

LIGHTHOUSE

R.L. INSTITUTE OF NAUTICAL SCIENCES

TVR Nagar, Aruppukottai Road, Madurai - 625 022.

Published by Marine Engineers and Navigators Association (MARENA)

voyage - 24

JUNE - 2024

CALL - 6

Different Problems and Troubleshooting of Marine Refrigeration System on Ship

Srisha Udupa - GME

Here are some of the major problems and their troubleshoot in the ship's refrigeration plant:

Undercharging of Refrigeration System

Indication:

- The compressor is running hot and the performance of the compressor falls off due to high Superheat temperature at the suction side of the compressor.
- The suction and discharge pressure of the compressor is low.
- Large vapor bubbles in the liquid sight glass.
- Low gauge readings in the condenser.
- The ammeter reading for the compressor motor is lower than normal.
- Rise in room temperature which is to be cooled.
- The compressor is running for an extended period of time.

Causes:

- Leakage of the refrigerant at the shaft seal, flange couplings, valve gland, etc.
- The expansion valve may be blocked at the strainer.
- Partial blockage of the refrigerant at the filter or drier or evaporator may cause undercharging.

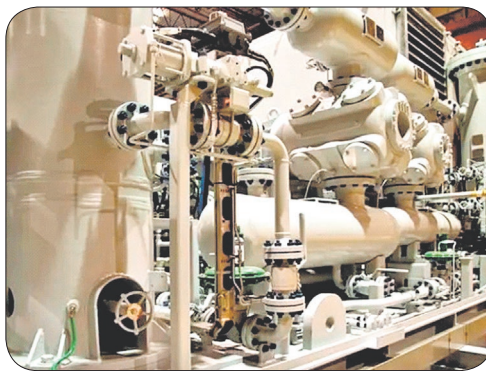
Action:

- Identify and rectify the leakage of refrigerant from the system.
- Clean the filter and drier.
- Charge the system with fresh refrigerant as required.

Overcharge of Refrigeration System

Indication:

- The liquid level in the condenser is too



■ As a Marine Engineer, you may face many problems onboard a ship. The refrigeration system can also get into some trouble from time to time. Some of these problems are common but require immediate attention.

high (high condenser gauge reading). This will reduce the available condensing surface, with a corresponding increase in the saturation temperature and pressure.

- The high-pressure switch of the refrigerant compressor activates and stops the compressor.
- The suction and the discharge pressures are high.

Causes:

- It may be due to the reason that excessive refrigerant has been charged in the system.
- Air in the system may also cause overcharging indications.
- It may also be due to the formation of ice on the regulator.

Action:

- Remove the refrigerant from the system. This is done by connecting a cylinder to the liquid line charging valve, starting the compressor, and then operating the

charging valve.

- Purge the air from the system and maintain effective cooling.
- Remove ice from the regulator by using any of the defrosting methods.

Moisture in the System

This normally comes with the ingress of air in the system. Moisture may freeze at the expansion valve, giving some of the indications of undercharging. It will contribute to the corrosion in the system. It may cause lubrication problems and the breakdown of the lubricating oil in the refrigerant compressor.

Action:

- Renew silica gel in case of minor moisture.
- collect refrigerant and remove all air and moisture by vacuum pump if the amount is huge.

Air in the System

Indication:

- This may cause the refrigeration compressor to overheat, with a high discharge pressure and normal condensing temperature.
- There are possibilities of small air bubbles in the liquid sight glass of the condenser.
- Condensing pressure of the refrigerant in the condenser may be high.
- If there is excessive air, it may reduce the cooling capacity of the system, making the compressor run for an extended period of time.
- It may cause the gauge pointer of the condenser to jump indefinitely.

Causes:

- During charging, air may enter the system.

TEAM MARENA

PATRON

Dr. R.Lakshmipathy, President, RLINS

PRESIDENT-MARENA

Capt. Gnana Edison Raj, Principal, RLINS

SECRETARY

Dr. M.Kumarasamy

SECRETARY (CADET)

Sreesha Udupa - GME

TREASURER (CADET)

Lohit Ishwar Moger - GME

MARENA CO-ORDINATORS (CADETS)

Denis Starwin - GME

Jenith Praveen Thambu - GME

TEAM LIGHTHOUSE

EDITOR IN CHIEF

Mr. M. MuthuKumar, Senior Faculty

EDITOR

Mr. V.V.Sundaram

ASSOCIATE EDITORS

Mr. S. Thiagarajan

Mr. G. Balasubramanian

EDITOR (CADET)

Abraar ur Rahman - GME

ASSISTANT EDITORS (CADETS)

Rishikesh Muruganandham - GME

Saif Anjum - GME

PHOTOGRAPHER (CADETS)

Ankit Kumar - G.P Rating

REPORTERS

Santhosh Nirbhavane - G.P Rating

Arjun Kumar - G.P Rating

LIGHTHOUSE

A Monthly Technical Magazine

Published by Marine Engineers and Navigators Association [MARENA]

R.L. Institute of Nautical Sciences, Madurai.

voyage - 24 | CALL 6 | JUNE-2024

- If Freon-12 is used air may leak into the suction line because the working pressure of the Freon-12 refrigerant is less than the atmospheric pressure.

Action:

- Air in the system can be removed by collecting the system gas in the condenser, leaving the condenser cooling water on, and venting out the air from the top of the condenser because air will not be condensed in the condenser but remains on top of the condenser above the liquid refrigerant.
- Connect the collecting cylinder to the purging line of the condenser, open the valve, and collect air in the cylinder.
- After purging the air from the system don't forget to shut the purging valve.
- Check the level of the refrigerant in the system. If required, charge the system with fresh refrigerant.
- Restart the compressor with all safety precautions.

Oil in the Refrigeration System

Indication:

- Temperature is not dropping in the cold rooms as normal, due to the fact that oil acts as insulation in the evaporator.
- It may cause excessive frost on the suction line.
- The refrigerant compressor runs for an extended period of time.
- The lubricating oil level in the compressor will drop.
- The refrigerant level will fall if the oil has caused the blockage.

Causes:

- This may happen if the oil separator is not working properly.
- Oil may carry over from the compressor and may not come back to the compressor due to blockage in the system.
- Defective piston rings or worn-out liner of the compressor may cause the oil to carry over along with the refrigerant.
- The compressor may take a high capacity current during starting.

Action:

- Check the oil separator for proper functioning.
- Check the drier for proper cleaning and if it requires cleaning clean it
- The evaporator coil should be drained to remove any trace of oil.
- If there is oil in the cooling coils, increase the condenser and evaporator temperature differentials and remove excess frost on the suction

pipe.

- Heat pipes with the blow torch.

Flooding of Refrigerant in the System

This is seen as liquid getting back to the suction of the refrigerant compressor. It may be due to a faulty or incorrectly adjusted expansion valve and also due to solenoid valve leakage. It may also result from overcharging of the refrigeration system. Flooding may lead to an iced-up evaporator.

Evaporator Coil Icing

The icing of the evaporation coils may happen due to:

Cause 1: Too low temperature setting
Action: Increase the coil temperature by adjusting TEV or it's sensor.

Cause 2: The coil capacity is less
Action: Install large capacity evaporator coils

Cause 3: Defrost is not operational
Action: Check if the defrost system is functioning at regular intervals.

Compressor Start and Stops Frequently

If while maintaining the correct temperature of the ship's provision room or reefer cargo, the reefer compressor is frequently cutting in and out, then such a problem needs to be sorted out immediately. The most normal causes for such operation are:

Cause 1: Wrong Setting of Cut outs: It may be because the high pressure (HP) cut out is set too high or LP cutout is set too low

Action: Check and change the setting to advisable limit

Cause 2: Differential Setting Span is Small: The low pressure (LP) cut out is provided with starting and stopping pressure setting. If the setting span is too small, it will lead to frequent cut-in and cut-out of the compressor

Action: Change the setting and increase the span between starting and stopping compressor pressures.

Cause 3: Defective Valves: If the compressor discharge valve is leaky or the line solenoid valve is not closing properly, this will lead to variation in sensor pressure and result in frequent cut-in and cut-out of compressor

Action: Replace all the defective valves

Cause 4: Clogged Suction Filters: The compressor is provided with a filter in the suction line. If that is clogged, it will lead to frequent LP cut out.

Action: clean the filter.

Compressor Starts But Stops immediately

When the compressor in the reefer circuit starts and suddenly stops, it can

be because of the following reasons:

Cause 1: Low pressure cut out gets activated

Action: Ensure that all the suction line valves are in open condition, the refrigeration is properly charged and the low pressure cut out is not defective.

Cause 2: Defective oil pressure cut out

Action: Check for the proper functioning of the oil pressure cut out and replace the defective cutout.

Cause 3: Defrosting timer is getting activated frequently

Action: If the defrost timer is getting activated frequently, leading to cut out of compressor, check and repair defrost timer.

Cause 4: The lube oil level is below required level

Action: This can be because of leakage of lube oil from seal or carry over of oil. Rectify the leakage and refill the oil level.

Cause 5: Foaming of oil leading to reduced oil pressure

Action: Ensure no foaming takes place, renew the oil if required.

Cause: Motor overload cutouts are activating

Action: Ensure that electrical motor trips are working properly.

Excessive icing up at Compressor suction

Causes:

- Abnormal operation of TEV.
- Overcharge of the system.
- Moisture in the system owing to dirty Dryer.
- Defective Suction valve.

Indication:

- Continuous running of Compressor.
- Insufficient cooling effects.
- Noisy operation.
- High suction pressure.
- Defective Discharge valve:

Indication:

- Continuous running of Compressor.

- Insufficient cooling effects.
- Noisy operation.
- High suction pressure during running.
- Low discharge pressure during running.
- Suction pressure rises faster after the Compressor is shut down.
- Warm cylinder head.

Choked Expansion valve

Causes:

Due to dirt and freeze-up of water present in the system.

Effects:

- Starved Evaporator
- High Superheat temperature.
- Rapid Condenser pressure rise can cause stopping of Compressor.

Remedy:

- Clean Expansion valve and filter
- Renew Dehydrator.

courtesy: bright mariner.com

Maritime security in the Indian Ocean region

Valli Kumar Alagan - GME

Maritime security in the Indian Ocean region is critical due to its strategic importance for global trade and geopolitical interests. Key concerns include piracy, illegal fishing, smuggling, and potential terrorist activities. Cooperation among countries in the region, along with international initiatives, is essential to address these challenges effectively.

How to Eradicate Piracy

Eradicating piracy requires a multifaceted approach, including:

- **Enhanced Maritime Patrols:** Increase surveillance and patrols by naval forces to deter and intercept pirate activities.
- **International Cooperation:** Foster collaboration among countries in sharing information, conducting joint patrols, and prosecuting pirates.
- **Economic Development:** Address underlying socio-economic factors that drive individuals to engage in piracy, such as poverty and lack of economic opportunities.
- **Legal Framework:** Strengthen laws and legal frameworks to prosecute pirates and dismantle their networks effectively.
- **Technology:** Utilize modern technology such as satellite surveillance, drones, and maritime security systems to monitor and respond to pirate threats.
- **Community Engagement:** Engage local communities in coastal areas to report suspicious activities and discourage support for piracy.



- **Private Security Measures:** Encourage the use of private security measures on ships, such as armed guards and secure protocols.
- **Addressing Root Causes:** Tackle the root causes of piracy, including instability, political unrest, and lack of governance in coastal regions.
- **International Support:** Secure support from the international community through initiatives like the Contact Group on Piracy off the Coast of Somalia (CGPCS) and the United Nations' counter-piracy efforts.

By implementing these measures in a coordinated manner, piracy in the Indian Ocean region can be significantly reduced and

eventually eradicated.

How to control illegal fishing

Controlling illegal fishing requires a combination of regulatory measures, enforcement actions, technological advancements, and international cooperation. Here's how:

- **Strengthening Laws and Regulations:** Implement and enforce robust legal frameworks at national and international levels to combat illegal fishing. This includes defining clear regulations, establishing penalties for offenders, and enhancing monitoring and surveillance capabilities.
- **Monitoring and Surveillance:** Utilize technology such as satellite imagery, drones, and vessel monitoring systems (VMS) to monitor fishing activities in maritime zones. This helps authorities detect and deter illegal fishing practices.
- **International Cooperation:** Foster collaboration among countries through regional agreements, joint patrols, and information sharing mechanisms to address cross-border illegal fishing activities effectively.
- **Port State Measures:** Enforce port state measures to prevent illegally caught fish from entering markets by inspecting and verifying documentation of fishing vessels and their catches.
- **Traceability and Transparency:** Implement traceability systems to track fish from catch to market, ensuring

transparency and accountability in the seafood supply chain.

- **Capacity Building:** Provide support and capacity-building initiatives to coastal states to enhance their monitoring, control, and surveillance capabilities.
- **Public Awareness:** Raise awareness among fishing communities, consumers, and stakeholders about the impacts of illegal fishing on marine ecosystems, livelihoods, and food security.
- **International Agreements:** Ratify and implement international agreements and conventions aimed at combating illegal, unreported, and unregulated (IUU) fishing, such as the FAO Port State Measures Agreement and the UN Fish Stocks Agreement.

By implementing these measures comprehensively and collaboratively, illegal fishing can be effectively controlled, promoting sustainable management of marine resources and protecting marine ecosystems.

How to prevent smuggling

Preventing smuggling requires a combination of measures aimed at deterrence, detection, and enforcement. Here's how:

- **Border Controls:** Strengthen border controls at ports, airports, and land crossings through increased surveillance, use of technology (such as scanners and X-ray machines), and thorough inspection procedures.
- **Intelligence Gathering:** Enhance intelligence gathering and information sharing among law enforcement agencies to identify smuggling routes, methods, and criminal networks.
- **International Cooperation:** Foster collaboration with neighboring countries and international partners to exchange information, coordinate operations, and address transnational smuggling networks effectively.
- **Legal Framework:** Enact and enforce comprehensive laws and regulations to prohibit and penalize smuggling activities, including measures to seize contraband goods and assets of smugglers.



- **Customized Risk Assessment:** Implement risk-based approaches to target high-risk cargo and individuals for inspection, focusing resources where they are most likely to intercept smuggling attempts.
- **Public Awareness:** Raise public awareness about the negative impacts of smuggling on economies, security, and society, encouraging citizens to report suspicious activities to authorities.
- **Technology and Innovation:** Invest in advanced technology and innovation, such as electronic surveillance systems, drones, and data analytics, to enhance detection capabilities and stay ahead of evolving smuggling techniques.
- **Strengthening Institutions:** Provide training and capacity building to law enforcement agencies, customs officials, and border security personnel to enhance their skills in detecting and preventing smuggling.
- **Addressing Root Causes:** Address underlying factors that contribute to smuggling, such as poverty, corruption, and lack of economic opportunities, through socio-economic development initiatives and governance reforms.

By implementing these measures in a coordinated and integrated manner, countries can effectively prevent and combat smuggling activities, safeguarding national security, public safety, and economic integrity.

Dangers of terrorist activities

Terrorist activities pose significant dangers on various fronts, including:

- **Loss of Life:** Terrorist attacks often result

in the loss of innocent lives, including civilians, law enforcement personnel, and military personnel. These attacks can target crowded public places, transportation systems, government buildings, or critical infrastructure.

- **Disruption of Society:** Terrorist activities aim to instill fear and disrupt societal stability. They can lead to panic, distrust among communities, and psychological trauma among the affected population.
- **Economic Impact:** Terrorist attacks can have severe economic consequences, including damage to infrastructure, loss of tourism revenue, disruptions to supply chains, and increased security costs.
- **Political Instability:** Terrorist activities can destabilize governments, undermine confidence in leadership, and exacerbate existing political tensions. They may also lead to changes in government policies and security measures.
- **Social Division:** Terrorist attacks often target specific ethnic, religious, or ideological groups, leading to social division, discrimination, and the stigmatization of certain communities.
- **Global Security:** Terrorism is a global phenomenon, and terrorist groups often operate across borders. Their activities can destabilize regions, fuel conflicts, and pose challenges to international peace and security.
- **Weaponization of Fear:** Terrorist organizations aim to spread fear and intimidation through their actions, using violence as a tool to achieve their ideological, political, or religious objectives.
- **Radicalization and Recruitment:** Terrorist activities can contribute to the radicalization of individuals, both locally and internationally, leading to the recruitment of new members and supporters for extremist causes.

Addressing the dangers of terrorist activities requires a comprehensive approach, including counterterrorism efforts, intelligence-sharing, community engagement, addressing root causes of extremism, and promoting tolerance and inclusivity.

Search for Crew member Feared Overboard Called Off When He Was Found on Ship

Capt. Gabriel

After a search spanning more than two days and covering hundreds of miles in the Pacific, the U.S. Coast Guard was informed that the suspected missing crew member was found safe aboard his ship.

Teams had been urgently searching while the USCG coordinated an effort from Guam after receiving what turned out to be a false alarm.

Details were not provided on the incident

with the USCG Joint Sub-Center Guam saying that the multi-national search effort had been concluded. They said the master of Daiwan Glory reported that the missing crew member, identified as a 39-year-old

Vietnamese citizen, was safe aboard the ship after all.

The incident began on June 25 when the Daiwan Glory, a 35,500 dwt bulker managed from Taiwan and registered in Panama, reported to the Japan Coast Guard that it had a missing crew member. The vessel issued a distress alert that morning and the USCG in Guam was notified of the man overboard situation. The report said the crew member had last been seen around 9:45 a.m. wearing orange coveralls.

The Coast Guard noted that communications with the vessel were challenging due to the distance. Updates were relayed through emails.

The Daiwan Glory reported it was searching a reciprocal track line approximately 600 nautical miles south of Guam in the area between Guam and Papua New Guinea. The USCG used the AMVER (Automated Mutual-Assistance Vessel Rescue) system to issue an alert to all vessels in the region.

The Singapore-flagged containership Kota Gabung and the bulker Golden Hope both altered course to join the search. The fol-



lowing day, another bulker the Hupeh also joined in the search as well as the LNG tanker Cesi Beihai.

A USCG HC-130 Hercules and crew from Hawaii were sent to Guam to the search. The Australian Defense Force also offered an aircraft while it was seeking diplomatic clearances for the needed airspace access. The ships reported a strong 25-knot wind but said visibility was good at 10 nautical miles. Seas were also calm at three to five feet and a warm 87 degrees Fahrenheit water temperature gave hope to the search.

66
USCG HC-130 Hercules and crew from Hawaii were sent to Guam to join the search. The Australian Defense Force also offered an aircraft while it was seeking diplomatic clearances for the needed airspace access.

99
Early on the morning of June 27, the USCG Guam reports it was informed that the crew member had been found. There was no explanation as to why the person had gone undetected for so many hours. The Coast Guard highlights that the effort however demonstrated the AMVER resource and the capabilities to respond to emergencies.
courtesy: marine executive

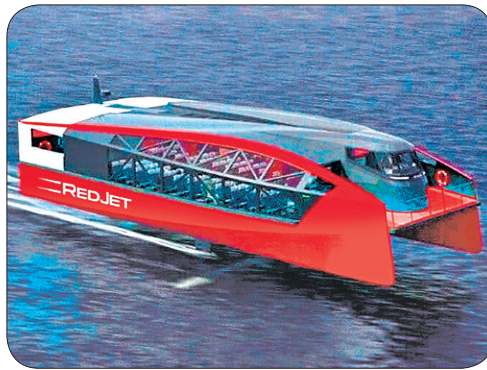
First Hydrofoiling Electric High-Speed Ferry to Launch in the UK in 2025

Madan Kanagaraj - GME

UK ferry operator Red Funnel confirmed that it plans to introduce a high-performance, emission-free high-speed vessel on its service crossing the Solent in late 2025. The unique vessel is an all-electric e-foiling passenger ferry developed by Artemis Technologies.

The design was introduced in 2022 reporting that the fast catamaran will ride above the water on three foils, and its all-electric drive will push it to speeds as high as 36 knots. Artemis has said that it expects to get a range of 70 nautical miles out of the vessel at a 25-knot cruise speed, with zero emissions and higher efficiency. Once in service, they are projecting the electric ferry will initially save 3,700 tonnes of CO2 per year and that it can be increased to approximately 4,150 tonnes when electricity from renewable energy sources is available. Passenger capacity will be up to 150, and while hydrofoiling, the ride will be more comfortable, with less vessel motion. Wake effects will also be minimized, says Artemis.

Artemis said without naming the other companies that Red Funnel will be one of three ferry operators adopting the technology. The company reported in May 2024 that it had its first vessels under construction.



■ **Red Funnel plans to launch the electric hydrofoiling ferry in late 2025 (Red Funnel).**

The company's first vessel to demonstrate the hydrofoiling technology is a 12-meter workboat. It was put in service operation along the Belfast waterfront to demonstrate the concept. The company has also received financial grants from the UK as part of the efforts to promote new green technologies. Red Funnel is one of the oldest operating and ferry companies tracing its origins to 1861. Today, the company reports it carries 3.4 million passengers and 860,000 vehicles across the Solent between Southampton, England and West Cowes on the Isle of Wight.

The company has been running a fleet of high-speed passenger ferries for more than two decades on the route. This spring they announced the sale of the Red Jet 4, which was built by North West Bay Ships in Tasmania in 2003. Powered by two MTU diesel engines, each driving an MJP waterjet to give a service speed of 35 knots the vessel carried up to 271 seated passengers and four crew. It is going to an operator in South Korea, but Red Funnel continues to operate two other high-speed vessels, Red Jet 6 built in 2016 and Red Jet 7 built in 2018. The passenger jet ferries make the transit in approximately 28 minutes while the traditional vehicle ferries take approximately an hour for the 12-mile trip.

Artemis recently reported that it entered into an agreement with DNV to collaborate to ensure that the testing and certification processes ensure that the safety requirements under the relevant international regulations and DNV rules are met or exceeded.

Red Funnel says it will be working with Artemis over the coming months for testing and sea trials of the vessel. Its high-speed crews will also be undergoing training to be prepared for the arrival of the new ferry.
Courtesy: marine executive

Lohit Ishwar Moger - GME

Modern ships are high-tech vessels, with so many of their functions connected to the internet. Thanks to modern connection options (satellite, etc.), you will have internet even in the open seas. With this, you can implement more smart solutions and use advanced technology to enhance the quality of life on the boat and even boost the functionality of the boat as a whole.

The problem is that, since your vessel is connected to the internet, it's not exposed to all sorts of cyberattacks, and protecting it needs to be your top priority. Sure, a hacker turning your lights off at random sounds like a nightmare scenario, but imagine them having the ability to turn off your systems while you are out in the open (potentially in the middle of the night).

Fortunately, the risks of this are minimal if you approach your cybersecurity right. Here is what you should do.

1. Using the right software

Seeing as how all the maritime systems are digital, it is essential that you have a robust antivirus system installed. This will play a crucial role in protecting both your ship and shore-based operations from cyber threats. You see, it is not just about the boat and boat systems. There is often a communication line with the team on shore, and this team sometimes operates on more traditional operating systems.

Just remember that there is a lot at stake here. It's not like getting your device infected with a virus or malware and losing a few files or having a few photos leaked. Sure, even this can be a serious blow to one's life and reputation, but when it comes to maritime systems, we're talking about lives being at stake.

This is why you can't just randomly pick a system. You need to find a reviewer who's always testing antivirus software and go with some of their top picks. Also, going with a free version is never advised when so much is at stake.

2. Cybersecurity awareness and training programs

Your cybersecurity methods are only effective if the persons in question use them the right way. Proper protocols are in place for a reason, and most of it is not really intuitive. This means that you have to commit to onboarding and training; otherwise, all your efforts will be for nothing.

One of the things that everyone in the system needs to understand is the importance of collaborating and sharing information through the proper channels. This way,



there's no interference or intercepting.

Also, sharing information with organizations like the Maritime Cybersecurity Center gives you more insight that you need in order to improve your cybersecurity systems. Just think about the state that anti-malware and antivirus systems would be in if they had to analyze every single scenario on an individual basis.

These centers are collaborative spaces working together to make the world of maritime cybersecurity safer as a whole. Since protecting the global shipping industry is so important, a lot of resources and interest have been poured into this field.

3. Enhanced endpoint security

The most important thing about maritime cybersecurity is to find a way to provide protection to the endpoint users. This is what really counts, what really matters. If the system is not secure enough on this end, it is not safe to use. This should always be a top priority.

The first thing you need is a range of endpoint protection platforms. We've already discussed one of these platforms in the first section (the antivirus). You also need an anti-malware system, as well as a firewall. These create digital barriers that the majority of online threats won't be able to cross. These tools are supposed to protect your users by detecting threats and acting to remove them. They need to notify, block, warn, and take protective measures to prevent users from accidentally making matters worse.

Just think about it: the majority of users are not cybersecurity experts. They're ordinary people out in the sea or even commercial sailors. In the past, these weren't positions where you didn't need to know much about cybersecurity. This will have to change.

4. AI and machine learning in cybersecurity

One of the biggest advances in the field of cybersecurity is definitely the introduction of AI and machine learning. This is a relatively complex concept that can be brought

down to two simple things.

First, the autonomy of cybersecurity methods is far higher, which means that AI can now detect and eliminate threats much more effectively, often without even having to ask for your permission and without causing any problems. This is a huge boost to maritime cybersecurity, seeing as how the entire team usually already has their hands full with actually running the ship.

Second, it can learn more effectively from previous breaches and cybersecurity incidents. This means that, with each incident, the system will become more robust and more dependable, since it will have more data to study.

5. Integration of cybersecurity with physical security

Navigation systems, communication networks, and even cargo management systems on ships predate the Internet by quite a bit. Most of the time, these systems are deliberately separated for the sake of cybersecurity, but what if this didn't have to be the case?

In order for this split to be unnecessary, you would have to ensure that your digital systems are safe on the network to the level where they never really endanger the physical security of your ship.

Also, you need to understand that these threats are far more serious than their counterparts. After all, we're talking about someone tampering with your navigation while you're out in the open. It's really hard for a sailor to come up with anything riskier.

6. Regulatory compliance and standards

The shipping industry, private vessels, and the navy are always heavily regulated. Why? Well, because this transportation, although ancient, is problematic for a lot of different reasons. Just think about it, the transportation vessels are valuable, potential incidents can be catastrophic, and there's even a risk of an ecological disaster if things go wrong.

The worst part is that, due to the modern

level of digitalization in this field, these challenges are now even more dangerous (and more likely). A remote malicious party could mess with your navigation and cause a crash or a spill, which is why maritime cyber security is already heavily regulated. In other words, you have to tend to this in order to abide by regulatory compliance. All in all, you have to do it, and it's not optional.

7. Automated threat response systems

The last thing you need is the automated threat response systems in place. This way,

you'll ensure three things.

- First, you'll ensure that the speed of response is adequate. This is often crucial in preventing or averting a full-blown disaster.
- Second, you'll minimize the impact of a disaster that actually happens. Usually, it takes time for a breach to cause any real damage.
- Third, you'll eliminate the most unreliable part of your response - the human factor.

In the end, if you have the option to automate the system, you should always use the

opportunity to do so.

Maritime cyber security has never been more important

Ultimately, with more and more boat systems using the internet and more and more smart devices in use on ships, the issue of cyber security is more important than ever. This is why you need to educate yourself on the latest cyber security measures used in the industry. This is just one of the ways to stay safe out in the open sea.

Courtesy: The opinions expressed herein are the author's and not necessarily those of The Maritime Executive.

Vizhinjam Port to host India's pioneering wave energy project

Lohit Ishwar Moger- GME

An Israel based company has initiated plans to install a generating plant at the Vizhinjam Port. Israel-based Eco Wave Power, an onshore wave energy developer, has begun discussions with the Adani Group to establish a wave energy generation plant at Vizhinjam Port, Kerala, according to a senior company official.

We are in discussion with Adani Vizhinjam Port Private Limited (AVPP) for installing power oaters as they are building a new port where they want to make renewable energy," Inna Braverman, founder and CEO of the Nasdaq-listed said.

The Vizhinjam port recently received the shipping ministry's approval as the country's first transshipment port, marking a significant milestone in India's maritime infrastructure.

An Eco Wave Power official stated, "We are currently having discussions with AVPP surrounding the potential implementation of a wave energy project, initially utilizing the 980 meters of breakwaters for a prototype and later potentially incorporating the existing 3,000 meters of breakwaters in subsequent project phases." Each megawatt (MW) of installed capacity at the port site will require 270 linear meters of breakwater space.

Braverman highlighted the regulatory challenges faced by the wave energy sector, noting that it lacks specific regulations and legislation. "While it takes around six months to build a power station, regulatory approval takes around three years," she said. Braverman also acknowledged past failures of wave energy projects in Australia, Portugal, and Europe, primarily due to difficulties with off shore installations.

In August 2023, Eco Wave Power connected its station at the Port of Ja a to Israel's national power grid, becoming the first



company to supply electricity generated from waves. The Ja a station, with an installed capacity of 100 kilowatts (kW), can power around 100 homes at peak e ciency, supported by Israel's Ministry of Energy and EDF Renewables IL.

The cost of building a 1 MW wave energy plant is approximately \$1.5 million, comparable to investments in wind and solar energy, according to Braverman.

Founded in 2011, Eco Wave Power is also set to launch the rst-ever US wave energy pilot in collaboration with Shell at AltaSea in the Port of Los Angeles. Additionally, the company received approval for the world's rst commercial-scale wave energy project in Porto, Portugal, with a 20 MW facility to supply electricity to 20,000 households. Eco Wave Power initially raised capital from venture capitalists and was listed on Nasdaq in July 2021.

Currently, Braverman and David Leb own 26.5% and 26.7% shares in the company, respectively, with the remaining holdings owned by Alpha Capital, Pirveli Investments, and others.

The collaboration with Adani at Vizhinjam port represents a signi cant step forward in harnessing renewable wave energy in India, aligning with the global shift towards sustainable energy solutions.

Courtesy: india shipping news.

NATIONAL TOPPER AWARD TO GP RATING CADET



■ Cadet Ms.Trisha Banerjee, GP Rating, 2023 batch receiving the certificate of topper in the national level for scoring highest mark (female category)

PLACEMENT DRIVE AT RLINS

R L Institute of Nautical Sciences began a new chapter in the placement cell by offering placement opportunities for the cadets taking this as an integral part of its commitment to make them employable soon after completing their course successfully. To make this drive a successful one, a dynamic placement officer has been inducted into the system to continuously sustain the

efforts of bringing various shipping companies to the institute. Capt.Thirumurthy, Head –Placement Cell took charge as a placement officer and initiated the process of bringing more prospective companies to the institute with his vast span of experience in the leading shipping industries. In this academic year, current batch of ETO cadets have been placed in the leading shipping

companies such as T.K Tankers, Synergy, MSC and Eastaway. Twelve cadets who have been placed in these shipping companies are from current batch of February -2024. Still the process is continuing for the remaining cadets to be placed from other courses in the near future. The following is the profile of students who have been placed in different shipping companies.



BARATHKUMAR S
(EASTAWAY)



DAONIL JEBIN
(EASTAWAY)



DENIS STARWIN
(SYNERGY GROUP)



JOGANNA JESVAN
(TEEKAY TANKERS)



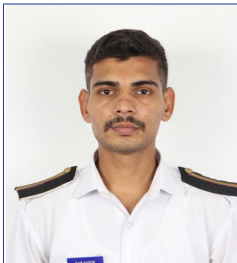
JOSEPH DERWIN
(EASTAWAY)



LOHITH MOGER
(SYNERGY GROUP)



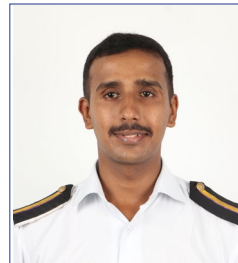
NAGENDRAN N
(MSC)



SAIF ANJUM
(SYNERGY GROUP)



SILUVAI CHARLES
(TEEKAY TANKERS)



SREESHA UDUPA
(SYNERGY GROUP)



SYED ISAMUDDIN
(SYNERGY GROUP)



THINEESH
(TEEKAY TANKERS)



SAIL TO PROSPER

*Enjoy world Travel with International Pay Scale
A rewarding career in the Merchant Navy*

4 MONTH ELECTRO TECHNICAL OFFICER'S COURSE (ETO) -

With Low Voltage

Entry Standard : Diploma / Degree in EEE
ECE Electronics and Instrumentation
Medical Fitness as per DGS norms

1 YEAR GRADUATE MARINE ENGINEERING (GME) For

Graduate Mechanical Engineers
Entry Standard : Graduation in
Mechanical Engineering
Marine Engineering or Naval Architecture

For details visit : www.rlins.edu.in email:admission@rlins.in/rlins@rlins.in

Admission Co-ordinator : +91 98940 07317 / 73391 32159 / 94890 07317

R.L. INSTITUTE OF NAUTICAL SCIENCES

(Approved by Directorate General of Shipping, Ministry of Shipping Govt. of India)

(An ISO 9001 : 2015 Certified organisation)

T.V.R. Nagar, Aruppukottai Road,

MADURAI-625 022

Phone : 7397788618

email : admission@rlins.in/rlins@rlins.in



Premium
Maritime
Institute
Since 1999



GP Rating

(6 Months Residential)

Eligibility : Pass with aggregate 40% marks in 10th Standard from recognized Board with Science, Mathematics as subject and with minimum 40% marks in English subject.

Age Limit : On the date of commencement of course
Minimum age 17½ Years Maximum age 25Years

Frequency : 2 Batches every year-January and July

Medical fitness : As per DGS norms.

Career Path

- 6 Months Pre-Sea Training Approved by (D.G. Shipping Govt. of India)
- After 6 Months of training on board ship get Watch keeping certificate (DG Shipping)
- After 36 Months of Sea time appear for 2nd mate NCV/MEO Class IV NCV. Then sail as a III officer/IV-Engineer