

# 安全完善度等级 SIL 的概念与划分原则研究

燕 飞<sup>1a</sup>, 唐 涛<sup>1b</sup>, 闫宏伟<sup>2</sup>

(1. 北京交通大学 a. 轨道交通运行控制系统国家工程研究中心,  
b. 轨道交通控制与安全国家重点实验室, 北京 100044; 2. 中国铁路经济规划研究院, 北京 100038)

**摘 要:**安全完善度等级(Safety Integrity Level, SIL)是标识安全相关系统安全性要求的重要概念,它主要是根据系统安全功能一旦失效可能造成后果的严重程度及事故的发生频率进行划分.在轨道交通安全相关产品的设计开发过程中,需要根据 SIL 的高低确定设计开发团队的组成和所采用的设计方法,系统的安全防护措施等.目前,我国轨道交通行业在应用 SIL 概念时,存在一些误区,比如认为 SIL 越高越好,把某个产品或是系统描述为可以达到某个 SIL 等级要求.本文基于国际轨道交通安全标准对于 SIL 的定义,澄清了一些错误使用 SIL 的概念,总结了安全完善度等级的划分原则和方法,方法包括定量和定性两种,并通过实例加以说明.

**关键词:**安全完善度等级;安全评估;风险分析;轨道交通

**中图分类号:**TP309      **文献标志码:**A

## Research on concept and allocation principle of safety integrity level

YAN Fei<sup>1a</sup>, TANG Tao<sup>1b</sup>, YAN Hongwei<sup>2</sup>

(1a. National Engineering Research Center of Rail Transportation Operation and Control System,  
1b. State Key Lab of Rail Traffic Control & Safety, Beijing Jiaotong University, Beijing 100044, China;  
2. China Railway Economic and Planning Research Institute, Beijing 100038, China)

**Abstract:** The Safety Integrity Level(SIL) is an important concept for safety related system to identify safety requirements. It is classified by the severity and frequency of the accidents caused by the failure of safety system. When designing and developing rail traffic safety related products, it is necessary to determine the developing team, their design methods and safety measures according to the level of SIL. Currently, there is some misunderstanding of the application of SIL concept in domestic rail transit industry. For example, some believe that the higher the level of SIL the better the product will be, and some describe a product or system as meeting the requirements of certain SIL. This paper describes the definition of SIL using international rail transit standard. It clarifies some incorrect use of the concept of SIL and introduces the definition, classification and determination methods of SIL, which includes quantitative and qualitative methods. Finally the paper illustrates these methods through application cases.

**Keywords:** safety integrity level; safety assessment; risk analysis; rail transit

收稿日期:2016-09-26  
基金项目:中国信息安全评测中心项目(CNITSEC-KY-2016-01);北京市教委项目(W16H100030)  
Foundation items: China Information Technology Security Evaluation Center Project (CNITSEC-KY-2016-01); Beijing Municipal Education Commission Project(W16H100030)  
第一作者:燕飞(1980—),男,安徽怀远人,副教授,博士.研究方向为轨道交通系统安全保障和评估.email: fyan@bjtu.edu.cn.  
引用格式: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—84.  
YAN Fei, TANG Tao, YAN Hongwei. Research on concept and allocation principle of safety integrity level[J]. Journal of Beijing Jiaotong University, 2017, 41(5): 79—84.(in Chinese)

安全完善度等级(SIL)是描述安全苛求系统安全功能要求高低的重要指标,是开展轨道交通安全苛求系统设计和评估工作的重要依据.在实际应用过程中,SIL 又是最容易被误解或是错误使用的一个术语.

SIL 这个概念需要和安全苛求系统所实现的安全功能相对应,可是在表达 SIL 等级时,通常会说某个产品或是某个系统达到 SIL2 或是 SIL4 级.有的时候设备供货商为了说明自家的产品安全质量水平高,一味地宣传自己的产品能够达到 SIL4 级,即最高安全等级要求,还有的厂家将不涉及安全功能的产品宣传为满足某个 SIL 等级要求.这些错误使用 SIL 概念的情况不仅给大家带来了困扰,还可能会影响我们国家轨道交通行业安全保障工作的开展.

为此,本文作者认为非常有必要说明一下国际标准对于 SIL 是如何定义的,应当如何正确使用 SIL 这个概念.

1 CENELEC 标准中 SIL 的定义

在欧洲各国家所实施的安全标准与技术之上,结合 IEC61508 国际标准<sup>[1]</sup>,欧洲电工标准化委员会(CENELEC)制定了 EN50126<sup>[2]</sup>、EN50129<sup>[3]</sup>与 EN50128<sup>[4]</sup>等铁路安全防护标准.

要求在明确系统的定义后,要辨识可能出现的危险.分析这些危险涉及的风险.随后,辨识出危险控制措施:即安全措施,安全功能或降低风险的措施.并为针对安全功能衍生出相应的安全需求.如何针对系统安全功能推导出这些要求,过程中可能涉及安全完善等级的分配,简称 SIL.

在铁路领域,存在不同的对 SIL 概念的理解和应用,这可能会引起误解和误用.如 SIL 实际上对于运营商或供应商的含义是什么,应当被应用到功能或系统元素,或只等同于故障率等.

基本上,SIL 应用于系统功能,如安全相关系统实现的安全功能.SIL 可由风险评估产出,为后来在系统开发过程中使用.由运营商确定 SIL,把 SIL 作为容许的危险率(Tolerable Hazard Rate,THR)的区间,THR 表示可容忍危险侧故障率.针对运营商制定具体一套措施和技术设备,来实现预定安全目标.研发过程中,可以理解为系统供应商对设计实现的系统安全完善水平的预测,如图 1 所示.

而在 CENELEC 标准中,将安全完善度定义为:在安全系统中保障系统安全的能力.SIL 是其定量指标,用来表现系统所要求的安全性完善水平.根

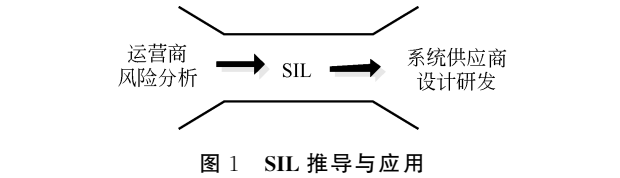


图 1 SIL 推导与应用

Fig.1 SIL derivation and application

据安全功能失效的频率及失效后产生危险严重程度将安全完善度划分 SIL1—SIL4 的 4 个等级,不同等级的定量要求如表 1 所示.

注意的是,不同的自动化等级具有的不同的功能对应的安全要求,这是风险分析和系统 SIL 分配的先决条件.

表 1 安全完善度等级

| Tab.1 Safety integrity level |                              |
|------------------------------|------------------------------|
| SIL                          | THR(每小时单个功能)                 |
| 4                            | $\geq 10^{-9}$ 至 $< 10^{-8}$ |
| 3                            | $\geq 10^{-8}$ 至 $< 10^{-7}$ |
| 2                            | $\geq 10^{-7}$ 至 $< 10^{-6}$ |
| 1                            | $\geq 10^{-6}$ 至 $< 10^{-5}$ |

1.1 系统安全完善度的概念

某一具体系统要求可以分为:安全要求和非安全要求.安全要求又分:安全功能要求和安全完善度要求.安全功能要求是指系统要实际实现的安全相关功能;每个安全功能所要求的安全完善度等级则由安全完善度要求规定,如图 2 所示.

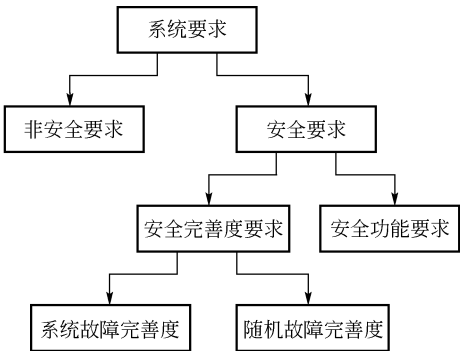


图 2 安全完善度要求

Fig.2 SIL requirements

1.2 影响安全功能的因素

安全相关功能完善性受系统失效、随机失效和外部影响三项因素影响<sup>[5]</sup>.系统安全依赖于系统所采用的预防或容忍系统失效及控制随机故障的适当措施.要达到系统足够高的 SIL,需要兼顾系统失效安全完善度以避免系统失效,随机失效安全完善度以控制随机失效,从而保证系统安全性的实现.

1) 系统故障完善度.

它在安全完善度中是一个非定量的部分,它与系统的软硬件的系统故障有关,通常是由整个生命周期内人为因素造成的.因此,系统故障完善度是需要通过质量管理和安全管理来达到的,同时在技术上给予相应的要求.

2)随机故障完善度.

它是随机故障相关的安全完善度的部分,它是系统硬件可靠性的体现.随机故障完善度是通过安全技术措施达到的.随机故障完善度的定量评估就是进行系统风险和危害可能性的计算,在计算前必须知道整个系统或设备的硬件器件的故障失效率 and 相应的故障模式.

英国黄页第 4 版<sup>[6]</sup>给出了冗余结构实现 SIL 的方案,如表 2 所示,前提条件是:低等级的功能物理上独立且使用了不同的设计原则;如果其中一个较低等级的功能失效,此连接器将抑制由此失效导致的所有危险源;连接器需继承最高的 SIL.

表 2 连接器机制可接受 SIL 分配表

Tab.2 SIL allocation for connector

| 最高的 SIL | 下一级安全功能的 SIL |      | 连接器  |
|---------|--------------|------|------|
|         | 主要           | 其他   |      |
| SIL4    | SIL4         | 无    | 无    |
|         | SIL4         | SIL2 | SIL4 |
|         | SIL3         | SIL3 | SIL4 |
| SIL3    | SIL3         | 无    | 无    |
|         | SIL3         | SIL1 | SIL3 |
|         | SIL2         | SIL2 | SIL3 |
| SIL2    | SIL2         | 无    | 无    |
|         | SIL1         | SIL1 | SIL2 |
| SIL1    | SIL1         | 无    | 无    |

2 对于 SIL 认识的误区

国际标准对于 SIL 概念定义为以下 3 点<sup>[7]</sup>.

1)安全功能.一定要针对系统或是产品所实现的安全功能来描述 SIL;而在城市轨道交通信号系统招标文件中经常可以看到描述列车自动保护(Automatic Train Protection,ATP)的安全等级要求为 SIL4.

2)量化指标.SIL 是一个被量化的指标,使用 THR 来表达,表示的是安全功能处于危险侧的概率,但是这个指标不能与可靠性定量指标混为一谈;有时候会错误的把可靠性中的平均故障间隔时间(Mean Time Between Failures,MTBF)和 THR 联系在一起;当某个信号产品获得 SIL4 级证书后,就认为这个产品各方面都是最好的.某产品安全性满足一定指标后就可认证获得 SIL4 级证书,但还需要针对其可靠性、可用性和性能指标进行分析,看

它能否满足实际应用的要求.

3) SIL 划分.SIL 分为 0 到 4 级,4 级为最高,但是并不等于说 SIL4 就是最好的,这里没有高低之分,只有适合与不适合.如果将 SIL 等级确定太高,则要求在系统设计时采取更复杂、成本更高的技术来保证;如果将 SIL 等级确定太低,则系统的安全性达不到规定的要求.很多招标文件对于列车自动监督系统(Automatic Train Supervision System, ATSS)的要求为 SIL2,对于车门控制的要求甚至提升到 SIL4.要知道 SIL 是对于系统安全功能的要求,不能一味地把可用性和可靠性方面的要求强加到安全性方面.根据第 1 节的叙述,可以了解到国际安全标准对于 SIL4、SIL2 和 SIL0 的要求差别很大,不能随便更改.因为轨道交通领域的安全性更多的是通过故障导向安全或是紧急停车实现的,这样列车可能在运行过程中因为很小的故障,就紧急停车,造成整个运营秩序被打乱.

2.1 安全功能要求与 SIL 概念混淆

在工程项目中有一些使用 SIL 概念的误区.在轨道交通行业,如一条线路的信号系统是由若干子系统组成的,如果每个子系统的安全功能满足 SIL4 要求,就认为整个信号系统就满足 SIL4 要求,这也是对于 SIL 概念的错误认识.当某个产品获得 SIL4 证书,说明其主要的安全功能可以达到 SIL4 所规定的要求,不过当若干不同的产品组合在一起,它们所共同完成的功能可能会发生变化,这时需要进行系统性分析,看看这时候的安全功能是什么,它的表现如何.另外在一整条线路中,设备的数量是很多的,这时候不光要关注 SIL,更需要从整条线路的安全目标考虑,分配给信号系统的安全目标是多少,能否达到要求.如假设一个安全苛求系统是由 10 个满足 SIL4 安全功能要求的产品组成的,每个安全功能的 THR 应小于  $10^{-8}/h$ ,如果简单的去累加这些功能,10 个安全功能串接在一起,THR 是累加的概念,整个系统的安全功能的 THR 只能达到  $10^{-7}/h$ ,也就是说只能满足 SIL3 要求,因为这个系统当中的 10 个安全功能是各不相同,不能够像可靠性指标一样进行计算.

2.2 系统可靠性和可用性与 SIL 概念混淆

还有一类 SIL 概念的错误使用误区,就是将系统可靠性、可用性方面的要求用 SIL 进行表达.如现在大地铁的轨道交通运营压力都很大,一旦发生故障,线路很容易出现延误等影响运营的情况.为了提高轨道交通可用性,会发现对于轨道交通通信、电源供电、人机显示功能等相关设备和功能提出 SIL2

要求,这就是错误的把可靠性和可用性方面的要求用安全性的要求表达出来,这不仅不能有效解决可靠性和可用性方面的问题,反而会降低系统的相关性能,为了提高系统的安全性,往往会采用冗余和故障导向安全等技术手段.但为了保证安全性而增加系统组成的设备数量,往往会降低整个系统的可靠性和可用性,牺牲一些可靠性的指标要求.

3 确定 SIL 的定量方法

3.1 THR 的确定

对于任何安全苛求系统绝对安全是不存在的,通过国际通行的原则(ALARP、GAMAB、MEM等)采用一定范围数字的方法来确定可容忍风险指标,即什么样的危险可能性是能接受的.

1)可容忍目标.在铁路交通运输系统通常规定为 $R_i \leq 10^{-5}$ 灾难性危险/人·年.信号系统在铁路运输中要求较高的安全性,因此在一般信号系统的可容忍目标在分析和评估中规定为 $R_i \leq 10^{-6}$ 灾难性危险/人·年,并且将该值认为是 ATP 车载设备的 THR.

2)单点风险率.对每个风险进行估计,可以用下式来描述单点风险率(Individual Risk of Fatality, IRF)

$$IRF_i = \sum_{\text{所有危险} H_j} N_i \{ (HR_j \times (D_j + E_{ij})) \sum_{\text{事故} A_k} C_j^k \times F_i^k \}$$

(1)

式中: $N_i$  是系统或设备特定功能的使用次数(每年或每小时); $HR_j$  是风险模式下造成的危害率,可以作为  $THR_j$  的参考值; $D_j$  是系统或设备暴露在危险状态的时间; $E_{ij}$  是系统或设备在故障状态的时间; $C_j^k$  是风险模式的危害度; $F_i^k$  是灾难事故的概率.

3.2 SIL 的定量确定

配合行业权威部门制订的单风险容忍度 TIR,计算出每个风险的 IRF 为

$$IRF_i \leq TIR = 10^{-6}$$

(2)

式中:单风险的  $THR_i$  就通过满足该目标可容忍度下的  $HR \leq THR_i$  得出.

取每个安全功能的  $THR_n$  中后最小值作为一个子系统或设备的  $THR_s$ ,即

$$THR_s = \min[THR_1, THR_2, THR_3, \cdots, THR_n]$$

(3)

$SIL_s = \max[SIL_1, SIL_2, SIL_3, \cdots, SIL_n]$  (4)  
最终系统的 SIL 就可以对照标准的 THR 范围确定.

3.3 SIL 的定量划分

以列车运行控制系统完成的超速防护功能为例,说明如何确定 SIL.先设定列车运行控制系统的基本参数如下.

1)预估行驶中列车每小时遇到红灯的最大次数为 4 次,每次遇到红灯进行处理的时间为 100 s,设备的处理周期为 100 ms,则 ATP 车载设备处理红灯安全防护功能的总次数为

$$4 \times (100/0.1) = 4000, \text{ 设 } N_i = 4000.$$

2)车载设备强大的自检功能可以在出现故障时很快检测出,并实施紧急制动使列车停车,因此设定车载 ATP 设备处于危险状态的时间  $D_i$  最大为 5 s.结合车载 ATP 设备的故障检测和回段处理等过程修复时间,设定在停车后车载 ATP 设备处于故障状态的时间为  $E_i = 4$  h.

3)由于车载设备出现安全故障,则其危害程度将相当严重,认定为将有 10~100 人处于危险之中,则  $C_1^k = 10^{-2}$ ,同时对于严重危险和危害程度较大的风险,认定  $F_i^k = 1$ . 根据式(1)、式(2)得出

$$IRF_i = N_i (HR_1 \times (D_1 + E_i) \times \sum C_1^k \times F_i^k) = 4\,000 \times (HR_1 \times (4 + 5/3\,600) \times 10^{-2} \times 1) \leq TIR = 10^{-6}.$$

要求上式满足,则需要  $HR_1 \leq 6.25 \times 10^{-9}$ ,则可以认为  $THR_1 = 6.25 \times 10^{-9}$ .

通过和 IEC61508 的 SIL 表和 EN50129 的 SIL 表,列车超速防护功能的 SIL 为 SIL4.

以上只是对一个安全功能的计算和分配,如果想得到整个 ATP 车载设备的评估,必须对每个功能的  $THR_i$  和  $SIL_i$  进行分析.根据式(3)、式(4)的系统  $THR_s$  和系统  $SIL_s$ .确定整个车载 ATP 设备 SIL 的数值.

确定功能与子系统的对应关系,找出每个子系统中功能的最高 SIL,将此 SIL 作为子系统的 SIL.如表 3 所示,子系统 2 包含安全相关功能 F2、F4, F2 为 SIL2, F4 为 SIL4,因此子系统 2 的 SIL 等级应当与 F4 的 SIL 相同为 SIL4.

表 3 子系统 SIL 分配表

Tab.3 Allocation table of subsystem SIL

| 功能     | SIL 等级 | 子系统 1 | 子系统 2 | ... | 子系统 n |
|--------|--------|-------|-------|-----|-------|
| F1     | 1      | ✓     | —     |     | ✓     |
| F2     | 2      | —     | ✓     | ... | —     |
| F3     | 2      | —     | —     |     | ✓     |
| F4     | 4      | —     | ✓     |     | —     |
| 最高 SIL | —      | 1     | 4     | ... | 2 3   |

注:✓表示承担安全功能;—表示不适应.



4 确定 SIL 的定性方法

4.1 用风险图确定 SIL

IEC 61508 标准采用风险图确定 SIL 等级:此方法是基于功能的风险水平确定 SIL 等级.功能的风险水平由公式  $R = f \times C$ .其中, $R$  是安全相关系统的风险; $f$  是安全相关系统的危险源频率; $C$  是危险源发生后果(后果可以是对于人的伤害、财产损失或是对于环境的破坏).

危险源频率  $f$  由 3 个因素组成:1)危险源发生频率和危险区域暴露时间;2)避免危险源发生概率;3)无任何安全相关系统(但是存在外部风险减轻设施)时危险源发生概率—被称作非期望事故的概率.

因此风险包括以下 4 个参数<sup>[8]</sup>:1)危险源后果  $C$ ;2)危险源发生频率和危险区域暴露时间  $F$ ;3)避免危险源的概率  $P$ ;4)非期望事故的概率  $W$ .

依据图 3 的风险图确定其风险减轻值,取值可能是  $a$ 、 $b$ 、 $c$ 、 $d$ 、 $e$ 、 $f$ ,然后对照表 4 得出该功能的 SIL 等级.确定每个功能的以上 4 个参数的等级见表 5.

图 3 中各参数的定义见表 4 和表 5.

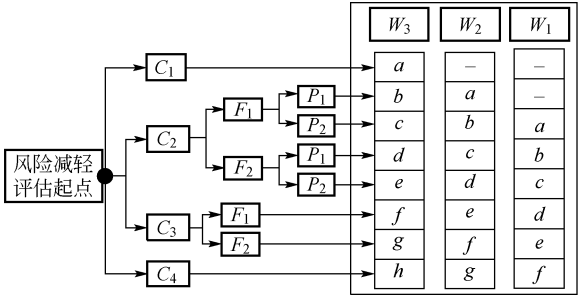


图 3 风险图

Fig.3 Risk map

表 4 W 中各等级的定义

Tab. 4 Definitions of grades in W

| 最少需要的风险减轻值 | 安全完善度等级 SIL    |
|------------|----------------|
| —          | 无安全要求          |
| a          | 无特殊安全要求        |
| b, c       | 1              |
| d          | 2              |
| e, f       | 3              |
| g          | 4              |
| h          | 单个安全相关系统不能满足要求 |

表 5 参数定义

Tab.5 Parameter definitions

| 风险参数                | 等级             | 备注                                                                                                                                                                               |
|---------------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 后果(C)               | C <sub>1</sub> | 发生轻伤                                                                                                                                                                             |
|                     | C <sub>2</sub> | 发生重伤、多人轻伤或对环境有较严重威胁                                                                                                                                                              |
|                     | C <sub>3</sub> | 单人死亡,多人重伤或对环境造成严重破坏                                                                                                                                                              |
|                     | C <sub>4</sub> | 多人死亡或对环境造成重大破坏                                                                                                                                                                   |
| 危险源发生频率和危险区域暴露时间(F) | F <sub>1</sub> | 几乎不到经常暴露在危险区域                                                                                                                                                                    |
|                     | F <sub>2</sub> | 频繁到永久暴露在危险区域                                                                                                                                                                     |
|                     | P <sub>1</sub> | 在一定条件下可能                                                                                                                                                                         |
| 避免危险源的概率(P)         | P <sub>2</sub> | 几乎不可能                                                                                                                                                                            |
|                     |                | 这个参数需考虑:<br>监控或者未监控(如由技术熟练或技术不熟练人员)的流程;<br>危险源发展速率(如突然、快速或缓慢);<br>危险识别的难易(如很容易被识别,通过技术措施检测或无须任何技术措施就可检测);<br>危险源规避(如可能的、不可能的或者一定条件下可能的逃避路线);<br>实际的安全经验(在一些相同或类似的受控设备中存在的类似安全经验) |
| 非期望事故的概率(W)         | W <sub>1</sub> | 非期望事故发生概率很小,且有很少数事故可能发生                                                                                                                                                          |
|                     | W <sub>2</sub> | 非期望事故有发生的可能性,有一些且非期望事故可能发生                                                                                                                                                       |
|                     | W <sub>3</sub> | 非期望事故发生的可能性相对较高,且频繁的非期望事故可能发生                                                                                                                                                    |

4.2 SIL 的定性划分

计算机联锁系统是一个对于安全性要求很高的信号产品,它通过列车进路、信号机和道岔直接的联

锁关系保证列车行车的安全<sup>[9]</sup>,表 6 列举了联锁系统相关功能.

以表 6 中的 3.1.1.1 办理列车进路功能为例说

明确定 SIL 等级,办理列车进路如果处理不当可能造成列车相撞等严重事故,后果等级设定为  $C_4$ ,非期望事故概率设定为  $W_2$ ,通过图 3 得知这个安全功能的 SIL 等级应该划分为 SIL4 级,如图 4 所示。

表 6 联锁功能列表

Tab. 6 Interlocking functions list

| 参考编号    | 相关功能    |
|---------|---------|
| 3.1     | 联锁功能    |
| 3.1.1   | 进路控制    |
| 3.1.1.1 | 办理列车进路  |
| 3.1.1.2 | 办理折返进路  |
| 3.1.1.3 | 调车进路    |
| 3.1.1.4 | 引导进路    |
| 3.1.2   | 进路解锁    |
| 3.1.2.1 | 自动解锁    |
| 3.1.2.2 | 非自动解锁   |
| 3.1.3   | 道岔信号机控制 |
| 3.1.3.1 | 信号关闭    |
| 3.1.3.2 | 信号重开    |
| 3.1.3.3 | 信号单操    |
| 3.1.3.4 | 信号单锁    |
| 3.1.3.5 | 信号单解    |
| 3.1.3.6 | 信号强扳    |
| 3.1.3.7 | 封锁功能    |

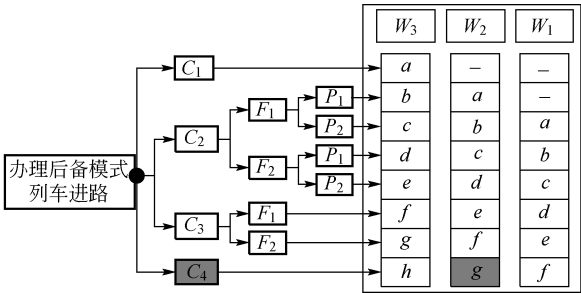


图 4 办理列车进路功能的 SIL 分配

Fig. 4 SIL allocation for train route function

4.3 定性与定量方法的比较

定性方法使用矩阵评估风险,以文字方式而不是数字方式描述,如用类似“灾难性的”或者“严重的”之类的短语形容严重程度.定性的方法依赖于用户选择风险参数所基于的假设和判断.定性的方法可能会使用模棱两可的说明短语,需要由次方法的不同的用户商讨得出共识,如“灾难性”或“严重的”的两个短语可以用来表示风险的严重程度的定义需要有度量标准.当选择了一个错误的风险参数时,由于定性的方法使用一定范围和短语相结合粗略的描述风险参数,在选错误数量级会立即导致不同的结果。

定量的方法使用明确的(或一定范围)的数字作为安全目标计算的输入,如危险出现的频率可以使用每小时的事件数表示.定量的方法可能更容易出现计算结果的错误.对于定量方法,可能会出现参数

的轻微变化,并不一定会导致不同的结果。  
但是,无论什么方法,如果无法准确估计参数,应该选取保守的结果.此外,过于复杂的应用计算或分析方法要求安全人员拥有更多的成功的应用的经验和诀窍。

5 结语

本文作者基于 CENELEC 标准论述了安全完善度等级 SIL 概念和含义,安全完善度等级蕴涵了每个等级对安全性的定量要求,为系统安全设计和评估提供了依据.我们在应用安全完善度等级时需要首先识别出系统或是设备应完成的安全功能,然后再去分析其 SIL 等级,而不是泛泛的支出某个设备的 SIL 等级.本文给出的 SIL 等级确定方法来自于国际安全标准,可以为安全管理和分析人员提供参考。

参考文献 (References):

[1] Functional Safety of electrical/electronic/programmable electronic safety-related systems: IEC 61508—2000 [S]. 2000.

[2] CENELEC. Railway applications: the specification and demonstration of reliability, availability, maintainability and safety: EN 50126—1999[S]. 1999.

[3] CENELEC. Railway applications: safety related electronic systems for signalling: EN 50129—1999[S]. 1999.

[4] CENELEC. Railway applications: software for railway control and protection systems: EN 50128—1998[S]. 1998.

[5] 邱兆阳. 如何正确理解 SIL 概念[J]. 铁路通信信号工程技术, 2009, 6(5): 14—15.

QIU Zhaoyang. How to understand the concept of SIL correctly[J]. Railway Signaling & Communication Engineering, 2009, 6(5): 14—15. (in Chinese)

[6] Railtrack PLC. Engineering safety management issue 4 volumes 1 and 2 fundamentals and guidance[R]. 2006.

[7] Adtranz Company. Establishing safety integrity level from frequency of failure[R]. 1998.

[8] BEUGIN J, RENAUX D, CAUFFRIEZ L. A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems[J]. Reliability Engineering & System Safety, 2007, 92(12): 1686—1700.

[9] 郝春海, 唐涛, 燕飞. 轨道交通 ATP 安全完善度等级 SIL 的分析[J]. 控制工程, 2003, 10(增 2): 34—36.

GAO Chunhai, TANG Tao, YAN Fei. Analysis and research of the safety integrity level for ATP system of rail traffic[J]. Control Engineering of China, 2003, 10 (S2): 34—36. (in Chinese)