面向服务架构的汽车功能安全开发研究*

杨雪珠　李军　陈虹旭　李海霞

（中国第一汽车股份有限公司研发总院，长春 130013）

【摘要】为实现面向服务架构（SOA）的整车功能安全开发，在分析SOA特点的基础上，结合ISO 26262标准，建立基于SOA的汽车功能安全正向开发流程，提出了基于功能的概念开发阶段和基于架构的系统开发阶段的功能安全设计方法：在概念开发阶段，面向产品能力导出功能安全需求，定义产品能力的功能安全等级；在系统开发阶段，基于软件组件架构、物理部署等实现技术安全需求的进一步导出与分配。

关键词：功能安全　面向服务架构　电子电气架构　正向开发流程

中图分类号：U461.91　　**文献标志码：**A　　**DOI：** 10.20104/j.cnki.1674-6546.20240276

Research of Automotive Functional Safety Development for Service Oriented Architecture

Yang Xuezhu, Li Jun, Chen Hongxu, Li Haixia

(Global R&D Center, China FAW Corporation Limited, Changchun 130013)

【Abstract】In order to realize the development of vehicle functional safety based on Service Oriented Architecture (SOA), the forward development process for automotive functional safety based on SOA is established combining with the ISO 26262 standard. The functional safety design methods of function-based concept phase and architecture-based system development are proposed. On the one hand, for the concept development phase, the functional safety requirements are derived based on the product capabilities, and the function safety class of product capabilities is defined. On the other hand, for the system development phase, the technical safety requirements are derived and distributed based on the software component architecture and physical deployment.

Key words: Functional safety, Service Oriented Architecture (SOA), Electrical and/or Electronic (E/E) architecture, Forward development process

【引用格式】 杨雪珠, 李军, 陈虹旭, 等. 面向服务架构的汽车功能安全开发研究[J]. 汽车工程师, 2024(10): 16-22.

YANG X Z, LI J, CHEN H X, et al. Research of Automotive Functional Safety Development for Service Oriented Architecture[J]. Automotive Engineer, 2024(10): 16-22.

1　前言

随着智能化、网联化、电动化和共享化的快速推进，汽车功能日益复杂，软件的快速迭代推动着汽车电子电气架构由传统的“面向信号”到“面向服务”开发方式的转变。传统架构下软件与硬件高度耦合，存在硬件资源不能充分共用、新功能开发周期长等问题[1]。近年来，各大整车制造商积极推出基于面向服务架构（Service-Oriented Architecture，SOA）的平台[2]。

SOA提供了一种架构设计理念，定义了可通过服务接口复用软件组件的方法[3-4]，结合以高性能计算平台为核心的集中型电子电气架构，SOA将成为“软件定义汽车”和“数据驱动服务”的重要技术基础。

自ISO 26262《道路车辆 功能安全》发布以来，国内外整车企业及相关高校围绕汽车电子电气系统的功能安全设计与验证展开了积极研究[5-10]。目

*基金项目：国家重点研发计划项目（2022YFB2503001）。

通信作者：陈虹旭，工程师，工学硕士，主要研究方向为汽车系统功能安全设计，chenhongxu3@faw.com.cn。

前，针对功能安全开发的研究多以技术实现为主，较少探讨SOA的功能安全开发方案。

面向传统架构的功能安全开发通常围绕单一电子控制单元（Electronic Control Unit，ECU）进行，由于软、硬件的高度耦合，功能安全需求或技术安全需求可以较快速地分配至软、硬件层级，进行功能安全开发设计。然而，SOA平台下功能安全开发存在新的挑战。首先，功能安全设计会对电子电气架构开发进行约束与补充，为保证产品的研发周期，需要将汽车功能安全开发统一到架构开发过程；其次，SOA将硬件能力抽象为服务的形式，从而实现软、硬件解耦，在新架构平台下，需要合理定义相关项、优化概念阶段对系统层级的输出产物，以适应面向服务的架构设计理念；进一步，SOA软件上的松耦合增强了对服务接口安全等级的适配性要求，硬件上的灵活部署在一定程度上受限于硬件固有安全等级能力，SOA低耦合、可复用的设计思想实现了功能的快速更新和复用，但这也给系统层面的技术安全需求在软、硬件间的分配提出了挑战。

综上，本文提出基于SOA的功能安全正向开发流程，从基于功能的概念开发阶段和基于架构的系统开发阶段两方面说明SOA的功能安全设计方法，以实现SOA与功能安全开发的有机结合，为SOA的整车功能安全开发提供有益参考。

2 面向服务的架构开发

SOA通过标准化服务接口，提供松耦合、易扩展的服务机制，为整车开发提供了更灵活的功能分配、更快速的功能迭代能力。

2.1 服务定义

SOA将整车的不同功能及硬件能力抽象为服务，各服务间通过标准化接口相互访问、扩展和组合[1]。服务可划分为3个层级[11]：

a. 元服务。元服务为底层最小服务单元，汽车传感器、执行器等基本接口可封装为元服务，实现车辆硬件基础能力被上层服务调用。

b. 基础服务。基础服务在元服务层级之上，可以调用元服务，也可被更上层服务调用，例如“环境感知”基础服务调用了“车辆状态”元服务、“雷达等传感器信息”元服务。

c. 应用服务。应用服务为最高层级服务，可以实现更多用户场景的应用。元服务和基础服务强调了架构的灵活性，应用服务更多地强调功能本身。

2.2 SOA软件架构设计

根据高层级服务调用低层级服务、低层级服务不能调用高层级服务这一原则，建立SOA软件分层架构，如图1所示。

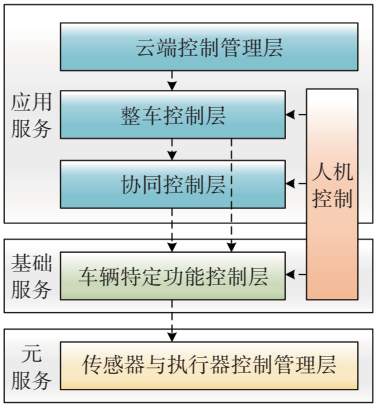

图1 SOA软件分层架构

传感器与执行器控制管理层实现了整车的硬件能力以元服务形式被上层调用，通过访问标准化服务接口实现车辆功能的软、硬件解耦。高层级的软件模块除满足不同层级间的软件调用关系外，还具有模块内高内聚、模块间松耦合的特性，从而有效发挥SOA可重用、易集成等优势。

3 SOA功能安全正向开发流程

3.1 ISO 26262标准

ISO 26262提供了汽车安全生命周期，并为产品开发的不同阶段提供过程参考模型。

针对汽车电子电气系统的开发，通过采用如图2所示的“V”模型开发流程，ISO 26262为与车辆安全相关的系统、软件、硬件的安全设计与安全确认提供了指导。

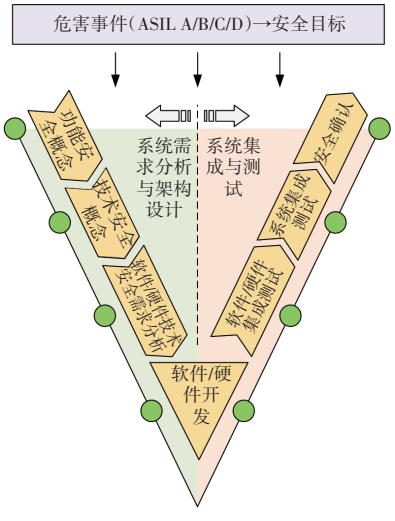

图2 电子电气系统功能安全开发

3.2 基于SOA的功能安全正向开发流程

基于SOA的汽车正向开发流程如图3所示：

a. 以用户需求为导向，基于用户场景定义整车功能，功能安全开发针对每个用例（Use Case，UC）分析功能失效时的危害事件，进行危害分析与风险评估（Hazard Analysis and Risk Assessment，HARA）得到该用例下危害事件的汽车安全完整性等级（Automotive Safety Integration Level，ASIL）和安全目标（Safety Goal，SG），迭代更新到功能定义文档。

b. 功能设计阶段基于每个用例提取出功能对系统的需求，即产品能力（Product Capability，PC），该阶段将车辆的E/E架构抽象为逻辑架构，得到PC时序图，在功能安全概念开发阶段，以该用例的PC时序图作为相关项初始架构，分析PC的失效或PC间交互的失效是否违背相应的安全目标，从而得出功能安全需求（Functional Safety Requirements，FSR），分配给功能安全相关的PC。

c. 基于SOA软件架构的系统设计阶段以PC时序图为基础，定义软件组件（Software Components，SWC）架构、设计SWC服务接口和SWC内部软件模块，其中SWC架构设计满足如图1所示的软件分层架构。

在功能安全系统开发阶段，首先基于功能安全相关PC选择应用服务、基础服务和元服务；根据SWC服务架构进行安全分析，得到技术安全需求（Technical Safety Requirements，TSR），增加安全机制保证架构设计满足功能安全要求，新增的功能安全相关SWC及接口迭代更新到SWC架构设计中。

d. 物理部署阶段通过定义软、硬件接口（Hardware-Software Interface，HSI）规范完成安全机制SWC服务接口的实现，根据硬件网络拓扑，将SWC部署到中央计算平台、区域控制器和ECU中。功能安全开发根据SWC架构和物理部署，进一步分配TSR到软件、硬件要素，导出软件安全需求（Software Safety Requirements，SSR）和硬件安全需求（Hardware Safety Requirements，HSR）。

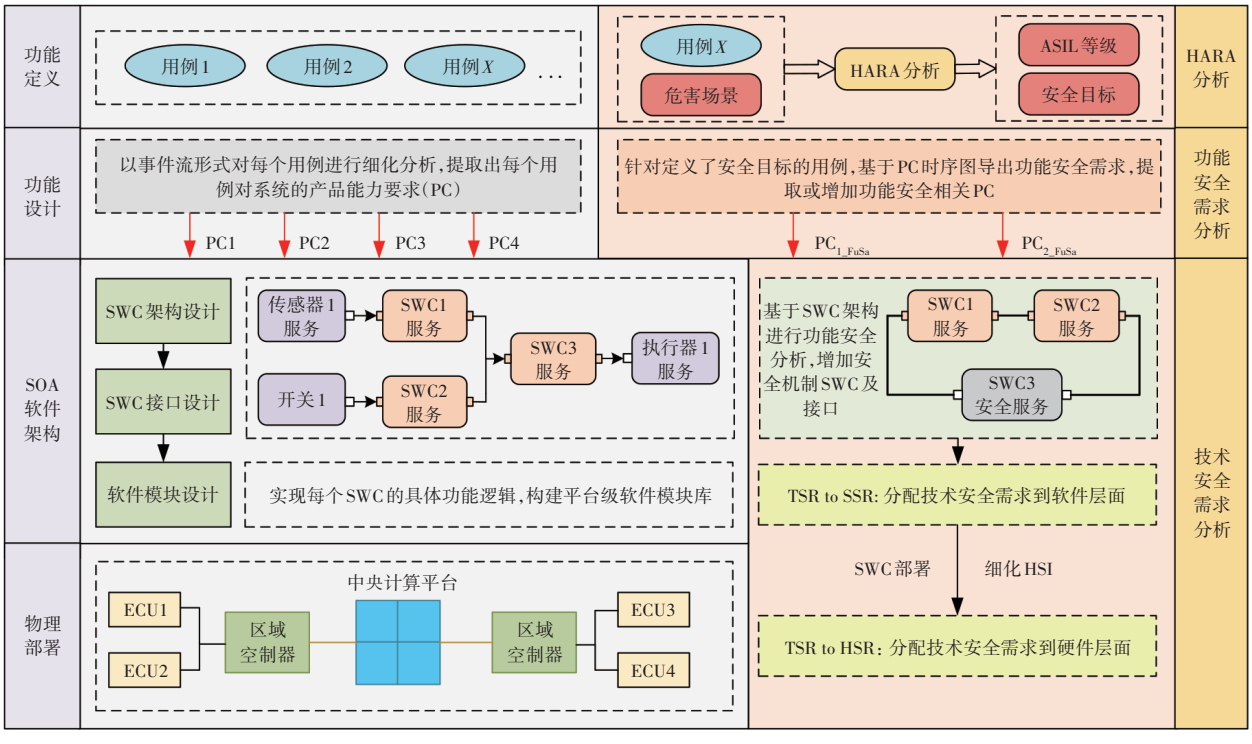

图3 基于SOA的功能安全正向开发流程

综上，面向SOA的功能安全开发流程可以总结为基于功能的概念开发阶段（包括HARA分析与功能安全需求分析）和基于架构的系统开发阶段（包括技术安全需求分析与软、硬件安全需求分配），覆盖了从功能定义落地到物理部署的汽车SOA正向开发流程。

4 SOA的功能安全开发

4.1 基于功能的概念开发阶段

4.1.1 危害分析与风险评估

SOA架构的顶层功能定义针对每个功能进行用户场景的详细分析，提取终端用户对该功能的

UC，HARA分析根据UC和车型性能等内容，分析功能异常导致整车层面的危害事件，通过对危害事件的评估确定该UC下的SG及ASIL。该阶段下功能安全开发活动流程如图4所示，以“提供驱动扭矩”功能为例，定义的用例图如图5所示，对应的安全目标如表1所示。

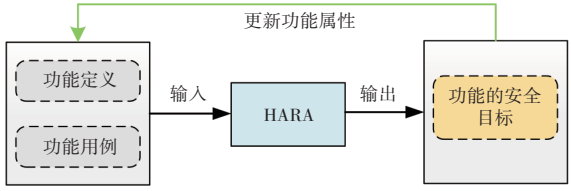

图4　HARA阶段开发活动流程

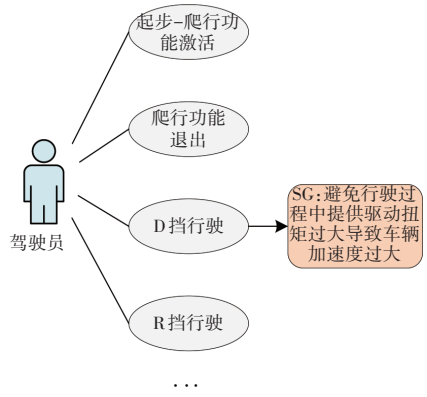

图5　提供驱动扭矩功能用例图

表1　安全目标

项目	内容
ID	SG1
安全目标	避免行驶过程中提供驱动扭矩过大导致车辆加速度过大
ASIL	C
安全状态	扭矩清零，报警提示驾驶员
故障容忍时间间隔（FTTI）/ms	500
UC	D挡行驶

通过构建用例与安全目标的联系，建立了功能安全目标与用户需求和系统开发间的双向追溯关系。

4.1.2　功能安全概念

根据对UC的分析结果进行功能设计，在这一阶段整车的E/E架构抽象为不同逻辑的子系统，PC向上承接功能实现，向下传递给逻辑子系统。采用PC时序图描述“D挡行驶”用例，如图6所示。

PC时序图反映了系统的逻辑架构，本文以此作为概念阶段的相关项初始架构，通过安全分析对SG提出相应的FSR，并将其分配到各PC，同时更新PC的ASIL，表2列出了SG1的部分FSR及PC分配关系，该阶段功能安全开发活动流程如图7所示。

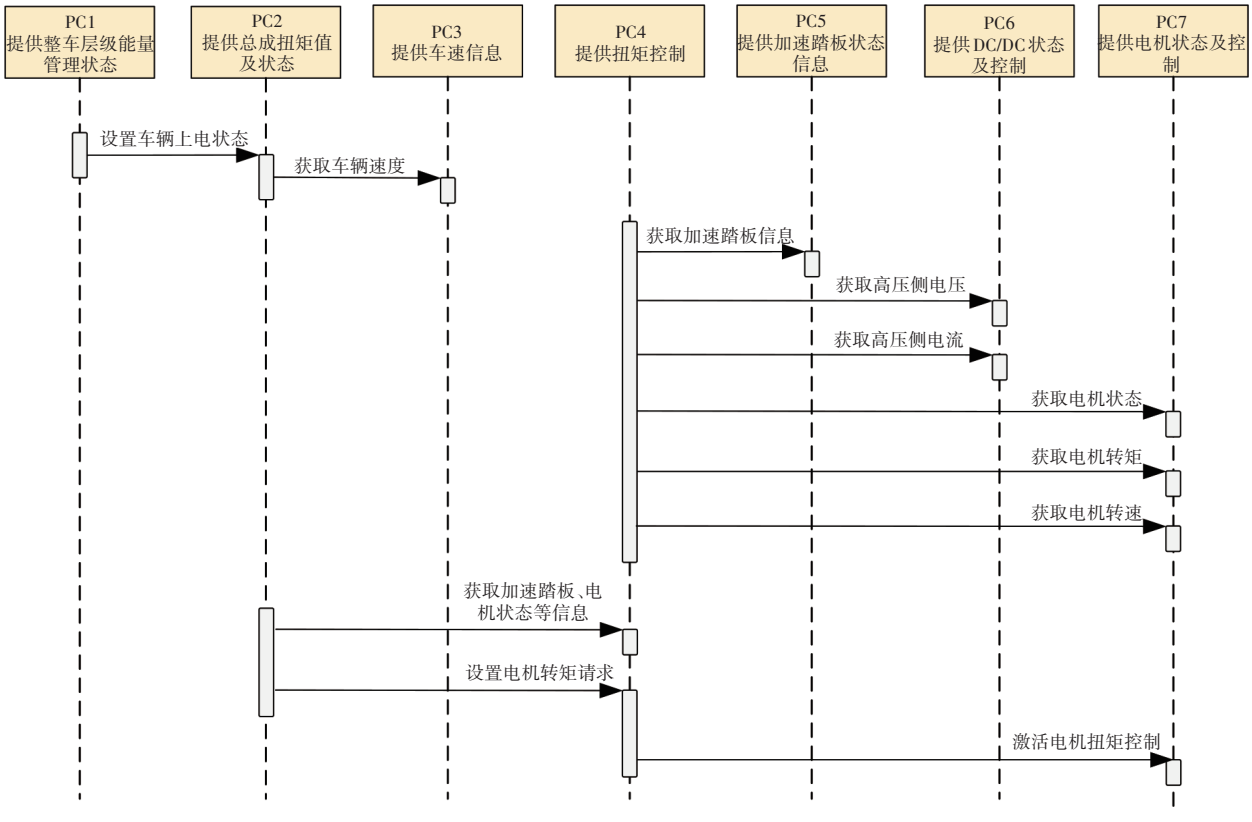

图6　D挡行驶PC时序图

表2　功能安全需求

ID	描述	ASIL	分配
FSR01	应诊断加速踏板位置信号故障导致的驱动扭矩过大故障，并发送故障标志位	C	PC5
FSR02	应避免计算和请求过大的电机驱动扭矩	C	PC4
FSR03	应根据驱动扭矩请求指令正确驱动电机	C	PC7
…	…	…	…

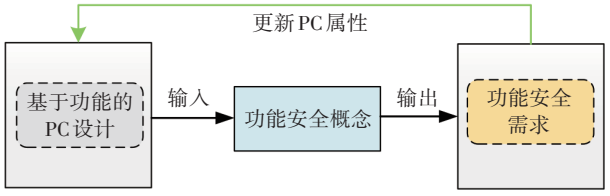

图7　功能安全概念阶段开发活动流程

不同于传统功能安全开发对系统架构的定义，PC描述了系统高层级的功能能力，它并不涉及具体的物理架构，以便于不同车型间的复用。因此，在这一阶段得到的FSR并不具备指导系统设计的能力，即不具备ASIL分解的能力，FSR将作为该PC属性的一部分，随着SWC对PC的继承关系而进一步细化。

4.2　基于架构的系统开发阶段

4.2.1　技术安全概念

为实现PC，需要系统从下至上定义硬件抽象元服务、平台基础服务、应用服务。每个服务对应一个或多个SWC。因此，应基于PC时序图定义SWC架构和设计SWC服务接口，最后根据网络拓扑将SWC部署到具体的物理架构中。以“提供驱动扭矩功能-D挡行驶”的PC设计为例，根据表2得到功能安全需求及如图8所示的SWC架构，得到功能安全需求部署如表3所示。

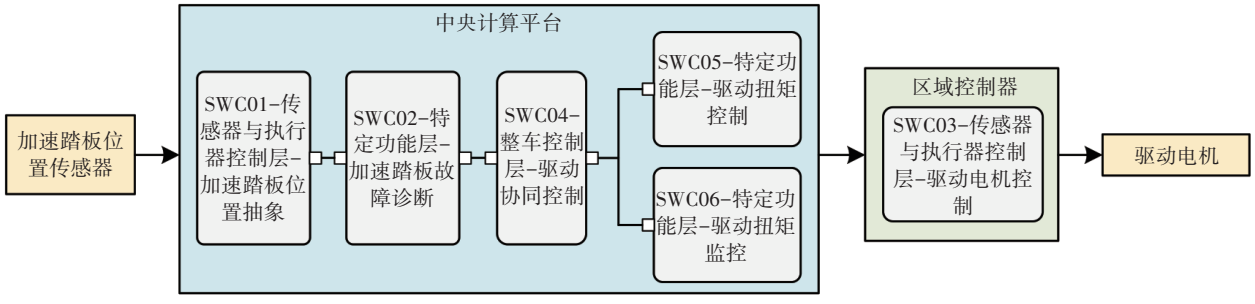

图8　SWC架构及部署

表3　功能安全需求部署

ID	描述	ASIL	PC	SWC	物理部署
FSR01	应诊断加速踏板位置信号故障导致的驱动扭矩过大故障，并发送故障标志位	C	提供加速踏板状态信息	01-传感器与执行器控制层-加速踏板位置抽象 02-特定功能控制层-加速踏板故障诊断	中央计算平台
FSR02	应避免计算和请求过大的电机驱动扭矩	C	提供驱动扭矩	04-整车控制层-驱动协同控制 05-特定功能控制层-驱动扭矩控制 06-特定功能控制层-驱动扭矩监控	中央计算平台
FSR03	应根据驱动扭矩请求指令正确驱动电机	C	提供电机状态及控制	03-传感器与执行器控制层-驱动电机控制	区域控制器
…	…	…	…	…	…

根据SWC架构及部署视图，通过故障树分析（Fault Tree Analysis，FTA）或失效模式与影响分析（Failure Mode and Effect Analysis，FEMA）识别当前架构设计中的风险点，增加安全机制保证系统架构设计满足功能安全需求，即开展技术安全概念开发。如果没有合适的SWC提供安全机制，新增SWC及其接口确认后更新到SWC部署视图。技术安全概念阶段的功能安全开发活动如图9所示。

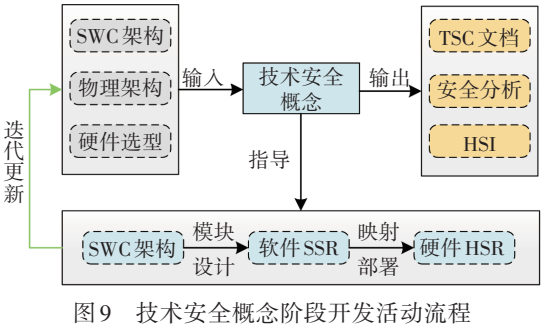

图9　技术安全概念阶段开发活动流程

4.2.2　技术安全需求分配

进一步，在由SWC架构部署到物理架构的过程中，完成SWC服务接口的实现、SWC到硬件的映射部署，实现软硬分离。SWC架构和物理架构确立后，根据硬件选型，分配TSR到软件、硬件和HSI，部分技术安全需求分配情况如表4所示。

表4　技术安全需求分配

FSR	TSR	ASIL	要素分配		
			软件	硬件	HSI
FSR01	TSR01：检测加速踏板1、2供电电压过压、欠压故障	C	Y	Y	Y
FSR02	TSR02：监控驱动扭矩控制模块失效，导致计算的驱动扭矩请求大于需求值	C	Y		
FSR03	TSR03：对控制器局域网（CAN）转矩指令信号进行端到端（E2E）检查	C	Y		Y
…	…	…	…	…	…

综上所述，SOA开发流程下功能安全控制流程如图10所示，SOA架构下的功能安全开发实现了基于功能的功能安全概念（Functional Safety Concept，FSC）和基于架构的技术安全概念（Technical Safety Concept，TSC）开发：FSC开发面向产品能力，确保安全目标、PC和FSR之间的追溯关系；TSC开发基于SWC架构、物理架构与硬件选型，实现软件解耦与软、硬件分离。

5　结束语

面向服务架构是未来汽车电子电气架构开发的核心，本文介绍了以用户场景为驱动的汽车正向开发流程，并结合ISO 26262提出了面向服务架构的功能安全开发方案，覆盖了从功能定义到物理部署的架构开发流程，为面向服务架构的汽车功能安全开发提供参考。

未来，随着智能互联技术的不断发展，车端与云端的信息联通，在SOA开放架构下建立功能安全开发的快速迭代能力，以应对车云一体化生态平台带来的功能安全挑战，是后续的研究重点。

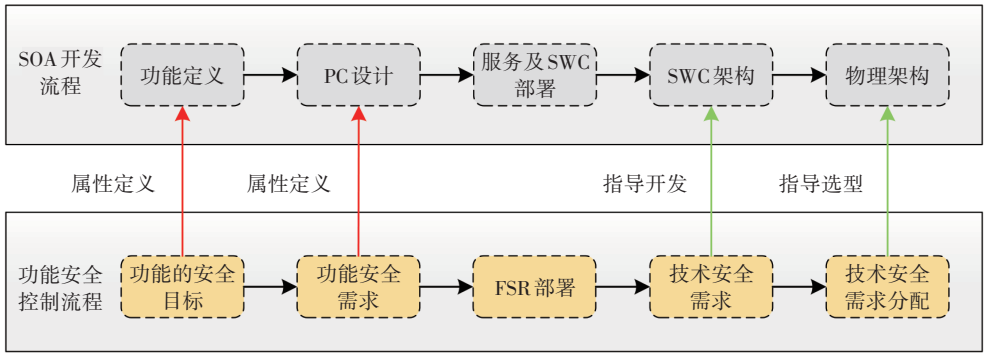

图10　功能安全控制流程示意

参　考　文　献

[1] 鲁涛. 基于SOA面向服务架构的正向开发方法在汽车中的应用研究[J]. 装备制造技术, 2021(12): 147-151.
LU T. Research on Application of the Automobile Industry Based on Service Oriented Architecture Forward Development Method[J]. Equipment Manufacturing Technology, 2021(12): 147-151.

[2] 付朝辉, 王华阳. 功能架构在电子电气架构开发中的应用和实践[J]. 汽车工程, 2021, 43(12): 1871-1879.
FU Z H, WANG H Y. Application of Functional Architecture in Electrical Electronics Architecture Development[J]. Automotive Engineering, 2021, 43(12): 1871-1879.

[3] ERL T. Service-Oriented Architecture: Concepts, Technology, and Design[M]. Upper Saddle River, NJ, United States: Prentice Hall PTR, 2005.

[4] AUTOSAR. Adaptive Platform: R23-11[S/OL]. Hörgertshausen, Germany: AUTOSAR, 2023. (2023-11-23)[2024-08-26]. https://www. autosar. org/standards/adaptive-platform.

[5] BECKER C, YOUNT L, ROZEN-LEVY S, et al. Functional Safety Assessment of an Automated Lane Centering System: DOT HS 812 573[R]. Washington, DC, United States: National Highway Traffic Safety Administration, 2018.

[6] WILHELM U, EBEL S, WEITZEL A. Functional Safety of Driver Assistance Systems and ISO 26262[M]// WINNER H, HAKULI S, LOTZ F, et al. Handbook of Driver Assistance Systems. Cham, Switzerland: Springer International Publishing, 2016: 109-131.

[7] KRAMPE J, JUNGE M. Injury Severity for Hazard & Risk Analyses: Calculation of ISO 26262 S-Parameter Values from Real-World Crash Data[J]. Accident Analysis and

Prevention, 2020, 138.

[8] 尚世亮, 赵向东. ISO26262中可控性参数指标的建立方法[C]// 2015中国汽车工程学会年会. 上海: 中国汽车工程学会, 2015: 147-150.
SHANG S L, ZHAO X D. Method of Controllability Metric Definition in ISO26262[C]// 2015 China SAE Congress. Shanghai: China SAE, 2015: 147-150.

[9] 童菲, 尚世亮, 熊志刚. 汽车系统功能安全架构的设计与发展展望[J]. 汽车文摘, 2019(5): 12-17.
TONG F, SHANG S L, XIONG Z G. The Design and Development Perspectives of Functional Safety Architecture for Automotive Systems[J]. Automotive Digest, 2019(5): 12-17.

[10] 卜纯研. 面向路径跟踪控制功能安全的智能汽车多传感器冗余定位策略[D]. 长春: 吉林大学, 2022.
BU C Y. Multi-Sensor Redundant Localization Strategy of Intelligent Vehicle for Path Tracking Control Functional Safety[D]. Changchun: Jilin University, 2022.

[11] 刘佳熙, 施思明, 徐振敏, 等. 面向服务架构汽车软件开发方法和实践[J]. 中国集成电路, 2021, 30(增刊1): 82-88.
LIU J X, SHI S M, XU Z M, et al. Development Methodology and Practice of Automotive Software Based on Service Oriented Architecture[J]. China Integrated Circuit, 2021, 30(Z1): 82-88.

（责任编辑　斛　畔）

修改稿收到日期为2024年8月16日。