姚航. 基于 DRIVE Thor 辅助驾驶平台功能安全的设计与应用[J]. 智能计算机与应用,2026,16(4):167-172. DOI:10.20169/j.issn.2095-2163.25110801

# 基于 DRIVE Thor 辅助驾驶平台功能安全的设计与应用

姚 航
(英伟达半导体科技(上海)有限公司, 上海 200232)

**摘 要**: 随着汽车智能化技术迅猛发展,L3 级以上辅助驾驶系统的功能安全要求日益严格,成为制约技术产业化的关键瓶颈。本文以英伟达 DRIVE Thor 辅助驾驶平台为研究对象,系统分析了集中式高算力平台的功能安全设计理论与实现机制。研究深入探讨了 DRIVE Thor 平台的核心安全架构:硬件层面采用模块化冗余电源管理、功能安全岛(FSI)独立监控、瑞萨 U2A16 专用安全 MCU 等关键技术,能够实时检测系统硬件故障;软件层面基于 AUTOSAR Classic Platform 和 QNX Safety OS 构建多层次安全防护体系,通过 Safe MCU 系统监控和 Thor SoC 混合关键性计算实现安全与非安全功能的有效隔离;系统层面建立了涵盖硬件监控、软件保护、协调响应的立体化故障处理机制,能够实时监控系统的运行状态,极大地提高了系统的安全性和可靠性。本研究为高算力辅助驾驶平台的功能安全设计提供了完整的方法论和技术方案,对推动辅助驾驶技术安全落地具有重要指导价值。

**关键词**: 功能安全; DRIVE Thor; 辅助驾驶系统; ISO 26262; 集中式架构
**中图分类号**: TP399 **文献标志码**: A **文章编号**: 2095-2163(2026)04-0167-06

# Functional safety design and application of DRIVE Thor advanced driver assistance platform

YAO Hang
(NVIDIA Semiconductor Technology (Shanghai) Co., Ltd., Shanghai 200232, China)

**Abstract**: With the rapid advancement of automotive intelligent technologies, functional safety requirements for L3+ Advanced Driver Assistance Systems (ADAS) have become increasingly stringent, constituting a critical bottleneck that constrains technology industrialization. This paper takes NVIDIA DRIVE Thor ADAS platform as the research subject and systematically analyzes the functional safety design theory and implementation mechanisms of centralized high-performance computing platforms. The research comprehensively investigates the core safety architecture of the DRIVE Thor platform: at the hardware level, key technologies including modular redundant power management, Functional Safety Island (FSI) independent monitoring, and dedicated Renesas U2A16 safety MCU are employed, enabling real-time detection of system hardware faults; At the software level, a multi-layered safety protection system is constructed based on AUTOSAR Classic Platform and QNX Safety OS, achieving effective isolation between safety-critical and non-safety-critical functions through Safe MCU system monitoring and Thor SoC mixed-criticality computing; at the system level, a multi-dimensional fault handling mechanism encompassing hardware monitoring, software protection, and coordinated response is established, enabling real-time monitoring of system operational status and significantly enhancing system safety and reliability. This research provides a complete methodology and technical solution for functional safety design of high-performance ADAS platforms, offering significant guidance value for promoting the safe deployment of advanced driver assistance technologies.

**Key words**: functional safety; DRIVE Thor; Driver Assistance Systems; ISO 26262; centralized architecture

## 0 引 言

近年来,随着国家一系列政策的支持和推动,新能源汽车获得了大力的发展和推进。中国新能源汽车核心技术日趋成熟,在电池技术、驱动系统和能源管理等领域已达到国际领先水平。随着汽车电动化进程的逐步完善,智能化已成为汽车产业发展的下一个重要赛道。现代汽车正在从传统的机械交通工

作者简介: 姚 航(1990—),男,硕士,工程师,主要研究方向:汽车电子嵌入式软件开发,自动驾驶基础软件开发。Email:Samuel189@126.com。

收稿日期: 2025-11-08

具向智能移动终端转变,集成了越来越多的先进传感器、高性能计算平台和人工智能算法。

据统计,全球主要汽车制造商和科技企业在自动驾驶领域的累计投资已超过千亿美元规模,系统复杂度呈指数级增长,传统分布式 ECU 架构建在 L3 级以上自动驾驶技术逐步进入商业化阶段后在在算力、实时性、成本等方面面临严峻挑战[1-3]。更为关键的是,自动驾驶系统直接关系到驾驶员、乘客和道路使用者的生命安全,功能安全成为技术落地的关键瓶颈[4-5]。

英伟达 DRIVE Thor 作为新一代集中式车载计算平台,代表了当前自动驾驶硬件技术的前沿水平。该平台不仅提供强大的 AI 计算能力,更在架构设计中充分考虑了功能安全要求。然而,目前关于集中式高算力平台功能安全设计的系统性研究相对缺乏,特别是硬件冗余机制、软件安全架构和故障处理策略的深入分析。本文以 DRIVE Thor 平台为研究对象,系统分析其功能安全设计与实现机制,包括:(1)深入分析集中式平台的硬件安全架构设计原理和实现方法;(2)系统阐述基于 AUTOSAR 和 QNX 的软件安全体系;(3)建立多层次故障检测与处理的理论框架。研究成果为辅助驾驶系统的安全设计提供重要的理论指导和实践经验。

## 1 辅助驾驶平台与功能安全

### 1.1 辅助驾驶平台

汽车电子电气架构(Automotive Electrical/Electronic Architecture)是电子元器件连接和协同运行的基础,可为实现汽车复杂功能和多样化需求提供重要支撑[6-7](如图 1 所示)。

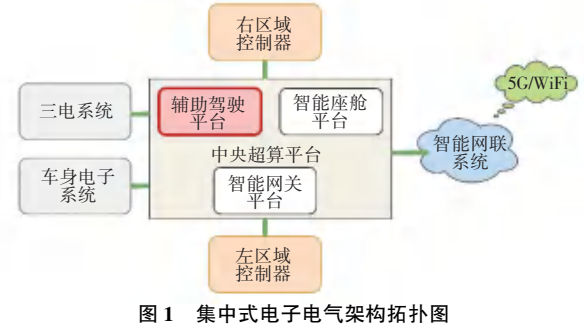


图 1 集中式电子电气架构拓扑图

Fig. 1 Topology diagram centralized electronic and electrical architecture

图 1 为一个典型的集中式电子电气架构,主要由中央超算平台、左、右域控制器、三电系统,车身电子系统、智能网联系统等组成。而中央超算平台中则包含了智能驾驶、智能座舱和智能网关三大“智能”控制器,负责整车所有的数据,信号的收集、处理和运算,以及下发相应的控制指令。

辅助驾驶平台是智能汽车的重要组成部分,是实现汽车智能化必不可少的核心载体。辅助驾驶平台包含了一颗或多颗高算力高性能的 SOC 芯片,多个高精度、高灵敏度的传感器(如高精摄像头、毫米波雷达、超声波雷达等),以及多个车规级的 MCU 控制芯片等核心硬件。如图 2 所示,典型的辅助驾驶平台的系统框图由多个不同的摄像头(前视、后视、环视、红外等),不同的雷达(超声波雷达、毫米波雷达、激光雷达等)及 GNNS 卫星导航系统组成的感知层。决策层是高性能高算力的 SOC 芯片融合各个传感器的输入来完成相应的决策。同时,整个系统还配备了电源模块、功能安全 MCU、以太网交换机、显示模块、通信模块等必要的外设组成[8]。

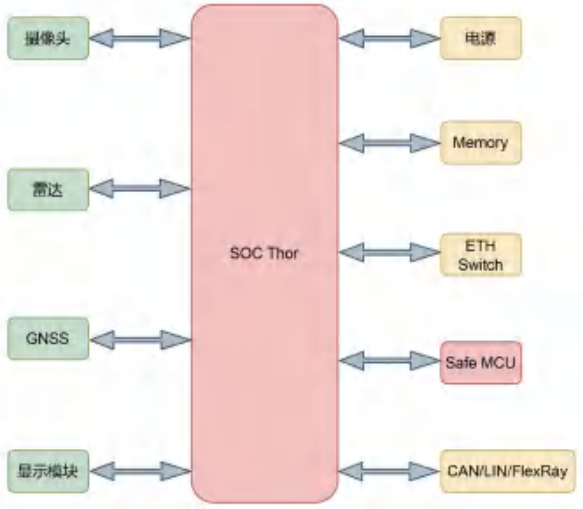


图 2 辅助驾驶系统的系统框图

Fig. 2 Block diagram of the advanced driver assistance system

### 1.2 功能安全

随着新一代汽车电子电器架构的演进,汽车电子软硬件的复杂度呈指数级增长,来自系统失效和随机硬件失效的风险也剧增。与安全相关的软件、硬件出现了任何一个失效,都可能给驾乘人员,车辆和周围环境带来非常严重的后果。基于此,国际标准化组织于 2011 年 11 月正式发布了 ISO26262《道路车辆功能安全》标准,首次针对乘用车电子电器系统提出了全生命周期安全管理要求,该标准通过危害分析和风险评估方法确定汽车安全完整性等级(ASIL),并建立如图 3 所示的功能安全 V 模型开发流程[9]。2018 年 12 月份修订并发布了第二版,新增了第 11 部分“半导体应用指南”和第 12 部分“适用于摩托车的标准”,从而形成涵盖 12 个技术章节的完整标准体系。ISO26262 标准分别从功能安全管理、概念、系统级研

发、软硬件的研发、生产和操作等方面对产品的整个生命周期进行了规范和要求，从而确保系统的每个细节都经过严密的安全评估和验证。这种完整系统级的分析、开发、生产的方法能够提升汽车电子电器系统在面对复杂环境和突发状况时的容错能力，最大程度上减少因系统失效带来的安全隐患[10]。

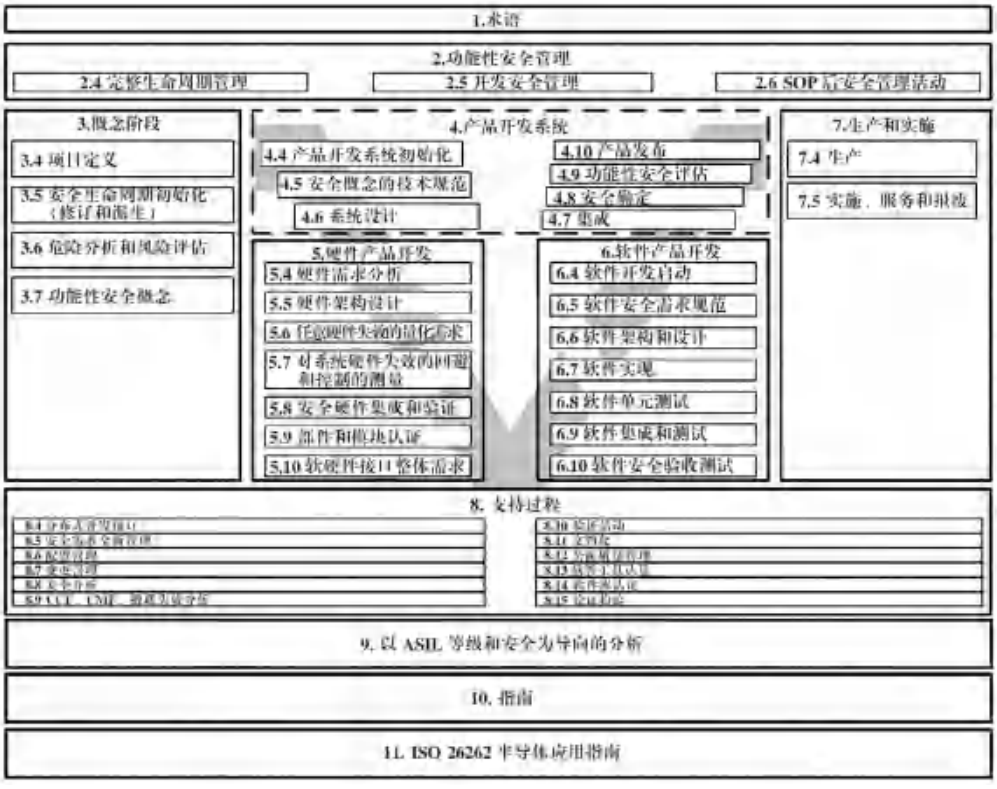


**图 3　ISO26262V 模型开发流程图**

**Fig. 3　ISO 26262 V-model development process diagram**

英伟达（NVIDIA）新一代系统级芯片 DRIVE Thor 能够将各个智能汽车功能整合到同一 AI 计算平台，这款车规级系统级芯片基于最新的 CPU 和 GPU 打造，可提供每秒 2 000 万亿次浮点运算性能，在大幅度提升性能的同时，还能降低整体系统的运行成本。配合已获得 ASIL-D 等级功能安全产品认证的 NVIDIA DRIVE 软件开发套件，可以加快应用程序开发，快速的完成辅助驾驶中各个功能的开发部署和实现[11-13]。

## 2　DRIVE Thor 辅助驾驶平台的硬件功能安全设计

### 2.1　DRIVE Thor 电源模块

为了实现功能安全 ASIL D 的目标，DRIVE Thor 辅助驾驶平台采用了模块化的电源管理架构，如图 4 所示。该架构基于“冗余设计+实时监控+故障隔离”的安全理念，确保单一组件故障不会影响系统整体安全。该平台采用多输入源设计，核心电源管理由一颗电源时序芯片来严格控制各路电源的上电时序，最大支持 12 路电源时序的控制。Thor 芯片中的 CPU，GPU 等核心电源通过专用的双轨多相电源芯片可精确，高效地动态调节输出电压。同时，为了能够实时，准确的监控各路电压的输出情况，采用了多颗电源监控芯片，监控电源的过压、欠压、序列错误故障，确保电源系统的稳定、可靠运行。电源管理芯片通过独立的 $I^2C$ 总线和 MCU、SOC 进行参数配置和状态监控。每一颗电源专用芯片都支持芯片自检、CRC 校验，最高可满足功能安全 ASIL-D 等级要求。

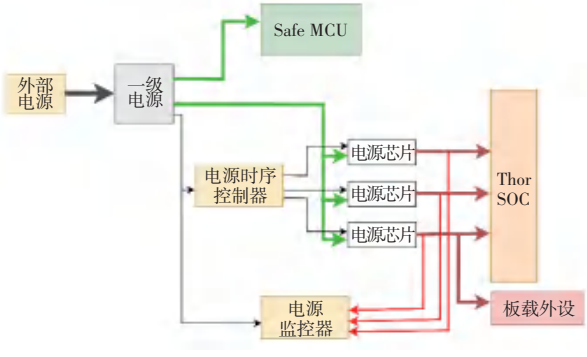


**图 4　DRIVE Thor 辅助驾驶平台电源框图**

**Fig. 4　Power block diagram of DRIVE Thor assisted driving platform**

### 2.2 DRIVE Thor 主控芯片

DRIVE Thor 是英伟达公司推出的最新一代集中式车载计算平台,旨在将数字仪表盘、信息娱乐、自动驾驶、泊车、驾乘人员监控等多种功能整合到单一的低能耗计算系统中,如图 5 所示。该平台采用英伟达最新的异构计算架构,集成了高性能 CPU 集群、GPU 计算单元、专用 AI 加速器和功能安全岛等多个功能模块,提供了强大的计算能力和灵活的架构配置,最高支持 2 000 TOPS 的 AI 性能和 2 000 TFLOPS 的浮点算力,能够支持复杂的深度学习算法和多传感器数据融合处理。这种强大的计算能力为实现 L4 级自动驾驶提供了硬件基础。

图 5 辅助驾驶平台硬件实物图

**Fig. 5 Hardware diagram of assisted driving platform**

为了实现更高级别的功能安全目标,DRIVE Thor 内集成了功能安全岛 FSI(Functional Safety Island),FSI 里有独立的电源、4 颗 ARM R52 双锁步核、独立的内存空间、IO 接口,确保资源的隔离,提高系统的可靠性。主 CPU 集群采用 ARM Cortex-A78 架构,支持非对称多处理(AMP)和对称多处理(SMP)模式。在功能安全应用中,可配置为主-从核架构,其中主核运行关键安全功能,从核处理非安全关键任务。

### 2.3 功能安全 MCU

在 DRIVE Thor 辅助驾驶平台里还设计采用了一个车规级的功能安全 MCU 芯片,瑞萨 U2A16 芯片,该芯片搭载了瑞萨针对车载应用领域设计的 RH850 G4MH 内核,集成 4 颗独立的双锁步核,最高支持 400 MHz 主频的运算能力,同时提供了高可靠性的片内 flash 和 RAM 存储空间[14]。功能安全 MCU 负责控制 Thor SOC 的上电下电,进出低功耗模式,并且实时监控 SOC 的运行状态,针对不同的异常情况,实时快速的进行响应。

### 2.4 其他外设

为了使整个系统达到一个更高的功能安全等级的目标,除了 SOC 主控芯片、MCU 芯片之外,还设计采用了车规级的电子器件、512 GB 的 UFS 外部存储器、64 M 的 Secure Nor Flash,64 GB 的 DDR 来满足系统的存储需求。在网络通信方面采用了 Marvell 88Q5152 车规级高速以太网交换机,和 TJA1145 CAN 收发器,支持和车内其他控制器之间的网络通信。

## 3 DRIVE Thor 辅助驾驶平台的软件功能安全设计

在 DRIVE Thor 辅助驾驶平台中 Safe MCU 主要负责实时监控 Thor SOC 的运行状态,并根据不同类型不同严重等级的错误,执行对应的处理和动作;同时负责和车内其他的 ECU 控制器进行交互,接收整车下发的指令数据来协调整个辅助驾驶系统的工作。Thor SOC 主要负责辅助驾驶平台的核心功能,包括(1)感知模块对多源异构传感器集群采集的海量数据进行系统化处理和深度语义解析;(2)决策模块将多维度输入信息转化为可执行的控制指令,构建从环境认知到行为执行的智能决策闭环;(3)执行模块将对应的控制指令转化为车辆底层执行机构的具体动作(如加速、转向、制动),实现对车辆运动状态的精准控制。图 6 为 DRIVE Thor 辅助驾驶系统的软件框架图,从用户视角来看, Thor SOC 主要由主 CPU 集群和 FSI 两部分组成,主 CPU 集群运行的是 Linux 或者 QNX 操作系统,在系统之上部署构建功能安全相关的 safety service,以此提升软件系统的功能安全等级。FSI 和 Safe MCU 类似,运行的是基于 AUTOSAR Classic Platform(以下简称 AUTOSAR CP)标准来开发的商业 AUTOSAR 协议栈,集成了满足功能安全 ASIL D 等级的 RTE、BSW、MCAL 等模块,配合对应的 AUTOSAR 配置生成工具,从而确保整个软件系统能够达到功能安全 ASIL D 等级的要求[15]。

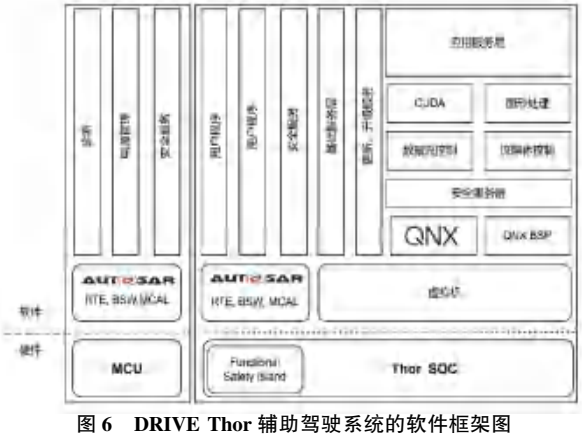


图 6 DRIVE Thor 辅助驾驶系统的软件框架图

**Fig. 6 Software framework diagram of DRIVE Thor assisted driving system**

### 3.1　Safe MCU 的功能安全的设计

在 Safe MCU 中运行的是 AUTOSAR CP 软件协议栈，在 AUTOSAR CP 软件安全机制中，主要提供了 Safe BSW、Safe RTE 和 Safe tools 三大类的安全保障。Safe BSW 里主要包含了 Safe OS 实时操作系统、Safe WDG 看门狗监控、Safe E2E（端到端）通信等内容。Safe RTE 一般配合 Safe tools 来使用，通过对应用业务进行拆解，建模和接口定义，来设计不同 SWC 之间的交互接口和逻辑。通过 Safe tools 工具来生成 Safe RTE 接口。

Safe OS 基于 MCU 芯片的 MPU 内存保护机制来对整个软件系统进行内存保护，隔离不同功能安全等级软件模块之间的内存访问，以及跨核之间的内存访问，确保功能安全低等级的软件模块无法访问功能安全高等级的软件模块的内存空间。Safe WDG 对整个系统的软件执行时间、系统心跳和程序流进行监控，确保系统里各个任务，软件模块都是按照预期的方式在正确的执行中。Safe E2E 通过增加了 CRC 校验、序列号和计数器的手段，确保数据能够准确无误的发送出去，并且成功的被接收方所接收，详细通信过程如图 7 所示。Safe RTE 和 Safe tools 通过认证过的软件配置工具来对软件组件的接口进行设计和配置，完成 RTE 接口的代码生成，通过统一的工具能够最大程度确保 RTE 接口的准确性和安全性。

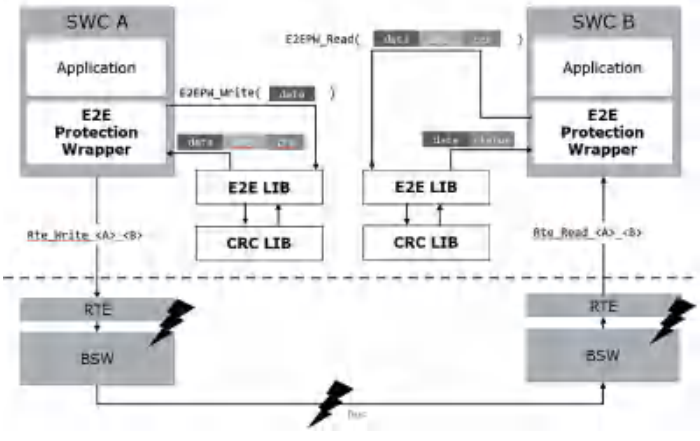


**图 7　AUTOSAR CP E2E 通信示意图**

**Fig. 7　AUTOSAR CP E2E communication diagram**

对于整个辅助驾驶平台来讲，Safe MCU 承担了整个系统的控制和故障失效监控，包含了电源芯片、板载外设芯片的自检管理，Thor SOC 芯片的自检管理，系统的电源管理、电压监控、温度监控、Thor SOC 芯片的安全运行状态监控以及故障失效处理等。

### 3.2　Thor SOC 的软件功能安全设计

在 Thor SOC 中对用户可见的是 FSI 和主 CPU 集群，在 Thor SOC 芯片内 FSI 是有独立的电源、内存空间、时钟源、I/O 资源以及 4 个双锁步核组成，最高可支持 ASIL D 的功能安全等级。在 FSI 中运行的是 AUTOSAR CP，主要用于实时监控 Thor SOC 芯片内部的运行状态，收集上报软硬件故障信息，以及系统故障信息。

在主 CPU 集群中运行的是 QNX 操作系统（QNX OS for Safety，功能安全等级为 ASIL D），该操作系统基于微内核架构，提供了内存保护机制、确定性实时调度特性、故障检测与处理机制，最大程度减少操作系统层面上的失效风险。

为了最大程度的减少辅助驾驶系统的软硬件的失效风险，提升系统的功能安全等级，定义了一系列软硬件故障信息，用于实时监控整个系统的运行状态，如图 8 所示。在硬件方面，如果 Thor SOC 芯片内部硬件出现了故障（系统时钟频率故障、看门狗故障、存储器故障等），将通过特定的硬件中断的方式通知给 FSI，由 FSI 来收集进一步的故障信息，并进行相应的处理，上报给 Safe MCU。对于板载外设（如存储、通信模块等）及 Safe MCU 本身的故障，则由 MCU 来实时进行监控和处理。

软件方面，在 QNX 操作系统之上，各个应用软件模块完全独立的监控自身的运行状态，并通过统一软件接口来进行故障上报（软件超时通信故障内存溢出等），然后通过 Thor SOC 芯片内部的通信机制将故障信息上报给 FSI，FSI 获取进一步的故障信息，进行后续的处理，并上报给 Safe MCU。

不同类型不同影响范围的故障分别设定了不同的安全等级，对于某些严重的故障信息（如某个功

能模块失效或硬件单元失效)不仅会上报故障信息给 FSI,同时还会同步拉低 Thor SOC 故障状态引脚(SOC Error pin)。Safe MCU 不仅会接收处理 FSI 发送过来的故障信息,会实时监控 Thor SOC 的故障状态引脚的电平状态。一旦检测到电平状态发生了变化,便会快速响应启动故障处理机制(如重启 SOC,进入救援模式等),最大程度的减少故障带来的负面影响,降低对驾乘人员和车辆的安全威胁。

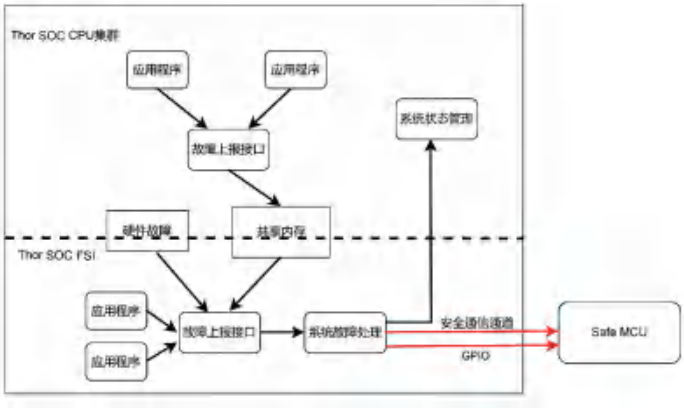


**图 8 DRIVE Thor 故障检测,上报示意图**

**Fig. 8 DRIVE Thor fault detection and report schematic diagram**

## 4 结束语

英伟达 DRIVE Thor 作为 DRIVE Orin 的技术演进,在继承前代平台优势的基础上实现了显著的性能提升,在辅助驾驶、智能座舱、智能网联等关键领域展现出强大的技术竞争力。该平台正加速推动辅助驾驶技术的产业化进程,在 2025 年上海车展上,已有多家本土汽车企业将 DRIVE Thor 集成到其智能驾驶技术方案中,标志着该平台在中国市场的快速落地。本文以 DRIVE Thor 辅助驾驶平台为研究对象,系统分析了其功能安全设计与实现机制。通过深入研究硬件冗余架构、软件安全体系、故障检测处理机制以及系统安全保障策略,构建了完整的辅助驾驶平台功能安全解决方案。研究成果验证了该平台满足 ISO 26262 ASIL-D 级功能安全要求的技术可行性,为上层应用功能的可靠实现提供了坚实的安全基础,有效降低了系统整体功能失效风险。

## 参考文献

[1] 凌艳城. 面向 L2 级高级辅助驾驶系统的视觉信息智能分析关键技术与应用研究[D]. 广州:华南理工大学,2024.

[2] 彭衍飞. 自动驾驶预期功能安全决策研究[D]. 大连:大连理工大学,2024.

[3] 张恒,何胜学. 基于联网自动驾驶车辆的环形交叉口双层优化轨迹模型研究[J/OL]. 智能计算机与应用(2025-12-01)[2026-01-06]. DOI:10.20169/j.issn.2095-2163.25052605.

[4] 罗通强,刘坚坚,赵炳根,等. 智能汽车系统功能安全保障机制的现状与展望[J]. 汽车工程学报,2024,14(6):921-933.

[5] 《中国公路学报》编辑部. 中国汽车工程学术研究综述·2023[J]. 中国公路学报,2023,36(11): 1-192. DOI:10.19721/j.cnki.1001-7372.2023.11.001.

[6] 李克强,戴一凡,李升波,等. 智能网联汽车(ICV)技术的发展现状及趋势[J]. 汽车安全与节能学报, 2017,8(1):1-14.

[7] BANDUR V, SELIM G, PANTELIC V, et al. Making the case for centralized automotive E/E architectures [J]. IEEE Transactions on Vehicular Technology, 2021,70(2):1230-1245.

[8] 李升波,江昆,田野,等. 汽车智能驾驶技术发展与趋势展望[J]. 前瞻科技,2025,4(2):144-157.

[9] 许汇鑫. 考虑功能安全的线控转向系统故障诊断与容错控制策略研究[D]. 长春:吉林大学,2025.

[10] 李元晟,周俊杉,唐雨蒙,等. 汽车芯片功能安全评估解析[J]. 电子产品可靠性与环境试验,2024,42(5):120-126.

[11] KANI A. NVIDIA DRIVE Thor 突破 AI 性能极限,可在单个计算平台实现全车的智能驾驶和智能座舱功能[EB/OL]. (2022-09-20). https://blogs.nvidia.cn/blog/drive-thor/.

[12] 高闯,王潇逸,李彬,等. 基于 Xavier 嵌入式平台的高效航空遥感目标检测方法[J/OL]. 智能计算机与应用(2025-07-14)[2025-07-14]. DOI:10.20169/j.issn.2095-2163.25061001.

[13] 王苑丞,文靖豪,张祺睿,等. 基于 Jetson Nano 的智能双足人形机器人[J]. 智能计算机与应用, 2024, 14(4):177-179.

[14] 瑞萨电子株式会社. RH850/U2A 区域/域微控制器系列[EB/OL]. (2019-02-25)[2025-11-08]. https://www.renesas.cn/zh/products/rh850-u2a.

[15] 邹渊,马文斌,张旭栋,等. 基于 AUTOSAR 的汽车控制器软件优化部署研究[J]. 北京理工大学学报, 2024,44(11):1192-1198.