文章编号:1671-4598(2021)09-0233-05 DOI:10.16526/j.cnki.11—4762/tp.2021.09.043 中图分类号:TP29 文献标识码:A

基于 CODAC 框架的托卡马克装置人身安全联锁系统研究

孙 江,夏 凡,吴 豪,李 波,王 硕
(核工业西南物理研究院,成都 610041)

摘要:为了保护实验人员安全,避免 HL-2A 主机大厅在放电期间存在许多危险因素,比如高电压、危险气体、电磁辐射、电离辐射等对人身安全的危害,确保放电期间任何人不会出现在主机大厅,因此参考 ITER CODAC 的安全保护设计,并结合 HL-2A 装置的工程需要,搭建了专用的安全联锁网络,设计了一套基于 EPICS 的人身安全联锁保护系统;该系统采用 EPICS CA 协议和西门子 S7nodave 驱动实现了软 IOC 读取 PLC 变量,并结合 SQL 数据库和 C# 编程实现了对主机大厅门禁访问系统的控制,保障了主机大厅设备和实验人员的安全,经三年多的投入使用,该系统提高了 HL-2A 的安全保护级别和放电效率。

关键词:安全联锁;门禁访问;EPICS

Research on Personal Safety Interlocking System of Tokamak Based on CODAC

SUN Jiang, XIA Fan, WU Hao, LI Bo, WANG Shuo
(Southwestern Institute of Physics, Chengdu, Sichuan 610041, China)

Abstract: In order to protect the safety of personal, avoid many dangerous factors in the hall of HL-2A tokamak during discharge, such as high voltage, magnetic field and radiation, and ensure that no one is allowed to stay in the hall during plasma discharge. With reference to the safety protection design of ITER CODAC (Control, Data Access and Communication), combined with the engineering needs of the HL-2A, a dedicated safety interlocking network was built and a set of personal safety interlock protection system based on EPICS (Experimental Physics and Industrial Control System) was designed. The system uses the EPICS CA (Channel Access) protocol and Siemens S7nodave driver to realize the soft IOC (Input Output Controller) reading PLC (Program Logical Control) variables, and combines SQL database and C# programming to realize the control of the access control system of the Tokamak machine hall, ensuring the safety of the hall equipment and experiment personnel. After operation for more than three years, the system has improved the safety protection level and plasma discharge efficiency of HL-2A.

Keywords: security interlock; access control; EPICS

0 引言

HL-2A 托卡马克装置主机大厅是开展核聚变物理研究和工程实践的最重要的场所。在主机大厅里面,主机周围分布着各个子系统的上百件套不同设备,实验人员在实验期间根据实验目的不同需要出入主机大厅对其所负责的设备进行相关的调试调整。考虑到 HL-2A 主机大厅里面存在许多危险因素,比如上万伏特的高压、零下一两百多度液氮液氦、中性束注入期间产生大量的中子辐射、大功率的微波辐射等等,都是对人体有害的[1]。这些危险因素一般出现在等离子体放电期间,所以放电期间实验人员必须全部离开主机大厅,才能保证人员和设备的安全。

在之前的 HL-2A 放电实验中,采用放电前打铃 60 秒的方式通知主机大厅里面的实验人员立即离开。但是这种方式存在的弊端是主机大厅空间大、噪音大,有些角落听不清铃声。因此有必要重新设计一套人身安全联锁系统,确保实验人员在等离子体放电前全部离开主机大厅,且等离子体放电期间不会有人误入主机大厅,及时制止各种可能的安全事故发生。

1 人身安全联锁系统

人身安全联锁系统是 HL-2A 托卡马克装置中央安全控制系统的重要组成部分,主要用于主机大厅的人身和设备安全联锁保护。参考 ITER CODAC 并根据当前时代背景下的技术条件和控制运行理念,有效地结合装置的运行状态及保障设备和人员安全的需求,设计了一套人身安全联

收稿日期:2021-01-19; **修回日期**:2021-03-18。
基金项目:国家磁约束核聚变能发展研究专项(2018YFE0302104)。
作者简介:孙 江(1988-),女,湖南常德人,硕士,工程师,主要从事机电控制设计及维护方向的研究。
引用格式:孙 江,夏 凡,吴 豪,等.基于 CODAC 框架的托卡马克装置人身安全联锁系统研究[J].计算机测量与控制,2021,29(9):233-237.

锁系统。

人身安全联锁系统的开发设计，主要针对实验人员人身安全及仪器设备财产安全而展开，是一个以保护概念为核心的专用系统。它分为两个部分：中央安全控制系统和门禁访问控制系统。本文从总体结构，系统框架，通讯网络等方面介绍了人身安全联锁系统的设计和实现。

1.1 总体结构与 CODAC 的关系

中央安全控制系统（central safety system，CSS）需要对门禁访问控制系统（access control system，ACS）进行实时监视和安全控制[2-4]。图 1 是 ITER 门禁访问控制系统的接口关系图，深灰色为门，浅灰色为 CSS 部分，无色为 ACS 部分。

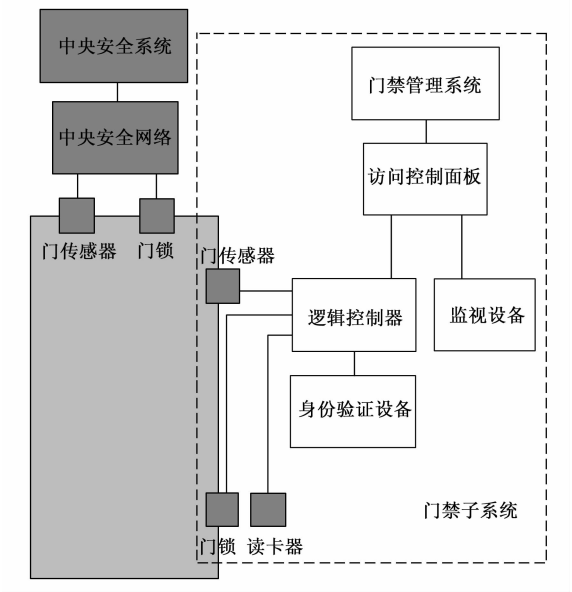

图 1 ITER 典型的门禁访问监视控制框架图

ITER 的门禁访问安全控制系统主要对进出受保护的区域提供安全联锁。根据安全级别和装置运行状态等综合因素考虑，通过使用令牌进出控制门来实现门禁访问。当进入的该区域处于“限制”状态时，每个人都应使用令牌通过控制门进入。直到真正离开受限制的区域后，将令牌返还给分配箱。每个令牌的状态（插入或移出的状态）应被监控，并发送给 CSS。

1.2 人身安全联锁系统框架

ITER CODAC 对人员安全保护（Safety）和设备联锁保护（Interlock）作出划分。但是，由于 HL－2A 装置与 ITER 有一定差异，所以我们不完全照搬 CODAC 相关设计标准。对于较复杂的涉及人员安全的子系统，我们对其设立安全和联锁保护，而对于一些较为单一的诊断设备等子系统，我们仅对其设立联锁保护，不加入人员安全保护功能。

CSS 是一个中央协调器，通过中央安全网络（CSN，central safety network）接收各个子系统的布尔事件，并向这些子系统发出指令，也需要处理一些模拟量信号。CSS 控制逻辑不受人工干预和手动控制，但某些人工功能（比如急停）要放到中控[5-6]。CSS 具体负责的任务有：

1）处理来自现场设备的警报和事件；

2）将访问控制警报和事件推送到大屏显示；

3）跟踪和记录存储事件。

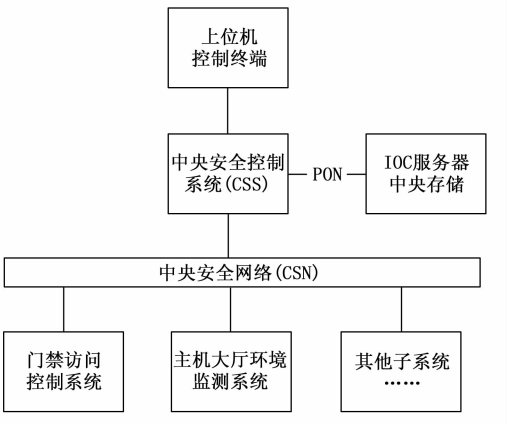

图 2 中央安全控制系统框架图

ACS 主要包括门闸设备和控制终端、视频拍照和红外探测功能等[7-9]。门禁系统的安全设计通过双门互锁、防尾随功能以及对人进出行为的严密逻辑控制程序实现安全性更高、可靠性更强的门禁控制管理，有效地监测托卡马克装置大厅是否有人逗留或者闯入[10-15]。门禁访问控制系统负责的任务有：

1）获取实验人员身份和配置他们的访问权限，并将身份和访问权限下载到门闸控制器中；

2）授予/拒绝来自门闸控制器的访问请求，保存访问记录；

3）根据每个实验人员的身份和当前装置运行状态来确定是否允许当前人员对安全控制区的访问。

1.3 中央安全控制系统硬件

中央安全控制系统由一套西门子冗余 400 系列 PLC、ET200 分布式 IO 采集、千兆交换机组成并装配到 EMC 屏蔽机柜，用来处理与装置和人员安全有关的事件，同时具有机柜状态监控功能，主要监视机柜前后门状态和机柜温度。如果机柜内温度超过 25 度，则自动启动风扇。机柜内部正面从上往下的布局依次是供电，冗余 PLC 和 ET200 设备，交换机和温控显示和接地，背面是端子排用来接外部信号。

1.4 EPICS 和网络布置

EPICS 是用于实验物理和工业控制平台的一套开源软件框架。EPICS 的软件包主要包括 Base、各种模块（Module）和扩展（Extension）。其中 Base 是 EPICS 软件的主体部分，而模块和扩展则是在 Base 的基础上为 EPICS 提供软硬件支持和其他辅助功能[16]。

EPICS 采用了客户端/服务器架构实现不同主机之间的

通信。在 EPICS 中扮演服务器角色的是 IOC，它们负责完成具体的输入/输出动作及本地控制任务，并利用 CA 协议从网络中接收来自客户端的信息或向客户端发布自身状态信息。EPICS IOC 的基本结构如图 3 所示。

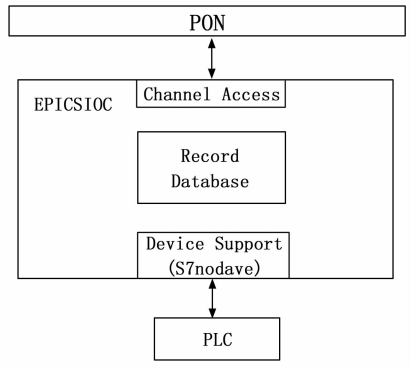

图 3　EPICS IOC 的结构示意图

EPICS 使用各种类型的记录（Record）来表示输入/输出量，而 IOC 内存中所有 Record 的集合则被称为 IOC 数据库（Database）。局域网内通常包含多个 IOC，它们的 IOC 数据库便组成了一个分布式数据库。当 Record 需要与硬件交互时，则需要调用相应的 Device Support 实现和硬件之间的通讯。IOC 数据库中的 Record 通过 CA 协议发布到网络中，成为能够被 CA 客户端访问的过程变量（process variable，PV）。

中央安全控制系统拥有自己的 IOC，将门禁访问控制系统的变量通过 CA 协议发布到 PON 网络中。CSN 采用千兆光纤星型网实现各系统之间的通讯，在中央机房放置一台西门子交换机 XR528－6M，VLAN 设有 2 个网段，一个属于 CIN 网，一个属于 CSS 网。

PON（Plant Operation Network）网络对应于 ITER 的装置运行网。所有与 EPICS 相关的机器均在此网段内。所有连接 CIN 和 CSN 的子系统中的控制器、数据服务器和上位机操作终端均接入 PON 网络。PON 网络承载所有子系统常规控制和安全联锁的监视数据流。

2　在 HL－2A 上的应用

这节主要详细说明门禁访问控制系统在 HL－2A 现场是如何布置和运行的。

2.1　HL－2A 人身安全联锁系统设计

人身安全联锁系统的总体设计结构图如图 4 所示。在现有的设备和网络基础上，新安装了门禁设备和门禁软件。

在主机大厅的两个出入口分别安装了门闸设备，其通电由 PLC 驱动继电器完成。实验人员需要刷员工卡才能开闸通过，且一次只能通过一个人。控制门闸设备的屏蔽（非使能）和激活（使能）功能实现多门互锁。门闸设备具有反潜回功能，当同一个人刷卡进去后需要刷卡出来后才具有再次刷卡进去的权限，不允许进去时刷卡，出来时却不刷卡。

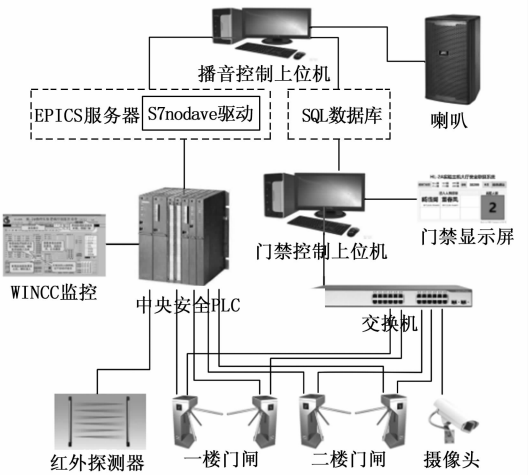

图 4　HL－2A 人身安全联锁系统的总体设计图

门禁管理系统一般为门闸自带工具，负责登记用户进出权限并将刷卡进出的人员信息记录存储到 SQL Server 数据库中。没有登记授权的人员不允许刷卡进入主机大厅。只有具有访问权限，门闸才解锁允许通过。

每天第一炮放电前，由专人对主机大厅区域进行巡逻检查，确定大厅没有逗留任何人的情况下，开启门闸设备。门禁访问控制系统与中央安全控制系统有互锁保护，门禁系统会实时监测、统计和显示主机大厅内的人数，并将计算结果发送到中央安全控制系统，确保在放电过程中主机大厅无任何人员。若主机大厅内部的人数不为 0，那么中控台就不能发出开始放电的指令。放电期间禁止刷卡进入主机大厅，门禁刷卡开闸功能无效。

同时，在大厅的两个出入口上方均安装有一个显示屏，用来显示进入到主机大厅的实验人员的名字、进去时间、当前人数和实验状态等信息。此外，还在主机大厅内放置了 4 个大功率喇叭，在准备开始放电之前，喇叭会不断广播停留在主机大厅内的实验人员的名字，催促他们迅速刷卡离开主机大厅。

2.2　HL－2A 门禁访问控制系统软件设计

在门禁访问控制系统硬件的基础上，还需要软件编程完成进出人员的记录、显示、广播等功能。所以门禁控制上位机还需要运行两个程序，其中一个程序 Alarm 负责广播，另一个程序 Display 负责显示进出人员信息。都采用 C＃编程，使用 EpicsSharp 库，利用 CA 协议对 PV 进行读写。

中央安全控制系统搭建有一台 EPICS 软 IOC，利用 s7nodave 驱动包将与门禁控制有关的 PLC 变量和 PV 对应起来，网页配置好 PV 生成 DB 文件并应用配置[17-18]。软 IOC 就能与 PLC 通讯，并通过 Archiver Appliance 实现 PV 的归档存储。PLC 中 5 个与门禁控制有关的变量如图 5 所示。

这 5 个变量表示的含义分别是：

CCO－CSS－IOC：MJ－BELL 打开广播喊人；

CCO－CSS－IOC：MJ－BELL1 每天第一炮广播喊人；

图 5 门禁控制 PLC 变量

CCO－CSS－IOC：MJ－STOP－BELL 关闭广播喊人；

CCO－CSS－IOC：MJ－RESET 门禁显示屏信息清零；

CCO－CSS－IOC：MJ－PEOPLE－IN 主机大厅里面有人。

用 C＃编写的 Alarm 和 Display 程序要一直监听前 4 个 PLC 变量的变化而触发相应的动作。实验运行人员在中控 WINCC 界面点击不同的指令，Alarm 和 Display 程序监听到对应的 PV 有变化后，触发不同的动作。下面是 C＃利用 CA 协议定义 PV 通道和监听 PV 的实时值。

```
channel_FirstCall = client.CreateChannel<int>("CCO－CSS－IOC:MJ－BELL1");
channel_FirstCall.MonitorChanged＋＝new EpicsDelegate<int>(channel_FirstCall_Changed);
channel_StopCall = client.CreateChannel<int>("CCO－CSS－IOC:MJ－STOP－BELL");
channel_StopCall.MonitorChanged＋＝new EpicsDelegate<int>(channel_StopCall_Changed);
channel3 = client.CreateChannel<int>("CCO－CSS－IOC:MJ－BELL");
channel3.MonitorChanged ＋＝ new EpicsDelegate＜int＞(channel3_Changed);
channel4 = client.CreateChannel<int>("CCO－CSS－IOC:MJ－RESET");
channel4.MonitorChanged ＋＝ new EpicsDelegate＜int＞(channel4_Changed);
```

Alarm 程序每 2 秒从 SQL Server 数据库中读取当前进出入大厅的人员记录。门禁系统在每次有效进入后，增加当前大厅内的人员数量，在有效退出后，抵消刷卡进去的记录，减少人员数量，从而判断主机大厅里的剩余人数。

门禁系统的 Display 程序也是 C＃编写，程序任务和结构跟 Alarm 程序类似，也是需要配置 PV 通道并监听它们。这里由于显示内容更多，所以需要监听的 PV 更多。

```
channel1 = client.CreateChannel<int>("CCO－CSS－IOC:MJ－PEOPLE－IN");
channel2 = client.CreateChannel<int>("CCO－CSS－IOC:MJ－AMOpen");
channel3 = client.CreateChannel<int>("CCO－CIS－IOC:TCN_ccBegin");
channel4 = client.CreateChannel<int>("CCO－CIS－IOC:TCN_ccExit");
channel5 = client.CreateChannel<int>("CCO－CSS－IOC:MJ－RESET");
channel6 = client.CreateChannel<int>("CCO－CIS－IOC:SHOT－NUM");
channel7 = client.CreateChannel<int>("CCO－CSS－IOC:MJ－BELL");
```

Display 程序也是每 2 秒从 SQL 数据库读取进出人员的姓名、进去时间，并按刷卡时间的先后顺序将每个人的姓名、进去时间显示在屏幕上。屏幕显示还包括门禁状态、实验状态、当前人数、当前炮号。门禁系统的状态显示屏如图 6 所示。主机大厅当前人数为 0 的时候显示背景为绿色，有人时显示背景为红色，并显示总人数。实验人员能清晰的看到当前主机大厅的访问状态。

图 6 主机大厅门禁访问控制系统显示屏

3 HL－2A 门禁系统的运行

每天实验前试验运行人员开启门禁系统并将之前的人员记录清除复位。每天第一炮放电前，播报第一炮的语音对主机大厅进行清场，清场完毕后开始第一炮放电。从第二炮放电开始，根据门禁系统记录的进入主机大厅的人员信息，播报对应人员的姓名，催促他们尽快离开。

中控 WINCC 监控界面如图 7 所示。中控实验人员在每天第一炮放电前按下“第一炮喇叭喊人”按钮（对应变量 CCO－CSS－IOC：MJ－BELL1），Alarm 程序收到指令后触发主机大厅里面的喇叭开始循环播放语音“即将开始第一炮放电，请尽快离开主机大厅，放电结束之前不要返回

主机大厅”。除开每天第一炮放电以外的其他炮放电，开始放电前都是点击“喇叭”按钮（对应变量 CCO－CSS－IOC：MJ－BELL），喇叭开始广播“即将开始放电，请[名字 1]，[名字 2]，[名字 3] 等迅速离开主机大厅”，直到主机大厅里面的人全部刷卡出来后，喇叭播报一遍“大厅已清空，准备放电”，才可以启动放电。当中控人员按下“停止喊人”按钮（对应变量 CCO－CSS－IOC：MJ－STOP－BELL），喇叭停止广播。当按下“门禁复位”按钮（对应变量 CCO－CSS－IOC：MJ－RESET），门禁显示屏的进出人员信息全部清空。

门禁系统与中控互锁，在主机大厅内有人时，不能启动放电。Alarm 程序判断主机大厅里面有人时，变量 CCO－CSS－IOC：MJ－PEOPLE－IN 的值为 1，中控 WINCC 界面闪烁提示此时主机大厅里面有人，禁止启动放电。

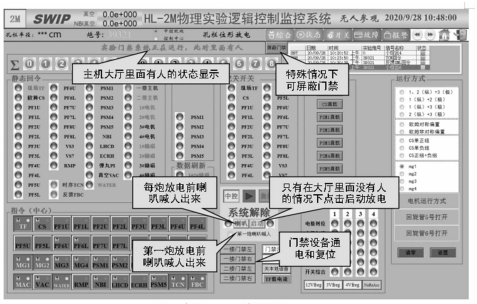

图 7　中控 WINCC 监控界面

门禁系统在实际运行中会遇到各种突发情况，比如需要外来人员协助修理设备时，需要持临时卡进入。有设备突发故障需要让出通道方便进出时，需要将门禁系统断电并停止工作，门禁系统再次投入前需由专人巡逻清场，再采用第一炮放电前清人的方式，然后启动放电。

4　结束语

基于 CODAC 框架下的人身安全联锁系统改善了硬件架构和网络结构，更好地集成了各个与安全相关的系统，实现了毫秒级的错误互锁，提供了友好的可视化界面，也降低了以后的改造花费和时间成本。人身安全联锁系统已经应用在 HL－2A 的放电实验中，保证了在放电期间，主机大厅不会有人逗留，通过门禁系统的区域人数计算功能，能准确计算进入区域的有效持卡人的数量。经过多轮实验运行测试，取得了较好的安全保障效果，解决了以前主机大厅存在的安全隐患。即保证了放电期间的人员安全，又提高了 HL－2A 的放电效率。

本系统目前正在进行改造升级，未来考虑采用生物识别设备（指纹仪、人脸识别）代替读卡器，提高身份认证的可靠性，减少卡片丢失的风险。

参考文献：

[1] 李　强. HL－2A 托卡马克装置的工程和实验概况 [J]. 原子能科学技术，2009，43：204－208.

[2] PATISSON L，AGUERO D，NIVESSE R. Interface Control Document between Personal Access Control（PBS 62.24）and Access Control & Security（PBS 69）[M]. ITER Internal Use，2014.

[3] SIMROCK S，BARNSLEY R，BERTALOT L，et al. Integration of the ITER diagnostic plant systems with CODAC [J]. Fusion Engineering and Design，2011，86：1145－1148.

[4] SCIBILE Luigi，JOURNEAUX Jean－Yves，KLOTZ Wolf－Dieter，et al. The ITER safety control systems—Status and plans [J]. Fusion Engineering and Design，2010，85：540－544.

[5] 罗　芳，阮群生，李志亮，等. 辐射安全联锁系统的数字化控制 [J]. 河南教育学院学报（自然科学版），2015，24（3）：36－38.

[6] 李裕熊，宁欣全，李汪忻，等. 合肥国家同步辐射实验室人身辐射安全联锁系统 [J]. 辐射防护，1992，12（1）：25－31.

[7] WANG W T，SONG Y，WANG J Y，et al. Design of the Personnel Radiation Safety Interlock System for High Intensity D－T Fusion Neutron Generator [J]. J Fusion Energ，2015，34：346－351.

[8] TAKAHASHI Hiroki，MAEBARA Sunao，KOJIMA Toshiyuki，et al. Safety managements of the linear IFMIF/EVEDA prototype accelerator [J]. Fusion Engineering and Design，2014，89：2066－2070.

[9] 李铁辉，王庆斌，陈志兴，等. 门禁控制技术在加速器人身安全联锁系统中的应用 [C] //第三届全国计算机在加速器中应用学会交流会，2005.

[10] 孙晓阳，罗家融，季振山，等. EAST 安全巡检与联锁保护系统设计与实现 [J]. 核技术，2008，31（4）：293－297.

[11] HRONA M，SOVA J，SIBA J，et al. Interlock system for the COMPASS tokamak [J]. Fusion Engineering and Design，2010，85：505－508.

[12] 马应林，王庆斌，王宇飞，等. 中国散裂中子源辐射安全联锁门禁系统的设计 [J]. 核安全，2017，16（4）：84－89.

[13] 张会杰，马应林，王庆斌，等. 基于 PLC 的高能同步辐射光源人身安全联锁系统设计 [J]. 工业控制计算机，2019，32（10）：16－18.

[14] 李铁辉，陈志兴，张清江，等. 北京正负电子对撞机重大改造工程（BEPC II）人身安全联锁门禁系统 [C] // 全国放射性流出物和环境监测与评价研讨会论文汇编，2003：544－549.

[15] 李俊刚，李铁辉，陈志兴. BEPCⅡ数字化辐射防护平台研究及应用 [J]. 核电子学与探测技术，2010，30（9）：1144－1149.

[16] Experimental Physics and Industrial Control System [EB/OL]. [2021－01－19]. https://epics.anl.gov/.

[17] S7nodave Device Support for EPICS [EB/OL]. [2021－01－19]. https://oss.aquenos.com/epics/s7nodave/,2012.

[18] Sebastian Marsching. S7nodave for EPICS Manual [EB/OL]. [2021－01－19]. https://oss.aquenos.com/epics/s7nodave/docs/2.1.4/manual.html，2012.