安全、風險和合規管理

IMO網絡風險管理指南初級讀本

知道什麼以及如何遵守

ABS Group

THE AMERICAN CLUB 1917

目錄

鼓勵組織在2021年1月1日之後對公司的合規文件進行首次年度驗證之前，在安全管理系統中應對網絡風險管理。

過去20年來，海上網絡安全一直是困擾並引起人們爭論的焦點問題之一。過去5年中，各國政府、船旗國、船舶所有人和經營人等一直將海上網絡安全視為主要的安全問題和操作風險，並致力於就海洋產業如何有效控制不斷進化的網絡威脅提供建議和指引。

> 對許多於航運安全和海洋環境保護非常重要的系統的操作、控制而言，網絡技術已經變得至關重要。-IMO

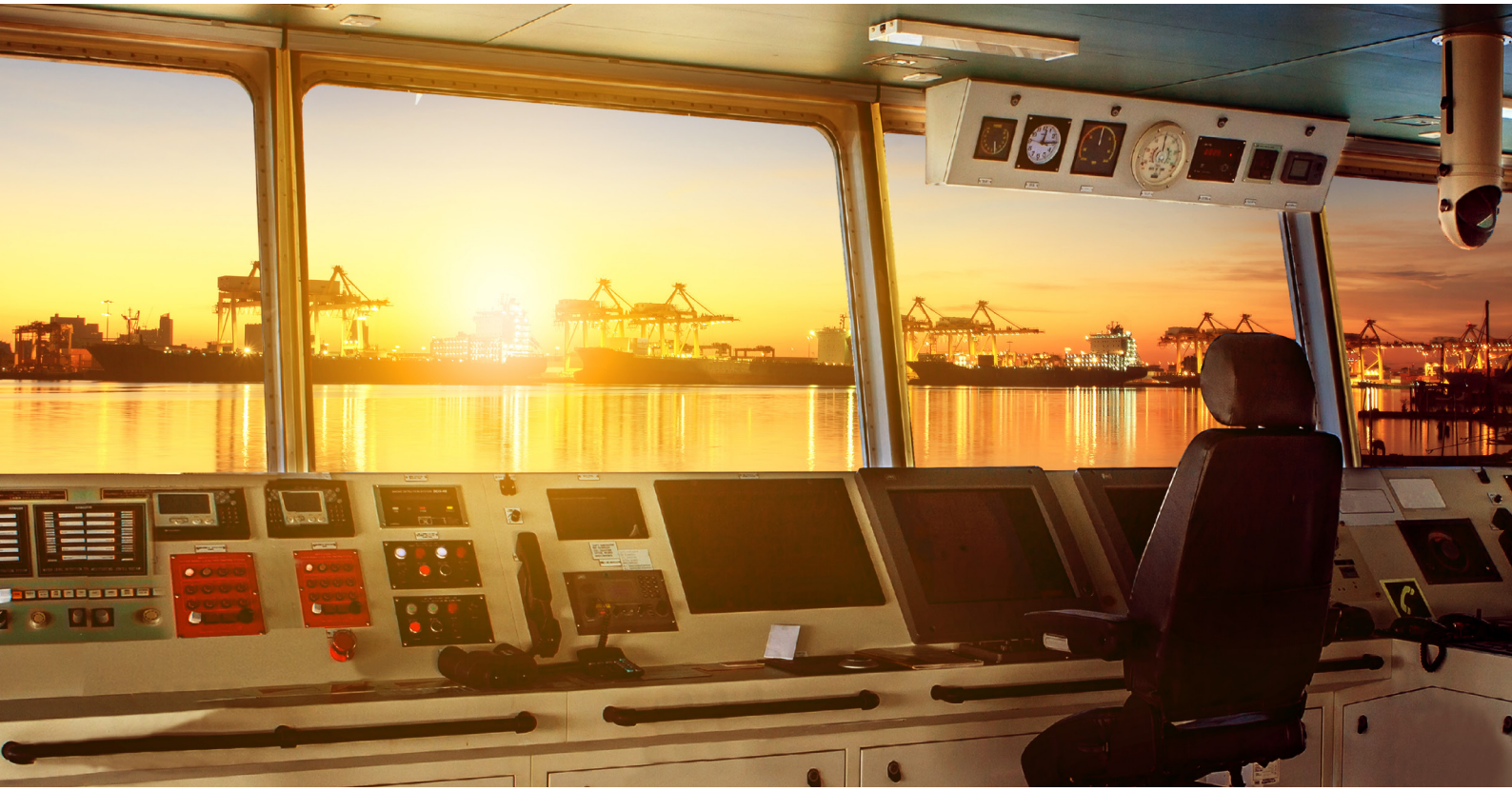
國際海事組織（IMO）提升了海上人命安全和環境。2017年，IMO發佈了通函《海事網絡風險管理指南》（《網絡風險管理指南》），並在2018年通過了一項旨在對航運業抵御潛在網絡攻擊或者事故的安全措施提供幫助的決議。

IMO的《網絡風險管理指南》建議海事組織開始實施網絡風險控制並建立網絡彈性。IMO決議建議組織在2021年1月1日之後對公司的合規文件進行首次年度驗證之前，在安全管理系統中應對網絡風險管理。

安全和風險管理的重要性

儘管IMO2017年的決議僅是「鼓勵」網絡風險管理（CRM）合規，重要的是大家應當認識到，網絡安全對您的業務，對海上財產和操作的安全性、完整性、可靠性都至關重要且起到決定作用。

在採用IMO的前瞻性指南支持有效的網絡風險管理實踐的同時，我們建議各個組織建立一套全面的網絡安全功能，以促進與國際標準和/或船旗國和港口管理要求的適當程度的合規。



IMO的網絡風險管理模型源於被普遍採用的國家標準與技術研究所（NIST）網絡安全框架。

IMO的CRM模型

根據從IMO獲取的信息，CRM是「識別、分析、評估並傳達與網絡相關的風險，並接受、避免、轉化或者減輕這種風險至一個可接受的水平，考慮對利益相關者採取行動的成本和收益的程序。」

除了IMO指南，一個聯合行業集團，包括波羅的海國際航運公會（BIMCO）、國際郵輪協會（CLIA）、國際航運商會（ICS）、國際乾散貨船東協會（INTERCARGO）、國際船舶管理人協會（IMTERMANAGER）、國際獨立油輪船東協會（INTERTANKO）、國際海上保險聯盟（IUMI）、石油公司國際海事論壇（OCIMF）和世界航運理事會（WORLD SHIPPING COUNCIL），發佈了深入的《船上網絡安全指南》。該《指南》在眾多的合規要素中，對IMO的網絡指南、風險評估和深度和廣度風險防禦進行了增補。

升級您的SMS，意味著理解並採納CRM原理，實施適當水平的網絡風險管理，建立網絡安全能力和對整體網絡彈性的持續監管，以預防、應對網絡事故並在發生網絡事故後恢復。

圖1 – NIST網絡安全框架

專注於CRM概念

IMO首先將海上網絡風險定義為一種衡量技術資產（例如，海上船舶上的系統）受到潛在情況或事件威脅，導致與航運相關的操作失靈或者出現安全故障的程度的度量。其中包括由於網絡事件而被破壞、丟失或破壞的信息或系統。

網絡風險管理表示識別、分析、評估並傳達與網絡相關的風險，並避免、轉化或者減輕這種風險至一個可接受的水平的程序。

IMO表明，有效的CRM應當考慮暴露或者利用網絡漏洞對信息技術（IT）系統和操作技術（OT）系統的安全影響。

健康、環保、安全和質量系統，包括SMS，是經過深思熟慮得出的成果，並且包含了恰當控制這些風險的政策和程序。控制與安全相關的網絡風險要求對現有的SMS有深刻的理解，並且網絡相關元素要融入安全系統並與之成為一個整體。

IMO的CRM模型源於被普遍採用的國家標準與技術研究所（NIST）的網絡安全框架。NIST框架為構建網絡安全計劃提供了清晰的過程模型，該模型參考了許多國際網絡最佳實踐，從確定您組織的關鍵技術一直到安全地從網絡事件中恢復過來，都可以參考。

IMO指南匯聚了支持有效海上安全的功能要素，或者僅是以最優實踐對CRM進行了補充：

- **識別**——定義人員在CRM中的角色/責任，識別混亂時對船舶運營構成危險的系統、財產、數據和能力。
- **保護**——實施風險控制流程和措施，制定應急計劃以防範網絡事件並確保船舶運營的連續性。
- **探測**——制定並實施必要的活動以及時發現網絡事件。
- **應對**——制定並實施活動和計劃，以提供因網絡事件而受損的運輸操作或服務所必需的彈性和恢復系統。
- **修復**——確定措施來備份和恢復受網絡事件影響的航運運營所必需的網絡系統。

因此，IMO建議對網絡風險採取一種具有彈性的風險管理方法，這種管理方法作為現有安全的自然延伸可以不斷進化。

建立網絡安全深度和廣度防禦

聯合企業集團在其網絡安全指南中強調的一個重要概念是「在深度和廣度上進行防禦」。在技術層面這個概念的含義分三個部分：知道必須實施的建立和保持約定水平的網絡安全的必要行動，知道在組織中誰對網絡安全管理負責，以及發展多層次的保護和探測手段。深度防禦是一種強有力的、一體的並且分層次的方法，包括程序、政策和技術等；廣度防禦意味著要覆蓋所有的脆弱的網絡技術，基本上是系統的系統方法。

聯合企業集團指出，用多層保護措施來保護關鍵系統和數據是非常重要的，這些措施考慮了人員、程序和技術在以下方面的作用：

- 增加檢測到網絡事件的可能性
- 增加IT系統和OT系統的保護信息、數據或可用性所需的精力和資源

風險控制	企業	船舶
風險評估	✓	✓
培訓與瞭解	✓	✓
供應商風險管理	✓	✓
應變管理	✓	✓
事件應對計劃	✓	
發展策略	✓	
網絡體系結構審核		✓
漏洞掃描		✓
登錄監管		✓
資產清單		✓

風險控制	企業	船舶
事件響應能力	✓	✓
風險管理程序	✓	
數據修復	✓	✓
訪問控制(IDAM)	✓	✓
郵件/網絡管理	✓	✓
漏洞管理		✓
補丁管理		✓
入侵檢測		✓
白名單		✓
惡意軟件管理		✓
實體安全		✓
可移動媒體		✓
資產管理		✓

圖 2 – ABS集團建議採用上述網絡安全控制措施以符合IMO要求

聯合企業集團強調，船載OT系統應該要求一項以上的技術和/或程序保護措施。通過深度和廣度的防禦方法，船舶所有人將考慮保護和檢測的組合，從根據船舶安全計劃的船舶物理安全到網絡保護和入侵檢測，再到定期與網絡安全控制有關的掃描/測試和程序性活動。

深度和廣度防禦指南要求您制定一套全面的安全措施，也稱為控制措施。

建立或增強網絡安全計劃的關鍵程序

開發CRM程序不僅僅涉及程序和政策，還在於技術的實施和管理。CRM主題和功能與多個SMS（ISM代碼）保持一致。每個組織的正確解決方案將有所不同。這會有共同的元素，但這取決於風險環境。聯合企業集團建議先進行風險評估，然後再制定攻略以開發適合其情況的能力

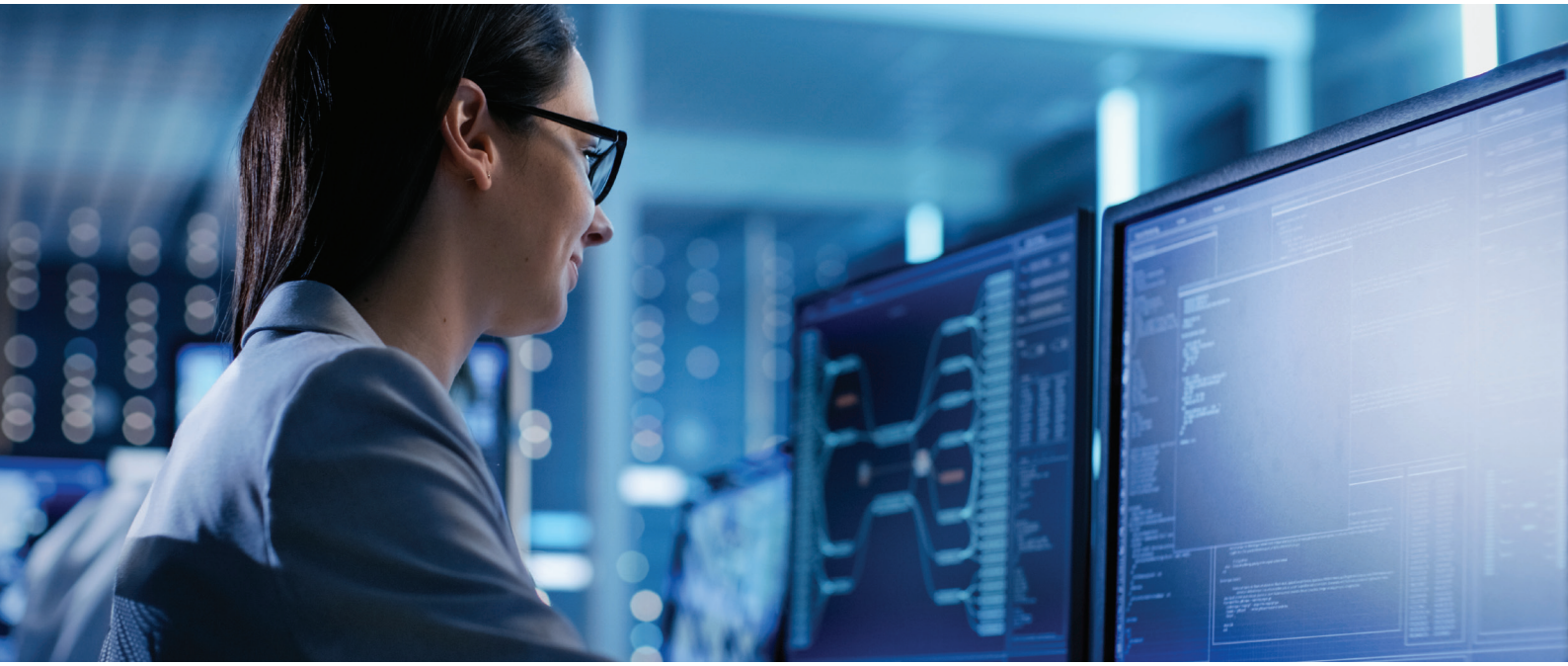
CRM 差距評估：針對IMO2021的要求，實施自我評估或第三方差距分析，此類評估或分析應專注於IMO和聯合企業集團對五個關鍵CRM基本原理的關注：識別、保護、探測、應對及修復

CRM-SMS線路圖：制定基於風險的策略以更新SMS，並在您的組織中建立CRM性能

CRM–SMS集成：通過集合您的CRM政策、過程和策略來開發程序中的保護措施以便更新SMS

安全措施實施：實施全面的網絡程序和性能，以滿足IMO准則

建立和維護網絡安全功能所需的大部分工作都集中在補救、緩解和管理關鍵技術中的漏洞。因此，首先要著重於確定網絡技術和漏洞，以便更好地瞭解為CRM的投資計劃和預算。



識別易受攻擊的船載網絡技術

據國際海事組織(IMO)表示,網絡技術(關鍵技術)已成為眾多系統運行和管理必不可少的系統,這些系統對於運輸的安全和保障以及海洋環境的保護至關重要。這些系統中的漏洞可能是由於設計,集成和維護實踐不充分(例如人為錯誤)或缺乏與組織內保護網絡系統相關的技術專業知識,能力或管理所致。

暴露於網絡風險中的易受攻擊的OT資產,包括但不限於:

- 橋梁導航系統
- 貨物裝卸和管理系統
- 推進和機械管理及動力控制系統
- 控制登陸系統
- 行政及船員的福利系統
- 交流系統

因為航運產業的科技在快速發展,且數字化已經成為市場現實,但網絡威脅的發展速度快於能力建設的速度。這種變化和不確定性不僅鼓勵網絡威脅參與者利用虛擬漏洞和漏洞,而且使船東和經營者僅通過技術標準來解決網絡風險變得困難。

"網絡彈性是現有安全管理機制的自然延伸。"

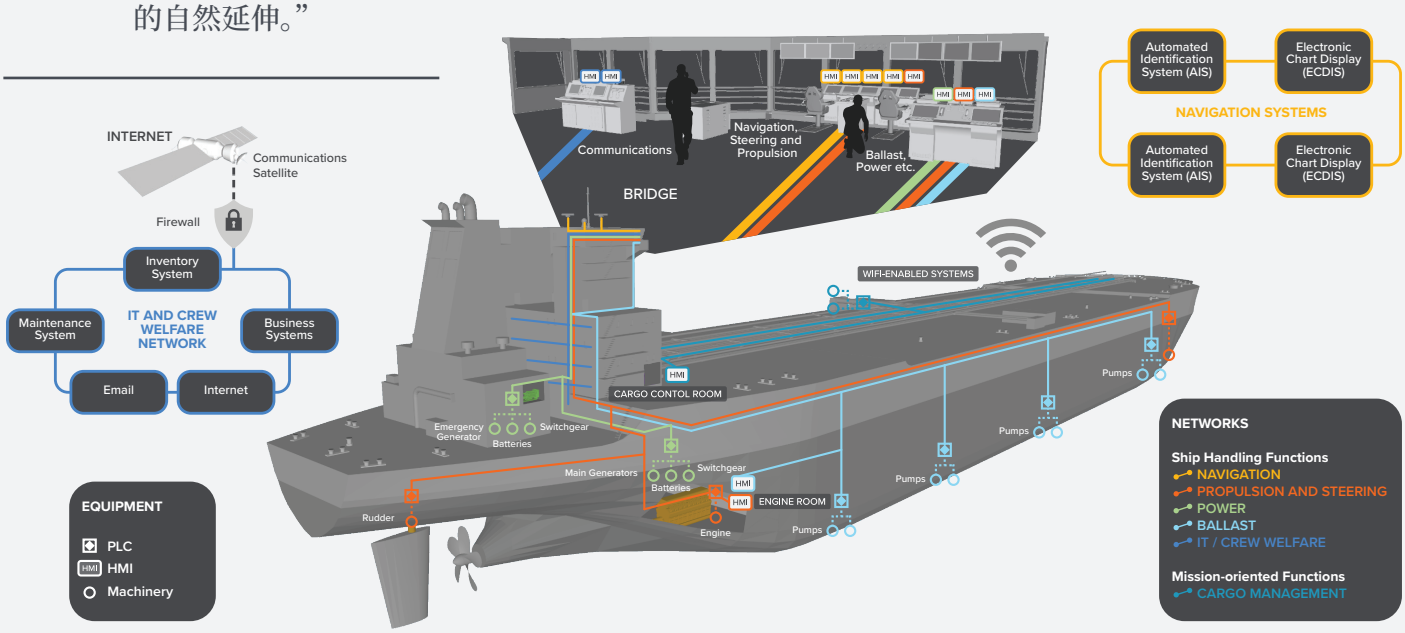


圖 3 –暴露於網絡風險中的易受攻擊的OT資產包括導航,推進,訪問控制,管理和通信系統。

關於網絡風險管理的實踐方法,聯合企業集團建議會員確定組織存在哪些威脅和漏洞,評估風險,制定保護和檢測措施,制定應急計劃以及(如果發生網絡事件)知道如何應對並從網絡安全事件中恢復。聯合企業集團表示,這種實踐方法是從深度和廣度上對網絡風險管理的防禦。

關於 ABS Group

ABS集團公司（www.abs-group.com）通過其運營子公司，提供數據驅動的風險和可靠性解決方案以及技術服務，以幫助客戶確認關鍵資產和運營的安全性、完整性、質量和環境效率。ABS集團總部位於得克薩斯州的Spring，在20多個國家/地區擁有1,000多名專業人員，為海洋和近海，石油，天然氣和化工，政府和工業部門提供服務。ABS集團是ABS（www.eagle.org）的子公司，ABS是世界領先的海洋和海洋工程船級社之一。

cyber@abs-group.com | www.abs-group.com/cyber

關於美國船東互保協會

1917年，美國船東互保協會（美保）於紐約成立，其總部位於紐約，是美國唯一一家互保協會。近年來，美保以其美國傳統，成功打造了業內數一數二的國際保險公司。美保的日常管理由位於紐約總部的船東索賠局負責。美保能夠為所有時區的會員提供當地服務，並能夠用多種語言與會員進行溝通。同時，美保在倫敦，比雷埃夫斯，香港，上海和休斯敦設有辦公室，此外，美保還設有全球通代網絡。美保是國際保賠協會集團的成員之一，國際保賠協會集團由13個協會組成，共同為世界90%的航運提供保賠險服務。關於美保的更多信息，請見如下網址 www.american-club.com.

保賠險

保護和賠償保險（通常簡稱為「保賠險」）為船東和租家在商業營運中提供第三方責任險；其典型的承保風險範圍包括貨損、污染、乘客或船員的傷病亡以及碼頭和其他設施的損壞。基於互惠互利的非營利原則，傳統的保賠險與船舶險同時使用，這與通常的海上保險形式不同，因為協會會員既是保險人又是被保險人。

info@american-club.com | www.american-club.com