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)：0.1

日期(Date)：2022-06-14

|  |  |  |
| --- | --- | --- |
| 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 | 0.1 | 初稿 | Draft | 黄海军、秦天宇/2022/6/14 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Contents**

[1 引言(Introduction) 1](#_Toc106114214)

[1.1 目的(Goal) 1](#_Toc106114215)

[1.2 范围(Scope) 1](#_Toc106114216)

[1.3 参考文档(Reference) 1](#_Toc106114217)

[1.4 术语和缩略语(Terms And Abbreviations) 1](#_Toc106114218)

[2 软件系统概述(Software System Overview) 2](#_Toc106114219)

[2.1 软件系统背景(Software System Background) 2](#_Toc106114220)

[2.2 软件系统目标(Software System Goal) 2](#_Toc106114221)

[2.2.1 安全传感器和安全事件 2](#_Toc106114222)

[2.2.2 ⼊侵检测系统管理器 2](#_Toc106114223)

[2.2.3 ⼊侵检测系统报告器 2](#_Toc106114224)

[2.3 外部关联 (External Association) 3](#_Toc106114225)

[3 功能需求(Functional Requirement) 3](#_Toc106114226)

[3.1 事件生成 3](#_Toc106114227)

[3.1.1 [SWRD-IDSM-00100]安全事件标识 3](#_Toc106114228)

[3.2 报告模式 3](#_Toc106114229)

[3.3.1 [SWRD-IDSM-00201] 设置报告模式 3](#_Toc106114230)

[3.3.2 [SWRD-IDSM-00202] 根据报告模式处理 4](#_Toc106114231)

[3.3 过滤链 4](#_Toc106114232)

[3.3.1 [SWRD-IDSM-00301] 安全事件和过滤链关联 4](#_Toc106114233)

[3.3.2 [SWRD-IDSM-00302] 过滤链在报告模式之后应用 5](#_Toc106114234)

[3.3.3 [SWRD-IDSM-00303] 过滤链组成 5](#_Toc106114235)

[3.3.4 [SWRD-IDSM-00304] 聚合过滤链的过滤器 6](#_Toc106114236)

[3.3.5 [SWRD-IDSM-00305] 过滤链中过滤器顺序 6](#_Toc106114237)

[3.4 机器状态过滤器 7](#_Toc106114238)

[3.4.1 [SWRD-IDSM-00401] 机器状态过滤规则 7](#_Toc106114239)

[3.5 机器状态过滤器 7](#_Toc106114240)

[3.5.1 [SWRD-IDSM-00501] 采样过滤器 7](#_Toc106114241)

[3.6 聚合过滤器 8](#_Toc106114242)

[3.6.1 [SWRD-IDSM-00601] 聚合Sev的周期处理事件 8](#_Toc106114243)

[3.7 阈值过滤器 9](#_Toc106114244)

[3.7.1 [SWRD-IDSM-00701] 阈值N及应用规则 9](#_Toc106114245)

[3.8 外发 QSEvs 9](#_Toc106114246)

[3.8.1 [SWRD-IDSM-00901] 配置IDSR 9](#_Toc106114247)

[3.8.2 [SWRD-IDSM-00902] IDS 消息分片 10](#_Toc106114248)

[3.9 速率和流量限制 10](#_Toc106114249)

[3.9.1 [SWRD-IDSM-001103] 速率限制 10](#_Toc106114250)

[3.9.2 [SWRD-IDSM-001104] 流量限制 11](#_Toc106114251)

[3.10 IdsM报告Sevs 11](#_Toc106114252)

[3.10.1 [SWRD-IDSM-01401] IdsM自身报告安全事件内容 11](#_Toc106114253)

[3.10.2 [SWRD-IDSM-01402] 自身安全事件优先级 12](#_Toc106114254)

[3.11 IDS协议通用要求 12](#_Toc106114255)

[3.11.1 [SWRD-IDSM-02201] 通用要求 12](#_Toc106114256)

[3.12 IDS 协议之基本事件帧 13](#_Toc106114257)

[3.12.1 [SWRD-IDSM-02301] 协议版本和标头 13](#_Toc106114258)

[3.12.2 [SWRD-IDSM-02302] IdsM 实例 ID 和传感器实例 ID 14](#_Toc106114259)

[3.12.3 [SWRD-IDSM-02303] 事件定义 ID 15](#_Toc106114260)

[3.12.4 [SWRD-IDSM-02304] 调用IdsM API的次数 15](#_Toc106114261)

[3.12.5 [SWRD-IDSM-02305] 保留项 16](#_Toc106114262)

[3.13 IDS 消息分离 16](#_Toc106114263)

[3.13.1 [SWRD-IDSM-02701] IDS 消息分离数据格式 16](#_Toc106114264)

[3.14 IDS 消息示例 17](#_Toc106114265)

[3.14.1 [SWRD-IDSM-02801] IDS 消息示例内容 17](#_Toc106114266)

[3.15 IDS 错误信息 17](#_Toc106114267)

[3.15.1 [SWRD-IDSM-02901] 错误信息 17](#_Toc106114268)

[4 非功能需求(Non-Functional Requirements) 18](#_Toc106114269)

[4.1 制约(Constraint) 18](#_Toc106114270)

[4.1.1 [SWRD-ID]非功能需求1(Non-Function Requirement No.1) 18](#_Toc106114271)

[4.1.2 [SWRD-ID]非功能需求2(Non-Function Requirement No.2) 19](#_Toc106114272)

[4.2 性能质量要求(Performance Quality Requirements) 19](#_Toc106114273)

[4.2.1 [SWRD-ID]错误状态机制 19](#_Toc106114274)

[4.2.2 [SWRD-ID]非功能需求4(Non-Function Requirement No.4) 20](#_Toc106114275)

[5 接口说明(API) 20](#_Toc106114276)

[5.1 接口头文件(API Header files) 20](#_Toc106114277)

[5.2 接口共同数据类型(API Common Data Types) 20](#_Toc106114278)

[附录A- 信息定义 20](#_Toc106114279)

[附录B- 配置信息 22](#_Toc106114280)

# 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

安全传感器是可以产生预定义事件的进程，AUTOSAR BSW (CP)、CDD(CP) 、FC(AP)和 SWC（AP/CP） 都可以充当安全传感器， 安全传感器根据需要可以产生安全事件（SEv）并向 IdsM 报告。安全事件是与信息安全相关的一些异常行为，可供云端SOC等进行运营分析的数据，具体的安全事件可由客户自定义。

### 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。

## 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] 采样过滤器

|  |  |
| --- | --- |
| **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 |

## 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 |

## 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 |

## 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) |

## 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 |

## IDS协议通用要求

### [SWRD-IDSM-02201] 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 |

## IDS 协议之基本事件帧

### [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 消息分离

### [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 |

## IDS 消息示例

### [SWRD-IDSM-02801] IDS 消息示例内容

|  |  |
| --- | --- |
| **SWRD\_ID** | SWRD-IDSM-02801 |
| **Type** | Valid |
| **Description** | 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\_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协议最小帧长度是否为8字节；  成功标准：   1. 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** |  |
| **Upstream ID** |  |
| **Dependencies** |  |
| **Verification method** |  |
| **Verification Criteria** |  |
| **ASIL** |  |
| **Status** |  |
| **Priority** |  |
| **CR** |  |
| **Risk** |  |
| **Change Type** |  |

### [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* |  |
|  |  |  |  |
|  |  |  |  |