王牌冷气

轨道车辆空调系统 SIL2 级安全认证

所属部门 Responsible Division	文件类型 Document Type	CP 编号 CP Number	项目代号 Project Number
研发中心 R&D Department	技术方案	/	/

编制 Written by：

校对 Checked by:

审核 Reviewed by:

批准 Approved by:

签字（Signature）　　日期（Date）

内部文件编号 Internal Document No.

TPR002852

客户文件编号 Customer Document No.	版本 Rev.	客户代号 Customer Code
/	C.1	/

石家庄国祥运输设备有限公司

王牌冷气

历史记录

Revision Log

版本 Revision	更改描述 Description	作者 Author	日期 Date
A	初版	郝腾飞	2020.11.05
B	增加方案说明	郝腾飞	2020.11.27
C	修改 6/8 章节部分内容，增加第 7 章节	陆倩	2020.11.27

目录

1 概述 3
2 要求 3
3 功能简述 3
3.1 紧急通风 3
3.2 车外火灾模式 3
3.3 车内火灾模式 4
3.4 功能安全等级要求 4
3.5 交付物基本要求（不限于下述） 4
4 初步方案说明 5
5 咨询公司要求 5
6 咨询认证方案基本要求 6
6.1 文档工作 6
6.2 培训工作 10
6.3 方案咨询工作 11
6.4 预评估工作 12
7 专家指导服务 12
8 服务技术团队人员保障 12
9 合同及其他事项 12

1 概述

石家庄国祥运输设备有限公司（以下简称“国祥公司”）将对轨道车辆空调系统进行安全评估，安全评估主要依据的标准为 EN50129，EN50128，EN50126 等。

石家庄国祥运输设备有限公司位于：河北省石家庄市高新区长江大道 255 号。

本方案联系人如下：

郝腾飞：

Tel：0311-89912759

Email：tengfei.hao@guoxiang.com.cn

2 要求

国祥公司将邀请第三方咨询公司协助完成安全认证工作，咨询公司应提供相应的咨询服务和认证服务，确保国祥公司顺利通过 SIL2 认证，此次安全认证工作国祥公司将会根据需要开发新的空调控制器硬件平台和软件平台，安全认证服务覆盖空调内部/外部火灾模式和紧急通风，含空调控制器硬件系统认证等级为 SIL2（CNAS），最终取得空调相应等级的 SIL 独立安全评估证书和报告。

3 功能简述

以下涉及空调系统安全认证的功能（空调内部/外部火灾模式，紧急通风）的描述为空调系统在轨道车辆上的常见逻辑，以下描述仅作为方案和报价参考，最终逻辑实现以认证过程实际需求为准。

3.1 紧急通风

x 台空调机组检测到 AC380 电源故障，自动切至紧急通风回路，延时 xx 秒（此逻辑可通过时间继电器等硬件实现），紧急通风接触器吸合，并给逆变器启动信号，通风机工作在紧急通风模式。

回风阀关闭/打开，新风阀关闭/打开。（此部分逻辑可通过硬线实现）

3.2 车外火灾模式

烟雾探测器检测到车外烟雾浓度超过阈值后，输出车外火灾信号，控制器对车外火灾信号滤波时间为 x 秒，收到车外火灾信号后延时 xx 秒，控制器新风压力波阀、废排压力阀、新风阀、废排风阀关闭/打开，回风阀关闭/打开。模式转为停机/通风/自动。

3.3 车内火灾模式

收到车辆火灾硬线信号，控制器对车内火灾信号的滤波时间为 x 秒，延时 x 秒（此逻辑可通过时间继电器等硬件实现），切断压缩机、电加热、冷凝风机、通风机等接触器线圈或变频器使能管脚，部件停机（此部分逻辑可通过硬线实现）；延时 y 秒（此逻辑可通过时间继电器等硬件实现），控制新风阀关闭/打开，回风阀关闭/打开（此部分逻辑可通过硬线实现）。

3.4 功能安全等级要求

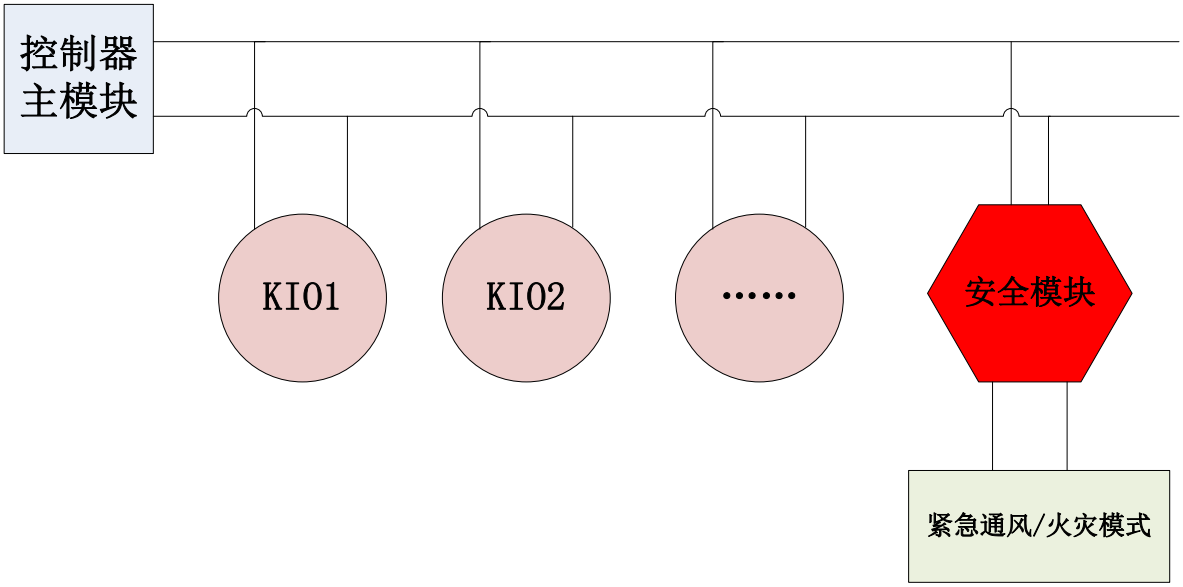
安全功能	SIL 要求
紧急通风模式	SIL2
车外火灾模式	SIL2
车内火灾模式	SIL2

3.5 交付物基本要求（不限于下述）

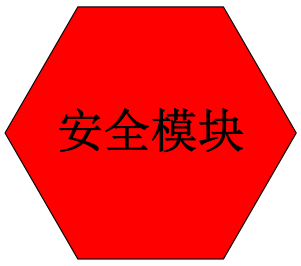
- ✓ 开口项清单
- ✓ 项目月报
- ✓ 证书
- ✓ 评估报告
- ✓ 审核报告
- ✓ 评估记录

4 初步方案说明

根据国祥公司空调系统 SIL2 安全认证过程的需要，国祥公司可开发平台型的产品用于将来的项目应用，初步规划此次满足 SIL2 认证要求的平台架构如下：



根据以上方案展示，国祥公司本次空调系统 SIL2 安全认证的主要对象是“安全模块”其特点如下：



- ✓ 无操作系统
- ✓ 功能参数可配置
- ✓ 硬件/软件与其他模块高度隔离

国祥公司空调控制器软硬件平台说明：

- ✧ 硬件：STM32 系列单片机
- ✧ 软件：C 语言

5 咨询公司要求

根据以上要求及方案展示，咨询公司需准备咨询认证方案以及报价，如对以上方案有任何疑问的可与方案联系人联系，国祥公司将采用招标的方式进行咨询公司选定。

中标的咨询公司将与国祥公司签订合同，相关咨询认证工作须在合同中详细描

述。

参标的咨询公司需提前准备以下资料和信息：

- ✧ 公司简介（宣传页）以及行业业绩（打印）
- ✧ 咨询认证方案（打印）
- ✧ 报价（无需打印，现场竞标时使用）

6 咨询认证方案基本要求

中标的咨询/认证公司在合同中的工作需要覆盖（但不限于）以下基本要求（最终方案以双方签订最终合同为准，文档以最终评估认证方确认为准）

6.1 文档工作

阶段	文件名称	甲方	乙方
系统定义阶段	项目开发计划	根据项目实际对初版进行完善	提供初版及最终完善确认
	质量保证计划	根据项目实际对初版进行完善	提供初版及最终完善确认
	软件质量保证计划	根据项目实际对初版进行完善	提供初版及最终完善确认
	软件质量保证计划验证报告	-	编制完善
	系统定义	根据项目实际对初版进行完善	提供初版及最终完善确认
	安全计划	根据项目实际对初版进行完善	提供初版及最终完善确认
	RAM 计划	根据项目实际对初版进行完善	提供初版及最终完善确认
	配置管理计划	根据项目实际对初版进行完善	提供初版及最终完善确认
	验证计划	根据项目实际对初版进行完善	提供初版及最终完善确认
	确认计划	根据项目实际对初版进行完善	提供初版及最终完善确认

阶段	文件名称	甲方	乙方
	软件编码规范	提供初稿	完善确认
	系统定义阶段验证报告	-	编制完善
风险分析阶段	危害记录册	根据模板编写初稿	提供模板及最终完善确认
	初步危害分析	根据模板编写初稿	提供模板及最终完善确认
	风险分析阶段验证报告	-	编制完善
系统需求阶段	系统需求说明书	根据模板编写初稿	提供模板及最终完善确认
	系统需求测试说明书	根据模板编写初稿	提供模板及最终完善确认
	系统危害分析(SHA)	根据模板编写初稿	提供模板及最终完善确认
	接口危害分析(IHA)	根据模板编写初稿	提供模板及最终完善确认
	操作与支持危害分析(O&SHA)	根据模板编写初稿	提供模板及最终完善确认
	系统需求阶段验证报告	-	编制完善
	系统需求阶段安全审核报告	-	编制完善
系统架构设计阶段	系统架构设计说明书	根据模板编写初稿	提供模板及最终完善确认
	系统集成测试说明书	根据模板编写初稿	提供模板及最终完善确认
	系统架构设计阶段验证报告	-	编制完善
硬件需求阶段	硬件需求说明书	根据模板编写初稿	提供模板及最终完善确认
	硬件测试说明书	根据模板编写初稿	提供模板及最终完善确认

阶段	文件名称	甲方	乙方
	设计实效模式及影响分析(DFMEA)	根据模板编写初稿	提供模板及最终完善确认
	事件树分析(FTA)	根据模板编写初稿	提供模板及最终完善确认
	型式试验大纲	提供初稿	完善确认
	硬件需求阶段验证报告	-	编制完善
硬件设计阶段	硬件设计说明书	根据模板编写初稿	提供模板及最终完善确认
	单板电原理图	提供初稿	完善确认
	单板 PCB 文件	提供初稿	完善确认
	型式试验报告	提供初稿	完善确认
	硬件设计阶段验证报告	-	编制完善
软件需求阶段	软件需求说明书	根据模板编写初稿	提供模板及最终完善确认
	整体软件测试说明书	根据模板编写初稿	提供模板及最终完善确认
	软件需求阶段验证报告	-	编制完善
软件架构设计阶段	软件架构设计说明书	根据模板编写初稿	提供模板及最终完善确认
	软件接口说明书	根据模板编写初稿	提供模板及最终完善确认
	软件集成测试说明书	根据模板编写初稿	提供模板及最终完善确认
	软硬件集成测试说明书	根据模板编写初稿	提供模板及最终完善确认
	软件架构设计阶段验证报告	-	编制完善
软件组件设计阶段	软件组件设计说明	根据模板编写初稿	提供模板及最终完善确认
	软件组件测试说明	根据模板编写初稿	提供模板及最终完善确认

阶段	文件名称	甲方	乙方
	软件组件设计阶段验证报告	-	编制完善
	软件源代码	提供	-
	软件源代码验证报告	-	编制完善
软件组件测试阶段	代码走读报告	根据模板编写初稿	提供模板及最终完善确认
	软件组件测试报告	根据模板编写初稿	提供模板及最终完善确认
软/硬件集成测试阶段	软件集成测试报告	根据模板编写初稿	提供模板及最终完善确认
	软件硬集成测试报告	根据模板编写初稿	提供模板及最终完善确认
整体软件测试阶段	整体软件测试报告	根据项目实际对初版进行完善	提供初版及最终完善确认
	软件确认报告	根据模板编写初稿	提供模板及最终完善确认
硬件测试阶段	硬件测试报告	根据模板编写初稿	提供模板及最终完善确认
系统集成测试阶段	系统集成测试报告	根据模板编写初稿	提供模板及最终完善确认
系统需求测试阶段	系统需求测试报告	根据模板编写初稿	提供模板及最终完善确认
	测试缺陷报告	根据模板编写初稿	提供模板及最终完善确认
	测试阶段验证报告	-	编制完善
	测试阶段安全审核报告	-	编制完善
确认阶段	安全例证报告	根据项目实际对初版进行完善	提供初版及最终完善确认
	系统确认报告	根据项目实际对初版进行完善	提供初版及最终完善确认
	工具确认报告	根据项目实际对初版进行完善	提供初版及最终完善确认
	例行试验大纲	提供初稿	完善确认
	例行试验报告	提供初稿	完善确认
	确认阶段验证报告	-	编制完善
	确认阶段安全审核报告	-	编制完善
部署阶段	发布和部署计划	根据模板编写初稿	提供模板及最终完善确认
	部署手册	根据模板编写初稿	提供模板及最终完善确认

阶段	文件名称	甲方	乙方
	发布单	根据模板编写初稿	提供模板及最终完善确认
	部署记录	根据模板编写初稿	提供模板及最终完善确认
	部署阶段验证报告	-	编制完善
维护阶段	问题日志	根据模板编写初稿	提供模板及最终完善确认
	维护计划	根据模板编写初稿	提供模板及最终完善确认
	维护记录	根据模板编写初稿	提供模板及最终完善确认
	变更记录	根据模板编写初稿	提供模板及最终完善确认
	用户手册	根据模板编写初稿	提供模板及最终完善确认
	维护阶段验证报告	-	编制完善
其他	各阶段质量检查记录表	-	编制完善
	各阶段技术评审记录表	-	编制完善

注：

甲方负责编制相关的文件，乙方需对文件进行完善和确认，保证文件的正确性，通过审核方的认证。

初版指乙方为甲方项目专供的一份完善度高的文档，但不涉及一些项目具体的信息；

初稿指针对产品编制的文件；

模板指乙方提供业内专业的安全保证文档模板。

6.2 培训工作

为帮助甲方能够对相关标准有充分的理解和认识，乙方须本着以下原则对甲方实时进行相关培训工作：

- 循序渐进，系统化原则。
- 理论结合实际原则。
- 授课与技术交流结合实施原则。

培训内容应该覆盖（不限于）标准培训、专题培训和案例分析。

1. 标准培训

通过对 EN5012X 系列标准的分析，帮助甲方项目团队掌握 SIL 相关标准的基本要求，初步了解与 SIL 认证相关的标准，理解满足 SIL 认证产品的基本要求。

2. 专题培训

通过对专题的培训与技术交流，帮助甲方安全认证项目团队掌握标准对安全相关的要求，比如与安全相关的需求，安全原理，安全通信原理，软件安全编码，危害识别结束，故障树分析等（具体专题可根据项目情况制定）

3. 案例分析

通过具体的案例与甲方安全认证项目团队现在正在研发的产品进行分析，以及结合标准中对 SI L 认证涉及的技术要求与非技术性的要求（各种方面的管理求）建立文件模板，并对模板进行分析解读，可以在加深标准理解的同时，减少被评估方对文件模板的探索的工作量。

文档工作的每个阶段需提供不少于一次的现场专题培训和案例分析，以帮助甲方能够更好的完成体系建立和文档编制工作。

6.3 方案咨询工作

基于目前甲方项目组团队 SIL 项目经验，需中标的咨询/认证公司与甲方深入讨论定制各个阶段方案（实际方案咨询工作可根据项目需要增减）：

序号	咨询选项	咨询内容
1	项目组织结构独立性及职责划分	结合项目组实际情况，确认人员组织结构及 SIL2 认证独立性要求，包含软件设计，硬件设计，质量，安全，测试，项目管理等。
2	系统认证范围界定	确认空调系统的认证范围，包含系统功能，通讯协议，系统边界，系统架构，安全功能的划分。
3	应用配置方案设计	根据项目实际情况，划分通用配置及特定配置信息，应确认配置方案，包含通用及特定配置数据的设计和实现。
4	软件设计方法交流	软件模块化设计工具及方法，安全通讯协议的设计等软件设计方法咨询。

序号	咨询选项	咨询内容
5	测试流程及技术	测试用例设计方法，软件测试工具，故障注入测试技术等方法咨询。
6	硬件设计方法交流	根据项目情况，提供硬件安全设计要素如硬件安全架构定义、硬件安全输出等

6.4 预评估工作

乙方需向甲方提供预评估服务，在正式评估前，即文档预审核和安全保障活动预评估，主要是根据甲方公司现有的、已完成的或计划实施的项目技术方案、技术和管理相关的文档状态以及项目安全组织框架和安全管理活动进行预评估。具体、真实、客观、全面地说明甲方的技术文档与安全管理活动等与评估目标可能存在的所有差距，输出预评估意见。

7 专家指导服务

甲方为乙方提供专家指导服务，主要包括内容如下：

1. 对认证提出的意见提供针对性的整改建议；
2. 根据甲方的项目进展提供现场专家辅导服务；
3. 对于甲方非现场的以邮件、电话或其余通讯方式的任何请求，乙方咨询师应给予长期的免费咨询答疑（自合同签订起至认证通过后三年）

8 服务技术团队人员保障

乙方团队稳定性承诺，项目主要成员应为公司资深咨询认证工作人员，稳定性好；

乙方参与咨询的主要成员在签订合同前，应与甲方安全团队进行远程或面对面沟通了解，在执行过程中，如因特殊原因需要更换老师时，需要获得甲方的同意。

项目组所有成员均应为乙方公司专职人员，咨询服务时间有保障。

9 合同及其他事项

根据本方案基本要求，乙方须在合同中将本项目的实施方案和计划详细列述并得到甲方的确认，最终实时方案和计划以合同签订为准。