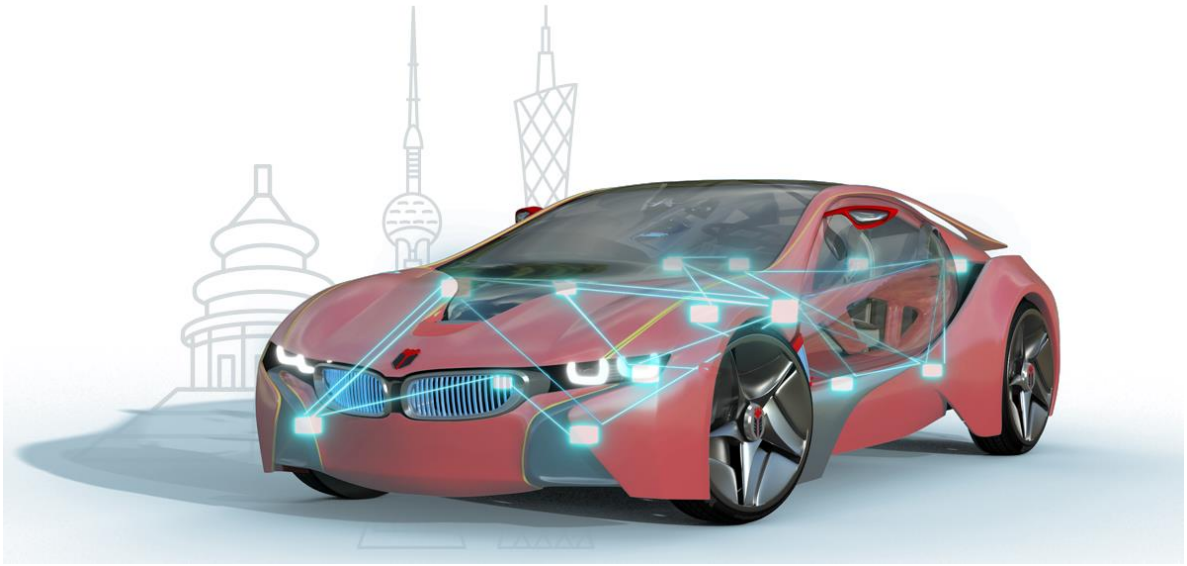
知从木牛安全通信方案手册

ZC.MuNiu SecOC Solution Manual

知从木牛基础软件平台安全通信模块

ZC.MuNiu Basic Software Platform SecOC



知从木牛安全通信方案手册
ZC.MUNIU SECOC SOLUTION MANUAL

知从木牛基础软件平台安全通信模块

ZC.MuNiu Basic Software Platform SecOC

1 方案介绍 INTRODUCTION TO THE SOLUTION

在目前的车载网络中，大部分数据传输都是在没任何安全措施的情况下进行的。例如应用最广的 CAN 通讯设计之初是没有考虑过信息安全问题的，其明文传输、报文广播传输、极少网络分段等特性，让进入整车网络的黑客轻松便可以伪造报文对车辆进行控制。

In the current in-vehicle network, most data transmissions are carried out without any security measures. For example, the widely used CAN communication was not designed with Cybersecurity in mind initially. Its characteristics of plaintext transmission, message broadcasting, and minimal network segmentation make it easy for hackers who enter the vehicle network can easily forge messages to control the vehicle.

SecOC 是在 AUTOSAR 软件包中添加的信息安全组件（组件位置及可应用的通讯方式如下图所示），该 Feature 增加了 CMAC 运算、秘钥管理、新鲜值管理和分发等一系列的功能和新要求。SecOC 模块在 PDU 上为关键数据提供有效可行的身份验证机制，认证机制与当前的 AUTOSAR 通信系统无缝集成，同时对资源消耗的影响应尽可能小，以便为旧系统提供附加保护。

SecOC is a Cybersecurity component added to the AUTOSAR software package (the component location and applicable communication methods are shown in the figure below). This feature adds a series of functions and new requirements such as CMAC calculation, key management, freshness value management, and distribution. The SecOC module provides a viable authentication mechanism for critical data on the PDU, integrating the authentication mechanism seamlessly with the current AUTOSAR communication system, while minimizing the impact on resource consumption to provide additional protection for legacy systems.

Cybersecurity on the MCU side is a crucial part of the overall vehicle Cybersecurity system:

- 数据真实性（Message Authentication）验证接收到数据的来源是可信的、被授权的发送者，防止假冒节点/欺骗攻击；

  Message Authentication provides authentication to confirm that received data is from a legitimate source and prevents fraudulant nodes or spoofing attacks.

- 数据完整性（Data Integrity）确保数据从发送方发出到接收方接收的整个传输过程中，没有被篡改、损坏或意外修改，防止数据篡改攻击；

  Data Integrity ensures that data is not tampered with or corrupted during transmission, protecting against data tampering attacks.

- 防御重放攻击（Protection against Replay Attacks）确保接收到的数据是最新的、非重复的，而不是攻击者记录并重新发送的旧有效报文，防止重放攻击；

  Freshness validation ensures that only the most recent data is accepted, effectively blocking replay attacks that rely on retransmitting old messages.

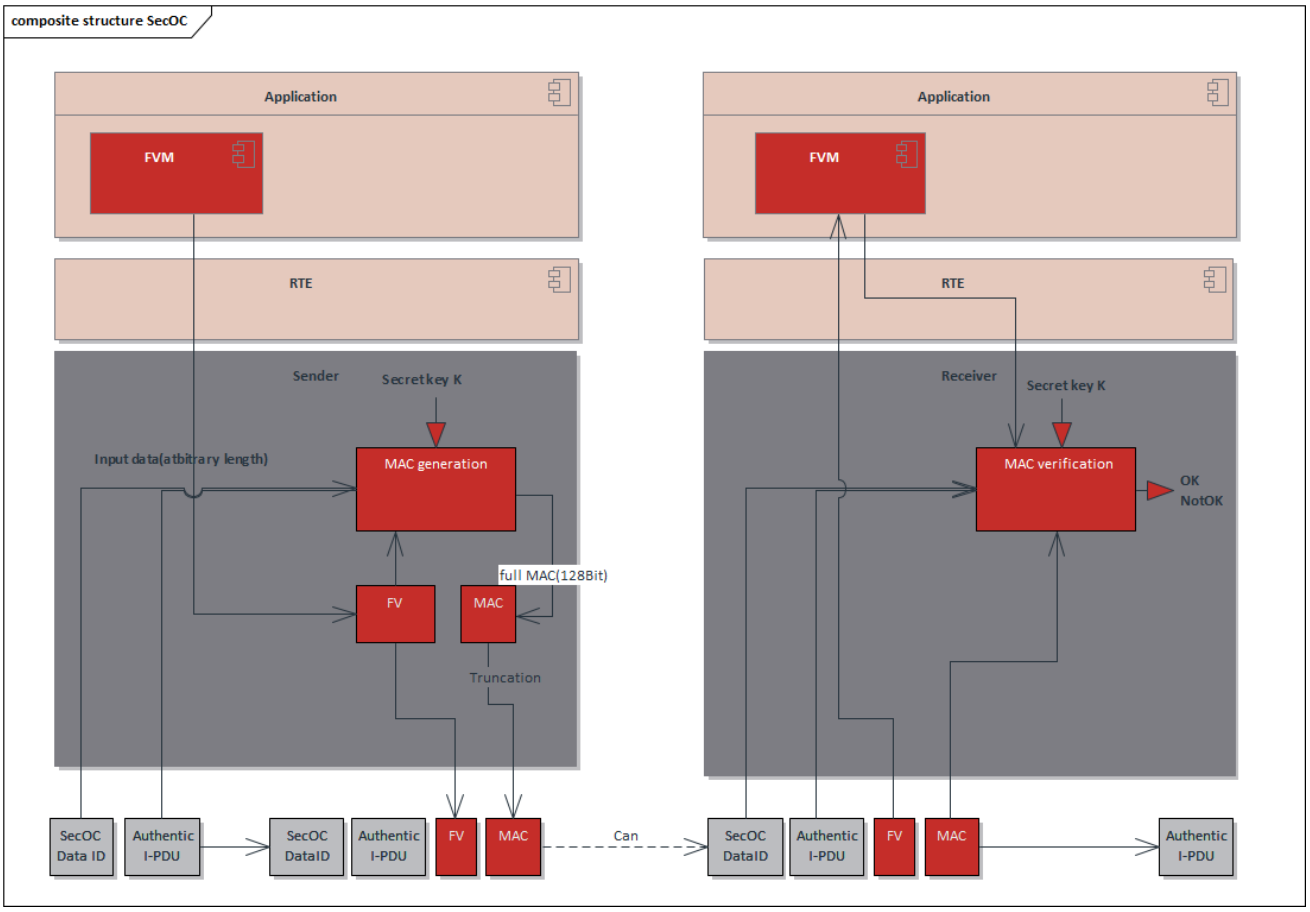


FIGURE 1 SECOC

2 数据真实性 MESSAGE AUTHENTICATION

知从科技可以为客户提供 Message Authentication 完整方案，并可针对项目特定需求和模块定制开发：

ZC can provide customers with a complete Message Authentication solution and can customize development for specific project requirements and modules:

数据真实性（Message Authentication）的核心是密码学身份验证。其实现不依赖于单一模块，而是通过 SecOC 与 AUTOSAR 基础软件栈中的多个模块协同工作，构成一个完整的安全通信链条。SecOC 使用消息验证码（Message Authentication Code, MAC） 来实现数据真实性。MAC 有时也被称为密码学标签（Cryptographic Tag） 或认证标签（Authentication Tag）。

For data authenticity, cryptographic authentication is fundamental. This is realized not by a single component, but via SecOC's cooperation with various modules in the AUTOSAR Basic Software stack, which together create a comprehensive secure communication chain. A Message Authentication Code (MAC) is the mechanism SecOC employs for this purpose. The MAC may also be termed a Cryptographic Tag or Authentication Tag.

- 关键模块 Key Modules

SecOC 模块：认证流程的协调者。负责触发 MAC 的生成与验证，组装和解析安全 PDU，但不执行具体的密码学计算。加密服务管理器（Crypto Service Manager, Csm/CryptoSM）：密码学服务的抽象层。SecOC 通过调用 Csm 的标准化接口，请求 MAC 的生成或验证，从而与底层具体的加密实现解耦。加密驱动（Crypto Driver）： 密码学操作的执行者。在硬件安全模块（HSM）或软件加密库中实际执行 MAC 算法。PDU 路由器（PduR）： 通信的枢纽。负责在 SecOC、通信接口模块（如 CanIf, EthIf）和 COM 模块之间路由安全 PDU 和普通 PDU。

SecOC Module: The orchestrator of the authentication process. It is responsible for triggering the generation and verification of the MAC, and for assembling and parsing the secured PDUs, but it does not perform the actual cryptographic computations. Crypto Service Manager (Csm/CryptoSM): The abstraction layer for cryptographic services. SecOC calls the standardized interfaces of Csm to request MAC generation or verification, thereby decoupling from the underlying specific cryptographic implementation. Crypto Driver: The executor of cryptographic operations. It performs the actual MAC algorithm within a Hardware Security Module (HSM) or a software cryptographic library. PDU Router (PduR): The hub of communication. It is responsible for routing secured PDUs and normal PDUs between the SecOC module, communication interface modules (e.g., CanIf, EthIf), and the COM module.

➢ 详细实施流程 Detailed Implementation Process

发送端：MAC 生成与安全 PDU 组装。上层软件组件（SWC）通过 RTE 将需要保护的数据发送至 COM 模块，形成 I-PDU。COM 模块将该 I-PDU 传递给 SecOC 模块。SecOC 从新鲜度值管理器（FVM） 获取当前的新鲜度值。SecOC 将认证数据（即 I-PDU 中的有效载荷）与新鲜度值 拼接，形成待认证的完整消息。SecOC 调用 Csm 接口，发起一个 GenerateMac 作业。Csm 将请求派发给底层的 Crypto 驱动。Crypto 驱动在 HSM 或 CPU 中，使用指定的密钥（如 AES-128）和算法（如 CMAC），计算出完整的 MAC。SecOC 接收 Csm 返回的 MAC。根据配置，可能对 MAC 进行截断（Truncation）以节省带宽（例如，只取前 4 个字节）。SecOC 将认证数据、截断后的 MAC 和可能需要传输的部分新鲜度值，组装成一个新的、受保护的 I-PDU。SecOC 将这个安全 I-PDU 通过 PduR 路由到具体的总线驱动（如 CanIf），最终发送到总线上。

The Transmitter Side: MAC Generation and Secured PDU Assembly Upper-layer Software Components (SWCs) send data requiring protection to the COM module via the RTE, forming an I-PDU. The COM module passes this I-PDU to the SecOC module. SecOC acquires the current freshness value from the Freshness Value Manager (FVM). SecOC concatenates the authentication data (i.e., the payload within the I-PDU) with the freshness value, forming the complete message to be authenticated. SecOC calls the Csm interface, initiating a GenerateMac job. Csm dispatches the request to the underlying Crypto Driver. The Crypto Driver, within an HSM or via CPU software, uses the specified key (e.g., AES-128) and algorithm (e.g., CMAC) to compute the full MAC.SecOC receives the computed MAC from Csm. Depending on the configuration, the MAC may be truncated to save bandwidth (e.g., taking only the first 4 bytes).SecOC assembles the authentication data, the truncated MAC, and potentially a part of the freshness value requiring transmission into a new, protected I-PDU.SecOC routes this secured I-PDU via the PduR to the specific bus driver (e.g., CanIf), ultimately transmitting it onto the bus..

接收端：MAC 验证与身份确认接收安全 PDU：从总线驱动接收到的安全 I-PDU 通过 PduR 传递给 SecOC 模块。解析安全 PDU：SecOC 模块根据预定义的格式，从 PDU 中解析出认证数据、接收到的 MAC 和新鲜度值。验证新鲜度值（前置条件）：FVM 首先验证新鲜度值的有效性（防御重放攻击）。如果新鲜度值验证失败，则直接判定为失败，无需进行 MAC 验证。SecOC 使用解析出的认证数据和新鲜度值，构建出与发送端相同的完整消息。调用 Csm 接口，发起一个 VerifyMac 作业。Csm 将请求派发给 Crypto 驱动。Crypto 驱动使用相同的密钥和算法，对接收到的数据重新计算 MAC，并将计算结果与接收到的 MAC 进行逐位比较。验证成功（MAC 匹配）：Csm 返回 CSM_OK。SecOC 判定数据真实可信，将认证数据部分剥离出来，传递给上层的 COM 模块，最终送达目标 SWC。验证失败（MAC 不匹配）：Csm 返回

CSM_E_MAC_INVALID。SecOC 判定数据来源不可信或已被篡改，立即丢弃该 PDU。在验证失败时，SecOC 会通过诊断事件管理器（Dem） 报告一个诊断事件（如 SECOC_E_AUTHENTICATION_FAILURE）。可以配置基础软件模式管理器（BswM） 来对此错误做出反应，例如，限制 ECU 功能、增加错误计数器或触发安全状态切换。

Receiver Side: MAC Verification and Identity Confirmation. The secured I-PDU, received from the bus driver, is delivered to the SecOC module via the PDU Router (PduR). The SecOC module parses the received PDU according to a predefined format, extracting the authentication data, the received MAC, and the freshness value.The Freshness Value Manager (FVM) first validates the effectiveness of the freshness value (a defense against replay attacks). If the freshness value verification fails, the process is immediately deemed a failure, and MAC verification is bypassed. Using the parsed authentication data and freshness value, SecOC reconstructs the complete message, identical to the one formed at the transmitter side.It then calls the Crypto Service Manager (Csm) interface to initiate a VerifyMac job. Csm dispatches the request to the underlying Crypto Driver.The Crypto Driver, utilizing the same cryptographic key and algorithm, recalculates the MAC for the received data and performs a bit-wise comparison between the newly computed MAC and the received MAC. Verification Success (MAC Match): Csm returns CSM_OK. SecOC concludes that the data is authentic and trustworthy. It then strips off the authentication data portion and passes it to the upper-layer COM module, which finally delivers it to the target Software Component (SWC).Verification Failure (MAC Mismatch): Csm returns CSM_E_MAC_INVALID. SecOC determines that the data source is untrustworthy or the data has been tampered with and immediately discards the PDU. In the event of verification failure, SecOC reports a diagnostic event (e.g., SECOC_E_AUTHENTICATION_FAILURE) through the Diagnostic Event Manager (Dem).The Basic Software Mode Manager (BswM) can be configured to react to such errors, for instance, by restricting ECU functionality, incrementing an error counter, or triggering a transition to a safe state.

3 数据完整性 DATA INTEGRITY

知从科技可以为客户提供数据完整性方案，并可针对项目特定需求和模块定制开发，实现的安全特性.

ZC can provide customers with a complete Data integrity solution and can customize development for specific project requirements and modules.

数据完整性（Data Integrity）的核心是确保信息在传输过程中不发生任何非预期的改变。在 SecOC 中，这与数据真实性通过同一套密码学机制实现，但其技术侧重点和保障维度有所不同。数据完整性通过消息验证码（Message Authentication Code, MAC） 的固有特性来实现。

The core of data integrity is to ensure that information does not undergo any unintended alterations during transmission. In SecOC, this is achieved through the same cryptographic mechanism as data authenticity, but its technical focus and assurance dimensions differ. Data integrity is realized by leveraging the inherent properties of a Message Authentication Code (MAC).

关键模块（Key Modules）： SecOC 模块负责解析接收到的安全 PDU，分离数据与 MAC。触发 MAC 重新计算流程。根据 MAC 比较结果，做出数据是否完整的最终裁决。加密服务管理器（Csm）提供标准化的 VerifyMac 服务接口。将 SecOC 的验证请求路由至底层加密驱动。加密驱动（Crypto Driver）在 HSM 或软件库中，使用与发送方相同的密钥和算法，对接收到的数据执行 MAC 计算。执行精确的 MAC 值比较。PDU 路由器（PduR）完整性校验数据的传输通道。确保从总线接收到的安全 PDU 被无误地路由至 SecOC 模块。

The SecOC module is responsible for parsing the received secured PDU, separating the data from the MAC, and triggering the MAC recalculation process. It makes the final determination on data integrity based on the MAC comparison result. The Crypto Service Manager (Csm) provides a standardized VerifyMac service interface, routing SecOC's verification requests to the underlying Crypto Driver. The Crypto Driver, operating within an HSM or software library, executes the MAC calculation using the same key and algorithm as the transmitter and performs a precise comparison of the MAC values. Serving as the transport channel for integrity verification data, the PDU Router (PduR) ensures that secured PDUs received from the communication bus are accurately routed to the SecOC module.

SecOC 模块从 PduR 接收到完整的安全 PDU。此 PDU 在传输过程中可能已因电磁干扰（意外）或恶意攻击（故意）而发生改变。SecOC 根据预定义的、与发送端对称的格式，精确地解析 PDU。SecOC 将解析出的认证数据与新鲜度值，按照与发送端完全相同的顺序和格式进行拼接。此步骤的准确性至关重要，任何格式差异都将导致后续计算失败。SecOC 调用 Csm

的 VerifyMac 服务。执行完整性校验 Csm 将请求派发给 Crypto 驱动。Crypto 驱动用指定的密钥和算法，对 DataPtr 指向的数据块进行计算，生成本地 MAC。将本地 MAC 与接收到的 MAC 进行恒定时间的逐位比较，以防止时序旁路攻击。校验成功（MAC 完全匹配）：Csm 返回 CSM_OK。从概率学上（概率极高）证明，从发送方生成 MAC 到接收方验证 MAC 的整个过程中，认证数据和新鲜度值都未被修改。SecOC 判定数据完整，将认证数据剥离并传递给上层 COM 模块。校验失败（MAC 不匹配）：Csm 返回 CSM_E_MAC_INVALID。技术含义：数据在传输过程中一定发生了改变。SecOC 立即丢弃整个 PDU。这是保障安全的关键措施，防止不完整或恶意的数据影响 ECU 功能。

The SecOC module receives the complete secured PDU from the PduR. This PDU may have been altered during transmission due to electromagnetic interference (unintentional) or malicious attacks (intentional). SecOC parses the PDU precisely according to a predefined format that is symmetrical with the transmitter. It then concatenates the parsed authentication data and freshness value in the exact same sequence and format as used by the transmitter. The accuracy of this step is critical, as any formatting discrepancy will cause subsequent calculations to fail. SecOC invokes the Csm's VerifyMac service to perform the integrity check. Csm dispatches the request to the Crypto Driver, which uses the specified key and algorithm to compute a local MAC for the data block pointed to by DataPtr. The driver then performs a constant-time, bit-wise comparison between the local MAC and the received MAC to prevent timing side-channel attacks. If the comparison succeeds (MACs match exactly), Csm returns CSM_OK. This indicates with extremely high probability that neither the authentication data nor the freshness value has been modified between MAC generation by the sender and verification by the receiver. SecOC then determines the data is intact, strips off the authentication data, and forwards it to the upper-layer COM module. Conversely, if the comparison fails (MAC mismatch), Csm returns CSM_E_MAC_INVALID. This technically signifies that the data has definitely been changed during transmission. SecOC immediately discards the entire PDU as a crucial security measure to prevent incomplete or malicious data from affecting ECU functionality.

4 防御重放攻击 PROTECTION AGAINST REPLAY ATTACKS

知从科技可以为客户提供 PROTECTION AGAINST REPLAY ATTACKS 完整方案，并可针对项目特定需求和模块定制开发，实现安全特性

ZC can provide customers with a complete Secure Update solution and can customize development for specific project requirements and hardware modules, implementing secure upgrade features including:

重放攻击的防御，核心不在于防止报文被记录，而在于使接收方能够识别并拒绝这些被重复发送的旧报文。SecOC 通过引入和管理新鲜度值 来实现这一目标。新鲜度值是一个由发送方生成、并与受保护数据关联的、单调变化的数值。

The defense against replay attacks does not primarily focus on preventing messages from being recorded, but rather on enabling the receiver to identify and reject these retransmitted old messages. SecOC achieves this goal by introducing and managing a Freshness Value. This value is a monotonically varying number generated by the transmitter and associated with the protected data.

发送端：获取新鲜度值：当 SecOC 需要保护一个 PDU 时，它首先向 FVM 请求当前的新鲜度值。SecOC 将此新鲜度值与认证数据一起，用于计算 MAC。这意味着 MAC 不仅依赖于数据，也依赖于这个动态变化的新鲜度值。SecOC 将认证数据、MAC 和可能需要传输的部分新鲜度值组装成安全 PDU 并发送。发送成功后，FVM 会立即更新其新鲜度值状态（如将计数器递增）。这是防御重放的关键一步，确保了下一个报文将使用一个更新的值。

At the transmitter side, the SecOC module first requests the current freshness value from the FVM when a PDU requires protection. It then incorporates this freshness value with the authentication data to compute the MAC, meaning the cryptographic tag depends not only on the data but also on this dynamically changing parameter. Subsequently, SecOC assembles the authentication data, the MAC, and potentially a partial freshness value into a secured PDU for transmission. Crucially, upon successful transmission, the FVM immediately updates its freshness value state (e.g., by incrementing the counter), which is essential for preventing replay attacks by ensuring subsequent messages utilize an updated value.

接收端：验证报文的“新鲜度”SecOC 从接收到的 PDU 中解析出认证数据和新鲜度值。FVM 将接收到的新鲜度值与内部维护的预期值 和接受窗口 进行比较。新鲜度验证成功：SecOC 才会继续执行 MAC 验证（检查真实性和完整性）。新鲜度验证失败：SecOC 立即丢弃该 PDU，并跳过计算量更大的 MAC 验证。这既是安全措施，也是性能优化。

Receiver Side: Verifying Message Freshness.The SecOC module parses the authentication data and the freshness value from the received PDU. The FVM then compares the received freshness value against its internally maintained expected value and acceptance window. If the freshness verification is successful, SecOC proceeds to perform the subsequent MAC verification, thereby checking both authenticity and integrity. Conversely, if the freshness verification fails, SecOC immediately discards the PDU and skips the more computationally intensive MAC verification. This approach serves both as a critical security measure and a performance optimization.

MCU 端的信息安全是汽车整车信息安全体系中的重要环节：

Cybersecurity on the MCU side is a crucial part of the overall vehicle Cybersecurity system:

- 安全启动（SecureBoot）对用户定义的 Flash 中关键程序的数据完整性和真实性进行验证，可以有效防止攻击者恶意篡改软件；
  Secure Boot verifies the integrity and authenticity of key programs in user-defined Flash, effectively preventing attackers from maliciously tampering with software.
- 安全诊断（SecureDiagnostic）确保了应用数据不会被第三方获取，避免信息泄露；
  Secure Diagnostic ensures that application data cannot be accessed by third parties, preventing information leaks.
- 安全升级（SecureUpdate）保证授权软件才可被控制器使用，搭配安全启动功能，可有效避免非官方程序被控制器执行；
  Secure Update ensures that only authorized software can be used by the controller, and when paired with Secure Boot, it can effectively prevent the execution of unofficial programs by the controller.
- 安全通信（SecOC）可有效确保通信数据安全，防止行车过程中通信数据被攻击篡改导致危险事故；
  Secure Communication (SecOC) can effectively ensure the security of communication data, preventing data tampering during driving that could lead to dangerous accidents

- 安全调试（SecureDebug）防止控制器内部安全数据被非法导出修改；
  Secure Debug prevents illegal export and modification of internal security data in the controller.
- 安全存储（SecureStorage）避免控制器数据内部数据被非法软件获取；
  Secure Storage prevents illegal software from accessing internal data of the controller.
- 安全日志（SecureLog）可以有效记录控制器产生的异常数据，并且防止控制器被异常篡改和信息窃取，保护控制器的信息安全。
  Secure Log can effectively record abnormal data generated by the controller and prevent the controller from being tampered with or information being stolen, protecting the controller's Cybersecurity.

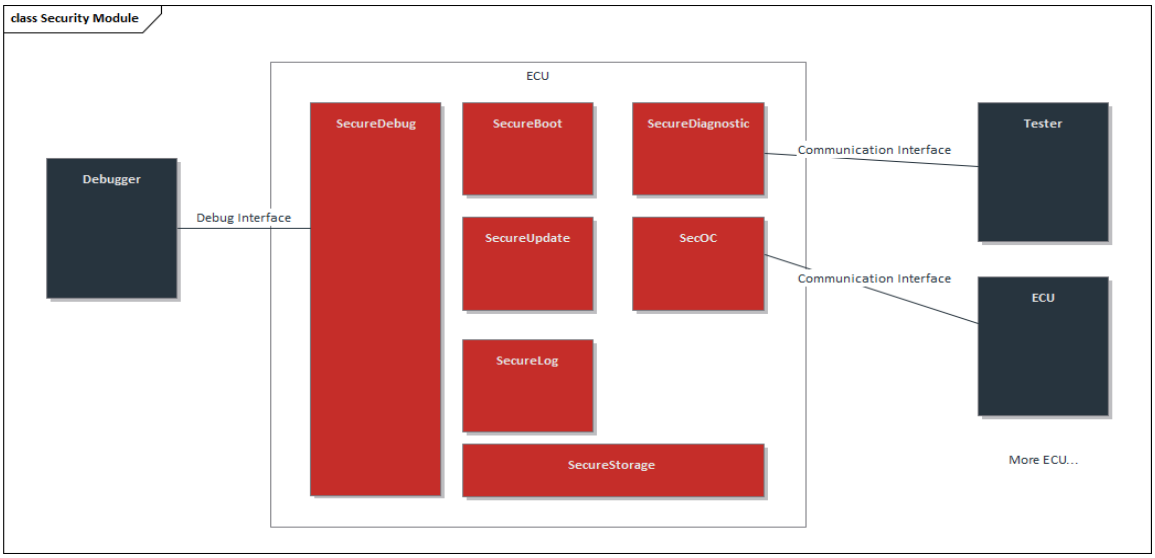


FIGURE2 ECU SECURITY MODULE