智慧船闸电气控制系统设计

张　陆
身份证号码：320112198608281632

摘　要：本文依据《智慧船闸架构模型设计》为指导思想，继续深入研究基于智能化理念的船闸电气控制系统。以多源数据综合运用为核心，设计以船舶数据、船闸数据、航道数据和环境安全数据为支撑的新型船闸电气控制系统，具备自动化特性，支持船闸少人/无人运营模式；另一方面从工控信息安全角度出发，对控制系统网络安全区域划分，从而打造具备自动控制功能、高安全系数的新型船闸电气控制系统。

关键词：智慧船闸；远程控制；自动化船闸

Design of electrical control system for intelligent ship lock

Lu Zhang
ID No.: 320112198608281632

Abstract: Based on the guiding ideology of "Intelligent Lock Architecture Model Design" as the guide, this paper continues to study the electrical control system of ship lock based on intelligent concept. With the comprehensive application of multi-source data as the core, the new lock electrical control system supported by ship data, ship lock data, channel data and environmental safety data, has automation characteristics and supports ship lock / unmanned operation mode; on the other hand, from the perspective of industrial control information security, the control system network security area, so as to create a new lock electrical control system with automatic control function and high safety factor.

Keywords: Smart lock; Remote control; Automatic lock

引言：

根据《江苏省十四五智慧交通发展规划》的要求，在“十四五”期间，要提高综合运输体系的效能，通过提高效能从而降低物流运输的能耗和成本。降低物流运输的能耗和成本，一方面服务于国家碳达峰碳中和的绿色高质量发展要求，另一方面服务于区域物流经济的高质量发展。

智慧船闸的发展建设也是智慧交通发展中的重要环节，基于《智慧船闸架构模型设计》一文，智慧船闸体现在对船闸闸况、过闸船舶状况、船闸环境安全及航道水文数据，四类数据的感知、分析和应用服务方面；而目前常规的船闸控制系统，基于现地人工控制模式为主，对过闸船舶状况、船闸环境安全及航道水文数据，主要依赖人工判断和决策，控制系统缺乏对此类数据的感知和分析，所以新型的船闸电气控制系统是从传统的常规的工控系统基础上进行更数字化、信息化的创新发展。[1]

一、船闸经典控制系统

船闸目前的电气控制系统仍然是比较典型的线性定常系统，是单输入、单输出的控制系统，属于传统的工业控制系统范畴。

其控制原理图如下图1所示：

根据经典控制理论，船闸控制系统的控制对象主要是过船的闸门和输水的阀门设备，以及配套的交通信号设备。所以控制系统的主要反馈信号是围绕控制对象展开，包括闸阀门的电机拖动数据、闸阀门的液压启闭机数据、闸阀门的行程数据。以上反馈数据基本为控制系统提供了较为全面的船闸运转件反馈数据。再加上保障船舶过闸安全的水位数据，形成了船闸的控制系统架构。

但船闸控制系统运行的工况，并不是标准工况，船舶航行状况和航道水文状况都是影响控制系统工况的因素。而现有的基于PLC设备为核心的控制系统，因为数据通讯能力和数据处理能力的限制，无法接受船舶航行数据和航道水文数据进行分析、应用服务于控制船闸运行，所以现阶段大多数船闸控制系统必须以人为媒介，通过人工确认船舶数据和航道数据后，参与到船闸的控

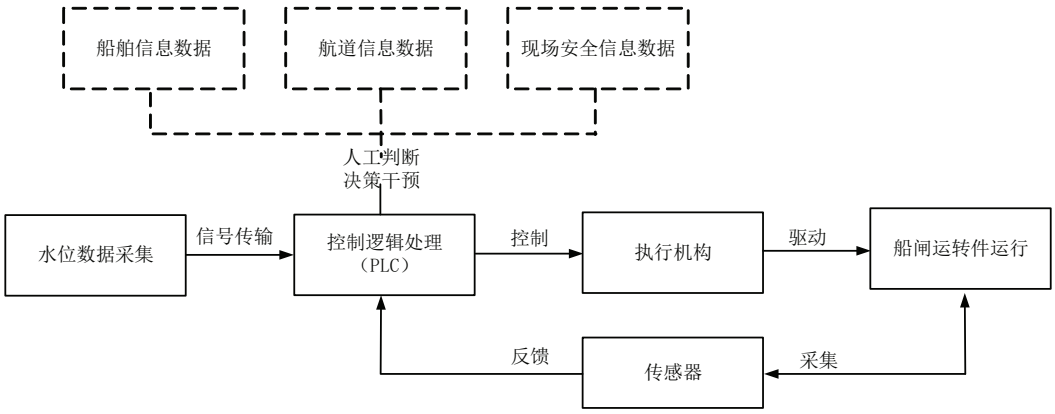

图1　船闸控制原理图

制流程中。从而当前的控制系统能效是受到人工效率的限制，而且参与控制系统操作的人员的能动性也被限制在操作控制系统中，无法发挥最大效能。

二、智慧船闸新型自动化控制系统

智慧船闸理念下的新型自动化控制系统，所谓自动化控制的实现，需要厘清自动化控制的服务对象和控制内容；船闸的自动化控制为船舶提供过闸服务，需要控制的对象是船闸闸阀门的启闭和通航的信号指示，所以新型的自动化控制系统和传统控制系统最大的区别是纳入了航道数据、船舶数据和非结构化的船闸运行数据，针对航道、船舶、船闸三者互为关联的对象进行较为综合全面的感知，通过对感知数据的分析、决策和应用，从而达到无人干预、自动化运行的效果。

新型控制系统的原理图如图2所示：

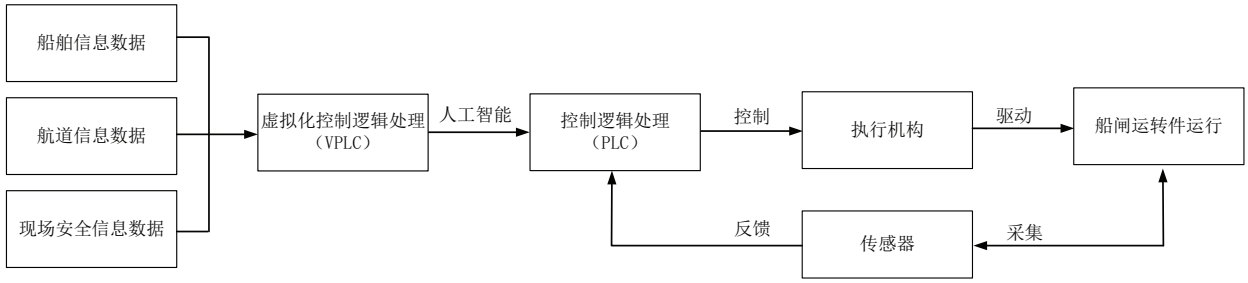

图2　新型控制系统原理图

新型自动化控制系统在现有的控制系统基础上，增加一层VPLC（虚拟化可编程逻辑控制器）系统，可满足感知并分析航道数据、船舶数据和船闸非结构化数据及环境安全数据等多源数据的条件。

结合船闸现有的调度系统和电气控制系统，无人值守的自动化控制的实现不需要融合调度系统和电气控制系统。船舶调度系统在智慧船闸中的定位，不是子系统，而是智慧船闸的一项技能，而船闸电气控制系统是智慧船闸的一项综合感知和反馈系统。船舶调度技能需要电气控制系统的支撑可以实现智能化的调度，而电气控制系统需要的船舶、船闸、航道及环境数据，通过多源数据的支撑实现无人的自动化控制。

船闸自动化控制系统的现场控制权限最高。因为最高权限应该具备自动化控制的所有功能，所以自动化控制的核心应该在现场，贴近具化的使用场景，而不是异地，不依赖远程的集中控制中心，不依赖远程通信网络。自动化控制核心（大脑）在现场，而展示可以在远端，包括远端的控制，所以船闸的自动化控制系统具备远端控制功能，但现场控制权限最高，远端的控制权限最低。

船舶、船闸、航道、环境多源数据的综合感知和分析已经超脱了传统工业控制的范畴，所以船闸自动化的控制系统架构是在工业控制技术（OT）和网络通信技术（IT）融合基础上形成的系统，IT侧负责多源数据的汇聚和分析，OT侧负责船闸运行的控制。

而OT和IT融合的关键就是通过分析综合数据而去指导工业控制的通讯链路的打通。传统船闸控制系统的网络环境相对单一，网络设备少，数据量小，网络防护薄弱，但对网络实时性，稳定性要求高，不允许有错误数据和丢失数据。多源数据的综合处理是在IT侧，其网络环境相对复杂，设备较多，数据通讯量大，网络的实时性和稳定性稍逊OT侧，网络的干扰因素较多，但干扰耐受性强于OT侧。所以OT和IT的网络环境有较大区别。

从网络安全稳定等级上来划分，船闸自动化控制系统的OT侧网络环境安全等级高，IT侧的网络环境安全等级较低，所以OT侧的船闸控制反馈数据可以单向传输至IT侧的网络环境中，配合IT侧的数据分析。而IT侧往OT侧的数据传输，应该在确保数据安全的情况下进行传输，在传输前应该分析具体哪些数据由IT侧传输给OT侧，根据数据量的大小来选择合适的通讯方式。根据船舶过闸的八步工艺和控制对象进行分析，IT侧需要传输至OT侧数据只是船舶过闸8步工艺相关的控制指令，数据量很小，所以可以设计选用硬接线的方式传输数据，同时在OT和IT的边界增加一套边缘PLC设备，参考“云计算”的端-边-云理念。从而形成VPLC（IT侧）-边缘PLC（边界）-核心PLC（OT侧）的船闸自动化控制架构。

架构图如下图3所示：

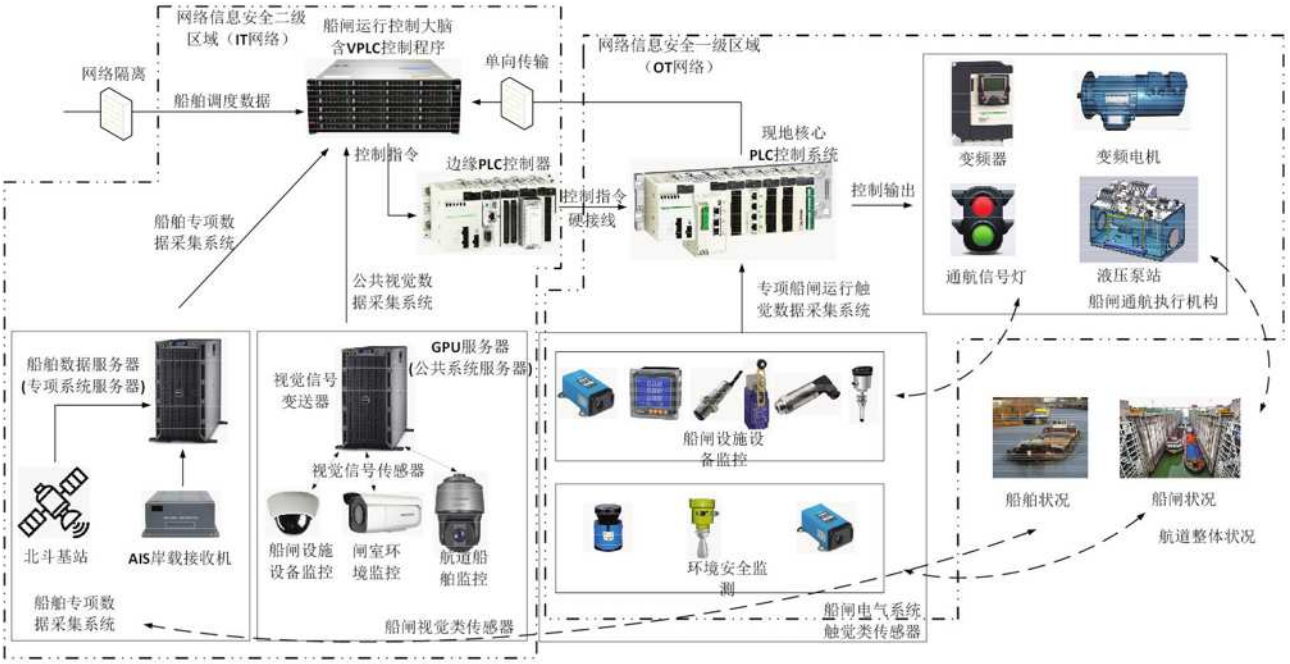

图3　新型船闸自动化控制架构

新型船闸自动化控制系统架构下，通过视频监控系统作为综合感知公共系统和AIS、北斗、激光检测等专项系统，对船舶、船闸、航道及船闸环境进行全面综合的感知，而在IT侧的服务器设施上部署虚拟化可编程逻辑控制器（VPLC），在服务器上的VPLC，得益于服务器的数据通信采集的多样性和强大的数据处理能力，就可以融合IT侧和OT侧的船闸/船舶/航道感知数据进行综合分析和计算。

其后通过感知数据的分析计算结果来控制船闸运转件的运行，替代工作人员的操作、决策和干预，从而达到自动化运行的效果。

三、新型控制系统信息安全防护

针对船闸新型控制系统的信息安全而做的防护，首先需要了解新型控制系统会存在哪些网络风险。

根据国家信息安全漏洞共享平台（https：//www.cnvd.org.cn/）显示，工控产品不分国籍、行业、类型，网络产品均有漏洞存在；针对控制系统，主要有几下几类入侵方式。

1.底层固件攻击（Payload攻击）

固件是指运行在PLC设备底层硬件之上的操作系统，PLC控制程序以固件为载体进行运行。常规PLC系统正常运行后，基本不会进行固件升级，所以固件原有的漏洞，可能成为被攻击的地方。

常规固件从官网下载，然后进行逆向分析，确定各个参数的寄存器地址，匹配设备功能，然后修改，对固件进行重新打包，并下载更新到PLC中，进而干扰控制程序的正常运行，导致不可知的故障发生。

2.网络扫描、探测

所谓扫描探测就是通过对OT侧的PLC设备和其他网络设备进行扫描，获取PLC设备信息和网络情况。通过利用nmap扫描、shodan等搜索引擎扫描以及第三方扫描脚本等方式，扫描获取相关信息。

3.中间人攻击

在船闸控制系统运行过程中，上位机软件通过PC和PLC进行程序的上下载、程序的监控诊断、网络通信质量查看，进行数据区的修改等操作。在这个通讯交互的

过程中，如果通讯协议本身没有进行加密或存在安全漏洞，那么对该通讯协议进行破解，对传输的数据包进行修改、重置，欺骗两边的设备，就可以干扰PLC的正常运行，导致船闸运转设备按照错误的参数或控制命令运行，这就是“中间人攻击”。

4.DDOS攻击

DDOS攻击，即为分布式拒绝服务攻击，当有单位入侵进入控制系统OT侧后，即可以在OT侧网络中通过一个攻击者控制了位于不同位置的多台机器并利用这些机器对控制设备同时实施攻击。由于攻击的发出点是分布在不同地方的，这类攻击称为分布式拒绝服务攻击，其中的攻击者可以有多个，由于PLC设备的计算资源和内存资源是有限，采用DDOS攻击，就会耗尽PLC的计算资源、网络资源、存储资源，PLC识别最终将不堪重负，而无法响应正常的请求，导致系统宕机。

5.控制逻辑攻击

即通过向原来的PLC控制程序中注入错误代码或者数据，影响PLC设备的正常运行，甚至可以获取PLC的系统控制权，进而破坏PLC系统的逻辑程序。一般都会经过3个步骤：获取PLC控制程序代码数据，进行反编译，注入恶意控制代码。

我们可以了解以上5类入侵方式均需要通过网络访问的方式，才可进行攻击，所以通过部署常规的网络安全防护设备，包括防火墙、单向网闸、入侵检测、入侵防御、日志审计、工业安全审计、堡垒机、监管平台等固然可以防范，但网络访问的链路只要存在就存在网络攻击的风险，所以在新型控制系统设计中，采用边缘PLC控制器作为IT侧往OT侧传输数据的载体，边缘PLC控制器具备一定数据处理计算能力、网络通讯能力，并可以将数字化数据转换成模拟量数据，从而使网络攻击无端口可用，那以上5类攻击均可避免。即便有网络攻击入侵边缘PLC控制器，通过边缘PLC控制入侵OT侧，因为模拟量数据的转换，也只能简单的进行错误逻辑指令攻击，核心PLC控制系统完全具备屏蔽错误指令的功能，不会产生较大的安全生产事故。

所以船闸新型控制系统做到了OT和IT的融合，IT侧完全可以将数据传输给OT侧设备进行船闸运行的全自动化控制。

四、结语

船闸的自动化控制应该结合多源数据感知，通过采集船闸数据、船舶数据、航道数据和环境安全数据，综合判断后，来控制船闸运行，船舶调度。用人工智能、大数据分析来替代人工的操作、干预和决策，从而实现船舶过闸全流程的少人化和无人化。无人化和少人化的实现，可以从现地少人值守开始，通过人工智能新技术的应用，人工从现场操作退至后台中心决策干预，再至完全的退出，不参与操作，决策，甚至不干预船闸运行。但不干预船闸运行不代表船闸的无人化，只是船舶过闸业务的无人化模式得到实现，船闸的各项机械电气设备、网络设备还是需要大量的维护人员进行维护才能做到船舶过闸业务流程的无人化。

参考文献：

[1]张陆.智慧船闸架构模型设计.中国新技术新产品.2021.4.

[2]严立励.扬州智慧船闸建设的相关问题研究与建议.科技创新与应用.2022.4

[3]丁付进.澹港闸船闸电气控制系统设计与应用[J].黑龙江水利科技，2020，48（07）：156-159.

[4]张雷.江苏省交通船闸电气控制系统解析精要[J].中国水运（下半月），2019，19（10）：53-54.

[5]颜廷雪.探究船闸PLC电气系统中的故障原因与维护处理技术[J].江苏科技信息，2019，36（13）：58-60.