Manual de AUTOSAR

KPIT Technologies Ltd.

Traducido por Aldo Núñez Tovar
Versión: 0.1

15 de julio de 2024

Índice general

1. Introducción a AUTOSAR **5**
1.1. AUTOSAR . . . 5
1.2. Modelo de capas AUTOSAR . . . 6
1.3. Diseño y comunicación de componentes de software . . . 7
1.4. Método AUTOSAR . . . 8
1.5. Interfaces AUTOSAR . . . 8
1.6. Módulo de software básico AUTOSAR . . . 8

2. Descripción de AUTOSAR, productos y actividades del trabajo **10**

3. Descripción de AUTOSAR. Módulo del Software Básico (BSW) **12**

4. Servicios del Sistema AUTOSAR **16**
4.1. Sistema Operativo AUTOSAR . . . 16

5. Soporte multinúcleo **22**
5.1. Introducción: . . . 22

6. Seguridad funcional **24**
6.0.1. Introducción: . . . 24
6.1. Implementación de la arquitectura y la seguridad en AUTOSAR en R4.0: . . . 24

7. Cadena de Herramientas del Editor K-SAR **28**
7.0.1. Introducción . . . 28
7.1. Entradas utilizadas: . . . 29
7.2. Características del Editor K-SAR . . . 31
7.3. Términos utilizados . . . 32

8. Acerca de KPIT **33**
8.1. Experiencia en KPIT AUTOSAR . . . 33
8.2. Ventajas de KPIT . . . 33
8.3. Servicios/Productos de Software Proporcionados por KPIT . . . 36

Glosario

ADC Analog to Digital Converter - Convertidor Análogo/Digital. 15, 20

ALU Arithmetic Logic Unit. 21

API Application Programming Interface. 8

ASIL Automotive Safety Integrity Levels. 27

AUTOSAR **Aut**omotive **O**pen **S**ystem **AR**chitecture. 4–8, 16, 20, 21, 24, 29, 33, 34

BOM Bill of Material. 33

BSW Basic Software. 6–9, 11, 15, 19, 33

CAN Controller Area Network. 8, 20

CANNM CAN Network Management. 14

CRC Cyclic Redundancy Check. 19, 26

CSV Comma-separated values. 29

DBC CAN Database. 31

DCM Diagnostic Communication Manager. 14

DEM Diagnostic Event Manager. 18

DIO Digital Input/Output. 15, 20

E-Gas Electronic Gas Pedal. 24

E2E End-to-End. 25, 26

EA EEPROM Abstraction. 15

ECU Engine Control Unit. 6–8, 11, 13–16, 18, 20, 21, 28, 29, 31–33

EEPROM Electrically Erasable Programmable Read-Only Memory. 15, 20

EMI Electromagnetic Interference. 26

FEE Flash EEPROM Emulation. 15

Fibex Field Bus EXchange. 31

FlexRay FlexRay, es un protocolo de comunicaciones para buses de datos en el automóvil desarrollado por el consorcio FlexRay. 13, 20, 24

FLS Flash Driver. 15

FLSEXT External Flash Driver. 15

FRNM Flex Ray Network Management. 14

HTML HyperText Markup Language. 31

HW Hardware. 8, 25, 26

ICU Input Capture Unit. 20

IOC Inter OsApplication Communication. 25

LDF Log Database File. 31

LIN Local Interconnect Network. 8, 14, 20

LINIF LIN InterFace. 14

LINTP LIN Transport Protocol. 14

LINTRCV LIN Transceiver Driver. 14

MCAL Microcontroller Abstraction Layer. 19, 33

MCU Microcontroller Unit. 21

MMU Memory Management Unit. 16

MPU Memory Protection Unit. 16, 24

MRU Most Recently Used. 31

NVRAM Non-volatile Random Access Memory. 15, 18

ODM Original Design Manufacturer. 4

OEM Original Equipment Manufacturer. 4, 5

OS Operating System. 8, 18, 24, 25

PDU Protocol Data Unit. 14

PLL Phase Locked Loop. 21

PWM Pulse Width Modulation. 15, 20

RAM Random Access Memory. 20, 21

RTE Run Time Environment. 6–8, 11, 15, 18, 19, 25, 31

RTOS Real Time Operative System. 16

SCHM Scheduler Module. 19

SPI Serial Peripheral Interface. 20

SW Software. 18, 25

SWC Application Software Component. 6–8, 11, 15, 18, 24–27

Tier1 Tier1 se refiere a los proveedores que proporcionan componentes y sistemas críticos directamente a los OEM. Estos proveedores de nivel 1 desempeñan un papel vital en la cadena de suministro automotriz, particularmente en la implementación de estándares AUTOSAR dentro de sus productos. 4

TTM Time to Market. 34

UDS Unified Diagnostic Services. 14

VFB Virtual Functional Bus. 7

WDGEXT External Watchdog Hardware. 15

XML eXtensible Markup Language. 8, 9, 29

SOLUCIONES AUTOSAR

Miembro Premium del consorcio AUTOSAR desde 2005, KPIT provee productos y servicios para las distintas capas de la pila AUTOSAR para OEMs, Tier1 y ODM de semiconductores (Fabricantes de Diseño Original). Participamos activamente en la estandarización automotriz en todo el mundo y ayudamos a los clientes en cada etapa de su desarrollo AUTOSAR a lo largo de toda la cadena de herramientas AUTOSAR en asociación con proveedores de herramientas líderes de la industria.

CAPÍTULO 1
Introducción a AUTOSAR

1.1 AUTOSAR

La industria automotriz se enfrenta a una complejidad cada vez mayor
Los sistemas de los vehículos son cada día más complejos. Actualmente, el proceso de desarrollo basado en hardware y componentes se orienta cada vez más a los requisitos y funcionalidades. La ingeniería del futuro no pretende optimizar componentes individuales sino optimizar a nivel de sistema, para lo cual requiere una arquitectura abierta así como módulos de software escalables e intercambiables.
AUTOSAR (AUTomotive Open System ARchitecture), es un consorcio mundial de OEMs, proveedores y otras empresas, fundado en 2003, ha estado trabajando en el desarrollo y la introducción de una arquitectura de software abierta y estandarizada para la industria automotriz.
Reducir el esfuerzo de desarrollo y mejorar la calidad son razones importantes para introducir un procedimiento uniforme independiente de la plataforma del sistema. El hardware y el software están desacoplados entre sí para garantizar dichos resultados.
El concepto AUTOSAR se basa en componentes modulares con interfaces definidas.

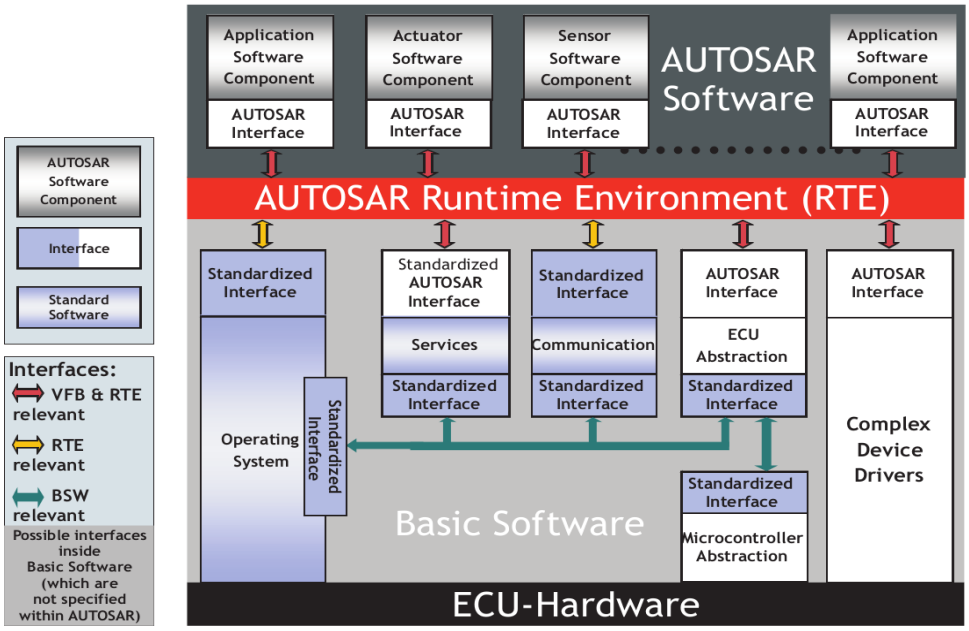


Figura 1.1: **Vista de componentes simplificada**

1.2 MODELO DE CAPAS AUTOSAR

En AUTOSAR, el software de la ECU se abstrae y se subclasifica como capa de software (BSW), capa de entorno de Ejecución (RTE) y capa de aplicación.

La Capa de Abstracción del Microcontrolador contiene controladores internos, que son módulos de software con acceso directo al microcontrolador y a los periféricos internos.

La Capa de Abstracción de la ECU ofrece acceso uniforme a todas las funciones de una ECU, tales como las comunicaciones, la memoria o las E/S, sin importar si estas funciones son parte del microcontrolador o se realizan mediante componentes periféricos. Los controladores para dichos componentes periféricos externos residen en esta capa.

La Capa de Servicio provee varios tipos de servicios en segundo plano, como servicios de administración y comunicación en red de vehículos, servicios de diagnóstico, administración de memoria, administración del estado de la ECU, administración de modos y supervisión del flujo de programas lógicos y temporales. El sistema operativo también forma parte de esta capa.

El **RTE** integra la capa de aplicación con el BSW. Implementa el intercambio de datos y controla la integración entre el componente de software de aplicación (SWC) y el BSW.

La **Capa de Aplicación** contiene los SWCs, que realizan la funcionalidad de la aplicación de la ECU.

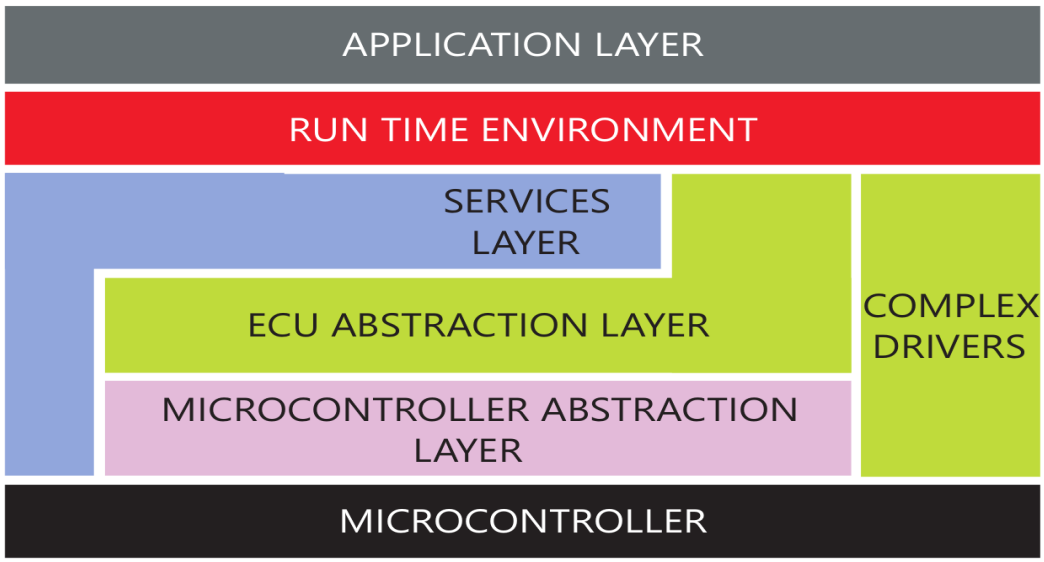


Figura 1.2: **Arquitectura de capas de AUTOSAR**

1.3 DISEÑO Y COMUNICACIÓN DE COMPONENTES DE SOFTWARE

Un concepto de diseño fundamental de AUTOSAR es la separación entre Aplicación e Infraestructura. Una aplicación en AUTOSAR consta de “componentes de software de AUTOSAR” interconectados. Las interfaces de cada SWC (componente de sofware) están formalmente definidas. La comunicación entre los SWCs se produce principalmente a través de dos tipos de puertos, **puertos Cliente/Servidor** donde el servidor es un proveedor de un servicio y el cliente es un usuario de un servicio y **puertos Remitente/-Receptor** donde un remitente distribuye información a uno o varios receptores en entornos síncronos y asíncronos. La implementación arquitectónica del SWC se define formalmente en términos de las llamadas entidades ejecutables. Ellas corresponden a procedimientos y se ejecutan en un evento específico, como una activación periódica o la recepción de un nuevo valor de entrada. Durante la fase de diseño del sistema, los SWCs se pueden integrar con su entorno (por ejemplo, el hardware, el controlador, el sistema operativo, etc) basado en **Bus Funcional Virtual (VFB)**. El bus funcional virtual es la abstracción de las Interconexiones de Componentes de Software de AUTOSAR de todo el vehículo.
Una vez que el sistema de los SWCs se despliega en una determinada arquitectura de red de vehículos, el RTE y el BSW de las ECUs involucradas realizan la comunicación entre el SWC ya sea como comunicación ECU-local o como comunicación basada en red.

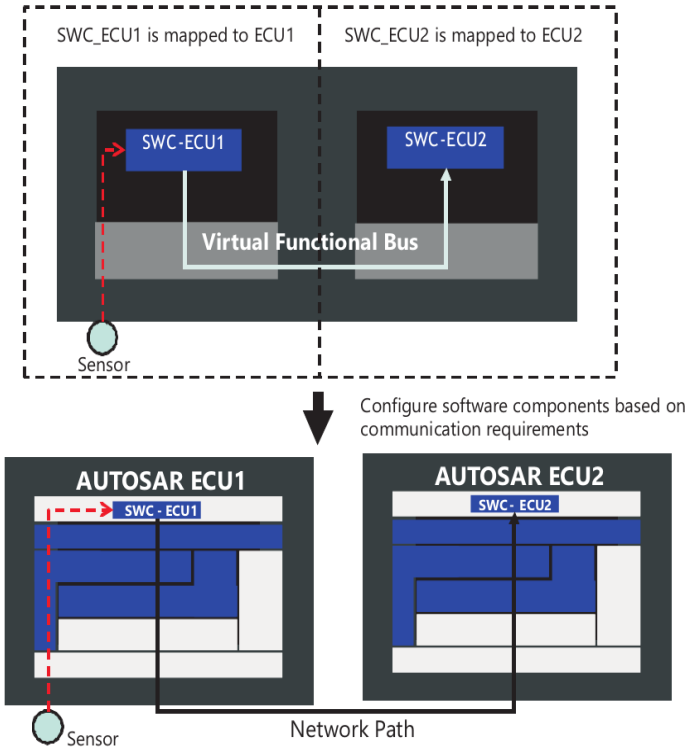


Figura 1.3: **AUTOSAR system design**

1.4 MÉTODO AUTOSAR

Los Métodos AUTOSAR (en las especificaciones AUTOSAR también llamado “Metodología”) describen el flujo de trabajo que podría seguirse, desde la configuración del sistema hasta la generación final de un ejecutable para una determinada ECU.
Las actividades están respaldadas por herramientas AUTOSAR dedicadas.
Para intercambiar productos de trabajo entre dichas herramientas, AUTOSAR definió un archivo detallado en formato XML.
Para obtener una descripción detallada del flujo de trabajo de AUTOSAR, consulte la Parte 2, del manual Descripción de AUTOSAR, productos de trabajo y activaciones.

1.5 INTERFACES AUTOSAR

Las interfaces AUTOSAR se utilizan para definir los puertos de los componentes de software y/o módulos BSW. A través de estos puertos, los componentes de software y/o módulos BSW pueden comunicarse entre sí (Enviar o recibir información o invocar servicios). AUTOSAR permite implementar esta comunicación entre Componentes de Software y/o módulos BSW ya sea localmente o a través de una red. (Consulte la figura 1, página 3 del manual)

- La **Interfaz AUTOSAR** es una interfaz genérica que se deriva de los puertos de un SWC. El RTE es el encargado de proveer las interfaces AUTOSAR y sirven como interfaz entre los SWCs o entre un SWC y el firmware de la ECU (IO HW (Input/Output) y Controladores Complejos). Mediante estas interfaces, un SWC puede leer un valor de entrada o escribir un valor de salida.
- La **Interfaz AUTOSAR estandarizada** es una Interfaz AUTOSAR particular, que ya está predefinida por el estándar AUTOSAR. Los SWCs utilizan dichas interfaces para acceder a los Servicios AUTOSAR, que son suministrados por los módulos BSW de la Capa de Servicio, como el administrador de ECU o el administrador de eventos de diagnóstico.
- La **Interfaz Estandarizada** es una interfaz predefinida por el estándar AUTOSAR como una API en lenguaje C. Se utiliza entre el módulo BSW dentro de una ECU, entre el RTE y el sistema operativo (OS), o entre el RTE y la capa de comunicación.

1.6 MÓDULO DE SOFTWARE BÁSICO AUTOSAR

AUTOSAR ha definido un conjunto de módulos BSW. Estos son responsables de diferentes tareas:

- Sistema operativo
- Acceso a memoria no volátil
- Comunicación vía CAN, LIN, FlexRay y Ethernet
- Manejo de diagnósticos
- Acceso a puertos de E/S
- Servicios del sistema como el administrador del estado de la ECU.

Además, se pueden integrar los llamados Controladores de Dispositivos Complejos dentro de una ECU AUTOSAR. Estos se utilizan para acceder a las funciones de la ECU que no están cubiertas por el estándar BSW de AUTOSAR. Se incluye la descripción detallada de los parámetros del módulo BSW en un archivo

XML específico del módulo: la Descripción del módulo BSW (compárese con la Figura 4 y la tabla en la parte 2 de este manual). Puede encontrar una lista de todos los módulos de BSW y una breve descripción en la parte 3 de este manual.

CAPÍTULO 2

Descripción de AUTOSAR, productos y actividades del trabajo

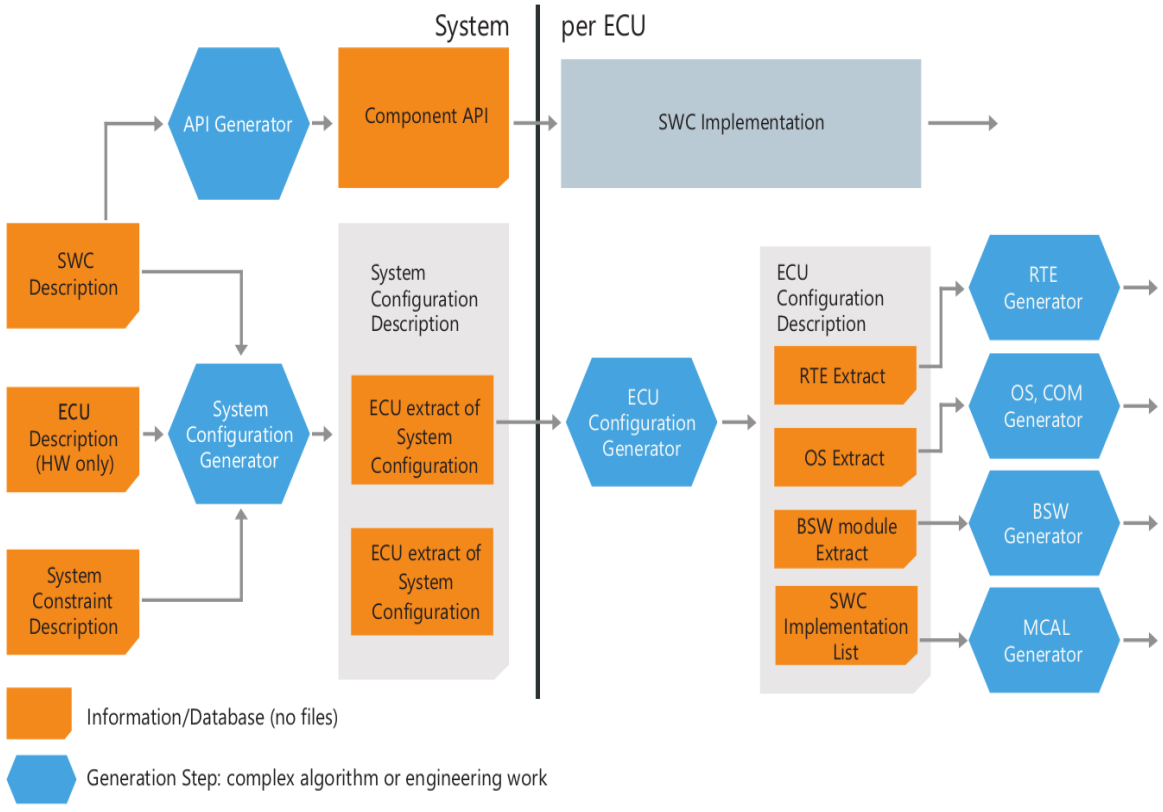


Figura 2.1: **Descripción general del método AUTOSAR**

Información / actividades	**Descripción**
Restricciones del sistema	Estas son restricciones que deben considerarse durante la configuración del sistema. Un ejemplo de tales Restricciones del Sistema es una matriz de comunicación determinada (parcial) de la última serie de vehículos, que no debe cambiarse al diseñar la nueva serie de vehículos.
Generador de la Configuración del Sistema	Esta actividad crea una Descripción del Sistema completa junto con la Descripción del SWC requerida y la Matriz de Comunicación del sistema asociado. Además, esta actividad requiere la toma de decisiones de diseño a nivel del sistema tomando en consideración la ECU y los recursos de red disponibles. Esto incluye la definición de la topología de la red, la definición del mapeo del SWC a las ECUs y la especificación de la comunicación de red.
Descripción de la Configuración del Sistema	Esto incluye toda la información del sistema y la información que debe acordarse entre diferentes ECUs, incluida la topología de la red y la asignación de los componentes a las ECUs. Una Descripción del Sistema siempre se completa con las Descripciones del SWC necesarias y una Matriz del Sistema de Comunicación asociado.
Descripción del SWC	Esta especifica la información sobre un SWC, incluyendo sus puertos y entidades ejecutables.

Información / actividades	**Descripción**
Extracción de la ECU de la Configuración del Sistema	El resultado de este trabajo contiene la información necesaria de la ECU específica a partir de la Descripción de la Configuración del Sistema. Este incluye la descripción de los SWCs acerca de esta ECU, así como el subconjunto de la matriz de comunicación relevante para la ECU.
Generador de la configuración de la ECU	Esto crea una descripción de la configuración de la ECU. La base es el extracto de la ECU y la descripción del módulo BSW específica del proveedor. Además, esta actividad requiere que las decisiones de diseño se tomen a nivel de la ECU. Esto incluye establecer valores para los parámetros configurables de todos los módulos BSW y el RTE, como el mapeo de entidades ejecutables a tareas del sistema operativo, definir el diseño de la memoria o configurar el sistema operativo.
Descripción de la Configuración la ECU	Esta describe toda la información local de una ECU específica; el software ejecutable se puede crear a partir de esta información y el código del componente de software.
Generador del BSW	Esta actividad genera la parte configurable del módulo BSW de una ECU. La Descripción de la configuración de la ECU es la base para este proceso de generación de la ECU. Esta actividad no requiere decisiones de diseño.
Extracción del BSW de la configuración de la ECU	Esta describe todos los parámetros de configuración de un módulo BSW particular, incluye los parámetros específicos del proveedor. Esta descripción siempre refleja una implementación concreta del módulo BSW. Por lo tanto, el proveedor del módulo BSW lo proporciona y no se cambia durante el proceso de configuración de la ECU.
Generador del RTE	Esta actividad genera el RTE de una ECU. Esta actividad no requiere decisiones de diseño.

CAPÍTULO 3

Descripción de AUTOSAR. Módulo del Software Básico (BSW)

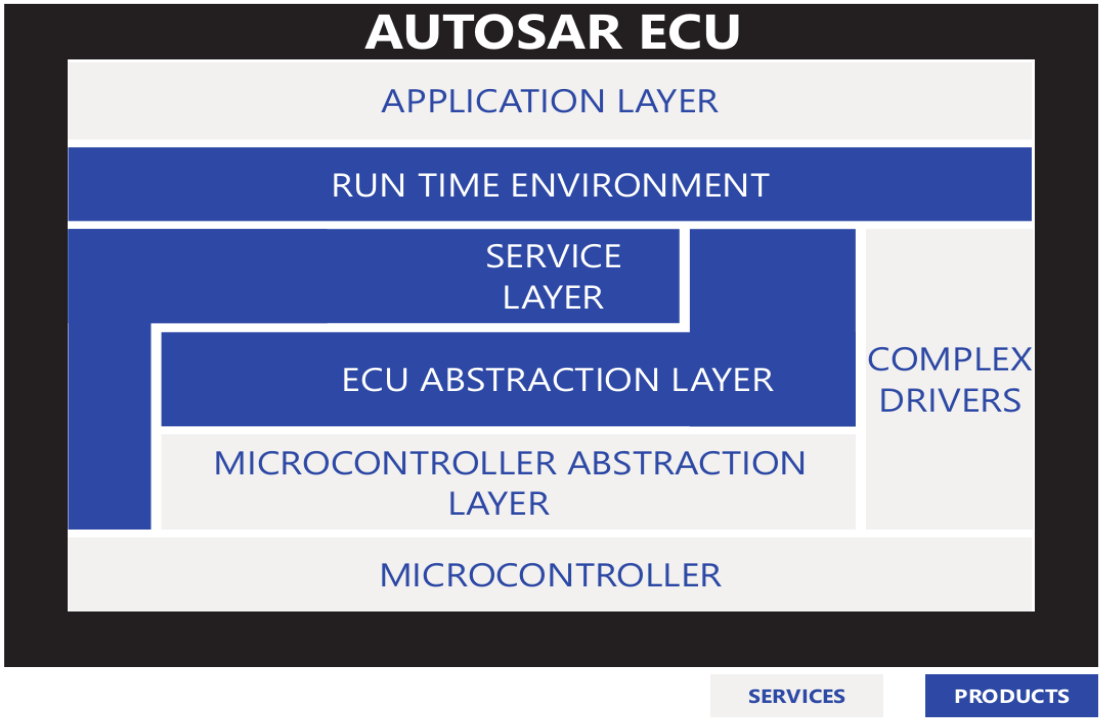


Figura 3.1: **Pila de AUTOSAR y Propuestas de KPIT**

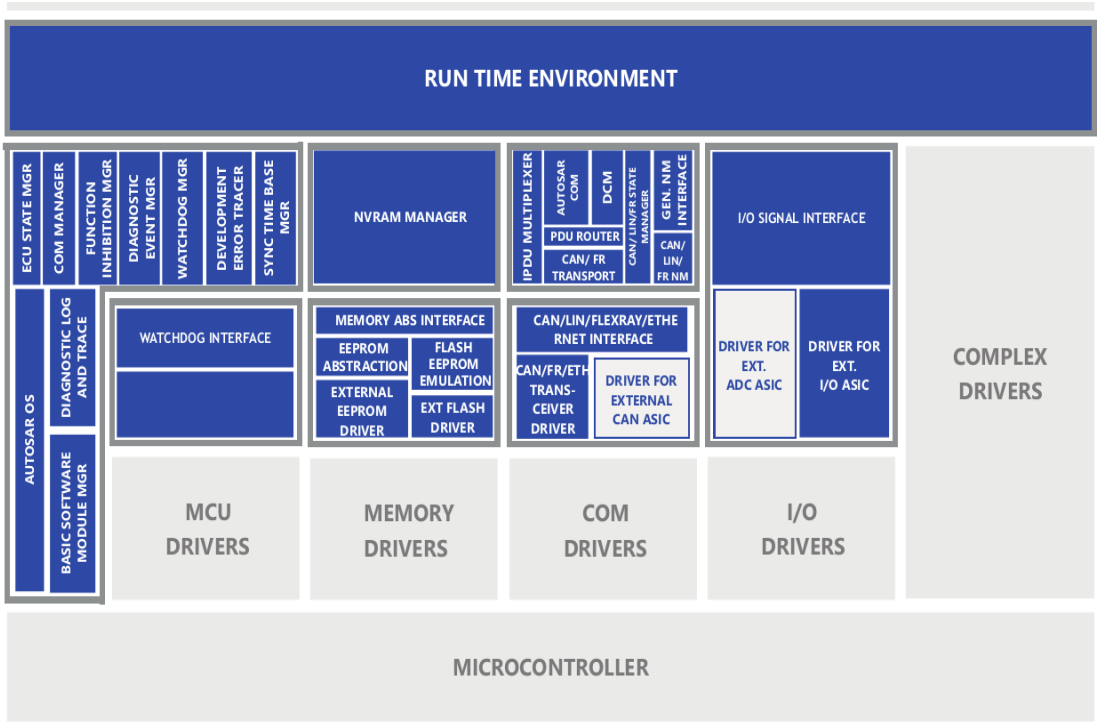


Figura 3.2: **Módulos BSW (no se muestran todos los módulos)**

Nombre del Módulo	Descripción
Interfaz FlexRay	La interfaz FlexRay provee mecanismos de acceso idénticos para los canales FlexRay de las ECUs, independientes de su implementación (microcontrolador interno o externo). Extrae el número de controladores FlexRay y administra la sincronización con el tiempo global de FlexRay.
Administrador de la Red FlexRay	Este módulo es responsable de la administración de la red FlexRay. Coordina la transición entre la operación normal y el modo de inactividad del bus de la red.
Administrador de Estados de FlexRay	El Administrador de Estados de la Red FlexRay controla y monitoriza la actividad y el inicio del nodo en el clúster FlexRay.
Capa de Transporte de FlexRay	El protocolo de transporte FlexRay segmenta los paquetes de datos largos en la dirección de transmisión, recopila datos en la dirección de recepción y controla el flujo de datos. Se detectan errores como pérdida de mensajes, duplicación de mensajes o errores de secuenciación.
Controlador del Transceptor de FlexRay	El controlador para un transceptor FlexRay externo es responsable del diagnóstico de la Red y del encendido y apagado de un transceptor.

Nombre del Módulo	Descripción
Interfaz LIN	La interfaz LIN provee una interfaz independiente del hardware para el acceso a las tramas LIN. Además, administra el procesamiento de la Tabla de Planificación y la implementación de la Capa de Transporte LIN y la Administración de la Red LIN.
Administración de la Red LIN	Este módulo es responsable de la administración de la red LIN. Coordina la transición entre la operación normal y el modo inactivo del bus de la red.
Administrador de Estados de la Red LIN	El Administrador de Estados de la Red LIN cambia las tablas de planificación, así como los grupos PDU en COM y los servidores de la interfaz LIN en términos de inactividad y actividad. Además, administra la activación del controlador del Transceptor LIN.
Capa de Transporte de la Red LIN	Los segmentos de datos del protocolo de transporte LIN en la dirección de transmisión, recopilan datos en la dirección de recepción y controlan el flujo de datos. Se detectan errores como pérdida de mensajes, duplicación de mensajes o errores de secuenciación. El LINTP es parte del LINIF.
Controlador de Transceptor LIN	El controlador LINTRCV para un transceptor LIN externo es responsable de monitorizar y controlar las funciones de actividad e inactividad.

Nombre del Módulo	Descripción
Interfaz Ethernet	Este módulo provee a las capas superiores a una interfaz independiente del hardware para el sistema de comunicación Ethernet que comprende múltiples controladores y transceptores Ethernet diferentes. Esta interfaz es uniforme para todos los controladores y transceptores Ethernet. De este modo, las capas superiores (Protocolo de Internet, Protocolo de resolución de direcciones) pueden acceder al sistema de bus subyacente de manera uniforme.
Controlador del transceptor Ethernet	El módulo provee a la capa superior (interfaz Ethernet) una interfaz independiente del hardware que comprende múltiples transceptores iguales. Esta interfaz es uniforme para todos los transceptores. De este modo, la capa superior (interfaz Ethernet) puede acceder al sistema de bus subyacente de manera uniforme. Sin embargo, la configuración del controlador del transceptor Ethernet es específica del bus, ya que tome en cuenta las características específicas del transceptor de comunicación.
Administrador de Estados Ethernet	El Administrador de Estados Ethernet proporcionará una interfaz abstracta al Administrador de Comunicaciones AUTOSAR para iniciar o apagar la comunicación en un clúster de Ethernet. No accede directamente al hardware Ethernet.

Nombre del Módulo	Descripción
Interfaz para la Administración de una Red Genérica	El módulo NM provee una interfaz general independiente de la red para acceder a los módulos de Administración de Red dependientes del bus (CANNM y FRNM). Además, el módulo administra el apagado síncrono entre redes del sistema de comunicación junto con otras ECUs.
Comunicación	La capa de comunicación provee una interfaz de datos basada en señales para la aplicación y manda mensajes según los tipos de envío definidos. Se proveen interfaces adicionales en forma de mecanismos de mensajería para el envío y recepción exitosos de datos, así como sus tiempos de espera . Para ECUs multicanal, el módulo COM también provee una opción para enrutar señales entre buses de comunicación (puerta de enlace de señales)
Administrador de Comunicación de Diagnóstico	Este módulo implementa comunicación de diagnóstico según ISO14229-1 (UDS). Las solicitudes de diagnóstico directamente se convierten en parte en el DCM (administración de sesiones de diagnóstico, lectura de códigos de error, EcuReset,...), y en parte se envían a componentes de software a través de interfaces de puerto (lectura, escritura y el control de identificadores de datos, ejecución de rutinas,...).

Nombre del Módulo	Descripción
Multiplexor IPDU	Este módulo trata sobre usos múltiples de PDU fijas con diferentes contenidos de datos.
Abstracción EEPROM	El módulo EA provee una interfaz independiente del hardware para acceder al controlador del EEPROM (EEP). Los bloques de datos se pueden leer, escribir o borrar. Además, el módulo EA distribuye la solicitud de escritura en diferentes áreas de la EEPROM para que todas las celdas de la EEPROM estén sujetas a la misma carga y su vida útil aumente.
Emulación de la Flash EEPROM	El módulo FEE provee una interfaz independiente del hardware para acceder a datos de la flash mediante un controlador flash (FLS). Los bloques de datos se pueden leer, escribir o borrar. Además, el módulo FEE distribuye las solicitudes de escritura en diferentes áreas de la memoria flash para que todas las celdas de la memoria flash tengan la misma carga y su vida útil aumente.
Interfaz de Abstracción de Memoria	Este módulo permite al administrador NVRAM acceder a varios módulos de abstracción de memoria (módulos FEE o EA). Este módulo se abstrae del número de módulos FEE o EA subyacentes y provee capas superiores con una segmentación virtual en un espacio de direcciones lineal uniforme.

Nombre del Módulo	Descripción
Controlador Externo	A solicitud, ofrecemos la implementación de controladores para componentes conectados externamente como una extensión de AUTOSAR 3.0. Estos ya están disponibles para el control de determinadas EEPROM (EEPEXT), por ejemplo: componentes flash (FLSEXT), Watchdog (WDGEXT),...
Interfaz del Watchdog	Este módulo provee acceso uniforme a los servicios del controlador del Watchdog (WDG), como el cambio de modos y el disparo.
Administrador del Watchdog	El Administrador del Watchdog monitoriza la confiabilidad y la seguridad funcional de la aplicación en una ECU. Esto incluye monitorizar la correcta ejecución de los módulos SWC y BSW, y la activación del Watchdog en los intervalos de tiempo requeridos. Reacciona ante posibles comportamientos incorrectos en numerosos niveles de recrudecimiento. Cuando es imposible reanudar la operación normal, el hardware Watchdog realiza un reset al microcontrolador.
Abstracción del Hardware de E/S	La abstracción de Hardware de E/S representa la conexión entre el RTE y los canales de E/S de la ECU. Encapsula el acceso a los controladores de E/S como el ADC, DIO o PWM, poniendo así a disposición las señales de E/S de la ECU.

CAPÍTULO 4

Servicios del Sistema AUTOSAR

4.1 SISTEMA OPERATIVO AUTOSAR

Este módulo es el sistema operativo de una ECU AUTOSAR. En realidad, es un sistema operativo OSEK extendido. Las extensiones están organizadas en las llamadas clases de escalabilidad (SC1-SC4). Estas cubren las siguientes características:

- **SC1:** La referencia es el RTOS determinista (tareas, eventos, contadores, alarmas, mensajes)
- **SC1:** Determinismo de tareas basado en el tiempo (baja latencia, tiempo preciso para tareas periódicas)
- **SC3** La protección de memoria (MMU/MPU) en tareas evita colisiones de memoria por seguridad.
- **SC4** Tareas temporales y de memoria protegidas, se utilizan todas las capacidades del Silicio para RTOS seguros y protegidos de grado automotriz.

	SC1	SC2	SC3	SC4	Hardware Requirements
OSEK OS (All Conformance Classes)	✓	✓	✓	✓	
Counter Interface	✓	✓	✓	✓	
Schedule Tables	✓	✓	✓	✓	
Stack Monitoring	✓	✓	✓	✓	
ProtectionHook		✓	✓	✓	
Timing Protection		✓		✓	Timers with high priority interrupt
Global Time/Synchronization Support		✓		✓	Global Time Source
Memory Protection			✓	✓	MPU
OS-Application			✓	✓	
Service Protection			✓	✓	
CallTrustedFuction			✓	✓	(non-) privilege Modes

Figura 4.1: **Detalles de las clases de escalabilidad**

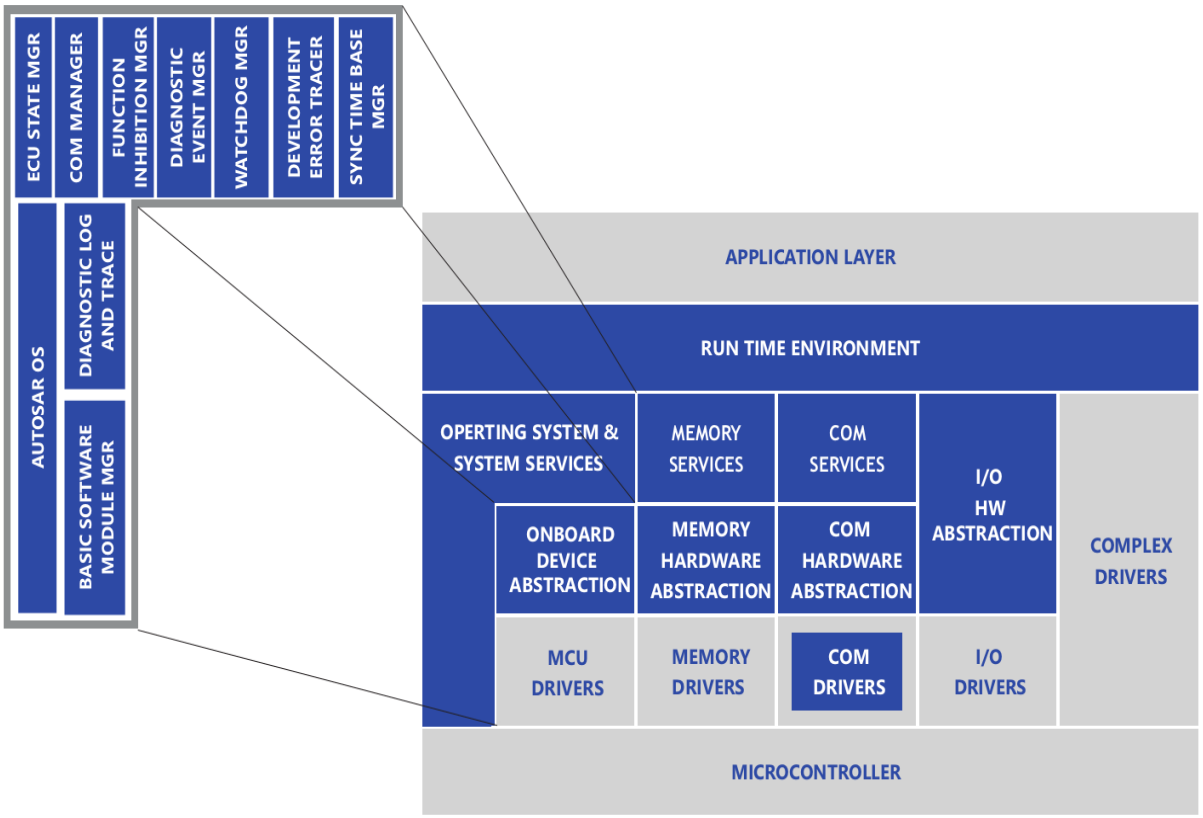


Figura 4.2: **Servicios del Sistema**

Nombre del Módulo	**Descripción**
Administrador del Estado de la ECU	El Administrador del Estado de la ECU realiza la inicialización/desinicialización de todos los módulos de software básicos, incluidos el RTE y el sistema operativo (OS). El módulo controla el estado de operatición de una ECU (Suspensión, Arranque, Activación, Apagado y Ejecución) en función de los eventos del sistema.
Administrador de la Comunicación	Este módulo controla el estado de todos los canales de comunicación conectados a la ECU y proporciona una interfaz a los SWCs independiente del bus (y, por lo tanto, a su aplicación) para solicitudes de comunicación externa.
Administrador de Inhibición de Funciones	Este módulo controla (habilita/deshabilita) las funcionalidades de los componentes SW en función de condiciones tales como: fallas, calidad de la señal, los estados de la ECU y del vehículo, comandos del probador de diagnóstico, etc.
Administrador de Eventos de Diagnóstico	Este módulo implementa un registro de errores de acuerdo a la documentación específica del fabricante. Una interfaz estandarizada para monitores de diagnóstico permite un desarrollo uniforme de componentes de software entre diversos fabricantes. El módulo de los DEMs es responsable de administrar los estados de los códigos de fallas de diagnóstico, los datos del entorno del error y de almacenar los datos en una NVRAM.

Nombre del Módulo	Descripción
Rastreador de Errores en la etapa de Desarrollo	Este módulo admite búsquedas de errores durante el desarrollo de software y proporciona una interfaz para el informe de errores. En caso de error, esta interfaz se llama desde cada módulo BSW.
Planificador del BSW	El módulo SCHM llama a la función cíclica para cada módulo BSW y pone a disposición las funciones que cada módulo BSW necesita llamar al inicio y al final de las secciones críticas. Este módulo es parte del RTE (Runtime Environment en R4.0)
Rutinas CRC	El módulo de verificación por redundancia cíclica (Cyclic Redundancy Check) proporciona una función de servicio para calcular la suma de verificación (checksum) de la CRC.
Entorno de Ejecución (RTE)	El RTE es responsable de la ejecución de los componentes del software y realiza el intercambio de datos entre los componentes de software y el software básico.

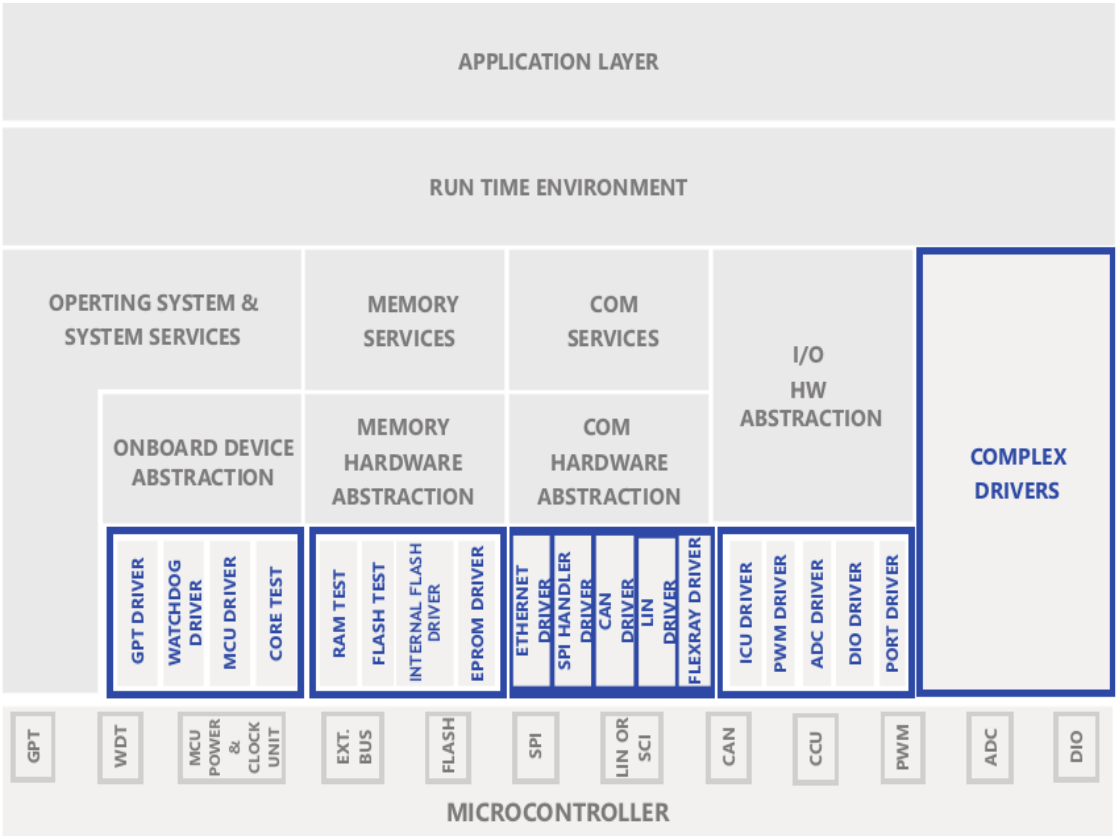


Figura 4.3: **Módulos MCAL del Editor K-SAR**

Nombre del Módulo	Descripción
Controlador de Puertos	Este módulo provee servicios para inicializar toda la estructura de puertos del microcontrolador
Controlador del DIO (Digital Input / Output)	El Controlador de Entradas y Salidas Digitales provee servicios de lectura y escritura a los canales DIO (pines), grupos de puertos y canales DIO.
El Controlador del ADC	El Controlador del ADC es responsable de controlar el convertidor analógico a digital y de acceder a los resultados de una conversión. Es decir, inicializa el convertidor, provee servicios para iniciar o finalizar una conversión, y para seleccionar la fuente de activación y para seleccionar la fuente de activación y la condición de activación.
Controlador del PWM	El Controlador del Modulador por Ancho de Pulso (PWM), provee servicios para la inicialización y el control de canales PWM del microcontrolador.
Controlador del ICU (Unidad de Captura de Entrada)	El controlador ICU proporciona servicios para la detección de flancos, medición de señales periódicas, asignación de marcas de tiempo de flancos y control de las interrupciones de activación (wake-up).

Nombre del Módulo	Descripción
Controlador del CAN	El controlador CAN provee servicios para inicializar el controlador CAN, enviar y recibir mensajes y cambiar los estados del controlador (inactividad, parada, etc.).
Controlador del FlexRay	El controlador FlexRay se utiliza para abstraer las diferencias relacionadas con el hardware entre diferentes controladores de comunicación FlexRay. Todas las propiedades necesarias del controlador de comunicación según la especificación del protocolo FlexRay están encapsuladas en este módulo y se puede acceder a ellas a través de su interfaz uniforme.
Controlador del LIN	El controlador LIN provee servicios para iniciar la transmisión de tramas (encabezado, respuesta, modo de suspensión y activación), así como para recibir respuestas, verificar el estado momentáneo y validar eventos de activación.
Controlador del Manipulador del SPI	El controlador SPI proporciona una opción para intercambiar datos a través de la interfaz SPI. Se utiliza principalmente para la conexión externa de la EEPROM y el Watchdog,...
Controlador del Ethernet	El controlador del Ethernet provee una opción para el intercambio de datos a través de la interfaz Ethernet. Con la interfaz Ethernet disponible, es posible desarrollar puertas de enlace muy potentes con una conexión MOST y así aprovechar las ventajas de la arquitectura AUTOSAR.

Nombre del Módulo	Descripción
Controlador del EEPROM	El controlador EEPROM permite un acceso uniforme e independiente del hardware al almacenamiento EEPROM. Pone a disposición servicios de lectura, escritura y comparación de datos, así como de eliminación de bloques.
controlador del FLASH Interno	El controlador flash provee un acceso uniforme e independiente del hardware a la memoria flash. Ofrece servicios de lectura, escritura y comparación de datos y borrado de bloques (sector).
Prueba de la RAM	Este módulo prueba las celdas RAM internas del microcontrolador. Se realiza una prueba completa durante el arranque y el apagado de la ECU, o se activa mediante un comando de diagnóstico. Durante el funcionamiento normal se realiza una prueba cíclica (bloque por bloque o celda por celda).

Nombre del Módulo	Descripción
Controlador del Watchdog	Este módulo provee servicios para controlar y activar hardware del Watchdog. La rutina de activación llama al administrador del Watchdog.
Driver del GPT	El Controlador del GPT (Temporizador de Propósito General) provee una interfaz para acceder a los temporizadores internos del microcontrolador. Se puede utilizar para controlar eventos que ocurren periódicamente o de forma única.
Controlador de MCU	El Controlador de la Unidad del Microcontrolador provee los siguientes servicios: ▪ Reset del microcontrolador disparado por software. ▪ Selección del modo de encendido del microcontrolador (PARO, SUSPENSIÓN, DETENCIÓN, etc.) ▪ Configuración del comportamiento de activador. ▪ Administración de la unidad de reloj interna PLL. Inicialización de áreas de RAM con valores predefinidos.
Pruebas del Núcleo	El controlador de Prueba del Núcleo provee servicios para configurar, iniciar, sondear, finalizar y notificar a la aplicación sobre los resultados de la Prueba del núcleo. También provee servicios para regresar los resultados de las pruebas de una forma predefinida. Además, provee varias pruebas para verificar la funcionalidad dedicada del núcleo, como por ejemplo: los registros de propósito general o la Unidad Aritmética y Lógica (ALU).

Nombre del Módulo	Descripción
Controladores Complejos	Los controladores complejos contienen controladores que no están estandarizados en AUTOSAR y que utilizan propiedades específicas de un microcontrolador o ECU (por ejemplo, dispositivos periféricos complejos). Estos incluyen funcionalidades para evaluación de sensores y monitorización de controladores con acceso directo al microcontrolador.

CAPÍTULO 5

Soporte multinúcleo

5.1 INTRODUCCIÓN:

A medida que la demanda por poder computacional aumenta rápidamente en el ámbito automotriz, los OEM (fabricantes de equipos originales) y TIER1 (proveedores de primer nivel) están introduciendo gradualmente ECUs multinúcleo en sus arquitecturas electrónicas. Además, estas ECUs multinúcleo ofrecen nuevas características, como mayores niveles de paralelismo, que facilitan el acatamiento de los requisitos de seguridad como ISO26262 y la implementación de otros casos de uso automotrices más complejos. Los principales casos de uso de ECUs multinúcleo pueden ser:

1. Complejidad decreciente de la arquitectura.
2. Manejo de aplicaciones que exigen recursos
3. Mejorar la seguridad
4. Uso dedicado de núcleos

Teniendo todo esto en cuenta, la versión 4.0 de AUTOSAR ha introducido soporte para sistemas operativos en tiempo-real embebidos para múltiples núcleos. Se han introducido nuevos conceptos como entidades localizables (LEs), inicio/apagado de múltiples núcleos, comunicador de aplicaciones entre sistemas operativos (IOC) y Spinlock en la especificación arquitectural del sistema operativo multinúcleo AUTOSAR para ampliar las especificaciones del sistema operativo de un solo núcleo.
El comunicador de aplicaciones entre sistemas operativos (IOC), que forma parte de AUTOSAR OS, proporciona servicios de comunicación a los que pueden acceder los clientes que necesitan comunicarse a través de los límites de las aplicaciones del sistema operativo en la misma ECU. Cada Core ejecuta una especie de administración del estado de la ECU. Cada núcleo también tendrá el módulo 'Core Test' ejecutándose en el BSW.

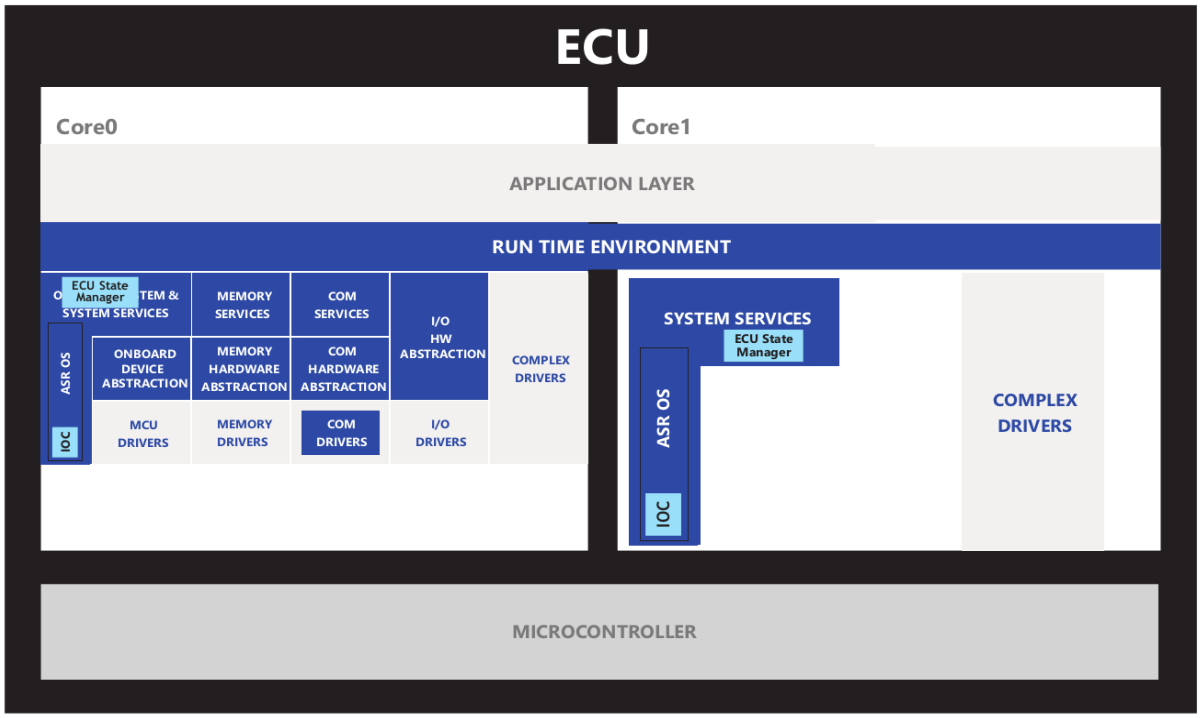


Figura 5.1: **ECU con un microcontrolador de dos núcleos**

CAPÍTULO 6

Seguridad funcional

6.0.1. Introducción:

La seguridad Funcional es parte de la seguridad general de un sistema que depende de la ejecución correcta de funciones específicas. El objetivo de la seguridad funcional es realizar la función prevista correctamente o el sistema fallará de manera segura predecible. El estándar de seguridad funcional ISO26262 que se deriva de IEC-61508 nos exige tener un enfoque basado en el riesgo automotriz específico para sistemas Eléctricos y Electrónicos (E/E). Esto se aplica a automóviles de pasajeros con un peso bruto máximo de hasta 3.5 toneladas.
Aspectos tales como la complejidad del diseño del sistema pueden ser relevantes para lograr la seguridad funcional en el campo automotriz. El software es un parámetro que puede influir en la complejidad a nivel del sistema. Se pueden usar nuevas técnicas y conceptos para el desarrollo de software para minimizar la complejidad y, por lo tanto, pueden aliviar el objetivo de la seguridad funcional.
Como una iniciativa de estandarización del software, AUTOSAR R4.0 considera aspectos de seguridad funcional relevantes para el desarrollo actual del software automotriz.

6.1 IMPLEMENTACIÓN DE LA ARQUITECTURA Y LA SEGURIDAD EN AUTOSAR EN R4.0:

- Características de Protección de Memoria (MPU) en el OS - “SC4”
- Características para el OS Multinúcleo
- Características relativas a la monitorización del E-Gas
- Características relativas a la monitorización del flujo del Programa
- Las características relativas a la temporización incluyen:
  - Características relativas a la provisión de bases de tiempo sincronizadas
    - Suministro de una base de tiempo sincronizada dentro de un clúster
    - Servicios para acceder a bases de tiempo sincronizadas
    - Sincronizar AUTOSAR OS con FlexRay Global Time de una manera bien definida
  - Características relativas a la sincronización del procesamiento de unidades de procesamiento asíncronas
    - Servicios para la sincronización de SWCs
  - Características para permitir que las aplicaciones sean implementadas de forma determinista en el tiempo
  - Características relativas a la protección contra violaciones a la temporización.

- Características relativas a la monitorización del flujo del programa
- Características relativas a la Pila de Comunicación así como al control de la secuencia de datos y múltiples enlaces de comunicación.
- Protección en la comunicación a todo lo largo (E2E) del SWC
- Características relativas a la partición de memoria y los modos de usuario/supervisor

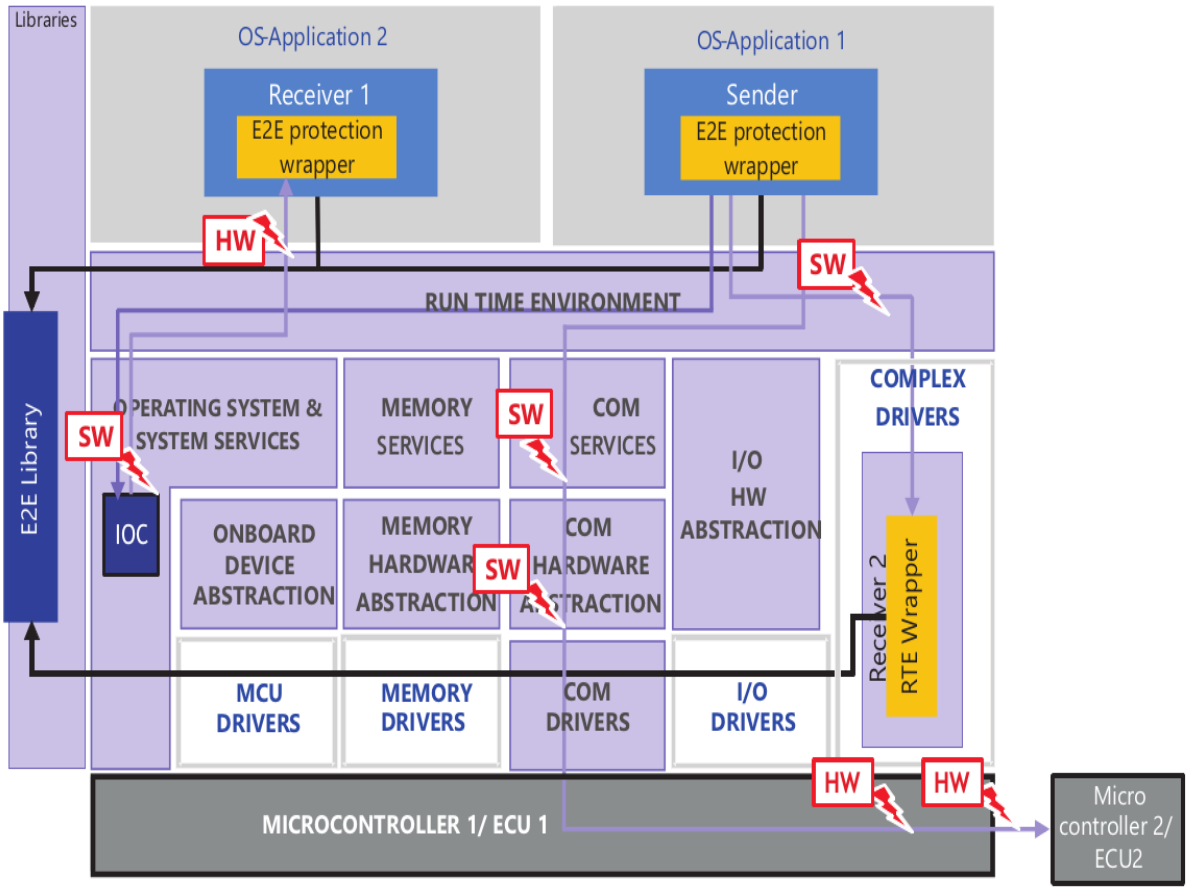


Figura 6.1: **Módulo de protección de la comunicación de extremo a extremo (E2E)**

La Figura 6.1 describe las fuentes típicas de interferencias, causantes de errores detectados por la protección del E2E:
Fuentes relacionadas con el SW:

- Errores en su mayoría generados en el RTE
- Errores en el COM, parcialmente generados y parcialmente por la codificación manual
- Error en la pila de la red
- Error generado en el IOC o en el OS

Error en RTE en su mayoría generado, Error en com parcialmente generado y parcialmente codificado a mano Error en la pila de red
Fuentes relacionadas con el HW:

- Error del microcontrolador durante el cambio entre núcleo/partición

- Falla del HW de la red
- Interferencia Electromagnética (EMI) en la red
- Falla del microcontrolador durante el cambio de contexto (partición) o en la comunicación entre núcleos

La biblioteca E2E LIB extiende las señales con información del CRC y, un Contador de Secuencias, en el lado del remitente y verifica la información en el lado del receptor, asegurando así la detección eficiente de "falla de comunicación" entre SWCs.

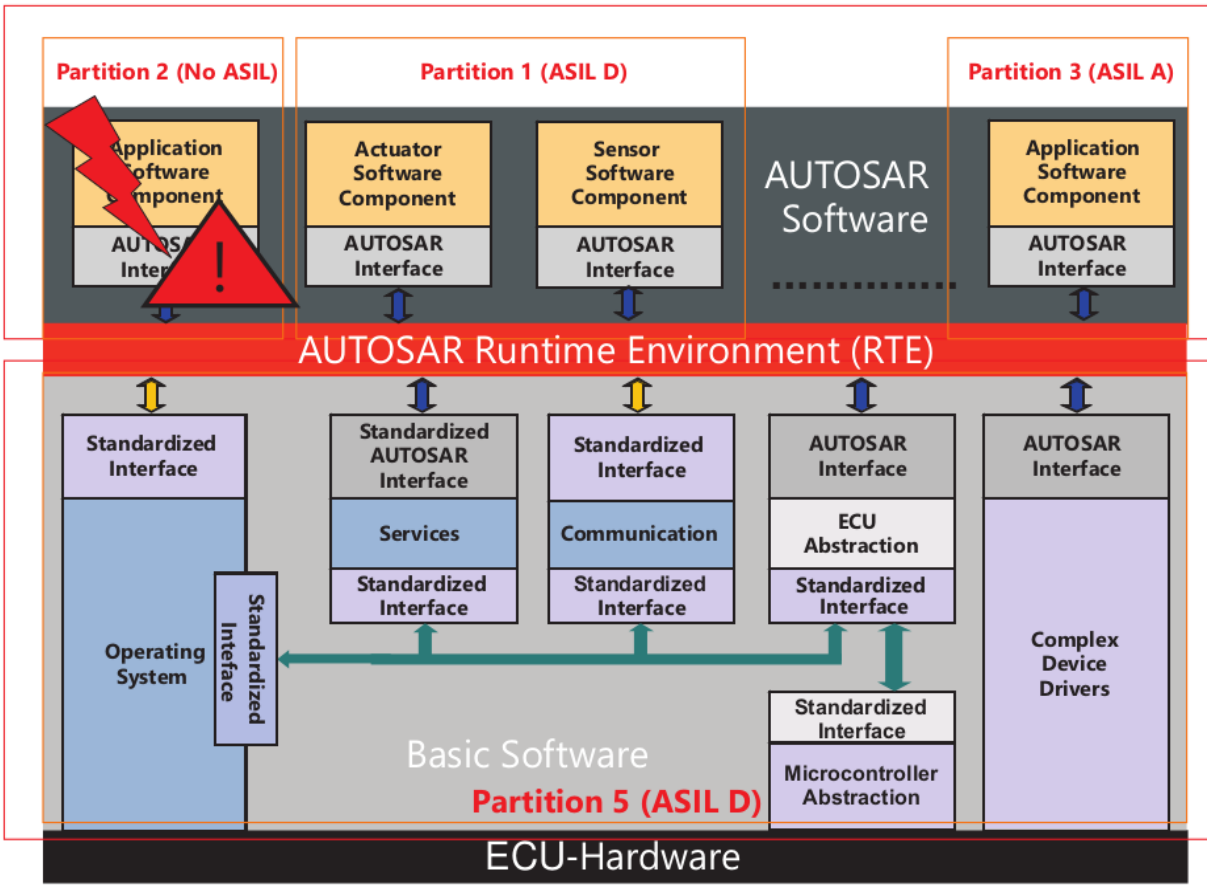


Figura 6.2: **Concepto de partición en seguridad funcional**

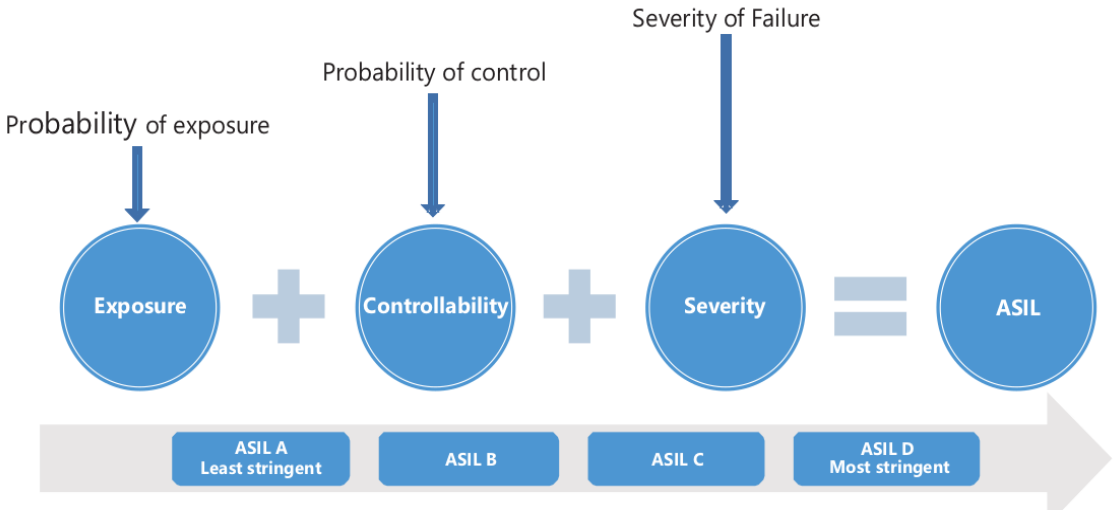


Figura 6.3: **Niveles de Integridad de la Seguridad Automotriz (ASIL)**

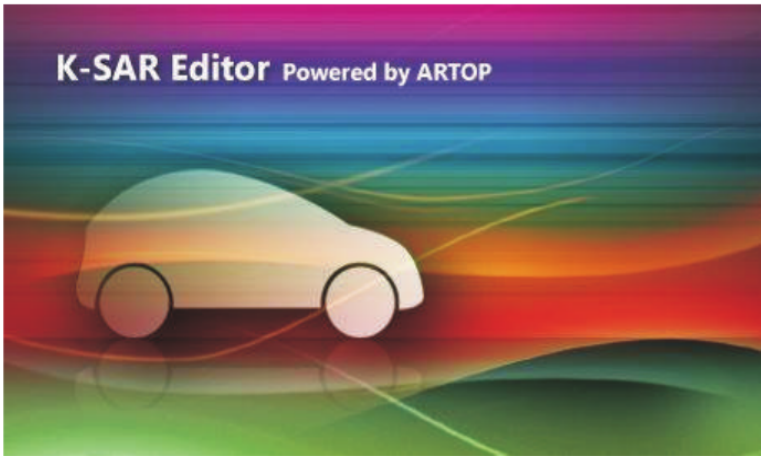
Con el concepto de partición en AUTOSAR R4.0, los SWCs se pueden colocar en particiones separadas de la ECU. Estas particiones se pueden terminar, monitorizar y reiniciar de forma independiente. El único propósito de estas particiones separadas es lograr la “Libertad de Interferencia”. Con estos SWCs con diferentes ASILs (según ISO26262) se pueden ejecutar en la misma ECU.

CAPÍTULO 7

Cadena de Herramientas del Editor K-SAR

7.0.1. Introducción

La cadena de herramientas del editor K-SAR de KPIT genera dinámicamente controles GUI para los módulos AUTOSAR especificados en el Archivo de Definición de Parámetros de Configuración de la ECU y también genera un archivo de descripción de configuración de la ECU.
La cadena de herramientas de Editor K-SAR admite la opción de complemento para las Herramientas de Generación, incluidas Herramientas de Generación de terceros. Con esta función, los archivos de encabezado (.h) y código fuente en 'C' (.c) se pueden generar directamente invocando la Herramienta de Generación desde el Editor K-SAR.



7.1 ENTRADAS UTILIZADAS:

Archivo(s) de Definición de Parámetros de Configuración de la ECU: en formato XML y contiene definiciones para Módulos, Contenedores y Parámetros. El formato del archivo XML debe cumplir con los estándares de especificación de AUTOSAR ECU.

Archivo CSV de Configuración Personalizada: como entrada al momento de cargar el archivo de Descripción de Configuración del Sistema. Este archivo CSV está en formato de texto y contiene las notificaciones específicas de tier-1 y la configuración de la ECU. se actualiza automáticamente en función de las notificaciones.

Salidas Generadas:
La salida del programa Editor K-SAR es un Archivo de Descripción de Configuración de la ECU en formato XML, y contiene los valores configurados para los Parámetros, Contenedores y Módulos. El formato del Archivo de la Descripción de la Configuración de la ECU debe cumplir con los estándares de especificación de la ECU de AUTOSAR.

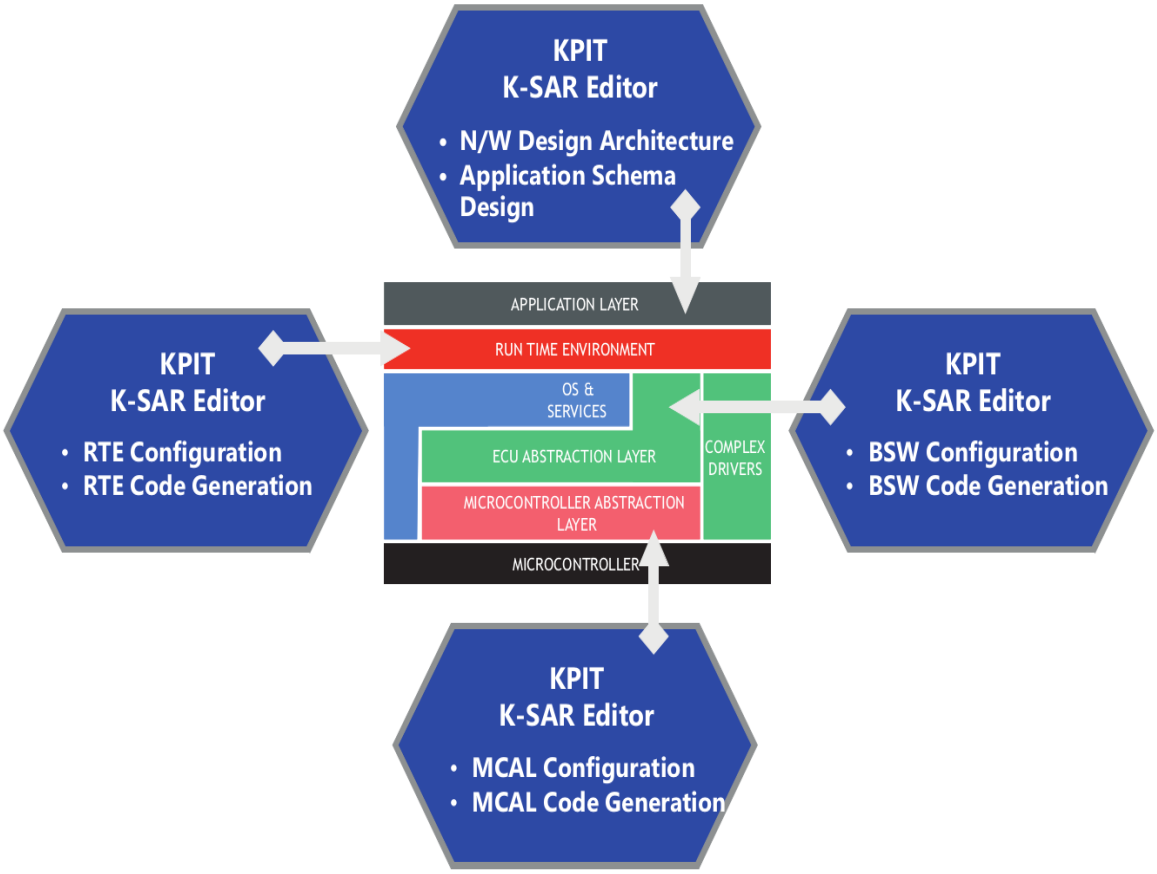


Figura 7.1: **Cadena de Herramientas del Editor KPIT-KSAR para el Desarrollo de Modelo en Capas AUTOSAR**

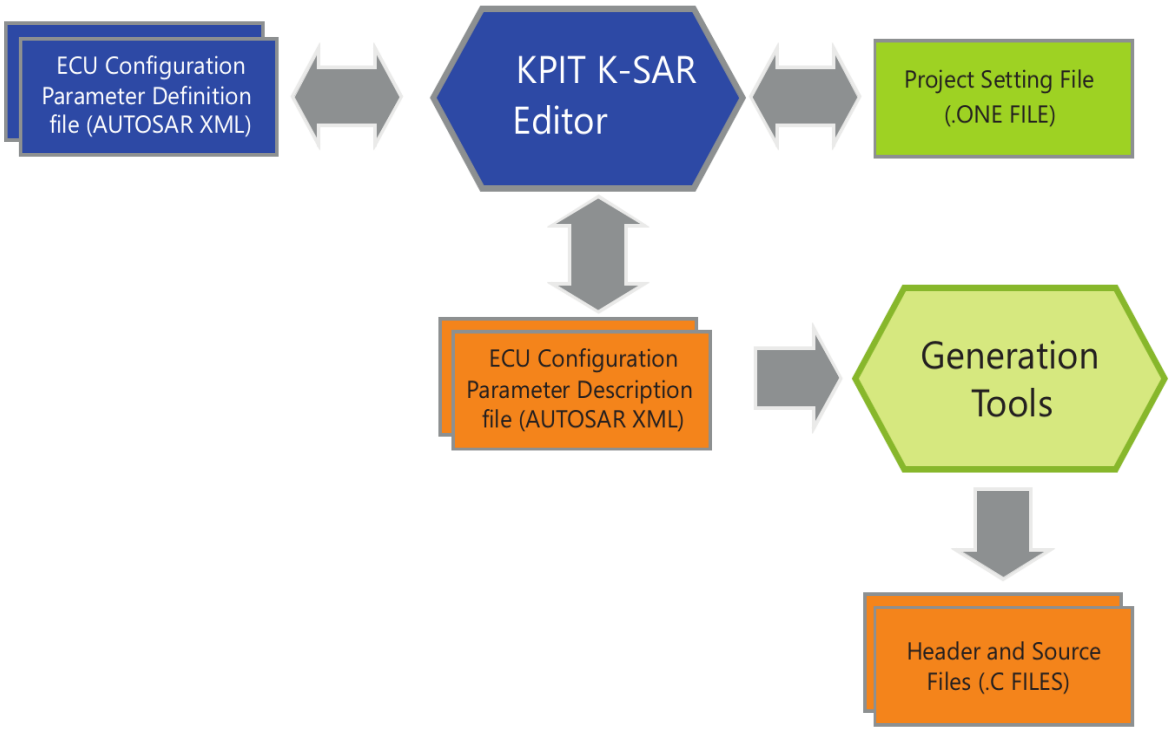


Figura 7.2: **Flujo de Trabajo del Editor K-SAR de Alto Nivel**

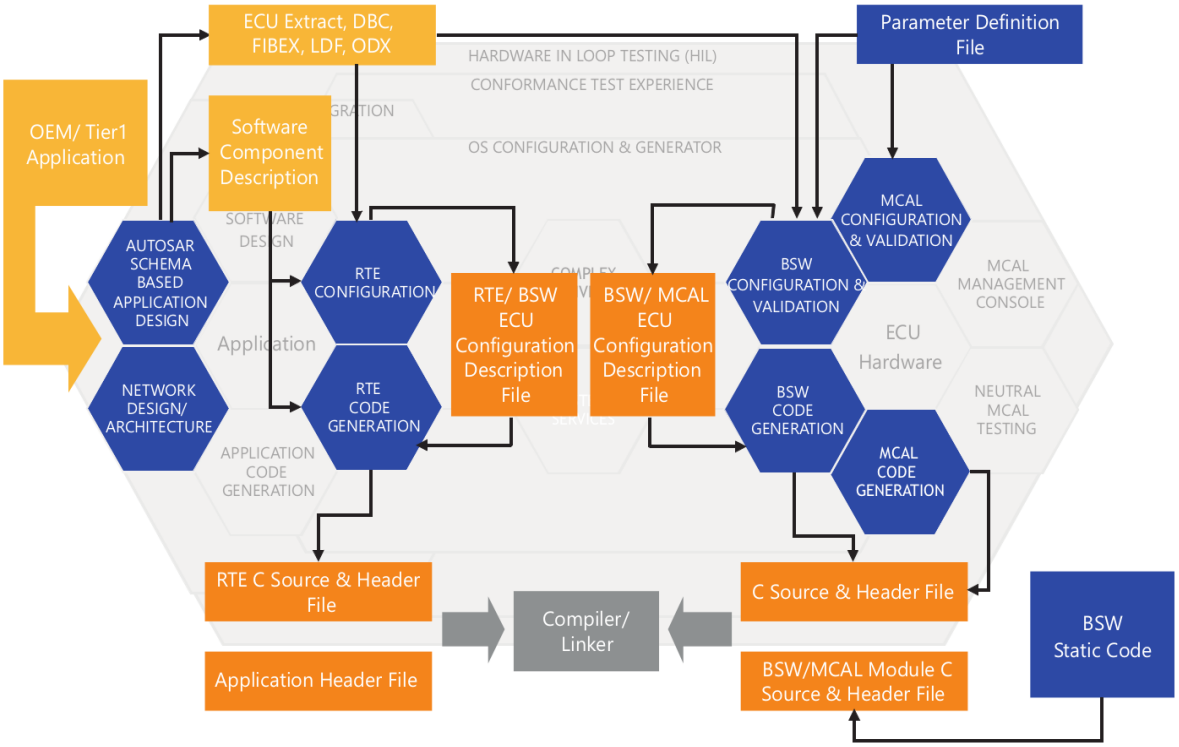
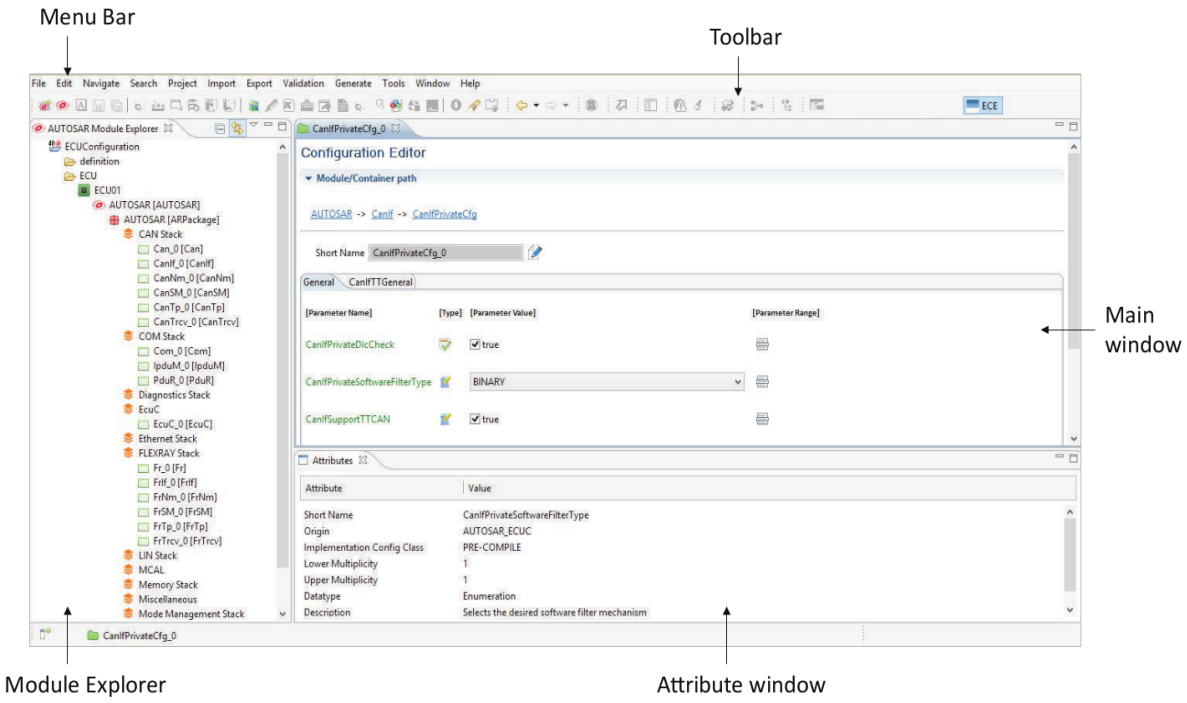


Figura 7.3: **Flujo de Trabajo del Editor K-SAR - Detallado**



7.2 CARACTERÍSTICAS DEL EDITOR K-SAR

- Fácil de usar como cualquier otra herramienta basada en Windows
- GUI fácil de usar
- Compatibilidad con la función MRU (usado más recientemente)
- Validación - se puede verificar que la configuración del módulo sea correcta y completa mediante la validación.
- Para cualquier inconsistencia y dependencia, el Editor despliega Error(es), Información y Mensaje(s) en la ventana 'Messages Info'
- Almacenamiento y Carga de datos de Configuración del Usuario
- Importación de datos AUTOSAR ECU Extract, DBC, LDF y Fibex
- Generación de Informes en HTML - el Editor permite al usuario obtener el resumen del projecto cargado
- Soporte de ayuda compatible con Microsoft
- Fácil instalación y configuración
- Menor consumo de memoria
- No depende de ningún RTE

7.3 TÉRMINOS UTILIZADOS

Proyecto:
Se utiliza un proyecto para almacenar la configuración.

Módulo:
Los módulos indican un Módulo de Software de los Parámetros de Configuración de la ECU. Se asigna un solo nombre a los módulos individuales. El número de instancias del módulo depende de la multiplicidad del módulo.

Contenedor:
Los Contenedores se usan para agrupar parámetros y referencias. El número de instancias de un Contenedor depende de la multiplicidad del Contenedor.

Sub-Contenedor:
También se utiliza un Sub-Contenedor para agrupar parámetros y referencias. El Sub-Contenedor es parte del Contenedor. Los Sub-Contenedores se definen dentro de Contenedores. El número de instancias de un Contenedor depende de la multiplicidad del Contenedor.

Multiplicidad:
La Multiplicidad se utiliza para especificar la frecuencia con el cual un elemento de configuración específico (módulo, contenedor, parámetro o referencia) puede ocurrir en un Archivo de Descripción de Configuración de una ECU. La Multiplicidad-Inferior y la Multiplicidad-Superior son dos atributos para especificar las ocurrencias mínimas y máximas. En cualquier caso, la Multiplicidad-Inferior debe ser menor o igual que la Multiplicidad Superior. Se menciona la Multiplicidad-Inferior como ’1’ significa que el elemento es obligatorio. La multiplicidad-Inferior mencionada como ’0’ significa que el elemento es opcional. La Multiplicidad-Superior mencionada como ’*’ significa que el parámetro puede ocurrir cualquier número de veces.

Conjunto de configuración múltiple:
Se utiliza para permitir la descripción de Varios Conjuntos de Configuración de la ECU.

Plantilla:
Las plantillas son definiciones de elementos configurables (Módulo, Contenedor o Sub-Contenedor). Este formato se toma del Archivo de Definición.

Fórmula de cálculo:
Se utiliza una fórmula de cálculo para proporcionar información sobre cómo se pueden calcular los valores. Utiliza referencias para abordar elementos ajenos para recabar la información requerida.

CAPÍTULO 8

Acerca de KPIT

8.1 EXPERIENCIA EN KPIT AUTOSAR

- El desarrollo de AUTOSAR en KPIT comenzó a principios de 2005 cuando nos convertimos en Miembros AUTOSAR Premium. Estamos contribuyendo activamente al movimiento de estandarización de AUTOSAR y hemos sido designados como contratistas generales para redactar las Especificaciones de Conformidad para el estándar AUTOSAR. También somos el contratista general del proyecto de prueba de conformidad AUTOSAR.
- Somos una empresa dedicada a la plataforma de software AUTOSAR y respaldamos la filosofía AUTOSAR de “Cooperar en materia de normas”.
- En AUTOSAR nos dedicamos a desarrollar Módulos BSW AUTOSAR y controladores MCAL como parte de la pila AUTOSAR y proveemos servicios en torno a estos módulos. Hemos desarrollado el primer producto completo MCAL.
- En nuestro esfuerzo por proporcionar componentes que cumplan con los estándares, de alta calidad y listos para la producción, cooperamos con herramientas especializadas AUTOSAR. Las expectativas de esta cooperación son hacer que nuestros componentes sean compatibles con estas herramientas de conformidad especializadas AUTOSAR.
- Apoyamos continuamente plataformas de Red para marcas premium en Europa durante los últimos 10 años. y hemos suministrado plataformas para unas 150 ECUs integradas en los vehículos de carretera. Este apoyo está siendo ampliando actualmente a AUTOSAR.
- También somos miembros Premium de JasPar.

8.2 VENTAJAS DE KPIT

- Se reduce el tiempo para completar la conformidad con AUTOSAR mediante el suministro de componentes que cumplan con el estándar AUTOSAR.
- Reducción de costos de la lista de materiales (BOM) a través de los componentes BSW de grado automotriz.
- Se mejora el rendimiento de las plataformas a través de la programación manual de Módulos AUTOSAR BSW optimizados incluyendo MCAL.
- Una migración AUTOSAR más rápida y completa de las aplicaciones heredadas mediante el diseño de Metodologías para la Migración de Aplicacio

y del tiempo de comercialización (TTM) general mediante el uso de KPIT AUTOSAR cadena de herramientas

- Reducción en la carga adicional de desarrollo y del Tiempo total de Comercialización (TTM) mediante el uso de la Cadena de Herramientas KPIT AUTOSAR.

Permite la Adopción de Nuevas Tecnologías	▪ Se ejecutó la migración de AUTOSAR para la ECU de seguridad. ▪ Sólida experiencia en la migración de aplicaciones críticas en cuestiones de seguridad para los próximos protocolos de comunicación mejorados como FlexRay.
Optimización	▪ La seguridad de la ECU de AUTOSAR creada con Tier1 funciona mejor que la heredada ▪ El Modelo de Negocio único hace que el proceso de migración sea más rentable y fluido. ▪ El cliente no queda Atado a una herramienta del proveedor o a una metodología específica
Mejoras Renovadoras	▪ La Metodología de Migración de Aplicaciones KPIT está diseñada para la extensibilidad y, por lo tanto, le ayuda a diseñar una estrategia AUTOSAR a largo plazo en lugar de experimentar solo con un piloto. ▪ La metodología de migración le ayuda a reutilizar su cadena de herramientas heredada y los modifica para adoptar requerimientos más nuevos tantos como sea posible
Ventajas en el Tiempo	▪ El modelo de participación In Situ + Deslocalizado mejora la velocidad de ejecución con eficiencias mayores ▪ Los conjuntos de pruebas de conformidad ya construidos y probados permiten el camino más rápido hacia la preparación de la producción
Permite la Conformidad	▪ La experiencia en Especificaciones de Conformidad de AUTOSAR le ayuda a crear una solución que pasa las pruebas de conformidad rápidamente ▪ La Infraestructura de Pruebas Abiertas y Automatización inventado por KPIT le ayuda a probar y validar el rendimiento del sistema en múltiples niveles en el ciclo V. ▪ Nuestras metodologías le ayudan a lograr el rendimiento deseado del sistema

8.3 SERVICIOS/PRODUCTOS DE SOFTWARE PROPORCIONADOS POR KPIT

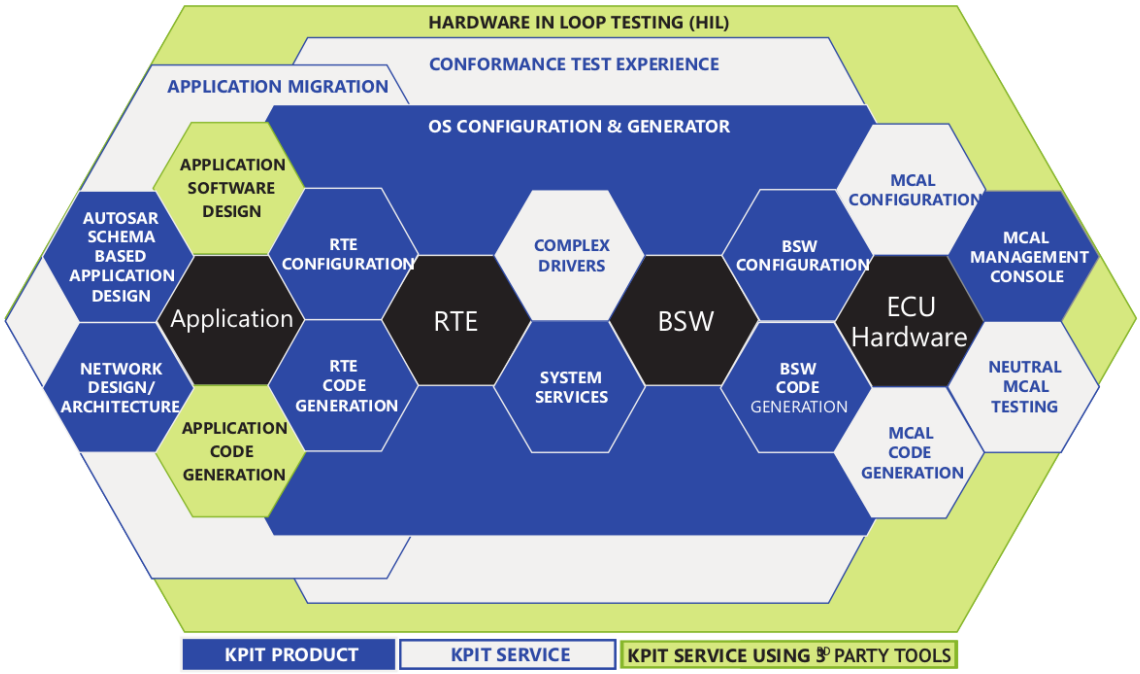


Figura 8.1: **Configuración del entorno AUTOSAR con KPIT**