image

**东软睿驰秘密(Neusoft Reach Secret)**

文件编号(File No.)：项目编号- D00-COP02-SW-T31-流水号

NeuSAR aCore

软件需求规格说明书

(Software requirement specification)

**(IDSM)**

版本(Version)：0.7

日期(Date)：2022-04-18

|  |  |  |
| --- | --- | --- |
| 编制  Prepared by | 审核  Reviewed by | 批准  Approved by |
|  |  |  |

东软睿驰汽车技术(沈阳)有限公司

**(版权所有，翻版必究)**

Neusoft Reach Automotive Technology(Shenyang) Co., Ltd

**(Copyright by Reach Corporation, All Rights Reserved)**

变更履历(Change Log)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **修改编号**  **No.** | **版本**  **Version** | **修改内容**  **Contents Revised** | **状态**  **Status** | **修改人/日期**  **Reviser/Date** | **审批人/日期**  **Approve/Date** |
| 1 | 0.7 | 初稿 | Draft | 黄海军、秦天宇/2022/4/18 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Contents**

[1 引言(Introduction) 1](#_Toc97295388)

[1.1 目的(Goal) 1](#_Toc97295389)

[1.2 范围(Scope) 1](#_Toc97295390)

[1.3 参考文档(Reference) 1](#_Toc97295391)

[1.4 术语和缩略语(Terms And Abbreviations) 1](#_Toc97295392)

[2 软件系统概述(Software System Overview) 2](#_Toc97295393)

[2.1 软件系统背景(Software System Background) 2](#_Toc97295394)

[2.2 软件系统目标(Software System Goal) 2](#_Toc97295395)

[2.3 外部关联 (External Association) 2](#_Toc97295396)

[3 功能需求(Functional Requirement) 2](#_Toc97295397)

[3.1 功能需求1(Function Requirement No.1) 2](#_Toc97295398)

[3.1.1 [SWRD-ID]功能子需求1-1(Function Requirement No.1-1) 2](#_Toc97295399)

[3.1.2 [SWRD-ID]功能子需求1-2(Function Requirement No.1-2) 3](#_Toc97295400)

[3.2 功能需求2(Function Requirement No.2) 3](#_Toc97295401)

[3.2.1 [SWRD-ID]功能子需求2-1(Function Requirement No.2-1) 3](#_Toc97295402)

[3.2.2 [SWRD-ID]功能子需求2-2(Function Requirement No.2-2) 4](#_Toc97295403)

[4 非功能需求(Non-Functional Requirements) 4](#_Toc97295404)

[4.1 制约(Constraint) 4](#_Toc97295405)

[4.1.1 [SWRD-ID]非功能需求1(Non-Function Requirement No.1) 4](#_Toc97295406)

[4.1.2 [SWRD-ID]非功能需求2(Non-Function Requirement No.2) 5](#_Toc97295407)

[4.2 性能质量要求(Performance Quality Requirements) 5](#_Toc97295408)

[4.2.1 [SWRD-ID]非功能需求3(Non-Function Requirement No.3) 5](#_Toc97295409)

[4.2.2 [SWRD-ID]非功能需求4(Non-Function Requirement No.4) 5](#_Toc97295410)

[5 接口说明(API) 6](#_Toc97295411)

[5.1 接口头文件(API Header files) 6](#_Toc97295412)

[5.2 接口共同数据类型(API Common Data Types) 6](#_Toc97295413)

[5.2.1 [SWRD-ID]数据类型1(Data Type1) 6](#_Toc97295414)

[5.2.2 [SWRD-ID]数据类型2(Data Type2) 7](#_Toc97295415)

[5.3 接口定义(API Reference) 7](#_Toc97295416)

[5.3.1 [SWRD-ID]接口1(API 1) 7](#_Toc97295417)

[5.3.2 [SWRD-ID]接口2(API 2) 8](#_Toc97295418)

[附录A- 信息定义 9](#_Toc97295419)

[附录B- 配置信息 11](#_Toc97295420)

# 引言(Introduction)

## 目的(Goal)

为idsM模块提供详细的软件需求的定义，给开发人员和测试人员提供设计和测试执行的标准。

## 范围(Scope)

本文使用者： 开发人员、测试人员、PSM、TeamLeader、TestLeader和产品负责人。

本文使用方法：

* 对于开发人员、根据本文档中定义的功能/非功能要求进行后续的设计。
* 对于测试人员、通过理解本文档中的要求，进行测试用例的制作和后续测试执行。

对于PSM、TeamLeader、TestLeader和产品负责人、来判断需求理解的正确性

## 参考文档(Reference)

|  |  |  |
| --- | --- | --- |
| **编号** | **SVN路径\文档名** | **文档版本** |
| 1 | AUTOSAR\_RS\_IntrusionDetectionSystem | AP-R21-11 |
| 2 | AUTOSAR\_RS\_SecurityExtractTemplate | AP-R21-11 |
| 3 | AUTOSAR\_SWS\_AdaptiveIntrusionDetectionSystemManager | AP-R21-11 |
| 4 | AUTOSAR\_PRS\_IntrusionDetectionSystem | AP-R21-11 |
|  |  |  |
|  |  |  |

## 术语和缩略语(Terms And Abbreviations)

|  |  |  |
| --- | --- | --- |
| **编号** | **缩写** | **说明** |
| 1 | idsM | ⼊侵检测系统管理器。 |
| 2 | IDS | ⼊侵检测系统 |
| 3 | IdsR | ⼊侵检测系统报告器 |
| 4 | SEv | 安全事件 |
| 5 | QSEv | 合格的安全事件 |
| 6 | Sem | 安全事件存储器 |
| 7 | SIEM | 安全事件和事件管理 |
| 8 | SOC | 安全运营中⼼ |
| 9 | DID | 根据统⼀诊断服务的数据标识符 |
| 10 | DTC | 诊断故障代码 |
| 11 | FC | 功能集群 |
| 12 | SecXT | 安全提取 |
| 13 | SWCL | 软件集群 |
| 14 | SWC | 软件组件 |
| 15 | CDD | 复杂设备驱动 |
| 16 | BSW | 基础软件 |

# 软件系统概述(Software System Overview)

## 软件系统背景(Software System Background)

NeuSAR aCore 架构将 NeuSAR aCore 基础的软件组织为功能集群。这些集群提供通用功能作为应用程序的服务。功能集群⼊侵检测系统管理器 是 NeuSAR aCore架构的一部分，为应用程序提供安全事件检测相关的服务。

## 软件系统目标(Software System Goal)

idsM为应用程序和其他自适应 AUTOSAR 功能集群提供了一些标准化接口，这些接口提供了系统安全功能。 这些功能主要包括识别，过滤，保存，上报安全事件等，以保证系统运行时对安全问题的预防与发现。

### 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 标准化了可以由 AUTOSAR BSW 报告的安全事件类型的子集。 每个 BSW SWS 都列出了由相应模块报告的安全事件类型。

### 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 ECU 上。

• 与/或序列化QSEv 并将其传输到IdsR。

### 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 协中在相应的规范中指定。

## 外部关联 (External Association)

略。

# 功能需求(Functional Requirement)

总体结构部分明确了IDSM模块的总体结构需求，包括总体结构的设计需求以及实现需求；以及对于各子模块的主要需求点。

## 功能集群生命周期

### [SWRD-IDSM-00001] 功能集群生命周期启动

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00001 |
| **Type** | Valid |
| **Description** | 使⽤ ara::core::Intitialize 和 ara::core::Deinitialize，应⽤程序可以初始化和注销其 idsm 库  当 ara::core::Intitialize 被调用时，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，访问结构可以包含应用程序进程和堆栈进程（如果有的话）或 idsM 所需的其他资源之间的通信通道； |
| **Upstream ID** | SWS\_AIDSM\_00001 |
| **Dependencies** | RS\_Ids\_00100 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：NeuSAR-aCore平台启动完成  主要测试点：测试NeuSAR-aCore平台启动完成后，idsM初始化是否正常，是否有初始化未完成项；接口异常测试，返回的错误码是否正确；  成功标准：   1. idsM启动初始化能正常完成； 2. 接口异常测试，返回的错误码正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-00002] 功能集群生命周期注销

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00002 |
| **Type** | Valid |
| **Description** | 应用不应该在ara::core::Intitialize 之前或 ara::core::Deinitialize之后调用IdsM的API； |
| **Upstream ID** | SWS\_AIDSM\_00002 |
| **Dependencies** |  |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：NeuSAR-aCore平台启动完成  主要测试点：idsM注销idsM后是否存在异常，线程中注销idsM是否存在内存泄漏。接口异常测试，返回的错误码是否正确；  成功标准：   1. idsM注销能正常完成； 2. idsM注销后没有内存泄漏的情况； 3. 接口异常测试，返回的错误码正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 事件生成

### [SWRD-IDSM-00100]安全事件标识

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00100 |
| **Type** | Valid |
| **Description** | 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.id 唯一标识； |
| **Upstream ID** | SWS\_AIDSM\_00101 |
| **Dependencies** | RS\_Ids\_00310 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：idsM初始化完成  主要测试点：测试SecurityEventDefinition.id 是否是唯一标识；对于不同事件的SecurityEventDefinition.id相互之间没有影响；接口异常测试，返回的错误码是否正确；  成功标准：   1. SecurityEventDefinition.id能够识别出对应的事件； 2. 不同的事件id，对事件检测结果相互没有影响； 3. 接口异常测试，返回的错误码正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 报告模式

### 3.3.1 [SWRD-IDSM-00201] 设置报告模式

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00201 |
| **Type** | Valid |
| **Description** | IdsM应当根据安全提取模板的建模参数SecurityEventContextProps.defaultReportingMode确定每个报告的SEv的默认报告模式； |
| **Upstream ID** | SWS\_AIDSM\_00201 |
| **Dependencies** | RS\_Ids\_00310 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：idsM初始化完成  主要测试点：默认报告模式选择是否正确；配置的报告模式是否成功；配置的报告模式是否正确；接口异常测试，返回的错误码是否正确；  成功标准：  1．默认报告模式正确；  2．报告模式可以配置；  3．报告模式配置的结果正确；  4. 接口异常测试，返回的错误码正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

### 3.3.2 [SWRD-IDSM-00202] 根据报告模式处理

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00202 |
| **Type** | Valid |
| **Description** | IdsM应该根据被报告的SEv所属的安全事件类型的报告模式处理该SEv  【off、brief、detail、brief\_bypassing\_filtersdetail\_bypassing\_filters】 |
| **Upstream ID** | SWS\_AIDSM\_00202 |
| **Dependencies** | RS\_Ids\_00310 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：设置报告模式实现完成  主要测试点：上报的SEv是否有异常；匹配上报的SEv是否正常；接口异常测试，返回的错误码是否正确；  成功标准：  1．上报的SEv正常；  2．匹配上报的SEv正常；  3. 接口异常测试，返回的错误码正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 过滤链

### [SWRD-IDSM-00301] 安全事件和过滤链关联

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00301 |
| **Type** | Valid |
| **Description** | 当一个SEv被报告时，idsM应该对其应用过滤链，该过滤链通过SecurityEventContextMapping和该SEv所属的SecurityEventDefinition（安全事件类型）关联； |
| **Upstream ID** | SWS\_AIDSM\_00301 |
| **Dependencies** | RS\_Ids\_00300  RS\_Ids\_00301 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：报告模式处理实现完成  主要测试点：idsM应该对其应用过滤链是否正确；接口异常测试，返回的错误码是否正确；  成功标准：  1．idsM应该对其应用过滤链正确；  2. 接口异常测试，返回的错误码正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-00302] 过滤链在报告模式之后应用

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00302 |
| **Type** | Valid |
| **Description** | IdsM应该在评估完报告模式后进行过滤链评估——IdsM对一个报告的SEv应用完默认报告模式后，再应用过滤链策略； |
| **Upstream ID** | SWS\_AIDSM\_00302 |
| **Dependencies** | RS\_Ids\_00610 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：idsM应用过滤链实现完成  主要测试点：IdsM先评估完报告模式是否正确；应用过滤链策略是否正确；接口异常测试，返回的错误码是否正确；  成功标准：  1．IdsM先评估完报告模式正确；  2．应用过滤链策略正确；  3. 接口异常测试，返回的错误码正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-00303] 过滤链组成

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00303 |
| **Type** | Valid |
| **Description** | 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 |
| **Upstream ID** | SWS\_AIDSM\_00303 |
| **Dependencies** | RS\_Ids\_00300 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：idsM应用过滤链实现完成  主要测试点：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，是否可以配置；接口异常测试，返回的错误码是否正确；  成功标准：  1．机器状态过滤器，转发每n个过滤器，聚合过滤器，阈值过滤器可以成功配置；  2. 接口异常测试，返回的错误码正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-00304] 聚合过滤链的过滤器

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00304 |
| **Type** | Valid |
| **Description** | 每个过滤器都可以被激活——通过在建模中的 SecurityEventFilterChain 对象上聚合的对应的过滤器对象； |
| **Upstream ID** | SWS\_AIDSM\_00304 |
| **Dependencies** | RS\_Ids\_00300 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：idsM应用过滤链实现完成  主要测试点：每个过滤器都是否可以被激活成功；接口异常测试，返回的错误码是否正确；  成功标准：  1. 每个过滤器都可以被激活成功；  2. 接口异常测试，返回的错误码正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-00305] 过滤链中过滤器顺序

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00305 |
| **Type** | Valid |
| **Description** | IdsM应当对报告的SEv按照（机器状态、每N转发、聚合、阈值）顺序执行该SEv所属的安全事件类型所有被激活的过滤器  如果SEv没有通过某个过滤器，那么IdsM应当直接丢弃该SEv，而不对其执行后续其他过滤器策略 |
| **Upstream ID** | SWS\_AIDSM\_00305  SWS\_AIDSM\_00306 |
| **Dependencies** |  |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：每个过滤器都可以被激活成功  主要测试点：安全事件类型所有被激活的过滤器是否成功；是否按照机器状态、每N转发、聚合、阈值顺序进行过滤；SEv没有通过某个过滤器，那么IdsM直接丢弃该SEv是否成功；  成功标准：  1．安全事件类型所有被激活的过滤器成功；  2．按照机器状态、每N转发、聚合、阈值顺序进行过滤成功；  3．SEv没有通过某个过滤器，那么IdsM直接丢弃该SEv成功； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 机器状态过滤器

### [SWRD-IDSM-00401] 机器状态过滤规则

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00401 |
| **Type** | Valid |
| **Description** | 执行机器状态过滤策略——如果IdsM判断当前机器状态等于SecurityEventStateFilter.blockIfStateActiveAp中的状态，那么IdsM应当丢弃该SEv； |
| **Upstream ID** | SWS\_AIDSM\_00401 |
| **Dependencies** | RS\_Ids\_00320 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：安全事件类型所有被激活的过滤器实现完成  主要测试点：执行机器状态过滤策略是否成功；当前机器状态是否等于SecurityEventStateFilter.blockIfStateActiveAp中的状态；等于SecurityEventStateFilter.blockIfStateActiveAp中的状态，IdsM是否丢弃该SEv；  成功标准：  1．执行机器状态过滤策略成功；  2．等于SecurityEventStateFilter.blockIfStateActiveAp中的状态，IdsM丢弃该SEv成功； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 机器状态过滤器

### [SWRD-IDSM-00501] 定采样值

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00501 |
| **Type** | Valid |
| **Description** | IdsM应当为SEv初始化采样过滤器，以至于第一个收到的应当被转发，执行采样过滤策略——对于每个SecurityEventDefinition（即每个安全事件类型），定义一个采样值N（SecurityEventOneEveryNFilter.n），IdsM将要丢弃N-1个，转发第N个； |
| **Upstream ID** | SWS\_AIDSM\_00501  SWS\_AIDSM\_00502 |
| **Dependencies** | RS\_Ids\_00330 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：安全事件类型所有被激活的过滤器实现完成  主要测试点：IdsM为SEv初始化采样过滤器，第一个收到是否被转发；执行的采样过滤是否丢弃N-1个，转发第N个；接口异常测试，返回的错误码是否正确；  成功标准：   1. 执行的采样过滤可以丢弃N-1个，转发第N个； 2. IdsM为SEv初始化采样过滤器，第一个收到能够被转发； 3. 接口异常测试，返回的错误码正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 聚合过滤器

### [SWRD-IDSM-00601] 聚合Sev的周期处理事件

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00601 |
| **Type** | Valid |
| **Description** | 集成商应当通过参数SecurityEventAggregationFilter.aggregationIntervalLength配置聚合过滤器的固定时间间隔;聚合过滤器在聚合时间间隔内不应当转发任何进来的SEv;在一个聚合时间周期，没有一个相同类型的SEv进入聚合过滤器，那么什么也不做;在一个聚合时间周期，如果相同类型的SEv有一个或者多个进来到聚合过滤器，则一个SEv将要转发到后续处理； |
| **Upstream ID** | SWS\_AIDSM\_00600 SWS\_AIDSM\_00601 SWS\_AIDSM\_00602  SWS\_AIDSM\_00603 SWS\_AIDSM\_00604 |
| **Dependencies** |  |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：安全事件类型所有被激活的过滤器实现完成  主要测试点：配置聚合过滤器的固定时间间隔是否成功；一个聚合时间周期，没有一个相同类型的SEv进入聚合过滤器，是否有其他行为；相同类型的SEv有一个或者多个进来到聚合过滤器接口异常测试，一个SEv将是否转发到后续处理；  成功标准：   1. 配置聚合过滤器的固定时间间隔正确； 2. 一个聚合时间周期，没有一个相同类型的SEv进入聚合过滤器，没有其他行为；   3. 相同类型的SEv有一个或者多个进来到聚合过滤器接口异常测试，一个SEv可以转发到后续处理； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-00605] 选定转发的Sev的使用聚合数据处理

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00605 |
| **Type** | Valid |
| **Description** | 在一个聚合时间周期，聚合的SEv将要被转发后续处理——如果SecurityEventAggregationFilter.contextDataSource等于IDSM\_FILTERS\_CTX\_USE\_FIRST，那么聚合的SEv应当使用第一个原始SEv的context data作为聚合SEv的context data；在一个聚合时间周期，聚合的SEv将要被转发后续处理——如果SecurityEventAggregationFilter.contextDataSource等于IDSM\_FILTERS\_CTX\_USE\_LAST，那么聚合的SEv应当使用最后一个原始SEv的context data作为聚合SEv的context data；在一个聚合时间周期，聚合的SEv将要被转发后续处理——聚合SEv的时间戳应当使用和context data一样来源{第一个或者最后一个原始SEv}； |
| **Upstream ID** | SWS\_AIDSM\_00605 SWS\_AIDSM\_00606 SWS\_AIDSM\_00607 |
| **Dependencies** |  |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：聚合Sev的周期处理实现完成  主要测试点：SecurityEventAggregationFilter.contextDataSource是否等于IDSM\_FILTERS\_CTX\_USE\_FIRST；SecurityEventAggregationFilter.contextDataSource是否等于IDSM\_FILTERS\_CTX\_USE\_LAST；聚合SEv的时间戳是否使用和context data一样来源；  成功标准：  1．SecurityEventAggregationFilter.contextDataSource等于IDSM\_FILTERS\_CTX\_USE\_FIRST，那么聚合的SEv使用第一个原始SEv的context data作为聚合SEv的context data；  2． SecurityEventAggregationFilter.contextDataSource等于IDSM\_FILTERS\_CTX\_USE\_LAST，那么聚合的SEv使用最后一个原始SEv的context data作为聚合SEv的context data；  3．聚合SEv的时间戳使用和context data一样来源； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 阈值过滤器

### [SWRD-IDSM-00701] 阈值N及应用规则

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00701 |
| **Type** | Valid |
| **Description** | 配置参数SecurityEventThresholdFilter.thresholdNumber用来配置指定类型的阈值N，当阈值过滤器在指定时间周期内收到的相同类型原始SEv小于阈值N时候，阈值过滤器应当drop这些原始SEv；配置参数SecurityEventThresholdFilter.thresholdNumber用来配置指定类型的阈值N，当阈值过滤器在指定时间周期内收到的相同类型原始SEv大于等于阈值N时候，阈值过滤器应当转发这些原始SEv到后续处理； |
| **Upstream ID** | SWS\_AIDSM\_00701 SWS\_AIDSM\_00702 |
| **Dependencies** | RS\_Ids\_00350 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：聚合数据处理功能实现完成  主要测试点：阈值过滤器在指定时间周期内收到的相同类型原始SEv小于阈值N时候，阈值过滤器是否drop这些原始SEv；当阈值过滤器在指定时间周期内收到的相同类型原始SEv大于等于阈值N时候，阈值过滤器是否转发这些原始SEv到后续处理；  成功标准：  1阈值过滤器在指定时间周期内收到的相同类型原始SEv小于阈值N时候，阈值过滤器应当成功drop这些原始SEv；  2当阈值过滤器在指定时间周期内收到的相同类型原始SEv大于等于阈值N时候，阈值过滤器应当成功转发这些原始SEv到后续处理； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 时间戳信息配置

### [SWRD-IDSM-00801] 时间戳信息标识设置

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00801 |
| **Type** | Valid |
| **Description** | 如果IdsmInstance.timestampFormat没有设置，那么IdsM不会添加时间戳给QSEv，同时也会忽略每个报告事件接口时间戳参数中的时间戳信息；如果IdsmInstance.timestampFormat被设置为“AUTOSAR”，并且ara::idsm::EventReporter::ReportEvent函数被无时间戳参数调用，IdsM将会添加时间戳信息(来自引用为IdsPlatformInstantiation.timeBase的TimeSync::TimeBaseResource) 到QSEv；如果IdsmInstance.timestampFormat被设置，并且ara::idsm::EventReporter::ReportEvent函数被有时间戳参数调用，IdsM应当用这个提供的时间戳信息到QSEv；如果IdsmInstance.timestampFormat被设置但不是“AUTOSAR”，并且ara::idsm::EventReporter::ReportEvent函数被无时间戳参数调用，IdsM将会添加时间戳信息(来自一个时间应用软件通过TimestampProvider的callback，这种需要OEM提供自己的时间应用来实现) 到QSEv；  如果IdsmInstance.timestampFormat被设置，并且ara::idsm::EventReporter::ReportEvent函数被有时间戳参数调用，IdsM应当用这个提供的时间戳信息到QSEv； |
| **Upstream ID** | SWS\_AIDSM\_00801 SWS\_AIDSM\_00802 SWS\_AIDSM\_00803  SWS\_AIDSM\_00804 SWS\_AIDSM\_00805 |
| **Dependencies** | RS\_Ids\_00503 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：阈值过滤处理实现完成  主要测试点：IdsmInstance.timestampFormat没有设置，是否会忽略时间戳信息；IdsmInstance.timestampFormat被设置为“AUTOSAR”， ara::idsm::EventReporter::ReportEvent无时间戳调用，IdsM是否会添加时间戳信息；IdsmInstance.timestampFormat被设置，ara::idsm::EventReporter::ReportEvent有时间戳调用，IdsM是否会添加时间戳信息；IdsmInstance.timestampFormat设置不是“AUTOSAR”，ara::idsm::EventReporter::ReportEvent没有时间戳，是否添加时间戳信息；IdsmInstance.timestampFormat被设置，有时间戳参数调用，IdsM是否提供的时间戳信息到QSEv；  成功标准：  1 IdsmInstance.timestampFormat没有设置，IdsM不会添加时间戳给QSEv并忽略时间戳信息；  2. IdsmInstance.timestampFormat被设置为“AUTOSAR”， ara::idsm::EventReporter::ReportEvent无时间戳调用，IdsM会添加时间戳信息；  3.IdsmInstance.timestampFormat被设置，ara::idsm::EventReporter::ReportEvent有时间戳调用，IdsM会添加时间戳信息；  4. IdsmInstance.timestampFormat设置不是“AUTOSAR”，ara::idsm::EventReporter::ReportEvent没有时间戳，添加时间戳信息成功  5. IdsmInstance.timestampFormat被设置，有时间戳参数调用，IdsM提供的时间戳信息到QSEv |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-00806] 时间戳格式

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00806 |
| **Type** | Valid |
| **Description** | 如果带有时间戳参数的调用ara::idsm::EventReporter::ReportEvent函数，IdsM 将通过 2 个最高有效位截断该值（时间戳参数），即保留 62 个最低有效位以供进一步使用； |
| **Upstream ID** | SWS\_AIDSM\_00806 |
| **Dependencies** | RS\_Ids\_00503 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：密钥管理模块实现完成 ，导入导出接口实现完成  主要测试点：IdsM 是否通过 2 个最高有效位截断该值（时间戳参数），即保留 62 个最低有效位使用；  成功标准：  1．IdsM通过 2 个最高有效位截断该值（时间戳参数），保留 62 个最低有效位使用成功； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-00807] 自定义时间戳

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00807 |
| **Type** | Valid |
| **Description** | TimestampProvider SWCL注册一个callback通过调用ara::idsm::RegisterTimestampProvider，这个callback将要返回一个时间戳； |
| **Upstream ID** | SWS\_AIDSM\_00807 |
| **Dependencies** | RS\_Ids\_00503 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：注册callback是否正确；callback将要返回一个时戳是否正确；  成功标准：  1．注册callback正确；  2．callback返回的时戳正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 外发 QSEvs

### [SWRD-IDSM-00901] 配置IDSR

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00901 |
| **Type** | Valid |
| **Description** | 如果IdsPlatformInstantiation聚合了角色networkInterface中的PlatformModuleEthernetEndpointConfiguration，IdsM应使用IDS-protocol协议发送QSEvs到通过 PlatformModuleEthernetEndpointConfiguration 配置的端点（IdsR）； |
| **Upstream ID** | SWS\_AIDSM\_00901 |
| **Dependencies** | RS\_Ids\_00510 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：时间戳信息标识设置实现完成  主要测试点：配置IDSR是否正确；接口异常测试，返回的错误码是否正确；  成功标准：  1.配置IDSR结果正确；  2.接口异常测试，返回的错误码正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-00902] IDS 消息分片

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-00902 |
| **Type** | Valid |
| **Description** | IdsM 应将 IDS 消息分离头的Message ID 字段设置为全零（0x00000000）； |
| **Upstream ID** | SWS\_AIDSM\_00902 |
| **Dependencies** |  |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：时间戳信息标识设置完成  主要测试点：IDS 消息分离头的Message ID 字段设置是否为全零；接口异常测试，返回的错误码是否正确；  成功标准：  1 IDS 消息分离头的Message ID 字段设置为全零；  2 接口异常测试，返回的错误码正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 外发Qsevs添加认证信息（3期做）

### [SWRD-IDSM-01001] 签名标识设置

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-01001 |
| **Type** | Valid |
| **Description** | 如果IdsM实例中聚合了角色signatureSupportAp的IdsmSignatureSupportAp对象，那么IdsM应当附加一个签名信息到每个QSEv,以便QSEv进行外发到IdsR和本地存储； |
| **Upstream ID** | SWS\_AIDSM\_01001 |
| **Dependencies** | RS\_Ids\_00505 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：配置IDSR实现完成  主要测试点：IdsM是否附加一个签名信息到每个QSEv；QSEv是否进行外发到IdsR和本地存储；  成功标准：  1．IdsM附加一个签名信息到每个QSEv成功；  2 . QSEv进行外发到IdsR和本地存储成功； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-01002] 签名使用算法和key slot引用

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-01002 |
| **Type** | Valid |
| **Description** | IdsM 使用参数 IdsmSignatureSupportAp.cryptoPrimitive 中指定的签名算法和角色 keySlot 中的 IdsmSignatureSupportAp 引用的 CryptoKeySlot 的密钥标识； |
| **Upstream ID** | SWS\_CRYPT\_00005 |
| **Dependencies** |  |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：NeuSAR-aCore平台  前提条件：配置IDSR实现完成  主要测试点：IdsM使用签名算法和密钥标识是否正确；  成功标准：  1.IdsM使用签名算法和密钥标识结果正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 速率和流量限制

### [SWRD-IDSM-001103] 速率限制

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-01103 |
| **Type** | Valid |
| **Description** | IdsM在外发时将会drop一个QSEv——如果该QSEv的外发将会引起当前时间周期内（IdsmRateLimitation.timeInterval）外发的QSEv的个数超过设定值（IdsmRateLimitation. maxEventsInInterval）； |
| **Upstream ID** | SWS\_AIDSM\_01101 SWS\_AIDSM\_01103 |
| **Dependencies** | RS\_Ids\_00511 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：虚拟机环境  前提条件：外发Qsevs添加认证信息实现完成  主要测试点：速率设定值是否正确；速率设定值比较结果是否正确；  成功标准：  1．速率设定值正确；  2．速率设定值比较结果正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | QM(C) |

### [SWRD-IDSM-001104] 流量限制

|  |  |
| --- | --- |
| **SWRD-ID** | SWRD-IDSM-01104 |
| **Type** | Valid |
| **Description** | IdsM在外发时将会drop一个QSEv——如果该QSEv的外发将会引起当前时间周期内（IdsmTrafficLimitation.timeInterval）外发的QSEv总字节数超过设定值（IdsmTrafficLimitation.maxBytesInInterval）； |
| **Upstream ID** | SWS\_AIDSM\_01101 SWS\_AIDSM\_01104 |
| **Dependencies** | RS\_Ids\_00511 |
| **Verification method** | 评审与测试 |
| **Verification Criteria** | 验证环境：虚拟机环境  前提条件：外发Qsevs添加认证信息实现完成  主要测试点：流量限制设定值是否正确；流量限制设定值比较结果是否正确；  成功标准：  1．流量限制设定值正确；  2．流量限制设定值比较结果正确； |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **CR** | - |
| **Risk** | 无 |
| **Change Type** | QM(C) |

## 依靠IAM来限制（3期做）

### [SWRD-IDSM-01201] 依靠IAM来限制

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01201 |
| **Type** | Valid |
| **Description** | IdsM 应限制进程可以生成的安全事件类型——通过进程在角色securityEvent中引用的SecurityEventDefinitions（type）限制，配置到进程执行清单中； |
| **Upstream ID** | SWS\_AIDSM\_01201 |
| **Dependencies** | RS\_Ids\_00200 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证环境：上位机及NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：IdsM 是否限制进程可以生成的安全事件类型；IdsM中的配置IAM是否正常；  成功标准：   1. IdsM 限制进程可以生成的安全事件类型成功；   2. IdsM中的配置IAM成功； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 诊断访问（3期做）

### [SWRD-IDSM-01301] 定义安全事件对应的诊断DTC代码

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01301 |
| **Type** | Valid |
| **Description** | 如果一个事件已成功限定并且该事件被配置为持久化（即，SecurityEventContextProps.persistentStorage == 1），则 IdsM 将限定事件引用的 DTC 并将事件数据作为快照记录添加到它； |
| **Upstream ID** | SWS\_AIDSM\_01301 |
| **Dependencies** | RS\_Ids\_00400 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证环境：NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：IdsM 是否限定事件引用的 DTC 并将事件数据作为快照记录添加到它；  成功标准：   1. IdsM限定事件引用的 DTC 并将事件数据作为快照记录添加到它成功； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-01302] 获取报告模式

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01302 |
| **Type** | Valid |
| **Description** | IdsM应该提供一个诊断服务来获取报告模式（通过指定安全事件id），返回该安全事件类型的当前报告模式； |
| **Upstream ID** | SWS\_AIDSM\_01302 |
| **Dependencies** | RS\_Ids\_00700 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境：NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：使用一个诊断服务来获取报告模式是否成功；  成功标准：   1. 使用一个诊断服务来获取报告模式成功； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** |  |

### [SWRD-IDSM-01303]支持密钥协商

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01303 |
| **Type** | Valid |
| **Description** | IdsM应该提供一个诊断服务来设置指定安全事件类型的报告模式（通过指定安全事件id，报告模式）； |
| **Upstream ID** | SWS\_AIDSM\_01303 |
| **Dependencies** | RS\_Ids\_00700 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证环境：NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：使用一个诊断服务来设置指定安全事件类型的报告模式；  成功标准：   1. 使用一个诊断服务来设置指定安全事件类型的报告模式成功。 |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## idsM报告Sevs

### [SWRD-IDSM-01401] IdsM自身报告安全事件内容

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01401 |
| **Type** | Valid |
| **Description** | IdsM可以报告的安全事件在<SWS\_IdsM\_91015>(2.11.2)中，对应于每个安全事件的十六进制值在 SecXT 中集中定义； |
| **Upstream ID** | SWS\_AIDSM\_01401 SWS\_IdsM\_91015 |
| **Dependencies** | RS\_Ids\_00820 RS\_Ids\_00810 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：每个报告的安全事件的十六进制值是否正确；  成功标准：  1．报告的安全事件的十六进制值正确； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-01402] 自身安全事件优先级

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01402 |
| **Type** | Valid |
| **Description** | IdsM应该确保IdsM内部安全事件可以被处理，即使没有buffer可用；  IdsM内部的SEvs不被rate和traffic策略限制； |
| **Upstream ID** | SWS\_AIDSM\_01402 SWS\_AIDSM\_01403 |
| **Dependencies** | RS\_Ids\_00820 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：IdsM是否确保IdsM内部安全事件可以被处理，即使没有buffer可用；IdsM内部的SEvs是否rate和traffic策略限制；  成功标准：   1. IdsM确保IdsM内部安全事件可以被处理成功，即使没有buffer可用；   2. IdsM内部的SEvs不被rate和traffic策略限制； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## IdsM接收Sev

### [SWRD-IDSM-01501] IdsM自身报告安全事件内容

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01501 |
| **Type** | Valid |
| **Description** | IdsM缓存接收到的SEv,直到被完全处理结束; |
| **Upstream ID** | IdsM\_User\_defined\_0001 |
| **Dependencies** | RS\_Ids\_00210 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：IdsM是否缓存接收到的SEv到被完全处理结束；  成功标准：  1．IdsM缓存接收到的SEv到被完全处理结束成功； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## IdsM存储Sev（3期做）

### [SWRD-IDSM-01601] IdsM自身报告安全事件内容

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01601 |
| **Type** | Valid |
| **Description** | IdsM应当支持本地持久化存储QSEv用户定义的诊断内存区（与其他诊断内存区隔离），可以供后面诊断仪等设备读取访问，而不依赖于网络传输。  存储格式：  IDS-Protocol header  IdsM instance ID  sensor module instance ID  合格的 SEv 的标识符—eventid  该QSEv的计数（聚合过滤链）  时间戳【可选】  上下文信息【可选】  认证签名信息【可选】 |
| **Upstream ID** | IdsM\_User\_defined\_0002 |
| **Dependencies** | RS\_Ids\_00400 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：是否支持本地持久化存储QSEv；持久化存储格式是否正确；  成功标准：   1. 支持本地持久化存储QSEv；   2. 持久化存储格式正确 |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 上位机可配置

### [SWRD-IDSM-01701] 上位机配置事件上报

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01701 |
| **Type** | Valid |
| **Description** | 应当可以配置哪些安全事件报告给IdsM—依赖于一个工程特定的安全分析，有些安全事件可以被忽略，有些需要被报告处理，为了避免不必要的call to IdsM，因此应当可以在每个IdsM实例配置需要被处理的每个安全事件类型; |
| **Upstream ID** | IdsM\_User\_defined\_0003 |
| **Dependencies** | RS\_Ids\_00600 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：是否可以配置哪些安全事件报告给IdsM；  成功标准：  1．可以成功配置哪些安全事件报告给IdsM； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-01702] 上位机配置合格过滤链

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01702 |
| **Type** | Valid |
| **Description** | 在IdsM上可以被配置哪个合格过滤链应用到一个SEv—依赖于一个工程特定的安全分析，不同的安全事件类型可以去适配不同的过滤规则。 |
| **Upstream ID** | IdsM\_User\_defined\_0004 |
| **Dependencies** | RS\_Ids\_00610 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：是否可以配置合格过滤链应用；是否可以适配不同的过滤规则；  成功标准：  1. 支持配置合格过滤链应用；  2. 可以适配不同的过滤规则； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-01703] 上位机配置本地持久化存储（3期做）

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01703 |
| **Type** | Valid |
| **Description** | 可以为QSEv配置是否进行本地持久化存储—依赖于一个工程特定的安全分析和可用资源（存储），可以配置QSEv是否持久化存储（不关联到具体的安全事件类型） |
| **Upstream ID** | IdsM\_User\_defined\_0005 |
| **Dependencies** | RS\_Ids\_00620 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：配置是否进行本地持久化存储；  成功标准：  1. 配置本地持久化存储成功； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-01704] 上位机配置IdsR

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01704 |
| **Type** | Valid |
| **Description** | IdsM中，QSEv是否需要传送给IdsR需要被配置—依赖于一个工程的特定安全分析和可用资源（带宽），决定QSEv是否发送到IdsR |
| **Upstream ID** | IdsM\_User\_defined\_0006 |
| **Dependencies** | RS\_Ids\_00630 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：QSEv是否发送到IdsR；  成功标准：  1. QSEv发送到IdsR成功； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 软件升级

### [SWRD-IDSM-01801] 更新配置

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01801 |
| **Type** | Valid |
| **Description** | 【需要重启】替换完整的过滤链配置：IdsM应该允许替换完整的过滤链配置—在生产线编程结束、车间中的 ECU 初始化或通过 OTA 推出新更新等情况下，应该可以更换完整的过滤器链配置。 |
| **Upstream ID** | IdsM\_User\_defined\_0007 |
| **Dependencies** | RS\_Ids\_00710 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：是否可以替换完整的过滤链配置；  成功标准：  1．替换完整的过滤链配置成功； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 安全传感器

### [SWRD-IDSM-01901] 记录读取历史

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01901 |
| **Type** | Valid |
| **Description** | 支持检测 QSEv 记录的操作：内存堆栈应能够选择性地检测对持久 QSEv 记录的操作。 如果检测到对 QSEv 记录的操作，则内存堆栈应产生安全事件报告。 |
| **Upstream ID** | IdsM\_User\_defined\_0008 |
| **Dependencies** | RS\_Ids\_00430 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：是否支持检测 QSEv 记录的操作；  成功标准：  1．支持检测 QSEv 记录的操作； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-01902] 智能传感器

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-01902 |
| **Type** | Valid |
| **Description** | 基本软件安全事件：和安全相关的基础软件模块应当报告安全事件给IdsM—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。 |
| **Upstream ID** | IdsM\_User\_defined\_0009 |
| **Dependencies** | RS\_Ids\_00810 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM相关配置完成  主要测试点：基本软件是否报告安全事件；  成功标准：  1．基本软件报告安全事件成功； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## 上位机配置

### [SWRD-IDSM-02001] P2与安全事件相关的要求

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02001 |
| **Type** | Valid |
| **Description** | 安全提取应当支持定义和配置安全事件，它应尽可能去传送事件（来自一个传感器和安全相关联的信息）到IdsM去处理；定义安全事件的过滤连—目的是过滤安全事件，安全提取应当支持安全事件的过滤链的定义；安全事件的限制过滤—目的是限制QSEvs外发的网络负载，安全提取应当支持安全事件的限制过滤定义；关联安全事件和ECU(CP)/machine(AP)—目的是基于一个给定的ECU报告安全事件  安全提取应当支持定义ECU和安全事件的关系；定义安全事件的默认报告模式，安全提取应当支持安全事件的不同细节的默认报告模式（5个：OFF/brief/details/brief\_bypass\_filter/detail\_bypass\_filter）；关联安全事件和一个平台模块——目的是报告一个安全事件从一个给定的平台模块，安全提取应支持安全事件与作为安全问题主题的平台模块之间关系的定义，平台模块是基本软件模块（适用于经典平台）或功能集群（适用于自适应平台），配置安全事件从给定的平台模块（IdsM for AP）；支持定义安全事件的严重等级——目的是给报告的安全事件添加额外的严重等级信息，安全提取应当支持定义安全事件的严重等级；为一个安全事件定义产生它的安全传感器ID，安全提取应当支持为安全事件定义一个安全传感器的ID； |
| **Upstream ID** | IdsM\_User\_defined\_0010 IdsM\_User\_defined\_0011 IdsM\_User\_defined\_0012 IdsM\_User\_defined\_0013 IdsM\_User\_defined\_0016 IdsM\_User\_defined\_0017 IdsM\_User\_defined\_0020 IdsM\_User\_defined\_0022 |
| **Dependencies** | RS\_SECXT\_00001 RS\_SECXT\_00002 RS\_SECXT\_00003 RS\_SECXT\_00004 RS\_SECXT\_00007 RS\_SECXT\_00008  RS\_SECXT\_00018 RS\_SECXT\_00023 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：上位机可配置  主要测试点：安全提取是否支持定义和配置安全事件；是否支持定义安全事件的过滤连；是否支持安全事件的限制过滤；是否关联安全事件和ECU(CP)/machine(AP)；是否支持定义安全事件的默认报告模式；是否支持关联安全事件和一个平台模块；是否支持定义安全事件的严重等级；安全提取是否支持为安全事件定义一个安全传感器的ID；  成功标准：   1. 安全提取支持定义和配置安全事件；   2. 支持定义安全事件的过滤连；  3. 支持安全事件的限制过滤；  4. 关联安全事件和ECU(CP)/machine(AP)；  5. 支持定义安全事件的默认报告模式；  6. 支持关联安全事件和一个平台模块；  7. 支持定义安全事件的严重等级；  8. 安全提取支持为安全事件定义一个安全传感器的ID； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-02002] P3与安全事件相关的要求

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02002 |
| **Type** | Valid |
| **Description** | 关联安全事件和一个通讯总线——目的是可以从给定的通信总线报告一个安全事件,如果安全事件用于报告与相关通信总线有关的问题，则安全提取应支持安全事件和通信总线之间关系的定义; 支持安全事件的持久化存储——目的是在指定ECU上存储合格安全事件  安全提取应当支持配置给定的安全事件的持久化存储,配置来源于给定的通信总线的安全事件被报告; 支持安全事件带有上下文数据【可选】——目的是报告安全事件可以带有上下文数据,安全提取应当支持一个安全事件的可选上下文数据的定义，应该可以配置使用附加上下文数据报告给定的安全事件; 安全事件预合格规定——目的是报告预合格安全事件;作为经过过滤链成为QSEv的替代方案，（智能）传感器应能够报告预合格的安全事件，该事件应由 IdsM 直接作为合格的安全事件处理;关联安全事件和应用——目的是从给定的应用报告一个安全事件,安全提取应当支持安全事件和产生它的应用的关系定义; |
| **Upstream ID** | IdsM\_User\_defined\_0014 IdsM\_User\_defined\_0015  IdsM\_User\_defined\_0018 IdsM\_User\_defined\_0019  IdsM\_User\_defined\_0021 |
| **Dependencies** | RS\_SECXT\_00005 RS\_SECXT\_00006 RS\_SECXT\_00009 RS\_SECXT\_00012 RS\_SECXT\_00021 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：上位机可配置  主要测试点：是否支持关联安全事件和一个通讯总线；是否支持安全事件的持久化存储；是否支持安全事件带有上下文数据；是否支持安全事件预合格规定；是否支持关联安全事件和应用；  成功标准：   1. 支持关联安全事件和一个通讯总线； 2. 支持安全事件的持久化存储； 3. 支持安全事件带有上下文数据； 4. 支持安全事件预合格规定； 5. 支持关联安全事件和应用； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-02003] P2与 IdsM 实例相关的要求

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02003 |
| **Type** | Valid |
| **Description** | IdsM实例的可选配置——目的是定义和部分配置IdsM实例，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；给一个IdsM实例分配网络配置，不管是AP还是CP，安全提取模板应当描述一个IdsM实例和它的网络配置怎样关联的，除安全事件外，安全提取还应部分有助于 IdsM 实例的配置； |
| **Upstream ID** | IdsM\_User\_defined\_0023 IdsM\_User\_defined\_0027 |
| **Dependencies** | RS\_SECXT\_00013 RS\_SECXT\_00017 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：上位机可配置  主要测试点：是否支持IdsM实例的可选配置；是否支持给一个IdsM实例分配网络配置；  成功标准：   1. 支持IdsM实例的可选配置； 2. 支持给一个IdsM实例分配网络配置； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-02004] P3与 IdsM 实例相关的要求

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02004 |
| **Type** | Valid |
| **Description** | 时间源提供的可选配置——目的是为了可以配置安全事件的时间戳信息（可选）,IdsM如果被配置则给QSEv打上时间戳，安全提取应当支持配置IdsM实例是否提供时间戳信息给QSEv，如果是那么时间源使用autosar的还是OEM第三方指定的；配置时间戳格式——目的是根据配置格式去添加时间戳，安全提取应当支持配置IdsM使用何种时间格式添加到QSEv，格式可以是autosar标准的或者第三方的；配置安全事件消息是否带有认证信息【可选】，不管在AP还是CP，安全提取都应当支持配置IdsM实例去添加认证信息到所有它要发送到网络的的安全事件消息【可选】； |
| **Upstream ID** | IdsM\_User\_defined\_0024 IdsM\_User\_defined\_0025  IdsM\_User\_defined\_0026 |
| **Dependencies** | RS\_SECXT\_00015 RS\_SECXT\_00016 RS\_SECXT\_00014 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：上位机可配置  主要测试点：是否支持时间源提供的可选配置；是否支持配置时间戳格式；是否支持配置安全事件消息带有认证信息；  成功标准：   1. 支持时间源提供的可选配置； 2. 支持配置时间戳格式； 3. 支持配置安全事件消息带有认证信息； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## AUTOSAR 方法相关的要求

### [SWRD-IDSM-02101] 与 AUTOSAR 方法相关的要求

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02101 |
| **Type** | Valid |
| **Description** | 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,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; 标定autosar标准安全事件,安全提取应当支持标定autosar标准的安全事件; 支持定义IDS的范围和系统边界——从系统级别描述一个IDS  安全提取应当支持在设计和实现阶段定义一个IDS的边界,IDS 设计通常涉及车辆内所有 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; 支持部分/完全交换安全定义——目的是为了IDS的分布式开发（或者合作开发）,安全提取应当支持部分或者完全的安全事件定义的交换在不同的开发伙伴之间,为了实现IDS的分布式开发（比如不同的传感器可能是来源不同的开发伙伴），因此需要使用安全提取文件去描述整个IDS的设计，每个开发伙伴都可以获取和增加，或者由设计者统一定下文档，分发给各个开发伙伴; |
| **Upstream ID** | IdsM\_User\_defined\_0028 IdsM\_User\_defined\_0029 IdsM\_User\_defined\_0030 IdsM\_User\_defined\_0031 |
| **Dependencies** | RS\_SECXT\_00011 RS\_SECXT\_00010 RS\_SECXT\_0019  RS\_SECXT\_00020 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：符合autosar整体需求  主要测试点：是否支持与 IdsM 模块的安全事件相关处理；是否支持标定autosar标准的安全事件；是否支持定义IDS的范围和系统边界；是否支持部分/完全交换安全定义；  成功标准：   1. 支持与 IdsM 模块的安全事件相关处理； 2. 支持标定autosar标准的安全事件； 3. 支持定义IDS的范围和系统边界 4. 支持部分/完全交换安全定义； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## IDS协议通用要求

### [SWRD-IDSM-02201] P2通用要求

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02201 |
| **Type** | Valid |
| **Description** | IDS协议的主要作用是IdsM传输QSEv到IdsR；IDS协议包含标准的安全事件帧和三个可选的域。它提供一些选项来发送最小的QSEv数据和发送带有更多详细内容扩展数据的QSEv；标准的QSEv是不携带其他数据的【即只有事件ID】；IDS协议使用大端字节序——网络序列，IDS消息从0开始增加字节；IDS协议独立于硬件和底层网络机制，它被优化设计既可以在以太网，也可以运行在标准的CAN总线（仅携带最小数据（event id））； |
| **Upstream ID** | PRS\_Ids\_00001 PRS\_Ids\_00002 PRS\_Ids\_00003 PRS\_Ids\_00004 PRS\_Ids\_00005 |
| **Dependencies** | RS\_Ids\_00510 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM初始化完成  主要测试点：是否支持提供一些选项来发送最小的QSEv数据；是否支持发送带有更多详细内容扩展数据的QSEv；是否支持标准QSEv不携带事件ID；是否IDS协议使用大端字节序；  成功标准：   1. 支持提供一些选项来发送最小的QSEv数据； 2. 支持发送带有更多详细内容扩展数据的QSEv； 3. 支持标准QSEv不携带事件ID； 4. IDS协议使用大端字节序； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-02202] P3通用要求（P3做）

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02202 |
| **Type** | Valid |
| **Description** | QSEv携带时间戳：如果除了 IdsR 提供的时间戳之外还需要更精确的时间戳，传感器或 IdsM 可以为每个 QSEv 添加时间戳，该选项必须由协议头中的相应配置位设置；QSEv携带上下文数据：上下文数据包含了传感器特定信息，IdsM不知道上下文的内容和数据结构，只是转发给IdsR，该选项必须由协议头中的相应配置位设置；QSEv携带签名：如果需要安全通信，可以给每个QSEv添加签名信息。该选项必须由协议头中的相应配置位设置； |
| **Upstream ID** | PRS\_Ids\_00400 PRS\_Ids\_00500 PRS\_Ids\_00600 |
| **Dependencies** | RS\_Ids\_00505 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM初始化完成  主要测试点：是否支持QSEv携带时间戳；是否支持QSEv携带上下文数据；是否支持QSEv携带签名；  成功标准：   1. 支持QSEv携带时间戳； 2. 支持QSEv携带上下文数据； 3. 支持QSEv携带签名； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## IDS 事件框架

### [SWRD-IDSM-02301] 协议版本和标头

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02301 |
| **Type** | Valid |
| **Description** | IDS事件帧长8 Bytes；IDS协议版本信息，bit 7- bit4(大端字节序),取值范围0-15，当前版本指定为 1，计算公式：协议版本=byte[0]&0XF0 >> 4；IDS协议头信息，包含特别功能开关的配置位  Bit[0]：上下文数据，0表示不包含，1表示包含  Bit[1]：时间戳，0表示不包含，1表示包含  Bit[2]：签名，0表示不包含，1表示包含  Bit[3]：保留  计算公式：协议头=byte[0]&0X0F；只有当 Timestamp、Context Data 或 Signature 可用时，相应的 Protocol Header Bit 才被设置为 1，Context Data 或 Signature 永远不会在 Length=0 的情况下传输；保留位应该被预置为0，接收者会忽略该位； |
| **Upstream ID** | PRS\_Ids\_00006 PRS\_Ids\_00008 PRS\_Ids\_00009 PRS\_Ids\_00010 PRS\_Ids\_00011 |
| **Dependencies** | 无 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsM接收信息完成  主要测试点：是否IDS事件帧长为8 Bytes；版本计算结果是否正确；Timestamp、Context Data 或 Signature 可用时， Protocol Header Bit 是否置为 1；Context Data 或 Signature 是否在 Length=0 时传输；是否支持保留位被预置为0；  成功标准：   1. IDS事件帧长为8 Bytes； 2. 版本计算结果正确； 3. Timestamp、Context Data 或 Signature 可用时， Protocol Header Bit 置为 1； 4. Context Data 或 Signature 不在 Length=0 时传输； 5. 支持保留位被预置为0； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-02302] IdsM 实例 ID 和传感器实例 ID

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02302 |
| **Type** | Valid |
| **Description** | IdsM 和传感器实例ID为2个字节的数据；发送安全事件的IdsM实例的唯一标识，取值范围0-1023.计算公式：IdsM实例ID（10 bit） = ((byte[2] & 0xC0) >> 6) | ((byte[1] << 2))；用来区分相同类型的传感器模块的多个实例，传感器实例ID取值范围0-63，如果传感器配置中只有一个实例，那么传感器实例ID的值默认为0，传感器实例ID在对应的基础软件配置中设置，获取传感器ID计算公式：ID (6 Bits) = (byte[2] & 0x3F)； |
| **Upstream ID** | PRS\_Ids\_00012 PRS\_Ids\_00013 PRS\_Ids\_00014 |
| **Dependencies** | 无 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：协议版本和标头解析完成  主要测试点：IdsM 和传感器实例ID2字节数据格式是否正确；发送安全事件的IdsM实例是否是唯一标识；是否用来区分相同类型的传感器模块的多个实例；  成功标准：   1. IdsM 和传感器实例ID2字节数据格式正确； 2. 发送安全事件的IdsM实例是唯一标识； 3. 能用来区分相同类型的传感器模块的多个实例； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-02303] 事件定义 ID

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02303 |
| **Type** | Valid |
| **Description** | 事件定义ID是一个安全事件唯一标识，它用来描述一个安全事件的种类；如果一个传感器产生多个相同类型的安全事件，则这个传感器称为事件实例；安全事件定义ID可以分为3个范围：  1. autosar内部ID: 0-0x7FFF (max. 32768 security events)  2. 客户自定义ID: 0x8000-0xFFFE (max. 32767 security events)  3. 无效ID：0xFFFF； |
| **Upstream ID** | PRS\_Ids\_00015 PRS\_Ids\_00016 PRS\_Ids\_00017 |
| **Dependencies** | 无 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：协议版本和标头解析完成  主要测试点：事件定义ID是否是一个安全事件唯一标识；是否支持识别传感器的事件实例；安全事件定义ID的范围是否正确；  成功标准：   1. 事件定义ID是一个安全事件唯一标识； 2. 支持识别传感器的事件实例； 3. 安全事件定义ID的范围正确； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-02304] 调用IdsM API的次数

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02304 |
| **Type** | Valid |
| **Description** | count字段代表该QSEv是call IdsM API的次数：一个事件创建，该字段初始化为1，聚合过滤中，会把多个相同类型的SEv聚合为一个，那么该字段需要修改为被聚合SEv的个数，如果安全事件是由smart sensor（已经进行过滤和预置count值）报告的，那么IdsM将会把预置count值进行累加，简而言之，就是IdsM进行处理时候，会把原始SEv的count进行累加，不管原来count是1还是N； |
| **Upstream ID** | PRS\_Ids\_00018 |
| **Dependencies** | 无 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsm初始化成功  主要测试点：调用IdsM API的次数计算是否正确；  成功标准：  1. 调用IdsM API的次数计算是否正确； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-02305] 保留项

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02305 |
| **Type** | Valid |
| **Description** | IDS协议的事件帧的byte[7]是保留字段；该保留字段全部预置为0，接收方将会忽略该字段； |
| **Upstream ID** | PRS\_Ids\_00019 PRS\_Ids\_00020 |
| **Dependencies** | 无 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsm初始化成功  主要测试点：保留项设置是否正确；  成功标准：  1. 保留项设置正确； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## IDS 协议中的时间戳 （P3做）

### [SWRD-IDSM-02401] 时间戳协议

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02401 |
| **Type** | Valid |
| **Description** | IDS协议提供时间戳作为配置选项；它在第一次检测到安全事件（第一次发生）时记录；毫秒是需要的，时间戳应该使用64 bit编码来适合单个CAN帧；在IDS协议中不同的时间戳源是可以配置的，bit[7]标识时间戳源，值为0表示使用AUTOSAR标准，值为1则使用OEM指定的，bit[6]保留使用；对于AUTOSAR时间格式，使用秒32 bits和纳秒30 bits；对于纳秒级别，仅提供30bit，可以编码为0—999999999ns，AUTOSAR的时间同步协议纳秒使用32bit编码，IDS协议的30bit截断不限制精度；秒用 32 位编码，可以表示大概127年范围；OEM时间源提供给用户可选的其他时间源，长度被限制为63bit.这种需要OEM的时间源应用提供接口，精度由OEM定义； |
| **Upstream ID** | PRS\_Ids\_00401 PRS\_Ids\_00402 PRS\_Ids\_00403 PRS\_Ids\_00404 PRS\_Ids\_00405 PRS\_Ids\_00406 PRS\_Ids\_00407PRS\_Ids\_00408 |
| **Dependencies** | RS\_Ids\_00502 RS\_Ids\_00503 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：接收数据功能完成  主要测试点：IDS协议提供时间戳是否作为配置选项；时间戳是否支持64 bit毫秒编码；是否支持时间戳源是配置；AUTOSAR时间格式，是否支持使用秒32 bits和纳秒30 bits；秒用 32 位编码，是否支持表示大概127年范围；提供30bit纳秒级别时间戳范围是否正确；是否支持OEM时间源；是否支持记录第一次检测到安全事件；  成功标准：   1. IDS协议提供时间戳作为配置选项； 2. 时间戳支持64 bit毫秒编码； 3. 支持时间戳源是配置； 4. AUTOSAR时间格式，支持使用秒32 bits和纳秒30 bits； 5. 秒用 32 位编码，支持表示大概127年范围； 6. 提供30bit纳秒级别时间戳范围正确； 7. 支持OEM时间源； 8. 支持记录第一次检测到安全事件； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## IDS 协议中的上下文数据 （P3做）

### [SWRD-IDSM-02501] 上下文数据协议

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02501 |
| **Type** | Valid |
| **Description** | IDS协议提供一个可选的flag来丰富被传输的标准的安全事件（给它携带更多详细信息），因此context data可以被添加，Context data是一个被传感器附加的二进制blob，这些数据包括安全事件的特定详细信息，可以被SOC等进行安全事件分析，IdsM不知道context data的内容和格式，只有产生该事件的传感器和SOC知道；"Context Data Size Long"包含4字节length字段,context data可以达到231-1字节；"Context Data Size Short"是带有1字节的length字段，context data最大可以是127字节；Context Data Length Encoding:表5.9是context data长度字段的编码方式，Context Data Byte[0] Bit[7]标记使用哪种长度：  值为0(short)：7bit长度信息被编码，context data范围1—127字节  值为1(long)：31bit长度信息，context data范围1—(231-1)字节； |
| **Upstream ID** | PRS\_Ids\_00501 PRS\_Ids\_00502 PRS\_Ids\_00503 PRS\_Ids\_00504 |
| **Dependencies** | 无 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：接收数据功能完成  主要测试点：IDS协议是否支持可选的flag来丰富被传输的标准的安全事件； Context Data Size Long字段长度是否正确；Context Data Size Short字段长度是否正确；context data长度字段的编码是否正确；  成功标准：   1. IDS协议支持可选的flag来丰富被传输的标准的安全事件； 2. Context Data Size Long字段长度正确； 3. Context Data Size Short字段长度正确； 4. context data长度字段的编码正确； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## IDS 协议中的签名数据 （P3做）

### [SWRD-IDSM-02601] 签名数据协议

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02601 |
| **Type** | Valid |
| **Description** | IDS协议提供一个可选的配置，可以给传输的QSEv添加签名，  一个数字签名可以被添加在IDS消息中；签名长度是2字节编码，范围为1—65535；签名数据范围是byte[2]—byte[65537]，签名的数据为：Event Frame + optional Timestamp + optional Context Data，  签名算法依赖于系统，IDS协议不规定任何特定的算法和格式； |
| **Upstream ID** | PRS\_Ids\_00601 PRS\_Ids\_00602 PRS\_Ids\_00603 |
| **Dependencies** | RS\_Ids\_00505 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：接收数据功能完成  主要测试点：IDS协议是否支持签名的可选的配置；签名字段长度是否正确；签名数据范围长度是否正确；  成功标准：   1. IDS协议支持签名的可选的配置； 2. 签名字段长度正确； 3. 签名数据范围长度正确； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## IDS 消息分离（P3做）

### [SWRD-IDSM-02701] IDS 消息分离数据格式

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02701 |
| **Type** | Valid |
| **Description** | 在以太网上，IDS 消息分离头是强制性的， 它用于明确地处理 IDS 消息， 除了通过以太网传输单个 IDS 消息外，还可以在单个以太网帧中收集和发送多个 IDS 消息；IDS消息分片头包含1个4字节消息ID字段（接收方唯一识别）和1个4字节消息长度字段（指定数据长度），二者都是大端字节序；IDS消息分片头ID是4字节，值是任意数，最好是0；IDS 消息分片头长度是通过添加 的IDS 消息长度和固定IDS 消息分片头长度（8 字节）来计算的，它以 4 个字节编码，可能的范围是： 消息长度byte[0..3]：16—2147549212 字节； |
| **Upstream ID** | PRS\_Ids\_00800 PRS\_Ids\_00803 PRS\_Ids\_00804 PRS\_Ids\_00805 |
| **Dependencies** | 无 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：接收数据功能完成  主要测试点：IDS 消息分离是否支持单个传输和多个消息发送；IDS消息分片头包识别是否正确；IDS 消息分片头长度解析是否正确；IDS消息分片头ID 4字节，是否初始化为0；  成功标准：   1. IDS 消息分离支持单个传输和多个消息发送； 2. IDS消息分片头包识别正确； 3. IDS 消息分片头长度解析正确； 4. IDS消息分片头ID 4字节，是否初始化为0； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-IDSM-02702] IDS 消息分离port信息

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02702 |
| **Type** | Valid |
| **Description** | 一个唯一的以太网port地址应该被IDS通信使用；some/ip和IDS消息不应该使用一个port，接收者无法区分 |
| **Upstream ID** | PRS\_Ids\_00801 PRS\_Ids\_00802 |
| **Dependencies** | 无 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：接收数据功能完成  主要测试点：IDS通信使用的port是否唯一；some/ip和IDS消息是否使用一个port；  成功标准：   1. IDS通信使用的port是唯一的； 2. some/ip和IDS消息不使用一个port； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## IDS 消息示例

### [SWRD-IDSM-02801] IDS 消息示例内容

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02801 |
| **Type** | Valid |
| **Description** | IDS消息最大长度，所有可选的都配置上，并且被配置为最大，那么加在一起就是2147549204字节长的IDS消息；IDS协议没有多余选项被配置，最小的只有事件帧，长度为8字节； |
| **Upstream ID** | PRS\_Ids\_00900 PRS\_Ids\_00901 |
| **Dependencies** | 无 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：接收数据功能完成  主要测试点：IDS消息最大长度是否超过2147549204；IDS协议最小帧长度是否为8字节；  成功标准：   1. IDS消息最大长度不超过2147549204； 2. IDS协议最小帧长度为8字节； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

## IDS 错误信息

### [SWRD-IDSM-02901] 错误信息

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02901 |
| **Type** | Valid |
| **Description** | 如果 IdsM 本身产生QSEv，则会将其发送到配置的接收器：  1.安全事件缓冲区溢出：没有更多的事件缓冲区可用处理安全事件；  2.上下文缓冲区溢出：没有更多的上下文缓冲区可用来存储上下文数据；  3.外发流量限制溢出：当前的流量超过了配置的限制； |
| **Upstream ID** | PRS\_Ids\_00720 |
| **Dependencies** | RS\_Ids\_00820 |
| **ASIL** | QM(C) |
| **Status** | Draft |
| **Priority** | H |
| **Verification Criteria** | 验证方法：ST  验证环境： NeuSAR-aCore运行环境  前提条件：idsm数据检测功能完成  主要测试点：是否上报安全事件缓冲区溢出错误；是否上报上下文缓冲区溢出错误；是否上报外发流量限制溢出错误；  成功标准：   1. 上报安全事件缓冲区溢出错误； 2. 上报上下文缓冲区溢出错误； 3. 上报外发流量限制溢出错误； |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

# 非功能需求(Non-Functional Requirements)

## 制约(Constraint)

*[*

1. *软件运行环境：考虑以下几个方面：*

*接口：与其他模块的接口；*

*环境：使用到其他模块数据类型，AutoSAR头文件的包含关系；*

1. *法律、法规和标准：如：必须按照ISO26262标准进行开发。]*

### [SWRD-ID]非功能需求1(Non-Function Requirement No.1)

|  |  |
| --- | --- |
| **SWRD-ID** |  |
| **Type** |  |
| **Description** |  |
| **Upstream ID** |  |
| **Dependencies** |  |
| **Verification method** |  |
| **Verification Criteria** |  |
| **ASIL** |  |
| **Status** |  |
| **Priority** |  |
| **CR** |  |
| **Risk** |  |
| **Change Type** |  |

### [SWRD-ID]非功能需求2(Non-Function Requirement No.2)

|  |  |
| --- | --- |
| **SWRD-ID** |  |
| **Type** |  |
| **Description** |  |
| **Upstream ID** |  |
| **Dependencies** |  |
| **Verification method** |  |
| **Verification Criteria** |  |
| **ASIL** |  |
| **Status** |  |
| **Priority** |  |
| **CR** |  |
| **Risk** |  |
| **Change Type** |  |

## 性能质量要求(Performance Quality Requirements)

*[从可用性，效率，可维护性，可移植性，可扩展性和性能等角度进行分析。*

1. *可用性：使用，操作相关需求*
2. *效率性：技术软件的反应速度和内存使用量，如：对Rom和Ram的使用量的约束、对内存大小、硬盘大小的约束，对CPU的约束等。*

*如：CPU符合率不满50%等，NVM相关使用参考“NVMList”*

1. *可维护性：变更解析相关、操作方式变化、运行环境的变化、接口变化、精度、时间性能等的需求发生变化时，该软件对这些变化的适应能力要求*
2. *可移植性：向其他制品的展开相关要求*
3. *可扩展性：派生开发要求*
4. *性能：软件相关的性能：如：数据精度要求，说明该软件的输入输出的的数据精度要求，可能包含传输过程中的精度要求；*

*时间性能要求，包括：响应时间、更新处理时间，数据转换和传送时间要求等]*

### [SWRD-ID]错误状态机制

|  |  |
| --- | --- |
| **SWRD-ID** |  |
| **Type** |  |
| **Description** | IDSM Stack API 应支持错误状态通知的有效机制;应提供有关检测到的错误状态的全面信息。 该信息应该足以识别错误条件并决定如何从错误状态中恢复并继续执行。 交付机制应方便应用程序的开发人员并满足 Autosar AP C++14 编码指南 |
| **Upstream ID** | RS\_IDSM\_02310 |
| **Dependencies** |  |
| **Verification method** | 评审 |
| **Verification Criteria** | 验证环境：无  前提条件：加密模块设计与实现完成；  主要测试点：错误状态返回通知机制是否合理；可否根据错误信息获取到错误点；编码是否满足要求；  成功标准：   1. 错误相关设计机制，可以能够满足需求； 2. 编码格式满足需求； |
| **ASIL** |  |
| **Status** | Draft |
| **Priority** | H |
| **CR** |  |
| **Risk** | 无 |
| **Change Type** | 新增 |

### [SWRD-ID]非功能需求4(Non-Function Requirement No.4)

|  |  |
| --- | --- |
| **SWRD-ID** |  |
| **Type** |  |
| **Description** |  |
| **Upstream ID** |  |
| **Dependencies** |  |
| **Verification method** |  |
| **Verification Criteria** |  |
| **ASIL** |  |
| **Status** |  |
| **Priority** |  |
| **CR** |  |
| **Risk** |  |
| **Change Type** |  |

# 接口说明(API)

*[记录AutoSar中接口相关信息，包括：API，服务接口，错误码等。该章节内容也可以引用“软件接口设计书”，在此处引用该文件即可。]*

## 接口头文件(API Header files)

## 接口共同数据类型(API Common Data Types)

附录A- 信息定义

|  |  |  |
| --- | --- | --- |
| 类别 | 结构 | 备注 |
| SWRD-ID | SWRD-{需求类型}-{功能简称}-流水号  功能简称：参见下面功能简称列表  需求类型：功能需求为空，非功能需求为NF,接口为API  流水号：从00001开始的5位自然数 | *例：*  *SWRD-Nvm-00001*  *SWRD-NF\_Nvm-00001*  *SWRD-API-Nvm-00001*  *SWRD-IDSM-00001* |

|  |  |
| --- | --- |
| 功能简称列表(aCore) | 说明 |
| DM\_DEM | Diagnostics management模块的诊断事件管理 |
| DM\_DCM | Diagnostics management模块的诊断通信管理 |
| DM\_DCM\_DOIP | Diagnostics management模块的DO/IP相关功能 |
| CoreTypes | 核心数据类型 |
| CM\_CommunicationAPI | Communication management模块的Communication API相关功能 |
| CM\_SOMEIP | Communication management模块的SOME/IP相关功能 |
| CM\_DDS | Communication management模块的DDS相关功能 |
| CM\_CommunicationGroup | Communication management模块的通信组相关功能 |
| CM\_SHM | Communication management模块的共享内存相关功能 |
| CM\_IPC | Communication management模块的IPC相关功能 |
| CM\_Raw | Communication management模块的raw data streaming相关功能 |
| CM\_TLS | Communication management模块的TLS相关功能 |
| CM\_S2S | Communication management模块的S2S相关功能 |
| CM\_E2E | Communication management模块的E2E相关功能 |
| UCM\_Master | Update and config management模块的主站相关功能 |
| UCM\_Server | Update and config management模块的从站相关功能 |
| LT | Log and trace模块相关功能 |
| PHM | Platform health management模块相关功能 |
| Per | Persistency模块相关功能 |
| SM | State management模块相关功能 |
| IDSM | IDSMgraphy模块相关功能 |
| EM | Execution mangement模块相关功能 |
| NM | Network management模块相关功能 |
| TS | Time synchronization模块相关功能 |

说明：根据项目情况可自己定义，增加功能简称

|  |  |  |
| --- | --- | --- |
| 安全等级(ASIL) | 解释说明 | 备注 |
| ASIL A | 根据S – Severity(严重度)  E – Exposure(暴露度) C – Controllability(可控性) 排定功能安全等级。详细理解可以参考26262标准文件。 | *如果有关于ASIL等级的特殊解释说明，请记录在此* |
| ASIL B |  |
| ASIL C |  |
| ASIL D |  |
| QM(A) | 从ASIL A到ASIL D 中分解出来，分解的标准，参考功能安全体系文件《功能安全需求分解指南\_FS.pdf》  其中:括号内的等级为原始等级。 |  |
| QM(B) |  |
| QM(C) |  |
| QM(D) |  |
| ASIL A(A) |  |
| ASIL A(B) |  |
| ASIL A(C) |  |
| ASIL A(D) |  |
| ASIL B(B) |  |
| ASIL B(C) |  |
| ASIL B(D) |  |
| ASIL C(C) |  |
| ASIL C(D) |  |
| ASIL D(D) |  |

|  |  |  |
| --- | --- | --- |
| 优先级(Priority) | 解释说明 | 备注 |
| H | 高优先级 | *例：被依赖的需求优先级设置为H级别* |
| M | 中优先级 | *例：* |
| L | 低优先级 | *例：其余功能均设置为L级别* |
| N/A | 不适用 |  |

|  |  |  |
| --- | --- | --- |
| 类型  (Type) | 状态说明 | 备注 |
| Valid | 有效 | *例：表示需要对应* |
| InValid | 不适用 | *例：表示不做对应* |
| TBD | 检讨中 | *例：表示正在检讨中* |

说明：根据项目情况可自己定义，但需要明确

|  |  |  |
| --- | --- | --- |
| 状态  (Status) | 状态说明 | 备注 |
| Draft | 草稿 | *例：表示新建* |
| In Review | 评审中 | *例：表示处于评审中* |
| Approved | 批准 | *例：表示通过评审* |
| Released | 发布 | *例：表示通过客户确认* |
| Modified | 修改 | *例：表示正在检讨修改中* |

|  |  |  |
| --- | --- | --- |
| 变更类型  (Change Type) | 解释说明 | 备注 |
| 新增 | 与AutoSAR标准*XXX*相比，新增的需求。 | 如果有关于每个变更类型的特殊解释说明，请记录在此 |
| 修改 | 与AutoSAR标准*XXX*相比，发生了修改的需求 |  |
| 不变 | 与AutoSAR标准*XXX*相比，没有变更的需求。 |  |
| 删除 | 与AutoSAR标准*XXX*相比，没有变更的需求。 |  |

说明：根据项目情况可自己定义，但需要明确

附录B- 配置信息

|  |  |  |  |
| --- | --- | --- | --- |
| 配置信息 | 说明 | 范围 | 备注 |
| *API configuration class* |  | *1、2、3* |  |
|  |  |  |  |
|  |  |  |  |