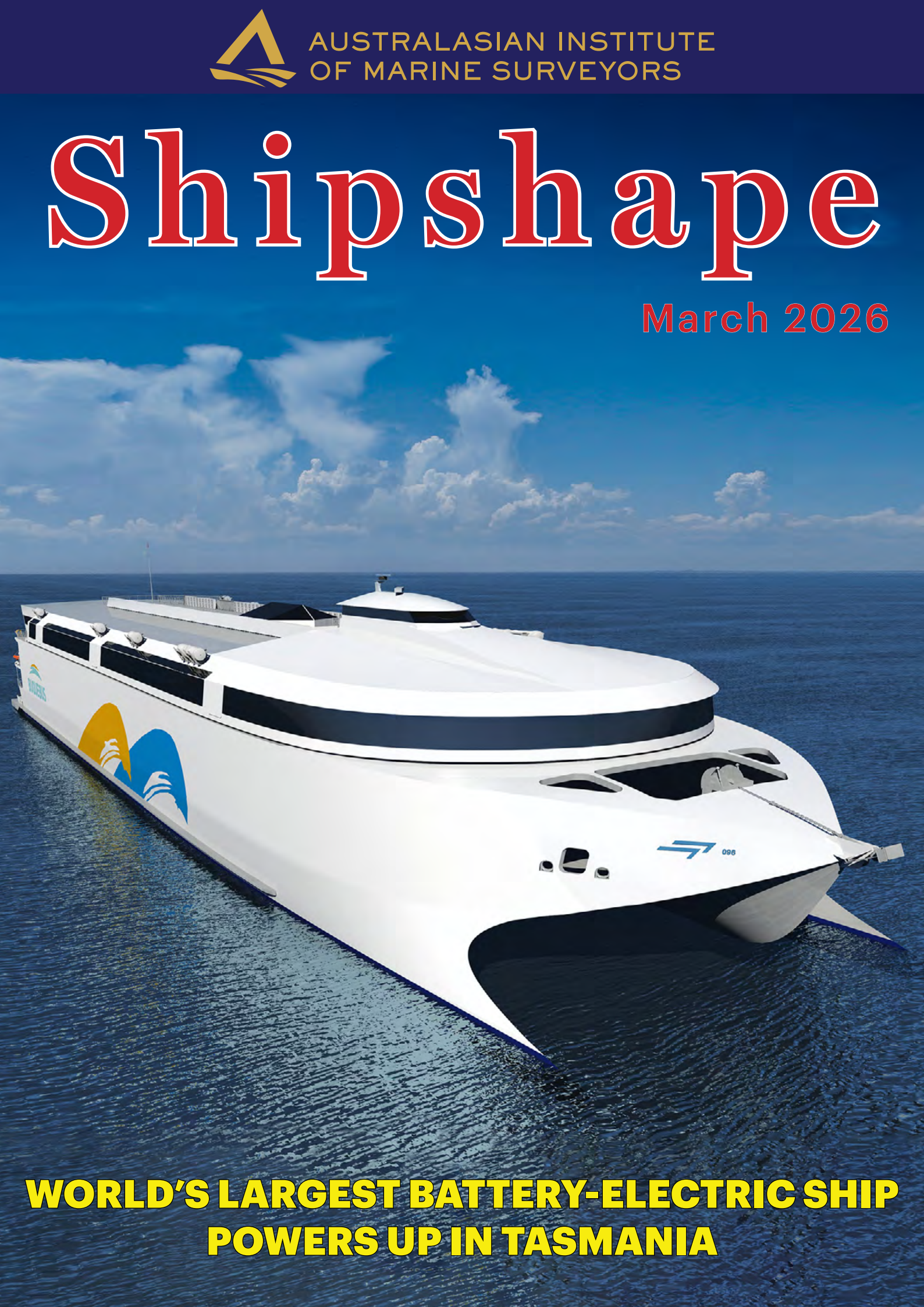
AUSTRALASIAN INSTITUTE
OF MARINE SURVEYORS

Shipshape

March 2026



WORLD'S LARGEST BATTERY-ELECTRIC SHIP POWERS UP IN TASMANIA

current AI era, however multiple layers of protection which spread across the computers, networks, programs or data that is protected may provide a degree of success that is reasonable to allow smooth operation until the investment in the cybersecurity industry can yield an absolute protection dividend.

In a maritime organisation, unified threat management – as in the form of coordinated cybersecurity management – may be the gateway system that is currently needed. For the maritime industry, with various security outposts, it may be easier to coordinate to checkmate cyberattacks, as the system of coordination already exists.

The vulnerabilities faced in the maritime industry are multifaceted; even when protected against outsiders, there is also a threat of a malicious insider manipulating or giving out security breaches. Cheating personnel wages and unreasonable sacking from work must be stopped to avoid cyberattack retaliatory actions, as these attacks can be performed remotely.

The attack in the European airports showcases weakness involved in being dependent on a single provider of software; there may be competition of software and poor design errors which overlooked weaknesses and security implications. Yet, investment in cybersecurity management and personnel training is the way to move forward for a cyber-secured maritime industry.

There is need for a targeted regulatory regime which grows with the cybersecurity industry – and in facts grows faster than it – to ensure compliance and that effective protection with a regulatory framework is available.

Nigeria may work with Australia collaboratively to exchange knowledge, experience and one another's working regulatory regimes, given that both nations are big maritime nations and apply the maritime Port State Control Memorandum of Understanding: for Nigeria, the Abuja MOU, and, for Australia, the Tokyo MOU or India MOU.

Professor Chief Emmanuel Tam. Ezekiel-Hart
AIMS Member

Note: This article is based on a lecture paper delivered by Professor Chief Emmanuel Tam. Ezekiel-Hart (Australia), who is Professorial Chair, Faculty for International Trade Relations and Logistics Management, EBS / HIBC College of Divinity, and an AIMS Member.

Cyber security

MARINE surveyors are on the frontline of the maritime industry, assessing the condition and safety of vessels.

Unlike the days before technology, the toolkit of a surveyor today has evolved from clipboards, film cameras and filing cabinets to tablets running specialised software, cloud-based data storage and artificial intelligence for data analysis.

With technology, marine surveyors are equipped with the digital tools to enhance efficiency, accuracy and reporting quality but they also introduce new risk. By relying on a chain of third-party software providers, surveyors inherit the security vulnerabilities of those platforms. Additionally, the amount of sensitive data surveyors handle is also seen as a treasure chest for cyber criminals.

Vessel blueprints, structural deficiency reports, client financial information and personally identifiable information make surveyors high-value targets for data theft and extortion.

The 2023 ransomware attack on maritime software provider DNV is a reminder that a similar flaw in a surveyor's software can also create a direct gateway for cyber criminals to steal data from the cloud or launch an attack that disrupts the surveyor's own operations.

In Australia, 62 per cent of small-to-medium enterprise (SME) businesses have experienced a cyber security incident. The average cost to recover from a cyber incident can easily reach six figures, an expense that a comprehensive Cyber Liability Insurance policy is designed to cover.

This insurance not only provides financial indemnity but also provides immediate access to the expert incident response, legal, forensic and public relations services necessary for business survival in the aftermath of an attack.

Getting a quote via our insurance partner is easy.

Follow this link now (Cyber Insurance - abcountrywide) and you will find Austbrokers Countrywide dedicated Cyber Insurance info page.

Alternatively, contact Amber Draffin at Austbrokers Countrywide Insurance Brokers on 1800 245 123.