# **车载地震紧急处置装置SIL安全认证**

# **服务需求****及技术规格**

1. **安全评估内容**
2. **系统范围**

车载地震紧急处置装置接收高速铁路地震预警监测系统通过GSM-R网络发送的紧急处置信息，根据警报级别的不同，通知司机施加最大常用制动或自动施加紧急制动。车载装置具有向司机发送语音、显示报警以及撤销语音、显示报警功能。在操作终端设有数据存储介质，可对事件数据进行存储，通过外接U盘或通过计算机互联将数据导出。车载地震装置由车载地震主机、车载地震终端及天线等组成，如下图所示。



图1 装置结构示意图

车载地震主机分别安装在动车组两端车载设备间，包括：IP地址查询与更新、基于GPRS方式的状态报告发送、基于GPRS方式的紧急处置信息接收及应答、自动触发紧急制动处置、警报解除、误报解除和震后恢复处置、制动控制解除、继电器状态回采、状态表示、隔离、自检、复位、远程检测、基于小区广播方式接收心跳报文（预留）、基于小区广播方式的紧急处置信息接收（预留）等功能。

车载地震终端安装在司机室控制台，包括：紧急处置输出表示、显示报警、语音报警、警报接收确认、制动控制解除、内部时钟、参数设置、车号端位写入、工作状态表示、语音提示、自检、复位功能、文档管理、协议转换、信息记录、数据格式化存储、文件存储、文件导出、文件删除、系统信息查看、日志查询等功能。

1. **评估范围**

依据本项目CARS的开发范围，本次评估范围为车载地震紧急处置装置。包含以下安全相关的功能：

1. 实时接收经GSM-R网络发布的地震警报信息、地震警报解除和恢复行车信息等。
2. 根据地震警报信息的不同等级，根据预先分析和预设计的安全原则，采取必要的安全处置措施，实现快速控车，使列车处于安全的状态。
3. 根据地震警报解除信息和恢复行车信息，采取相应的安全恢复措施，使得列车按相关规定恢复正常行车。

被评估系统的边界是：与动车组制动系统等的接口。

基于初步分析，该产品的功能失效均可能直接造成安全关键性影响，其安全完整度等级要求至少达到动车组制动系统SIL2的安全等级。这些安全功能的安全完整度等级最终定义还需要进一步对该产品进行分析。

1. **资格与能力要求**

1、安全评估行业资质

铁路产品(项目)安全评估机构应具有国际互认或所在国家级认证认可机构授予的ISO17065（项目）认证资质或许可（其中包括对EN50126、EN50128、EN50129的标准符合性的评估），并提供许可证书的标明许可范围的附件。

2、特殊能力

铁路产品安全认证机构应具有本地化的技术服务资质与能力，且具有被评估产品或项目相关的专业背景和业务经验。

3、保密要求

铁路产品安全认证机构应具备保密能力。对于从客户处得到的与服务有关的所有技术信息和操作资料，除非法律另有规定或客户另有要求或者履行合同项下服务所需，否则认证机构对此应采取保密措施，并不得使用或向任何第三方披露。

当项目有特殊要求时，可以根据客户的要求，对产品提交的敏感信息进行特殊的约定。

4、成功案例要求

1) 铁路产品安全评估机构应至少具备5项高铁和CTCS或ETCS信号系统SIL4评估的国际或国内产品的评估经验，且评估后的产品应用在实际项目中的使用时间不得少于3年。

2) 具有至少一项车载地震紧急处置装置相关的安全分析、安全咨询或安全评估的经验。

5、评估团队要求

主要评估人员需具备10年或以上、其他参与项目的评估人员需具备6至8年的SIL4安全产品的评估经验。

项目团队在现场从事评估活动的天数不得少于总服务天数的80%。

参与本项目评估的主要评估员应在对项目执行中的疑问进行及时响应，包含及时的面对面沟通，主要评估员面对面技术沟通的响应时间最长不应超过2天。

最终安全评估证书需被国际认可。

1. **合作模式**
2. 评估服务建议书

由评估公司提供评估服务建议书，评估服务建议书包括内容：

* 1. 简介；
  2. 评估方法，包括：概述、评估要求、系统描述、评估范围、评估流程、评估计划和进度、评估成果、售后和维保（若有）等内容；
  3. 项目组织及关键资源，包括：评估团队(含人员资质)、项目管理等方面；
  4. 付款计划；
  5. 质量管理等保障；
  6. 业绩证明。

1. 评估计划

合同签订后，评估机构提供评估计划，对评估的范围、内容、进度进行详细计划。

1. 评估问题交互

通过审核记录，对审核发现的问题及解决方式和状态进行记录。

1. 现场审核

评估期间进行1-2次现场审核。

1. 测试见证

根据需要对评估产品的测试活动进行见证。

1. 提交评估证书和报告

最终根据评估结果出具评估证书和评估报告。

1. **质量保证**

1、评估遵循的标准

适用的标准/法规/规范包括但不局限于下列各项：

* 1. EN 50126: 1999 – 铁路应用 –铁路设备可靠性、可用性、可维修性和安全性（RAMS）的规范和说明
  2. EN 50128: 2011 – 铁路应用 -通信、信号传输和处理系统铁路控制和保护系统软件
  3. EN 50129: 2003 – 铁路应用 -通信、信号和处理系统-信号的安全相关电子处理系统
  4. EN50159: 2010 – 铁路应用–通信、信号和处理系统-传输系统内的安全相关通信

参考标准与规范如下：

* 1. IEC 61508-2:2000–电子/电气/可编程电子安全相关系统的功能安全-第二部分：对电子/电气/可编程电子安全相关系统的基本要求
  2. 铁总科技 2015 9号 - 中国铁路总公司关于印发《车载地震紧急处置装置暂行技术条件》的通知

2、售后保障要求

在符合如下诸条件时，评估方可对原项目被评估对象的小型变更和升级继续提供补充评估服务：

1. 证书中遗留的限制条件，在项目完成后有新的证据补充时，根据证书更新相关评估成果；
2. 产品认定时，由于认定原因而进行的证书、评估报告等的配合工作；
3. 根据特定要求进行产品的变更升级的补充评估等维保工作。

其中a)、b)为必须考虑的条款，c）为可作为优选条件考虑的条款。

1. **交付与验收**

1、阶段性付款

根据项目阶段付款计划支付；如果项目比计划提前完成，则评估方在项目结束时，支付所有剩余项目款。项目阶段付款的条件是在过去3个月内评估方没有因为自身原因导致评估项目延期或未完成评估方应该完成的评估工作。

2、最终成果

1. 评估方提供的阶段性评估确认函
2. 最终的评估证书和评估报告
3. 维保过程中提供的确认函或评估证书、评估报告
4. 项目重大问题总结

3、工作语言及证书语言

1. 文件提交以中文为主，若需翻译成外文文件，由评估方承担。
2. 评估方应提供评估证书、相关报告、确认函的原文版及中文版。