

综
述
与
评
论国产化列车网络控制系统
安全完整性等级评估与认证赵 强¹, 常振臣¹, 李砾工², 王金田¹(1. 长春轨道客车股份有限公司, 吉林 长春 130062;
2. 中国北车股份有限公司大连电力牵引研发中心, 辽宁 大连 116022)

作者简介: 赵 强 (1976-), 男, 工程师, 长春轨道客车股份有限公司, 目前主要从事列车网络控制系统安全性及可靠性研究。

摘 要: 在对国产化列车网络控制系统 SIL 认证核心工作进行分析的基础上, 得出 TCMS 开发安全生命周期 SIL 过程活动评估的关键内容及其指标评估的具体方法。针对 TCMS 系统的安全要求及可容忍风险故障率的确定及分配进行了清晰的示意说明, 对安全功能的时间故障数的计算方法进行了详细的例解分析。

关键词: 列车网络控制系统; 安全完整性等级; 评估; 安全功能

中图分类号: TP393; U266.2 **文献标识码:** A **文章编号:** 1000-128X(2011)06-0001-05

Safety Integrity Level Assessment and Certification of Localization Train Network Control Management System

ZHAO Qiang¹, CHANG Zhen-chen¹, LI Li-gong², WANG Jin-tian¹

(1. Changchun Railway Vehicles Co., Ltd., Changchun, Jilin 130062, China;

2. China CNR Corporation Limited Dalian Electric Traction Research & Development Center, Dalian, Liaoning 116022, China)

Abstract: In this paper, on the basis of analyzing the core work for train network control system SIL certification, the key contents of SIL assessment activity process in TCMS development safety lifecycle were summarized, and a specific method for the SIL index assessment was brought up. In particular, a clear schematic description on determination and allocation process for the safety requirements and tolerable risk failure rate of TCMS was conducted. Meanwhile, a calculation method for failure in time (FIT) of safety function was also described in detail.

Key words: train network control management system; safety integrity level(SIL); assessment; safety function

0 引言

中国北车长春轨道客车股份有限公司与大连电力牵引研发中心共同研制开发应用于北京地铁 15 号线项目的国产化列车网络控制系统。针对 TCMS 运行环境为充分证明国产化 TCMS 能够达到高水平安全完整性等级, 根据欧洲电工标准化委员会认证标准要求, 长春轨道客车股份有限公司聘请瑞士 ENOTRAC 公司具有丰富经验与资质的评估师作为顾问共同工作, 同时选定欧洲铁路联盟委员会成员 SCONRAIL 公司作为独立的安全评估机构, 针对 TCMS 的安全完整性等级进行评估与认证。

1 认证执行标准

欧洲铁路联盟以 IEC61508 为基础制定了关于铁路安全相关系统开发 SIL 认证的执行标准。EN50129 作为铁路信号系统评估标准定义了铁路信号系统安全验收及认证的要求, 规定了安全信号相关系统硬件和软件开发在整个生命周期中的安全完整性等级评估内容, 是欧洲第一个相关领域的标准。EN50128 作为对铁路控制及防护设备中使用的可编程电子系统的软件开发和安全保障进行规范的标准, 规定了开发不同 SIL 等级的系统软件相应的技术和措施, 同时对软件生命周期各阶段的活动细则、文档规范及人员职责的分配都进行了说明。EN50155 是铁路上机车车辆使用的电子设备在环境温度、撞击与振动、相对湿度、大气污染物及电气

收稿日期: 2011-08-11

工作条件下标准规范,是针对硬件产品设计制造安全完整性评估必须执行的标准。

针对北京地铁15号线列车网络控制系统认证目标,要求系统及硬件达到SIL1、软件达到SIL2的标准,SCONRAIL独立审核员(ISA: Independent Safety Assessor)将整个的评估工作活动划分为两大部分:第一部分包括按照EN50129的要求,对与TCMS有关的(包括功能)硬件的评估;另一部分是按照EN50128的要求,对于TCMS软件的评估,并确定评估所采用的标准主要分配如下:

- ①软件应符合EN50128的要求;
- ②硬件与安全论据应符合EN50129的要求;
- ③一般要求应符合EN50126的要求;
- ④硬件的开发与论证应符合EN50155的要求;
- ⑤安全数据传输的软件通信应符合EN50159-1的要求。

2 认证方式

北京地铁15号线TCMS系统SIL认证采用文件评审结合面谈、对活动的观察及现场检验的方式进行。认证审核分为2次进行:首次认证审核包括组织机构及其职能的评估,程序、工具、方法、标准以及测试条件是否充分的评估,文件程序具体方面的现场检查及具体/随机选择文件的现场检查3个方面;末次认证执行测试见证与确认跟踪,审核TCMS系统是否已经按照具体的TCMS应用设计文件、规则以及标准要求进行了正确的执行与测试。

3 评估内容

SIL认证评估内容主要包括过程活动评估及指标评估2个方面。过程性评估尤为重要,其主要是针对TCMS系统开发过程的标准进行符合性验证,以确定整个开发体系符合SIL认证的标准要求;而指标评估则是对于TCMS安全功能SIL等级指标的选择、分配及最后实现过程确认与评估。

3.1 过程活动评估

过程活动评估是对生命周期中每一阶段的过程活动执行的严格性进行验证及确认,确定每一生命周期内TCMS开发所执行的质量、安全、配置管理活动的标准符合性及其活动管理的追溯性,每一开发阶段过程活动的追溯性及符合性验证是整个过程评估的重点。

图1为依据EN50126及EN50129建立起的北京地铁15号线TCMS系统开发总体生命周期模型。由于TCMS是一个电子的可编程的系统,其安全完整性必须进行详细的说明以论证其达到了相应等级安全要求。结合TCMS开发的具体特点及认证目标,ISA针对TCMS生命周期过程活动将以下几个方面作为关键点进行了重点评估。

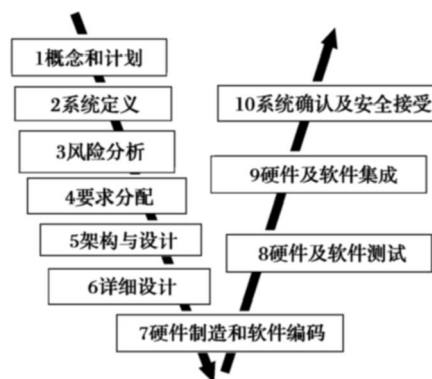


图1 TCMS系统开发生命周期

概念及计划：本阶段是从计划到进行的最为重要的活动,遵循差距评估原则,评估针对全面的TCMS安全周期模型及功能安全管理系统的建立标准性审核。安全生命周期模型审核标准对应于确定实施范围中核心前提条件的IEC61508和IEC61511^[1]的相应阶段,并且其开发过程的管理要求充分满足质量及配置管理流程。

系统定义：对于这一阶段来说,TCMS的功能需求、安全目标、系统接口定义及运营策略和环境准确性将作为评估审核的重点。此阶段系统定义的准确性直接影响系统安全接受与确认阶段中系统功能正确运行保证追溯性确认评估,同时也是保证安全分析完整性及其准确性的前提条件。

风险分析及要求分配：风险分析及要求分配是过程评估中的关键内容,是保证整个系统安全完整性的重要阶段。对于安全分析的完整性必须得到充分的证明,这需要从分析的方法、分析过程的输入(检查表、历史数据,行业经验等)及分析人员的经验能力水平等方面来证明。对安全控制的管理,需要从危害识别、分析及登记,直到危害关闭的整个闭环管理的追溯性进行有效评估,以保证TCMS开发过程中安全性保证措施得以实施。此外,对于风险分析过程中潜在风险不能有效控制的,安全要求是否有效提出,提出的安全要求是否进行了合理的分配(由系统到硬件及软件的安全要求分配)同样都是认证审核的关键性环节,可以说,安全要求的提出及分配是贯穿整个SIL过程评估的主线。图2说明了TCMS系统安全要求的确定过程,安全要求的分配过程如图3所示。

系统架构设计及详细设计：无论对系统架构设计还是对详细设计阶段来说,评估主要都是针对安全要求的具体实施情况的审查,包括对系统硬件、软件、设备、通信总线、软件功能模块、接口及嵌入式软件的架构定义过程的评估。其中,详细设计阶段的软件的评估主要审核每一条安全要求是否有效实施,软件SIL标准设计流程是否得以贯彻。而硬件,则侧重于审核安全要求及安全容忍率指标是否已经分配到系统设备级,故障模式影响分析FMEA或FMECA是否得以开展;同时,更为关键的是审核每一安全相关功能的安全

状态都进行准确地定义, 软件及硬件的功能是否能够确保系统在检测到故障后导向安全状态。

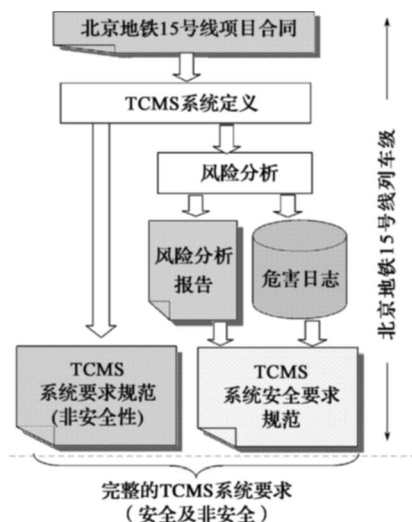


图2 TCMS系统安全要求的确定过程

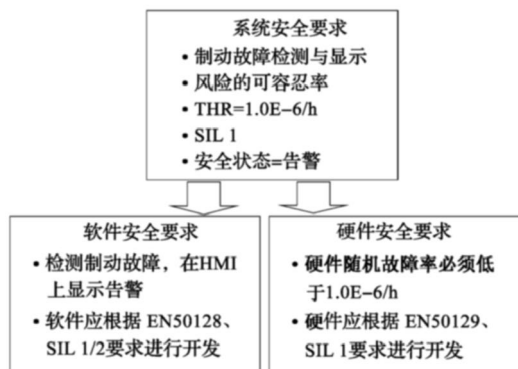


图3 系统安全要求的分配

硬件制造、软件编码及其测试：这3个阶段（图1中7、8、9）评估内容各有其针对性。硬件制造上，元器件筛选、工艺流程、硬件故障的可测试性等都将作为评估的重要点；软件编码方面，评估侧重审核TCMS应用软件采用的技术方法及工具是否满足EN50128附录中的定义；软件的模块化设计是否能够完成指定的安全功能，同时实现其可测性。数据传输通信方面的安全审核在验证EN50159-1中技术要求是否得以保证的基础上，更多的则是通过测试阶段的评估进行确认。此外，在软件及硬件测试的审核中，分别依据EN50128与EN50155，通过黑盒、白盒及例行、型式试验的方法验证TCMS软件模块中的所有程序与代码及其内部功能均得到有效、详细的测试，TCMS的硬件能否在充分满足其气候、机械、冲击、碰撞及电磁兼容等条件下，实现其所有安全功能。同时，对于硬件、软件测试所采用的工具及试验环境的可信性都需提供足够的证据进行有效的说明。集成测试阶段，软件模块的集成测试、软件及硬件集成的模块测试、软件集成的测试用例的定义及指定的集成测试都将进行全面的抽样性评估，以确定TCMS安全相关功能实现的有效性及其SIL目标实现的可达性。

系统确认及安全接受：执行确认的前提条件就是对做出结论的完全检验，确认的执行应该在确保满足所有的系统要求（其中包括与安全性相关的要求）的条件下进行，并且确保能够达到所要求的安全水平。因此，在阶段性验证审核和安全功能符合性测试结果基础上，TCMS的安全功能确认测试的说明、执行情况及证明文件依据将作为评估的重点进行审核。确认性测试评估包括在试验室及装机上车后执行的黑盒测试两部分，测试在确认员的监督下完成，同时经ISA抽样测试审核，确认预案包含整个TCMS软件及整个系统的确认，并在确认工作开始前提交ISA审核。此外，对TCMS质量管理及安全管理的确认同样是此阶段评估工作的关键点。虽然，此项工作在首次认证审核中已予以重点审查，而确认性评估更侧重审核TCMS功能、技术安全要求及相应安全容忍率的符合性确认，包括对硬件随机故障分析的最终论证其安全故障容忍率及相应安全故障百分比达到SIL要求。最终，针对北京地铁15号线项目，ISA负责在确认阶段对TCMS的系统、硬件及软件进行结论性的评估，同时出具权威的、具有公认性的评估报告。

3.2 指标评估

不同SIL等级要求的硬件及系统意味其安全完整性系数有不同的标准，因此硬件和系统是否达到其指标要求同样需要进行评估。指标的评估主要是针对硬件及系统的安全性功能而言的，对于SIL1系统可容忍的危险率要求 $1E-6/h \leq THR$ ^[2]。根据北京地铁15号线TCMS认证要求，目标是要论证相关于每一安全相关功能涉及的硬件可容忍的危险率满足 $1E-6/h \leq THR$ 。但是，值得注意的一个问题是，如果要求硬件达到SIL1标准，并不意味着所有通过硬件实现的功能的THR均能达到 $1E-6/h \leq THR$ ，SIL指标的评估同样更强调对硬件开发的过程控制。

3.2.1 评估分析中应用的概念

在指标评估的过程中，更需要有清晰的概念及明确的思路以保证SIL分析的正确性。

1) 故障率和“FIT”定义

为评估TCMS系统的SIL，每一硬件设备所对应的每一故障模式的故障率都必须明确。故障率通过执行故障模式影响分析（FMEA）的过程中导出。SIL指标的评估是论证相关于每一安全功能涉及的硬件的危险FIT（Failure In Time）数值小于目标值。为简化相关于一个功能的总故障率的计算，设备的故障率通常以FIT“时间故障数”单位定义，单位FIT表示1E9小时中发生的故障数：1FIT是每1E9小时1个故障。

2) 危险/非危险和检测到的/未检测到的故障

为了计算每一安全功能的FIT，该功能中涉及的每一设备的FIT同样必须得到明确。对于一般设备，不是所有的故障都是危险的（从安全的角度考虑，“危险”

意味着故障对于安全方面具有影响)。例如,如果电机接触器在过电流情况下打开,则故障“电机接触器闭合卡塞”应考虑为危险故障,而故障“电机接触器打开卡塞”则不应考虑为“危险”。

每一设备的危险故障分数(总故障率中危险故障的百分比)的计算包括在FMEA中。如果一些设备没有充分的数据可用(例如,客户的数据表不包括足够的信息)的话,可假定约50%的故障将考虑为“危险”^[3]。例如,假定1E-7/h(100 FIT)的电机接触器故障率,可以假定危险故障的故障率是5E-8/h(50 FIT)。

3) 检测到的故障/未检测到的故障

一般说来,对于TCMS这样的系统,其自身具有可检测系统故障和可对其反应的监督/保护功能,但是,并不是所有故障都可以通过其自身的诊断系统得到检测,总是有未检测到的余下的故障分数(危险和非危险)。

检测到的/未检测到的故障数值取决于检测系统的质量。IEC61508包括许多规则来导出检测到的故障的百分比,与TCMS硬件相似的SIL1系统中,检测到的故障的百分比要求并不是非常的高,可以假定SIL1系统的未检测到的故障的百分比近似为50%~60%^[3]。

4) 故障情况中安全状态的考虑

在许多情况中,仅仅检测到故障不足以保证系统的安全性,必须保证检测到的故障达到安全状态。所以,在执行硬件故障分析或者每一设备上的详细故障模式影响危害分析的过程中,必须确定考虑为“检测到”的故障是否能够在容忍时间内达到安全状态,否则,如果在特定设备的故障情况下不能达到安全状态,则该设备的所有FIT将在硬件指标评估中进行充分的考虑,因为该设备的所有故障是危险的并且属于“不安全”故障。

5) 执行指标评估分析的故障的考虑

计算每一安全功能中涉及设备的FIT所考虑的故障是“非安全故障”。如果可以达到安全状态,那么,“非安全故障”则是指那些危险的并且是未检测到的故障(注意,只有在故障情况下,可以达到安全状态,这才有效),否则,“非安全故障”的数值相当于相关考虑的设备的FIT的总数。例如,在电机接触器的情况中,如果考虑50%的故障为“危险”以及50%的危险为“未检测到”,则可以声明“非安全故障”为25%,这意味着在指标评估分析中需要考虑的FIT数值是25。

3.2.2 指标评估方法

TCMS是否履行其安全目标是最终确定系统能否达到SIL要求的前提条件,而论证是否符合其安全目标的方法是进行硬件故障分析,并以此为基础,从而评估其达到SIL1标准要求的可行性,执行SIL指标评估的通过安全功能和相关THR的确定、安全功能的硬件识别及功能框图的生成、安全功能的FIT的计算、通过/失

败的确认4个主要过程。

1) 安全功能和相关THR确定

安全功能通过进行危害分析得以确定。对于确定的安全功能,如“制动故障的检测与显示”,其安全要求需要根据风险评估的要求水平准确地提出,相应的可容忍故障率也需要在此过程中得以分配。在系统安全功能危害分析及安全要求提出、分配的基础上,软件及硬件安全要求也必须提出,并且在设计阶段有效实施以保证系统开发从硬件、软件2个方面均达到SIL标准要求。图3表示了系统安全要求分配的具体过程。

2) 安全功能的硬件识别及功能框图的生成

对于每一安全功能,必须首先确定TCMS系统所涉及的硬件设备,涉及设备间的逻辑连接也必须正确地建立。每一安全功能需进行详细分析,依据TCMS功能实现原理确定“硬件安全功能框图”,这样,相关于每一安全功能的FIT值才可进行准确计算,这也是SIL指标评估过程的最为关键前提。

3) 安全功能FIT的计算

硬件安全功能框图建立之后则需进行整个功能的FIT值的计算。由于安全功能总FIT等于每一设备的非安全故障的总和,因此FIT值的计算,取决于相关于设备的可用信息。以下给出了用于计算“非安全FIT”的数值方面有2种可能的“解决方案”。如果设备的可用数据是FIT值的总数,则可以采用第1个方案,一般来说,此方案主要是适用于直接采购设备;而对于内部开发和生产的设备,则应采取第2种方案。

方案1:如果设备的可用数据是FIT值的总数,那么,可以将非安全故障的数值计算为每一设备FIT的25%^[3],然后,对TCMS安全功能所涉及所有设备非安全故障数值进行求和,最终确定整个安全功能总FIT值。在许多情况中,以这一方式计算的FIT值将很高,并且硬件目标故障率不能得到满足。在这情况下,可以应用方案2,可给出比方案1更为精确的结果,因为它基于涉及到每一安全功能中的每一硬件设备以及部件/零件的详细分析。

第2个方案主要针对于自主开发的设备,如果设备的可用数据足够详细(或者供应商给出相关于每一设备的详细技术规范),那么,用方案1计算的结果不足以满足目标的话,方案2也可用于购买的设备。

方案2:如果方案1中应用考虑25%的故障为“非安全”,则每一设备考虑为黑盒并且FIT值考虑为该设备的总FIT值的计算方法过于悲观。实际上,并不是每一设备的所有的部件/零件都涉及在特定的安全功能中。为了更为精确地计算“非安全FIT”的值应当在每一设备FIT值计算中进行考虑,有必要仔细分析设备的哪些部件/零件实际上涉及在该安全功能中。然后,“非安全FIT”的数值在设备级上进行计算,而并非在系统级上计算。通过这种计算方式,则可以得到更为准确、较为

乐观的结果,如图4。

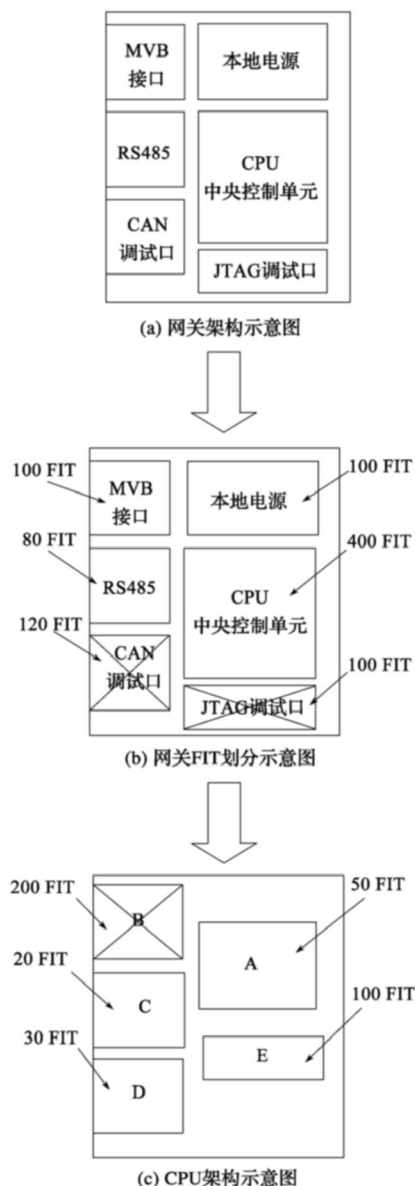


图4 FIT 计算过程示意图

以TCMS设备网关(GW)为例,可以说存在确定的不用于考虑安全功能的一些部件。例如,网关设备中CAN调试口模块和JTAG调试口模块确定不涉及在功能“制动故障的检测和显示”中,那么相关于不使用/不涉及这一设备部件在FIT值的计算过程中可以不予考虑。

假定GW的总FIT是900,并且假定如图4(b)所示划分,其中,220 FIT(相关于CAN调试口为120 FIT,相关于JTAG调试口为100 FIT)可作为非安全故障的计算

予以考虑。在这种情况下,FIT的数值计算为相关于GW(900-220FIT)的危险和未检测故障的总和。如果这一方式中计算的FIT的总数仍不足以满足目标的话,则每一设备的每一部件可继续进行划分为相应的组成部分以进行更为精确的FIT值计算。例如,GW的最关键部件是CPU,因为其FIT的数值(400)相对是最高,通过分析,CPU中的“B”部分对于既定的安全功能来说并没有实际起作用,那么,针对这种情况,相关于“B”部分的FIT值则不需要考虑,并且,对于CPU相关安全功能FIT值计算考虑的是余下(400-200FIT)的危险的、未检测到的故障。由此可以看出,在充分考虑安全功能中未实际起作用部件及危险的、未检测的故障的基础上,设备GW相关FIT值最终计算结果不仅更为精确,同时也更为乐观。

4) 指标评估通过/失败的确定

如果对于每一安全功能FIT的计算值小于指定值,则SIL指标评估才满足其要求。如果计算的FIT值高于特定功能的目标,那么,关键设备的考虑则认定为不充分,并且它们将重新设计或者用充分的设备替换,为满足SIL评估指标提供保证。

4 结论

针对目前国内铁路运营系统设备的安全状况,TCMS不能定义为具有完整安全性要求的系统。但是,对于列车运行控制的安全性以及运营服务的安全任务保证性,全面的、高标准的安全完整性要求对于TCMS的开发是完全有必要的,特别对于国内自主研发的TCMS其功能安全完整性的证明更显示出其重要性。在向国际公认的第三方安全完整性认证的挑战过程中,针对认证过程中通过ISA审核关键评估过程及重点内容进行了详细的分析,对于指标评估计算的及其可能出现的偏差问题给出了有效解决方案,这对于在国内轨道客车制造及开发商向国际公认安全性认证进行挑战具有实践的指导意义。

参考文献:

- [1] IEC61511, Functional Safety-Safety instrumented system for the process sector 2003 [S].
- [2] CENELEC. EN50129, Railway Application-Safety related electronic system for signaling 2003 [S].
- [3] IEC61508-2, Requirements for electrical/electronic/programmable electronic safety-related systems, 2010 [S].