基于STPA的安全分析方法在下一代列车运行控制系统中的应用

汇报人：

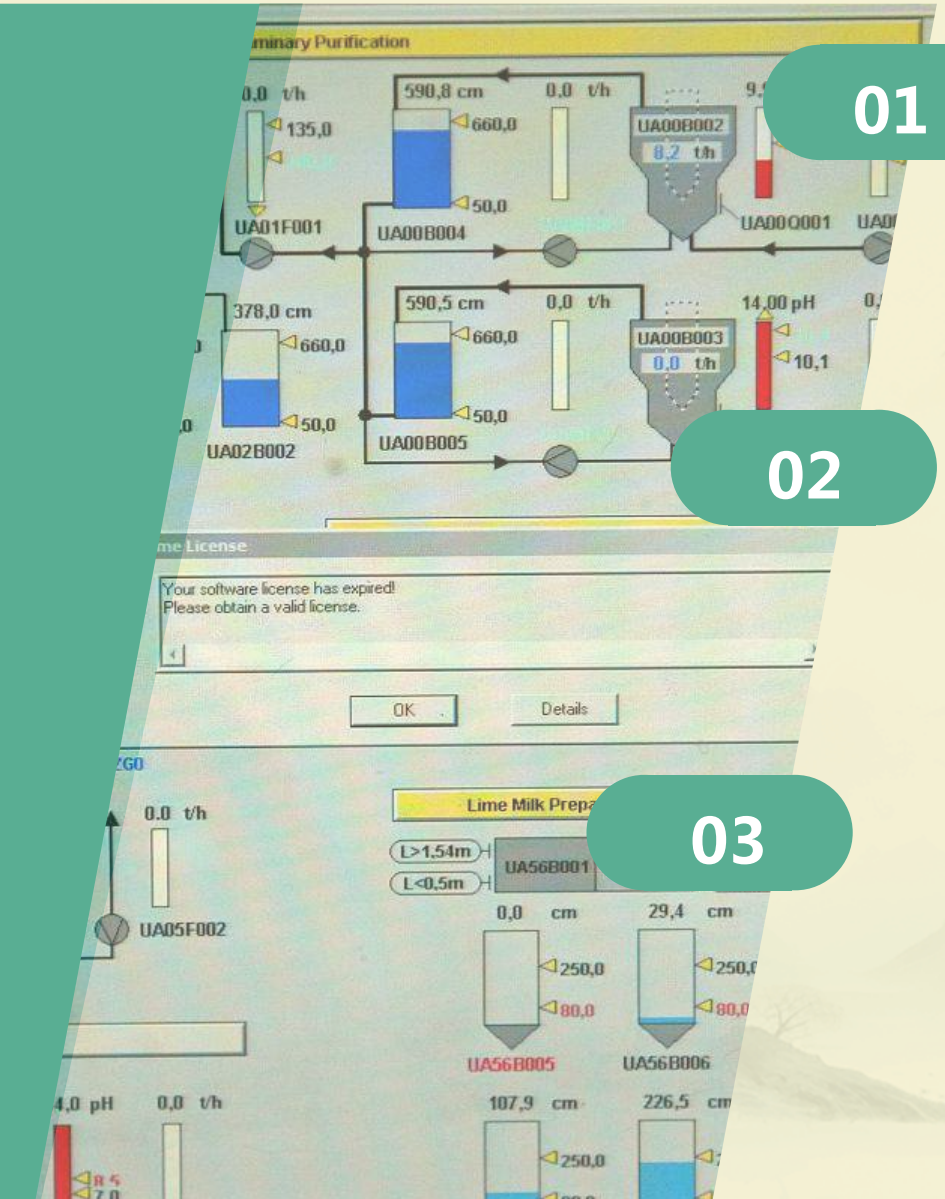
2024-01-11

目录

01

引言

研究背景与意义



01

列车运行控制系统的重要性

列车运行控制系统是保障列车安全、高效运行的关键技术之一，其安全性直接关系到乘客生命财产安全。

02

下一代列车运行控制系统的挑战

随着列车运行速度的不断提高和运营环境的日益复杂，下一代列车运行控制系统面临着更高的安全要求和挑战。

03

基于STPA的安全分析方法的意义

STPA（系统理论的过程分析）是一种基于系统理论的安全分析方法，能够从系统层面深入分析安全问题，为下一代列车运行控制系统的设计和开发提供有效的安全保障。

国内外研究现状及发展趋势

国内研究现状

目前，国内在列车运行控制系统的安全性研究方面取得了一定的成果，但主要集中在传统列车运行控制系统上，对下一代列车运行控制系统的安全性研究相对较少。

国外研究现状

国外在列车运行控制系统的安全性研究方面起步较早，已经形成了较为完善的研究体系，并在实际应用中取得了显著成效。

发展趋势

随着列车运行控制系统的不断发展和升级，未来研究将更加注重系统层面的安全性分析和评估，以及基于大数据、人工智能等技术的智能安全保障技术的研究和应用。

研究内容、目的和方法

要点一

研究内容

本研究将基于STPA的安全分析方法，对下一代列车运行控制系统的安全性进行深入分析，包括系统架构、功能需求、运行环境等方面的安全性问题。

要点二

研究目的

本研究旨在通过基于STPA的安全分析方法，识别下一代列车运行控制系统中的潜在安全风险，提出相应的安全保障措施和建议，为系统的设计和开发提供有效的安全保障支持。

要点三

研究方法

本研究将采用文献综述、案例分析、专家访谈等方法，收集相关数据和资料，运用STPA方法对下一代列车运行控制系统的安全性进行分析和评估。同时，结合实际情况，提出针对性的安全保障措施和建议。

02

STPA安全分析方法概述

STPA基本原理

基于系统理论的过程分析（STPA）

STPA是一种基于系统理论的安全分析方法，通过识别和分析系统中的不安全控制行为，以及导致这些行为的潜在原因，来预防事故和降低风险。

控制结构和控制行为的识别

STPA关注系统中的控制结构和控制行为，通过分析控制行为的执行条件和约束，来识别潜在的安全隐患。

危险致因的识别和分析

STPA强调对危险致因的识别和分析，包括设计缺陷、人为因素、环境因素等，以全面评估系统的安全性。

STPA在列车运行控制系统中的适用性

1

列车运行控制系统的复杂性

列车运行控制系统是一个复杂的系统，涉及多个子系统和交互界面，STPA能够全面分析系统中的不安全控制行为。

2

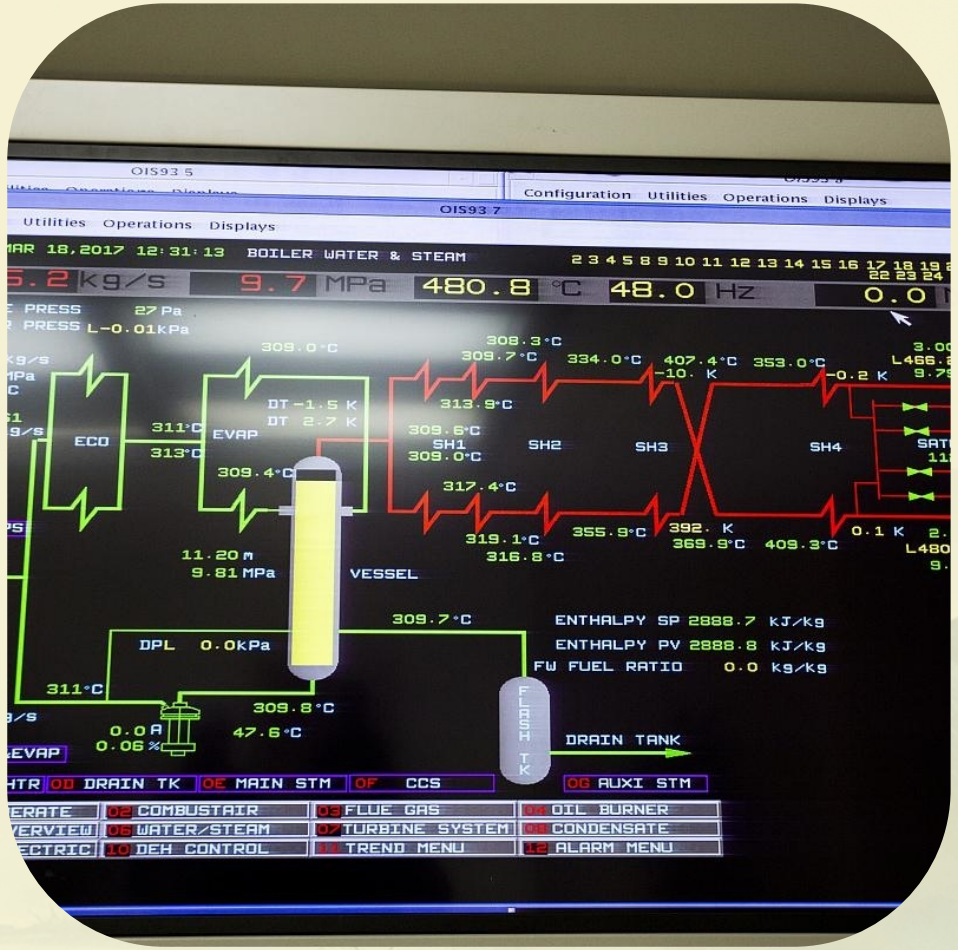
安全关键性

列车运行控制系统的安全关键性要求非常高，STPA能够深入识别和分析系统中的潜在安全隐患，提高系统的安全性。

3

事故预防

通过STPA分析，可以识别列车运行控制系统中的潜在危险致因，并采取相应的预防措施，降低事故发生的概率。



STPA与其他安全分析方法的比较

与FMEA的比较

FMEA（故障模式与影响分析）主要关注组件级的故障模式及其对系统的影响，而STPA更侧重于系统级的控制行为和危险致因分析。

与HAZOP的比较

HAZOP（危险与可操作性分析）主要关注工艺流程中的潜在危险和操作问题，而STPA更适用于复杂系统的安全分析，包括列车运行控制系统。

与FTA的比较

FTA（故障树分析）是一种自上而下的分析方法，通过构建故障树来识别导致顶事件的底事件。而STPA则是一种自下而上的分析方法，从系统的控制行为出发，识别潜在的安全隐患。

03

下一代列车运行控制系统概述

下一代列车运行控制系统架构与特点

分布式系统架构

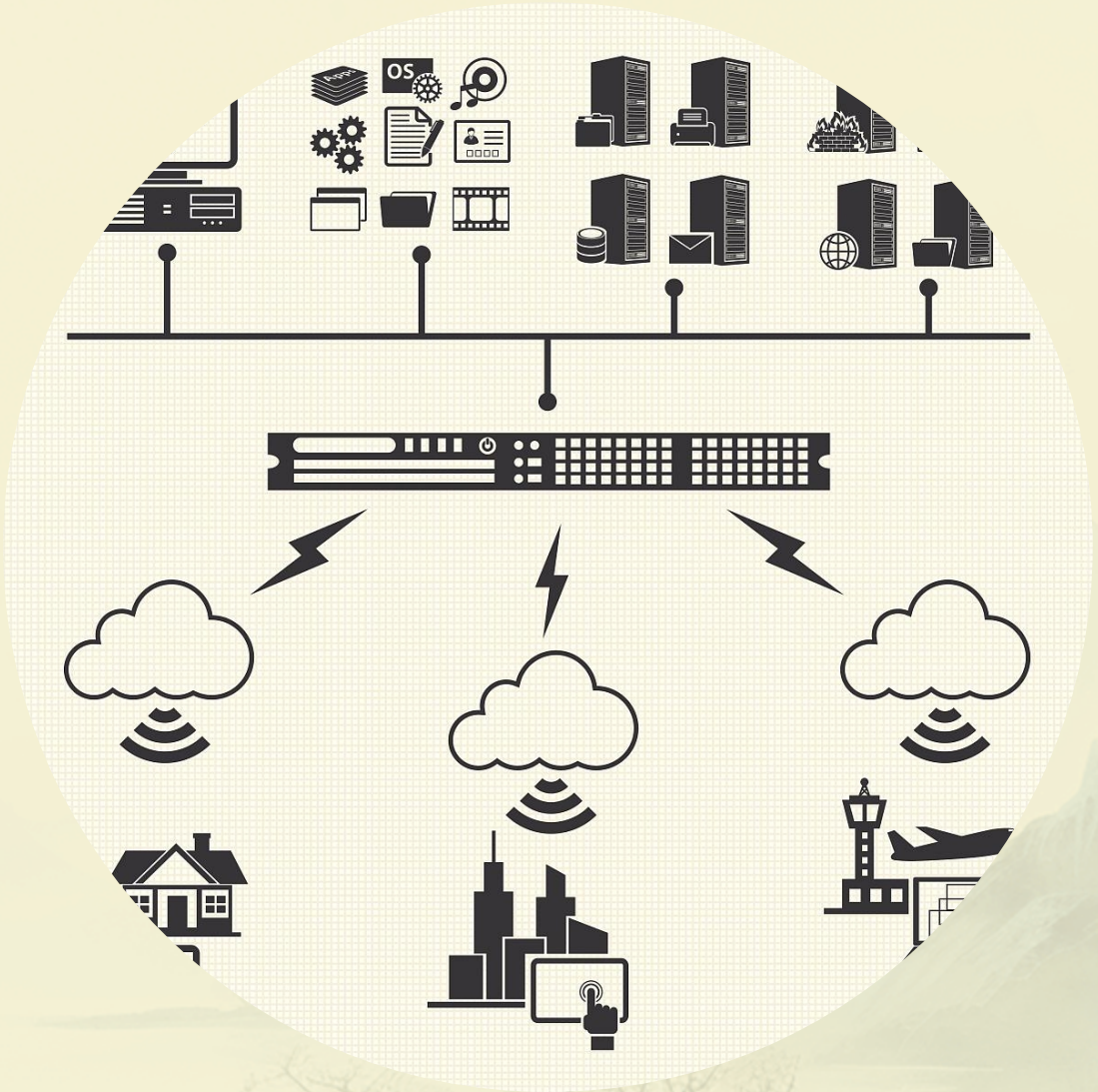
下一代列车运行控制系统采用分布式系统架构，实现车地协同控制和信息高效传输。

智能化决策支持

系统具备自主学习和决策能力，能够根据实时数据和历史经验进行智能分析和预测。

高可靠性设计

系统采用冗余设计和故障隔离技术，确保在设备故障或异常情况下仍能保障列车安全运行。



关键技术与挑战

01

车地通信技术

实现车地之间高速、可靠的数据传输，确保列车运行控制系统的实时性和准确性。

02

多传感器信息融合

对来自不同传感器的信息进行融合处理，提高系统对环境的感知能力和决策准确性。

03

人工智能技术应用

利用人工智能技术实现列车运行状态的实时监测、故障预测和智能调度等功能。

安全性要求及标准

功能安全标准

遵循国际电工委员会（IEC）的功能安全标准，如IEC 61508和EN 50128等，确保系统设计的安全性和可靠性。

安全完整性等级（SIL）

根据风险评估结果，确定列车运行控制系统的安全完整性等级，并采取相应的设计和验证措施。

安全生命周期管理

实施严格的安全生命周期管理，包括需求定义、设计、实现、测试、验证和维护等阶段，确保系统在整个生命周期内的安全性。