# 城市轨道交通车辆系统安全完整性等级分析

付世亮
（中车浦镇庞巴迪运输系统有限公司,241060,芜湖//工程师）

**摘　要**　介绍了轨道交通车辆系统安全完整性等级（SIL）的定义、分级和分配方法,论述了 SIL 在城市轨道交通全自动运行系统设计中的重要性。提出了一种基于风险图对轨道交通车辆系统进行 SIL 分析的模型和方法,并详细介绍了该方法在轨道交通车辆系统 SIL 分配中的应用过程。

**关键词**　城市轨道交通；车辆；安全完整性等级；风险图
**中图分类号**　U298.1+1:U266
DOI:10.16037/j.1007-869x.2019.10.018

## Safety Integrity Level Analysis of Urban Guided Transport Vehicle System

FU Shiliang

**Abstract**　The definition, classification and distribution method of safety integrity level (SIL) for urban rail transit vehicle system are introduced, the significance of SIL in the design of urban rail transit fully automation operation system is elaborated. Then, a model and method of SIL analysis for urban rail transit vehicle system based on risk map is proposed, the application of this method in the distribution of SIL for urban rail transit vehicle system is elaborated in details.

**Key words**　urban rail transit; vehicle; SIL; risk map

**Author's address**　CRRC PuZhen Bombardier Transportation Systems Ltd., 241060, Wuhu, China

与常规的轨道交通相比,全自动运行的轨道交通系统更强调系统的可用性和安全性,要求关键运行设备采用冗余设计,减少运行故障,并在满足系统正常运行的前提下,具备较强的抗干扰能力及故障恢复能力。因此,针对全自动运行线路车辆系统的安全也提出了新的需求。

国际标准 IEC 61508—2010[1] 和欧洲电工标准化委员会（CENELEC）制定的 EN 50126-1—2017[2]、CLC/TR 50126-2—2007[3]、EN 50657—2017[4] 等铁路安全防护标准都提出了安全相关系统的“安全完整性等级（Safety Integrity Level,简称 SIL）”概念。目前轨道交通行业非全自动运行系统中,主要围绕信号系统中涉及的安全功能提出了 SIL 要求。信号系统主要基于风险图方法来确认系统的 SIL[5]。

本文通过对轨道交通车辆系统的风险辨识、安全功能、安全完整性、安全要求等方面的内在联系进行分析,提出了一种基于风险图进行车辆系统 SIL 分配的方法。

## 1　安全完整性等级（SIL）

IEC 61508—2010 标准将 SIL 定义为一种离散的等级,共有 4 种可能等级,分别对应不同的安全完整性量值范围。其中:安全完整性等级 4（SIL4）最高,安全完整性等级 1（SIL1）最低。EN 50126-1—2017 和 EN 50657—2017 则是将 SIL 定义为多种离散的等级,用于指定相关功能的安全完整性要求,以便分配给与之相关的安全系统。

SIL 的定义[6] 可以概括为 3 个方面:安全功能、定量指标、SIL 的分配。因此,SIL 不仅是安全相关系统开发、设计的要求,也是安全相关系统评价的依据。

### 1.1　SIL 的安全功能

唯一确保安全的功能是安全功能。安全相关功能是一种系统失效影响安全的功能,因此,所有安全功能都是与安全相关的,反之亦然。

目前,轨道交通车辆系统安全功能识别方法有 3 种:

1）常规方法:通过识别危害清单进行风险分析,从而确认其安全功能。主要的风险识别方法包括初步危害分析（PHA）、危害与可操作性分析（HAZOP）、失效模式及影响（FMEA）、检查表等。但是,常规的识别方法主要依靠人的主观判定和经验,如通过头脑风暴法、专家评审法等进行识别。由于分析人员分析经验及主观判定等的局限性,造成安全功能识别的不完整,或安全判定存在偏差。针对此问题,可采用工程文件及历史故障经验梳理相结合的方式,全面、完整地识别出轨道交通车辆

系统的安全功能。

2）根据工程文件确定安全功能。运用需求管理逐条识别工程文件(技术合同)中技术章节,通过评审识别相应的功能需求,梳理出安全功能和非安全功能。例如,轨道交通项目车辆系统的招标文件经常要求将车辆制动系统紧急制动功能的安全等级定为 SIL4。

3）根据车辆系统的历史经验确定安全功能。由于轨道交通车辆系统并非是全新设计,而是在以往项目的基础上进行改建或优化,因此,可以直接使用以前项目确认的安全功能或者过往项目的涉及到安全的故障信息,用以确定车辆系统的安全功能。

通过以上 3 种方法分析或识别轨道交通车辆的安全功能后,再进行交叉检验和完整性确认,则可全面地识别出轨道交通车辆系统的安全功能。

### 1.2　SIL 的定量指标

安全完整性是在规定时间段内和规定条件下,安全相关系统成功执行规定安全功能的概率。安全完整性越高,安全相关系统未能按要求执行规定的安全功能或未能实现规定状态的概率就越低。安全完整性由硬件安全完整性和系统性安全完整性共同构成。

IEC 61508—2010 定义了电气/电子/可编程电子类安全相关系统的功能安全,可应用在电子、宇航、汽车、原子能、化工、冶金等多个领域。该标准定义了 4 个级别的 SIL,并对“要求时危险失效平均概率”($PFD_{avg}$)这一指标进行了量化。

铁路安全防护标准 EN 50126-1—2017 则定义了“每个功能可容忍故障率”(TFFR)的概念。表 1 是 SIL 与失效概率的对应关系[2]。

**表 1　SIL 与失效概率的对应关系**

| SIL | TFFR/$h^{-1}$ | $PFD_{avg}/h^{-1}$ |
|---|---|---|
| 1 | $10^{-6} \leqslant TFFR < 10^{-5}$ | $10^{-2} \leqslant PFD_{avg} < 10^{-1}$ |
| 2 | $10^{-7} \leqslant TFFR < 10^{-6}$ | $10^{-3} \leqslant PFD_{avg} < 10^{-2}$ |
| 3 | $10^{-8} \leqslant TFFR < 10^{-7}$ | $10^{-4} \leqslant PFD_{avg} < 10^{-3}$ |
| 4 | $10^{-9} \leqslant TFFR < 10^{-8}$ | $10^{-5} \leqslant PFD_{avg} < 10^{-4}$ |

注：表中“每个功能可容忍故障率”(TFFR)及“要求时危险失效平均概率”($PFD_{avg}$)的表示方法为原标准的写法

通过表 1 对 $PFD_{avg}$ 和 TFFR 进行对比可以看出,IEC 61508—2010 同样适用于轨道交通行业,但在进行具体的应用时,需要结合 EN 50126-1—2017 对参数进行优化。

### 1.3　SIL 的分配方法

IEC 61508—2010 推荐以风险图法作为 SIL 的分配方法。风险图法最早源于德国的安全标准,主要用于考察对人员造成的影响。德国高铁监管部门基于风险图方法,也制定了可用于确定轨道交通各系统 SIL 等级的方法。

基于定性和基于分级的方法,采用可能性、后果、处于危险区域的时间(暴露时间、暴露频率)和避免危害事件的可能性等 4 个参数来确定安全完整性水平。每一个参数都已有相应的分级标准,具体定义如下:

1）后果用 $C$ 表示。基中:$C_1$ 表示发生人员轻微伤害的事件;$C_2$ 表示造成对 1 人以上造成严重的永久性伤害或个人死亡的事件;$C_3$ 表示造成多人死亡的重大事件;$C_4$ 表示造成非常多人死亡的严重事件。

2）危害区域的频率和暴露时间:用 $F$ 表示。其中:$F_1$ 表示很少在危害区域暴露;$F_2$ 表示经常在危害区域长期暴露。

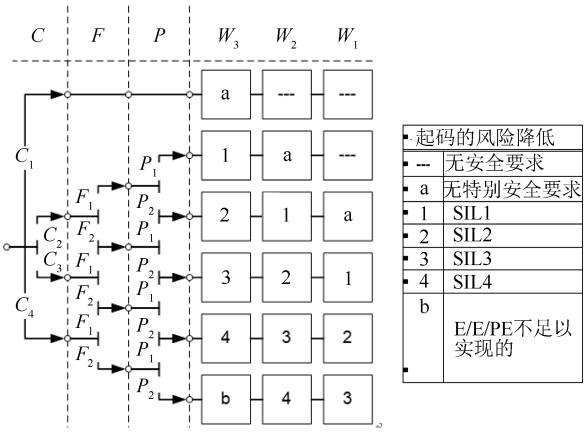
3）避免危害事件的可能性:用 $P$ 表示。其中:$P_1$ 表示在某些情况下可能;$P_2$ 表示几乎不可能;

4）不期望事件发生的概率:用 $W$ 表示。其中:$W_1$ 表示非常低,即有害事件发生的可能性非常小,只有少数有害事件可能发生;$W_2$ 表示低,即有害事件发生的可能性小,有害事件很少发生;$W_3$ 表示高,即有害事件发生的可能性相当高,可能频繁发生。

风险图法根据不同风险对人员、环境和财产的影响程度、发生频率等方面,以及人员出现频率和是否能避免事故发生等情况,确定 SIL 等级。图 1 为 IEC 61508—2010 推荐的风险图。

值得注意的是,由于铁路安全防护标准 EN 50126—2017 中第 E.10 条对风险图法的使用存在疑问,特别指出在安全完整性等级中如果采用风险图方法,其参数和类型中并没有在轨道交通行业内达成一致。

但是仅从轨道交通车辆系统角度看,车辆系统的复杂程度远低于整个轨道交通系统,而且,因车辆系统造成的危害场景和后果可以通过分析进行预判。因此,本文认为通过对风险图中 4 个参数和 SIL 定量指标的校核,风险图法可用于轨道交通车辆系统进行 SIL 分配,并可确定车辆系统各安全功能的 SIL。




注：E/E/PE为电子/电气/可编程电子安全相关系统

图 1　IEC 61508—2010 推荐的风险图

## 2　轨道交通车辆系统 SIL 分配的过程

城市轨道交通车辆系统是集合机械、电气、通信于一体的综合系统，各部分通过连接共同完成车辆系统的功能和安全功能。通常根据功能和物理架构将车辆系统分为多个子系统，如：车体、车体外部设备、车门、转向架、车内设备、空调系统、牵引辅助系统、制动系统、乘客信息系统、列车信息系统、防火安全系统等。针对车辆系统组成的复杂程度，在进行安全完整性等级分析时，需要从车辆系统顶层功能识别开始，直到明确各子系统/子功能的安全要求。整个 SIL 分配过程流程图如图 2 所示。

### 2.1　车辆系统安全功能识别

轨道交通项目车辆系统的招标文件（客户的技术规格书）中给出了部分功能需求。首先对车辆系统中相关功能并且可由 E/E/PE 执行的功能进行识别，再结合历史经验和工程经验进行查漏补缺。

对客户的技术规格书中功能列表和公司历史经验进行汇总形成功能列表后，进行交叉检查和完整性确认，使车辆系统安全功能列表更加完整。

### 2.2　危害识别

在进行车辆系统的风险分析之前，除了要确认系统安全相关控制功能之外，还需要对系统可能出现的功能性故障及由于该故障引起的危害进行分析。通常将由于车辆系统故障造成的危害等级分为 4 级：灾难性的、严重性的、次要的和轻微的。

对 IEC 61508—2010 和 EN 50126-1—2017 中严重等级的定义进行对比，表 2 列出 2 个标准间严重级别的关系。IEC 61508—2010 将重大损失分别考虑（$C_4$ 多人死亡），这主要是由于 IEC 61508—2010 还涉及到与化工、核电等行业。因此，在风险图法参数“后果 $C$”中需要校核 $C_4$ 的定义。严重等级 $C_4$ 只适用于会导致非常极端后果的危害。

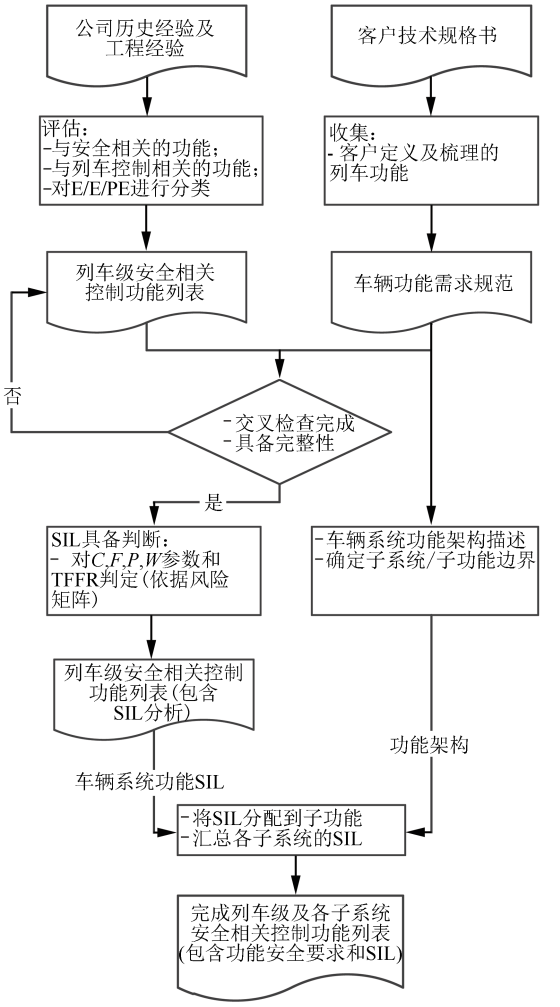



图 2　轨道交通车辆系统 SIL 分配流程图

### 2.3　风险图参数的校准

IEC 推荐的风险图法是一种定性分析方法，各参数缺少定量的指标。因此需要对风检图进行校准，为风险图的各参数进行赋值。因此，给每个参数分配 1 个指标或标准定义，使得当组合应用时，也可以对缺乏特定安全功能下存在的风险进行分析。这样做的其目的是通过某种方法描述所有参数，使分析人员或团队能根据风险图的具体应用进行客观和易于理解的判断，确保轨道交通车辆系统的 SIL 符合相应的风险准则；通过实际应用也可进一步验证参数选择的正确性。此外，这样做还确保了安全功能分配的安全完整性等级符合项目或实际的

表 2　EN 50126 和 IEC 61508 严重性级别的关系

| 严重等级 | EN 50126-1—2017 | | 严重等级 | IEC 61508—2010 | |
|---|---|---|---|---|---|
| | 对个人和环境的影响 | 对服务的影响 | | 类别 | 后果($C$) |
| I　灾难的 | 多人死亡/严重受伤/对环境造成大危害 | 列车运行服务中断 | I　灾难的 | 多人死亡<br>数人死亡 | $C_4$<br>$C_3$ |
| II　严重的 | 一人死亡/严重受伤/对环境造成危害 | 主要系统的损失 | II　严重的 | 对一人或多人造成严重的永久性伤害;个人死亡 | $C_2$ |
| III　次要的 | 多人轻微受伤/对环境造成严重威胁 | 系统的严重损坏 | III　次要的 | 轻微伤害 | $C_1$ |
| IV　轻微的 | 可能造成一人轻微受伤 | 系统的轻微损坏 | IV　轻微的 | – | – |

风险标准,并考虑了其他来源的风险。因此给每个参数赋予 1 个指标或标准定义,也可以对缺乏特定安全功能下存在的风险进行分析。表 3 列出了后果参数 $C$ 校准后的分类;表 4 列出了危害区域的频率和暴露时间参数 $F$ 校准后的分类;表 5 列出了避免危害事件的可能性参数 $P$ 校准后的分类。表 6 列出了不期望事件发生概率 $W$ 校准后的分类。

表 3　后果($C$)参数校准后分类

| 风险参数 | 校准后的表述 | 指标 |
|---|---|---|
| $C_1$ | 轻伤 | 0.01 的等值死亡 |
| $C_2$ | 对于 1 人或多人的严重的永久性损伤;1 人死亡 | 0.1 到 1 的等值死亡 |
| $C_3$ | 多人死亡 | 平均为 10 个等值死亡 |
| $C_4$ | 非常多的人死亡 | 平均为 100 个等值死亡 |

注:将对功能性故障相关事故的平均严重程度进行评估(不是最坏情况);$C_4$ 只适用于会导致非常极端后果的危害,如:两辆列车以高速相碰撞,或车辆全部着火等

表 4　危害区域的频率和暴露时间($F$)校准后的分类

| 风险参数 | 校准后的表述 | 指标 |
|---|---|---|
| $F_1$ | 极少到经常暴露在危险区中 | 暴露时间小于等于平均行程时间的 10% 或外部事件触发的事件 |
| $F_2$ | 频繁到持续暴露在危险区中 | 不满足 $F_1$ 指标的其他情况 |

注:假设 $F_1$ 为功能性故障,仅在外部事件触发时才有危险而这类事件并不经常发生

表 5　避免危害事件的可能性($P$)校准后的分类

| 风险参数 | 校准后的表述 | 指标/标准 |
|---|---|---|
| $P_1$ | 某些条件下可能 | 这种危险在超过规定时间(≈120 s)逐渐形成并显现或提供报警装置,显示安全功能已经失效 |
| $P_2$ | 几乎不可能 | 不满足 $P_1$ 指标的其他情况 |

注:$P$ 考虑了以下情况:受监督的流程操作(如由有技能或无技能人员操作)或未受监督的流程操作;危险事件的发展速度(如突然、快速);易于识别危险(如立刻识别或未通过技术措施检测);只需考虑受到影响人员避免危险的能力(因为全自动运行期间车上没有司机,主要考虑列车上的乘客)

表 6　不期望事件发生的概率($W$)校准后分类

| 风险参数 | 校准后的表述 | 指标/标准 |
|---|---|---|
| $W_1$ | 一个非常小的概率,即:几乎没有不期望事件发生 | 提供了外部风险降低设施,可降低这种事件发生的概率或列车具有单独的安全功能,从而可以避免危险 |
| $W_2$ | 一个小概率,即:只有很少的不期望事件发生 | 这种功能或者类似应用中的同类功能众所周知且已投入使用 |
| $W_3$ | 一个相当高的概率,即:不期望事件可能频繁发生 | 新功能,且相关的经验有限 |

注:确定 $W$ 时不得将功能本身的冗余作为减至 $W_1$ 的依据,只有外部风险降低或列车的独立安全功能才能考虑在内;$W$ 旨在评估意外事件发生的频率,条件为不增加任何安全相关的系统(E/E/PE 或其他技术),但应包括任何外部风险降低设施。如果列出了外部风险的降低措施,则选 $W_1$

## 2.4　车辆系统安全功能 SIL 分配应用

根据轨道交通车辆功能描述及其定义,确定车辆制动系统的主要功能为:提供减速度和维持车辆静止状态。图 3 为车辆制动系统顶层的功能框图。由图 3 可以看出,通过对车辆功能的危害分析,“使车辆降速(行车制动)”是制动系统的常规功能,并不属于安全功能;“防止故障(监测和诊断)”是制动

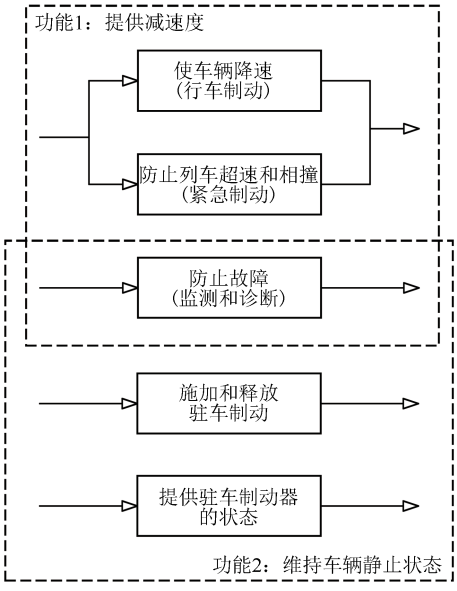



图 3　车辆制动系统的功能框图

系统的辅助功能,该功能属于安全功能。车辆制动系统的 SIL 要求为:①“防止列车超速和相撞(紧急制动)”功能应达到 SIL4;②“防止故障(监测和诊断)”功能应达到 SIL2;③“施加和释放驻车制动”的功能应达到 SIL2;④“提供驻车制动器的状态”功能应达到 SIL1;

据工程和历史经验,车辆制动系统在完成提供减速度时,“紧急制动”功能独立运行,且与行车制动并行。因此,将 SIL4 的要求分配在这 2 种功能之间。

分析和梳理车辆制动系统的子功能,包含了获取制动需求、优先考虑制动需求并选择制动模式、分配制动力、施加和缓解制动力、提供车轮滑行保护等方面。根据“防止列车超速和相撞(紧急制动)”功能应达到 SIL4 的要求,这些子功能的实现方式至少需要 1 条路径达到 SIL4 才能满足要求。

基于各子功能架构描述和确定边界,分析得到制动系统各子功能的安全完整性等级要求为:①获取制动需求:“分配制动力的列车线路径”功能应达到 SIL4,或 TFFR<$1\times10^{-8}$/h(列车线独立于列车控制与管理系统、制动控制单元和牵引控制单元);②分配制动力:“紧急制动阀施加 100%制动力(超越制动控制单元的命令)和牵引控制单元用以打开高速断路器(抑制和取消了电制动)”功能应达到 SIL4,或 TFFR<$1\times10^{-8}$/h;③施加和缓解制动力:“施加制动力(紧急制动阀)的列车线路径”功能应达 SIL4,或 TFFR<$1\times10^{-8}$/h(紧急制动阀的激活和功能独立于制动控制单元和牵引控制单元);④提供车轮滑行保护:电制动和空气制动不会在同一转向架上并行工作,“车辆滑行的时候切除电制动仅保留空气制动的硬件路径”功能应达到 SIL4,或 TFFR<$1\times10^{-8}$/h。

全自动运行系统中车辆系统承担的功能与整个运行系统的功能目标、安全功能分配、与其他系统的接口等密切相关,应从工程项目和系统角度出发对具体的车辆系统进行系统性的分析。

## 3 结语

城市轨道交通车辆系统安全完整性 SIL 的研究可为全自动运行系统中的车辆系统安全设计及评估提供依据。在新建项目的设计中,更需要识别安全功能及 SIL 的定量分析和项目特定应用的安全评估。针对全自动运行系统的其他核心设备,如综合监控、通信、站台门等,同样适用基于风险图法来确定系统的 SIL。

## 参考文献


[1] International Electrotechnical Commission. Functional safety of electrical/electronic/programmable electronic safety-related systems: IEC 61508—2010[S]. Geneva: International Electrotechnical Commission, 2010: 33.

[2] CENELEC. Railway Applications-The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)-Part 1: Generic RAMS Process: EN 50126-1—2017[S]. Brussels: CENELEC. 2017: 18.

[3] CENELEC. Railway Applications-The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)-Part 2: Guide to the Application of EN 50126-1 for Safety: CLC/TR 50126-2—2007 [S]. Brussels: CENELEC. 2007: 114.

[4] CENELEC. Railways Applications-Rolling stock applications-Software on Board Rolling Stock: EN 50657—2017[S]. Brussels: CENELEC. 2017: 14.

[5] 李彦华.轨道交通信号系统 SIL 定级实例探讨[J].铁路通信信号工程技术,2018,15(10): 91.

[6] 燕飞,唐涛,闫宏伟.安全完善度等级 SIL 的概念与划分原则研究[J].北京交通大学学报,2017,41(5): 79.


(收稿日期:2019-05-10)

## 是“跨坐式”还是“跨座式”?

科技名词和术语,反映的应是某一事物的本质特征。规范科技名词和术语,对正确理解某一事物的概念至关重要。然而,在城市轨道交通领域,“跨坐式单轨交通”这一术语中的“坐”字,究竟用“坐”还是用“座”,一直没有定论。

跨坐式单轨交通的英文原文是 straddle monorail transit。其中的 straddle,其中文释义是“跨骑”“跨坐”“叉开腿坐于”。straddle monorail transit 的本质特性,就是“列车骑跨上轨道梁在运行的单轨交通”。在中文里,“坐”字,为动词,本义是:人的止息方式之一。“座”字,为名词,本义是:座位;其对应的英文词是 seat。显然,用“跨座式”表达的是“座位”的概念,用以作为 straddle 的释义,就不甚妥当了。而用“跨坐式”,就可以很明确地表达“列车骑跨在轨道梁上运行的单轨交通”这一本质特性。 《城市轨道交通研究》编辑部