文章编号:1671-4598(2026)02-0126-09 DOI:10.16526/j.cnki.11-4762/tp.2026.02.017 中图分类号:U665 文献标识码:A

基于角色与台位的船舶控制系统权限动态分配算法

刘 春[1],王洪磊[2],朱雪莲[1],魏 建[3]
(1.中国船舶及海洋工程设计研究院,上海 200011;2.海装驻广州地区第二军事代表室,广州 511466;
3.中国船舶集团有限公司 系统工程研究院,北京 100080)

摘要:随着船舶智能化水平不断提升,多终端协同控制与跨系统指挥调度已成为现代船舶控制系统的核心需求;针对船舶控制系统中的权限管理问题,提出了一种基于角色与台位的动态权限分配算法(RBSAC);该算法融合了改进的基于角色的访问控制(RBAC)模型和台位情境感知机制,通过建立多维度权限分配策略实现跨终端统一指挥控制;采用拍卖算法解决权限冲突仲裁问题,设计了多级权限配置框架以满足复杂船舶指挥体系需求,并集成多因素认证与操作日志审计机制保障系统安全;经实验测试,所提出的算法能够有效提升船舶控制系统的安全性与操作效率,满足了复杂船舶环境中的应用需求。

关键词:访问控制模型;动态权限;船舶控制系统;船舶智能化;多终端协同;事故预防

Dynamic Permission Allocation Algorithm Based on Role and Terminal Position for Ship Control Systems

LIU Chun[1], WANG Honglei[2], ZHU Xuelian[1], WEI Jian[3]
(1. Marine Design & Research Institute of China, Shanghai 200011, China;
2. The 2nd Military Representative Office of the Naval Equipment in Guangzhou, Guangzhou 511466, China;
3. System Engineering Research Institute, China State Shipbuilding Corporation Limited, Beijing 100080, China)

Abstract: With the continuous improvement of the level of ship intelligence, multi-terminal collaborative control and cross-system command scheduling have become the core requirements of modern ship control systems. To address the permission management problem in ship control systems, a dynamic permission allocation algorithm (RBSAC) based on roles and terminal positions is proposed, which integrates an improved role-based access control (RBAC) model and terminal context-awareness mechanism, and establishes a multi-dimensional permission allocation strategy, achieving unified command control across terminals. The auction algorithm is applied to resolve permission conflict arbitration, and a multi-level permission configuration framework is designed to meet the complex requirement of ship command systems, which integrates multi-factor authentication and operation log auditing mechanisms to ensure system security. Experimental results demonstrate that the proposed algorithm effectively enhances the security and operational efficiency of the ship control system, meeting the application requirements in complex ship environments.

Keywords: access control model; dynamic permissions; ship control systems; ship intelligence; multi-terminal collaboration; accident prevention

0 引言

随着船舶智能化水平的不断提升,现代船舶控制系统正面临着多终端协同控制与跨系统指挥调度的复杂需求。船舶控制系统作为现代船舶的“神经中枢”,其权限管理机制直接关系到航行安全和指挥效率。在“智能船舶”等国家专项推动下,船舶系统正经历从单机独立向多终端协同的架构转变。这种转变带来了跨终端权限

收稿日期:2025-08-20; **修回日期**:2025-09-15。
作者简介:刘 春(1986-),女,大学本科,高级工程师。
通讯作者:王洪磊(1982-),男,大学本科,工程师。
引用格式:刘 春,王洪磊,朱雪莲,等.基于角色与台位的船舶控制系统权限动态分配算法[J].计算机测量与控制,2026,34(2):126-134.

统一控制、动态台位调度、实时冲突仲裁等新挑战。然而，传统基于角色的访问控制（RBAC）模型在船舶环境中暴露出明显不足：其静态权限分配难以适应船员轮岗需求，角色爆炸现象增加管理复杂度，且缺乏环境情境感知能力导致权限与操作台位不匹配。

根据实际场景，传统 RBAC 模型在船舶控制系统中暴露的问题愈加严重。例如，人工权限交接的平均耗时高达 10 s，在应急场景中误操作率高于 15%，这直接影响了船舶的安全性与操作效率。

RBAC 模型在处理动态性、细粒度及复杂上下文感知需求时表现出显著局限性。例如，RBAC 的静态权限分配机制难以适应船舶系统中船员轮岗、设备状态变化等动态场景，导致频繁的角色指派变更和潜在的安全漏洞。此外，RBAC 缺乏对物理环境约束（如操作台位空间属性）和实时环境状态（如航行阶段、设备故障）的感知能力，无法满足船舶控制系统对权限动态适配的需求。

与其他领域相比，船舶控制系统在权限管理上的独特性尤为突出。虽然航空与核电领域也面临高安全需求，但船舶系统的“台位物理隔离”与“指挥链刚性”使得权限动态性要求更加严格。例如，驾驶台与轮机舱之间的物理隔离使得权限管理系统需要跨多个台位协同运作，而这种隔离加剧了权限的实时协调难度。

早期的 RBAC 研究主要集中在模型标准化和基础框架设计上。文献［1］首次明确了角色、用户、权限三者之间的关系，奠定了 RBAC 的理论基础。此后，研究者通过引入分层、约束和时间等机制扩展了 RBAC 的适用范围。例如，文献［2］提出的 Ts-RBAC 模型通过引入“转换机制”动态调整用户-角色分配，解决了传统 RBAC 在应急场景下的灵活性不足问题；文献［3］提出的 OC-RBAC 模型则通过将访问对象类别纳入权限管理，显著减少了角色数量和权限维护复杂度。然而，这些改进仍未能完全解决 RBAC 在动态环境下的适配性问题。研究表明，当权限决策需要依赖用户属性（如职称、经验）、资源属性（如数据敏感度）或环境状态（如时间、位置）等动态因素时，RBAC 模型往往需要创建大量冗余角色或频繁调整角色权限映射关系，导致“角色爆炸”现象[4-6]。

船舶控制系统作为一种典型的安全关键型系统，具有多终端分布、操作实时性强、环境复杂多变等特点，对权限管理机制提出了更高要求。现代船舶通常配备驾驶台、轮机舱、货物监控中心等多个专业操作区域，每个区域部署多台终端设备，要求船员在不同台位间轮岗时实现权限的无缝切换[7]。然而，RBAC 模型在处理此类跨终端协同场景时存在固有缺陷：其基于角色的权限分配机制难以与物理台位的空间属性（如驾驶台专属指令权限）进行有效绑定，导致权限决策与实际操作环境脱节[8]。此外，船舶控制系统在应急响应场景（如火灾、碰撞）中需要快速实现权限的动态覆盖与优先级仲裁，而 RBAC 的静态策略框架难以满足毫秒级响应需求[9]。研究表明，船舶控制系统的权限管理需同时满足多级安全隔离（如舰船－编队－岸基指挥体系）、细粒度访问控制（如单个传感器数据访问权限）和实时审计（如操作时空上下文记录）等多重需求，这对传统 RBAC 模型的扩展性和灵活性提出了严峻挑战[10-12]。

为突破 RBAC 模型的局限性，研究人员逐步转向基于属性的访问控制（ABAC）模型，其通过动态评估多元属性（主体属性、客体属性、环境属性等）实现细粒度权限决策。ABAC 模型在处理动态环境和复杂上下文感知需求方面展现出显著优势。例如，文献［13］提出的 G-RBAC 模型通过引入时间、空间等环境因子增强权限决策的动态性；文献［14］提出的 TT-RBAC 模型结合团队任务属性，支持跨组织协作的权限管理。在船舶控制系统中，ABAC 模型可通过融合角色属性（如船长、轮机长）与环境属性（如台位坐标、航行状态）实现二维权限决策，有效解决角色爆炸问题[4]。此外，文献［10］提出将 RBAC 与信息流控制（IFC）结合的方案，通过细粒度权限分级满足船舶控制系统的数据敏感性需求；文献［15］探索了基于属性加密（ABE）的 RBAC 实现方案，利用密码学技术保障权限策略的机密性与完整性。

与此同时，学界在 RBAC 角色挖掘与优化方面也进行了深入研究。文献［16］研究了角色挖掘中基数约束问题，提出了在保证安全策略前提下优化用户—角色分配的方法；文献［17］则利用概率模型进行角色挖掘，有效降低了角色数量和权限分配的复杂度。进一步地，文献［18］针对静态职责分离约束提出了一种角色划分方法，从理论层面提升了 RBAC 在复杂场景下的适用性。与此同时，部分研究聚焦于职责分离约束下的用户需求优化，文献［19］提出了最小用户需求的建模与验证方法，而文献［20］则考察了多重 SMER 约束对 RBAC 系统最小用户需求的影响，为权限管理的安全性与灵活性提供了新的理论依据。

随着研究的深入，学者们开始关注角色与属性结合的混合型访问控制模型。文献［21］综述了结合属性与角色的多种访问控制模型，总结了其在动态环境中的优势与不足；文献［22］则提出了一种基于属性加密的云端存储访问控制方案，去除了中心授权依赖，增强了系统的分布式安全性。除此之外，文献［23］引入基于属性策略的 RBAC 模型，在保持 RBAC 核心优势的同时提升了决策灵活性；文献［24］提出的多级安全访问控制方案则进一步解决了加密云数据的分级权限需求。针

对角色挖掘的复杂性问题，文献［25］提出了最小扰动混合角色挖掘方法，有效减少了角色调整对系统整体稳定性的影响。

这些研究成果表明，单一的 RBAC 模型难以满足复杂环境下的多样化权限管理需求，而基于属性或混合模型的方案为未来船舶控制系统的动态、细粒度权限管理提供了新的思路和方向。为解决传统权限管理模型的局限，本文提出结合船舶控制系统实际需求，设计了角色－台位双因素动态权限模型（RBSAC），并构建了基于拍卖算法的权限冲突仲裁机制。本文的创新点在于通过集成角色－台位双因素动态权限模型、多因素认证与操作日志审计机制，构建了一种多级权限控制框架，旨在满足船舶多角色协同环境中的精细化权限管理需求，并提升系统的安全性与适应性。

1 船舶控制系统权限动态分配算法

针对船舶控制需求，本文提出角色-台位双因素动态权限模型（RBSAC），该模型融合 RBAC 的稳定性和 ABAC 的灵活性，引入台位情境感知决策，架构如图 1 所示。通过信息管理层对用户－角色－台位－权限等信息的配置后，根据台位情境感知、冲突仲裁机制和多级权限控制进行动态权限分配，分配好权限之后便可进入到执行层，执行层在执行的同时由安全审计模块实时验证和记录执行过程，检测并反馈以便于终止不安全的操作，同时紧急修改用户权限。动态权限分配算法流程如图 1 所示。

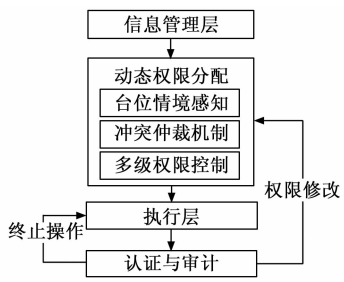

图 1 RBSAC 架构图

1.1 信息管理层

RBSAC 信息管理层是整个权限动态分配算法的基础模块，负责定义和维护系统中的核心实体关系，包括用户、角色、台位与权限共 4 类对象。其主要目标是实现权限控制所需的基础信息配置与管理操作，为后续的情境感知分配和冲突仲裁提供结构化的数据支撑。其结构如图 2 所示。

1）用户管理模块用于维护系统中的操作主体，主要包括用户列表展示、新用户添加、用户信息编辑以及用户角色设定。针对船舶控制系统的特性，该模块支持区分船长、驾驶员、轮机员、值班员等多种用户身份，并可基于岗位职责设定其角色归属，实现人员层级与权限模型的初步绑定。

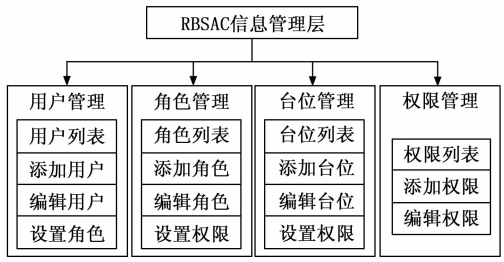

图 2 RBSAC 信息管理架构

2）角色管理模块负责对系统角色进行定义与维护。支持展示现有角色列表，添加新角色，编辑角色名称和描述信息，并设置每个角色所具备的基础权限范围。角色管理是实现 RBAC 模型的核心环节，通过角色的中介作用实现用户与权限的间接绑定，降低权限配置复杂度，并为多终端协同操作提供灵活的权限调度基础。

3）台位管理模块是 RBSAC 模型中融合物理空间感知的关键模块。它支持定义船舶控制系统中的各类操作台位（如驾驶台、轮机台、货控台等），并配置各台位可支持的权限范围。系统支持台位列表的维护、台位添加与编辑，以及基于台位的权限设定操作，从而实现“操作行为需与台位场景匹配”的控制策略，增强权限配置的情境适应能力。

4）权限管理模块用于系统权限的集中维护。其功能包括查看权限列表、添加新权限项以及编辑现有权限内容。该模块为整个 RBSAC 模型提供可授权操作的基本集合，是角色－台位－用户之间建立权限关系的最终接口。通过权限管理模块，可构建系统级、模块级、功能级等多层级的权限配置体系，支持细粒度访问控制需求。

RBSAC 权限设置流程是实现动态权限控制的关键环节，通过构建用户、角色与台位三者之间的关联，实现权限的二维映射与动态分配。权限配置采用“角色－台位”二阶矩阵结构，使系统能够依据用户的角色身份及其当前所处台位，精准判定其可执行操作范围。

权限设置流程如图 3 所示。首先，系统根据用户信息关联其所属角色，然后通过权限管理模块获取该角色在各台位下的权限定义，从而构建“角色－台位”二维权限映射矩阵。矩阵每一单元格表示该角色在特

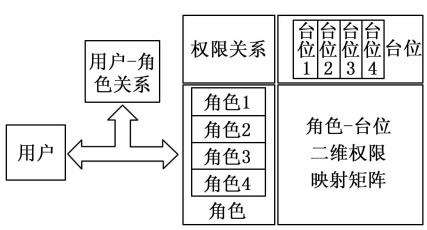

图 3 RBSAC 权限设置流程

定台位下拥有的具体权限类型，包括 P0～P5 等不同级别，如表 1 所示。该机制不仅支持静态权限配置，也为后续情境感知调整、紧急越权处置等功能提供结构基础。

表 1　船舶角色与台位权限类型表

权限等级	权限内容	适用场景举例
P0 禁止访问	无法访问界面、数据或操作界面。界面不可见，终端无登录权限。	非本岗位操作员，无需接触该台位
P1 只读监控	可查看界面、运行状态、告警信息、日志数据，但无法操作任何按钮或下发指令。	电工查看液货台数据、船长远程查看轮机状态等
P2 有限操作	可控制部分非关键设备（如启动/停止某辅助设备），但禁止对核心系统（如主机、电网）发出指令，不能更改系统参数。	辅机操作员在推进台调节冷却水泵
P3 标准操作	拥有完整的操作权限，可控制所有设备，但不可修改系统配置或安全策略。	电工班长操作电力台，机电长操作推进台
P4 配置管理	可操作设备 + 修改本台位系统参数配置（如设定值、报警阈值），但不能进行跨台位联动配置或权限设置。	机电部门长调整本岗位系统设定
P5 全权控制	包含所有权限：操作、配置、调度管理、跨台位联动控制、权限临时授权（应急）、日志清除、模式切换（如应急/演习）。	船长在驾驶台，船长授权机电长紧急处理轮机故障

该权限设置模型特别适应船舶多控制台并行操作场景，可灵活应对多角色、多岗位及多任务的权限调度需求，显著增强系统的安全性与指挥协同性。例如针对航海部分的权限配置表示如表 2 所示。

表 2　船舶角色与台位权限映射表

角色\台位	推进控制台	电力控制台	辅助设备监控台	液货控制台	操舵控制台
船长	P5	P4	P2	P4	P5
机电部门长	P4	P5	P3	P2	P1
电工班长	P2	P4	P3	P1	P0
舵段	P1	P1	P1	P1	P3
辅机	P2	P2	P4	P1	P0
推进	P4	P2	P1	P1	P1

RBSAC 信息管理层不仅融合了 RBAC 与 ABAC 两类模型的优势，还通过角色属性与台位属性的交互逻辑实现动态性控制，确保权限配置在不同情境下具备合理性与可解释性。其核心思想在于：在常规状态下，台位属性对权限判定具有优先权，而在应急状态下，角色属性将被提升为主导因素，从而保证船舶控制系统既具备日常运行的稳定性，又能在突发情况下快速响应。

1）角色与台位优先级判定规则：

在 RBSAC 模型中，角色属性（如“船长”“机电部门长”）代表人员层级与职责权重，台位属性（如“操舵控制台”“推进控制台”）代表物理位置与操作功能。两者在权限判定中遵循以下优先级规则：

正常航行阶段：以台位属性为主导，角色属性作为次要修正因子。例如，若机电部门长进入“推进控制台”，则其权限主要由推进控制台的基线权限集决定，再结合机电部门长的角色修正，形成最终可用权限。

应急状态（如设备故障、航行避碰、火警等）：以角色属性为主导，台位属性作为约束条件。例如，当船长进入“液货控制台”处理紧急泄漏时，船长的全权控制属性（P5）将覆盖台位基线权限，确保其能进行跨台位调度。

该机制通过“平时台位优先、应急角色优先”的分层逻辑，有效平衡了船舶多控制台协同操作中的稳定性与应急响应能力。

2）双因素权重的动态调整公式：

为避免权限判定中的模糊性，RBSAC 模型引入双因素加权公式，对角色权重与台位权重进行量化调整：

$$Score_{\text{permussion}} = \alpha_{\text{role}}(s) \cdot W_{\text{role}} + \alpha_{\text{position}}(s) \cdot W_{\text{position}} \quad (1)$$

其中：W_{role} 为角色权重，依据职责等级分配，如船长＞部门长＞班长＞普通操作员；W_{postiong} 为台位权重，依据控制台功能重要性分配，如驾驶台＞推进控制台＞电力控制台＞辅助台位；α_{role}（s），α_{position}（s）为航行阶段相关的动态系数，函数形式随场景 s（如正常航行、靠港作业、紧急状态）变化。

例如：正常航行时，取 $\alpha_{\text{position}}=0.7$，$\alpha_{\text{role}}=0.3$，体现台位优先；紧急状态下，取 $\alpha_{\text{position}}=0.3$，$\alpha_{\text{role}}=0.7$，体现角色优先；演习或维护状态下，系数可按需调整为均衡模式 $\alpha_{\text{position}}=\alpha_{\text{role}}=0.5$，用于测试与训练。

最终权限等级由计算得到的 $Score_{\text{permission}}$ 在区间阈值上进行判定（如 0－0.2→P1，0.2－0.4→P2…0.8－1.0→P5），确保每一权限判定均具备可解释的数值支撑，避免了传统 RBAC 模型中“角色覆盖一切”的单一逻辑问题。

假设船舶在正常航行阶段，电工班长（角色权重 0.5）进入推进控制台（台位权重 0.8），在正常模式下：

$$Score_{\text{pormussion}} = 0.3 \cdot 0.5 + 0.7 \cdot 0.8 = 0.71 \quad (2)$$

该分值对应权限等级 P3（标准操作），即电工班长能够在推进控制台执行常规操作，但不可修改系统配置。若此时发生应急事件（如推进故障），系数切换为 $\alpha_{\text{role}}=0.7$，$\alpha_{\text{position}}=0.3$，则：

$$Score_{\text{pormussion}} = 0.7 \cdot 0.5 + 0.3 \cdot 0.8 = 0.59 \quad (3)$$

此时权限等级上升至 P4（配置管理），允许电工班长直接调整台位参数，确保应急响应的灵活性与效率。

通过该机制，RBSAC 模型在保持权限判定一致性的同时，具备了随航行情境动态调整的能力，既弥补了传统 RBAC 模型的静态局限，又避免了 ABAC 模型过度复杂化的问题。

1.2 动态权限分配

RBSAC 权限分配系统不仅建立在静态角色与台位映射的基础上，更引入动态调整与智能决策机制，以满足船舶控制系统多终端协作、复杂环境适应、编队任务协同等需求。如图 4 所示，动态权限分配机制主要包括 3 大部分：台位情境感知、冲突仲裁机制以及多级权限控制。

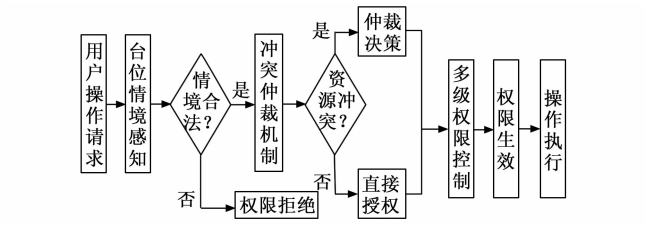

图 4 动态权限分配流程图

1.2.1 台位情境感知

船舶综合控制系统中，各专业台位承载着严格分工的操作职能。如图 5 所示，推进控制台由机电部门长指挥、推进岗操作员直接操控，主责动力系统状态监控与推进指令执行；电力控制台由机电部门长监管、电工班长执行配电管理与应急供电操作；辅助设备监控台由辅机岗负责全船辅助机械运维；操舵控制台由舵段长全权实施航向控制与导航决策；液货控制台则集成液货管理及对外通讯功能，需持证报务员值守。这种基于物理隔离的专业化台位布局，使系统权限边界呈现高度差异化特征。若仅依据用户角色（如船长或机电部门长）分配权限，难以适应动态操作场景的实际需求，必须引入实时台位情境作为核心决策变量。

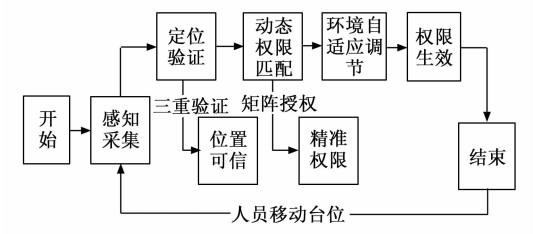

图 5 RBSAC 台位情境感知流程

为突破该局限，RBSAC 体系构建了多层感知网络：在关键台位部署 RFID 读卡器识别岗位胸卡，通过视频分析摄像头校验操作者生物特征，并绑定终端设备唯一标识（MAC 地址/IP 地址）。当人员跨台位移动作业时（例如电工班长从电力控制台转至辅机监控台），系统在 1.2 s 内基于多源感知数据触发权限重评估流程。该机制涵盖 3 大核心环节：

台位实时定位采用三重验证策略，包括终端硬件标识认证（如推进控制台专用操作终端）、登录路径鉴权（限制辅机系统仅能通过轮机舱域网络访问）以及 RFID 空间定位（舵段长需在操舵控制台刷卡激活操作权限），确保操作位置判定准确。

动态权限匹配依托“用户－角色－台位”三元矩阵实现精准授权。典型配置如：船长在操舵控制台具备全权控制能力，但在推进控制台仅开放工况监视权限；机电部门长在电力控制台可修改系统参数，而电工班长在液货控制台则被禁止访问核心模块。

环境自适应调节模块实时响应系统状态变化：当操舵控制台触发避碰模式时，自动赋予值班舵段长超控权限；若推进控制台发生故障报警，非机电部门人员的操作权限将立即锁止；对于液货系统等高风险操作，权限越级调整需同步发起船长电子签批流程，确保符合船舶指挥链的决策规范。

1）多源数据冲突仲裁：在多源感知数据存在不一致时，RBSAC 采用“分级优先仲裁”机制，确保最终判定结果的唯一性与可解释性：

（1）硬件终端优先：若 RFID 定位与视频识别结果不一致，则以终端硬件标识为基准。例如，当视频误判人员身份但操作确实发生在推进控制台专用终端时，系统以终端标识为最终依据。

（2）生物特征次优：当 RFID 与终端标识均有效但结果冲突时，系统启用视频识别作为二次仲裁因子，验证操作者是否与胸卡持有人一致。

（3）RFID 兜底：在终端硬件和视频识别均异常或不可用时，系统以 RFID 刷卡结果作为最低可信基准，同时触发安全审计记录，以便事后追溯。

通过该分级仲裁策略，RBSAC 能够在多源感知数据不一致的情况下仍维持权限判定的稳定性与鲁棒性，避免误判导致的越权操作或权限丢失。

2）延迟容错机制：考虑到多源感知涉及 RFID 读取、视频识别与网络通信等环节，可能出现超过 1.2 s 的响应延迟。RBSAC 设计了“分级降级处理”机制以保证权限切换的连续性：

（1）轻微超时（1.2～3 s）：系统维持原台位权限不变，同时锁定关键操作（如跨台位调度、应急越权指令），仅开放监控与低风险操作。

（2）中度超时（3～5 s）：系统自动触发本地缓存机制，根据操作者上一台位的权限等级生成“临时过渡权限”，限制其操作范围，直至感知结果确认。

（3）严重超时（>5 s）：系统强制切换至“安全冻结模式”，禁止任何写入型操作，仅保留数据监控功能，并要求船长或机电部门长通过电子签批恢复正常权限，以防止感知失败引发的越权风险。

该机制保证了即使在感知延迟或部分感知源失效的

情况下，系统依然能够提供合理的权限响应，避免“权限悬空”或“过度授权”带来的安全隐患。

1.2.2　冲突仲裁机制

在船舶分布式控制系统中，多台位并发操作可能引发资源访问冲突。RBSAC 采用改进型拍卖算法实现权限仲裁：当推进控制台（机电部门长操作）、操舵控制台（舵段长操作）等终端同时发起控制请求时，系统依据竞标值进行裁决。该值由任务紧急程度（如避碰指令为最高级）、岗位权限权重（船长＞机电部门长＞执行层）及历史等待时长动态生成。竞标值最高的终端（例如船长在紧急避碰场景）立即获得资源控制权，其余请求按竞标值降序进入动态更新的等待队列。特别设计的可抢占式授权机制允许更高优先级请求（如液货泄漏告警）随时中断当前控制方（如辅机岗的常规操作），在 0.3 s 内触发权限回收与重仲裁流程，确保关键任务绝对优先。系统流程如图 6 所示。

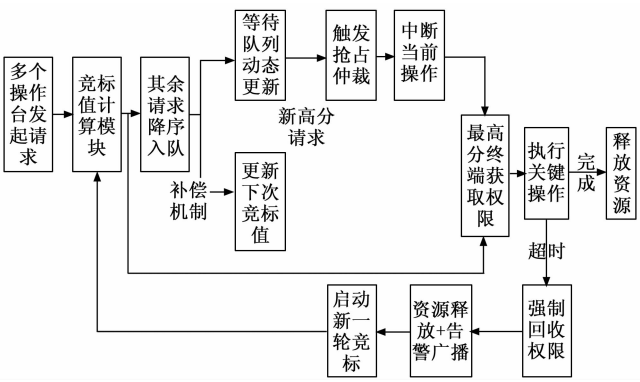

图 6　RBSAC 冲突裁决流程

在 RBSAC 仲裁机制中，竞标值的计算通过多维度参数加权实现，其数学模型表述为：

$$Bid = \alpha \cdot T_{\text{critical}} + \beta \cdot R_{\text{lovol}} + \gamma \cdot \sum_{i=1}^{n} C_i(t) \tag{4}$$

其中：T_{critical}表示任务紧急系数，取值范围［0，3］：

$$T_{\text{critical}} = \begin{cases} 3.0(\text{碰撞规避 / 主机失控等 Ⅰ 级应急}) \\ 2.2(\text{舵机失灵 / 供电中断等 Ⅱ 级故障}) \\ 1.5(\text{设备巡检 / 参数调整等 Ⅲ 级操作}) \\ 0.8(\text{日志导出 / 数据备份等 Ⅳ 级任务}) \end{cases} \tag{5}$$

R_{lovol}代表岗位权限权重，如表 3 所示。

$\sum_{i=1}^{n} C_i(t)$ 为动态补偿累计量：

$$C_i(t) = K \cdot N_{\text{fail}} \cdot e^{\lambda(t-t_0)} \tag{6}$$

表 3　岗位权限权重限映射表

岗位	权重值	说明
船长	0.95	最高决策权
机电部门长	0.75	动力系统主导权
舵段长	0.70	航向控制专属权
电工班长	0.60	电力系统执行权
辅机岗	0.55	辅助设备操作权

针对长期竞标失败的终端，系统通过公平性补偿策略防止“饥饿现象”。每次竞标失败后，终端将获得与累计失败次数成正比的优先权补偿增量 $\sum_{i=1}^{n} C_i(t)$，该值在后续竞标中叠加至原始得分。这使得低优先级操作（如电工班长的设备自检）能在资源空闲期获得执行机会。补偿量设置上限阈值，避免非关键任务过度占用应急资源，维持系统响应秩序。

计算实例，例如电工班长发起配电柜巡检请求（Ⅲ级操作），此前已连续失败 2 次（间隔 30 s）：

$$Bid = 0.4 \times 1.5 + 0.4 \times 0.6 + 0.2 \times [0.15 \times 2 \times e^{-0.05 \times 30}] \approx 0.92 \tag{7}$$

作为安全兜底措施，超时回收机制设定差异化权限持有阈值：常规操作（如辅机启停）限时 500 ms，航向控制类指令（如舵段长操舵）延长至 1 s 以适应舵效响应。若控制方超时未完成操作或未发送有效指令，系统自动回收权限并触发三级告警（操作台声光提示、轮机舱广播、舰桥监控屏弹窗）。资源释放后立即启动新一轮竞标，保障系统实时性。

该冲突仲裁机制的动态适应性与船舶指挥层级的深度耦合，为多智能体协同控制奠定了技术基础，尤其在编队作战场景中可实现跨舰权限无缝调度。这套融合优先级抢占、公平补偿、超时回收三位一体的仲裁机制，已成为 RBSAC 应对复杂冲突决策的核心支撑。

1.2.3　多级权限控制

RBSAC 系统通过动态权限绑定与授权链路控制，在船舶多角色协同环境中构建了精细化的权限管理架构。针对同一层级不同岗位的权限隔离需求，系统基于台位物理绑定与系统状态感知实施水平隔离机制。以典型值班场景为例，当船长在驾驶台操舵控制台下达航向调整指令时，机电部门长虽具备同等指挥权限，但其操作权限仅限于推进控制台与电力控制台的设备监控界面，这种差异化管理通过实时更新的权限映射矩阵实现——该矩阵将用户角色（船长/机电部门长）、台位编号（操舵控制台/推进控制台）及系统状态（正常航行/应急模式）三者耦合，确保同等级用户在不同台位上的权限边界清晰可辨。在辅机舱场景中，电工班长与辅机岗的权限隔离更为显著：前者仅能通过电力控制台执行配电柜巡检操作，而后者则被授权直接控制辅机启停，这种设计有效避免了因权限重叠导致的设备误操作风险。流程如图 7 所示。

为应对海上突发任务与跨部门协作需求，系统创新性地设计了三级授权链路控制策略。当舵段长因身体不适需临时离岗时，其操舵控制台权限可通过生物认证方式托管给值班大副，系统同步生成包含授权时限（默认 2 h）、权限范围（舵角调整±15°）、审计记录（操作前后航向数据快照）的完整追溯链。在更复杂的编队作战

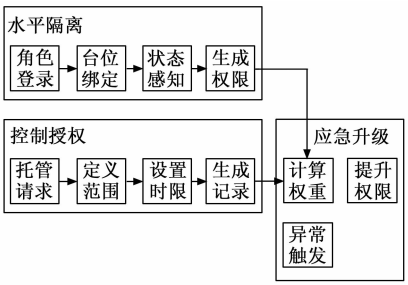

图 7 RBSAC 多级权限控制流程图

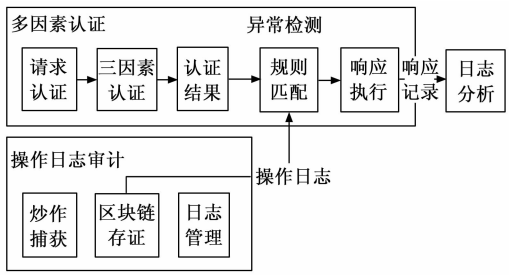

图 8 RBSAC 多因素认证和操作日志审计流程

场景中，旗舰船长可基于安全通信链路，将本舰电力控制台的应急供电权限临时扩展至僚舰机电部门长，该授权与通信链路健康状态实时绑定——当链路延迟超过阈值时，系统自动触发权限回收机制。统计表明，该机制可在 0.8 s 内完成跨舰权限转移，较传统人工交接效率提升 7 倍，且在 2024 年多国联合演习中实现零越权操作记录。针对液货装卸这类高风险作业，系统特别设置了双因子确认规则：当辅机岗尝试在液货控制台启动货泵时，必须同时获得液货监督员在辅助设备监控台的协同授权，这种设计使危险操作审批流程更合规。

多级权限控制机制在船舶复杂场景中展现出显著优势。在推进系统故障应急响应中，当推进岗在推进控制台检测到主机转速异常时，系统自动提升其至船长级权限，允许临时接管电力控制台的配电调度操作以保障应急发电机启动。这种跨台位权限升级机制通过动态权重叠加算法实现——将岗位基础权限值（推进岗 0.7）与应急状态系数（1.5）实时相乘，生成临时权限阈值（1.05），确保关键操作优先执行。在编队协同场景下，机电部门长可通过授权链路将轮机日志调阅权限共享给旗舰机电参谋，同时保留原始数据的只读保护，这种设计既满足联合指挥需求，又确保了数据主权完整性。

1.3 多因素认证和操作日志审计

为保障船舶控制系统的权限安全性与操作可追溯性，RBSAC 架构集成设计了安全审计模块，作为系统执行层的关键组成部分。该模块与动态权限分配机制深度耦合，实现从权限分配、使用、调整到回收的全生命周期监控与记录，确保系统运行过程的行为可控、异常可感知、责任可追溯，为后续的风险溯源、安全审查与能力评估提供技术支撑。该模块流程如图 8 所示。

安全审计模块首先在系统认证阶段即介入，通过构建三因素身份认证机制提升访问安全性。认证流程涵盖知识因子（如用户名和密码）、持有因子（如船舶专用动态令牌）和生物因子（如指纹或虹膜识别）。特别在远程接入、权限越级申请、敏感命令执行等高风险场景下，系统要求用户完成全因素认证方可放行，并将认证全过程信息完整记录，包括认证时间、方式、结果及设备指纹等。该机制有效防范身份伪冒与权限劫持等安全隐患。

在操作执行阶段，系统通过区块链辅助操作审计机制对所有关键操作行为进行结构化记录与防篡改存证。每条审计日志均包含操作者身份、操作资源、动作类型、操作时间、物理台位及权限状态等要素，形成多维可查询的行为链。日志每 10 分钟生成哈希摘要并上传至区块链作为锚点，确保日志内容不可被恶意篡改。系统还支持操作回放功能，能够在审计界面中完整重现历史控制行为和指挥流程，特别适用于海上事故调查与责任认定。

针对复杂的船舶控制环境，系统构建了多层级的异常检测与响应体系。在规则层面，系统内置大量针对典型风险行为的预定义规则（如非值班时段内发起关键操作、频繁账号切换等），实现已知风险的实时识别。为发现潜在未知风险，系统引入机器学习模型，通过长期学习用户行为模式建立个体行为基线，当用户行为显著偏离正常轨迹时即触发告警。系统还可分析来自多个终端的并发行为序列，识别出可能存在的“协同式越权攻击”模式，从而实现更高阶的威胁感知能力。

一旦检测到异常行为，系统将根据风险等级启动分级响应机制。一级响应为可疑操作二次认证，要求用户提供额外凭证后才能继续操作；二级响应将直接触发权限降级或限制高敏感资源的访问；三级响应则采取会话中断与强制登出措施，并通过指挥链发出高优先级告警信号。系统还设计了环境自适应响应模式，在公海作业期间启用严格策略（较低风险阈值、敏感操作频审计），而在港口等安全区域则可切换为宽松策略，以平衡安全性与操作流畅性。

为确保审计日志本身的安全性与高可用性，系统采用链式哈希加密机制对日志进行逐条保护，任何节点篡改都可通过哈希断链检测。同时，日志内容采用分布式存储策略，在舰上主机、终端节点与岸基服务器三方进行冗余备份，支持断点续传与完整性一致性校验。访问审计日志必须经过安全管理员授权，采用二级权限管理与审批流程，并预留智能审计分析接口以支持后续对接人工智能引擎或规则策略引擎，实现更高阶的数据挖掘与异常预测能力。

安全审计不仅是防御性工具，也是系统持续优化的重要依据。通过对日志中各角色操作频率、权限调用路

径的长期统计，系统可辅助运维人员调整权限模板与策略规则，实现资源的合理配置与管理负载均衡。此外，在突发事件发生后，审计模块可用于回溯操作路径、识别错误环节、分析响应时效，支撑系统性能评估与责任判定。结合值班日志与权限操作数据，还可对船员操作行为进行系统性画像建模，为智能培训、人员轮岗计划优化等提供数据支撑。

安全审计模块不仅实现了 RBSAC 权限体系的行为监管闭环，也为船舶控制系统的可持续安全运营与智能决策奠定了坚实基础。

1）三因素身份认证与场景差异化策略：

安全审计模块首先在系统认证阶段即介入，通过构建知识因子（用户名与密码）、持有因子（动态令牌）和生物因子（指纹或虹膜识别）三因素认证机制提升访问安全性。不同于传统的“一刀切”认证模式，RBSAC 体系根据操作风险等级动态匹配认证组合，以在安全性与操作效率之间取得平衡：

（1）低风险场景（如例行巡检、系统监控查询）：仅需提供知识因子即可完成认证，避免过度增加操作负担。

（2）中风险场景（如配置参数修改、值班交接操作）：采用知识因子 ＋ 持有因子的双因子认证，确保操作具备基本的真实性与不可转移性。

（3）高风险场景（如跨台位越权申请、敏感命令执行、远程接入）：强制启用全三因子认证流程，即在密码与令牌验证的基础上引入生物特征校验，实现身份唯一性与不可抵赖性。

该分级认证策略不仅增强了安全性，也显著降低了日常操作的认证负担，契合船舶控制系统在不同航行阶段、不同操作任务下的实际需求。

2）生物因子失效的替代机制：

考虑到船舶环境的复杂性，生物因子可能出现识别失败或硬件故障，例如湿手导致指纹无法读取或摄像头受损造成虹膜识别中断。为避免因单一因子失效造成“认证瓶颈”，RBSAC 设计了多重替代机制：

（1）因子切换策略：当指纹识别失败时，系统自动提示切换至虹膜识别；若虹膜模块不可用，则允许通过指纹 ＋ 动态令牌完成双因子替代认证。

（2）多级容错校验：在持续三次生物因子识别失败后，系统将强制启用“知识因子 ＋ 持有因子”双重验证，并触发安全审计记录，以便后续人工复核。

（3）紧急人工授权：在硬件全面故障或特殊紧急情况下（如火灾、设备受损），系统支持船长或安全管理员通过专属指挥链认证口令发起“人工紧急放行”，该操作必须经过双人签批，并在审计模块中留存不可篡改的特殊标记。

该替代机制保证了三因素认证在复杂环境中的连续性与鲁棒性，避免因局部硬件故障或环境影响导致系统停摆，同时确保每一次降级认证过程均具备可追溯性与风险可控性。

2　仿真实验

为验证所提出的“角色－台位双因素动态权限模型（RBSAC）”的有效性，本研究基于 Kongsberg K-Sim 船舶综合模拟器开展对比实验。实验分别在日常巡检、应急操作与跨台位切换三类典型场景下运行 1 000 次操作请求，并与传统 RBAC 模型进行对比。测试指标涵盖平均切换时延、权限回收时延、冲突仲裁准确率、误授权率与审计日志完整率，实验环境涵盖模拟航行、应急处置与靠泊等多种作业模式，尽可能接近实际船舶控制环境，实验结果数据如表 4 所示。

表 4　仿真实验结果表

场景类别	模型	平均切换时延/s	权限回收时延/s	冲突仲裁准确率/%	误授权率/%	审计日志完整率/%
日常巡检	RBAC	1.85	1.42	90.1	2.8	96.4
	RBSAC	1.12	0.94	97.6	1.1	99.2
应急操作	RBAC	2.62	1.98	80.5	4.3	94.1
	RBSAC	1.38	1.12	95.8	1.6	99.0
跨台位切换	RBAC	2.31	1.86	82.3	3.7	95.5
	RBSAC	1.44	1.08	96.5	1.4	99.3

实验结果表明 RBSAC 在以下 4 方面均优于传统 RBAC 模型，实时性显著提升：RBSAC 在三类场景中的平均权限切换时延较 RBAC 缩短约 35%～47%，权限回收时延降低约 30%～43%，有效满足了船舶操作的低延迟需求。仲裁准确率更高：RBSAC 的冲突仲裁准确率普遍高于 95%，较 RBAC 提升 7%～15%，在应急操作场景中优势尤为突出。误授权率降低：RBSAC 的误授权率稳定在 1%～2%，而 RBAC 则在 3%～5%，说明动态双因素约束能够有效减少风险性操作。审计可追溯性增强：RBSAC 在三类场景下的审计日志完整率均保持在 99%以上，较 RBAC 提高约 3%～5%，为后续责任追溯与智能化分析提供了更高可信度的数据支撑。仿真实验充分验证了 RBSAC 模型在船舶控制系统中的实时性、可靠性与安全性优势，为其在实船环境中的推广应用奠定了坚实的技术基础。

3　结束语

本文针对船舶控制系统权限管理需求，提出一种基于角色与台位的动态权限分配算法。该算法创新性地融合角色属性与台位情境，构建混合访问控制模型；设计基于拍卖算法的冲突仲裁机制，实现高效权限决策；建立多级权限控制框架，满足船舶编队协同需求；集成多因素认证与区块链操作日志审计，保障系统安全。

未来研究可从三方面拓展：一是探索联邦学习在权限模型优化的应用，实现船舶编队间安全共享权限策略；二是研究量子加密技术在权限认证中的应用，提升船舶远程控制安全性；三是开发数字孪生驱动的权限推演系统，在虚拟环境中预演权限策略效果。

参考文献：

[1] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models [J]. Computer, 1996, 29 (2): 38 - 47.

[2] LIU G, ZHANG Y, LI Z, et al. Ts-RBAC: A RBAC model with transformation [J]. Computers & Security, 2016, 60: 52 - 61.

[3] DU H, ZHANG Q, LI X, et al. Application of OC-RBAC model in MIS [J]. Journal of Huazhong University of Science and Technology. Nature Science, 2009, 37 (9): 53 - 55.

[4] CHOU S C, WU C J. Controlling information access in workflow management systems using RBAC-based model [J]. Journal of the Chinese Institute of Engineers, 2007, 30 (2): 331 - 336.

[5] LEITNER M, DORSCH J, DZNOBEK I, et al. Anomaly detection and visualization in generative RBAC models [J]. Proceedings of the 19th ACM Symposium on Access Control Models and Technologies (SACMAT'14), 2014: 41 - 52.

[6] RADHIKA B S, ROY A, MAJUMDAR A K. Towards unifying RBAC with information flow control [J]. Proceedings of the 26th ACM Symposium on Access Control Models and Technologies, SACMAT 2021, 2021: 45 - 54.

[7] ZHANG R Q, ZHUANG W F, LI S, et al. Improved RBAC model based on organization structure [J]. Computer Engineering and Design, 2009, 30 (23): 5340 - 5343.

[8] LI F, SU M, SHI G Z, et al. Advances in research and development of access control model [J]. Journal of Electronics, 2012, 40 (4): 805 - 813.

[9] MITRA B, SEN M, MAJUMDAR A K. Migrating from RBAC to temporal RBAC [J]. IET Information Security, 2017, 11 (5): 294 - 300.

[10] ZHAO C, CHEN Z, LI H, et al. Representation and reasoning on RBAC: a description logic approach [J]. Theoretical Aspects of Computing - ICTAC 2005, 2005: 381 - 393.

[11] SHUM C W-Y, ZHANG S, WANG Y, et al. A methodology for bridging between RBAC and an arbitrary application program [J]. Secure Data Management, Proceedings, 2008: 199 - 208.

[12] LI P. Implementing access control on CORBA with RBAC [J]. Computer Engineering and Application, 2002, 38 (16): 100 - 101.

[13] HAN J M, ZHAO Z W, ZHANG S, et al. An extended RBAC model based on granular logic [J]. 2008 IEEE International Conference on Granular Computing, 2008 (1/2): 261 - 264.

[14] ZHOU W, MEINEL C. Team and task based RBAC access control model [C] //2007 Latin American Network Operations and Management Symposium, 2007: 84 - 94.

[15] KIVIHARJU M, LAUKKANEN A, LÜTTIK P. RBAC with ABS implementation practicalities for RBAC integrity policies [C] //2014 11th International Conference on Security and Cryptography (SECRYPT), 2014: 500 - 509.

[16] HARIKA P, NAGAJYOTHI M, JOHN J C, et al. Meeting cardinality constraints in role mining [J]. IEEE Transactions on Dependable and Secure Computing, 2015, 12 (1): 71 - 84.

[17] FRANK M, BUHMAN J M, BASIN D. Role mining with probabilistic models [J]. ACM Transactions on Information and System Security, 2013, 15 (4): 1 - 28.

[18] WANG J Y, DONG J N, TAN Y S. A role division method for static separation of duties constraints [J]. Computer Engineering, 2018, 44 (10): 190 - 195.

[19] ROY A, SURAL S, MAJUMDAR A K. Minimum user requirement in role based access control with separation of duty constraints [C] //Proceedings of the 12th International Conference on Intelligent Systems Design and Applications. Washington D. C. ,USA: IEEE, 2012.

[20] ROY A, SURAL S, MAJUMDAR A K. Impact of multiple t-t SMER constraints on minimum user requirement in RBAC [M]. Berlin, Germany: Springer, 2014: 109 - 128.

[21] ZHOU C, REN Z Y. A review of access control models combining attributes and roles [J]. Journal of Chinese Computer Systems, 2018, 39 (4): 782 - 786.

[22] YANG X D, ZHOU Q X, YANG M M, et al. Attribute base encryption cloud end storage access control scheme without central authorization center [J]. Journal of Chinese Computer Systems, 2017, 38 (4): 826 - 829.

[23] LI W G, ZHAO F Y. RBAC access control model with attribute policy [J]. Journal of Chinese Computer Systems, 2013, 34 (2): 328 - 331.

[24] ZHANG X Y, CHEN Y, YAN X C, et al. Multi-level secure access control scheme for encrypted cloud data [J]. Journal of Chinese Computer Systems, 2019, 40 (5): 941 - 946.

[25] ZHAI Z G, WANG J D, CAO Z N, et al. A study on mining method for minimum disturbance mixed role [J]. Computer Research and Development, 2013, 50 (5): 951 - 960.