文件名	入侵要求 检测系统
文档所有者	AUTOSAR
文件责任	AUTOSAR
证件编号976	

文件状态	发表
AUTOSAR 标准的一部分	基础
标准版本的一部分	R21-11

文档更改历史			
日期	版本更改者		描述
2021-11-25	R21-11	AUTOSAR 释放 管理	· 内容不变
2020-11-30	R20-11	AUTOSAR 释放 管理	· 初始发行

免责声明

AUTOSAR 发布的本作品（规范和/或软件实施)及其中包含的材料仅供参考。 AUTOSAR 和为其做出贡献的公司对作品的任何使用概不负责。

本作品中包含的材料受版权和其他类型的知识产权保护。对本作品中包含的材料进行商业利用需要获得此类知识产权的许可。

可以以任何形式或通过任何方式未经任何修改地使用或复制本作品，仅供参考。未经出版商书面许可，不得以任何形式或任何方式出于任何其他目的使用或复制作品的任何部分。

这项工作仅针对汽车应用而开发。它既没有针对非汽车应用进行开发，也没有经过测试。

AUTOSAR 一词和 AUTOSAR 标志是注册商标。

目录

1 文件范围

本文档规定了 AUTOSAR入侵检测系统(IDS)的要求。以下部分概述了 IDS 的元素以及描述该元素的 AUTOSAR 文档。

1.1 分布式板载 IDS 的一般架构

符合 AUTOSAR 标准的板载 IDS 包含以下元素：

- 安全传感器
- 入侵检测系统管理器 (IdsM)
- 安全事件记忆 (Sem)
- 入侵检测系统报告器 (IdsR)

图 1.1显示了分布式板载 IDS 的原理架构。

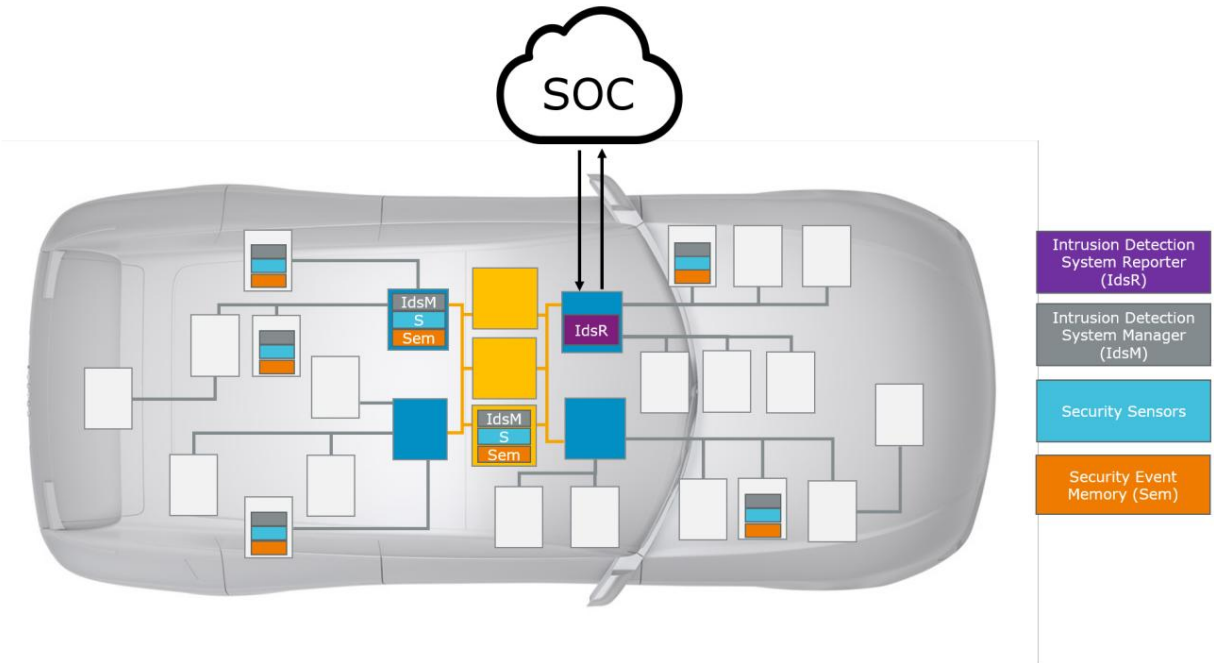

图 1.1:分布式板载 IDS 的架构

以下部分简要介绍了板载 IDS 的元素。

1.2 安全传感器和安全事件

AUTOSAR BSW 模块、CDD 和 SWC 可以充当安全传感器。安全传感器向 IdsM 报告安全事件(SEv) 。 AUTOSAR 标准化了一组可由 AUTOSAR BSW 报告的安全事件类型。每个 BSW SWS 都列出了由相应模块报告的安全事件类型，如 SWS BSW General [1] 中所述。

由 AUTOSAR 标准化的安全事件类型的概述可通过通用定义安全事件[2] 获得。

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。由特定 ECU 报告的安全事件类型的属性可以通过使用安全提取(SecXT) [3]来指定。

1.3 入侵检测系统管理器

IdsM缓冲报告的安全事件。此外，IdsM 将一组连续过滤器应用于报告的 SEv。一组连续的过滤器称为过滤器链。如果 SEv 通过其过滤链，则它们被视为合格安全事件(QSEv)。

根据配置，IdsM 可以

- 将 QSEv 传递到安全事件存储器(Sem)以将其保存在本地
  电子控制单元。
- 和/或序列化QSEv 并将其传输到IdsR。

在本文档中指定了 IdsM 的系统要求。 SWS IdsM CP [4]规定了经典平台 IdsM 的软件要求。 SWS IdsM AP [5]规定了自适应平台 IdsM 的软件要求。

1.4 入侵检测系统报告器

入侵检测系统报告器(IdsR)从不同 ECU 的 IdsM 实例接收 QSEv。 IdsM 实例和 IdsR 之间的通信协议在 IdsM 协议规范[6] 中指定。

IdsR 通常应该进一步丰富接收到的数据，例如使用地理位置。
根据 OEM 的需求，可以将数据传播到SOC ，以便在SIEM解决方案中进行进一步分析。 AUTOSAR 不提供 IdsR 的规范。

2 使用的约定

2.1 文档约定

AUTOSAR 文档中的需求表示遵循指定的表格
在 [TPS_STDT_00078] 中,参见标准化模板,支持可追溯性一章
（[7]）。

[TPS_STDT_00053] 中规定的义务表达的口头形式应
用于指示要求,请参阅标准化模板,支持一章
可追溯性（[7]）。

3 首字母缩略词

3.1 首字母缩略词

首字母缩略词	描述：
过滤链	一组应用于安全事件的连续过滤器入侵检测系统是一种安全控制,可检测
入侵侦测系统	并处理安全事件。
入侵侦测系统 经理	入侵检测系统管理器处理安全事件 由安全传感器报告。
入侵检测系统报告器	入侵检测系统报告器处理从 Idsm 实例接收到的合格安全事件。
安全提取	安全提取指定处理哪些安全事件 通过 IdsM 实例及其配置参数。
安全事件类型	安全事件类型可以通过其安全事件类型来识别 ID。安全事件类型的实例称为安全事件 并共享相同的安全事件类型 ID。
安全事件	板载安全事件是安全事件类型的实例 由 BSW 或 SWC 向 IdsM 报告。
安全事件记忆	用户定义的独立诊断事件存储器 从主要诊断事件存储器。
安全传感器	向 Idsm 报告安全事件的 BSW 或 SWC。
合格的安全事件	通过过滤链的安全事件被视为 合格的安全事件。
安全事件和事件 管理	处理已确认安全事件的流程
安全运营中心	正在分析的安全和领域专家的组织 安全事件并有助于减轻威胁。

表 3.1:首字母缩略词

3.2 缩写

缩写	描述：
身份识别系统	入侵侦测系统
身份证件	入侵检测系统管理器
IdsR	入侵检测系统报告器
SecXT	安全提取
SEv	安全事件
QSEv	合格的安全事件
扫描电镜	安全事件记忆
SIEM	安全事件和事件管理
SOC	安全运营中心

表 3.2：缩写

4 需求规范

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
- 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
- UC9：保护传输中和静止中的 IdsM 数据

用例 ID 引用自以下要求。

图 4.1显示了 IDS 的抽象功能架构。本金分配
的功能元素指的是 CP 和 AP，尽管实际的技术
体系结构不同，如各自 SWS 中所述。该图显示了整体
IDS 的功能元素以及 IdsM 涵盖哪些功能元素。

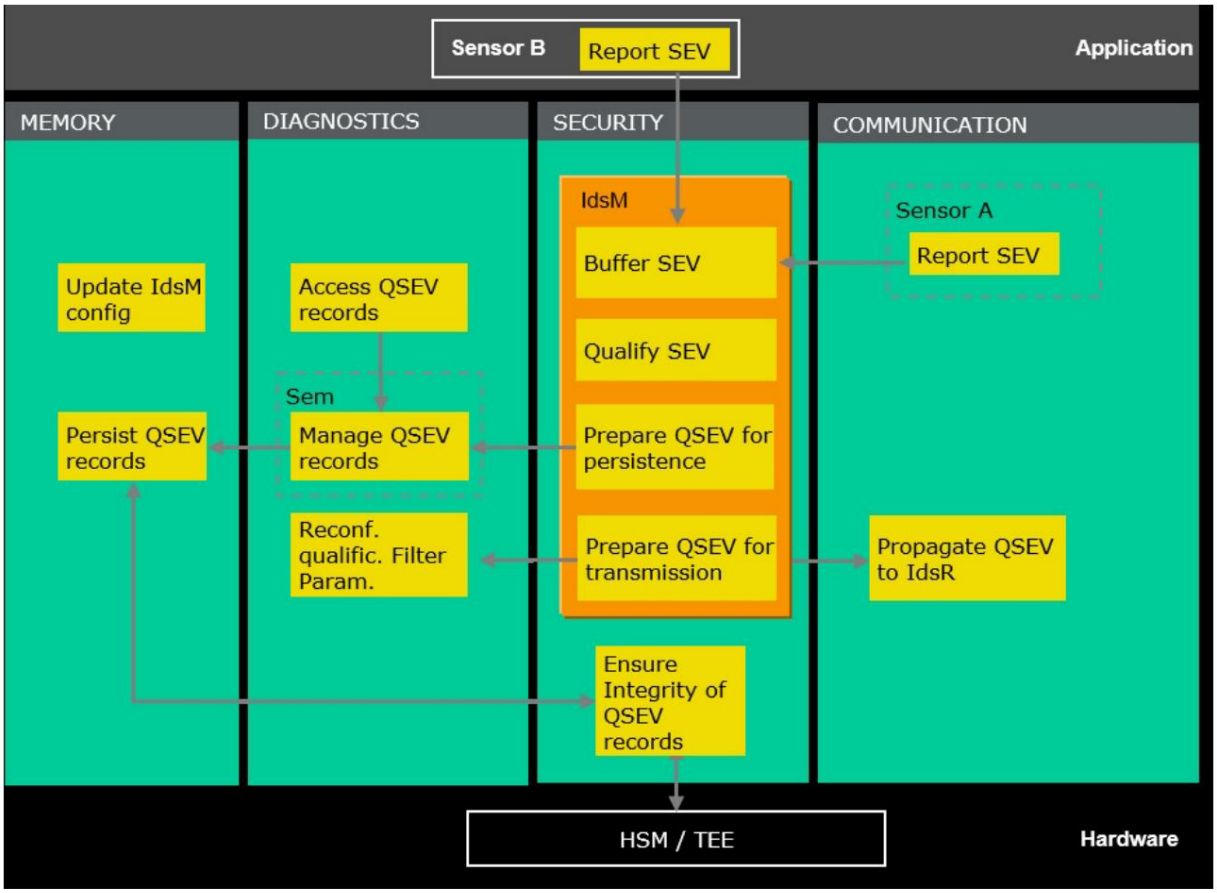

图 4.1:IdsM 的抽象功能元素

4.1 功能要求

4.1.1 初始化

[RS_Ids_00100]{DRAFT} IdsM d的初始化

描述：	IdsM 资格规则应在启动时初始化 IdsM 需要配置信息来执行其操作。因此,此
理由：	信息应在 NVM 开始处理操作之前从 NVM 中恢复并初始化。
依赖关系： -	
用例：	UC8
适用于：	CP、美联社
配套材料：	–

c(RS_BRF_02038)

4.1.2 SEv 报告

[RS_Ids_00200]{DRAFT}提供用于报告 SEv d的接口

描述：	IdsM 应提供用于报告 SEv 的接口。接口应允许报告以下 SEv 属性： · 安全事件类型:唯一标识安全事件类型 · 上下文数据:可用于分析安全性的可选数据 SOC 中的事件。 · 时间戳:传感器提供的可选时间戳。 · 计数:传感器提供的可选计数。
理由：	安全事件可以通过基本软件、复杂设备驱动程序和应用软件报告给 IdsM。
依赖关系： -	
用例：	UC1
适用于：	CP、美联社
配套材料：	–

c(RS_BRF_02038)

4.1.3 报告 Sev 的缓冲

[RS_Ids_00210]{DRAFT} IdsM 应为调用者d缓冲报告的 SEv

描述：	IdsM 应为调用者缓冲报告的 SEv
理由：	IdsM 应为 SEv 传感器缓冲 SEv 和上下文数据,直到 IdsM 完全处理数据。
依赖关系： -	
用例：	UC1
适用于：	CP、美联社
配套材料：	–

c(RS_BRF_02038)

4.1.4 SEv的资格

4.1.4.1 上报方式

[RS_Ids_00310]{DRAFT}配置每个安全事件类型的报告模式和
IdsM 实例d

描述：	IdsM 应支持为IdsM 实例处理的每个安全事件类型配置报告模式。报告模式应包括以下选项：(a) 关闭 SEv 的处理，(b) 丢弃上下文数据，以及 (c) 绕过后续过滤器。
理由：	报告模式允许控制事件是否完全感兴趣以及是否应该进一步处理。
依赖关系： -	
用例：	UC2
适用于：	CP、美联社
配套材料：	–

c(RS_BRF_02038)

报告模式级别	相关行为
离开	IdsM 将丢弃 SEv 而无需进一步处理。
简短的	如果SEv已被报告包括上下文数据，IdsM 应丢弃上下文数据以进行进一步处理、传输和存储。
详细的	如果SEv已被报告包括上下文数据，IdsM 应保留上下文数据以用于 QSEv 的潜在传输或持久化。
Brief_BYPASSING_FILTERS IdsM 应在没有上下文的情况下报告或保留SEv 无需进一步应用任何过滤器链的数据。	
从 TAILED_BYPASSING_FILTERS	IdsM 应使用上下文数据（如果由传感器提供）报告或持久化SEv ，而无需进一步应用任何过滤器链。

表 4.1：报告模式过滤器值

4.1.4.2 过滤器链

[RS_Ids_00300]{DRAFT}为合格的 SEv d提供可配置的过滤器链

描述：	IdsM 应通过对报告的 SEv 应用可配置的过滤器链来支持 SEv 的鉴定。一个配置的过滤器序列称为过滤器链。
理由：	并不总是应将单个 SEv 作为合格的安全事件直接处理。 根据项目特定的安全分析，一个或多个过滤器可以应用于报告的 SEv。如果一个 SEv 通过了所应用过滤器链的所有过滤器，则该事件是合格的（即，它是一个QSEv）。然后将传输和/或保留该事件。

依赖关系：-	
用例：	UC2
适用于：	CP、美联社
配套 材料：	–

c(RS_BRF_02038)

[RS_Ids_00301]{DRAFT}提供多个过滤器链d

描述：	IdsM 应支持创建多个过滤器链和 将给定安全事件类型的每个 SEv 单独分配给 每个 IdsM 实例的特定过滤器链。
理由：	不同的安全事件定义可能需要不同的过滤器链。
依赖关系：-	
用例：	UC2
适用于：	CP、美联社
配套 材料：	–

c(RS_BRF_02038)

4.1.4.3 机器状态过滤器

[RS_Ids_00320]{DRAFT}支持机器状态过滤器

描述：	IdsM 应支持 ECU/机器状态依赖的 SEv 处理。
理由：	某些事件定义可能仅在某些状态下相关，并且应该 在其他州被忽略。
依赖关系：-	
用例： UC2	
适用于： CP、AP	
配套 材料：	–

c(RS_BRF_02038)

4.1.4.4 采样滤波器

[RS_Ids_00330]{DRAFT}支持采样过滤器

描述：	IdsM 应支持 SEv 的抽样。
理由：	以非常高的频率发生的安全事件的数据速率可以 被减少。
依赖关系： -	
用例：	UC2
适用于：	CP、美联社
配套 材料：	–

c(RS_BRF_02038)

4.1.4.5 聚合过滤器

[RS_Ids_00340]{DRAFT}支持聚合过滤器d

描述：	IdsM 应支持将多个 SEv 聚合成一个 QSEv 表示聚合 SEv 发生的频率。
理由：	事件聚合可以减少发生在 高频率，同时保持事件总数的信息 发生。
依赖关系： -	
用例：	UC2
适用于：	CP、美联社
配套 材料：	–

c(RS_BRF_02038)

4.1.4.6 阈值过滤器

[RS_Ids_00350]{DRAFT}支持阈值过滤器d

描述：	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。
理由：	SEvs 可以通过正常操作定期触发，这不应该 被报告，然而，偏离正常频率可能表明 应该报告的事件。
依赖关系： -	
用例：	UC2
适用于：	CP、美联社

配套 材料：	–

c(RS_BRF_02038)

4.1.5 事件时间戳

[RS_Ids_00502]{DRAFT}事件时间戳d

描述：	IdsM 应提供向 SEv 添加时间戳的机制
理由：	事件分析可能需要事件发生的时间。
依赖关系： -	
用例：	UC1
适用于：	CP、美联社
配套 材料：	–

c(RS_BRF_02038)

[RS_Ids_00503]{DRAFT}时间戳源d

描述：	IdsM 应提供机制让应用程序或传感器软件提供 时间戳。
理由：	项目特定的应用程序或传感器可能会提供更准确的时间戳
依赖关系： -	
用例：	UC1
适用于：	CP、美联社
配套 材料：	–

c(RS_BRF_02038)

4.1.6 QSEv 向 IdsR 的传播

[RS_Ids_00510]{DRAFT} IdsM 应允许将 QSEv 传输到 IdsR d

描述：	IdsM 应允许使用 IDS 协议传输QSEv和上下文数据 [6]独立于底层总线技术。

理由：	QSEv 由 ECU 报告,这些 ECU 可以通过各种总线系统连接到 E/E 架构的其余部分。 IdsR可以将事件中继到 SOC。
依赖关系： -	
用例：	UC4
适用于：	CP、美联社
配套材料：	–

c(RS_BRF_02038)

4.1.7 QSEv 的持久化

[RS_Ids_00400]{DRAFT}保留 QSEv 记录d

描述：	IdsM 应该能够通过用户定义的诊断存储器在本地保存 QSEv。用户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。 （这种用户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： · IDS 协议标头,指示协议版本和使用的协议选项 · IdsM 实例的标识符 · 传感器模块实例的标识符 · 合格的 SEv 的标识符 · 指示 SEv 在报告之前报告的频率的计数器 合格的 · 时间戳（可选）,指示 SEv 的时间点 合格 · 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。 · 签名（可选）,支持 IdsM 到SOC的完整性和真实性
理由：	可以在稍后的时间点访问持久性 QSEv 以进行分析,而不依赖于例如网络连接。
依赖关系： -	
用例：	UC3、UC5
适用于：	CP、美联社
配套材料：	–

c(RS_BRF_02038)

4.1.8 配置

[RS_Ids_00600]{DRAFT} SEv d的配置

描述：	将哪个 SEv 报告给 IdsM 应该是可配置的。
理由：	根据项目特定的安全分析，一些SEv被认为是相关的，而其他 SEv 被认为是不相关的。为了避免传感器模块对 IdsM 的不必要调用，该属性应可根据每个 IdsM 实例的安全事件类型进行配置。
依赖关系： –用例： UC1适	
用于： CP、AP支持材料：	
	–

c(RS_BRF_02038)

[RS_Ids_00610]{DRAFT} SEv d资格筛选器的配置

描述：	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。
理由：	
依赖关系： -	
用例：	UC1
适用于：	CP、美联社
配套材料：	–

c(RS_BRF_02038)

[RS_Ids_00620]{DRAFT}配置 QSEv d的持久性处理

描述：	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
理由：	析和可用资源（例如 NVM）决定是否持久化 QSEv。相应的属性（例如缓冲区的大小）需要是可配置的。
依赖关系： -	
用例：	UC3
适用于：	CP、美联社
配套材料：	–

c(RS_BRF_02038)

[RS_Ids_00630]{DRAFT} QSEv d的传播处理配置

描述：	如果将 QSEv 传播到 IdsR,它应该是可配置的
理由：	取决于项目特定的安全分析和可用资源 将做出关于 QSEv 传播的决定（例如,机载频段）。 相应的属性（例如 QSEv 的 I-PDU)需要是可配置的。
依赖关系： -	
用例：	UC6
适用于：	CP、美联社
配套 材料：	–

c(RS_BRF_02038)

4.1.9 重新配置

[RS_Ids_00700] 运行时重新配置d

描述：	支持在运行时重新配置报告模式
理由：	应该可以在运行期间改变 SEv 的报告模式。这 IdsM 应提供一个可供诊断程序使用的接口。
依赖关系： -	
用例：	–
适用于：	CP、美联社
配套 材料：	–

c(RS_BRF_02038)

4.1.10 IdsM 配置更新

[RS_Ids_00710] 更换完整的过滤器链配置d

描述：	IdsM 应允许替换完整的过滤器链配置。
理由：	在生产线编程结束、车间中的 ECU 初始化等情况下,或 通过OTA推出新的更新应该可以更换完整的过滤器 链配置
依赖关系： -	
用例： UC7	
适用于： CP、AP	
配套 材料：	实际替换/更新可以是逻辑块的标准软件更新 由 FBL 或 OTA 执行。

c(RS_BRF_02038)

4.1.11 安全相关要求

4.1.11.1 基本软件安全事件类型

[RS_Ids_00810] 基本软件安全事件d

描述：	被认为与安全相关的基本软件模块应向 IdsM 报告安全事件。
理由：	基本软件模块是否被视为与安全相关,由专门的 AUTOSAR 工作组讨论和决定。安全事件类型的规范是根据所涉及的 AUTOSAR 成员的需要完成的。
依赖关系： -	
用例：	UC1
适用于：	CP、美联社
配套材料：	–

c(RS_BRF_02038)

4.1.11.2 IdsM 安全事件类型

[RS_Ids_00820] IdsM 安全事件d

描述：	IdsM 应在以下情况下报告 IdsM 特定安全事件： · 如果超出 IdsM 流量限制 · 如果 IdsM 上下文缓冲区已用尽 · 如果 IdsM 事件缓冲区已用尽
理由：	IdsM 应提供支持他自己的安全事件的方法
依赖关系： -	
用例：	UC1
适用于：	CP、美联社
配套材料：	–

c(RS_BRF_02038)

4.1.11.3 传输的 QSEv 的 End2End 真实性

[RS_Ids_00505]{DRAFT} QSEvs d的真实性

描述：	IdsM 应支持签署 QSEv,包括所有可选数据（例如,上下文数据、时间戳）。
理由：	可以保证事件的真实性。
依赖关系： -	
用例：	UC9
适用于：	CP,美联社
配套材料：	–

c(RS_BRF_02038)

4.1.11.4 存储的 QSEv 记录的真实性

[RS_Ids_00430]{DRAFT}支持检测 QSEv 记录d的操作

描述：	内存堆栈应该能够选择性地检测持久化的操作 QSEv 记录。如果检测到对 QSEv 记录的操作,则内存堆栈应引发安全事件。
理由：	根据 OEM 的安全分析,可能需要检测操纵 QSEv 记录。
依赖关系： -	
用例：	UC7
适用于：	CP,美联社
配套材料：	–

c(RS_BRF_02038)

4.1.11.5 可用性

[RS_Ids_00511]{DRAFT}限制事件率和流量d

描述：	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。
理由：	限制由 IDS 引起的网络总线负载。
依赖关系： -	
用例：	UC9
适用于：	CP,美联社
配套材料：	–

c(RS_BRF_02038)

4.2 非功能性要求（质量）

5 需求追踪

下表引用了[8]中指定的功能并链接到这些功能的实现。

特征	描述	满意
[RS_BRF_02038] AUTOSAR 应支持入侵检测系统 (IDS) 安全控制		[RS_Ids_00100] [RS_Ids_00200] [RS_Ids_00210] [RS_Ids_00300] [RS_Ids_00301] [RS_Ids_00310] [RS_Ids_00320] [RS_Ids_00330] [RS_Ids_00340] [RS_Ids_00350] [RS_Ids_00400] [RS_Ids_00430] [RS_Ids_00502] [RS_Ids_00503] [RS_Ids_00505] [RS_Ids_00510] [RS_Ids_00511] [RS_Ids_00600] [RS_Ids_00610] [RS_Ids_00620] [RS_Ids_00630] [RS_Ids_00700] [RS_Ids_00710] [RS_Ids_00810] [RS_Ids_00820]

6 参考文献

[1] 基本软件模块通用规范
AUTOSAR_SWS_BSWGeneral

[2] 用于定义 AUTOSAR 的标准化 M1 模型
AUTOSAR_MOD_GeneralDefinitions

[3] 安全提取模板
AUTOSAR_TPS_SecurityExtractTemplate

[4] 入侵检测系统管理器规范
AUTOSAR_SWS_IntrusionDetectionSystemManager

[5] 自适应平台入侵检测系统管理器规范
AUTOSAR_SWS_AdaptiveIntrusionDetectionSystemManager

[6] 入侵检测系统协议规范
AUTOSAR_PRS_IntrusionDetectionSystem

[7] 标准化模板
AUTOSAR_TPS_标准化模板

[8] AUTOSAR 特性要求
AUTOSAR_RS_Features