ORIENTAIS®

AUTOSAR

普华灵智基础软件平台产品手册

普华基础软件股份有限公司

版权所有

目录

一、基本情况 2
二、普华灵智车用基础软件平台ORIENTAIS Classic AUTOSAR 2
（一）操作系统与模式管理系统 3
1.1AUTOSAR Safety OS 4
1.2 模式管理系统 6
（二）通信系统 6
2.1 现场总线通信 7
2.2 车载以太网通信 8
2.3 网络管理 10
2.4 诊断 12
2.5 标定 13
2.6 J1939 协议栈 15
（三）存储管理 16
（四）功能安全和信息安全 18
4.1 功能安全 18
4.2 信息安全 20
（五）Bootloader 22
（六）时间同步 22
（七）FOTA 解决方案 24
三、集成开发环境 25
附录 28

一、基本情况

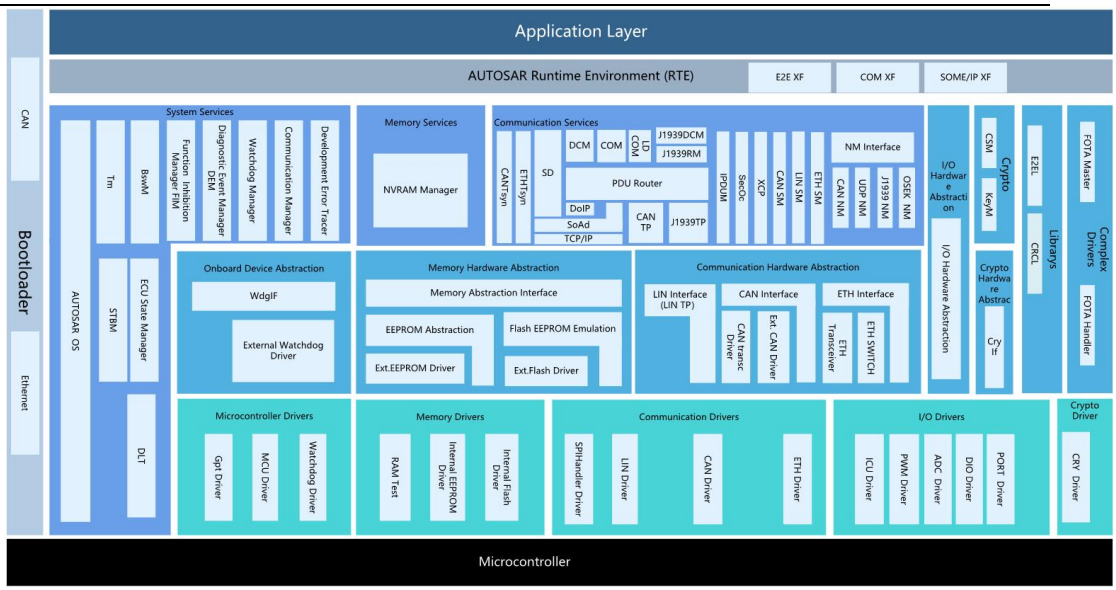
普华基础软件自2009年起深耕AUTOSAR车用基础软件领域，作为AUTOSAR组织高级合作伙伴，拥有强大的AUTOSAR专业技术团队。普华基础软件为国内各大OEM整车厂和主要的零部件供应商提供基于AUTOSAR标准的国产化汽车电子基础软件平台、开发工具和软硬件一体化解决方案、优质的本土化技术支持、现场软件集成支持及售后技术支持，具有丰富的用户案例和AUTOSAR集成服务实战经验。

二、普华灵智车用基础软件平台ORIENTAIS Classic AUTOSAR

随着汽车向高性能、多功能化发展，电控单元的数量和功能复杂度不断递增，软件开发在汽车电子领域的重要性日益显著，对整车软件的一致性、复用性、高效率开发的要求越来越高。在此行业背景下，汽车电子软件实现平台化，可以使零部件供应商以及主机厂专注于上层应用的开发，从而使应用控制开发脱离对底层软件及硬件平台的深度依赖，增强软件系统可移植性和可维护性，进而提高测试和开发效率。

普华基础软件提供符合业界现行标准的国产自主基础软件整体平台解决方案—普华灵智车用基础软件平台 ORIENTAIS Classic AUTOSAR。该平台定位于满足汽车电子应用开发及测试需求，提供一体化的系统解决方案、定制开发和本地化技术支持。

为了使不同厂家生成的ECU方便可靠地集成到通信网络中，普华灵智车用基础软件平台为用户提供了操作系统与模式系统服务、通信系统、存储管理、功能安全和信息安全、Bootloader、时间同步、FOTA解决方案等基础软件模块及集成开发环境。



图• 普华灵智车用基础软件 ORIENTAIS Classic AUTOSAR平台架构图

产品特性

(1) 完整的 Classic AUTOSAR集成开发环境，包括SWC设计工具，BSW基础软件配置工具，RTE 配置及代码生成工具

(2) 覆盖支持Classic AUTOSAR 标准 3.1.5/4.2.2/R19-11

(3) AUTOSAR Safety OS 产品通过德国莱茵 ISO 26262 功能安全 ASIL D 最高安全等级产品认证

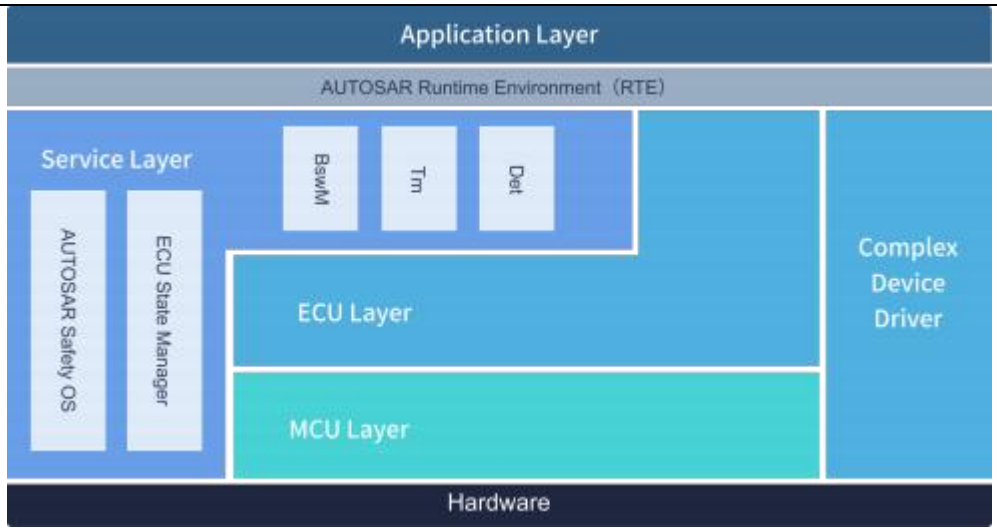
(4) 支持以太网、CAN/CANFD、LIN 总线

(5) 支持信息安全

(6) 支持OTA、FOTA

（一）操作系统与模式管理系统

随着汽车工业的快速发展，汽车在降低能耗、提高安全性和舒适度等方面的要求越来越高，极大的促进了汽车电子技术在整车系统的应用和创新，同时汽车电子软件的开发难度和复杂性也不断上升，其强实时、高可靠、网络化、平台化及标准化的要求和趋势日益显著，使得汽车电子专用的嵌入式实时操作系统和开发环境正成为支撑汽车电子软件开发和运行的基础。AUTOSAR OS 加上系统服务模块，实现电控单元最小软件系统，实现电控单元软件系统的状态和生命周期管理。



图• ORIENTAIS Classic AUTOSAR 操作系统与模式管理系统

1.1AUTOSAR Safety OS

AUTOSAR OS 是针对汽车嵌入式领域的一种实时操作系统，秉承消耗最低的运行时间和灵活配置的原则，能为汽车电子厂商的应用软件提供最优化的操作系统内核。它具有代码精简、中断屏蔽时间短、中断响应及任务切换快、应用隔离保护、内存保护、时间保护、应用保护、模式管理、同步时基等特点，在具备良好性能的同时能为汽车电子应用提供一个资源消耗小、可裁剪、可扩展、移植性强的运行平台，是专门为汽车电子领域开发的可抢占多任务的实时操作系统。

支持多芯片平台移植，目前支持的有AURIX TC2xx/TC3xx、Tricore TC17xx、NXP S32K14x、NXP S32K3xx、MPC57xx、ST SPC58xx、Renesas RH850、芯驰 G9X 等。

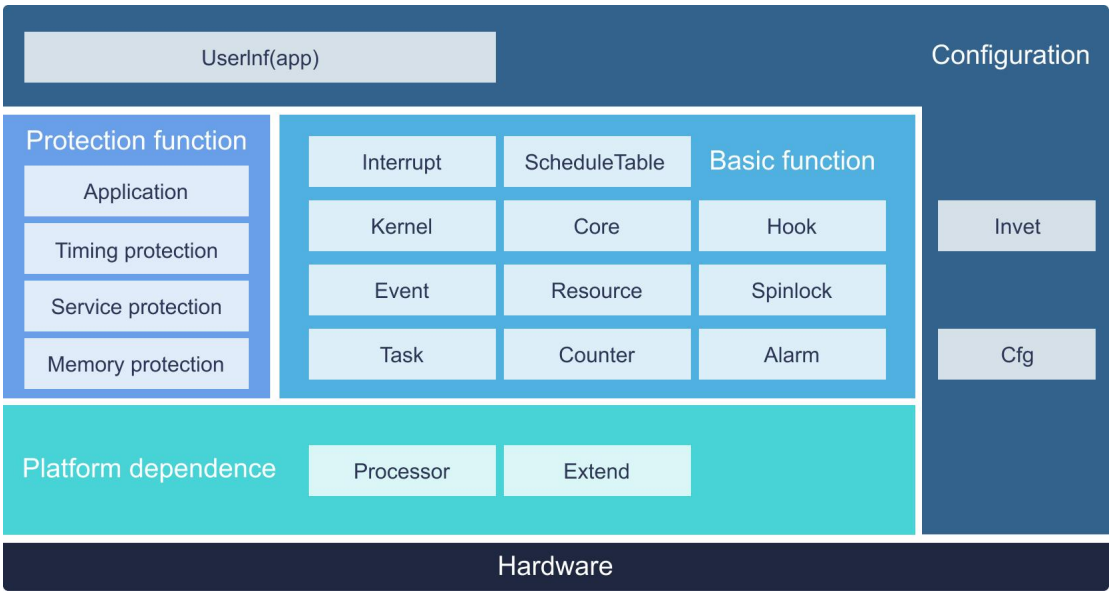
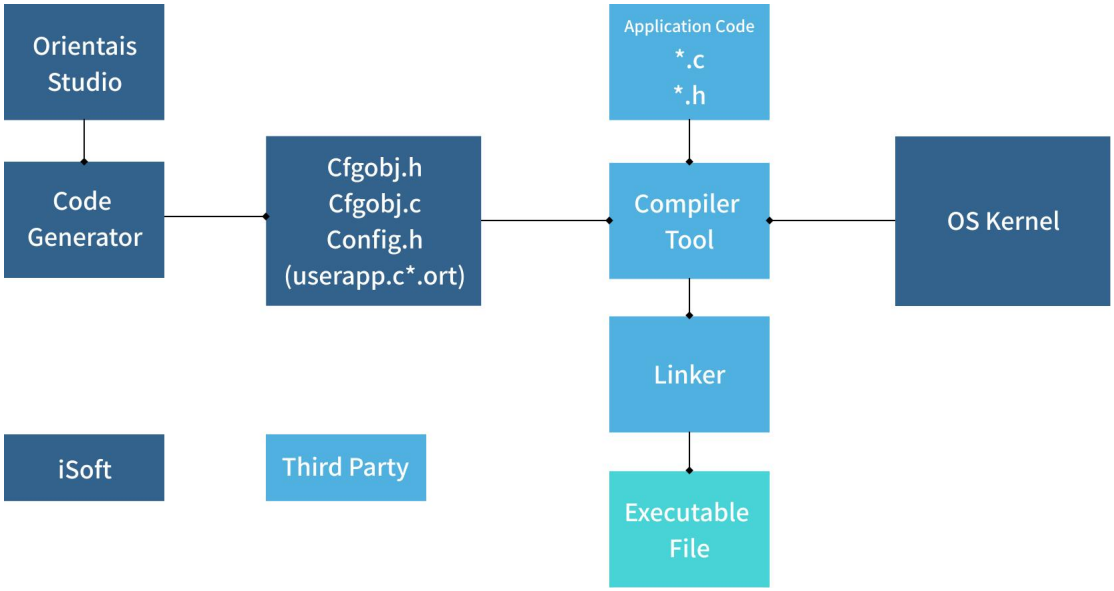


图 • AUTOSAR Safety OS 实时操作系统模块结构

 版权所有



图·AUTOSAR Safety OS 操作系统配置开发流程

产品特性：

(1) 基于 AUTOSAR 4.2.2、涵盖部分 R19-11 版本功能，以及兼容 OSEK/VDX OS 2.2.3 标准

(2) 支持 SC1-SC4 级别功能，涵盖国内外所有主流内核架构

(3) 支持多核架构，并提供多核间通信 IOC 方式

(4) 最大支持16个核，提供核启动关闭、核间同步、跨核调用功能

(5) 支持中断嵌套，提供一类和二类中断

(6) 最大支持 4095 个任务、255 个资源、16 种应用模式、32 个事件

(7) 提供堆栈溢出、堆栈使用率检测以及 CPU 负载率检测功能

(8) 提供核内资源互斥访问机制

(9) 提供核间资源互斥访问机制——自旋锁

(10) 提供软硬件计数器功能

(11) 支持周期警报、调度表

(12) 提供外设地址访问接口

1.2 模式管理系统

AUTOSAR系统服务是一组模块和函数，这些模块和函数可以被所有软件层模块使用。比如操作系统（包括定时器服务）和错误管理。系统服务的实现与 ECU 硬件以及应用程序有部分关联，其上层接口与 ECU 硬件无关。

系统服务中模式管理相关的模块主要包括 EcuM（ECU 状态管理）和 BSWM（基础软件模式管理），与操作系统（OS）模块组成 ECU 基础软件平台的基础系统，执行ECU软件功能调度与模式管理。

（二）通信系统

现代汽车随着电子设备的不断增加，造成线束数量的不断增多，汽车空间内布线越来越困难，限制了功能的扩展，同时线束质量的增加也增加了车辆油耗。

汽车ECU并不是与负载设备简单地连接，更多需要与外围设备、传感器及其它电控单元进行信息交流，经过复杂的控制运算，发送控制指令，这些功能简单的线束连接已经不能实现。如今CAN、LIN、ETH等总线已经被汽车电子产品开发广泛采用，简化布线，提高了ECU之间通讯的可靠性，同时保证整个系统数据的一致性，做到一次取得数据，整个系统共同使用。标准化的通信组件的需求使基于总线的软件开发工作越来越重要。

AUTOSAR COM提供了一种标准化的访问汽车通讯系统和 ECU（Electronic Control Unit）通讯的方式，提出了一个在不同速率的总线网络之间进行数据交换的方法。它为汽车控制单元应用软件提供了一个统一的通信环境，为内部和外部通信定义了公共的软件通信接口和行为，增强了应用软件模块的可移植性。

AUTOSAR COM提供了基本的通信服务，主要实现信号的收发、信号网关、报文网关等功能，使得应用层专注于信号的处理。

ComM 模块：对ECU电控单元所有通信总线资源进行统一管理，为模式管理系统和应用功能提供统一的接口管理总线资源状态。

Com 模块：实现Signal的封装及解析，Signal网关，Tx-PDU的发送模式，以及基于 Signal/PDU 的多种辅助监测机制，如信号收发超时监测，报文时序管理，信号过滤，无效信号检测，信号 Update-bit 机制等。

LdCom 模块：实现“Large Data" 信号的收发，即每个 PDU 默认只包含一个信号，模块只简单实现基于 PDU 的收发。

PduR 模块：实现基于 PDU 的路由，确定每个 PDU 的传递路径。PDU 的路由分发送路由、接收路由、网关路由三种类型。

IPduM 模块：实现 PDU 的多路复用，即将上层多个 I-PDU 封装到下层 L-PDU进行统一收发。

与通信系统相关的模块有：现场总线通信、车载以太网通信、网络管理、诊断、标定和 J1939 协议栈。

2.1 现场总线通信

现场总线通信包含 CAN/LIN 总线的通信支持，除总线无关上层模块外还包括模块：CAN 总线 CanSM、CanTp、CanIf、Can、CanTrcv，LIN总线LinSM、LinIf（包含 LinTp）、Lin、LinTrcv，各类总线相关模块实现 PDU 在各自总线上的收发。

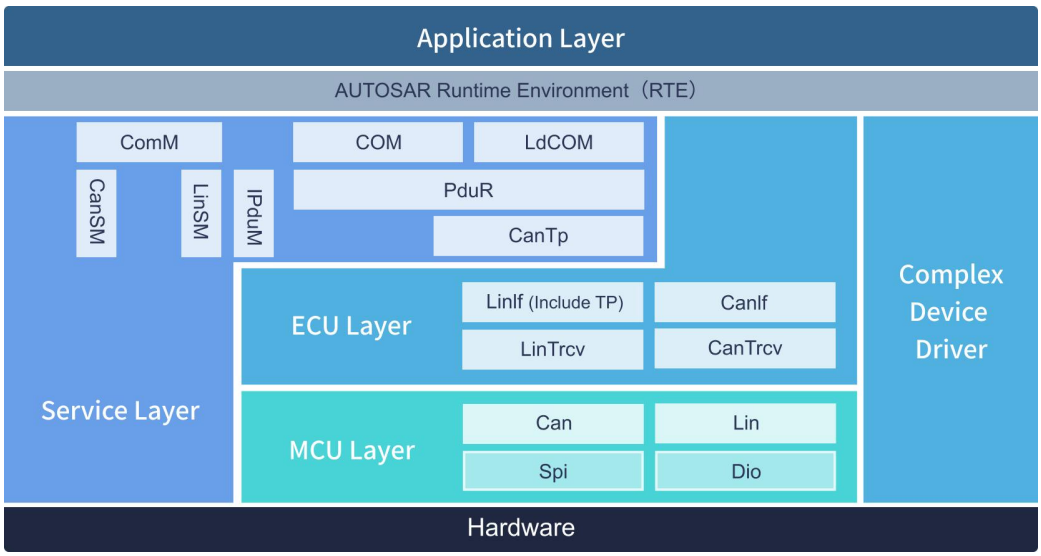


图 • 现场总线通信

产品特性 ：

(1) 遵循 AUTOSAR 4.2.2/R19-11 标准

(2) 支持 DBC 文件导入

(3) 支持标准帧和扩展帧

(4) 支持 CAN/CANFD 功能

(5) 报文收发支持中断或者轮询方式

(6) 支持整型和数组类型信号收发

(7) 支持 PDU 周期性发送、触发发送和混合发送模式

(8) 支持信号大小端转换和过滤

(9) 支持 PDU 网关，信号网关

(10) 支持信号发送接收超时监控和通知机制

(11) 提供通信驱动模块定制开发（CAN/LIN）

(12) 支持 LIN 通信，符合 ISO17987 标准，支持主从节点：

1) 调度整个 LIN 网络报文的收发，并支持切换调度表

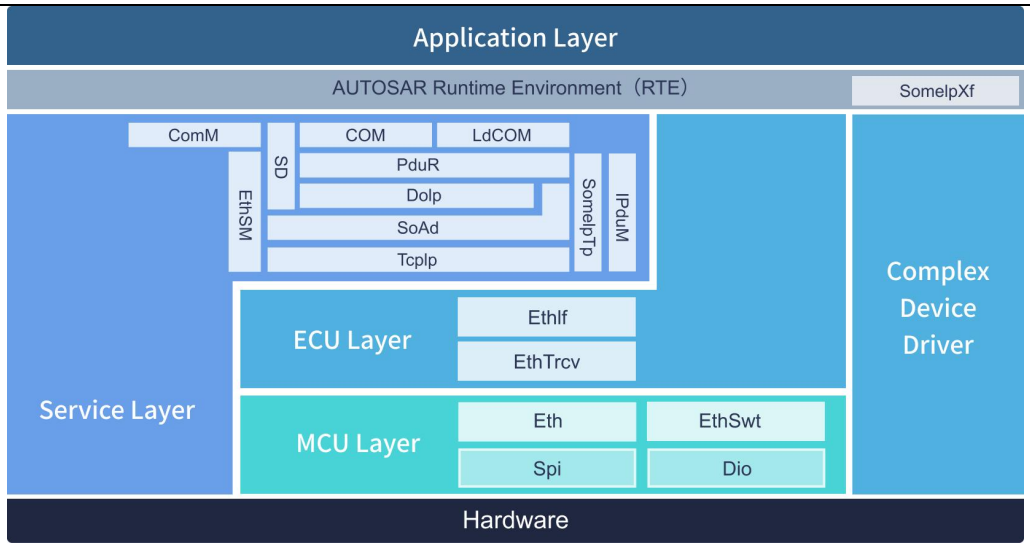
2) 支持不同 LIN 数据帧类型的处理，包括事件帧、零星帧、诊断帧、无条件帧等

3) LIN 诊断传输层报文的处理

2.2 车载以太网通信

随着汽车行业的发展，智能互联、车载娱乐和网络安全等领域对带宽的要求越来越高，加上博通 BroadR-Reach 方案解决了传统以太网标准在车载应用中的各种问题，使得车内网络对以太网的需求越来越多。车载以太网模块就是为了适应这些新的变化开发出来的标准 AUTOSAR 组件。

作为车载通信总线的一种类型，实现基于以太网的通信、诊断、网络管理、标定功能。以太网通信除上层无关模块外还包括以太网总线特有的 EthSM、EthIf、SoAd、TcpIp、DoIP、SD、SOMEIPTP 等模块。



图·以太网通信

EthIf 模块：作为底层驱动（Eth、EthTrcv）和上层模块的桥梁，进行收发、休眠唤醒、时间同步等接口的上下层传递。

SoAd 模块：将上层模块基于 PDU 的通信转换为下层基于套接字 Socket 的 TCP/UDP 通信，实现 AUTOSAR 通信服务层与 TCP/IP 协议的衔接。

TcpIp 模块：实现 TCP/IP 协议簇的功能(ARP/IPv4/ICMPv4/UDP/TCP/DHCPv4/AUTOIP)，与上层模块实现基于 TCP/UDP 的通信。

DoIP 模块：支持车辆通告和车辆发现功能；车辆检索功能；连接状态建立、维持功能；诊断数据路由功能等。

SD 模块：探测外部是否有可用的服务，定位服务位置，向外部提供可用的服务，实现发布/订阅机制，以控制 Event 报文的订阅和发布。

SomeIpXf 模块：将原始数据序列化为符合 SOME/IP 要求的格式。将符合 SOME/IP 格式的报文反序列化为原始数据。

SomeIpTp 模块：SOME/IP TP 为使用 UDP 发送长度大于 1400 字节的 SOME/IP 报文提供了可能。在发送端，SOME/IP TP 将原始数据进行分段，插入 TP 报头后分段发送出去。在接收端，SOME/IP TP 利用 TP 报头将接收的分段进行重组，传递给上层用户。

车载以太网模块提供了基于 AUTOSAR 4.2.2/R19-11 的标准Socket接口，用于封装以太网数据。同时提供 SOME/IP、DOIP、UDPNM等应用层协议，用于客户车载以太网通讯、诊断和网络管理功能的实施。

产品特性：

(1) 遵循AUTOSAR4.2.2/R19-11标准

(2) 支持TCP/IP协议族（IPV4）

(3) 支持服务和事件报文的发现，支持SOME/IP数据的序列化和反序列化

(4) 支持 ISO-13400-2，支持基于TCP和UDP的DOIP报文收发

(5) 支持 UDP 报文的同步休眠和唤醒

(6) 支持以太网协议栈移植到Linux平台

2.3 网络管理

随着汽车电子电气化程度的提高，各个电子控制单元需要同其他控制单元交换更多的信息，确保对自身功能和整车功能进行更加有效的控制。传统布线方法无法满足电子控制单元间大量信息的通讯需求，汽车网络的出现不仅解决了日益复杂的线束布置问题，同时也给汽车的优化控制带来了质的飞跃。为了保证 ECU 之间通讯安全可靠，支撑对临时故障的最大容错性，同时支持同网络有关的诊断功能，需要网络管理功能来支持和维护汽车通讯的整个网络。

网络管理模块采用分布式网络管理方式并具有强实时性、高容错性、低资源占用率的特性，通过监控网络状态的诊断功能确保了通信网络的安全性和可靠性，使网络中的 ECU 节点有序地睡眠和唤醒，在没有通信需求的时候睡眠，可以节约能耗，提高总线利用率。

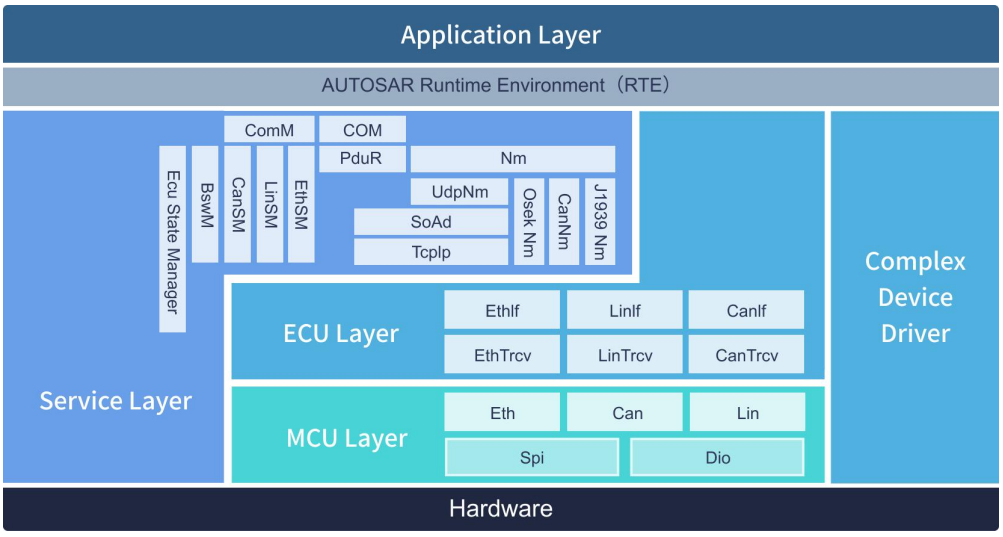


图 • 网络管理

网络管理除了CAN和以太网总线底层基本通信和状态管理模块外还包含实现网络管理算法的NmIf、CanNm、UdpNm、J1939Nm等模块，以及按照OSEK直接网络管理算法以满足 AUTOSAR 网络管理 CDD 接口实现的 OSEK NM。

ComM：面向用户简化网络管理细节，ComM 模块封装了控制底层的通信服务，通信管理模块从通信请求者那里收集总线通信访问请求，并协调这些请求。

NmIf：多总线类型的归集与协调关闭，NmIf 功能由两部分组成 ，一是与特定于总线的 NM 模块一起在 ECU 上运行 AUTOSAR NM 所需的基本功能，二是网关ECU 使用 NM 协调器功能来同步关闭一个或多个总线。

CanNm：CAN 网络的 NM PDU 管理，CanNm 模块的核心功能是协调网络正常运行和总线睡眠模式之间的转换。

UdpNm：Eth 网络的 NM PDU 管理，UdpNm 模块的核心功能是协调网络正常运行和总线睡眠模式之间的转换。UdpNm 提供网络管理接口（Nm）和 TCP / IP 堆栈（TCP / IP）之间的适配。

CanSM：CAN 总线的状态管理器 CanSM，负责实现 CAN 网络控制流程的抽象。CanSM 提供 API 以便 ComM 来请求 CAN 网络进行通信模式的切换。ComM 请求切换网络模式的时候，会传递一个参数（用来标识是哪个网络）。对应网络收到这个请求之后，会执行对应的通信模式切换。在网络通信模式切换的过程中，会执行对应的CAN外设控制和PDU处理。

EthSM：EthSM基于以太网，针对上层对 Network 的请求，通过EthIf模块控制底层的一个或多个 Controller和 Transceiver，从而达到关闭或者开启通信的目的。

产品特性 ：

(1) 支持OSEK/VDX NM 2.5.3 或支持 AUTOSAR4.2.2/R19-11

(2) 支持CAN控制器睡眠、唤醒及BUSOFF恢复机

(3) 支持CAN、LIN、以太网网络同步唤醒及同步睡眠机制

(4) 支持网络节点上线通知及本地节点状态通知

(5) 支持远程睡眠提示

(6) 支持定制化用户数据

(7) 支持部分网络PNC功能

(8) 支持通信控制功能

2.4 诊断

车辆法规对汽车排放、安全的要求不断提高，使得车辆在运行时必须通过对传感器、执行机构和ECU等进行实时监测来实现对车辆各个工作系统运行情况的监测，并且记录存储故障代码，提供实时警告。另一方面，工程人员通过诊断设备同整车通讯，达到维修和监测的目的。针对诊断设备和汽车ECU之间的数据交换，各大汽车公司制订了相关的标准和协议，这一整套从物理层到上层应用的协议叫做通信诊断协议栈。

诊断产品是针对汽车电子电控单元和非车载诊断设备进行通信，为其提供诊断通信服务的软件模块。通过诊断软件可以在ECU产品开发过程中读写系统信息和诊断数据；生产过程中做功能测试以及辅助完成零部件的生产；在售后市场上支持对ECU的诊断信息的读取和控制。

诊断协议栈包括CanTp、Dcm、Dem、FIM、DoIP等模块，主要对诊断请求进行处理与响应，针对故障进行管理等。

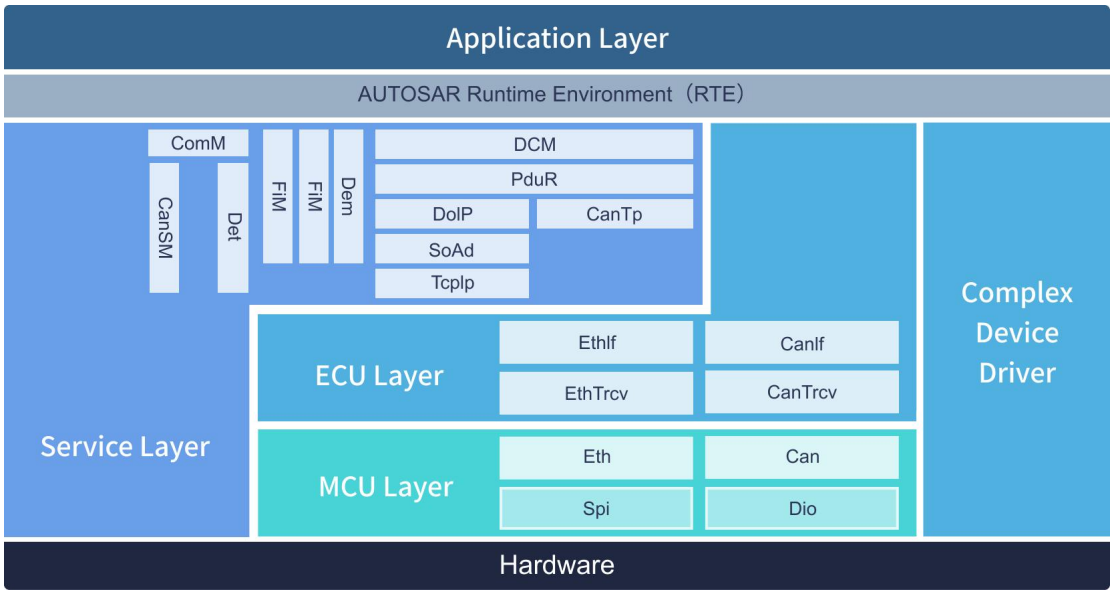


图 • 诊断协议栈

CanTp 模块：实现依据ISO 15765-2标准规范中定义的CAN总线数据在传输层的数据接收发送功能。在ISO 15765-2中，CanTp模块需要实现数据的发送拆包、接收数据重组、数据流控和错误处理机制，需要支持CANFD、MetaData、半双工通信与全双工通信。按照 AUTOSAR4.2.2 标准规范的定义，CanTp模块还实现了发送请求的取消处理。

DCM 模块：实现依据ISO 14229-1和ISO 15031-5等标准规范中定义的UDS诊断和OBD诊断功能。在接收到一个诊断请求后，需要对诊断请求进行分析，包括请求的服务是否支持，寻址方式是否正确，会话级、安全级、长度、子服务等是否正确。

DEM 模块：支持对诊断故障进行相应的管理，当诊断故障被报告时，检查操作循环和使能条件是否满足，然后根据故障状态对相应的状态位进行改变，在触发存储时，判断存储使能条件是否满足，满足时进行存储。

FIM 模块：支持功能禁止管理，根据故障状态状态位，与故障关联的FID的MASK 进行计算，如果计算结果满足抑制，则FID的抑制计数器加1，如果计算结果不满足抑制，则FID的抑制计数器减1，当FID的抑制计数器等于0 ，FID 为允许状态，当抑制计数器不等于0，FID为抑制状态 。

DoIP 模块：支持车辆通告和车辆发现功能；车辆检索功能；连接状态建立、维持功能；诊断数据路由功能等。

产品特性：

(1) 支持 UDS、OBD等

(2) 可灵活配置诊断协议

(3) 可灵活配置传输层时间参数

(4) 可以协助用户制定诊断规范

(5) 支持多帧传输

(6) 支持物理地址及功能地址寻址

(7) 支持安全校验等诊断功能

(8) 灵活详细的配置选项及说明

(9) 支持用户自制加密算法、支持多安全级、多会话层、多服务列表的配置

(10) 支持用户自定义 DID、DTC数据的读写机制

(11) 可以协助用户定制和开发诊断故障码管理策略

2.5 标定

ECU 软件系统最终匹配和优化，由V模型开发的一个重要环节——标定来完成。该过程涉及到一系列复杂的ECU软件参数值修改，需采集大量实验数据，并

做技术处理和验证，最终实现控制策略及其参数的确定，实现电控单元的性能调优。

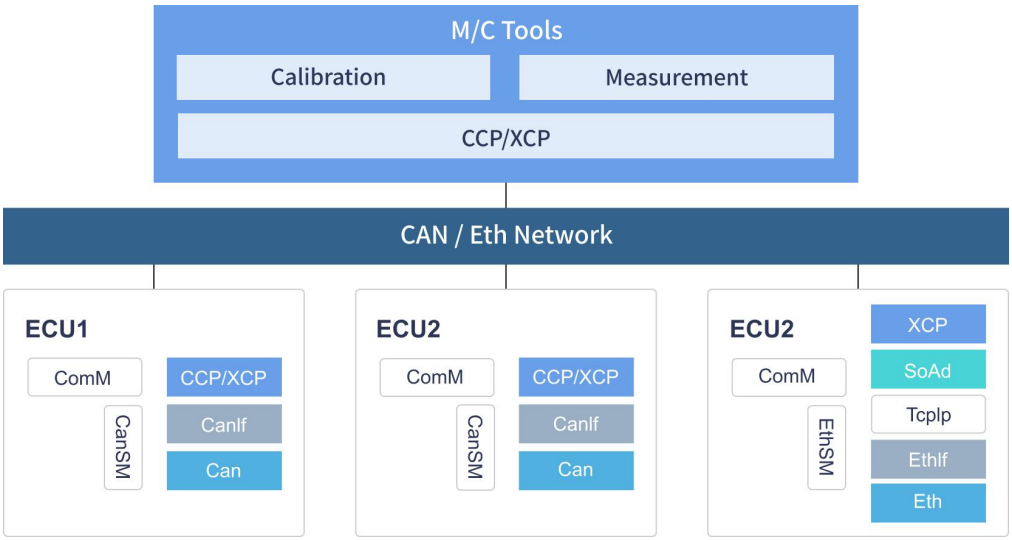


图 • 标定系统

XCP 模块基于欧洲自动化及测量系统协会 (ASAM) 关于标定的协议研发，主要实现ASAM XCP规范定义的57条命令（主要分为 STD/CAL/PAG/DAQ/PGM 五大类），XCP协议栈主要存在于 ECU 中，通过命令流的方式与上位机（如 CANape/INCA）等进行交互，达到在线标定（calibration）、测量（Measurement）的功能。

产品特性：

(1) 支持 ASAM XCP 1.1，支持CAN/ETH总线

(2) 兼容 ETAS INCA 及 Vector CANape标定上位机

(3) 支持 Synchronous data acquisition（DAQ 上传）

(4) 支持 RESUME 功能

(5) 支持 Synchronous data stimulation（STIM）

(6) 支持在线标定功能

(7) 支持页切换功能

(8) 支持静态、动态 DAQ 配置

(9) 支持 Master/Slave块传输通信模式

(10) 支持 Interleaved通信模式

(11) 支持 Seed & Key保护，支持用户自定义安全算法实现

(12) 支持 Flash Program

(13) 支持时间戳功能

2.6 J1939 协议栈

J1939是基于德国 Bosch公司（Robert Bosch GmbH）的控制器局域网络（CAN: Controller Area Network）开发的通信协议。该协议栈实现了 SAE J1939 标准的大部分功能，J1939 主要应用场景是中重型道路车辆中电气设备通讯以及电动汽车充电桩领域；J1939 协议栈实施在经典 CAN 总线上，波特率限定为 250Kbps 使用扩展 CanID；AUTOSAR 实现了 SAE J1939 21 中的大数据传输、Request、Request2、AckM 收发；实现了 SAE J1939 73 中诊断的大部分 DMx，以及 SAE J1939 81 网络管理地址申明与仲裁。

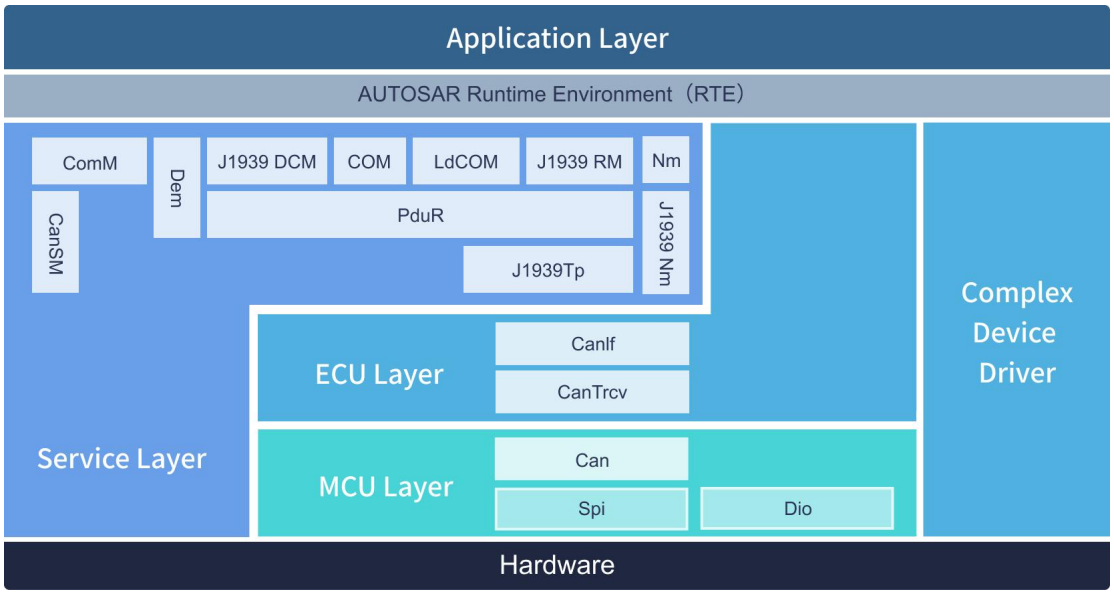


图 • J1939 协议栈

J1939 协议栈相关的模块包括：J1939DCM、J1939TP、J1939NM、J1939RM等。

J1939DCM：定义了诊断消息（DM）的结构与行为。主要用于通过若干预设的诊断信息，向司机台周期性广播车辆故障情况，并激活预设的警告报警灯，以提醒司机车辆状态。以及在车辆维修时向维修人员提供维修辅助信息。J1939DCM 主要功能点是对诊断信息请求处理与应答，具体诊断信息的产生逻辑需要借助AUTOSAR中的Dem模块实现；J1939DCM 参考规范为 SAE J1939 73-2010。

J1939TP：主要用于响应网络中的 BAM 和 CMDT 请求，建立会话连接，对接收的多包数据进行重组或者对要发送的大数据进行拆包。J1939TP 参考规范为 SAE J1939 21-2006。

J1939NM：主要用于 J1939 功能栈中的网络管理功能，区别于其它网络管理模块的功能，J1939NM并不负责网络睡眠和唤醒工作。1939NM主要负责定义网络中的 CA、管理地址分配、管理网络错误、声明节点地址、管理通道状态等。J1939NM参考规范为 SAE J1939 81-2011。

J1939RM：主要用于 J1939 功能栈中的请求管理功能，主要负责 Request、Request2收发处理， 以 及 ACKM 的收发处理；J1939RM对收到的Request、Request2进行识别后转发给 AUTOSAR 中的其他通讯模块，其他通讯模块将对请求进行应答；对于自身节点请求网络中其他节点的应答，J1939RM 支持对网络中节点的请求应答识别与转发。

产品特性：

(1) 支持 SAE J1939-73 中定义的DMx处理

(2) 支持 SAE J1939-81 地址管理声明

(3) 支持 SAE J1939-21 中 Request/Request2 ACKM收发

(4) 支持 SAE J1939-21 中定义的大数据收发

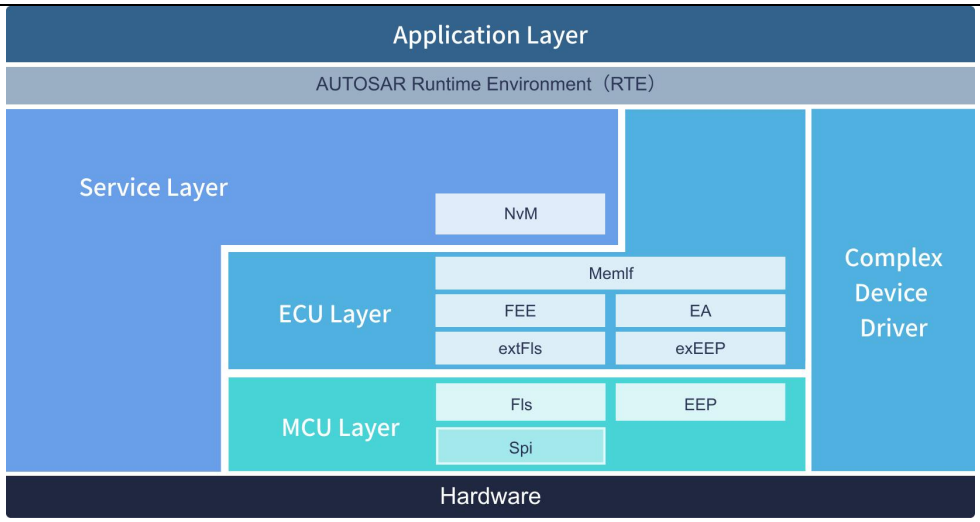
(5) 支持满足 SAEJ1939 的动态数据长度收发

(6) 支持满足 SAEJ1939 的大数据重传与并发链接

（三）存储管理

随着汽车工业的发展，各种嵌入式系统被广泛地用于汽车电子之中，良好的汽车电子软件可以增加汽车的舒适性，保证车辆的安全，为用户提供便捷的操作。在所有汽车电子软件中，存储管理模块起到了至关重要的作用。

存储管理模块采用层次化的结构设计方法，针对汽车电子应用特点，对底层的物理存储器进行抽象，包含一个功能齐全，可配置的底层驱动模块和一套统一的硬件抽象接口。不仅极大地简化了对存储器的操作，提高效率，而且也实现了上层软件的平台无关性，降低软件的开发复杂度，提高软件的可移植性和复用性。



图·存储管理

存储栈可以根据客户对数据的不同需求，提供对 NV（非易失性）数据的管理，包括存储、维护、读取、写入等功能。存储栈可以管理 EEPROM 和 FLASH EEPROM仿真设备的NV数据。

与存储栈相关的模块包括 NvM、MemIf、EA、EEP 等。

NvM 模块：提供队列机制缓存请求；使用 CRC 来检查数据一致性；在数据错误的情况下，提供不同的恢复机制；提供写保护功能等。

MemIf 模块：用于 NvM 统一调用存储接口的抽象，并能够灵活映射Fee或EA抽象层的非易失性存储单元的读取/写入/擦除等操作。

EA 模块：对设备特定地址结构和分段进行抽象，在不直接操作硬件的情况下对EEPROM进行逻辑块的划分。

EEP 模块：对底层 EEPROM 存储单元进行读取，写入，擦除等一系列操作，还可用于比较 EEPROM 中的数据块与内存 RAM 中的数据块；依赖于 SPI 通信。

产品特性：

(1) 遵循 AUTOSAR 4.2.2 标准

(2) 提供 NVM/MEMIF/FEE/FLS 和 NVM/MEMIF/EEA/EEP两条线的存储栈

(3) 模块功能可裁减

(4) 可根据客户需求定制开发

（四 ） 功能安全和信息安全

4.1 功能安全

在现代汽车领域中，各智能 ECU 模块广泛使用，给汽车行业带来巨大的变革。但由于设计中的缺失，以及开发过程中风险管理意识的不足，这些存在设计缺陷的 ECU流入车辆安全控制系统中，导致大量人员伤亡事故的发生。为此，车辆功能安全标准ISO 26262 越来越受到各车厂和零部件供应商的重视。

Certificate

Functional Safety

TÜVRheinland CERTIFIED

www.tuv.com
ID 0000000000

No.: 968/FSP 2053.00/20

Product tested	Real Time Operating System (RTOS)	**Certificate holder**	iSoft Infrastructure Software Co., Ltd. 12F No.448 Hongcao Rd., Xuhui District, Shanghai, 200233, P.R.China
Type designation	Safety ORIENTAIS OS for released and approved versions refer to the "Revision List"		
Codes and standards	ISO 26262-2:2018 (in extracts) ISO 26262-6:2018	ISO 26262-8:2018 (in extracts)	
Intended application	The Safety ORIENTAIS OS product complies with the requirements of the relevant standards (ASIL D according to ISO 26262) and can be used as a Safety Element Out of Content (SEooC) in terms in order to realize safety goals up to ASIL D according to ISO 26262. The configuration tool ORIENTAIS Studio satisfies the requirements for "Validation of the software tool" as a TCL 3 tool qualified according ISO 26262-8 clause 11.4.9 up to ASIL D when the rules described in the Tool User Manuals are observed. The user is responsible for applying and configuring appropriate protection mechanisms in order to guarantee interference freeness between applications, if necessary.		
Specific requirements	For the use of the Safety ORIENTAIS OS the operating conditions and functional characteristics, as specified in the Safety Manuals and the User Manuals provided by the manufacturer, need to be observed. The current versions of software are specified in the currently valid revision list, this is released by the manufacturer in cooperation with the Certification Body.		

Valid until 2025-05-25

The issue of this certificate is based upon an evaluation in accordance with the Certification Program CERT FSP2 V1.0:2017 in its actual version, whose results are documented in Report No. 968/FSP 2053.00/20 dated 2020-05-25. This certificate is valid only for products, which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2020-05-25

Certification Body Safety & Security for Automation & Grid

Dr.-Ing. Thorsten Gantevoort

www.fs-products.com
www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZE-11052-02-01

TÜVRheinland®
Precisely Right.

图 • ISO 26262 ASIL D功能安全认证证书

ISO 26262 功能安全要求的是从产品定义、软硬件开发、测试到生产的一个安全流程。而 AUTOSAR 是一个软件架构，因此，仅从产品软件方面来讲，AUTOSAR 的各种特性是最符合 ISO 26262 功能安全要求的软件架构。

普华 ORIENTAIS Classic AUTOSAR 基础软件对操作系统、WDG 等模块采用 ISO 26262 标准最高安全等级 ASIL D 进行设计开发。通过OS、E2Elib 和 WDG 提供相关功能安全机制来阻止和检测软件故障，确保 AUTOSAR 组件间“免受干扰”，实现整个 AUTOSAR 系统的功能安全。

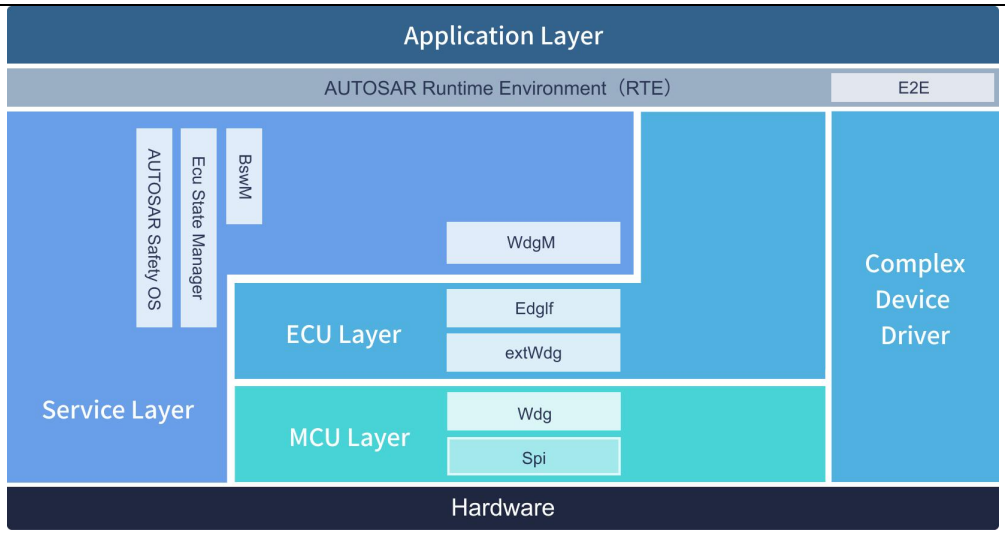


图 • 功能安全

4.1.1 E2E

E2E 的各个 profile 提供了一种可以满足功能安全目标的数据保护机制，各个E2E profile 通过不同的算法和 API 完成以下类型的数据保护机制：

(1) 集成CRC库的CRC保护机制

(2) 接收端检测接收报文的递增计数器，判断接收数据是否有序递增

(3) 接收端通过检测心跳计数器判断数据是否发生改变

(4) 通过特定的 ID 来区分不同的 I-PDU 组

(5) 超时检测机制（接收报文超时和发送确认超时）

(6)E2E profiles 的用户需要根据自己的应用场景决定选用哪种类型的 E2E profile

4.1.2 看门狗协议栈（Watchdog）

WDGM 是 AUTOSAR（服务层）的基本软件模块。它通过对程序执行时间和程序执行逻辑的监控，实现对程序故障的预警和复位，减少程序失控造成的损害。

AUTOSAR 的分层体系架构，将看门狗拆分为看门狗管理 (WDGM)，看门狗抽象（WdgIF）和看门狗驱动（WdgDriver）。

产品特性：

(1) 符合汽车电子领域能够从硬件看门狗实体的触发中监督程序执行

(2) 用于监督一个可配置数量的所谓监督实体的执行

(3) 当检测到对程序执行的已配置的时间和（或）逻辑约束的违反时，它需要许多可配置的操作来从失败中恢复

(4) 通过 WdgIf 模块和看门狗驱动模块为应用程序和监控硬件提供 API

(5) WdgIf 是允许 WdgM 管理多个看门狗硬件的设备抽象层

4.2 信息安全

随着车辆和 ECU 网络化和互联化程度的加深，对于车辆数据信息安全的需求在持续增加。以往的车辆总线通信传输的都是未经加密的数据，一旦被第三方侵入，便可直接读取车辆的关键数据，如转速、转向、刹车等信息，一旦被非法利用，后果不堪设想。在此背景下，AUTOSAR 引入了 SecOC（Secure Onboard Communication） 模块，SecOC 模块调用的加密算法由 crypto 协议栈提供。

普华 ORIENTAIS AUTOSAR Classic Platform基础软件提供基于AUTOSAR标准的安全通信和密码服务管理模块，以及基于硬件芯片和 / 或软件实现的国际主流密码算法和国密算法，满足客户的信息安全要求。

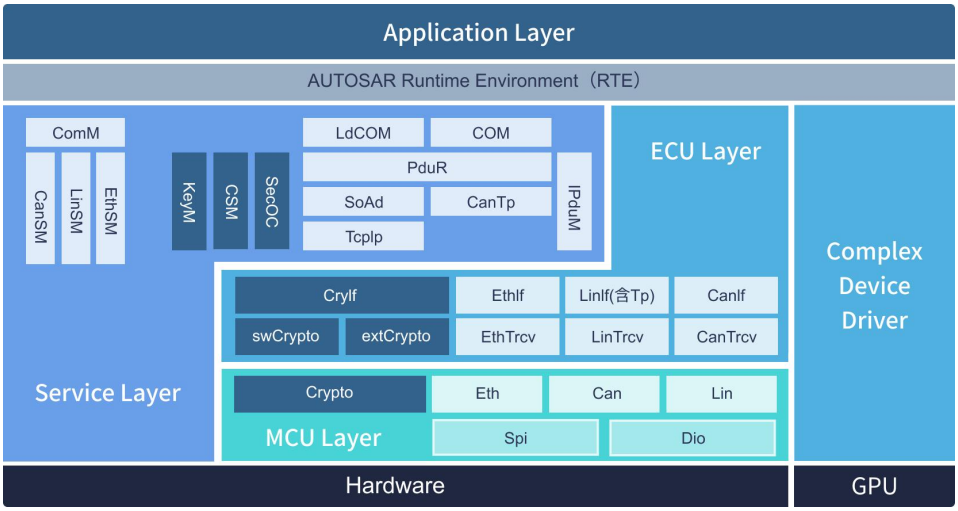


图 • 信息安全

4.2.1 Crypto 加密栈

基于不同应用场景的加密需求，需要 ECU 内部实现一套复杂的加密算法。一般的解决方案是通过软件实现一个算法库，需要涉及到加密和解密操作时便调用软件算法库中的相应算法，但是随着信息安全需求越来越高，算法复杂度越来越大，单纯的软件算法不能满足实时性的要求。芯片厂商为了解决这个问题，在 MCU 内集成了 Hardware Security Modules（HSM），负责对加密计算进行硬件加速。

Crypto 协议栈通过标准化的接口支持对软件和硬件加密算法的统一使用，主要包含 CSM、KeyM、CryIf、Crypto 等几个模块。

- CSM

CSM 主要功能是为用户提供统一的加密服务接口，对接上下层，负责管理所有的加密请求，并把加密请求传给 CryIf 进行加密处理。

- KeyM

Key Management，在Crypto栈中主要负责对秘钥和证书的管理和维护。主要用户为需要用到秘钥及证书的各种应用。它分为两部分：秘钥子模块和证书子模块。

秘钥子模块用于初始化、更新和维护 key 和 key element。有些加密算法需要秘钥才能够正常运行，KeyM 中秘钥子模块正是对秘钥的发放与撤销等权限进行管理。

证书子模块主要用于对证书的解析、发放与认证。证书子模块中引入了 PKI 规范，其核心为认证中心 CA ，CA 负责管理 PKI 结构下的所有用户 (包括各种应用程序) 的证书，把用户的公钥和用户的其他信息捆绑在一起，从而为用户身份认证提供基础。

- CryIf

CryIf 主要功能是连接 CSM 和 CryptoDriver，可通过 CryIf 支持多个CryptoDriver。

- Crypto

Crypto 主要功能是向上层提供各种加密算法，如（散列算法 SHA-256 、对称加密 AES、非对称加密 RSA 以及随机数生成等）。加密算法可通过软件或者硬件 HSM模块实现。

目前发布版本加密驱动主要指软件加密库，包含如下加密算法：

Aes128、RSA1024、Hash 1/256、CMAC-aes128、CTR-DRBG 以及密钥交换算法DH。

4.2.2 SECOC

SecOC 是对 PDU 级别数据进行保护。通过对敏感数据添加认证信息，对数据进行认证和完整性保护，用于防止非法篡改和重放攻击，SecOC 通过调用 CSM 提供加密手段，来对 PDU 进行保护。

（五）Bootloader

ECU 的开发周期较长，并且汽车电子产品开发对安全性、可靠性的指标要求很高，所以软件更新的情况在开发过程及售后都有可能出现。为了方便售后服务，同时避免对 ECU 硬件产品造成破坏，汽车行业按照各种标准采用专门的诊断测试设备，通过标准的通信接口对ECU控制程序或者数据进行更新。Bootloader 是为了完成上述功能，常驻在ECU内部Flash特定位置的程序。

作为常驻内存的软件组件，Bootloader 的主要功能是使得ECU具备了在线的可再编程能力。HIS Bootloader 主要是通过标准的通信接口对 ECU 进行再编程。HIS Bootloader 的软件设计基于 ISO 14229、ISO 15765-2、ISO 13400-2、HIS 标准、AUTOSAR标准等，从而与国内外整车厂自定义规范保持着较好的兼容性。

HIS Bootloader 产品特性：

(1) HIS Bootloader 提供丰富的数据集管理功能，便于实时掌握烧写流程的相关关键信息，以及版本检查

(2) HIS Bootloader 提供安全访问机制，确保被烧写对象不会受到外来设备的非法意外烧写

(3) 采用读取校验的方式，保证数据烧写的正确性和完整性

(4) 采用上电校验方式，保证运行数据的正确性和完整性

(5) 允许单独更新部分程序或数据，以逻辑块为最小单位的可编程单元，可单独更新某个逻辑块。支持跨物理 gap 的烧写，同一个逻辑块中，支持非连续烧写序列

（六）时间同步

时间同步功能为应用程序提供了基于硬件时钟的时间同步管理功能，它用于记录和处理各应用之间由于硬件或通信等因素产生的时间误差，并通过此误差使各应用的时间与同一个作为标准的主时间同步。时间同步功能包括 StbM、EthTSyn、CanTSyn 等三个模块。

StbM：Synchronized Time-Base Manager 同步时间基管理

EthTSyn：TimeSyncOverEthernet 以太网时间同步模块

CanTSyn：TimeSyncOverCAN CAN 时间同步模块

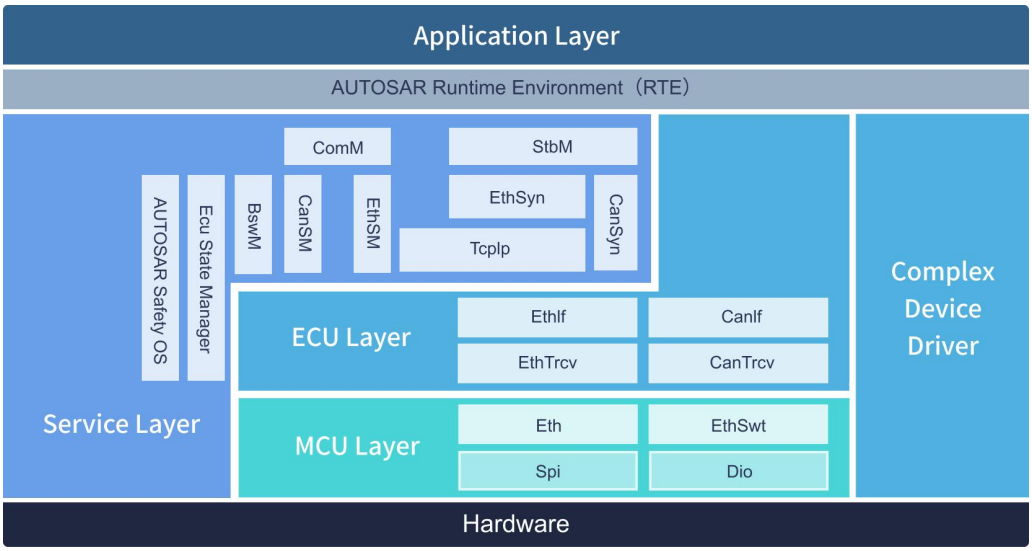


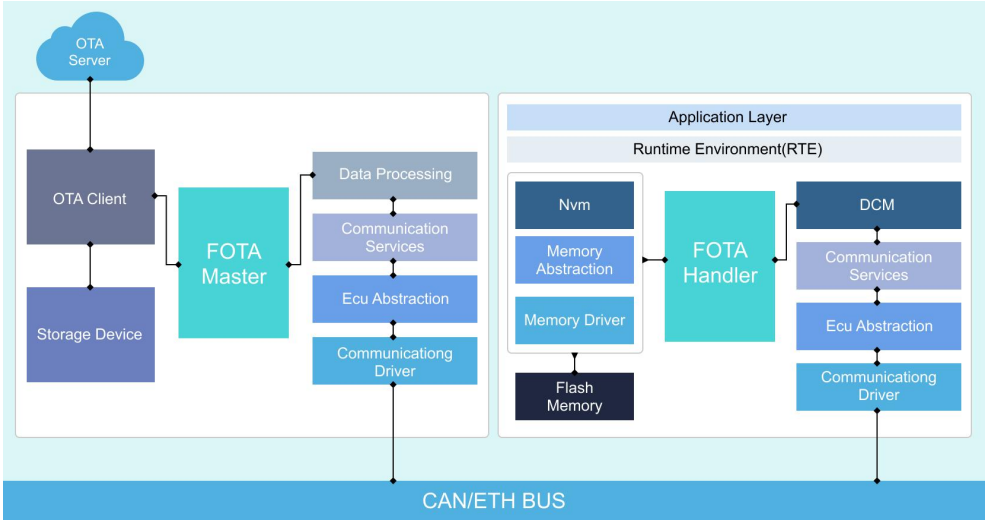
图 • 时间同步

(1) StbM 从GPT和EthTSyn或OS获取本地时间。从节点通过CanTSyn和EthTSyn 获得全局时间并根据配置通过偏移修正或速率修正的方式校正时间基，供应用获取；而 StbM 的主节点通过上层应用获取全局时间，供应用以及CanTSyn，EthTsyn 获取从而传递给从节点主节点的全局时间。

(2) EthTSyn 和 CanTSyn 主节点根据配置来从不同的时间来源获取时间，例如硬件时钟，主节点的 StbM 等，发送给子节点后，子节点计算在总线上传输时会产生的误差，并将计算好的时间传给自己的 StbM 设置新的时间组。

(3) 此外，StbM 还包括时间记录和定时器的功能。

（七）FOTA 解决方案



图·FOTA解决方案

FOTA（Firmware Over-The-Air）主要解决的是 ECU 脱产程序更新的问题，以及作为车载终端对车上其他 ECU 发起程序刷写的操作。完整的车端 FOTA 协议栈包含的功能模块有 FOTA Master，FOTA Handler，以及相关的通信栈、诊断栈、存储栈、信息安全栈等。通讯栈用于刷写数据流在不同通信总线上的重组与分片。存储栈主要是将下载的刷写数据写入非易失存储设备中，并对数据读写进行管理。诊断栈用于刷写流程中诊断服务请求的响应和处理。

FOTA Master 作为客户端主动发起刷写操作，用于刷写整车中其他 ECU 节点，FOTA Master 可同时对多个 ECU 发起刷写请求，每个请求的刷写流程可以单独配置；针对刷写过程可能出现的异常，FOTA Master 可以根据接收到的状态信息发起回滚操作。

FOTA Handler 作为被刷 ECU 流程控制单元，主要实现对刷写请求的响应、刷写数据的流程管理和存储等操作。被刷端的 ECU 存储空间提供了至少 2 个分区用于应用程序切换，处于活动状态的分区将更新数据流下载到备选的非活动区域；下载完成且校验通过后，根据用户选择完成启动时分区切换，从而实现“不停车升级”，下载流程因条件不满足的中断，支持掉电或复位后从上次中断点继续进行下载，避免了流程的反复重新开始。

本项目发布的内容仅包含 FOTA Handler。

三、集成开发环境

ORIENTAIS Studio 集成开发环境提供全套基础软件平台开发工具链，提供SWC的配置、DBC文件的导入、ECU系统描述的萃取和 RTE配置与代码的生成等功能。可配置的基础软件模块包括：操作系统、通信/网络管理、诊断、RTE 等；开发环境集成了代码编写及配置过程，支持代码自动生成，实现了软件组件之间的无缝集成。ORIENTAIS Studio集成开发环境帮助用户使用界面友好的工具配置方式取代繁琐的手工配置方式，不仅使开发变得更加轻松有效，而且极大的缩短了开发周期。

产品特性：

(1) 基于 Eclipse 开放架构，插件化开发，可扩展性强，兼容性强，软件体系成熟

(2) 基于 Artop 基础软件架构，全面支持 AUTOSAR

(3) 提供 SWC 设计的功能

(4) 支持对 DBC 文件的导入功能

(5) 支持对 ODX 文件的导入功能

(6) 支持对 LDF 文件的导入功能

(7) 支持对 ECU Extract ARXML 文件的导入功能

(8) 支持第三方 MCAL 配置 ARXML 导入功能，以此完成与第三方 MCAL 工具集成的工作

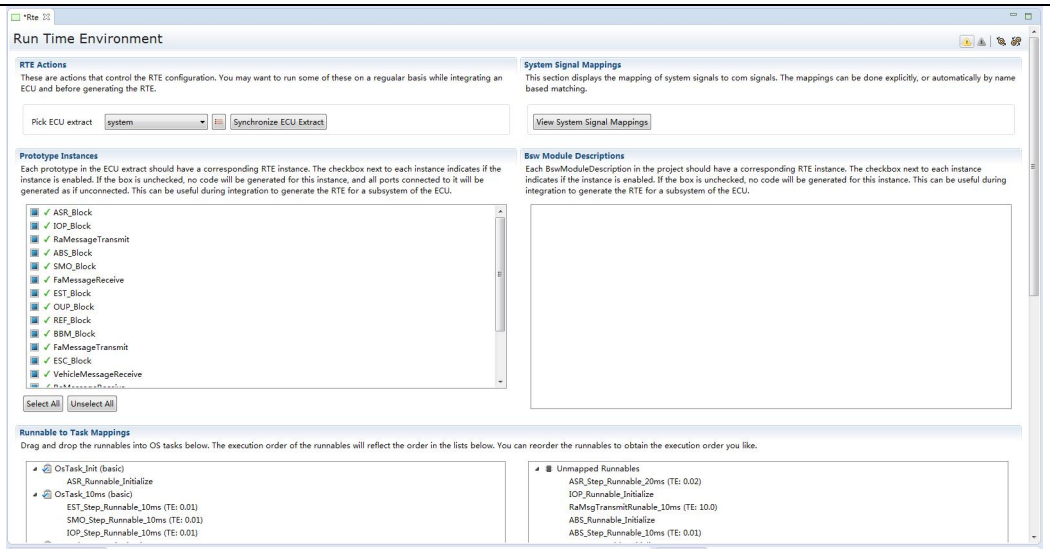
(9) 支持配置数据的一致性校验

(10) 产品级的自动代码生成

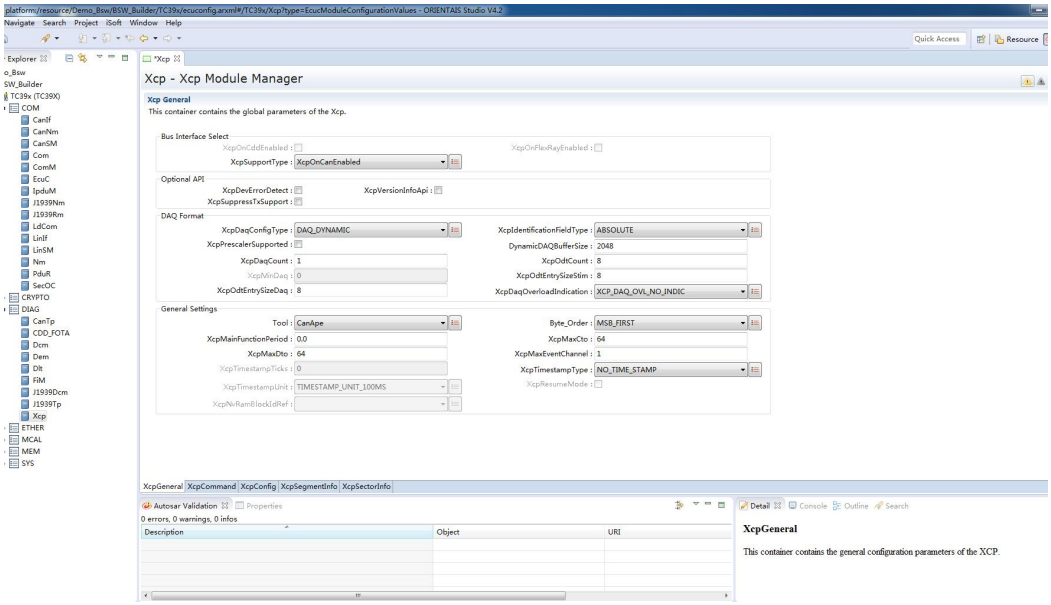
(11) 可以根据客户需要灵活配置和裁减功能组件

(12) 强大的错误检查和提示纠正机制

(13) 可跨平台运行



图·ORIENTAIS RTE Configurator/Generator



图·ORIENTAIS BSW Configurator/Generator

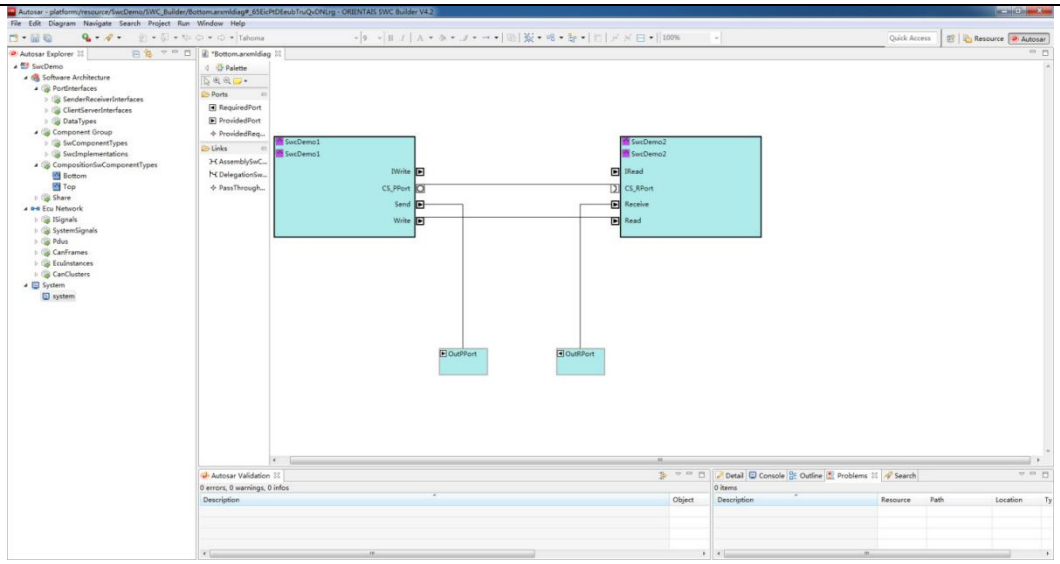


图 • ORIENTAIS SWC Builder

附录

缩写	英文全称	中文介绍
PDU	Prototcol Data Unit	协议数据单元
IPDU	Interaction Protocol Data Unit	交互层协议数据单元
ASW	Application Software, comprising any number o f SWCs and/or Compositions	应用软件
SWC	SoftWare Component (or component, for short),the‘smallest’application software entity in AUTOSAR	软件组件
RE	Runnable Entity, containing executable code of SWCs	可运行实体
Composition	Means to create hierarchies within the ASW. Compositions may contain anynumber of SWCs, and possibly other compositions also	部件
RTE	Run-Time Environment	运行环境
BSW	Basic Software	基础软件
OS	Operating System	操作系统
CDD	Complex Device Driver	复杂驱动
MCAL	Micro-Controller Abstraction Layer	微控制抽象层
DBC	DataBase for CAN	Can 数据描述文件
LDF	LIN Description File	Lin 描述文件

我们的愿景

让汽车软件开发变得简单

我们的使命

为软件定义汽车提供最好的服务

CETC

普华基础软件

ORIENTAIS®