doi: 10.7690/bgzdh.2025.06.009

基于区块链技术的往来函证数字化平台

贾　凤，余　宏，周　晶，牟　慧，孙广文，董启春
（国网山东省电力公司物资公司，济南 250001）

摘要：针对往来函证容易丢失或被篡改，流转过程中存在很大的安全风险问题，设计基于区块链技术的往来函证数字化平台。通过平台基础层、业务层以及应用管理层设计平台 3 层架构，在平台架构下，确认实体关系和数据库表，完成平台数据库设计；基于区块链技术设计平台业务单元：电子函证生成单元、函证分类归档单元、函证区块存储单元、平台安全防护单元，实施平台应用测试，结果表明：基于区块链技术平台的重叠系数和安全性指数均达到相对最大值，证明了平台的功能性。

关键词：区块链技术；往来函证；数字化平台；应用测试
中图分类号：TP309　　**文献标志码：**A

Digital Platform for Correspondence Based on Blockchain Technology

Jia Feng, Yu Hong, Zhou Jing, Mou Hui, Sun Guangwen, Dong Qichun
(*Material Company*, *State Grid Shandong Electric Power Company*, *Ji'nan* 250001, *China*)

Abstract: In order to solve the problem that correspondences are easy to be lost or tampered with, and there are great security risks in the process of circulation, a digital platform for correspondences based on blockchain technology is designed. The three-layer architecture of the platform is designed through the platform basic layer, the business layer and the application management layer. Under the platform architecture, the entity relationship and the database table are confirmed, and the platform database design is completed. The platform business units are designed based on the blockchain technology: the electronic correspondence generation unit, the correspondence classification and filing unit, the correspondence block storage unit, and the platform security protection unit. The application test of the platform shows that the overlap coefficient and safety index of the platform based on blockchain technology reach the relative maximum, which proves the functionality of the platform.

Keywords: blockchain technology; correspondence; digital platform; application testing

0　引言

电力公司承担了全国各地居民的供电任务，因此体系庞大，每部分都非常重要。电力物资公司就是旗下的一个重要分支，主要工作是负责电力物资采购，包括各种电气设备、电工产品、金属材料以及技术服务等。在这种情况下，该公司每天的往来流水金额也十分庞大。为理清账目，确保财政的准确性，预防舞弊或错误导致的特别风险，电力物资公司会定期进行内部审计。审计工作质量全部客观依赖所获取到的审计证据，其中往来函证就是证据中最为重要的一部分，是审计底稿编写的基础材料[1]。基于此，往来函证的管理十分重要。当下，企业的函证多以手工办理的纸质形式呈现。该形式的函证更加直观，但也存在很大的弊端。函证一般会经过十多道环节的流转，在该过程中存在很大的安全风险，致使数据或者信息很容易丢失或者被篡改，从而影响了函证的可靠性[2]。面对这种情况，随着信息技术的发展，函证形式开始发生转变，数字化电子函证出现并开始逐渐取代纸质函证。电子函证相比较纸质函证来说，存储和调取更加方便，极大减少了函证工作流程的周期时长。基于上述背景，设计往来函证数字化平台具有重要的现实意义。数字化平台由于核心技术的不同，具有不同的设计方案。例如，基于 RFID 技术的平台，该平台可以利用 RFID 标签实现对目标的全过程追踪，以保证目标对象在流转过程中的安全性，避免资产丢失[3]。还有基于身份认证和加密技术的平台，其原理是通过对访问者身份进行验证，对目标数据进行加密，以保证其安全[4]。上述 2 个平台的安全性指数较小，致使平台的安全性较低，不能保证函证数据的安全。

区块链技术具有很强的存在性、完整性及不可篡改。针对上述平台存在的问题，笔者结合区块链

收稿日期：2024-08-11；**修回日期：**2024-09-20
基金项目：国网山东电力物资公司项目(710603220007)
第一作者：贾　凤(1988—)，女，河北人，硕士。

技术，设计往来函证数字化平台。将区块链技术应用到本平台设计中，可以实现函证数据资料的分布式存储，从而保证函证数据的安全。

1 往来函证数字化平台设计

往来函证是重要的财务信息，对于识别财务报表错误与舞弊行为至关重要[5]；为此，设计往来函证数字化平台。区块链技术具有完整性、存在性以及不可篡改性。将其应用到本平台中，能够将函证数据分布式存储在不同的节点上，在保证函证数据的安全的同时，也实现了函证的数字化管理，方便了函证数据的流转与调取。

1.1 平台架构设计

架构是平台的基础框架，是平台设计的第一个环节。通过该环节设计，为整个平台的构建提供了重要的指导[6]。参考 B/S 设计的基于区块链技术的往来函证数字化平台主要分为 3 层，即平台基础层、平台业务层以及平台应用管理层，具体如下：

1) 平台基础层：顾名思义，是整个平台的“地基”。在该层中包含了大量的服务器节点，一个节点代表一个参与方身份，如企业、银行、监管机构等。因此，主要负责各节点间及服务器节点间的管理。除此之外，还负责封装了各个节点的分布式网络、终端以及各类资源等[7]。

2) 平台业务层：是整个平台的核心层，包含了各种业务逻辑程序，负责处理函证的生成、审核、分类归档、加密保存、安全防护等[8]。

3) 平台应用管理层：是整个平台的最顶层，是使用方进入平台的窗口，负责与平台之间信息交互以及操作指令的输入与执行结果的展示[9]。

1.2 平台数据库设计

数据库是函证数据存储的地方，其设计主要包括实体关系设计和数据库表设计 2 个部分。

1) 实体关系设计。

实体关系描述了围绕函证，各个参与方之间的相互逻辑关系，是数据模型建立的基础，其中审计单位、被审计单位、监管机构等属性与询证单位相同[10]。图 1 为本平台数据库的实体关系。

2) 数据库表设计。

数据库表中描述了数据库是由哪些性质的信息所组成，在数据库设计中不可或缺[11]。设计的部分数据库如表 1 所示。

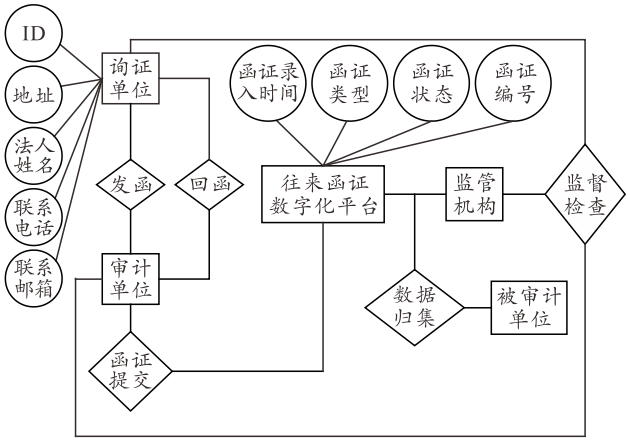

图 1 平台数据库的实体关系

表 1 数据库表(部分)

描述	字段名	数据类型	长度
企业	Company	Varchar	42
企业 ID	Certificate ID	Varchar	20
地址	Address	Varchar	80
消息内容	Message	Varchar	500
法人姓名	Legal Name	Varchar	30
电话	Tel1	Varchar	18
邮箱	Email1	Varchar	18
用户权限	Authoritytype	Int	15
函证编号	Confirmation ID	Varchar	20
函证录入时间	Conf Entry Time	Datetime	10
函证类型	Confirmation Tpye	Int	10
函证状态	Conf Cndition	Int	10
被审计单位名称	Audit Unit Name	Varchar	50
审计单位名称	Audit Name	Varchar	30
监管机构	Regulators	Varchar	50

1.3 基于区块链技术的平台业务单元设计

平台业务单元也叫平台功能模块，是平台设计中的核心环节，属于平台业务层，在该层中，根据需求选择不同的单元，完成不同的处理[12]。平台业务单元主要包括 4 个，即电子函证生成单元、函证分类归档单元、函证区块存储单元、平台安全防护单元，具体分析如下。

1.3.1 电子函证生成单元

传统函证大多是纸质版的，为实现其数字化，生成电子函证。针对以往已经存在的纸质函证，可以利用扫描仪扫描成电子版的形式；针对当下正在办理中的函证，可以直接登录平台，直接生成电子版函证[13]。生成过程如下：

步骤 1：审计单位与电力物资公司通过智能合约在区块链上签署《业务约定书》，并在节点上索取被询证单位、会计师事务所等企业信息。生成对应的电子版哈希值上链；同时，与被询证对象签署相

关的协议信息。

步骤 2：确定函证类型并申请。

步骤 3：审计单位根据《业务约定书》从链上选择本次询证的要素，根据财政部统一模板生成对应的电子询证函并从链上通过分布式网络进行发函。

步骤 4：被询证对象接收询证函。

步骤 5：被询证对象在线检查电子询证函内容。

步骤 6：判断其上信息是否属实。

属实，签订确认书并将函证相关数据嵌入审计单位发送的电子询证函中，完成在线填写询证函；不属实，拒绝签订属实确认书并回函给审计单位要求进行更正，然后回到步骤 2，重新生成对应的电子询证函并发函。

步骤 7：通过公钥对函证相关数据进行验签并加盖签章。

步骤 8：被询证对象在链上发布回函请求。

步骤 9：审计单位同意请求并接收回函。

步骤 10：区块链网络通过共识机制推选出记账节点。

步骤 11：记账节点将函证打包生成区块并向全网广播。

步骤 12：基于哈希值和时间戳验证、延迟确认等机制，将该区块添加至区块链，实现往来函证数字化。

函证是审计工作进行最重要的证据。通过生成电子函证，能够有效提高审计工作效率。

1.3.2　函证分类归档单元

函证类型多样，包括银行函证、应收账款函证、其他函证(往来款项、涉及第 3 方的其他资产、相关事项)等。由于往来函证会经过十多道环节的流转，容易丢失或者被篡改，流转过程中存在很大的安全风险，为方便访问和应用，需要对函证进行分类归档，把函证数据归入档案，分类保存。笔者采取的方法为 BP 神经网络法[14]，其运算过程简单，能够快速分类归档函证数据，降低函证数据在流转过程中的安全风险。函证数据标准化后，通过 BP 神经网络法构建函证分类模型，将函证数据作为样本，输入到 BP 神经网络的函证分类模型中进行多次迭代训练，以保证其输出的准确性，从而输出函证类型概率，确定函证类型，并将同一类型的函证归为一档。具体过程如图 2 所示。

1) 函证数据标准化。

$$x=(\hat{x}-b)/c\text{。}\tag{1}$$

式中：x、$\hat{x}$ 为标准化和原始函证区块头；b、c 为方差和标准差。

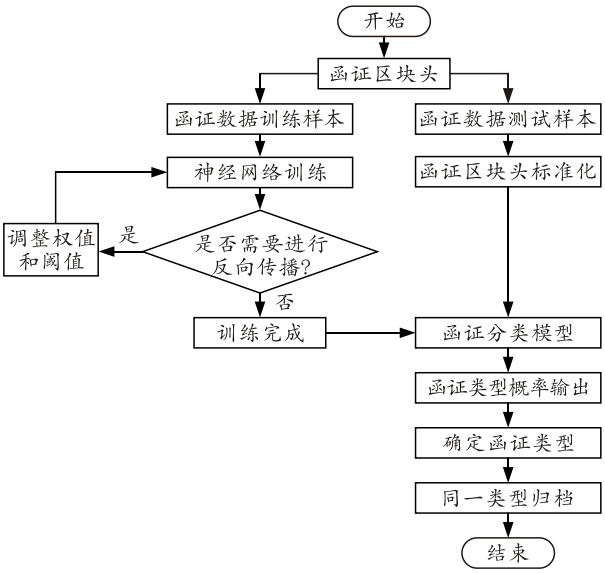

图 2　函证分类归档过程

2) 采用 BP 神经网络法构建函证分类模型。

$$a_j^l=\sigma\left(\sum_k a_k^{l-1}\times w_{jk}^l+b_j^l\right)\text{。}\tag{2}$$

式中：a_k^{l-1} 为降采样；σ 为选择的激活函数；w_{jk}^l 为权重；b_j^l 为偏置。

3) 将函证数据作为样本，输入到 BP 神经网络的函证分类模型中进行多次迭代训练，输出函证类型。

$$Y_k=\sum_{k=1}^{m}G_j w_{jk}-h_k,\ k=1,2,\cdots,m,\ j=1,2,\cdots,n\text{。}\tag{3}$$

式中：w_{jk} 为连接权值；h_k 为阈值；m、n 为神经元数量；Y_k 为 BP 网络输出层输出的函证类型；G_j 为上一层输出。

1.3.3　函证区块存储单元

针对获得的函证数据，需要将其存储到区块链各节点中。相比较其他存储技术可以避免询证函资料被篡改，保障函证数据的完整性和存在性，从而保证审计结果的可靠性[15]。函证区块基本形式如图 3 所示。

区块头					
版本号	前一区块哈希值	Merkle根值	时间戳	随机数	目标值

区块体					
函证1	函证2	函证3	函证4	……	函证n

图 3　函证区块基本形式

将函证区块串联起来，就形成了区块链。为保证区块链上函证数据的安全性，实现安全存储，结合 RSA 算法进行函证数据加密。具体过程如下：

步骤 1：输入待加密的函证数据。

步骤 2：选择 RSA 算法作为加密算法。

步骤 3：利用 RSA 算法生成密钥。具体过程如下：

1) 随机选择 2 个素数，记为 u 和 v。

2) 计算 u 和 v 之间相乘值，记为 P。

$$P=u\bullet v$$

3) 计算 P 的欧拉函数。计算公式如下：

$$f(P)=(u-1)(v-1)。\tag{4}$$

式中 $f(P)$为 P 的欧拉函数。

4) 随机选择一个整数 s。选择条件是 $1<s<f(P)$，且 s 与 $f(P)$互质。

5) 求解下述公式，得到整数 d：

$$d\bullet s \bmod f(P)=1。\tag{5}$$

式中 mod 为模运算。

6) 得到密钥 $F=(P, u, v, d, s)$，由此定义加密变换和解密变换。

7) 对 u 和 v 进行销毁，得到公开密钥$\{s, P\}$和私有密钥$\{d, P\}$。

步骤 4：利用得到的$\{s, P\}$和$\{d, P\}$对函证数据进行加解密。若选择前者进行加密，就利用后者进行解密；否则，则相反。所有函证统一使用相同密钥，将私钥存储在一个可以信任的服务器中，当用户需要私钥进行工作时，可以通过访问该可信任的服务器以获得认证。并结合一种增强口令认证钥匙交换协议算法，应用在公钥分发的过程中，不仅确保公钥在分发过程中不会被篡改，而且进一步增强了防范攻击能力。

1.3.4 平台安全防护单元

基于区块链技术的往来函证数字化平台中汇总了大量的各种类型的函证数据。这些都是审计证据，通过这些能够发现其中异常风险和行为[16]。在此背景下，为保证函证数据安全，预防违法者篡改或偷取数据，需要进行平台安全防护。具体过程如下：

步骤 1：用户输入身份信息到平台登录页面。

步骤 2：平台对用户身份进行验证。

步骤 3：判断用户身份是否合法。若合法，平台同意用户的访问请求，并进行下一步；否则，需要回到步骤 1，用户修正填写的身份信息并进行验证，当重复超过 3 次没有成功后，平台冻结该用户信息。

步骤 4：对用户的访问权限进行判断。不同的用户身份具有不同的访问权限，超过自己权限范围外的资源不允许访问。这能够在很大程度上避免非法访问情况的发生，确保往来函证数据的安全性[17]。权限判断过程如下：

1) 遍历权限存储区块。根据身份信息，每名用户的权限都是提前划分好并存储在区块上，当有需要时，可以根据用户的登录身份信息，遍历权限存储区块，寻找权限属性集合。

2) 判断区块头部 Merkle 根值是否等于解析权限请求后的 flag。若二者相等，则结束操作，完成权限寻找工作，输出权限集合；否则，继续寻找。

3) 利用区块链技术中的智能合约申请调用权限信息。

4) 对密文权限进行解密。

5) 生成明文权限。

步骤 5：根据获得的用户权限，控制用户访问操作。

2 平台应用与测试

针对平台的功能进行测试，证明所设计平台的实际应用效果，同时以便能够发现设计中的不足并进行改进。功能测试包括 2 个测试项目。第 1 个项目为测试平台的函证分类归档功能，第 2 个测试项目为平台安全性功能。并将文献[3]设计的基于 RFID 技术的平台和文献[4]设计的基于多级身份验证和轻量级加密的平台作为对比平台，与本文中平台进行测试对比。

2.1 平台测试环境

基于上文平台设计理论，搭建函证数字化平台，以此作为应用测试环境，如图 4 所示。

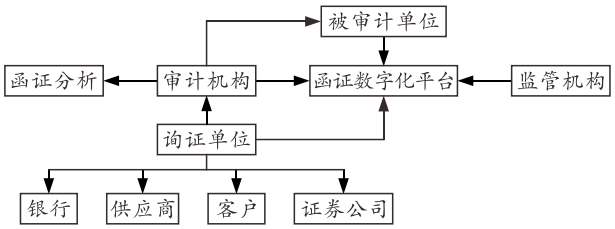

图 4 平台测试环境

将下述函证样本导入到上述平台当中，作为测试样本，如图 5 所示。

2.2 函证分类归档功能测试

为保证测试结果的有效性，将平台的分类归档结果与实际结果之间的重叠系数进行多次计算，并

取平均数，通过计算平台的分类归档结果与实际结果之间的平均重叠系数来测试平台单元的分类归档准确性。结果如表 2 所示。

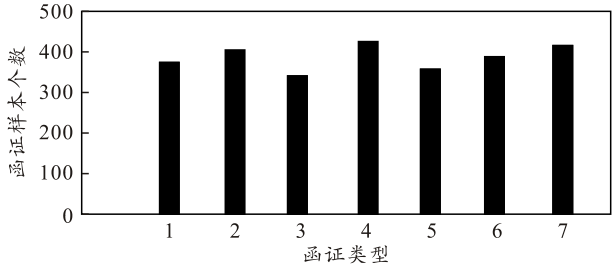

图 5　函证数据样本

表 2　函证分类归档功能测试结果

项目	基于区块链技术的平台	基于 RFID 技术的平台	基于多级身份验证和轻量级加密的平台
函证类型 1	0.952	0.847	0.878
函证类型 2	0.947	0.874	0.880
函证类型 3	0.935	0.869	0.866
函证类型 4	0.950	0.854	0.874
函证类型 5	0.964	0.866	0.872
函证类型 6	0.926	0.868	0.859
函证类型 7	0.933	0.877	0.894

从表 2 中可以看出，基于区块链技术的平台的平均重叠系数要大于基于 RFID 技术的平台、基于多级身份验证和轻量级加密的平台的应用结果，证明了平台的分类归档准确性。

2.3　平台安全性测试

模拟冒充攻击、重放攻击和 DDoS 攻击等 3 种方式，测试本文中平台、基于 RFID 技术的平台和基于多级身份验证和轻量级加密的平台的安全性。安全性指数由非法访问成功次数以及函证解密成功次数加权累加得出，计算公式如下：

$$Y=\left(WN+\hat{W}M\right)\Big/2; \tag{6}$$

$$W+\hat{W}=1。 \tag{7}$$

式中：Y 为安全性指数；N 为非法访问成功次数；M 为函证解密成功次数；W、$\hat{W}$ 为权重。

结果如图 6 所示。

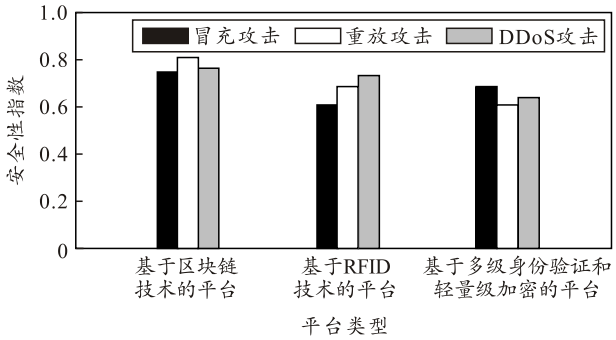

图 6　平台安全性测试结果

从图 6 可以看出：与基于 RFID 技术的平台、基于多级身份验证和轻量级加密的平台相比，笔者设计的基于区块链技术的平台的安全性指数更大，说明本平台的安全性更高，更能保证函证数据的安全。

3　结束语

为实现函证的高效和安全管理，设计一种基于区块链技术的往来函证数字化平台。通过区块链技术，不仅实现了函证的分布式存储，而且实现了其加密以及安全访问。最后进行了平台应用测试，通过测试平台安全性和分类归档准确性，验证了平台的功能性。在下一步的研究中，将平台应用于实际环境，进行进一步的测试；另外，性能表现也对平台至关重要，因此也需要将其考虑在内。

参考文献：

[1] 王栋, 杨珂, 王瑜, 等. 基于区块链的联盟信任分布式认证在电力行业的应用探索[J]. 电力系统自动化, 2022, 46(8): 1−10.

[2] 谢开, 张显, 张圣楠, 等. 区块链技术在电力交易中的应用与展望[J]. 电力系统自动化, 2020, 44(19): 19−28.

[3] 张鋆, 张明皓, 仝杰, 等. 用于电力资产在线感知的 eRFID 标签设计[J]. 电工技术学报, 2020, 35(11): 2296−2305.

[4] 任天宇, 王小虎, 郭广鑫, 等. 基于多级身份验证和轻量级加密的电力物联网数据安全系统设计[J]. 南京邮电大学学报(自然科学版), 2020, 40(6): 12−19.

[5] 胡翠华, 罗嘉滨, 李岩, 等. 基于区块链的审计监管云平台构建[J]. 科技管理研究, 2022, 42(14): 149−156.

[6] 孙正龙, 赵靖博, 庄钧植, 等. 基于OPC的电力信息物理系统仿真平台研究[J]. 电力系统及其自动化学报, 2022, 34(5): 70−78.

[7] 胡平, 王忠群, 刘涛, 等. 基于分布式 OSGi 的通用电力数据平台[J]. 计算机工程, 2014, 40(3): 71−75.

[8] 翟峰, 杨挺, 曹永峰, 等. 基于区块链与 K-means 算法的智能电表密钥管理方法[J]. 电力自动化设备, 2020, 40(8): 38−46.

[9] 张显, 冯景丽, 常新, 等. 基于区块链技术的绿色电力交易系统设计及应用[J]. 电力系统自动化, 2022, 46(9): 1−10.

[10] 陈广, 宋志伟, 陈少兵, 等. 数据感知技术在电力物资供应链数据质量管理中的应用[J]. 科技管理研究, 2021, 41(18): 182−191.

[11] 王柯元, 于雷, 颜拥, 等. 基于区块链的电力数据资产

化及交易系统设计[J]. 东北大学学报(自然科学版), 2021, 42(2): 166−173.
[12] 林洁瑜, 崔维平. 基于双链区块链的电力数据资产交易系统架构[J]. 中国电力, 2021, 54(11): 164−170, 180.
[13] 吉斌, 昌力, 朱丽叶, 等. 区块链系统节点私钥泄露的电力数据防篡改方法与验证机制设计[J]. 电力自动化设备, 2021, 41(12): 87−94.
[14] 王凌宇, 傅宏, 杨云, 等. 基于区块链的电力营销数据存储机制[J]. 重庆大学学报, 2021, 44(8): 156−164.
[15] 沈佳, 刘昆, 贾俊强, 等. 面向电网中数字资产存证的区块链 Baas 设计[J]. 中国电子科学研究院学报, 2020, 15(10): 996−1001.
[16] 苏寅生, 周挺辉, 郑外生, 等. 基于云计算的电力系统计算分析平台构建[J]. 南方电网技术, 2022, 16(7): 67−75.
[17] 王冰, 刘维扬, 陈献慧, 等. 区块链技术下配电侧电力市场交易平台研究[J]. 河海大学学报(自然科学版), 2021, 49(6): 567−574.

****

（上接第 16 页）

4 结束语

笔者利用 ADAMS 对用于水面舰船的储弹机构传动机构开展了研究，对接触力参数进行了选取，着重对考虑海浪情况的滚珠丝杆传动系统中丝杠应力应变情况进行了分析，得到以下结论：

1) 通过对 ADAMS 中滚珠丝杠副接触力对比分析后，得到了较为合适的接触力参数设置。

2) 在 6 级和 9 级综合海况下，柔性螺杆最大应力时刻均发生在丝杠启动加速阶段，最大应力区域在靠近电机左端部。

3) 在 6 级和 9 级综合海况下，柔性螺杆最大应变时刻也发生在丝杠启动加速阶段，最大应变区域发生在丝杠左侧与滚珠刚接触区域。

笔者通过 ADAMS 对用于水面舰船的滚珠丝杠副开展了研究，可为用于水面舰船的滚珠丝杠副的改进强化工作提供参考。

参考文献：

[1] 唐文献, 袁海波, 李虎. 基于 ADAMS 的某舰炮供弹系统仿真研究[J]. 江苏科技大学学报(自然科学版), 2010, 24(1): 61−65.
[2] 李利, 魏立新, 樊永锋. 基于刚-柔耦合模型的供弹系统动力学分析[J]. 舰船科学技术, 2018, 40(23): 150−154.
[3] 葛杨, 张家泰, 谭定中. 新型舰炮供弹凸轮轮廓线设计的研究[J]. 哈尔滨工程大学学报, 2004(6): 769−772, 798.
[4] 傅圆圆, 杨超, 姚远, 秦皇岛海洋站海浪特征分析[J]. 海洋环境科学, 2022, 41(6): 842−846.
[5] 郑祥靖, 李雪丁, 徐啸, 台湾海峡海浪数值模拟和特征分析[J]. 海洋预报, 2021, 38(5): 31−39.
[6] ZHENG C W, LI C Y. Variation of the wave energy and significant wave height in the china sea and adjacent waters[J]. Renewable & Sustainable Energy Reviews, 2014, 43: 381−387.
[7] LI C Y, XU M T, SONG W J, et al. A Review of Static and Dynamic Analysis of Ball Screw Feed Drives, Recirculating Linear Guideway, and Ball Screw[J]. International Journal of Machine Tools and Manufacture, 2023, 188: 1−42.
[8] ALTINTAS Y, VERL A, BRECHER C, et al. Machine tool feed drives[J]. CIRP Annals-Manufacturing Technology, 2011, 60(2): 779−796.
[9] SOBOLEWSKI J Z. Vibration of the ball screw drive[J]. Engineering Failure Analysis, 2012, 24: 1−8.
[10] BRECHER C, EßER B, FALKER J, et al. Modelling of Ball Screw Drives Rolling Element Contact Characteristics[J]. Cirp Annals, 2018, 67(1): 409−412.
[11] ZHEN N, AN Q. Analysis of stress and fatigue life of ball screw with considering the dimension errors of balls[J]. International Journal of Mechanical Sciences, 2018,137: 68−76.
[12] ZAEH M F, OERTLI T, MILBERG J, et al. Finite Element Modelling of Ball Screw Feed Drive Systems[J]. Cirp Annals, 2004, 1(53): 289−292.
[13] CHEN Y J, ZHAO J H, YUAN C F, et al. Analysis of contact characteristics of ball screws under the combined loads considering non-uniform load distribution[J]. Journal of Mechanical Science and Technology, 2023, 37(4): 1613−1621.
[14] GAO X S, ZHANG X R, YANG J S, et al. Dynamic modeling and analysis on lateral vibration of ball screw feed system[J]. The International Journal of Advanced Manufacturing Technology, 2022, 124: 4211−4229.
[15] 国家市场监督管理总局, 国家标准化管理委员会. 海浪等级: GB/T 42176-2022[S]. 北京: 中国标准出版社, 2022.
[16] 崔濛, 刘昕, 龚家烨. 不同海况下风浪对船舶排气扩散的影响研究[J]. 中国造船, 2023, 64(1): 257−267.
[17] 李增刚. ADAMS 入门详解与实例[M]. 北京, 国防工业出版社, 2014.