



LN2000 分散控制系统安全控制器(LN-PU-S)整体设计方案

山东鲁能控制工程有限公司

摘要：介绍了山东鲁能控制工程有限公司研发的 LN2000 分散控制系统安全控制器的功能、结构特点以及软硬件开发的整体设计方案，安全控制器的设计提高了 DCS 分散控制系统数据控制单元的稳定性和安全性，避免了事故的发生，对工控行业的安全运行提供了保障。

关键词：安全控制器 无扰恢复 安全存储系统

1. 概述

目前主流的 DCS 厂家的 DPU（数据控制单元），在出现严重故障，导致系统重启后，所有的数据会清零，所以主流 DCS 厂家的 DCS 系统采用 DPU 的冗余设计，来避免这种严重故障引起设备跳闸、机组停机等严重后果。但是如果出现以下类似情况也难以避免故障的发生。

- （1）供电消失，UPS 出现故障；
- （2）由于网络故障引起双 DPU 同时重启，如网络风暴，阻塞等；
- （3）一个重启另外一个还没有开始正常运行又重启；
- （4）由于接地不好电荷累计引起的双 DPU 同时重启；

山东鲁能控制工程有限公司通过市场调研在 DCS 领域提出控制器复位无扰恢复思想，研发安全控制器，通过实时保存控制器的工作参数，在控制器异常失电或发生故障复位时，即使没有备用数据站，也可以快速恢复工作现场，使得控制平稳，设备故障也可以无扰恢复，确保 DCS 在异常出现时能够快速恢复，确保工业控制信

息系统稳定、可靠运行。

2. 安全控制器的功能和特点：

2.1 系统功能

安全控制器具有不丢失快速安全存储系统，控制器运行过程中实时保存控制器工作状态，在设备故障时可以在安全存储系统中取得现场设备上一时刻的运行参数（其中包括 IO 数据，数据库、以及 SAMA 组态中数据状态信息等）。在控制器异常失电或发生故障复位时，即使没有备用数据站，也可以快速恢复工作现场，使得控制平稳，设备故障也可以无扰动恢复。

2.2 系统特点

控制器重启数据不清零。双 PU 同时重启 IO 数据不清零、数据库强制信息不清零、SAMA 组态强制信息不清零、SAMA 算法块状态数据不清零、数据库和 sama 图及监控画面所有数据和状态不清零（均保持重启时刻的值）。

单控制器运行下装数据不清零。IO 数据不清零、数据库强制信息不清零、SAMA 组态强制信息不清零、SAMA

算法块状态数据不清零。

安全控制器采用低功耗 CPU，可维护性强，无需风扇散热，极大的延长了使用寿命，提高了工作稳定性和可靠性。

安全控制器的采用的是低功耗不丢失快速安全存储系统，擦写次数无限次、读写时间 NS 级、静态工作电流 5UA，安全存储系统供电电源采用的主供电电源加后备电池的冗余结构，保证存储数据安全可靠。

3. 安全控制器系统结构设计

为实现安全控制器的实时存储功能，需要满足两方面的硬性需求首先是实时存储，数据读取和写入的速度要快。其次存储系统模块使用寿命要长，在整个控制器工作的过程中，要实时的存储数据。为了满足上述的硬性需求，采用标准的 ISA 工业总线方式，而其中电源部分则采用主供电电源加后备电池的供电的方式。

3.1 ISA 总线

ISA 总线也称为 PC 总线，采用 16 位工业标准结构总线，其寻址空间最大到 16MB，操作速度为 8MHz，数据传输率为 16Mb/S，其引线如图 3. 1. 1 所示。

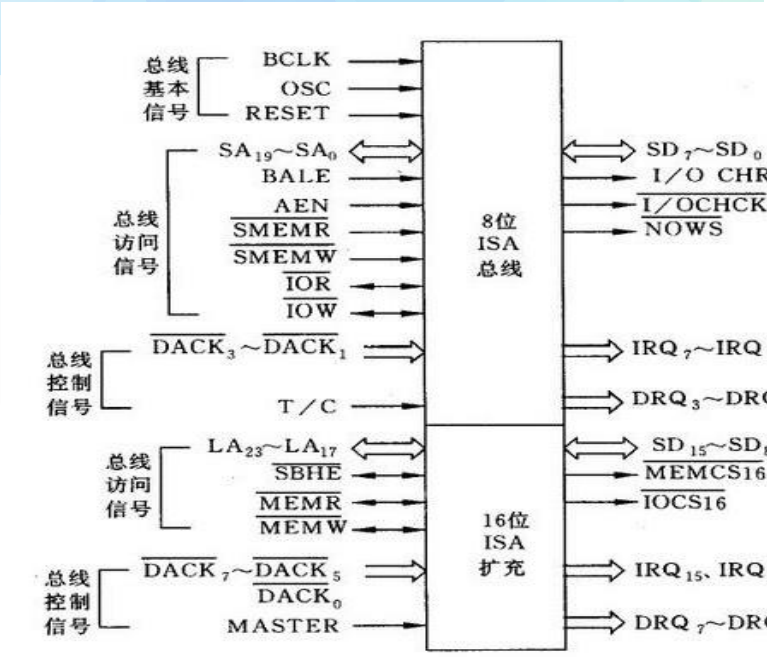


图 3. 1. 1 ISA 总线

3.2 低功耗不丢失快速存储系统

其主要具有以下特点：

- 擦写次数无限次
- 读写时间 nS 级
- 静态工作电流 5uA
- 工业级芯片

详细参数如下：

OPERATING TEMPERATURE	Vcc RANGE	SPEED (ns) 55ns:3.0~5.5V 70ns:2.7~5.5V	POWER DISSIPATION			
			STANDBY (Iccsbr, Max)		Operating (Icc, Max)	
			Vcc = 3.0V	Vcc =5.0V	Vcc = 3.0V 70ns	Vcc =5.0V 70ns
+0° C to +70° C	2.4V ~ 5.5V	55 / 70	5uA	30uA	24mA	58mA
-40° C to +85° C	2.4V ~ 5.5V	55 / 70	10uA	60uA	25mA	60mA

图 3. 2. 1 系统参数

3.3 供电方式

为实现掉电存储数据不丢失，采用主供电电源加后备电池的方式来实现。

- 主电源供电时，后备电池不供电，工作时长没有任何限制
- 主电源丢失，后备电池供电，采用 CR2032 电池，其标称容量为 240mAh，理论工作时长为 $(240 \times 1000) / 5 / 24 / 365$ 即 5.47 年的时间。
- 主电源和后备电池同时出现问题时，数据也可以保持 350S 左右时间，因为在存储模块的供电端采用了一颗具有极低 ESR 特性的滤波电容，起到了类似于 UPS 的作用，可以存储一定的电量来保持安全存储系统中的数据不丢失。

4. 安全控制器的软件结构

安全控制器软件部分实现了功能配置，数据的冗余备份存储，数据读取时的校验等功能。流程图见 4.1

- 功能配置：安全控制器可以在上电初始化阶段配置该功能是否启用，以及数据保存的有效时长。
- 数据的备份存储：为了保证数据的准确，可靠性，采用冗余备份的方式即将需要保存的数据，保存到两个不同的存储分区中。并且在数据存储过程中添加相应的校验处理。
- 数据读取过程：读取数据采用特定校验方式，来保证数据的准确性。

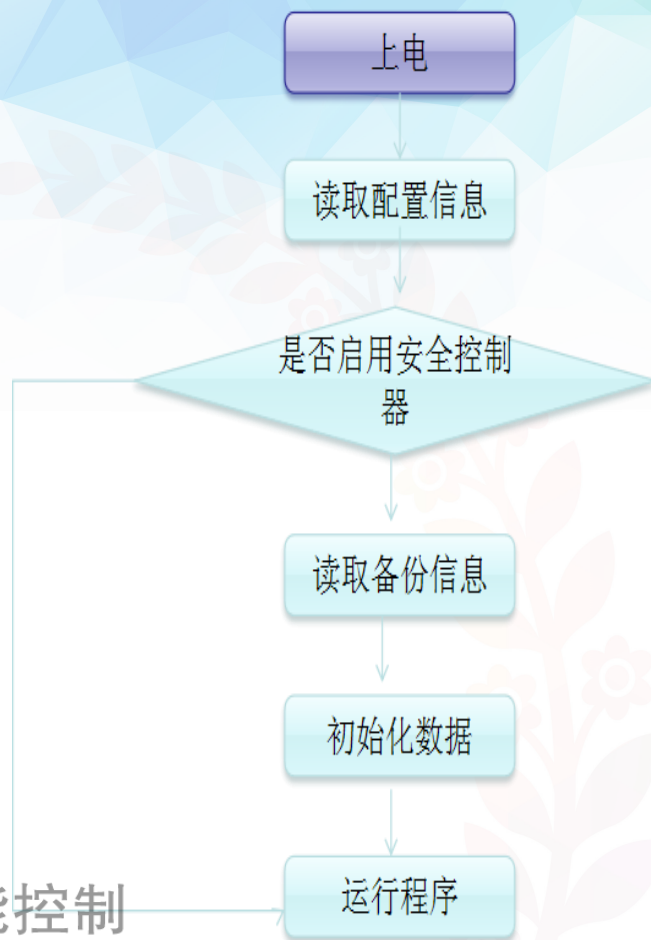


图 4.1. 安全控制器软件流程

结束语：

LN2000 分散控制系统安全控制器通过实时保存控制器的工作参数，在控制器异常失电或发生故障复位时，即使没有备用数据站，也可以快速恢复工作现场，使得控制平稳，设备故障也可以无扰恢复，确保 DCS 在异常出现时能够快速恢复，现已在多个项目中应用，产品运

行稳定可靠。

参考文献

- (1) LN2000 分散控制系统使用说明书
- (2) 安全控制器使用说明书

有关更多信息

想要了解更多鲁能控制 DCS 分散控制系统的产品、技术与服务信息，请访问公司网站：

www.lnkz.com

或拨打咨询电话：0531-87526166、87526966

或扫描二维码关注公司微信公众账号，了解更多最新资讯：



鲁能控制

LUNENG CONTROL

鲁能控制公司版权所有，内容如有更改，恕不另行通知。