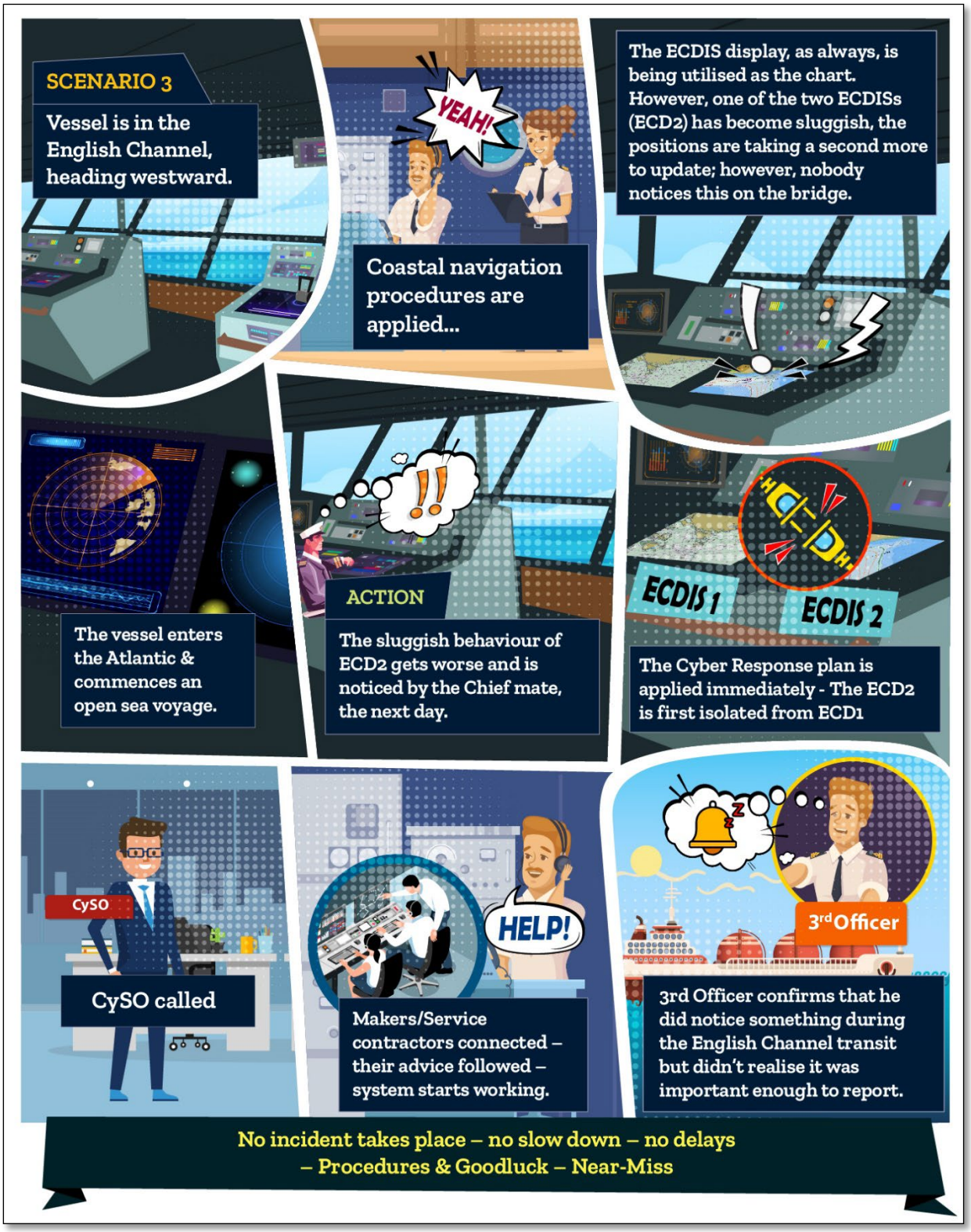
cleaning, tuning efforts, etc. Hence, actual causation is seldom arrived at, even after the makers have reset the machinery and things are working normally. It is only on a very few occasions, when a software corruption is discovered, and a subsequent investigation reveals when and where it took place. Resetting of the entire software is the more prevalent practice, especially when time is a constraint. Unfortunately, this may not clean the system but may be a temporary fix, only to experience problems again, after a period of time.

Hence, every malfunction of critical equipment, major and minor, must be approached from a cyber point of view, in addition to the mechanical investigation. This may save loads of time and effort. Makers or shore service contractors must be brought into the picture early and the probability of a cyber issue be discussed at the very onset.

In a nutshell, identifying a cyber element in a malfunction is not easy & to conclude a near-miss situation, extremely difficult!! The following section depicts a few scenarios which may be considered to be a near-miss.

4. OT Near Miss Scenarios

I have tried to build scenarios which could be considered as a “near-miss”. These are not exhaustive but only meant for gathering the thought process of seafarers in the right direction, & hope that the same may help for onboard near miss reporting.



5. Conclusion

With the development in technology, where humans are slaves to available conveniences, comforts & luxuries of equipment & machines, the brain is tuned to recognize any interruptions as a “mechanical fault”. For example, if our good old automatic washing machine at home is not cleaning the clothes properly, we suspect a weak motor, or a worn-out drum, or insufficient water pressure, etc. How many of us ever consider the corruption of the operating software? Similarly, consider this – The 3rd Officer plots a radar fix on the ECDIS chart, to find a difference of 1 NM with the position being repeated from the GPS – what do we first deduce? Poor bearing and distance measurement, or wrong interpretation of the coast. How many of us immediately consider a GPS spoofing possibility? Unfortunately, it is the same in the engine room – the main engine is having problems with emissions or maintaining RPM – piston rings have to be checked, governor to be inspected, etc. etc. – nobody ever considers a firmware or software corruption.

This thought process must change. If we must continue enjoying the benefits of technology and automation, we will have to consider their vulnerabilities and protect ourselves adequately. Simply put – we enjoy using the kindle or the iPad for reading books; It is convenient and even works as our library, however, if we do not protect our e-reader from the hazards of open internet, then it is better to go back to reading hard copy books. Unfortunately, going back in time is not an option.

The Cyber security threat is real, is here to stay and set to get more challenging in the future. The reporting of near-miss or an incident, investigation of the same, reaching the root cause, and providing experiential learning; this process is a corner stone in developing a healthy cyber hygiene culture. This culture is the single most important goal of a “Cyber Security Management plan”.

Seafarers must be encouraged to express ideas for recognizing and reporting of near misses. This is work in progress and any contribution has to be considered and treated valuable. The same goes for the readers of this article. I would be grateful and remain obliged if you could deliberate on the subject and come up with constructive suggestions.

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