文件名	入侵规范 检测系统管理器 自适应平台
文档所有者	AUTOSAR
文件责任	AUTOSAR
证件编号978	

文件状态	发表
AUTOSAR 标准的一部分	自适应平台
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	· 内容没有变化
2020-11-30	R20-11	AUTOSAR 释放 管理	· 初始发行

免责声明

目录

1 简介及功能概述

本规范描述了 AUTOSAR 自适应功能集群 IdsM 的功能、API 和配置。

2 首字母缩略词

2.1 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。
安全事件记忆	用户定义的诊断事件存储器，与 主诊断事件存储器。
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 2.1：首字母缩略词

2.2 缩写

缩写	描述：
做过	根据统一诊断服务的数据标识符
故障诊断码	诊断故障代码
足球俱乐部	功能集群
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
SWCL	软件集群

表 2.2：缩写

3 相关文档

本文档是 AUTOSAR IDS 规范的一部分,涵盖了自适应平台的软件规范。 IDS规范的其他方面,请参考以下文档:

·入侵检测系统的系统要求规范（RS IDS) [1]:指定 IDS 系统要求。

·合格安全事件传输的协议要求 (PRS IDS) [2]:指定安全事件传输之间的通信协议。

·安全提取模板[3]:指定安全提取。

3.1 输入文件及相关标准规范

[1] 入侵检测系统要求
AUTOSAR_RS_IntrusionDetectionSystem

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

[3] 安全提取模板
AUTOSAR_TPS_SecurityExtractTemplate

[4] 自适应平台核心规范
AUTOSAR_SWS_AdaptivePlatformCore

[5] 密码学规范
AUTOSAR_SWS_密码学

3.2 进一步适用规范

AUTOSAR 提供了一个核心规范[4] ,它也适用于入侵检测系统管理器。本规范的“所有功能集群的一般要求”一章应被视为实施入侵检测系统管理器的附加和必需规范。

4 约束和假设

没有已知的限制和假设。

4.1 已知限制

没有已知的限制。

5 对其他功能集群的依赖

可以使用诊断服务访问通过 IdsM API 生成的安全事件。发送到 IdsR 的安全事件可以使用在 FC Crypto 中建模的密钥进行签名。

5.1 协议层依赖

通过 IdsM API 生成的安全事件可以使用 PRS IDS [2] 中指定的协议传输到 IdsR。

6 需求追踪

下表引用了系统要求中指定的要求
入侵检测系统 (RS IDS) [1]规范和实现的链接
这些。请注意，如果“满足于”列对于特定要求为空，则此
表示本文件不满足此要求。

要求	描述	满意
[RS_Ids_00100]	IdsM 的初始化	[SWS_AIDSM_00001] [SWS_AIDSM_00002]
[RS_Ids_00200]	提供报表接口 SEv	[SWS_AIDSM_01201]
[RS_Ids_00300]	提供可配置的过滤器链 对于符合条件的 SEv	[SWS_AIDSM_00301] [SWS_AIDSM_00303] [SWS_AIDSM_00304] [SWS_AIDSM_00305] [SWS_AIDSM_00306]
[RS_Ids_00301]	提供多个过滤器链	[SWS_AIDSM_00301]
[RS_Ids_00310]	配置每个报告模式 安全事件类型和 IdsM 实例	[SWS_AIDSM_00101] [SWS_AIDSM_00201] [SWS_AIDSM_00202]
[RS_Ids_00320]	支持机器状态过滤器	[SWS_AIDSM_00401]
[RS_Ids_00330]	支持采样过滤器	[SWS_AIDSM_00501] [SWS_AIDSM_00502]
[RS_Ids_00340]	支持聚合过滤器	[SWS_AIDSM_00600] [SWS_AIDSM_00601] [SWS_AIDSM_00602] [SWS_AIDSM_00603] [SWS_AIDSM_00604] [SWS_AIDSM_00605] [SWS_AIDSM_00606] [SWS_AIDSM_00607]
[RS_Ids_00350]	支持阈值过滤器	[SWS_AIDSM_00701] [SWS_AIDSM_00702]
[RS_Ids_00400]	保留 QSEv 记录	[SWS_AIDSM_01301]
[RS_Ids_00502]	事件时间戳	[SWS_AIDSM_00801]
[RS_Ids_00503]	时间戳源	[SWS_AIDSM_00802] [SWS_AIDSM_00803] [SWS_AIDSM_00804] [SWS_AIDSM_00805] [SWS_AIDSM_00806] [SWS_AIDSM_00807]
[RS_Ids_00505]	QSEv 的真实性	[SWS_AIDSM_01001] [SWS_AIDSM_01002]
[RS_Ids_00510]	IdsM 应允许传输 QSEv 到 IdsR	[SWS_AIDSM_00901] [SWS_AIDSM_00902]
[RS_Ids_00511]	限制事件率和流量	[SWS_AIDSM_01101] [SWS_AIDSM_01103] [SWS_AIDSM_01104]
[RS_Ids_00610]	资质配置 SEv 过滤器	[SWS_AIDSM_00302]
[RS_Ids_00700]	运行时重新配置[SWS_AIDSM_01302]	[SWS_AIDSM_01303]
[RS_Ids_00810]	基本软件安全事件	[SWS_IdsM_91015]

要求	描述	满意
[RS_Ids_00820]	IdsM 安全事件	[SWS_AIDSM_01401] [SWS_AIDSM_01402] [SWS_AIDSM_01403]

7 功能规格

本章规定了自适应平台的 IdsM 的功能行为。

7.1 功能集群生命周期

使用 ara::core::Intitialize 和 ara::core::Deinitialize,应用程序可以初始化和取消初始化其 ara::idsm 库。

[SWS_AIDSM_00001]{DRAFT} d当调用 ara::core::Intitialize 时,IdsM 应读入清单信息并准备必要的访问结构,以从应用程序生成事件。c(RS_Ids_00100)访问结构可以涵盖之间的通信通道应用程序进程和堆栈进程（如果有)或 IdsM 所需的其他资源。

[SWS_AIDSM_00002]{DRAFT} d当调用 ara::core::Deinitialize 时,IdsM 应关闭所有获取的句柄并释放所有访问结构。c(RS_Ids_00100)

应用程序不应在 ara::core::Inti tialize 之前或 ara::core::Deinitialize 之后调用 IdsM 的任何 API。

7.2 事件生成

SWCL和FC可以使用IdsM API生成新的安全事件。可以由SWCL生成的所有事件类型都在清单中配置并链接到 SWCL 的端口原型。生成新事件涉及三个步骤：

1.使用短名称路径构造一个InstanceSpecifier对象
PortPrototype 引用事件类型作为参数。

2.通过传递Instance构造一个ara::idsm::EventReporter对象
说明符。

3. 调用ara::idsm::EventReporter::ReportEvent函数
ara::idsm::EventReporter对象。

使用ara::idsm::EventReporter::ReportEvent函数,应用程序可以选择提供时间戳、计数器和/或上下文数据。

[SWS_AIDSM_00101]{DRAFT}安全事件类型d 每个安全事件类型由模型中的一个SecurityEventDefinition对象表示,并应由模型参数SecurityEventDefinition 唯一标识。 id.c(RS_Ids_00310)

7.3 上报方式

[SWS_AIDSM_00201]{DRAFT}报告模式dIdsM应确定默认值
来自SecXT模型参数Securi tyEventContextProps.defaultReportingMode.c(RS_Ids_00310)的每个报告
的SEv的报告模式

[SWS_AIDSM_00202]{DRAFT}报告模式选项dIdsM应根据表7.1.c （ RS_Ids_-

00310)

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应从进一步丢弃上下文数据 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供潜在的 QSEv的传输或持续存在。
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应使用上下文数据报告或持久化SEv （如果由传感器提供)无需进一步应用 任何过滤器链。

表 7.1:报告模式过滤器值

7.4 过滤链

过滤器链使用SecXT模型元素SecurityEventFilterChain 进行配置。

[SWS_AIDSM_00301]{DRAFT}过滤器链选择d当报告一个SEv时，
IdsM应应用映射到SecurityEventDefinition的过滤器链
通过SecurityEventContextMapping.c(RS_Ids_00300 , RS_-
ids_00301)

[SWS_AIDSM_00302]{DRAFT}过滤器链评估dIdsM应在评估报告模式后评估过滤器链。c(RS_Ids_00610)

[SWS_AIDSM_00303]{DRAFT}可能的过滤器d每个过滤器链可能包含
以下过滤器：

- 机器状态过滤器
- 转发每n个过滤器
- 聚合过滤器

· 阈值过滤器

c(RS_Ids_00300)

[SWS_AIDSM_00304]{DRAFT}过滤器链配置dEach 过滤器可以通过在model.c(RS_Ids_00300)中的SecurityEventFilter Chain对象处聚合相应的过滤器对象来激活

[SWS_AIDSM_00305]{DRAFT}过滤器链顺序dIdsM应评估所有激活的
按 MachineState 过滤器、Forward-Every-nth 过滤器、聚合过滤器的顺序过滤，
阈值过滤器.c(RS_Ids_00300)

[SWS_AIDSM_00306]{DRAFT}删除 SEvs dIf评估一个过滤器
导致丢弃SEv， IdsM不应评估任何额外的过滤器。c(RS_Ids_-
00300)

在成功评估配置的过滤器链后，我们定义安全事件
合格（QSEv）。

7.4.1 机器状态过滤器

[SWS_AIDSM_00401]{DRAFT}机器状态过滤器dIf IdsM评估机器
状态过滤器和当前机器状态等于引用的状态之一
SecurityEventStateFilter.blockIfStateActiveAp，则IdsM应丢弃
SEv.c(RS_Ids_00320)

7.4.2 采样滤波器

[SWS_AIDSM_00501]{DRAFT}采样过滤器d如果 IdsM评估SEv 的采样过滤器， IdsM将删除所有SEv ，但每个SecurityEventDef 的每第 n 个，其中 n 由SecurityEventOneEveryNFilter.nc(RS_Ids_-

00330)

一个实现通常会为每个SecurityEventDefinition维护一个计数器，当采样评估给定类型的SEv时，该计数器将递增
筛选。如果计数器等于 n，则SEv不会被丢弃并且计数器重置为 0。

[SWS_AIDSM_00502]{DRAFT}采样过滤器初始化dIdsM应初始化
SEv的采样过滤器，以便转发每个SecurityEventDefinition接收到的第一个SEv。c (RS_Ids_00330)示例：
SecurityEventOneEveryNFil ter.n对于某个事件类型设置为 3，然后SEvs 1, 4, 7, ... 将被转发

IdsM （1 描述重置后报告的第一个SEv ）。

7.4.3 聚合过滤器

在配置的时间间隔内发生的给定类型的所有SEv被聚合到
一个带有附加计数器信息的SEv ,该信息表明多久
事件发生在时间间隔内。

[SWS_AIDSM_00600]{DRAFT}聚合过滤器的配置

给定类型应聚合.c(RS_Ids_00340)

[SWS_AIDSM_00601]{DRAFT}间隔 d 期间无事件转发聚合过滤器不应在聚合间隔内转发（即,到下一个过滤器)任何传入的SEv。c (RS_Ids_00340)

在每个聚合间隔结束时,聚合过滤器应为每个安全事件类型实现以下逻辑：

[SWS_AIDSM_00602]{DRAFT}间隔结束:没有事件dIf没有相同的SEv
在过去的聚合时间间隔内聚合过滤器已接收到事件类型，
不应采取任何行动。c(RS_Ids_00340)

[SWS_AIDSM_00603]{DRAFT}间隔结束:一个或多个事件dIf 一个或
聚合过滤器接收到更多相同事件类型的SEv
过去的聚合间隔,一个SEv应该被转发到 chain.c 中的下一个过滤器
(RS_Ids_00340)

[SWS_AIDSM_00604]{DRAFT}间隔结束:计数dIf SEv转发到
过滤器链中的下一个过滤器， SEv的计数参数应等于
聚合过滤器处理的给定事件类型的所有SEv的所有计数参数
在过去的时间间隔.c(RS_Ids_00340)

[SWS_AIDSM_00605]{DRAFT}间隔结束:第一个上下文数据d如果 SEv是
转发到过滤器链中的下一个过滤器,如果SecurityEventAggregation Filter.contextDataSource等于
IDSM_FILTERS_CTX_USE_FIRST,则
上下文数据应等于给定类型的SEv的第一个上下文数据，
在过去的时间间隔内在聚合过滤器处收到。c(RS_Ids_00340)

[SWS_AIDSM_00606]{DRAFT }间隔结束:最后一个上下文数据已收到的给定类型

在过去时间间隔的聚合过滤器中。c(RS_Ids_00340)

[SWS_AIDSM_00607]{DRAFT}间隔结束:时间戳dIf转发SEv
到过滤器链中的下一个过滤器,时间戳应取自相同的SEv
上下文数据来自哪个（通过SecurityEventAggregation Filter.contextDataSource 配置）.c(RS_Ids_00340)

请注意,如果SecurityEventAggregationFilter.contextDataSource
等于 IDSM_FILTERS_CTX_USE_LAST,则报告或存储的QSEv将包含在配置的时间间隔内创建的最后一个SEv的
上下文数据,但
在配置的时间间隔内创建的第一个SEv的时间戳。

7.4.4 阈值过滤器

[SWS_AIDSM_00701]{DRAFT}事件低于阈值d 阈值
如果所有SEv的计数参数的总和过滤器应丢弃给定类型的SEv
当前阈值间隔内由阈值过滤器处理的给定类型小于配置的参数SecurityEventThresholdFilter。

thresholdNumber.c(RS_Ids_00350)

[SWS_AIDSM_00702]{DRAFT} Event Forwarding Above Threshold dThe thresh old filter 将转发给定类
型的SEv ,如果
在当前阈值间隔内由阈值过滤器处理的给定类型是
等于或大于配置的参数SecurityEventThresholdFilter.thresholdNumber.c (RS_Ids_00350)

7.4.5 资格

在SEv成功通过过滤器链的最后一个配置的过滤器后,它是
被认为是QSEv。根据配置， QSEv可以传输到
IdsR 和/或在本地持续存在。

7.5 时间戳

时间戳是可选的,可以以不同的方式提供给IdsM 。

[SWS_AIDSM_00801]{DRAFT}时间戳是可选的dIf IdsmInstance。
timestampFormat未设置， IdsM不得将时间戳添加到QSEv并且应
忽略通过事件报告接口的时间戳参数提供的时间戳。c(RS_Ids_00502)

[SWS_AIDSM_00802]{DRAFT}堆栈提供的时间戳dIf IdsmIn stand.timestampFormat等于
AUTOSAR 并且ara::idsm::EventReporter::ReportEvent函数在没有时间戳参数的情况下调用,则
Idsm
应从引用为Id sPlatformInstantiation.timeBase的 TimeSync::TimeBaseResource 中添加一个时间戳到存
储和传输的 QSEvs.c(RS_Ids_-
00503)

要添加的时间戳的格式在[2] 中指定。

[SWS_AIDSM_00803][DRAFT]通过事件报告接口提供的时间戳

应使用此提供的时间戳参数来传输或存储QSEv.c
(RS_Ids_00503)

[SWS_AIDSM_00804][DRAFT]通过应用软件 dIf 提供的时间戳
IdsmInstance.timestampFormat不等于 AUTOSAR 和ara::-
idsm::EventReporter::ReportEvent函数在没有时间戳参数的情况下调用,则IdsM应添加应用软件提供的时间戳
通过 TimestampProvider 回调到QSEv.c(RS_Ids_00503)

[SWS_AIDSM_00805][DRAFT]时间戳已配置但未提供dIf
IdsmInstance.timestampFormat不等于“ AUTOSAR” ,但ara::-
idsm::EventReporter::ReportEvent函数在没有时间戳参数的情况下被调用并且没有
TimestampProvider 被注册,那么IdsM不应添加
QSEv.c(RS_Ids_00503)的时间戳

[SWS_AIDSM_00806][DRAFT]截断时间戳参数dIf ara::-
idsm::EventReporter::ReportEvent函数使用时间戳参数调用,然后IdsM应将该值截断 2 个最高有效位,即只保留
62 个最低有效位以供进一步使用.c(RS_Ids_00503)

[SWS_AIDSM_00807][DRAFT]时间戳提供者dThe TimestampProvider
SWCL 应使用函数ara::idsm::RegisterTimes tampProvider 注册回调。回调应返回时间戳。
c(RS_Ids_00503)

请注意,虽然指定了 TimestampProvider API,但集成和
TimestampProvider 的配置仍然是特定于堆栈供应商的。

7.6 QSEv 的传播

[SWS_AIDSM_00901][DRAFT] QSEv 传输dIf PlatformModuleEther netEndpointConfiguration
在IdsPlatformInstantiation聚合
在角色networkInterface 中， IdsM应使用 IDS 协议传输QSEvs
在[2]中定义到通过PlatformModuleEthernetEnd pointConfiguration.c(RS_Ids_00510)配置的端点

[SWS_AIDSM_00902][DRAFT]消息 ID dIdsM应设置消息 ID 字段
IDS 消息分隔标头全部为零 (0x00000000).c(RS_Ids_00510)

7.7 传输的 QSev 的真实性

IdsM可以选择使用密码保护传输的QSEv的真实性
签名。

[SWS_AIDSM_01001]{DRAFT}签署 QSEv d 如果IdsmSignatureSupportAp在角色signatureSupportAp中的 IdsmInstance 聚合,则IdsM应将加密签名附加到传输到 IdsR 的每个QSEv和每个本地持久性QSEv.c(RS_Ids_00505)

[2]中规定了应根据哪些数据计算签名以及应如何将签名包含在传输到IdsR的消息中。可以使用IdsmSignatureSupportAp模型元素配置应使用哪个签名原语和哪个密钥：

[SWS_AIDSM_01002]{DRAFT} Primitive 和 Key dIdsM应使用参数IdsmSignatureSupportAp.cryptoPrimitive中指定的签名算法和由角色keySlot.c(RS_Ids_00505)中IdsmSignature SupportAp引用的CryptoKeySlot标识的密钥

要使用的签名算法的命名方案在 SWS Cryp tography [5] 中指定。

7.8 速率和流量限制

[SWS_AIDSM_01101]{DRAFT}速率和流量限制d在向 IdsR 发送QSEv之前， IdsM应应用可能导致丢弃QSEv.c(RS_Ids_00511)的速率和流量限制

[SWS_AIDSM_01103]{DRAFT}速率限制dIdsM应从传输中删除QSEv ,如果其传输会导致在IdsmRateLimitation.timeInterval中指定的当前间隔内传输的 QSEv数量超过配置为IdsmRateLimitation的最大传输数量. maxEventsInInterval.c(RS_Ids_00511)

[SWS_AIDSM_01104]{DRAFT}流量限制dIdsM应从传输中删除QSEv ,如果其传输会导致在IdsmTrafficLimitation.timeInterval中指定的当前间隔内传输的字节数超过配置为IdsmTrafficLimitation的最大字节数。 maxBytesInInterval.c(RS_Ids_00511)

7.9 访问控制

安全事件的产生受到访问控制,即可以通过配置来限制特定的SWCL可以产生哪些事件类型。访问控制由 IAM 在自适应平台上实施。

[SWS_AIDSM_01201]{DRAFT} dIdsM应将流程可以生成的事件类型限制为清单中角色securityEvent中流程引用的那些SecurityEventDefinitions.c (RS_Ids_00200)

TimestampProvider 接口也需要受到访问控制,以防止恶意或受损的应用程序向IdsM提供错误的时间戳为了支持项目特定的 TimestampProvider（例如,基于硬件或驱动程序）,对 TimestampProvider 的访问控制是超出了本规范的范围,并且必须以特定于项目的方式强制执行。

7.10 诊断访问

IdsM允许诊断访问以支持两个用例:首先,可以通过诊断访问读取持久事件。其次,可以通过诊断访问重新配置报告模式。

7.10.1 访问持久事件

每个安全事件都引用一个诊断事件,而该诊断事件又引用一个DTC。

[SWS_AIDSM_01301]{DRAFT}对持久事件的访问d如果一个事件已成功限定并且该事件被配置为持久（即,Securi tyEventContextProps.persistentStorage == 1）,则IdsM应限定事件引用的DTC并添加事件数据作为它的快照记录。c(RS_- Ids_00400)

7.10.2 重新配置报告模式

IdsM标准化了一个DID ,用于在运行时读取和更改事件的报告模式。

[SWS_AIDSM_01302]{DRAFT}获取当前报告模式dIdsM应提供诊断服务 GetReportingMode(SecurityEventDefinition.id),返回查询的SecurityEventDefinition.c(RS_ -Ids_00700) 的当前报告模式

[SWS_AIDSM_01303]{DRAFT}设置当前报告模式dIdsM应提供诊断服务 SetReportingMode(SecurityEventDefinition.id, ReportingMode) 设置给定SecurityEventDefinition.c (RS_Ids_00700)的报告模式

7.11 IdsM 提供的 SEv

IdsM本身也可以用作安全事件传感器。

[SWS_AIDSM_01401]{DRAFT} IdsM 提供的 SEvs dIdsM模块报告的安全事件列在 [SWS_IdsM_91015].c(RS_Ids_00820)

请注意,对应于每个安全事件的十六进制值在 SecXT 中集中定义。

[SWS_IdsM_91015] IDSM d的安全事件

姓名	描述	ID
IDSM_INTERNAL_EVENT_NO_EVENT_ BUFFER_AVAILABLE	无法处理 SEv,因为没有更多 可用于处理事件的事件缓冲区。	46
IDSM_INTERNAL_EVENT_NO_CONTEXT_ DATA_BUFFER_AVAILABLE	无法存储传入事件的上下文数据 因为没有更多的上下文数据缓冲区可用。	47
IDSM_INTERNAL_EVENT_TRAFFIC_ LIMITATION_EXCEEDED	当前流量超过配置的流量限制。	48
IDSM_INTERNAL_EVENT_COMMUNICATION_ 错误	通过 PDU 发送 QSEv 时发生错误。	49

c(RS_Ids_00810)

请注意,术语缓冲区是指事件和上下文所在的内存
数据被存储,独立于具体实现。

[SWS_AIDSM_01402]{DRAFT}缓冲区可用性dIdsM应确保即使没有可用缓冲区也可以处理内部事件中的IdsM。c (RS_Ids_00820)
一个实现可以通过例如为IdsM预分配内存缓冲区来实现这一点
提供的事件。

[SWS_AIDSM_01403]{DRAFT}旁路限制过滤器dIdsM内部SEvs应
不被速率和流量限制过滤filter.c(RS_Ids_00820)

8 API规范

8.1 API 常用数据类型

[SWS_AIDSM_10201]{草稿} d

种类:	类型别名
象征:	上下文数据类型
范围:	命名空间 ara::idsm
源自:	ara::core::Span<std::uint8_t>
句法:	使用 ContextDataType = ara::core::Span<std::uint8_t>;
头文件:	#include ara/idsm/common.h
描述:	ContextDataType 用于将上下文数据发送到 IdsM 。

C ()

[SWS_AIDSM_10202]{草稿} d

种类：	类型别名
象征：	时间戳类型
范围：	命名空间 ara::idsm
源自：	标准::uint64_t
句法：	使用 TimestampType = std::uint64_t;
头文件：	#include ara/idsm/common.h
描述：	TimestampType 用于为事件设置可选的特定于传感器的时间戳。
笔记：	只有 62 个最低有效位用作时间戳值并存储或传输， 分别

C ()

[SWS_AIDSM_10203]{草稿} d

种类：	类型别名
象征：	计数类型
范围：	命名空间 ara::idsm
源自：	标准::uint16_t
句法：	使用 CountType = std::uint16_t;
头文件：	#include ara/idsm/common.h
描述：	CountType 用于为传感器预先限定的事件设置可选计数。

C ()

8.2 API 参考

8.2.1 事件报告器

[SWS_AIDSM_10101]{草稿} d

种类：	班级
象征：	事件报告器
范围：	命名空间 ara::idsm
句法：	类 EventReporter {...};
头文件：	#include ara/idsm/event_reporter.h
描述：	用于向 IdsM 报告安全事件的类。

C ()

[SWS_AIDSM_10301]{草稿} d

种类：	功能
象征：	EventReporter(const ara::core::InstanceSpecifier &eventType)

4

范围：	类 ara::idsm::EventReporter	
句法：	EventReporter (const ara::core::InstanceSpecifier &eventType) 没有例外；	
参数（in）：	事件类型	EventDefinition 的 InstanceSpecifier 为 由此 EventReporter 对象报告
异常安全：	无例外	
头文件：	#include ara/idsm/event_reporter.h	
描述：	构造一个新的 Event Reporter 对象。由传感器为每个事件类型调用 事件类型指定的实例。	

C ()

[SWS_AIDSM_10302]{草稿} d

种类：	功能	
象征：	ReportEvent(const CountType=1)	
范围：	类 ara::idsm::EventReporter	
句法：	void ReportEvent (const CountType=1) noexcept;	
方向不 定义	计数类型	–
返回值：	没有任何	
异常安全：	无例外	
头文件：	#include ara/idsm/event_reporter.h	
描述：	在 IdsM 创建一个新的安全事件。 .	

C ()

[SWS_AIDSM_10303]{草稿} d

种类：	功能	
象征：	ReportEvent(const TimestampType 时间戳,const CountType=1)	
范围：	类 ara::idsm::EventReporter	
句法：	void ReportEvent (const TimestampType timestamp, const CountType=1) 没有例外；	
参数（in）：	时间戳	应用程序提供的时间戳
方向不 定义	计数类型	–
返回值：	没有任何	
异常安全：	无例外	
头文件：	#include ara/idsm/event_reporter.h	
描述：	在 IdsM 上使用传感器提供的时间戳创建一个新的安全事件。 .	

C ()

[SWS_AIDSM_10304]{草稿} d

种类：	功能	
象征：	ReportEvent(const ContextDataType &contextData, const CountType=1)	
范围：	类 ara::idsm::EventReporter	
句法：	void ReportEvent (const ContextDataType &contextData, const Count 类型=1) 无例外；	
参数（in）：	上下文数据	上下文数据
方向不 定义	计数类型	–
返回值：	没有任何	
异常安全：	无例外	
头文件：	#include ara/idsm/event_reporter.h	
描述：	在 IdsM 上使用传感器提供的上下文数据创建新的安全事件。 .	

C ()

[SWS_AIDSM_10305]{草稿} d

种类：	功能	
象征：	ReportEvent(const ContextDataType &contextData, const TimestampType timestamp, const 计数类型=1)	
范围：	类 ara::idsm::EventReporter	
句法：	void ReportEvent (const ContextDataType &contextData, const Timestamp 类型时间戳,const CountType=1) noexcept;	
参数（in）：	上下文数据	上下文数据
	时间戳	应用程序提供的时间戳
方向不 定义	计数类型	–
返回值：	没有任何	
异常安全：	无例外	
头文件：	#include ara/idsm/event_reporter.h	
描述：	使用传感器提供的上下文数据和传感器提供的新安全事件 IdsM 的时间戳。 .	

C ()

8.2.2 时间戳提供者

[SWS_AIDSM_20101]{草稿} d

种类：	功能	
象征：	RegisterTimestampProvider(std::function<TimestampType()> 回调)	
范围：	命名空间 ara::idsm	
句法：	无效 RegisterTimestampProvider (std::function< TimestampType()> 打回来）；	
参数（in）：	打回来	提供时间戳的 std::function 回调 IdsM

4

返回值：	没有任何
头文件：	#include ara/idsm/timestamp_provider.h
描述：	注册回调以向 IdsM 提供时间戳。

C ()

9 服务接口

IdsM 不提供任何服务接口。

提到的清单元素

为了完整起见,本章包含一组表示
本文档上下文中提到但未包含的元类
直接在描述特定元模型语义的范围内。

章生成。

班级	加密密钥槽			
包裹	M2::AUTOSARTemplates::AdaptivePlatform::PlatformModuleDeployment::CryptoDeployment			
笔记	此元类表示定义用于加密操作的具体密钥的能力。 标签: atp.ManifestKind=机器清单 atp.Status=草稿			
根据	ARObject,可识别,多语言可参考,可参考			
属性	类型	多。温馨提示		
分配阴影 复制	布尔值	0..1	属性	此属性定义是否此 Key 的卷影副本 应分配插槽以启用失败密钥的回滚 插槽更新活动（参见界面 BeginTransaction）。 标签:atp.Status=草稿
加密算法 ID	细绳	0..1	属性	该属性定义了一个加密算法限制（kAlgId 任何手段,不受限制）。该算法可以是 部分指定:家庭和长度、模式、填充。 未来的加密提供者可以支持一些加密 今天不为人所知/标准化的算法， 因此 AUTOSAR 没有提供具体的列表 加密算法的标识符并且不假设使用 数字标识符。取而代之的是供应商供应商 应提供支持算法的字符串名称 随附文件。加密货币的名称 算法应遵循规范中定义的规则 自适应平台的密码学。 标签:atp.Status=草稿
加密对象 类型	加密对象类型枚举	0..1	属性	可以存储在插槽中的对象类型。如果这个字段 包含“未定义”,则 mSlotCapacity 必须为 提供且大于 0。 标签:atp.Status=草稿
keySlotAllowed 修改	CryptoKeySlotAllowed 修改	0..1	聚合	限制如何使用这个 keySlot 标签:atp.Status=草稿
键槽内容 允许使用	CryptoKeySlot 内容 允许使用		聚合	存储到槽的密钥的允许使用限制。 标签:atp.Status=草稿
槽容量	正整数	0..1	属性	堆栈保留的插槽容量（以字节为单位） 小贩。一个用例是定义这个值,以防万一 cryptoObjectType 未定义,插槽大小可以 不能从 cryptoObjectType 和 cryptoAlgId 推导出来。 “0”表示可以从 cryptoObject 推导出槽大小 类型和 cryptoAlgId。 标签:atp.Status=草稿
插槽类型	CryptoKeySlotType 枚举	0..1	属性	该属性定义keySlot是否独占 由应用程序使用;或者是否被 Stack 使用 服务并由密钥管理器应用程序管理。 标签:atp.Status=草稿

表 A.1:加密密钥槽

班级	IdsPlatformInstantiation （抽象）			
包裹	M2::AUTOSARTemplates::AdaptivePlatform::PlatformModuleDeployment::IntrusionDetectionSystem			
笔记	这个元类充当实现入侵的平台模块的抽象基类 检测系统。 标签:atp.Status=草稿			
根据	ARObject, AdaptiveModuleInstantiation, Identifiable, MultilanguageReferable, NonOsModule 实例化,可引用			
子类	IdsmM模块实例化			
属性	类型	多。温馨提示		
网络 界面	平台模块 以太网端点 配置	0..1	参考	此关联包含的网络配置 应应用于 IDS 实体的实例。 标签:atp.Status=草稿
时基	时基资源	0..1	参考	该参考确定了适用的时基 资源。 刻板印象： atpVariation 标签： atp.Status=草稿 vh.latestBindingTime=系统设计时间

表 A.2:IdsPlatformInstantiation

班级	IdsmInstance			
包裹	M2::AUTOSARTemplates::SecurityExtractTemplate			
笔记	这个元类提供了在 EcuInstance 和特定类之间创建关系的能力 适用于在引用的 EcuInstance 上报告的所有安全事件的安全事件过滤器。 标签： atp.Status=草稿 atp.recommendedPackage=IdsmInstanceToEcuInstanceMappings			
根据	AUTOSARElement, ARObject, CollectableElement, Identifiable, IdsCommonElement, MultilanguageReferable, 可打包元素,可引用			
属性	类型	多。温馨提示		
idsmInstanceId	正整数	0..1	属性	该属性用于提供源标识 报告安全事件的上下文.. 标签:atp.Status=草稿
idsmM模块 实例化	idsm模块 实例化	0..1	参考	此参考标识定义了 特定设备上 IdsM 配置的属性 机器。 刻板印象： atpSplitable 标签： atp.Splitkey=idsmModuleInstantiation atp.Status=草稿
限速 筛选	IdsmRateLimitation	0..1	参考	此参考标识适用的速率限制过滤器 用于相关 EcuInstance 上的所有安全事件。 刻板印象： atpVariation 标签： atp.Status=草稿 vh.latestBindingTime=preCompileTime

4

班级	IdsmInstance			
签名 支持应用程序	Idsm签名支持 ap	0..1	aggr 此聚合的存在指定 IdsM 应为其发送的 QSEv 消息添加签名 到网络上。密码算法和密钥 用于此签名由进一步指定 专门为 Adaptive 聚合的元类 平台。 刻板印象： atpSplitable 标签： atp.Splitkey=signatureSupportAp atp.Status=草稿	
时间戳 格式	细绳	0..1	attr 该属性的存在指定 IdsM 应 将时间戳添加到它发送到的 QSEv 消息中 网络。即如果该属性不存在，则无时间戳 应添加到 QSEv 消息中。 该属性的内容进一步规定了 时间戳格式如下： - “AUTOSAR”定义 AUTOSAR 标准化时间戳格式根据 同步时基管理器 - 任何其他字符串 定义了专有的时间戳格式。 注意：定义专有时间戳格式的字符串 应以公司特定名称片段为前缀 避免碰撞。 标签：atp.Status=草稿	
流量限制 筛选	Idsm交通限制	0..1	参考	该参考确定了适用的流量限制 过滤相关 EcuInstance 上的所有安全事件。 刻板印象： atpVariation 标签： atp.Status=草稿 vh.latestBindingTime=preCompileTime

表 A.3：IdsmInstance

班级	IdsmRateLimitation			
包裹	M2::AUTOSARTemplates::SecurityExtractTemplate			
笔记	此元类表示安全事件的速率限制过滤器的配置。这意味着 如果在可配置的时间内处理的事件（任何类型）的数量，安全事件将被丢弃 窗口大于可配置的阈值。 标签：atp.Status=草稿			
根据	ARObject，AbstractSecurityIdsmInstanceFilter，可识别，多语言可参考，可参考			
属性	类型	多。温馨提示		
最大事件输入 间隔	正整数	1	属性	该属性配置丢弃阈值 安全事件，如果所有处理的安全数 事件在相应时间超过阈值 间隔。 标签：atp.Status=草稿
时间间隔	漂浮	1	属性	该属性配置时间间隔的长度 秒，如果所有的数量下降安全事件 处理的安全事件超出了可配置的 在相应的时间间隔内的阈值。 标签：atp.Status=草稿

表 A.4：IdsmRateLimitation

班级	IdsmSignatureSupportAp			
包裹	M2::AUTOSARTemplates::SecurityExtractTemplate			
笔记	该元类为自适应平台定义了加密算法和密钥,以供 用于在 QSEv 消息中提供签名信息的 IdsM 实例。 标签:atp.Status=草稿			
根据	AR对象			
属性	类型	多。温馨提示		
加密原语	字符串	1	属性	该属性将加密算法定义为 用于在 QSEv 中提供身份验证信息 消息。该属性的内容应符合 “加密原语命名约定”。 标签:atp.Status=草稿
键槽	加密密钥槽	0..1	参考	此参考表示要使用的加密密钥 通过密码算法提供 QSEv 消息中的身份验证信息。 标签:atp.Status=草稿

表 A.5:IdsmSignatureSupportAp

班级	Idsm交通限制			
包裹	M2::AUTOSARTemplates::SecurityExtractTemplate			
笔记	此元类表示安全事件的流量限制过滤器的配置。这表示 如果安全事件（任何类型)的大小（就带宽而言），则安全事件将被丢弃 在可配置的时间窗口内处理大于可配置的阈值。 标签:atp.Status=草稿			
根据	ARObject,AbstractSecurityIdsmInstanceFilter,可识别,多语言可参考,可参考			
属性	类型	多。温馨提示		
最大字节输入 间隔	正整数	0..1	属性	该属性配置丢弃阈值 安全事件,如果所有已处理的安全事件的大小 在相应的时间间隔内超过阈值。 标签:atp.Status=草稿
时间间隔	漂浮	0..1	属性	该属性配置时间间隔的长度 如果大小为 all 则丢弃安全事件的秒数 处理的安全事件超出了可配置的 在相应的时间间隔内的阈值。 标签:atp.Status=草稿

表 A.6:IdsmTrafficLimitation

班级	平台模块以太网端点配置			
包裹	M2::AUTOSARTemplates::AdaptivePlatform::PlatformModuleDeployment::AdaptiveModule 执行			
笔记	这个元类定义了端口、协议类型和 IP 地址的配置属性。 VLAN 上的通信。 标签: atp.Status=草稿 atp.recommendedPackage=PlatformModuleEndpointConfigurations			
根据	ARElement、ARObject、CollectableElement、可识别、多语言可参考、可打包 元素、PlatformModuleEndpointConfiguration、可引用			
属性	类型	多。温馨提示		

4

班级	平台模块以太网端点配置			
沟通 连接器	以太网通讯 连接器	0..1	参考	参考 CommunicationConnector (VLAN) 其中定义了网络配置。 标签:atp.Status=草稿
ipv4MulticastIp 地址	Ip4地址字符串	0..1	属性	消息将发送到的多播 IPv4 地址 传送。 标签:atp.Status=草稿
ipv6MulticastIp 地址	Ip6地址字符串	0..1	属性	消息将发送到的多播 IPv6 地址 传送。 标签:atp.Status=草稿
tcp端口	应用应用端点	0..1	参考	此参考允许配置 tcp 端口号。 标签:atp.Status=草稿
端口	应用应用端点	0..1	参考	此参考允许配置 udp 端口号。 标签:atp.Status=草稿

表 A.7:平台模块以太网端点配置

班级	过程			
包裹	M2::AUTOSARTemplates::AdaptivePlatform::ExecutionManifest			
笔记	此元类提供执行引用的可执行文件所需的信息。 标签: atp.Status=草稿 atp.recommendedPackage=进程			
根据	ARElement, ARObject, AbstractExecutionContext, AtpClassifier, CollectableElement, Identifiable, MultilanguageReferable、PackageableElement、Referable、UploadablePackageElement			
属性	类型	多。温馨提示		
设计	流程设计	0..1	参考	此参考代表的标识 拥有 参考。 标签:atp.Status=草稿
确定性的 客户	确定性客户端	0..1	参考	此参考添加了进一步的执行特性 确定性客户。 标签:atp.Status=草稿
可执行的	可执行文件	0..1	参考	对在进程中执行的可执行文件的引用。 刻板印象： atpUriDef 标签:atp.Status=草稿
函数簇 联系	细绳	0..1	属性	此属性指定哪个功能集群 过程隶属于。 标签:atp.Status=草稿
数量 重启尝试	正整数	0..1	属性	该属性定义了一个进程的频率 如果启动失败则重新启动。 numberOfRestartAttempts = 0 或属性不存在， 开始一次 numberOfRestartAttempts = 1 ,第二次开始 标签:atp.Status=草稿
预映射	布尔值	0..1	属性	该属性描述可执行文件是否为 预加载到内存中。 标签:atp.Status=草稿

5

4

班级	过程			
进程状态机器	模式声明组原型	0..1	聚合	为流程定义的一组流程状态。 标签:atp.Status=草稿
安全事件	安全事件定义	*	参考	该参考标识了 SecurityEvents 的集合可以由封闭的 SoftwareCluster 报告。 刻板印象： atpSplitable;属性定义 标签： atp.Splitkey=securityEvent atp.Status=草稿
状态依赖启动配置	状态依赖启动配置	*	aggr	适用的启动配置。 标签:atp.Status=草稿

表 A.8:过程

班级	安全事件聚合过滤器			
包裹	M2::AUTOSARTemplates::SecurityExtractTemplate			
笔记	这个元类表示聚合过滤器,它聚合在一个范围内发生的所有安全事件。 将时间框架配置为一个（即最后报告的)安全事件。 标签:atp.Status=草稿			
根据	ARObject,AbstractSecurityEventFilter,可识别,多语言可参考,可参考			
属性	类型	多。温馨提示		
上下文数据来源	安全事件上下文数据源枚举	0..1	属性	这个属性定义了第一个上下文数据是否 或最后一次聚合的安全事件应用于 产生的合格安全事件。
最低限度间隔长度	时间价值	0..1	属性	该属性代表最低配置 聚合过滤器的时间窗口（以秒为单位）。 标签:atp.Status=草稿

表 A.9:SecurityEventAggregationFilter

班级	SecurityEventContextMapping （抽象）			
包裹	M2::AUTOSARTemplates::SecurityExtractTemplate			
笔记	此元类表示在安全事件集合之间创建关联的能力， 处理安全事件和适用于安全事件的过滤器链的 IdsM 实例。 标签:atp.Status=草稿			
根据	ARElement,ARObject,CollectableElement,可识别,IdsCommonElement,IdsMapping， MultilanguageReferable、PackageableElement、Referable			
子类	SecurityEventContextMappingApplication、SecurityEventContextMappingCommConnector、安全 EventContextMappingFunctionalCluster			
属性	类型	多。温馨提示		
过滤链	安全事件过滤器链	0..1	参考	此参考定义了要应用于的过滤器链 每个引用的安全事件（取决于 报告模式）。 刻板印象： atpVariation 标签： atp.Status=草稿 vh.latestBindingTime=preCompileTime

5

4

班级	SecurityEventContextMapping （抽象）			
idsmInstance	IdsmInstance	0..1	参考	此参考定义了 IdsmInstance， 安全事件被映射。 刻板印象： atpVariation 标签： atp.Status=草稿 vh.latestBindingTime=系统设计时间
映射安全 事件	安全事件上下文 道具		aggr 这个聚合表示（通过进一步的参考） 要映射到 Idsm 的 SecurityEventDefinitions 具有附加映射相关属性的实例。 刻板印象： atpSplitable； atp变体 标签： atp.Splitkey=mappedSecurityEvent.shortName,映射 SecurityEvent.variationPoint.shortLabel atp.Status=草稿 vh.latestBindingTime=preCompileTime	

表 A.10：SecurityEventContextMapping

班级	SecurityEventContextProps		
包裹	M2::AUTOSARTemplates::SecurityExtractTemplate		
笔记	此元类指定要映射到 IdsmInstance 的 SecurityEventDefinition 并添加 此安全事件的映射相关属性仅对此特定映射有效。 标签：atp.Status=草稿		
根据	ARObject,可识别,多语言可参考,可参考		
属性	类型	多。温馨提示	
上下文数据	安全事件上下文 数据	0..1	aggr 这个聚合代表了 optional 的定义 安全事件的上下文数据。 刻板印象： atpVariation 标签： atp.Status=草稿 vh.latestBindingTime=系统设计时间
默认 报告模式	安全事件报告 模式枚举	0..1	属性 该属性定义了默认报告模式 引用的安全事件。 标签：atp.Status=草稿
执着的 贮存	布尔值	0..1	属性 该属性控制是否合格的报告 引用的安全事件应由 映射的 IdsmInstance 与否。 标签：atp.Status=草稿
安全事件	安全事件定义	0..1	参考 此参考定义了映射的安全事件 并由 SecurityEventMappingProps 丰富 映射依赖属性。 刻板印象： atpVariation 标签： atp.Status=草稿 vh.latestBindingTime=系统设计时间
传感器实例 ID	正整数	0..1	属性 该属性定义了安全传感器的 ID 检测引用的安全事件。 标签：atp.Status=草稿

5

4

班级	SecurityEventContextProps			
严重性	正整数	0..1	属性	此属性定义所引用的关键/严重程度 安全事件是。请注意,目前,严重程度 未指定特定整数值的级别含义 由 AUTOSAR 但留给负责 IDS 的一方 系统设计（例如 OEM）。 标签:atp.Status=草稿

表 A.11:SecurityEventContextProps

班级	安全事件定义			
包裹	M2::AUTOSARTemplates::SecurityExtractTemplate			
笔记	该元类将安全相关事件定义为入侵检测系统的一部分。 标签： atp.Status=草稿 atp.recommendedPackage=SecurityEventDefinitions			
根据	ARElement, ARObject, CollectableElement, Identifiable, IdsCommonElement, MultilanguageReferable, 可打包元素,可引用			
属性	类型	多。温馨提示		
事件符号 姓名	符号道具	0..1	aggr 此聚合可选地定义一个替代事件 SecurityEventDefinition 的名称,以防有 短名称的冲突。 刻板印象： atpSplitable 标签： atp.Splitkey=eventSymbolName.shortName atp.Status=草稿	
ID	正整数	0..1	属性	该属性代表数字标识 定义的安全事件。标识应为 在 IDS 范围内是唯一的。 标签:atp.Status=草稿

表 A.12:安全事件定义

班级	安全事件过滤链			
包裹	M2::AUTOSARTemplates::SecurityExtractTemplate			
笔记	此元类表示用于限定安全事件的可配置过滤器链。不同的 此过滤器链的过滤器按以下顺序应用:SecurityEventStateFilter、SecurityEventOneEvery NFilter、SecurityEventAggregationFilter、SecurityEventThresholdFilter。 标签： atp.Status=草稿 atp.recommendedPackage=SecurityFilterChains			
根据	ARElement, ARObject, CollectableElement, Identifiable, IdsCommonElement, MultilanguageReferable, 可打包元素,可引用			
属性	类型	多。温馨提示		
聚合	安全事件 聚合过滤器	0..1	aggr 这个聚合代表聚合过滤器 过滤链。 标签:atp.Status=草稿	
一个每个N	安全事件OneEvery 过滤器	0..1	aggr 这个聚合代表过滤器中的采样过滤器 链。 标签:atp.Status=草稿	

5

4

班级	安全事件过滤链			
状态	安全事件状态过滤器	0..1	aggr	这个聚合代表事件中的状态过滤器 链。 标签:atp.Status=草稿
临界点	安全事件阈值 筛选	0..1	aggr	这个聚合表示过滤器中的阈值过滤器 链。 标签:atp.Status=草稿

表 A.13:SecurityEventFilterChain

班级	SecurityEventOneEveryNFilter			
包裹	M2::AUTOSARTemplates::SecurityExtractTemplate			
笔记	这个元类表示一个采样（即每个第 n 个事件被采样)过滤器的配置 安全事件。 标签:atp.Status=草稿			
根据	ARObject,AbstractSecurityEventFilter,可识别,多语言可参考,可参考			
属性	类型正	多。温馨提示		
n	整数	0..1	属性	该属性代表采样的配置 过滤器,即它配置控制如何 许多事件 (n-1) 应在采样事件后丢弃 直到创建一个新样本。 标签:atp.Status=草稿

表 A.14:SecurityEventOneEveryNFilter

班级	安全事件状态过滤器			
包裹	M2::AUTOSARTemplates::SecurityExtractTemplate			
笔记	该元类表示安全事件的状态过滤器的配置。引用的状态 表示一个阻止列表,即如果引用的状态是 相关状态机（取决于 IdsM 实例是在 Classic 还是 Adaptive 平台）。 标签:atp.Status=草稿			
根据	ARObject,AbstractSecurityEventFilter,可识别,多语言可参考,可参考			
属性	类型	多。温馨提示		
阻塞状态 主动式	模式声明		参考	对于 AP,此参考定义了机器状态 阻止列表。这意味着,如果一个安全事件（映射到 SecurityEventStateFilter 所在的过滤器链 属于)当机器处于其中之一时报告 块列出的状态,IdsM 应丢弃报告的 安全事件。 标签:atp.Status=草稿 InstanceRef 实现者:FunctionGroupStateIn FunctionGroupSetInstanceRef

表 A.15:SecurityEventStateFilter

班级	安全事件阈值过滤器
包裹	M2::AUTOSARTemplates::SecurityExtractTemplate

5

4

班级	安全事件阈值过滤器			
笔记	此元类表示丢弃的阈值过滤器（在可配置的每个开头重复 时间间隔)可配置数量的安全事件。所有随后到达的安全事件（在 配置的时间间隔)通过过滤器。 标签:atp.Status=草稿			
根据	ARObject,AbstractSecurityEventFilter,可识别,多语言可参考,可参考			
属性	类型	多。温馨提示		
间隔长度	时间价值	0..1	属性	此属性配置以秒为单位的时间间隔 一个阈值过滤操作。 标签:atp.Status=草稿
临界点 数字	正整数	0..1	属性	该属性配置阈值数量,即如何 在配置的时间范围内的许多安全事件是 在后续事件开始通过过滤器之前删除。 标签:atp.Status=草稿

表 A.16:SecurityEventThresholdFilter

B 与其他功能集群的接口（资料性）

B.1 概述

AUTOSAR 决定不对功能集群之间专门使用的接口（仅在平台级别)进行标准化,以允许有效的实现,这可能取决于例如使用的操作系统。

本章通过对本文档的相关要求进行聚类来描述功能集群间 (IFC) 接口,提供了功能集群之间的交互方式的信息指南。此外,用户空间应用程序可访问的标准化公共接口（见第8章和第9 章)也可用于功能集群之间的交互。

目标是提供对功能集群边界和交互的清晰理解,而无需指定语法细节。这确保了指定不同功能集群的文档之间的兼容性,并支持不同功能集群的并行实现。接口的细节由平台提供者决定。可以添加额外的接口、参数和返回值。

B.2 接口表