SFMEA 方法在列控系统中的应用

焦 婷 王 薇
卡斯柯信号有限公司 北京 100070

【摘 要】列控系统作为轨道交通列车运行的中枢控制系统，是保证轨道交通行车安全和提高运输效率的重要技术装备，在该系统中，起核心控制作用的软件一旦失效可能会引发脱轨、撞车等一系列严重的行车事故，从而造成人员伤亡等灾难性的后果。因此，对于这一类承担行车安全功能的安全关键软件，在软件设计过程中开展安全性分析，避免系统故障导致严重安全事故是非常重要的一环。软件安全性分析常采用软件失效模式与影响分析 SFMEA 法、软件 FTA 等方法，本文主要利用 SFMEA 方法，对列车运行控制系统中的临时限速服务器（TSRS）子系统软件进行安全性分析，识别软件设计缺陷，并采取相应的改进措施，从而提高软件的安全性和可靠性。

【关键词】软件安全；列控系统；SFMEA

1.SFMEA 方法概述

SFMEA 主要应用于软件开发过程的早期，即软件需求和软件架构设计阶段。该方法通过识别软件失效模式，分析失效造成的后果以及失效原因，评估失效产生的影响并采取相应的改进措施来提高软件的安全性。该方法已被成功应用于军用产品、汽车、航空航天等领域。

2.SFMEA 在 TSRS 子系统中的应用

SFMEA 的实施流程如下：先定义软件约定层次，确定分析对象；再分析失效模式和失效原因；结合被分析软件的功能，分析失效产生的安全影响以及严重程度；针对产生安全影响的失效制定改进措施；编写 SFMEA 报告记录分析过程，汇总软件安全需求。

2.1.定义软件约定层次

定义软件约定层次的目的是为了确定 SFMEA 分析的对象。通过分解软件功能，将分析对象确定为每一个软件功能单元。本文分析的对象是 TSRS 子系统软件。在列控系统中 TSRS 子系统软件主要承担临时限速命令（TSR）处理的功能。TSR 命令是动车组控车的重要命令，统一由中心调度员通过 CTC 设置和取消，经由 CTC 下发给 TSRS 子系统，TSRS 子系统接收并处理 CTC 系统下发的 TSR 设置、校验、取消命令，并向外部接口 TCC、RBC、相邻 TSRS 系统下达 TSR 命令，用于指定区段的列车运行速度控制。TSRS 子系统软件的主要功能包括：①初始化功能用于加载离线数据文件；②输入数据解析功能用于接收、解析、保存来自外部设备 CTC、TCC、RBC、相邻 TSRS 的数据；③TSR 处理功能用于校验限速命令参数，并执行 TSR 命令；④TSR 状态综合功能用于对 TCC、RBC、相邻 TSRS 返回的 TSR 状态进行综合判定，并反馈给 CTC 设备；⑤限速初始化命令处理功能用于限速初始化命令的下达与判定；⑥生成输出数据功能用于生成发送给 TCC、RBC、相邻 TSRS 的数据包。

2.2.确定软件失效模式

软件失效模式是指软件失效发生的不同方式。软件的失效是由软件中潜在的数据错误、逻辑处理错误等软件的缺陷引起，均属于系统性失效。在国军标《GJB/Z 1391-2006 故障模式、影响及危害性分析指南》中，已经给出了嵌入式软件的失效模式分类以及举例。结合 TSRS 软件的特点，以限速命令处理功能为例，选取以下失效模式：未输出临时限速命令、输出错误的临时限速命令。

2.3.分析软件失效的原因

软件失效的原因是软件内部潜在的缺陷，在进行原因分析时，应结合该功能相关的软件需求全面地去分析。针对 TSRS 软件的 TSR 处理功能失效原因分析如下：（1）未输出 TSR 命令。TSR 处理功能未输出临时限速的原因可能是 TSRS 软件的 TSR 处理功能没有被软件执行；或者 TSR 命令获取失败，未读取到输入数据解析功能输出的 TSR 命令。（2）输出错误的 TSR 命令。中心调度员下发 TSR 命令的时候，可能存在错误操作，下发的限速未按照限速规则设置，导致 CTC 下发给 TSRS 的限速参数是非法的，当 TSRS 软件未对限速命令合法性进行检查就保存了限速命令，将不合法的参数，如操作者 ID，判断为合法参数，将导致限速的 TSR 处理功能输出错误的临时限速。

2.4.分析软件失效的影响及严重程度

分析软件失效的影响及严重程度的目的是为了识别软件失效之后对系统输出的影响，确定影响的严重等级，从而制定缓解措施。本文使用铁路行业广泛使用的 EN50129 标准中推荐的事故严重度，定义了四类危害严酷度等级：

I 特大 影响大量人员且导致多人死亡

II 重大 影响非常少的人员且导致至少一人死亡

III 次要 无死亡，只有严重或者轻微伤害

IV 轻微 可能会造成轻微伤害

影响分析过程如下：（1）未输出 TSR 命令。未输出 TSR 命令将导致 TSR 处理功能未能保存合法的限速命令，从而导致 TSRS 系统无法正常下发 TSR 命令给 TCC/RBC，影响系统可用性，无安全影响。（2）错误的 TSR 命令。错误的 TSR 命令将导致限速参数错误的 TSR 命令被保存下来，比如操作者 ID 错误、限速值错误等都将导致 TSRS 发送错误的 TSR 命令给 TCC/RBC，从而导致脱轨这样的重大事故。

2.5.制定缓解措施

基于 TSRS 临时限速命令处理功能失效分析，对每个失效的原因制定缓解措施。（1）未输出 TSR 命令。无安全影响，无需制定缓解措施。（2）错误的 TSR 命令。针对失效可能的原因，如操作者 ID 错误，执行缓解措施如下：TSRS 软件应对来自 CTC 的 TSR 命令中的操作者 ID 进行合法性检查，若操作者 ID 非法，TSRS 应丢弃该限速。

2.6.编写 SFMEA 报告

将上述分析的过程以软件 FMEA 表的形式形成记录，汇总安全需求，作为后续安全保障工作的输入。

3.结语

随着轨道交通行业的快速发展，铁路运输带给人们便利的同时，其安全性也一直被行业内外关注，但以目前的技术发展水平，无法保证软件的绝对安全。本文结合 SFMEA 方法，通过对执行安全功能的软件开展失效模式、失效原因、失效影响及严重程度的分析，针对产生危害的失效原因制定相应的缓解措施，可以尽早发现软件设计阶段的安全缺陷，再通过后续对缓解措施的安全管理，进一步提升软件了的安全性。

【参考文献】

[1]GJB1391—2006 故障模式、影响及危害性分析指南.

[2]张仝伟.SFMEA 方法在飞行控制软件中的应用.航天控制,2007.

[3]刘正高.软件 FMEA 技术的应用策略.质量与可靠性,2005.