基于既有部件的列车运行控制系统安全评估*

方云根[1,3]　潘　锋[2]　胡小莉[3]

（1. 同济大学交通运输工程学院，201804，上海；2. 中国合格评定国家认可委员会，100062，北京；
3. 上海轨道交通检测技术有限公司，200434，上海//第一作者，工程师）

摘　要　既有部件用在安全相关的列车运行控制系统之中完成部分系统功能，需要评估其对系统安全性的影响。首先分析既有部件的类型和特点，结合列车运行控制系统安全要求及其证明过程，指出应用既有部件需要解决的问题；然后对系统开发过程中应用既有部件的步骤和安全要求进行分析，提出既有部件的失效控制策略和技术要求；最后分析既有部件安全的证明过程，为基于既有部件的列车运行控制系统安全评估提供建议。

关键词　列车运行控制系统；既有部件；安全完整度等级；安全评估

中图分类号　U283.2

DOI：10.16037/j.1007－869x.2021.05.027

Safety Assessment of Train Operation Control System Based on Pre-existing Items

FANG Yungen，PAN Feng，HU Xiaoli

Abstract　Safety should be assessed when pre-existing items are used in safety-related train operation control systems as parts of system function. Firstly，the types and characteristics of the pre-existing items are analyzed，with the safety requirements and the demonstration process of the train operation control system，and the problems to be solved in the application of the pre-existing items are identified. Then the application steps and safety requirements of the pre-existing items in the system development process are analyzed，and the failure control strategy and technical requirements of the pre-existing items are suggested. Finally，the safety demonstration process of the pre-existing items is analyzed，and suggestions are put forward for safety assessment of train operation control system based on pre-existing items.

Key words　train operation control system；pre-existing items；safety integrity level；safety assessment

First-author's address　College of Transportation Engineering，Tongji University，201804，Shanghai，China

列车运行控制系统是采用通信、计算机、控制等技术构成的用以保障行车安全的关键系统，通常会基于如传感器、执行单元、通信模块、实时操作系统、安全计算机等既有部件进行列车自动运行、进路联锁控制等具体安全应用的设计开发，用以节省研发成本，加快开发进度。由于既有部件不一定是专门针对轨道交通安全控制系统定制开发的，不能直接满足轨道交通行业的安全要求，如何在系统开发早期选择并确定既有部件，开发过程中如何对既有部件进行安全分析，如何确定既有部件的失效检测和控制策略，如何针对既有部件进行验证和确认，如何证明基于既有部件能够满足系统功能的安全完整度等级（SIL）要求，以上这些是轨道交通列车运行控制系统安全评估过程中经常面临的问题。

1　既有部件的类型和特点

既有部件，是指相对于正在开发设计的系统来说已经存在且不是为当前系统开发的部件。从列车运行控制系统来看，常用的既有部件有商用实时操作系统、安全计算机平台、工控机、服务器、智能传感器等。从不同的角度，既有部件的分类如表 1 所示。

表 1　既有部件的分类

序号	分类标准	类型
1	来源	商业现货产品、企业自行开发的产品
2	物理形式	软件、硬件、软硬件结合体
3	安全证据	有 SIL 证明、无 SIL 证明
4	复杂度	低复杂部件、复杂部件

按照分类，有 SIL 证明的既有部件是按照轨道交通安全保障过程开发的，满足功能安全要求，并且能为新开发系统提供开发所要求的所有安全相关信息，如接口协议、既有部件的安全功能规范、硬件和软件配置、危险失效率、系统使用的限制和约束、定期检测和维护要求、安装和集成要求、安全相关应用条件、运行环境等信息。低复杂部件的特征

* 国家认证认可监督委员会项目（2019CNAS10）；国家市场监督管理总局科技计划项目（2019MK140）

是已经很好确定了每个独立元器件的失效模式，可以完全确定部件在故障情况下引发的行为。以上两种类型的既有部件应用相对简单，本文主要研究分析无 SIL 证明、通过市场采购或者企业以往开发的复杂既有部件的应用安全评估。

按照轨道交通安全标准的要求，为证明列车运行控制系统安全功能满足特定的 SIL 等级，需要提供整个系统开发过程的安全相关证据。从这个角度来说，既有部件存在以下特点：

1）缺少或不能提供全系统生命周期的质量和安全管理的过程证据，开发过程不以功能安全为导向，不能确保既有部件没有系统性失效。

2）缺少或不能提供功能和技术安全的证据，技术特性和功能是完全或部分未知的，或者从安全角度来看不能保证。由于设计不一定是安全导向的，并且没有提供用于容错和故障管理的嵌入式措施，因此无法确保控制系统性失效和随机性失效。

由于以上两个特点，使得在列车运行控制系统开发过程中采用既有部件需要进行安全分析并进行控制，以确保系统的安全功能满足 SIL 要求。

2　应用过程和需考虑问题

按照安全标准要求，作为安全关键系统，列车运行控制系统的开发需遵循系统安全生命周期，分阶段进行设计和开发，并在每一个阶段进行验证工作。由于既有部件在列车运行控制系统中承载部分系统功能，影响系统的安全性，需要在系统架构及需求分配阶段分析并确定既有部件应用的相关问题，如图 1 所示。

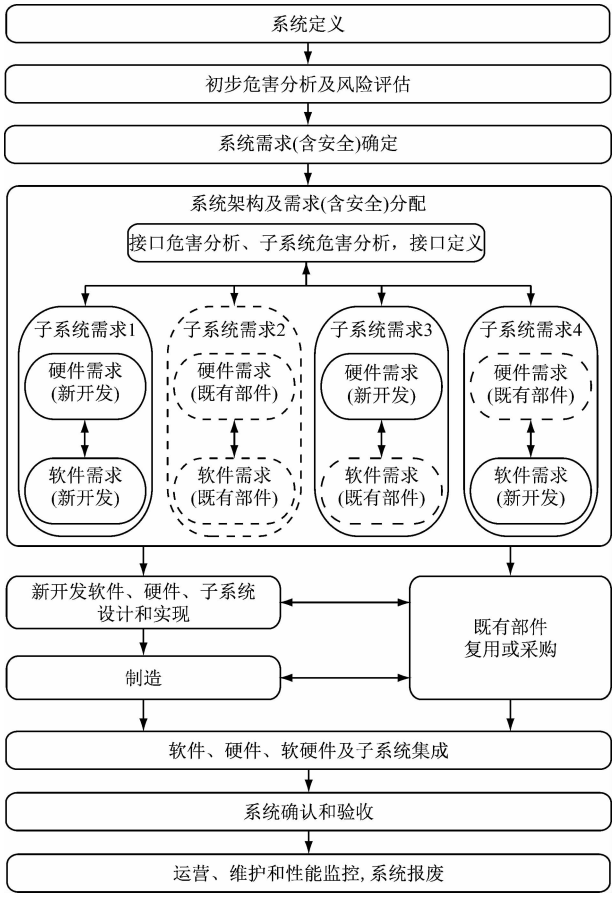

图 1　基于部件的列车运行控制系统开发过程

在系统架构及需求分配阶段，基于所考虑的系统规模和复杂度，设计人员将需求分配给指定的子系统（软件、硬件或者软硬件），并且确定所有子系统之间的接口。在这个过程中，如果确定采用既有部件，则需要考虑如下问题：①既有部件是否满足功能、性能和接口的需求？②采用什么类型的既有部件来满足系统需求？③既有部件的功能、性能、接口和应用条件如何？④既有部件的失效是否会危及系统相关的安全需求？⑤如何在系统集成过程中集成既有部件？⑥既有部件有哪些可获得的安全证明证据？

3　安全分析及证明

3.1　安全分析

列车运行控制系统是保障轨道交通行车安全的关键系统，其需要完成列车运行进路安全，追踪列车间距、列车运行速度、列车加速和制动等核心的安全功能。为完成这些安全功能，列车运行控制系统需要实时采集列车和线路的动态信息，进行逻辑运算后输出控制动作。从控制功能数据流的角度，既有部件在列车运行控制系统中有两种形式。

在第一种形式中（见图 2），既有部件作为安全控制数据流的一个独立节点，执行系统安全功能，如计算机联锁系统中采用外购的既有全电子执行单元。第二种方式如图 3 所示，既有部件和新开发部件一起作为系统安全控制数据流的一个独立节点，如轨旁的区域控制器采用安全计算机作为轨旁列车自动控制软件的应用平台。这两种形式中，既有部件都承担相应的安全功能，其失效都会影响整个列车控制系统安全功能的实现，因此需要采取相应的控制措施。

既有部件失效导致列车运行控制系统功能失效，从而不能完成安全控制功能的根本原因有随机性失效和系统性失效[1]。随机性失效发生在硬件上，主要是由于硬件本身固有物理、化学、机械等特

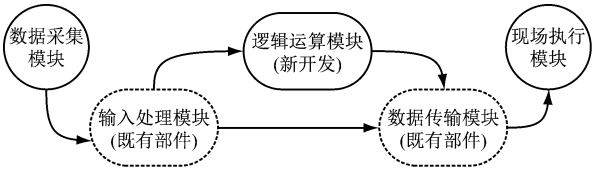

图 2　既有部件作为独立的节点

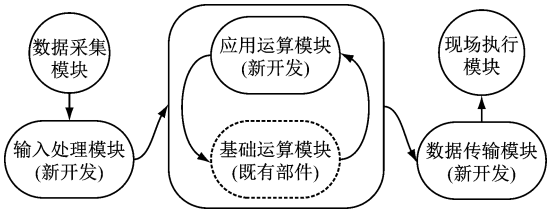

图 3　既有部件作为节点的一部分

性决定的退化机理而产生的,是在随机时间出现的失效,这类失效发生的概率可以预计,但具体发生的时间不可确定。系统性失效是由于系统的设计、实现、制造过程中,或者是运用和维护过程中由于人为错误造成的失效,系统性失效只有针对失效原因进行修改后才能消除,其发生的概率不可精确预计。从安全的角度,系统开发过程中需要识别并控制既有部件以上两种类型的失效。

3.2　安全证明策略

为保证系统安全,需要对既有部件引起的随机性失效和系统性失效进行识别并提出相应的控制措施。按照标准要求,系统失效的安全风险管控需要从质量管理、安全管理、技术安全设计和量化安全指标计算方面进行,如图 4 所示。

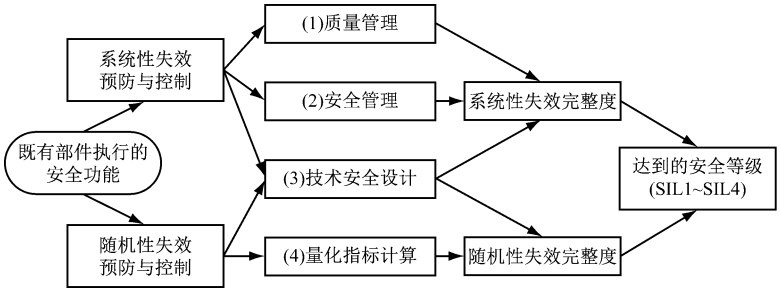

图 4　既有部件的安全保障过程

从失效的控制策略执行的角度,可以采用两种方式证明基于既有部件的列车控制系统满足系统的安全要求:①既有部件本身满足分配的安全功能要求和安全完整度要求;②在系统中采用措施消除或控制既有部件失效对系统安全功能的影响。

4　对既有部件的安全评估要求

列车运行控制系统中采用的既有部件应满足相关系统安全功能所分配的 SIL 要求,根据既有部件类型和控制策略,针对既有部件有如下安全评估的要求。

4.1　既有软件

既有软件作为一种常见的既有部件存在形式,应用于所有 SIL 的系统中,为执行开发过程中的安全分析、开发、验证和确认工作,开发人员应确保获取既有软件的以下信息:①开发中分配给既有软件的功能和性能要求;②既有软件已经具有的功能和性能;③既有软件对应用环境的要求;④既有软件的外部接口;⑤既有软件的具体配置。基于以上信息,开发人员在系统开发过程中将既有软件集成于系统的开发、测试、验证和确认,并形成相应的文件证据。

既有软件用于 SIL3 或 SIL4 的系统中,除了以上要求之外,还应预防既有软件可能出现的失效及其对整个软件系统的影响,同时采取相应措施,以检测既有软件的失效,并保护系统不受这些失效的影响[2]。在系统验证和确认过程中应确保:①既有软件满足所分配的需求;②系统可以检测到既有软件发生的失效,并可以保护系统不受既有软件失效的影响;③系统满足对既有软件的接口和环境条件。

4.2　包含软硬件的既有部件

系统采用由软硬件组成的既有部件,开发人员需要获得以下关于既有部件的信息:①所能满足的功能和性能;②对外接口;③应用限制条件;④失效率;⑤应用环境条件;⑥具体的配置信息。

开发人员需要采用 IHA(接口危害分析)或者 FMECA(失效模式及影响分析)来识别既有部件引起的危险功能失效。对于识别出来的既有部件每种危险功能失效,都需要根据相关安全功能的 SIL(SIL1 ~ SIL4)要求进行如下证明:①由于既有部件内部结构、数据结构或固有物理特性,这些危险功能失效不会发生;②或者为既有部件按照要求的

SIL 提供完整的安全证明;③或者在外部消除既有部件引起的危险失效,并在规定的时间内强制达到安全状态,以达到规定的安全目标。

在分析过程中,由于既有部件的失效模式不能追溯到失效的实际原因。因此,当既有部件执行安全功能时,计算系统的危险失效率计算中应将既有部件的所有失效率(安全失效和危险失效)纳入计算,必须证明既有部件的失效率与系统安全功能所需的 TFFR(可接受危险失效率)相匹配。

4.3　采用使用经验证明的要求

有的既有部件虽然在开发过程中没有遵循安全标准进行开发,但经过长时间的实际应用表明其可靠性和安全性达到了一定的水平,如果列车运行控制系统开发过程中采用了这一类既有部件,则可以考虑采用使用经验证明(Proven in Use)其安全性或可靠性的要求。采用这一方法时,进行安全评估时要考虑以下方面的证据:①既有部件在应用过程中的配置没有发生变化;②系统所需要的功能在既有部件的应用中已经使用;③既有部件至少在 10 个以上的不同地点进行 1 年以上的应用[1];④具有严格的故障报告记录系统,可以提供既有部件在应用过程中发生的所有故障信息;⑤根据 SIL 确定的具体无安全相关故障运行时间证明。

对于既有部件需要具有的无危险性失效的运行时间,参照基础安全标准 IEC 61508 中[3]的要求,针对不同的 SIL 和数据置信度,其要求的无失效总运行小时如表 2 所示。

表 2　既有部件的分类

SIL	每功能每小时的 TFFR	无失效总运行时间/h	
		置信度 0.95 时	置信度 0.99 时
1	$10^{-6} \leqslant TFFR < 10^{-5}$	3×10^6	4.6×10^6
2	$10^{-7} \leqslant TFFR < 10^{-6}$	3×10^7	4.6×10^7
3	$10^{-8} \leqslant TFFR < 10^{-7}$	3×10^8	4.6×10^8
4	$10^{-9} \leqslant TFFR < 10^{-8}$	3×10^9	4.6×10^9

5　结语

列车运行控制系统开发过程中采用既有部件可以加快开发进度,但既有部件的使用应满足系统所分配的安全要求。通过以上分析可知,采用既有部件承担部分列车运行控制系统安全功能是一个可行的做法,但需要针对既有部件的类型和特点进行安全分析,并将既有部件纳入到系统的设计、开发、验证和确认活动中,在这个过程中收集既有部件的相关信息和安全证据。同时,根据系统安全要求,开发设计过程中需要采取相应的安全措施,以检测并控制既有部件的失效。

参考文献

[1] CENELEC. Railway applications: safety related electronic systems for signalling: EN 50129[S]. Brussels, 2018:130.

[2] CENELEC. Railway applications: software for railway control and protection systems: EN 50128[S]. Brussels, 2011:41.

[3] IEC. Functional safety of electrical/electronic/programmable electronic safety related systems (part 7): overview of techniques and measures: IEC 61508-7[S]. Brussels, 2010:107.

(收稿日期:2021 - 01 - 14)

(上接第 129 页)

[6] 乔志. 跨座式单轨交通车辆-轨道梁耦合系统动力问题研究[D]. 北京:北京交通大学,2016.

[7] 刘国超. 跨座式单轨交通钢轨道梁地震响应分析[D]. 成都:西南交通大学,2011.

[8] 武农,雷慧锋,郭锴. 跨座式单轨作为中等规模城市轨道交通模式的适应性分析[J]. 隧道建设,2015(7):623.

[9] 马继兵. 跨座式单轨交通系统结构静动力行为研究[D]. 成都:西南交通大学,2008.

[10] 中华人民共和国住房与城乡建设部. 建筑结构荷载规范:GB 50009—2012[S]. 北京:中国建筑工业出版社,2012:12.

[11] 胡瑞青,王士民. 泥炭质土不同赋存条件对盾构隧道衬砌结构动力响应特性影响分析[J]. 铁道标准设计,2017(8):101.

(收稿日期:2019 - 05 - 10)