Q&A at iTrust Webinar: A Cyber Risk Management Study in Shipboard OT Systems

#	Question	Answer(s)
Questions related to Communication systems and Propulsion, machinery & power control systems		
1	What is the WiFi protection solution mentioned in the presentation?	WPA2 or WPA3 (Wifi Protected Access) as they use advanced encryption standards.
2	GPS/ AIS VSAT are different system. So if VSAT is hacked how will it affect GPS/AIS?	We mentioned that the power management system can be provoked to fail by tampering the NMEA messages by hacking the VSAT terminal. Thus, if the power management system's failure affects the automatic start of emergency generator in case of a blackout condition, there will be no electricity supply in the vessel. So, the main display systems of GPS, AIS, ECDIS, etc can be turned off.
3	What does it means by "Hacking Vsat"? Is it the provider's equipment or shipboard equipment?	We mean the entire satellite communication is hacked. The VSAT modem can be hacked through its web interface by using default credentials or brute force methods and get into the ship's network where one can tamper the NMEA messages.
4	Does the attacker need to be onboard the vessel while hacking the VSAT for compromising the NEMA or fuel system? In order to hack VSAT remotely, u require complex equipment to be able to do that and when VSAT is compromised, these system should have their manual bypass to resume operation instead of being idle?	The attacker need not necessarily be onboard the vessel, though it is possible too. The satcom terminals are available in the internet, hackers can easily hack them with username and password credentials, through which they can get into the ship's network and tamper the NMEA messages. Yes, if the attacker has the advanced skill and sufficient resources (like a state-sponsored one), then a valuable target will be mostly likely a victim. Also, may be yes, there might be manual bypass to resume operations, but still it takes time to analyse and identify the source and cause of attack and get back to normal operations.
5	Hacking Vsat might be possible, so do you suggest not to use Vsat and thereby ship damage due to Cyber attack can be avoided?	No. It is a must to use satellite communication as they provide stable link for the vessel sailing anywhere on the sea to send or receive communications. Vessels need internet connection for their operations and for the crew to communicate with their main offices and family when they are far from land.
6	Is it possible for cyber attack if vessel not fitted vsat? vessel only satellite fleet broadband (fbb) for email only?	VSAT will definitely be used in the vessel since satellite communication provides a reliable and stable link for their communication and operations. However, other means of cyber attack are also possible.
7	What safeguards do we have to make the NMEA tamper-proof?	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.

8	There are auto startup mechanism of generator when there are no power detected without intervention from the power management system. Does this lower the risk of scenarios or value of attack further?	Possible. Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.
9	How to prevent cross site scripting on the web interface of the modem?	Proper input sanitisation such as, filtering the input data on arrival and also encoding the data on output can help to reduce the risk.
10	Is any antivirus software can block nema hack behavior?	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.
Questions related to Navigation systems and Cargo management		
11	How about to protect and recovery for all the threat, attack and cyber risk of navigation equipment system?	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.
12	How to control the virus to attack the Navigation equipment such as ECDIS/RADAR? It is very important and critical equipment onboard vessel .	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.
13	What is the time to impact for these scenarios where ships collide or sink? I would think it will take a few hours for the ballast water attack? crew can respond in time?	Depending upon weight, ballast water attack can take a few hours to sink the ship. When the crew members have full knowledge on detection and mitigation mechanisms of attacks, they can respond in time.
Questions related to USB ports		
14	If crew injects Malware using USB then how do we use Crew to run ships ? What is your suggestion, so that such situations can be averted?	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.
15	Can the virus introduced by external USB will help also hijackers for easy access to ship's system?	Yes, hijackers can use this virus to perform various types of cyberattacks to ship's OT systems.
16	While all possible scenarios and types of attacks on various shipboard equipment has been shared, please share solutions to prevent the same other than what is being generally done such as blocking USB ports, Firewalls, updated AVs, genuine software etc.	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.

17	Is usb vaccine is effective in countering cyber attacks? some company offers usb vaccines, is this effective?	Panda labs USB vaccine is one of the well-known USB vaccines. It acts as a protection to the system and may help in disabling automatic execution of malicious files stored in the USB drive.
18	Any other way of attack, without accessing usb or internet?	Most of the attacks happens through USB or internet but there may be a chance of attack like insider threats.
19	If any malware introduced by USB to ships equipment but no internet or wifi onboard. Can hacker access?	In this case, hacker cannot use Malware without internet or Wifi to access the system.
	Other technical questions	
20	1.) Many of these scenarios require attacker to onboard? 2.) Ship operations will have manual overrides if captain detects abnormalities?	1) All the scenarios mentioned in presentation do not require the attacker to be onboard, but insider attacks are also possible, for example, one of the crew members can intentionally inject malware into the system via USB and disrupt its operations. 2) Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.
21	How effective is the firewall provided by various service providers to protect OT systems?	Firewalls may be helpful in preventing malicious software from accessing a computer or network. Even though firewalls are used, the systems are not 100% secure.
22	Is there any way to enhance the encryption?	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.
23	Please elaborate on the DOS, Spoofing & Man In the Middle Attack.	**DOS Attack**: Denial of Service (DOS) attack is caused by flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down, eventually stop and caused by exploiting the vulnerabilities that cause the system or service to crash. **Spoofing**: Spoofing attack is when a hijacker impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls. **Man-in-the-middle (MITM):** MITM attack is where a hijacker inserts him/herself into conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other.
24	Man in the middle attack not understood. Can you explain little more. Tks.	Man-in-the-middle (MITM): MITM attack is where a hijacker inserts him/herself into conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other.
25	What type of fall back the system have in the worst case scenario and what is the recovery process?	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.

26	What are other ways to transfer files to ship's computer from external drives other than using flash drives e.g. for printing, uploading documents by inspector etc.	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.
27	What are the symptoms of a malware infection to ships computer system? In order for us to identify that the computer or system is infected.	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.
28	How Does Good Cyber Security Operate?	Defining a well-established cyber security policy and enforcing them are some of the key steps to good cyber security.
	Questions related to guidelines	
29	What are some of the guidelines considered for the study?	The following are some of the existing guidelines we looked at: ➢ Limitation to and control of network ports, protocols and services ➢ Configuration of network devices such as firewalls, routers and switches ➢ Wireless access control, malware detection ➢ Antivirus Software must be installed ➢ Two factor Authentication while accessing Sensitive data ➢ Crew cybersecurity training/awareness ➢ Vulnerability Assessment should be done in regular intervals of time ➢ Default passwords must be changed We will be producing our own guidelines too and it will be discussed in the upcoming webinars.
30	Most OT manufacturers do not build in security in the systems how can the ship owner secure those systems?	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.
31	Request to provide positive control measures for all possible identified cyber security risk & attacks.	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.
32	Is there any information/ risk matrix which shipping/ marine operating sector or model that will be more likely exposed to risk of this potential cyber attack at this stage.?	Safeguarding measures/mitigating actions of cyber risks will be discussed in the next webinar.
33	There are groups who are establishing cyber security monitoring to assist members in	No. In our work, we first investigate the cyber risks associated with each of the sub-systems of the corresponding OT systems. Next, we will harmonize the existing guidelines for cyber risk management. And finally, we will produce our own guidelines for each sub-system,

	Detection, Response and Recovery. Are you going to do the same?	considering the balance of risk vs costs and also make it easy for adoption by ship owners and enforcement by maritime authorities.
		General Queries
34	What Is the Best Way to Train for Cyber Security?	SUTD has a fulltime/parttime course known as MSSD (Master of Science in Security by Design) specialising in cyber security. Through this course, you will learn core concepts of cyber security and have hands on sessions on SWAT (Secure Water Treatment Plant) Test bed. For more info, please visit https://istd.sutd.edu.sg/education/mssd/
35	Who takes precedence in terms of compliance? IMO or the Singapore Guideline? It is hard for ship owner to be compliant to 2 different standards	The company should follow IMO requirements as a minimum. Singapore guideline is a set of guidelines for the company to adopt suiting each company specific operational structure, needs and implementation. As a basis, the company should comply to the minimum requirement imposed by IMO, company's procedures and specific class requirement, if any.
36	What are countermeasures being implemented by Equipment makers and any regulation will be implemented for approval of secure equipment?	There is no specific requirement, but the company should follow any instructions by equipment makers / class, industry guidelines accordingly.
37	Must much shall we allocate to budget this CyberSecurity risk?	As different companies have different requirements we are unable to advise a budget.
38	Is there any strict regulations emphasized that contractors/service providers installing communication equipment onboard ship must have to comply such cyber security standards and compliance.	Refer question no. 35 & 36
39	Do you see the need of the Cybersecurity equipment used in the solution such as Firewall, required to be certified by maritime authority like IEC 60945 or DNV-GL?	Refer question no. 35 & 36
40	Any online course available for cybersecurity for seafearer to understand the concept.	Yes, there are many online courses on maritime cyber security which might help the seafarers to understand the concept.
41	What's the schedule for next webinnar	Feb/Mar 2021 and Aug/Sep 2021
42	What are the specific crew training to be provided?	This may be discussed in the next webinar.

43	We have prepared a Cyber Security Manual. Do you provide any services that reviews our Manual? How do we contact you for the review of our manual?	itrust@sutd.edu.sg