

# 信息流视域下的轨旁静态数据安全管理工作优化方法<sup>\*</sup>

江 迎 魏 倩 朱孟雯

(卡斯柯信号有限公司, 200071, 上海 // 第一作者, 高级工程师)

**摘 要** 为提高列车运行控制系统数据安全管理工作质量, 增强系统部署的安全信心, 从信息流的视域构建了列车运行控制系统安全信息流模型, 并结合信息安全流事故致因理论, 进行模型分析。轨旁静态数据安全管理工作对于整个列车运行控制系统安全性有重要意义。提出现有数据管理方法在 4 个维度上的缺陷, 利用 Python 语言开发验证软件, 实现了 4 个优化维度的设计。

**关键词** 城市轨道交通; 全自动列车运行控制系统; 安全信息流; 轨旁静态数据; 数据安全管理工作

**中图分类号** U231.6

**DOI:** 10.16037/j.1007-869x.2021.04.005

## Optimization Method of Trackside Static Data Security Management from Perspective of Information Flow

JIANG Ying, WEI Qian, ZHU Mengwen

**Abstract** In order to improve the data security management quality of the FAO train control system and to enhance the security confidence of the system deployment, a system security information flow model is constructed from the perspective of information flow. With information security flow accident cause theory, model analysis is conducted. Trackside static data security management is of great significance to the overall safety of the whole train control system. The defects of the existing data management methods are proposed from four dimensions. Python is used for verifying the software and realizing design optimization from the four dimensions.

**Key words** urban rail transit; FAO train control system; safety information flow; trackside static data; data safety management

**Author's address** CASCO Signal Ltd., 200071, Shanghai, China

城市轨道交通全自动驾驶系统是现阶段最新的城轨控制技术, 其核心目标是实现对列车的全程自动化控制。轨旁静态数据 (SGD) 是列车运行控制系统 (以下简称“列控系统”) 运行的基础数据信

息, 其详细表达了线路的基本参数状态、站台设置情况以及线路特殊的保护区域, 是实现列车高效安全运行的保障性数据信息, 是安全数据安全管理工作流的核心, 对驾驶控制、自动休眠及唤醒、软件系统控制升级等列车运营功能<sup>[1-2]</sup>具有重要的意义。现阶段, 对 SGD 的安全管理工作方法是按独立双链形式进行人工验证计算。这虽可以一定程度上提高数据的准确性, 但人为失误的不可消除性与验证方法的繁琐性, 致使 SGD 安全工作的效率低, 效果不佳。文献[3]曾指出: 人的工作流失误是导致事故的主要原因。文献[4]等认知心理学领域的相关研究结论表明: 表现层面的工作行为失误, 其本质来源于深层次的信息认知偏差。文献[5]论述了随着自动化控制系统的发展, 当出现信息流缺失或者短路时可能导致的严重安全事故后果。文献[6-8]阐明了信息流作为系统安全的生命线, 在系统各个控制层级的迭代控制作用中所起到的关键作用, 证明了构建系统安全信息流模型的重要性和必要性。

列控系统的 SIL (安全完整性等级) 分为 4 级, 却鲜有文献针对城市轨道交通列控系统, 从信息流视角进行安全模型构建。鉴于此, 本文将构建列控系统安全信息流模型, 依据信息安全流事故致因理论, 分析该模型的安全需求, 设计出优化 SGD 轨道静态数据的安全管理工作方法, 继而利用 Python 语言开发辅助软件工具来实践上述优化, 并对 SGD 的安全管理工作流程进行规范和优化, 以降低人为安全验证的失误率, 提高项目的安全可接受指标, 以期对开发数据辅助管理工具和实现整个系统更高的安全需求提供理论依据。

## 1 列控系统安全信息流模型

### 1.1 模型的理论基础

从安全原理的角度看, 列车全自动驾驶系统可

<sup>\*</sup> 上海市工业强基专项项目 (GYQJ-2018-2-03)

以抽象为物质流、能量流及信息流的耦合体<sup>[9]</sup>。对列控系统结构具象化描述如下:物质流层面由信号基础设备、车载设备、轨旁设备及联锁设备等组成;能量流体现在车辆动能状态控制、火灾检测信息反馈及车辆授权终点位置信息等方面;信息流在列控系统耦合体中是实时动态更新变化的,反映了列控系统即时的可用性状态和安全状态。系统安全运行的本质表现为安全相关信息流的稳定有序流动,因此,安全管理的着力点需立足于对安全相关信息的流动指示、导向、监测、控制、警戒和利用。

### 1.2 模型结构

如图 1 所示,列控系统安全信息流模型主要由 3 个圈层组成。

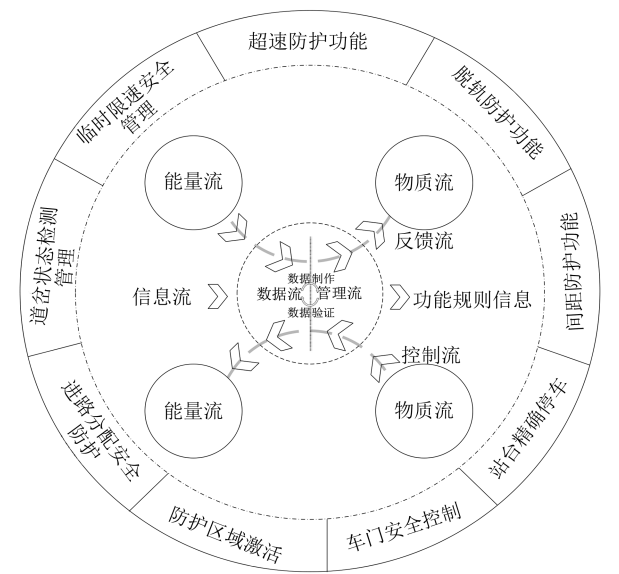


图 1 列控系统安全信息流模型

1) 核心圈层表示列控系统的安全信息流由数据流和管理流两部分组成。数据流包括 SGD、ZC (区域控制数据)、LC (全线同步控制数据) 及 CC (车载数据);管理流在数据制作阶段体现为线路基本运行规则、项目特殊配置规则、安全标准、特殊参数人工配置规范等知识类支持信息。数据流与管理流在系统设计制作的过程中,通过对应的数据制作和数据验证等管理活动,进行迭代更新,直到最终完成系统需求的全部功能和安全需求,形成稳定的功能规则信息,使得物质流可以对能量流进行有序的控制。

2) 中间圈层表示安全信息流是物质流和能量流的交流媒介。物质流→信息流→能量流的运行途径为列控系统控制流,能量流→信息流→物质流

的运行流程为列控系统反馈流。当安全功能对应的控制流和反馈流稳定正常流动时,列控系统就实现了安全有序的运行。

3) 最外的圈层概括了列控系统的 9 大功能:超速防护功能、脱轨防护功能、车间距防护功能、站台精确停车功能、车门安全控制功能、特殊防护区激活功能、进路安全分配联锁防护功能、道岔状态检测管理功能及临时限速安全管理功能。每个功能的实现依赖于内部多条信息流并行或有特定次序的流动。9 大功能的完整执行是信息流稳定流动的外在表象。

## 2 SGD 数据管理工作流的优化

### 2.1 工作流优化的必要性

基于上述安全信息流模型进行分析可知:物质流对能量流的有效控制依赖于数据流与管理流的协调统一;功能规则信息是构成控制系统的数据基础,有“信息阀门控制”作用;完善的功能规则信息可以将整个控制系统有机结合在一起。

随着列控技术的自动化程度日益成熟,列控系统安全功能对功能规则信息的依赖将更为明显。如图 2 所示,SGD 作为最基础的功能规则信息,通过与管理流信息的迭代更新、循环流动,生成其他数据信息,继而汇合统一构成功能规则信息,为能量流与物质流的交互流动创造规则路径和驱动力。

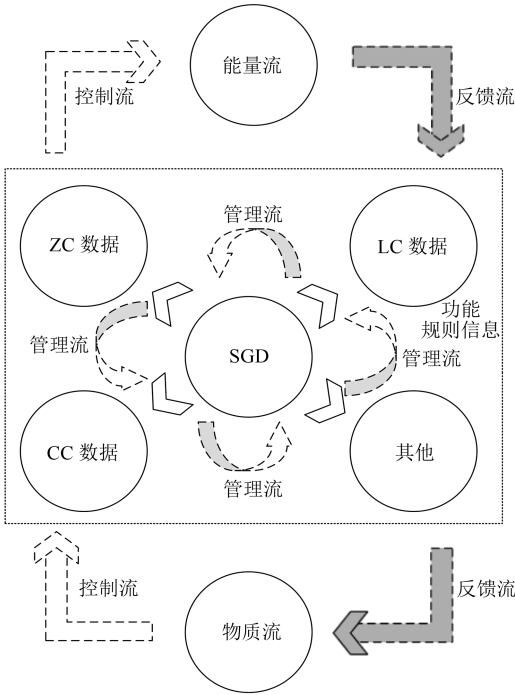


图 2 功能规则信息的组成

因此,SGD 的制作和验证是安全管理工作中最重要的一环。

### 2.2 信息流视域下的数据管理工作流四维度优化

数据管理工作流程实质是对各类规则信息的整合、分析和处理。从信息流角度来审视,数据管理工作可抽象为信息整合获取、信息分析处理及信息输出决策等 3 大阶段。相应的,现有数据管理工作流程为:人工判断上游输入文件信息、人工识别参数规则配置准确性、人工进行数据存储格式的转

变、人工生成验证报告结果。文献[10-11]提出了信息安全流事故致因理论中的个人风险决策研究框架为“技能-规则-知识( Skills-Regulations-Knowledges)”。由此可知,在以人为主的信息流处理流程中,风险主要来源于 4 个维度:技能缺失维、规则缺陷维、知识缺乏维及心理状态维。4 个维度优化流程如图 3 所示。当人工处理信息时,往往会由于这 4 个维度的影响而导致信息流的错误流动,从而为整个列控系统埋下安全隐患。

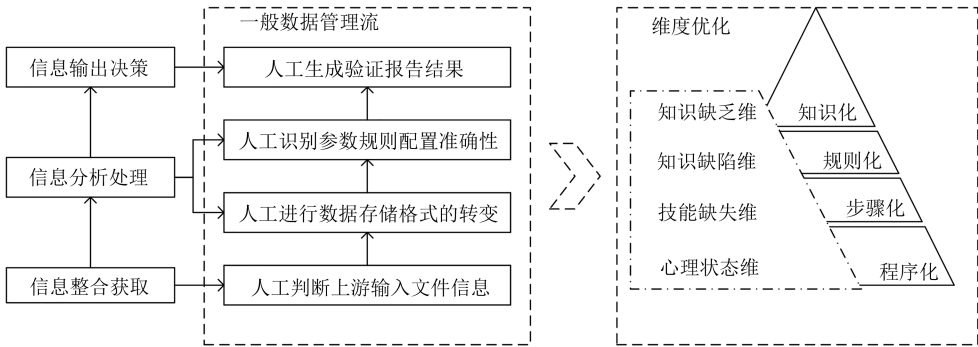


图 3 4 个维度优化流程

针对 4 个风险源维度,要提高列控系统的风险防控能力,就应从程序化、规则化、步骤化、知识化等角度,优化现有的 SGD 安全管理流程。

1) 程序化:基于 Python 语言开发的验证软件,可利用验证软件的高效和低错误率来规避人工劳动低效和随机出错的问题。

2) 规则化:将参数验证的规则方法内化为程序算法。将人的工作职责由原来的验证执行者变为验证监督者,从而提高验证结果的准确性。

3) 步骤化:利用程序运行的天然逻辑关系,将人工验证时容易出现的工作流无序、紊乱、倒流等特殊情况进行屏蔽。操作者根据程序的提示逐步完善数据管理工作。

4) 知识化:验证软件不仅能为验证者计算出推荐的参数值,而且还能将该参数涉及到的相关信息全部整理出来,以方便验证人员核查,并对该参数相关的知识进行必要的提示。

### 3 验证软件的开发

Python 语言配置了 openpyxl、tkinter、docx、xml 等类库。结合 SGD 数据管理流程的特殊性,以 4 个维度优化为着力点,验证软件的开发可实现以下功能:①整合各种格式的输入文件,将来自 Excel、

xml、Word 3 类不同文档中的数据进行保存、调用和处理,极大地提高了工作效率;②通过人机交互界面实现对验证者的数据管理工作流程把控,从而屏蔽可能出现的流程错误问题;③软件将 SGD 参数的配置规则内化为算法,可根据参数名来识别参数,进而调用来自其他格式输入文件的参数计算信息,进行对应的参数验证计算;④将各参数对应的计算验证方法和相关计算信息保存在验证报告中,供验证者对验证结果检查、学习和记忆,提高验证结果的准确性。图 4 为验证软件的交互界面。



图 4 验证软件的交互界面

验证软件的运行流程如图 5 所示。为使数据管理过程实现有序化和不可逆化,依次分 3 步进行:第 1

步,参数是否缺失确认工作;第2步,项目数据导出和转化工作;第3步,数据自动验证工作。每一步完成后,均要求验证人员判断阶段性数据结果。只有数据结果满足逻辑条件,才会将生成文件作为输入文件,参与到下一步的运算中。阶段性的检查有利于寻找数据错误的原因,提高最终数据验证结果的一致性。

由于不同项目可能具有不同的特殊环境或者特殊功能配置,软件内置的数据配置规则不可能完全适应于全部项目的所有参数配置;因此,只有软件的最终输出结果经过人工核查后,才可以确认数据验证工作的完成,从而实现完美的人机互补,发挥软件和人工在数据管理工作流中的各自优势。

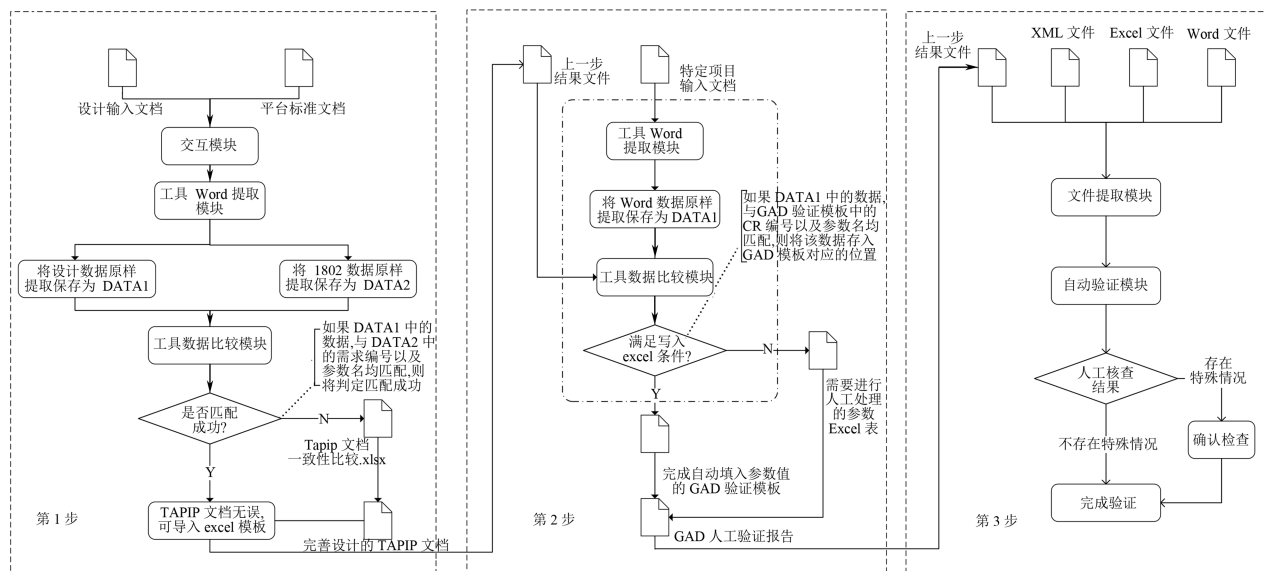


图5 辅助验证软件运行流程

## 4 结语

1) 构建了列控系统的安全信息流模型,并基于安全原理分析整个列控系统的信息流动。SGD 数据管理工作流是整个列控系统信息流安全的根本保障。

2) 立足于现有的数据管理工作流程,从信息事故致因的4个维度总结了风险产生的原因,进而对4个优化维度进行了重新设计,为下一步程序设计提供了理论指导。

3) 利用 Python 语言的特质,开发了可以整合各类数据信息、内化规则算法、提供知识帮助的辅助验证软件,提高了数据验证工作的效率和准确率。此项工作对提高整个列控系统的安全性能而言,意义重大。

## 参考文献

- [1] 孙守胜.城市轨道交通信号系统新技术发展前景[J].电子技术与软件工程,2019(24):33.
- [2] 张海涛,梁汝军.地铁列车全自动无人驾驶系统方案[J].城市轨道交通研究,2015(5):33.

- [3] PELOPIDAS B. Normal accidents living with high-risk technologies[J]. Critique,2012(783):710.
- [4] 鲁津维.认知诊断理论、模型及应用[J].科教文汇,2019(9):42.
- [5] LEVESON N. A new accident model for engineering safer systems[J]. Safety Science,2004(4):237.
- [6] WESTRUM R. The study of information folw: A personal journey[J]. Safety Science,2014(8):58.
- [7] HOVDEN J, STØRSETH F, TINMANNSVIK R K. Multilevel learning from accidents-case studies in transport[J]. Safety Science,2011(1):98.
- [8] HOVDEN J, ALBRECHTSEN E, HERRERA I A. Is there a need for new theories, models and approaches to occupational accident prevention? [J]. Safety Science,2010(8):950.
- [9] 黄浪,吴超,马剑.安全信息流视域下的事故致因模型构建[J].管理评论,2020(4):274.
- [10] RASMUSSEN J. Skills, rules, and knowledge; signals, signs, symbols, and other distinctions in human performance models[J]. IEEE Transactions on Systems Man & Cybernetics,1983,13(3):257.
- [11] WEI G. Prediction of soil settlement caused by double-line parallel shield tunnel construction [J]. Disaster Advances,2013(6):23.

(收稿日期:2020-09-25)