doi: 10.7690/bgzdh.2026.10.003

基于 FTA 和 FMEA 的连续式风洞安全联锁系统

肖厚元[1]，桑　博[2]，王　斌[1]，张文清[1]，刘轩岑[1]，何虹亮[1]
（1. 中国空气动力研究与发展中心设备设计与测试技术研究所，四川 绵阳 621000；
2. 中国空气动力研究与发展中心高速所，四川 绵阳 621000）

摘要：针对某连续式风洞系统组成庞大且运行复杂的特点，提出一种将故障树分析（fault tree analysis，FTA）和故障模式及影响分析（failure mode and effect analysis，FMEA）相结合的故障综合分析方法。以风洞运行故障为顶事件建立某连续式风洞的故障树模型，自上而下归纳出导致顶事件发生的重要故障底事件。利用 FMEA 对各底事件进行分析评定，识别出所有影响风洞运行安全的故障模式。在此基础上，开发一套基于分布式 PLC 的风洞安全联锁系统。风洞各工艺子系统对关联故障底事件进行状态监测，安全联锁系统负责采集所有子系统的故障判别结果和关键风洞状态信息，并在出现故障时统一调度实现整个风洞的安全联锁停车。测试结果表明：该安全联锁系统能及时发现风洞运行中的故障和隐患，并执行完善的紧急停车联锁逻辑，可以有效保障人员和设备的安全，并为操作人员进行故障检修提供可靠的决策辅助。

关键词：连续式风洞；FTA；FMEA；安全联锁；分布式 PLC
中图分类号：TP277.1　　**文献标志码：**A

Safety Interlock System of Continuous Wind Tunnel Based on FTA and FMEA

Xiao Houyuan[1], Sang Bo[2], Wang Bin[1], Zhang Wenqing[1], Liu Xuancen[1], He Hongliang[1]
(1. *Facility Design and Instrumentation Institute*, *China Aerodynamics Research and Development Center*, *Mianyang* 621000, *China*; 2. *High Speed Institute*, *China Aerodynamics Research and Development Center*, *Mianyang* 621000, *China*)

Abstract: Aiming at the huge system composition and complex operation of a continuous wind tunnel, a method of combining fault tree analysis (FTA) and failure mode and effect analysis (FMEA) is proposed. The fault tree model of a continuous wind tunnel is established by taking the operation fault of the wind tunnel as the top event, and the important fault bottom events leading to the top event are summarized from top to bottom. The FMEA is used to analyze and evaluate the bottom events, and identify all the failure modes that affect the safety of wind tunnel operation. On this basis, a set of wind tunnel safety interlocking system based on distributed PLC is developed. Each process subsystem of the wind tunnel monitors the status of the associated fault events, and the safety interlocking system is responsible for collecting the fault identification results of all subsystems and the key wind tunnel status information, and uniformly dispatching to realize the safety interlocking shutdown of the whole wind tunnel when a fault occurs. The test results show that the safety interlocking system can find the faults and hidden dangers in the operation of the wind tunnel in time, and implement the perfect emergency shutdown interlocking logic, which can effectively guarantee the safety of personnel and equipment, and provide reliable decision-making assistance for operators to troubleshoot.

Keywords: continuous wind tunnel; FTA; FMEA; safety interlock; distributed PLC

0　引言

某连续式风洞是一项集空气动力学、热力学、材料学、低温工程、测控理论等多学科的复杂试验装置，具有深低温无氧环境动态运行、宽工况复杂交变、流固热多态耦合、全自动精准操控等特点[1]。整个风洞共由数十个工艺子系统组成，这些子系统功能特性迥异，涉及不同学科和工程技术领域，使得该风洞运行过程极其复杂，进而对风洞的安全、高效运行提出了极高要求。另一方面，某连续式风洞工艺设备样式繁多，部件结构各异，动态特性复杂，尤其是涉及到大型压缩机旋转机械运行、大型多轴电液复杂机构多自由度复合运动，这些设备的性能和运行状态的好坏，直接关系到整个风洞的安全运行和人身安全。若操控不当、保护措施不完善，有可能出现重大设备损坏甚至是人员伤亡事故，造成巨大的经济损失，因此，风洞运行的安全、可靠性尤为重要。

安全联锁系统作为一种自动安全保护系统，被广泛应用于石油化工等各种工业自动化系统中，其

收稿日期：2025-02-08；**修回日期：**2025-03-08
第一作者：肖厚元（1996—），男，湖南人，硕士。
通信作者：桑　博（1990—），男，山东人，博士。

存在能够有效降低装置运行风险、提高企业生产效率[2]。某连续式风洞作为一种大型科学装置，其工作复杂性显著高于一般过程控制系统，造成运行故障的种类和原因十分庞杂，如何快速理清风洞运行故障的征兆、原因、后果以及处理措施对其安全联锁设计十分重要[3]；然而，在传统的风洞安全联锁设计中，故障分析常常开展得不够全面深入，存在分析时间短、参与人数有限、设计资料利用不充分、系统间联动考虑不足等问题，导致风洞安全联锁设计存在一系列的缺陷或者遗漏。

笔者采用故障模式及影响分析(FMEA)与故障树分析(FTA)联合的方法开展某连续式风洞安全联锁系统设计，通过 FTA 以风洞运行故障作为顶事件建立了风洞故障树模型，自上而下逐层分析导致上一层故障时间的原因，最终获取诱发风洞运行故障发生的重要故障底事件；针对每个故障底事件开展 FMEA 分析，剖析与故障底事件相关的子系统、部件及零件的各种失效模式原因及其对风洞运行可靠性、安全性造成的影响，并对此提出预防措施和改进措施。在此基础上，依托分布式 PLC 搭建安全联锁系统硬件平台，对风洞关键运行参数、故障底事件进行实时采集和监测，根据风洞各子系统之间的相互耦合、相互制约关系建立不同的联锁规则和安全联锁保护动作，确保风洞出现异常时采用正确的安全联锁停车操作，确保人员和设备的安全。

1 研究对象组成

如图 1 所示，某连续式风洞是以液氮为冷媒构造深低温环境进而提高试验雷诺数的特种地面试验设施。

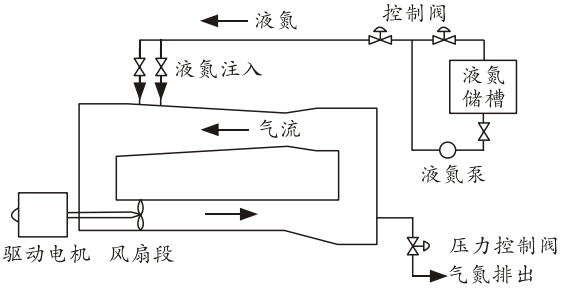

图 1 某连续式风洞工作原理

作为连续式风洞，由轴流压缩机驱动气流在闭合回路中循环，进而在试验段形成目标马赫数；通过在液氮喷射段注入液氮，液氮汽化后吸收压缩机做功以及洞壁传热产生的大量热量，进而降低洞内气流温度；通过气氮排出系统将汽化后的氮气从洞内排出至大气中，进而维持风洞试验所需的气流总压[4]。

按照实现功能不同，该风洞可细分为流动控制系统、洞体机械系统、动力系统、模型运输系统、液氮生产及供给系统、供配气系统、冷却水供给系统、测控系统等十余个工艺分系统，每个工艺分系统又包含许多二级甚至三级工艺子系统，整个风洞共由数十个工艺子系统组成。与此同时，该风洞运行流程极为复杂，涵盖试验准备、模型更换、风洞清洗、降温、增压、吹风试验、回温、气体置换等多种复杂运行工况，每种工况都存在着较多的安全风险，需要各工艺子系统互相解耦，密切配合才能顺利运转。

2 安全联锁功能需求分析

某连续式风洞系统组成复杂，运行流程极其繁琐，试验成本十分高昂，任何一次微小的故障都有可能损坏试验设备，造成重大损失。安全联锁系统作为保障风洞高效安全运行的关键子系统，其根本目的是实时采集并监控各工艺子系统的运行状态，在不同工况下编制不同的联锁规则和安全联锁保护动作，一旦监测到异常状态，自动启动安全联锁程序，并按照预设逻辑执行保护动作，确保风洞运行过程中人员和设备的安全[5]。具体来说，风洞安全联锁系统需要发挥的主要功能为：

1) 通过布置硬接线、传感器采集关键风洞重要运行参数和关键设备状态并监控；

2) 对风洞洞体、动力系统压缩机、部段运动机构等重要设备进行安全保护；

3) 在开洞、更换模型、氮气泄露等条件下对风洞试验人员进行安全保护；

4) 执行风洞各种运行工况前的有效性判断，避免无效吹风或其他动作所造成的人力物力消耗；

5) 安全联锁信息的告警及文本展示，辅助风洞运维人员处理故障。

3 FTA-FMEA 联合分析

3.1 概述

FTA 是一种“自上而下”的故障分析方法，通常采用演绎法建树。先选定一个系统不希望发生的故障作为顶事件，逆着顶事件发生的过程向下逐级分析子系统、部件及零件的故障，直到追溯到无法继续分解的最底层故障，并通过逻辑符号将各级故障之间的逻辑关系表示出来[6]。顶事件位于故障树最上层，一般为造成严重后果的故障事件；底事件

位于故障树各分支末端，是造成顶事件发生的最底层故障。位于故障树顶事件与底事件之间的被称为中间事件。

FMEA 是一种“自下而上”的故障分析方法，采用从局部到整体的归纳分析流程，先将实际系统进行结构肢解，划分成诸多最小单元，然后基于相关技术及质量文件，设计文件、历史收集数据、客户需求等资料对所有最小单元的潜在故障模式及其对系统造成的影响进行研究，包括故障特征、故障原因、故障影响、故障处理措施，并建立完整的故障分析表格，从而寻找预防或改进措施，减少系统故障率，提高系统的可靠性[7]。

FTA 与 FMEA 都是系统可靠性分析方法。FMEA 有条理，但涉及知识广阔，操作繁琐，且只分析与故障模式直接相关的故障特征和故障原因。FTA 逻辑性较强，分析全面，能够清晰地表达事件逻辑关系，但存在耗时长、无法直接用于故障诊断的问题[8]。某连续式风洞工艺设备庞杂，结构、功能及其故障关系复杂，如果单独使用 FTA 或 FMEA，容易存在分析故障原因不全、不准确等问题。若 FTA 的前期分析准备工作不够充分，很容易在建立故障树发生遗漏或冗余，这就对风洞各子系统的资料调研分析提出较高的要求。而 FTA 在资料调研分析阶段遇到的问题正好可以借助 FMEA 来解决。FMEA 中有关故障原因、影响的分析，又可以辅助建立风洞故障树的构造，增强故障树的客观性和合理性[9]。采用 FTA-FMEA 联合法对某连续式风洞进行故障分析，既可以抓住重点，又可以做到较为全面、深入的分析。

3.2　FTA 故障树构造

对于某连续式风洞这样的复杂试验装置，FTA 分析靠单打独斗是无法完成的，通常需要甲方参与风洞设计的各专业人员牵头，同时联合各工艺子系统的承制方深入分析，才能获得客观全面的 FTA 结果。FTA 分析最关键的步骤是建立研究对象的故障树模型，通常把系统的运行故障作为顶事件，然后找出运行故障与导致系统故障诸多因素之间的逻辑关系。选定“风洞运行故障”作为顶事件，根据对该风洞设计原理和工作过程的深入理解，结合其他风洞已有的实际运行状态数据，可以推导出直接引发顶事件发生的 8 个中间事件，分别是洞体结构存在损坏风险、保障系统运行异常、洞体条件预置异常、风洞关键运行参数报警、流场参数控制功能异常、外部(人工)输入故障命令、机构运动功能异常、试验参数测量功能异常。

考虑到某连续式风洞工艺设备数量众多，如果只用单棵故障树表征故障传递链，树的规模将会十分庞大，因此，采用主树和子树相结合的建树方式。顶事件和 8 个中间事件共同构成了该风洞故障树主树，如图 2 所示。

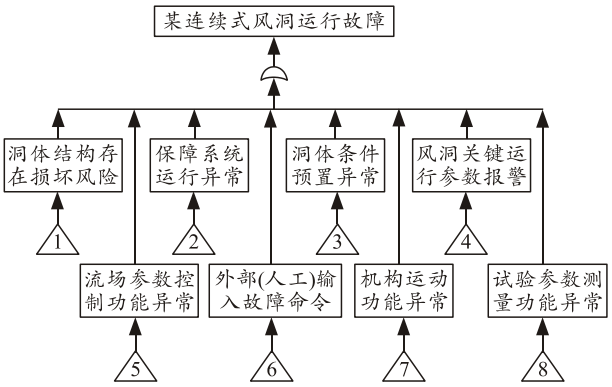

图 2　风洞故障树主树

对 8 个中间事件的发生原因进一步向下挖掘，可以形成 8 棵故障树子树，每棵故障子树将 1 个中间事件作为树顶，由上而下逐级分解直到找出最基本的故障底事件。图 3—6 给出了其中逻辑关系较为复杂的 5 棵故障子树。所构造的风洞运行故障树逻辑关系清晰全面，直观形象地呈现出故障发生的内在因果关系，共包含 248 个故障底事件，基本上包容了所有该风洞的常见故障，树中的逻辑关系以“或”的关系为主，任何底事件发生都会导致风洞运行故障。每个故障底事件直接关联到了单个工艺子系统或者工艺设备，可以很快定位到故障发生的薄弱环节，也便于后续的 FMEA 方法开展更为深入的故障模式及其影响分析。

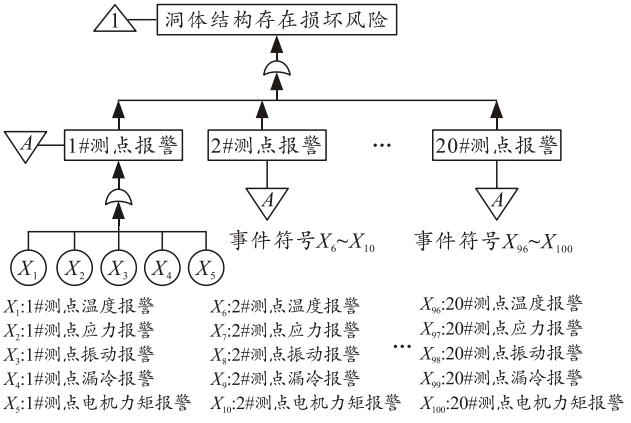

图 3　洞体结构存在损坏风险故障子树

3.3　底事件 FMEA 分析

通过 FTA 可以获得造成风洞运行故障发生的

所有重要故障底事件。然而，这些底事件仍然属于系统级或者设备级的故障，无法直接定位故障源，还需向下探寻零件级的故障模式，这也正是 FMEA 分析的意义所在。将每个故障底事件相关的子系统或者设备确定为研究对象，通过 FMEA 分析方法查找每一个研究对象潜在的故障模式和原因，识别出风险等级较高或者概率较大的故障，尽早在设计、制造阶段对其进行优化，提高风洞设计质量和运维效率。

故障底事件的FMEA分析需要对关联系统或设备十分熟悉，因此，这部分工作主要由各工艺子系统的承制方负责完成。各工艺子系统根据底事件明确故障模式分析范围，并结合该系统的任务和功能，确定故障模式的征兆、原因、影响 、检查方法、处理措施等信息，最终编制成 FMEA 分析表，所有 248 个故障底事件的 FMEA 表合并后形成整个风洞的 FMEA 表。同时，各工艺子系统通过布置传感器采集与各故障模式相关的物理量，并设计合理的阈值作为故障判据形成布尔量类型的故障判别结果，汇总本后一并传输至风洞安全联锁系统。风洞安全联锁系统实时监控有效故障信号是否被触发，并调度相关系统采取停车措施。

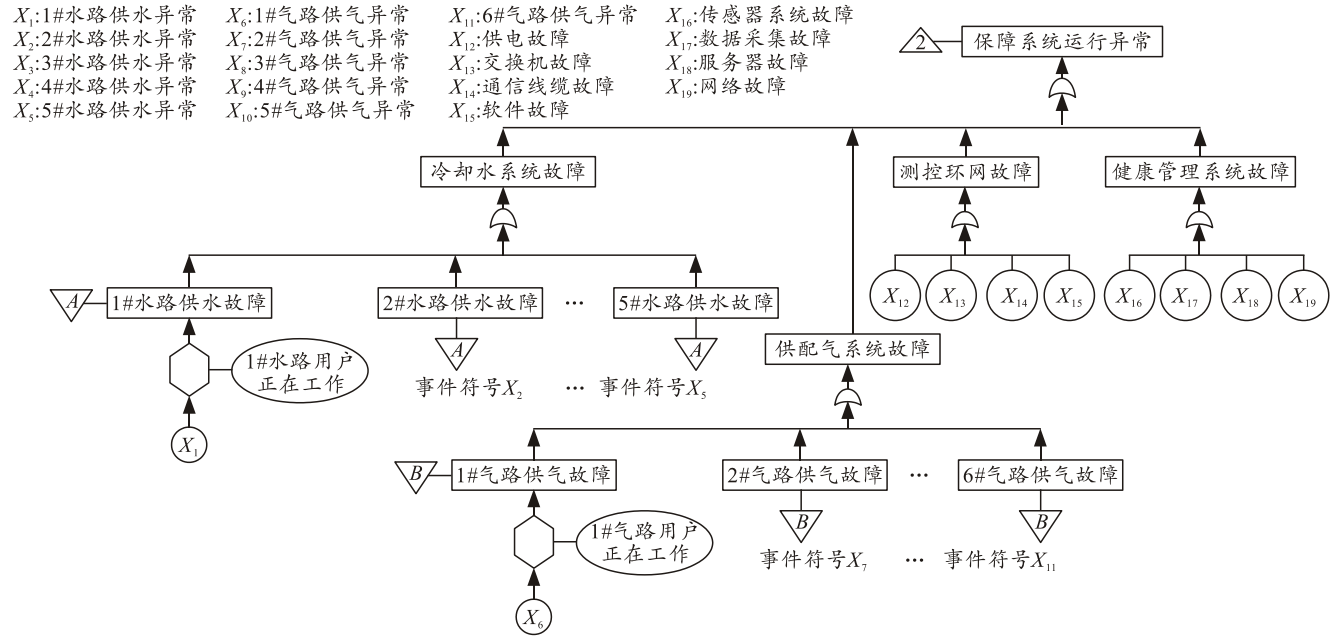

图 4　保障系统运行异常故障子树

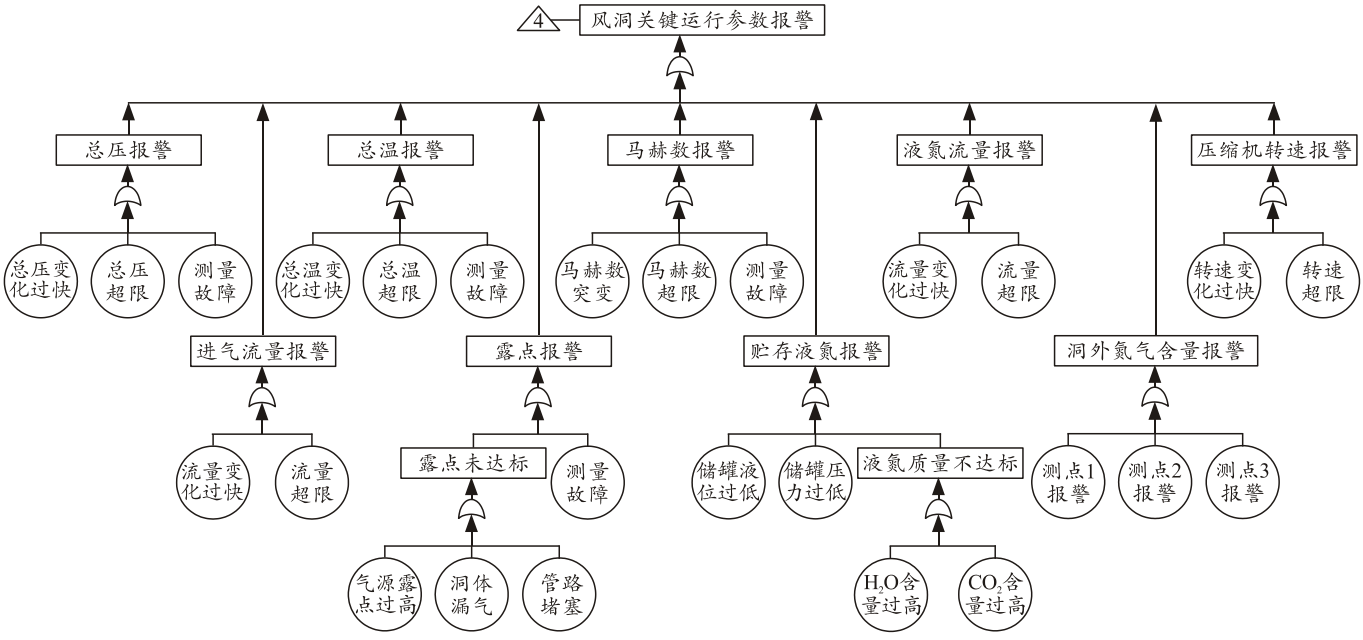

图 5　风洞关键运行参数报警故障子树

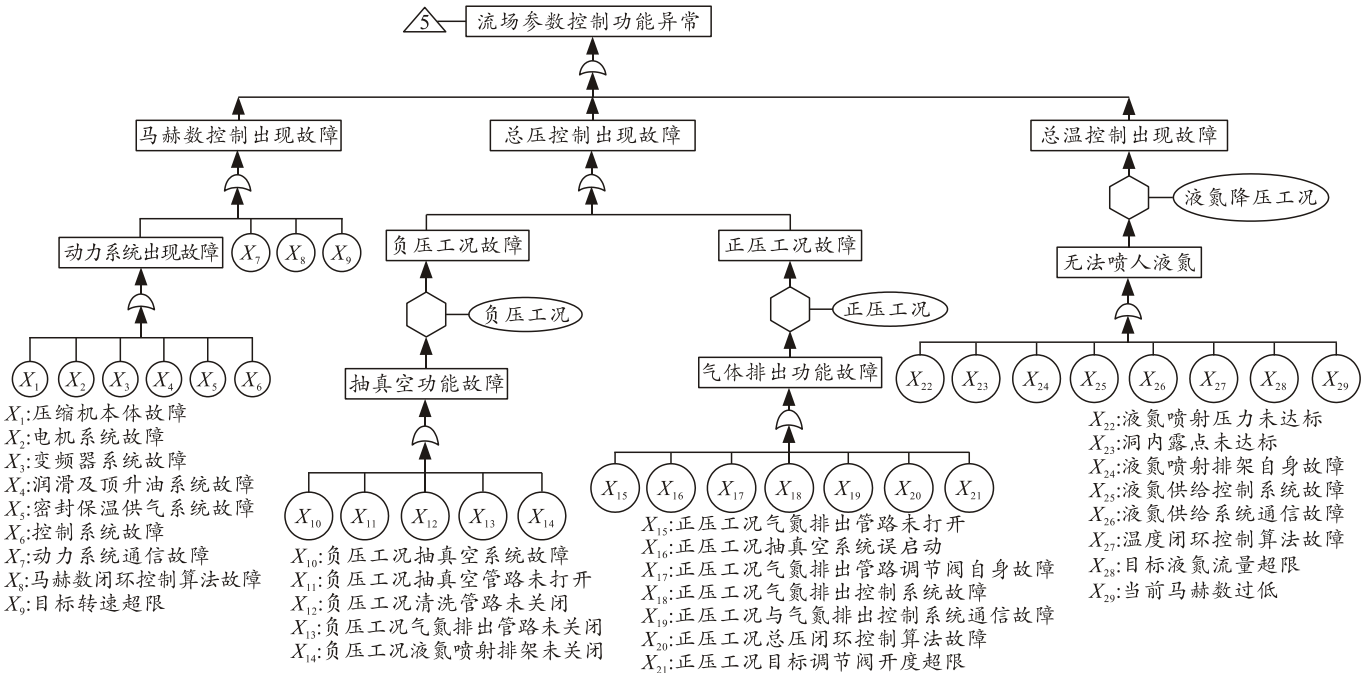

图 6　流场参数控制功能异常故障子树

以“负压工况下抽真空系统故障”底事件为例，根据 FMEA 分析小组开会探讨和国军标规定，通过分析抽真空系统的结构、组成单元以及运行机理，筛选出抽真空系统故障频率高的 12 个零部件，故障判定依据为零部件故障是否会导致抽真空系统无法正常使用。针对各零部件的每个故障模式，FMEA 分析小组根据各零部件与上层系统的关系，确定各零部件每个故障的故障模式、故障原因、故障影响、检查方法和处理措施，形成 FMEA 分析，如表 1 所示。其他故障底事件的 FMEA 分析采用相同方法，受篇幅所限分析结果不再一一列出。

表 1　“负压工况下抽真空系统故障”底事件 FMEA 分析

零部件名称	功能	故障模式	故障原因	故障影响	检查方法	处理措施
主泵	将洞内抽至所需的工作真空度	吸力不正常,抽速未达标	机械磨损或过热	洞内真空度无法达标	读取故障代码	停机排查
前级泵	维持主泵压强低于目标值	吸力不正常,抽速未达标	机械磨损或过热	主泵无法稳定运行	读取故障代码	停机排查
变频器	改变电源频率控制泵的电机转速	电路故障	过压、过流或过热	无法控制泵的抽气速率	读取故障代码	停机排查
列管式换热器	消除泵运行过程中产生的热量	换热失效	冷却水温度过高或水压不够	泵组无法正常运行	检查冷却水供水和回水温度	停机排查
排气消音器	排气过程降噪	消音效果欠佳	结构老化或破裂	排气异常	声音检测	停机排查
吸气入口阀门	控制进气管道通断	无法动作	老化或杂质卡塞	无法进气	尝试动作阀门	更换阀门
排气出口阀门	控制排气管道通断	无法动作	老化或杂质卡塞	无法排气	尝试动作阀门	更换阀门
水压传感器	测量供给换热器的冷却水水压	数据不准确	传感器损坏	无法显示正常水压	与冷却水系统数据对比	抽真空结束后排查
压力变送器	测量吸气入口管道压力	数据不准确	传感器损坏	无法显示正常气压	与其他系统数据对比	抽真空结束后排查
真空计	测量吸气入口管道真空度	数据不准确	传感器损坏	无法显示正常真空度	与其他系统数据对比	抽真空结束后排查
PLC 控制器	控制泵的抽速实现目标风洞压力	死机	软件故障	无法闭环控制洞内压力	读取故障代码	停机排查
管道	气体运输的载体	漏气	结构破损	无法进行抽真空工作	人工排查	停机排查

4　系统硬件设计

4.1　硬件架构

考虑到某连续式风洞运行流程较复杂，各工艺子系统在风洞运转过程中发挥的功能具有一定的独立性，因此采用“分散控制与集中管控”的集散型控制架构，通过任务和风险分配以及“集中控制与管理”来实现风洞运行控制[10]。每个工艺子系统均

配备有相应的测控系统，通过 Modbus、EtherCAT、Profinet 等现场总线协议接入风洞测控环网，与风洞运行控制系统、安全联锁系统等一起组成风洞测控系统。风洞测控系统可以划分为管理层、控制层和执行层 3 部分，其中运行控制系统、安全联锁系统组成管理层，完成风洞运行调度、集中监测和管控等功能；各工艺子系统的信号采集器、PLC 可编程控制器、嵌入式控制器、触摸屏等组成控制层，完成过程控制、数据采集、现场级人机交互和数据处理；各工艺子系统的现场传感器、执行机构等组成执行层，完成信号感知、能量转换和机构驱动[11]。整个系统整体拓扑架构如图 7 所示。

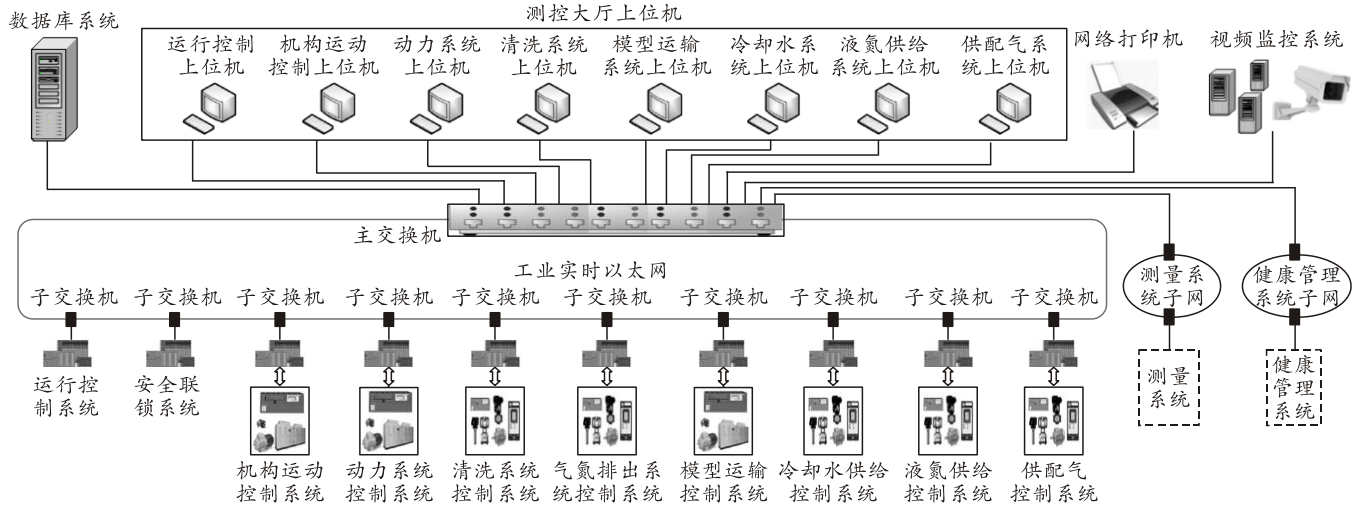

图 7　某连续式风洞测控系统拓扑架构

安全联锁系统采用分布式联锁架构，由风洞各工艺子系统与安全联锁系统相互配合实现对整个风洞的安全联锁保护功能，各工艺子系统负责实时采集和监控自身的工艺设备状态参数，安全联锁系统采集涉及风洞和人员安全的关键运行参数[12]。各工艺子系统基于设计原理和运行逻辑对设备状态进行故障判别，并通过测控环网将故障信息发送至安全联锁系统统一汇总，安全联锁系统则根据当前风洞工况对这些故障信息进行报警等级划分，并根据预定的安全联锁机制并决定是否执行安全联锁保护动作[13]。

4.2　系统组成

安全联锁系统独立于风洞运行控制系统单独开展研制，作为一套独立的 PLC 控制系统接入风洞测控环网，其硬件组成包括 PLC CPU、I/O 模块、通信接口模块、光电信号转换模块、电源模块、各类传感器，其硬件架构如图 8 所示，共配置 1 个主站和 3 个远程子站，每个站点配置 1 台控制柜。PLC CPU 安装于测控大厅主站控制柜中，实现对中央控制台操作按钮的状态采集和指示灯的信号显示；1 套远程子站通过硬接线采集风洞关键工艺子系统的就绪信号和故障信号，并在风洞出现故障时向这些工艺子系统发送安全联锁停车命令；另外 2 套远程子站布置于风洞回路不同位置处，通过所布置传感器获取风洞重要运行参数和关键设备状态参数信息。为了避免安全联锁功能受网络波动影响，安全联锁系统各子站之间单独布置网线实现内部通信，考虑到安全联锁各子站之间距离较远，3 个远程子站均通过光电介质转换模块进行通信距离扩展，最后统一接入内部交换机与主站 PLC CPU 进行组态，主站 PLC CPU 另一个网口接入风洞测控环网与风洞其他工艺子系统进行实时数据交互。

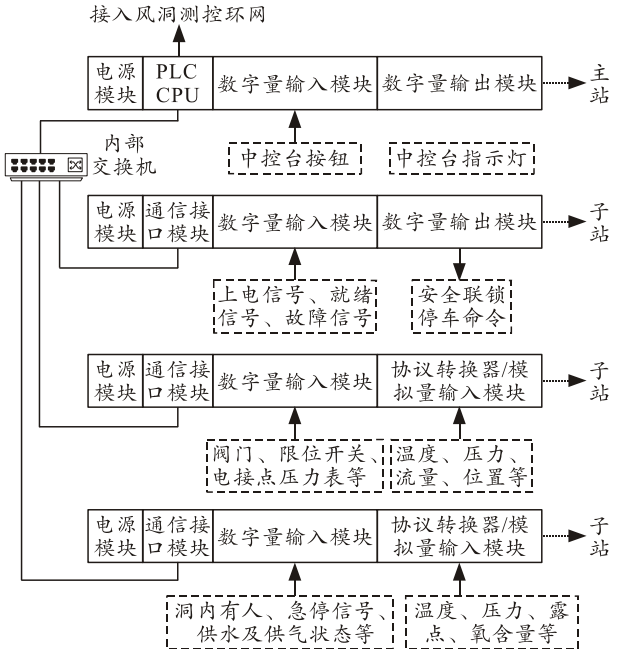

图 8　安全联锁系统硬件组成

5　安全联锁机制设计

5.1　报警策略

由于某连续式风洞系统组成复杂，报警信息多，为方便风洞运维人员及时判断并采取处理措施，根据各工艺子系统在各个流程中的参与情况，将报警信号分为：轻报警、重报警、一般故障、严重故障 4 个报警等级[14]，具体如表 2 所示。

表 2　报警等级划分对照

报警等级	名称	故障描述
4 级	轻报警	该故障影响单个设备自身功能，但不影响所在工艺子系统的整体功能
3 级	重报警	该故障影响所在工艺子系统整体功能的行使，但不影响当前工况下风洞运行流程的执行
2 级	一般故障	该故障已经影响当前工况下风洞运行流程的执行，风洞正常停车后进行检查
1 级	严重故障	该故障已严重威胁到风洞本体和试验人员的安全，需立即采取紧急停车措施

其中，轻报警是指只影响单个设备本身功能，不影响所在工艺子系统功能的故障信息，例如测控环网某个交换机冗余供电失效，但仍正常运行；重报警是指影响所在工艺子系统功能，但是不影响风洞当前工况下运行流程执行的故障信息，例如未进气时风洞清洗管路阀门故障；一般故障是指已经影响当前工况下风洞运行流程的执行，需停止风洞运行进行检查的故障信息，例如吹风试验时测量系统数据采集异常；严重故障是指已严重威胁到风洞本体和试验人员的安全，需立即采取紧急停车措施的故障信息，例如风洞超压。对于同一个故障，在不同的风洞运行工况下其报警等级也会不同。

各工艺子系统负责采集该系统内所有的故障信息，通过测控环网统一上传给安全联锁系统进行集中显示、记录和处理。对于轻报警、重报警、一般故障 3 类故障信息，各工艺子系统均通过测控环网传输至安全联锁系统即可。对于严重故障，为了避免网络故障造成安全联锁功能失效，除了通过风洞测控环网传输外，安全联锁系统还需通过布置硬接线从各工艺子系统处收集报警信号。

5.2　停车措施

安全联锁系统针对所有故障信息共设计 4 个报警等级，只有在出现一般故障和严重故障时才会触发风洞停车，且采取不同的安全联锁停车措施。当出现轻报警和重报警时，安全联锁系统只需通知风洞运行控制系统，由现场操作人员根据情况选择合适的处理方式。当出现一般故障时，安全联锁系统 PLC CPU 通过网络通信向参与风洞正常停车的子系统发送关车命令，实现风洞正常停车。当出现严重故障时，除了网络通信外，安全联锁系统还通过 I/O 模块和信号线向参与风洞紧急停车的子系统发送关车命令，实现风洞紧急停车。若安全联锁系统无法正常发送关车命令时，则由操作人员拍下中央控制台上设置的按钮，同样通过信号线发送关车命令实现风洞紧急停车[15]，中央控制台上共设置有紧急停车、正常停车、模型急停 3 个按钮。

风洞安全联锁停车涉及到动力系统、液氮供给系统、气氮排出系统、清洗系统、模型支撑系统、供配气系统、机构运动控制系统等多个工艺子系统，这些子系统接收来自安全联锁系统 PLC CPU、中央控制台的 2 种关车命令源，并按照预定的逻辑执行停车措施。对于大部分子系统来说，正常停车和紧急停车采取的措施是相同的，只有动力系统、液氮供给系统、气氮排出系统、模型支撑系统需要采取不同的停车措施，具体如表 3 所示。

表 3　各系统停车措施明细

系统名称	停车类型	停车措施
动力系统	正常停车	90 s 减速停车
	紧急停车	15 s 制动停车
液氮供给系统	正常停车	按照预设阶梯将喷入洞内的液氮流量从当前值降为零
	紧急停车	按照最快速度将喷入洞内的液氮流量从当前值降为零
气氮排出系统	正常停车	闭环控制管路阀门开度维持洞内压力在当前值
	紧急停车	打开所有管路阀门将洞内压力泄至常压
模型支撑系统	正常停车	按照预设运动速率逐步将模型角度回零
	紧急停车	模型运动急停，电机抱闸维持模型当前角度不变
供配气系统	正常停车/紧急停车	关闭向清洗系统供气的管路阀门
清洗系统	正常停车/紧急停车	关闭向洞内进气的管路阀门
机构运动控制系统	正常停车/紧急停车	喷管型面不变，二喉道角度回零

5.3　告警设计

风洞运行出现故障时，安全联锁系统除了统一调度实现风洞停车外，还必须通过显示设备和声音设备向操作人员进行警示，由操作人员根据风洞运行工况和运行风险确定下一步执行操作。因此，安全联锁系统专门配备一套声光告警系统，包括布置在测控大厅、风洞现场和厂房的告警电铃，测控大厅中央控制台上的指示灯以及吹风试验电铃。除此之外，还可通过测控大厅试验大屏的风洞运行控制系统上位机界面进行告警。当出现轻报警和重报警

时，安全联锁系统给出指令，试验大屏的上位机界面和中央控制台上的对应的报警指示灯闪烁。当出现一般故障和严重故障时，除了报警指示灯闪烁外，告警电铃还给出相应的声音提示，同时上位机界面给出该故障的FMEA分析文本描述，包括故障模式、故障原因、故障影响、检查方法、处理措施等。吹风试验电铃则用于试验前吹风警示，3 遍打铃后即将进入吹风试验状态。

6 安全联锁功能测试

风洞安全联锁系统功能测试分 2 个阶段：1) 系统单调阶段。主要测试风洞各工艺子系统的内部安全联锁功能是否实现。针对安全联锁系统的参数采集、状态监测、数据通信、信息显示等单系统功能进行测试，确保其基本功能满足要求；其他工艺子系统则根据在 FTA-FMEA 联合分析中梳理的FMEA 表，通过硬件设置或软件模拟的方式触发故障信号，测试其控制系统是否将对应的故障变量置位，也就是检验各工艺子系统是否能够有效监测本系统风洞运行故障树底事件的发生。2) 风洞联调阶段。默认各工艺子系统内部安全联锁功能正常，主要从故障判别、停车措施执行 2 方面对安全联锁系统开展功能性测试。在不同的风洞运行工况下，各工艺子系统通过变量置位模拟该系统故障底事件的发生，测试安全联锁系统 PLC CPU 是否接收到该故障信号，并考察在出现一般故障和严重故障时，安全联锁系统 PLC CPU 是否下发停车命令，以及参与停车的子系统接收到停车命令后或检测到通信故障时是否采取正确的停车措施。

所有 248 个故障底事件的安全联锁功能测试结果表明：风洞安全联锁系统功能完备，故障判定和联锁逻辑正确，能够对风洞运行状态进行有效监控，在影响风洞运行安全的故障出现时均能准确告警并采取正确的风洞停车措施，并通过故障信息的文本描述辅助风洞运维人员对故障进行研判，方便其快速识别故障风险性和处置方法，高效保障风洞试验和人员设备安全。

7 结束语

某连续式风洞作为复杂科学设备，内部故障模式众多，故障传递关系复杂。通过开展 FTA-FMEA 联合故障分析，能够对风洞进行全面深入的故障分析，快速对影响风洞安全的潜在风险进行评估分析，找出设备运行中的薄弱环节。在此基础上，依托分布式 PLC 硬件系统开展风洞安全联锁系统研制，实现对风洞运行全方位的状态监测，同时对报警策略、停车措施、告警方法等开展精细设计。测试结果表明：某连续式风洞安全联锁系统故障监测功能完备，在出现故障时能够快速采取正确的安全联锁措施，确保了风洞试验的安全、可靠运行。同时，还能够辅助风洞运维人员对故障进行研判，方便其快速排查和精准溯源，为人为介入处理故障提供决策辅助。

参考文献：

[1] 赖欢, 陈万华, 孙德文, 等. 0.3 m 低温连续式跨声速风洞结构设计[J]. 实验流体力学, 2020, 34(5): 89-96.

[2] 艾天伦, 唐明新, 陈晓侠. 紧急停车系统在化工生产中的应用[J]. 工业控制计算机, 2012, (1): 53-54.

[3] 黄知龙, 周平, 顾正华. 大型低温风洞中的测控技术设计需求[C]//中国空气动力学会测控专业委员会六次全国学术交流会. 中国空气动力学会测控专业委员会, 2015.

[4] 廖达雄, 黄知龙, 陈振华, 等. 大型低温高雷诺数风洞及其关键技术综述[J]. 实验流体力, 2014, 28(2): 7.

[5] 贺中华, 李强, 王丽萍. 基于 PLC 的 1.2 米风洞安全联锁系统[C]//2015 航空试验测试技术学术交流会. 航空工业测控技术发展中心, 2015.

[6] LEE W S, GROSH D L, TILLMAN F A, et al. Fault tree analysis, methods,and applications-a review[J]. IEEE Transactions on Reliability, 1985, 34(3): 194-203.

[7] 聂森. FMEA 技术研究与软件系统发展[D]. 合肥: 合肥工业大学, 2007: 14-16.

[8] YU S R, YANG Q Y, LIU J W, et al. A comparison of FMEA, AFMEA and FTA[C]//2011 qth International Conference on Reliabyitg, Maintainability and Safety. Guiyang, China: IEEE, 2011: 954-960.

[9] 张建国, 黄文敏. 大型机械产品 FMEA 和 FTA 综合分析方法[J]. 机械设计与制造, 2000(1): 3.

[10] 阎成, 邓晓曼, 高峰, 等. 基于分布式测控技术的风洞运行状态监测系统[J]. 兵工自动化, 2013, 32(2): 67-70.

[11] 黄昊宇, 凌忠伟, 刘为杰, 等. 基于现场总线和实时网络的某射流风洞安全连锁与状态监控系统研制及应用[J]. 计算机测量与控制, 2024, 32(8): 215-221.

[12] 荣祥森, 邓章林, 贾霜, 等. 基于 PROFINET 和 VXI 总线的 1.2 m 风洞测控系统设计与实现[J]. 计算机测量与控制, 2019, 27(5): 8795.

[13] 谢明伟, 宋巍巍, 王飞, 等. 基于实时以太网的某连续式风洞安全联锁系统[J]. 兵工自动, 2016, 35(9): 4.

[14] 马列波, 高鹏, 陈海峰, 等. 某亚跨超声速风洞安全联锁控制系统研制[J]. 测控技术, 2021, 9: 96-101.

[15] 马列波, 高鹏, 陈海峰, 等. 基于组态方式的风洞运行安全关车控制方法[J]. 计算机测量与控制, 2021, 29(6): 114-118.