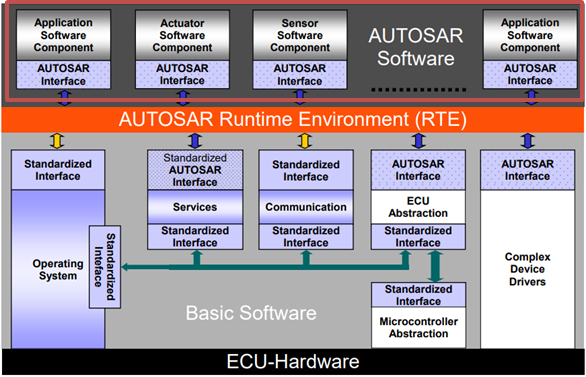
1. BSW 模块 基础软件层
2. CDD(Complex Device Driver or Complex Driver)是复杂设备驱动/复杂驱动的缩写
3. SWC Software [Component](https://so.csdn.net/so/search?q=Component&spm=1001.2101.3001.7020)（软件组件）一般位于AUTOSAR[架构](https://so.csdn.net/so/search?q=%E6%9E%B6%E6%9E%84&spm=1001.2101.3001.7020)的Application层只要了解过AUTOSAR的都知道，AUTOSAR分四层：**Application、RTE、BSW和MCAL**。
4. 
5. SWC 和 CDD 还可以报告在 AUTOSAR 中未标准化的⾃定义安全事件类型 自定义的这块没有BSW
6. 每个 BSW SWS 都列出了由相应模块报告的安全事件类型 没有CDD
7. IdsM缓冲报告的安全事件
8. Security Events (SEv)
9. Qualified Security Events (QSEv 合格安全事件)
10. Intrusion Detection System Reporter (IdsR ⼊侵检测系统报告器)
11. AUTOSAR 不提供 IdsR 的规范
12. IdsM 实例和 IdsR 之间的通信协议在 IdsM 协议规 范[6] 中指定。

传感器

SOC

多个ECU的上报

QSEv)

QSEv)

IdsR（接收多个ECU上报的信息）

与/或序列化QSEv

过滤器

Idsm

安全事件存储器(Sem) 合格安全事件

QSEv)

SEv

SEv

自主定义传输协义

1. 以下⽤例推动了对板载IDS 的要求。

• UC1：收集有关安全事件 (SEv) 的数据 ⽤例 ID 引⽤⾃以下要求。

• UC2：从安全事件数据中过滤合格的板载安全事件 (QSEv)

• UC3：本地存储 QSEv 记录

• UC4：通过SOC连接将QSEv 转发到 ECU

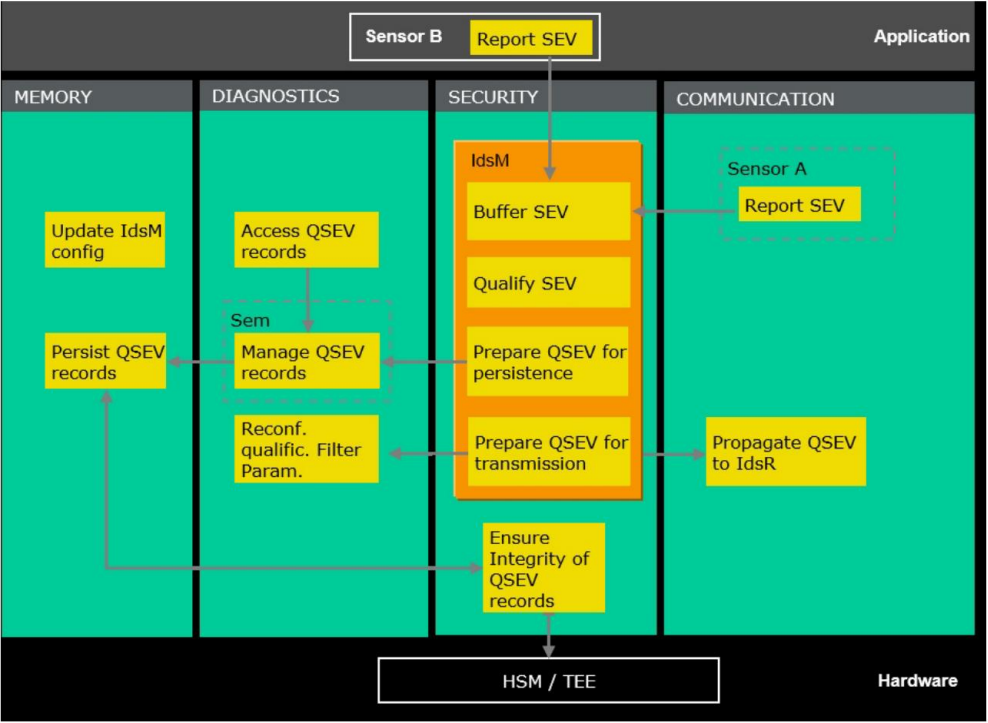
• UC5：提供对本地存储的 QSEv 记录的访问

• UC6：在操作期间重新配置资格参数

• UC7：更新 IdsM 配置 • UC8：保护 IdsM 配置

• UC8：保护 IdsM 配置

• UC9：保护传输中和静⽌



16.

IdsM 的初始化

提供⽤于报告 SEv 的接⼝

IdsM 应为调⽤者缓冲报告的 SEv

配置每个安全事件类型的报告模式和IdsM 实例

为合格的 SEv 提供可配置的过滤器链

提供多个过滤器链

⽀持机器状态过滤器

IdsM 应⽀持 SEv 的抽样

IdsM 应⽀持将多个 SEv 聚合成⼀个 QSEv

IdsM 应仅⽀持转发 SEv，如果它们发⽣得更频繁在可配置的时间间隔内超过可配置的阈值

IdsM 应提供向 SEv 添加时间戳的机制

IdsM 应提供机制让应⽤程序或传感器软件提供时间戳

IdsM 应允许将 QSEv 传输到 IdsR

IdsM 应该能够通过⽤⼾定义的诊断存储器在本地保存 QSEv。⽤⼾定义的诊断存储器应与主诊断存储 器分开，以允许对⽤于存储 QSEv 记录的 NVM 块进行单独的访问控制和保护

（这种⽤⼾定义的诊断 存储器也称为安全事件存储器）应保持QSEv的以下属性：

1. IDS 协议标头，指⽰协议版本和使⽤的协议选项
2. IdsM 实例的标识符
3. 传感器模块实例的标识符
4. 合格的 SEv 的标识符
5. 计数器，指示 SEv 在合格之前报告的频率
6. 时间戳（可选），指⽰ SEv 的时间点是合格的
7. 提供附加信息的上下⽂数据（可选），可由诊断测试仪或任何其他具有访问权限的安全分析实 例在 SOC 中进行评估。
8. 签名（可选），⽀持 IdsM 到SOC的完整性和真实性

将哪个 SEv 报告给 IdsM 应该是可配置的。

IdsM 将哪些资格过滤器应⽤于 SEv 应是可配置的，具体取决于项⽬特定的安全分析，需要应⽤不同 的资格过滤器来验证不同的 SEv 类型

如果 QSEv 应该在本地持久化，它应该是可配置的 根据项⽬特定的安全分

如果将 QSEv 传播到 IdsR，它应该是可配置的

⽀持在运行时重新配置报告模式·

IdsM 应允许替换完整的过滤器链配置

被认为与安全相关的基本软件模块应向 IdsM 报告安全事件。

⽀持检测 QSEv 记录d的操作

IdsM 应⽀持限制传输到 IdsR 的 QSEv 的速率和这些传输消耗的带宽

## 二．AUTOSAR\_RS\_SecurityExtractTemplate

1.安全提取的主要⽬的是将安全事件及其属性定义为⻋辆电⼦设备⼊侵检测系统的输⼊

2. 安全提取可用作交换文件，以在开发过程中以及在车辆已经在现场的维护过程中从多个来源收集安全事件及其属性。

3. 应该可以将与安全相关的事件和相关信息从传感器（实现为硬件或软件）传送到处理这些事件和相 关信息的软件模块。

4. 应该可以将安全事件与安全传感器的数字标识符相关联。

5. 应该可以配置使⽤附加上下⽂数据报告给定的安全事件

6. 应该可以为安全事件链接过滤器，以便多阶段可以实现由⼏种算法组成的过滤

7. 安全提取应⽀持安全限制过滤器的定义事件

8. 作为过滤限定的替代方案，（智能）传感器应能够报告预限定的安全事件，该事件应由 IdsM 直接作为合格的安全事件处理。

8.应该可以配置给定的 ECU 报告给定的安全事件

9. 应该可以配置为给定的通信总线报告给定的安全事件

10. 应该可以配置给定的应⽤程序报告给定的安全事件

11. 安全提取应⽀持给定安全事件的持久性配置。

12.安全提取应⽀持为安全事件配置具有不同详细级别的默认报告模式

13.当安全事件映射到 ECU 或机器时，安全提取应⽀持单独为安全事件定义严重性级别

14. 安全提取应⽀持⼀个或多个 IdsM 实例的可选定义和部分配置，与每个相应的 IdsM 实例 将在⾃适应平台上运行还是在经典平台上运行⽆关

15. 安全提取应⽀持配置 IdsM 实例是否为报告的安全事件提供时间戳信息，如果提供，该时间戳信息是否 为 AUTOSAR 标准化格式

16. 当向报告的安全事件添加时间戳信息时，安全提取应⽀持 IdsM 使⽤的配置格式。时间戳格式可能是 AUTOSAR 标准化的、由其他机构标准化的、公司标准化的或任意定义的

17. 对于 AUTOSAR 经典平台和⾃适应平台，安全提取应⽀持可选配置，即要求 IdsM 实例将⾝份验证信息 （即签名）添加到它发送到⽹络上的所有安全事件消息中。

18. 对于 AUTOSAR 经典平台和⾃适应平台，安全提取模板应描述如何定义 IdsM 实例与其⽹络配置的关 联

19.对于 AUTOSAR 经典平台和⾃适应平台，安全提取模板应描述如何定义 IdsM 实例与其⽹络配置的关 联。

20. IDS 设计通常涉及⻋辆内所有 ECU 的⼦集。该⼦集的每个 ECU 应能够报告单独定义和/或调 整的安全事件。因此，对于 IDS 的开发，Security Extract 需要能够定义属于 IDS 的所有系统部 分以及这些 IDS 系统部分的特定系统级功能。

21. 为了实现 IDS 的分布式开发，多个开发合作伙伴贡献了⼀个描述整个 IDS 设计的安 全提取⽂件。这些贡献者需要能够在 IDS 设计允许的情况下独⽴于其他⼈指定他们 的安全提取部分。

22. 处于系统 (M2) 级别的安全提取必须提供所需的信息，以获取与 ECU 的 IdsM 模块的安全事件相关的 配置参数（M1 级别）。因此，关于 AUTOSAR ⽅法，它同样⽤作诊断提取物或 ECU 提取物。

23. 推导相关ECU-C参数，安全提取应⽀持与 IdsM 模块的安全事件相关的 ECU-C 参数的派⽣。

24. 随着⼊侵检测系统管理器的引⼊，AUTOSAR 还将为现有的 BSW 模块（经典平台）或功能集群（⾃ 适应平台）提供标准化的安全事件。这些标准化的安全事件应使⽤安全提取模板指定，以启⽤⽂档⽣ 成的⾃动处理（单⼀来源原则）。