Callidus News

ADVOCATES, CONSULTANTS & NOTARY

BRANCHES : DUBAI | SINGAPORE | DELHI | MUMBAI | KOLKATA | CHENNAI | COCHIN info@calliduscmc.com

Dubai
Business Avenue Building
Office # 713,Port Saeed Road,
P.O. Box # 90992, Dubai, UAE.
Tel : +97142956664
Fax : +97142956099

Singapore
20 Maxwell Road
#04-02 D, Maxwell House
Singapore - 069113
Tel: +65 6221 4090

Delhi
D 1st 145 Basement (Rear)
Lajpat Nagar R 1
New Delhi - 110 024
Tel: +91 11 4132 1037

Mumbai
8-B, Dariya Building
2nd Floor, In between American
Dry Fruits & Zara, Dr. D.N.Road
Fort, Mumbai 400 001
Tel: 022-22853371

Chennai
Old No. 123, New No.255,
3rd Floor, Hussiana Manzil,
Ankapanaiken Street,
Parrys, Chennai - 600 001
Tel: +91 98 40 844463

Cochin
Near St.Joseph's High
School Chittoor Road,
Cochin - 12, India
Tel : +91 484 2391895
office@callidusindia.com

Message from the Managing Partner

As we step into 2025 with optimism and determination, I would like to take a moment to reflect on the journey of Callidus and express my heartfelt gratitude to everyone who has been a part of our success story.

The past year has been an incredible chapter of growth and accomplishments for Callidus. It is through the steadfast support of our clients, partners, and dedicated team that we have achieved significant milestones. Your trust and collaboration have been the cornerstone of our success, and for that, I extend my deepest thanks.

Looking ahead, 2025 marks an exciting phase in our journey. At Callidus, we are driven by a vision to expand our footprint and enhance our services to better serve the maritime and legal industries. This year, we are setting our sights on opening offices in Malaysia, Oman, and Saudi Arabia. These new ventures reflect our commitment to bringing our expertise closer to our clients and exploring opportunities in these dynamic regions.

Our mission for 2025 is not just about geographical expansion; it is about fostering innovation, strengthening relationships, and delivering excellence in every service we provide. We remain committed to staying at the forefront of the industry, empowering our clients with cutting-edge solutions and unparalleled expertise.

As we begin on this ambitious journey, I invite all of you to join hands with us, support us, and grow with us. Together, we can achieve greater heights and make 2025 a remarkable year for all.

Thank you once again for your continued trust and partnership. Here's to another year of success, growth, and shared achievements!

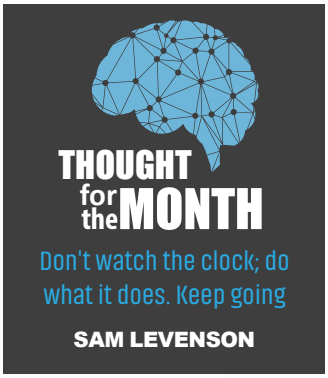
Warm regards,

Adv. Joy Thattil
Managing Partner
Callidus

CARGO CLAIMS RELATING TO DELAY

LEGAL FRAMEWORK AND JUDICIAL INTERPRETATIONS

In the global shipping and logistics industry, timely delivery of cargo is critical. However, due to the uncertainty of the industry, significant delays can still happen which could lead to various claims for both perishable and non-perishable cargo. More often than not, cargo claims relating to delay focus on business loss/profit loss and other operational loss caused by the failure to deliver the goods within the agreed timeline. Even though most of the major shipping carriers have provisions to protect themselves from delay claims, judicial interpretations consider all the related factors. This article explores certain governing principles



relating to the extent of the Carrier Liability, the burden of proof, and other considerations during delay claims.

Legal Framework for Cargo Claims Relating to Delay

International Conventions

Unlike the Hamburg Rules, which provide specific limitations on liability for delay (2.5 times the freight paid), the Hague-Visby Rules do not have a similar provision. Therefore, the outcome of a delay claim under the Hague-Visby Rules will depend on the circumstances surrounding the delay and whether the carrier can be shown to have acted improperly. Compared to these, the Rotterdam Rules, while not universally adopted, provide a more comprehensive framework, addressing liability for economic loss resulting from delays.

Essential Elements of a Cargo Claim for Delay

Generally, to succeed in a cargo claim for delay, the claimant must establish:

1. Existence of Delay: Proof that the goods were delivered after the agreed or reasonable timeframe.
2. Causation: Evidence that the delay directly caused financial loss or damage.
3. Carrier's Liability: Demonstration that the carrier failed to exercise due diligence to prevent the delay.
4. Quantum of Damages: Quantification of the financial loss incurred due to the delay.

Judicial Interpretations and Case Law

English Law

Under English law, courts have frequently emphasized the role of contractual obligations and exclusions. In **The Hollandia [1983] 1 AC 565**, the House of Lords held that time limits for delivery stipulated in a bill of lading must be strictly adhered to unless excused by an exception clause. However, in the case of **Aktieselskabet de Danske Sukkerfabrikker v Bajamar Compania Naviera SA (The Parana) [1986] 2 Lloyd's Rep 289**, the court clarified that carriers are not liable for delays caused by unforeseeable circumstances like adverse weather, provided they acted reasonably to mitigate the impact.

United States

In the United States, courts have often relied on the Carriage of Goods by Sea Act (COGSA) 1936, which incorporates the Hague Rules. The case of **Pan American World Airways, Inc. v United States, 371 U.S. 296 (1963)** underscored that carriers are liable for damages arising from delays unless they can demonstrate that the delay was beyond their control.

Interpretation of "Reasonable Dispatch"

The term "reasonable dispatch" is frequently contested in cargo claims. Courts have often interpreted it in light of the specific circumstances of each case, including the type of cargo, the agreed route, and external factors like port congestion or strikes. For instance, in **The Hansa Nord QB 44 (1976)**, the English Court of Appeal examined whether the delay was significant

enough to deprive the claimant of the contract's commercial purpose.

Limitations on Damages

Most international conventions cap liability for delays. For example, under the Hague-Visby Rules, damages for delay are limited unless a higher value is declared. The Hamburg Rules allow recovery of the total economic loss caused by the delay, provided it does not exceed two and a half times the freight payable.

Challenges in Cargo Delay Claims

Evidentiary Burden

The claimant must provide clear evidence of delay, causation, and financial loss. This often involves detailed documentation such as bills of lading, port records, and financial statements.

Defences Available to Carriers

Most effective defences used by the Carrier are-

1. Force Majeure: Delays caused by unforeseen events like natural disasters or political unrest.
2. Exclusion Clauses: Contractual terms limiting or excluding liability for delays.
3. Contributory Negligence: The argument that the claimant's actions contributed to the delay.

Conclusion

Cargo claims relating to delay remain a complex area of maritime and transportation law, influenced by international conventions, domestic legislation, and judicial interpretations. While claimants must overcome significant evidentiary and procedural hurdles, courts generally strive to balance the interests of carriers and shippers. Future developments, such as the wider adoption of the Rotterdam Rules, may provide greater clarity and uniformity in handling such claims ■

NAVIGATING DIGITAL DANGERS:
ADMIRALTY LAWS AND MARITIME CYBERSECURITY THREATS

Arundhathi B
National University Of Advanced Legal Studies

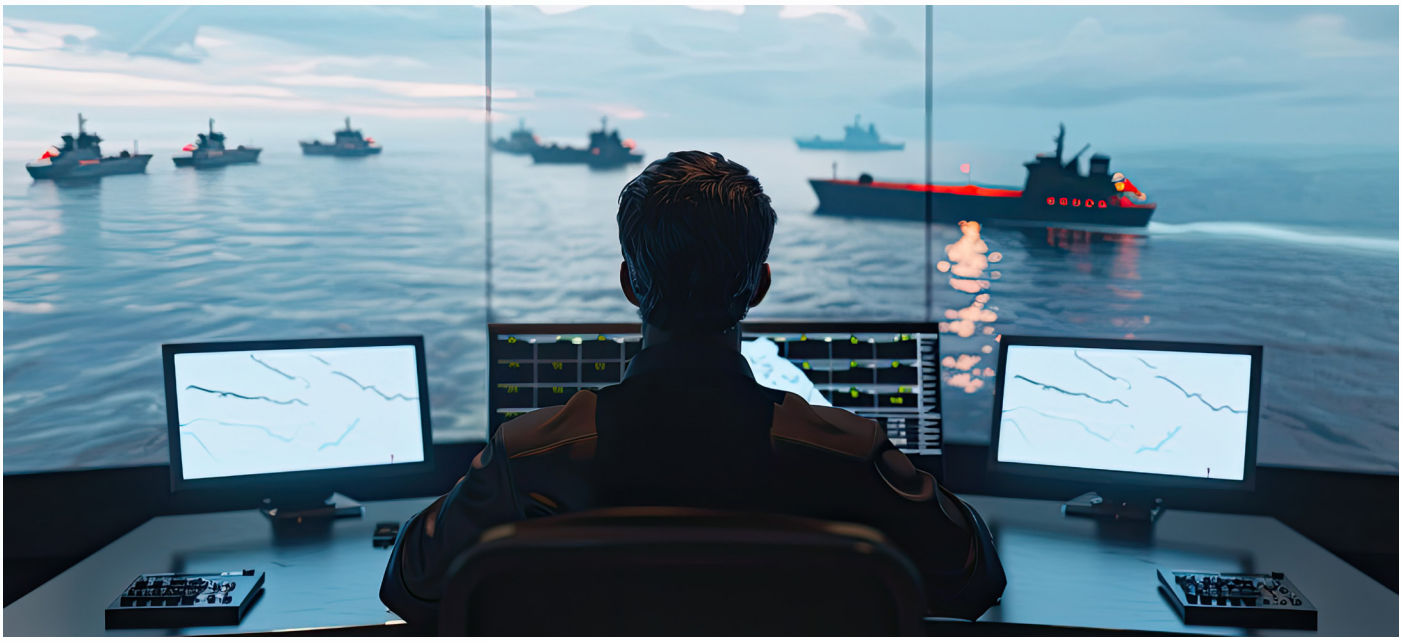
The maritime law, once concerned with maritime commerce and navigation, is now grappling with a new and formidable adversary: cyberattacks. Technological advances in the shipping industry, such as autonomous ships, drones, robotics, various block chain applications, and deep-level machine learning, hold considerable promise for the supply side of shipping. However, there is still uncertainty within the maritime industry regarding possible safety, security, and cybersecurity incidents, as well as concern about the diminishing role of seafarers, mainly from the developing world. Maritime security law has been developing for centuries. However, it still needs to be more effective in terms of difficult terrains and the impact of cyberattacks on the high seas.

Emerging Cybersecurity Threat in the Maritime Domain

The maritime sector covers many organizations and institutions, from ports to ships and satellites. Now, as one of the global economy's components, the sector relies on OT (operational technology) and IT (information technology) systems. Although digitalization is relevant for enhancing the industry in the current era, it also exposes the sector to cybersecurity risks with national security implications.

The IMO [International Maritime Organization] defines maritime cyber risk as a "measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised." Maritime cyber threats have become a serious issue over the years due to the complex operationalization of IT and OT systems, which can be the subject of malware, ransomware, and phishing attacks. Thus, there exists a need for maritime cybersecurity. Maritime cybersecurity includes the systems overseeing ships' operating software, navigation information, and traffic monitoring.

Cyber-attacks can target ships, ports, and associated logistical systems. One of the common threats is GPS Spoofing. The global navigation satellite system (GNSS signals of the GPS are often weak and can be deterred or even overload receiver circuitry by mere interference of the signal. Researchers at the University of



Texas successfully diverted the course of a yacht by exploiting the GPS Signal. The issue of GPS spoofing may not be relevant for a marine vessel in open seas, but it can still pose a problem if an attacker introduces an interference device disguised and loaded as cargo. Further, the cost of production for such a device is meagre and may even be obtained and utilized by an inexperienced hacker. This makes the issue of GPS spoofing very dangerous. In 2019, “aggressive” spoofing of the GPS signal in 20 coastal areas of the PR of China, including the ports of Shanghai, Fuzhou, Qingdao, Quanzhou, Dalian, and Tianjin, was reported by several entities and in particular by the US Coast Guard. The November 2019 MIT Technology Review magazine featured an article on this phenomenon, where analyst Bjorn Bergman evaluated a substantial amount of information contained in ships' AIS (Automatic Identification System). In this analysis, he identified at least 20 locations close to the Chinese coast where the spoofing occurred similarly during 2019, some of which were in oil terminals. Another common threat is ransomware attacks, where ships are disrupted for financial gain. The ransomware attack on DNV Ship Management Software is an example of this. The Ship Manager software was targeted in a cyberattack on 7th January 2023, which forced the company to shut down associated servers. The ransomware attack impacted 70 of its customers and roughly 1000 vessels. Data breaches and electronic piracy are also causes of concern.

Another notable incident was the NotPetya malware attack on Maersk in 2017. The NotPetya ransomware attack spread through Maersk’s network, causing the computer screen to fade to black. It was spread by Russia to attack Ukraine through a software called M.E.Doc that was used by nearly everyone who paid taxes and did business in Ukraine. NotPetya encrypts everything in its path and damages the data beyond repair. The attack disrupted Maersk's critical functions, including its network and most data. The estimated damages were well over $300 million. It took heavy repairs on the part of Maersk to get back their system. They patched all their systems and also built a new network for communication. This attack highlighted the importance of maritime security.

Legal Framework and Regulatory Response

Admiralty law traditionally governs activities involving ships, commerce, and navigation on navigable waters. Nevertheless, bringing these principles to bear on cyber incidents raises additional difficulties (not least questions of jurisdiction). Cyberattacks tend to originate from one country and hit entities in others, making jurisdiction murky. As such, the determination of jurisdiction requires legal innovation. Admiralty law must now consider whether digital assets and systems fall under its scope. Courts are beginning to explore how cybersecurity-related claims align with maritime contracts, torts, and liabilities. Several regulatory bodies and conventions are shaping the maritime sector's response to cyber threats:

International Maritime Organization (IMO)

While primarily focused on physical security, the IMO's International Ship and Port Facility Security (ISPS) Code includes some cybersecurity measures like access control and authentication. However, it mainly addresses physical threats. The Convention on Facilitation of International Maritime Traffic (FAL) has been updated to promote electronic information exchange between ships and ports, but this introduces new cybersecurity risks. To directly address maritime cybersecurity, the IMO has issued guidelines recommending the implementation of cybersecurity best practices. These guidelines emphasize the importance of identifying, protecting, detecting, responding to, and recovering from cyber incidents. Failure to comply with these guidelines can make a vessel unseaworthy. Additionally, the IMO, in collaboration with the International Electro-technical

Commission (IEC), has developed a new standard for maritime navigation and radio-communication equipment and systems. This standard sets cybersecurity requirements for shipborne equipment to ensure basic protection against cyberattacks. By implementing these measures, the maritime industry aims to mitigate cyber risks, protect critical infrastructure, and ensure the safety of ships, crews, and cargo.

The European Union (EU)

The EU Security Union Strategy for 2020-2025 warns of renewal in a whole-of-society approach to security, including the maritime sector. The Network and Information Security (NIS) Directive is a significant legislative act. The NIS Directive aims to ensure higher security of network and information systems accessed by essential services. Although it has significantly impacted cybersecurity improvement in the maritime industry, its vague criteria in defining Operators of Essential Services (OES) have created discrepancies among EU member states. To fill these gaps, the EU Commission has proposed the NIS 2 Directive, which will further tighten the cybersecurity requirements, establish stricter enforcement measures, and broaden the scope through essential services to include more maritime entities. Harmonization of cybersecurity standards coupled with strengthened regulatory oversight shall be targeted by the NIS 2 Directive to enhance the security posture of the EU's maritime sector.

Regional and National Regulations: Numerous countries have enacted or are developing cybersecurity laws applicable to the maritime sector. The U.S. Coast Guard has published rules regarding the cybersecurity of ports and vessels.

Insurance: Cyber insurance policies are witnessing increasing popularity as a means of offsetting losses due to cyberattacks.

Liability and Risk Allocation

The fast-evolving maritime cybersecurity environment has introduced intricate legal questions concerning liability and risk distribution. One key issue remains: who is responsible for a cyber incident affecting on-board systems? For example, if a vessel's navigation system is hacked, it becomes implicated whether the ship owner or the software provider is liable. Admiralty law continues to adjust by growing its principles to remedy this neglected duty. It will be soon that ship-owners and operators will be held legally responsible for implementing reasonable cybersecurity measures to safeguard their vessels, crews, cargoes, and the environment. Another important aspect is the interpretation of force majeure clauses within maritime contracts. Although cyberattacks can certainly be classified as unforeseen events, the subsequent debate lies in whether such attacks were genuinely unavoidable or simply avoidable with adequate cybersecurity measures. This underlines the need for clear specification of force majeure events in contracts and consideration of particular risks linked to cyber threats. The maritime cybersecurity incident has legal implications beyond the contractual aspect. Cyber insurance in marine contexts is increasingly pertinent, as traditional marine insurance policies may not adequately address the distinctive challenges of cyberattacks. Consequently, maritime entities are investigating more specialized cyber insurance products and risk assessment frameworks to hedge against potential financial losses. Conventional marine insurance covers little or no cyber-related loss; thus, the protection leaves a considerable gap. General Cyber insurance policies are being developed to fill this gap, but legal issues are still pending. For example, it is uncertain whether standard marine insurance covers losses resulting from ransomware attacks. Moreover, the question of whether a ship-owner was required to disclose cybersecurity weaknesses to insurers and would be liable for not implementing recommended actions is still debated. While admiralty law traditionally has been bound only loosely to insurance law, it is becoming increasingly necessary to resolve these questions and ensure that parties clearly understand their rights and responsibilities in the newly developing area of maritime cybersecurity.

Litigation Challenges in the Current Framework

Digital technologies continue to enter the maritime industry and have led to new and, more often than not, complex issues concerning cybersecurity. Even though some international and national regulations exist to counter these threats, some deficiencies exist, as detailed below.

Lack of Harmonization

Another potential problem is the absence of positive synergy between international, regional, and national legislation. Inconsistencies between the regulatory environment of different countries, regulatory requirements, standards, and compliance reduce clarity and impede implementation. The

lack of coherent and harmonized norms complicates the effectiveness and maintenance of compliance initiatives.

Lack of Appropriate Measures

Such structural changes usually have poor compliance enforcement measures being part of the regulatory framework. Lack of supervision, along with meagre funds placed into monitoring and failure to present an efficient enforcement mechanism, diminishes the influence of regulations and compliance. The approach could result in a lack of compliance with cyber security standards of the maritime sector and consequential risks to infrastructure and operations.

Rapid Evolution of Cyber Threats

The dynamics of technological changes are fast, and the continuously emerging new forms of cyber threats overwhelm the capacity to frame regulations. They are aware that such disparity opens a window of difference between regulation and addressing emerging threats.

Challenges for Developing Nations and Smaller Entities

The smaller independent states and the developing nations are particularly challenged when implementing sound cybersecurity in the sector. Lack of funds, lack of adequate technical standards, and ignorance prevent them from meeting strict regulatory requirements. This disparity results can make these entities relatively open to cyberattacks.

India and Maritime Security

India, with its ambitious plans to develop its maritime infrastructure, is not immune to the threats of cybercrimes. Recent cyberattacks on Indian ports, such as JNPT, have highlighted the urgent need for robust cybersecurity measures. India must develop a cogent cybersecurity policy for the maritime region to respond to the new cyberspace threats. This policy should consider several areas, such as the protection of critical infrastructures like ports, terminals, and shipping systems. Another way of managing cyber threats is creating acceptable responses for incidents to reduce the effects of cyber-attacks. Other responses are to train the maritime personnel on cybersecurity measures, conduct public awareness campaigns to enhance awareness of the cybersecurity risks and measures to be taken and work with other countries to share information and enhance the development of common countermeasures and solutions. The Indian Navy also plays a crucial role in maritime cybersecurity. It must implement strict cybersecurity protocols, conduct regular security audits, and invest in advanced cybersecurity solutions. Additionally, raising awareness among naval personnel about cyber threats and best practices is essential.

Recommendations

Legal frameworks and industry practices must be developed to address the growing cybersecurity risks in the maritime sector. Admiralty law should integrate clear and enforceable cybersecurity standards to protect vessels, ports, and associated digital infrastructure from cyber threats. Here are key recommendations to strengthen maritime cybersecurity through legal and regulatory measures:

1. Establishing Global Cybersecurity Standards

There is a need for standard international policies to fight the cyber menace in the marine sector. The International Maritime Organization (IMO) has done much by including cybersecurity risk management as mandatory in the ISM Code, but even more explicit and enforceable measures are required. Having a special international convention for implementing measures for the cybersecurity of ships can also unify the approaches to the regulation of different jurisdictions regarding best practices, respective imperatives, and sanctions for noncompliance.

2. Enhancing Contractual Clarity

Charter party agreements, like other maritime contracts, should state cybersecurity responsibilities. These contracts need to define how risks in the cyberattack will be shared, set a baseline of protection, and define procedures for reporting and remediation in case of an attack. Due to the integration of cybersecurity clauses in contracts, the parties are in a position to reduce and, where possible, avoid future disagreements while proactively addressing the potential risk.

3. Expanding Insurance Coverage

Ships' customary risk protection contracts have significant gaps concerning cyber risks that are mostly not covered. They should encourage or require the addition of cyber-related coverage into marine insurance policies. Thirdly, relying on the contributions of the insurance industry and other stakeholders, insurers should work out comprehensive policy solutions that consider the risks in the context of cyber threats and minimize the security risks by providing incentives to invest in protective measures.

4. Strengthening Port and Vessel Security Regulations

Ports and vessels constitute one of the links in the supply chain and, therefore, must be protected against cyber threats. National regulation must enforce the existing global standards, pay more attention to protecting operational technology, and prevent data leakage. There is no reason for such standards to be lax, so regular audits and certification should be required.

5. Building Capacity among Legal Practitioners

The complex nature of cybersecurity issues necessitates specialized expertise. Training programs for judges, arbitrators, and maritime lawyers can bridge the knowledge gap and enable effective adjudication of cyber-related disputes. Similarly,

establishing maritime cybersecurity task forces could facilitate faster legal responses to emerging threats.

Conclusion

With the current and further expansion of maritime business and operations digitalization, the industry is experiencing new emerging risks of cyber threats that endanger the global economy, particularly the maritime industry. In this paper, we demonstrate cybersecurity concerns, such as ransomware, GPS spoofing, and electronic piracy in the maritime industry, as areas of concern that require the attention of legal systems and actors. Another major subdivision of ocean law as the governing legal framework for the maritime domain calls for a response to these challenges by offering coherent legal responses that adequately ensure and protect emergent technology and important infrastructure.

One of the significant emerging disciplines is the interaction of maritime operations and cyberspace, an area characterized by dynamic and continuous threat evolution, which demands constant innovation and multidisciplinary cooperation. It, therefore, falls on admiralty law to work as a protector and a compass for the maritime market, enabling it to avoid cyber threats while embracing innovation. This would include synthesizing the guidelines intact in the inter guys and adopting clear cybersecurity terms in marine contracts and insurance that consider cyber-related dangers.

Therefore, Multilateralism is essential, especially between governments, regulators, shipping industry players, and technology developers. In this way, the maritime industry, with the help of consistent regulations, a better enforcement mechanism, and assistance to the smaller entities to implement better cybersecurity measures against the growing cyber threats, can set strong roots. Further, structural activities include official reviews of legal documents, improvements in contractual language to reduce opacity, and education and training of legal professionals working on these transactions will contribute to enhancing the sector's resilience.

However, cybersecurity in the maritime domain is not only an attempt to stop every imaginable threat. Speaking in a broader sense, the goals mentioned below are right: It is all about designing environments that have some capability to prevent or at least rapidly address cyber occurrences to minimize their impact. Part and parcel of this strategic flexibility are legal supervision, technological advancement, and prospective planning and assessment.

Consequently, admiralty law cannot remain a static construct, one capable of providing just a structural response to the problem; it must become a living legal system to deal with the issues of maritime and ship security issues. The maritime industry can thrive by fostering international cooperation and ensuring proactive, forward-looking legal mechanisms while safeguarding its critical role in global commerce. These efforts will protect the maritime sector and ensure the security and stability of international trade networks in the digital age ■

HOT NEWS

FUELEU MARITIME REGULATION COMES INTO EFFECT

As of January 1, 2025, the FuelEU Maritime regulation has been implemented to promote the adoption of low-carbon alternative fuels, driving the maritime sector towards net-zero emissions. Shipping companies like United European Car Carriers (UECC) have proactively embraced biofuels and liquefied bio methane (LBM) to comply with these regulations, achieving significant reductions in carbon intensity. This initiative aligns with the IMO's decarbonisation targets and highlights the importance of investing in sustainable technology and energy solutions to meet future compliance demands ■

www.manifoldtimes.com

Address: Near St.Joseph's High School, Chittoor Road, Cochin- 12, India, T:+91 484 2391895, office@callidusindia.com