文件名	安全要求 提取模板
文档所有者	AUTOSAR
文件责任	AUTOSAR
证件编号979	

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

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

免责声明

目录

参考

[1] 标准化模板
AUTOSAR_TPS_标准化模板

[2] 主要要求
AUTOSAR_RS_Main

1 简介

1.1 本文件的范围

本文档收集了安全提取模板的要求。

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

Extract 可以作为交换文件来收集安全事件及其属性
在开发过程中以及在维护期间从多个来源获取
当车辆已经在现场时进行处理。

安全提取文件用于配置入侵检测的安全事件
车辆的 ECU 或机器中的系统管理器 (IdsM) 实例。

例如,它还可以用作“安全事件和事件管理”(SIEM) 系统的输入,作为“安全运营中心”(SOC) 的一部分,从而能够解释从车辆的 IdsM 实例接收到的二进制数据.

简而言之,使用安全提取的关键方面是:

- 在开发过程中从多个来源收集安全事件定义
  过程
- 为车辆的 ECU 和机器的 IdsM 实例的安全事件配置输入
- SIEM 系统的输入,能够解释与安全相关的二进制数据
  活动

1.2 文档约定

AUTOSAR 文档中的需求表示遵循 [TPS_STDT_00078] 中指定的表格,请参阅标准化模板,支持可追溯性([1]) 一章。

[TPS_STDT_00053] 中规定的义务表达的口头形式应用于指示要求,请参见标准化模板,支持可追溯性([1]) 一章。

1.3 指导方针

应参考现有规范（以单一要求的形式）。与这些规范的差异被指定为附加要求。

所有要求应具有以下属性：

- 冗余要求不得在
  一项要求或其他要求中重复。

- 清晰度
  所有要求应仅允许一种解释的可能性。必须定义词汇表中未使用的技术术语。

- 原子性
  每个需求应仅包含一个需求。如果一个需求不能被分解成更多的需求，那么它就是原子的。

- 可测试性
  需求应可通过分析、审查或测试进行测试。

- 可追溯性 需求
  的来源和状态应始终可见。

1.4 需求追踪

下表引用了[2]中指定的要求和实现这些要求的链接。

要求	描述	满意
[RS_Main_00514]	AUTOSAR 应支持安全系统的开发	[RS_SECXT_00001] [RS_SECXT_00002] [RS_SECXT_00003] [RS_SECXT_00004] [RS_SECXT_00005] [RS_SECXT_00006] [RS_SECXT_00007] [RS_SECXT_00008] [RS_SECXT_00009] [RS_SECXT_00010] [RS_SECXT_00011] [RS_SECXT_00012] [RS_SECXT_00013] [RS_SECXT_00014] [RS_SECXT_00015] [RS_SECXT_00016] [RS_SECXT_00017] [RS_SECXT_00018] [RS_SECXT_00019] [RS_SECXT_00020] [RS_SECXT_00021] [RS_SECXT_00023]

表 1.1:需求跟踪

2 要求

2.1 与安全事件相关的要求

[RS_SECXT_00001]{DRAFT}安全事件定义d

描述：	安全提取应支持安全事件的定义和配置。
理由：	应该可以将与安全相关的事件和相关信息从传感器（实现为硬件或软件)传送到处理这些事件和相关信息的软件模块。
用例：	报告安全事件
依赖关系： -	
配套材料：	

c(RS_Main_00514)

[RS_SECXT_00023]{DRAFT}安全传感器 ID 的定义事件d

描述：	安全提取应支持安全事件的安全传感器 ID 的定义。
理由：	应该可以将安全事件与安全传感器的数字标识符相关联。
用例：	识别安全事件的来源
依赖关系： -	
配套材料：	

c(RS_Main_00514)

[RS_SECXT_00009]{DRAFT}支持安全事件的可选上下文数据d

描述：	安全提取应支持特定于安全事件的可选上下文数据的定义。
理由：	应该可以配置使用附加上下文数据报告给定的安全事件。
用例：	使用其他上下文数据报告安全事件
依赖关系： -	
配套材料：	

c(RS_Main_00514)

[RS_SECXT_00002]{DRAFT}安全事件的过滤链d

描述：	安全提取应支持安全过滤器链的定义 事件。
理由：	应该可以为安全事件链接过滤器，以便多阶段 可以实现由几种算法组成的过滤。
用例：	过滤安全事件
依赖关系： -	
配套 材料：	

c(RS_Main_00514)

[RS_SECXT_00003]{DRAFT}安全事件的限制过滤d

描述：	安全提取应支持安全限制过滤器的定义 事件。
理由：	应该可以限制对安全事件的进一步处理，以便 防止超出后续处理阶段的能力。
用例：	限制由安全事件引起的处理负载
依赖关系： -	
配套 材料：	

c(RS_Main_00514)

[RS_SECXT_00012]{DRAFT}安全事件资格预审规定d

描述：	安全摘录应支持资格预审是否是 是否为特定的安全事件提供。
理由：	除了通过过滤进行鉴定之外，(智能)传感器应能够报告 应直接作为合格处理的预限定安全事件 IdsM 的安全事件。
用例：	报告通过资格预审的安全事件
依赖关系： -	
配套 材料：	

c(RS_Main_00514)

[RS_SECXT_00004]{DRAFT}安全事件与 ECU/机器的关联

d

描述：	安全摘录应支持安全之间关系的定义 事件以及检测和报告事件的 ECU。

理由：	应该可以配置给定的 ECU 报告给定的安全事件
用例：	报告给定 ECU 上的安全事件
依赖关系： -	
配套 材料：	

c(RS_Main_00514)

[RS_SECXT_00008]{DRAFT}安全事件与平台模块的关联

描述：	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）
理由：	应该可以配置为给定平台模块报告给定安全事件。
用例：	报告给定平台模块的安全事件
依赖关系： -	
配套 材料：	

c(RS_Main_00514)

[RS_SECXT_00005]{DRAFT}安全事件与通信总线的关联d

描述：	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。
理由：	应该可以配置为给定的通信总线报告给定的安全事件。
用例：	报告给定通信总线的安全事件相关性： –支持材料：

c(RS_Main_00514)

[RS_SECXT_00021]{DRAFT}安全事件与应用程序d的关联

描述：	安全摘录应支持安全事件与作为安全问题主题的应用程序（经典平台或自适应应用程序的软件组件）之间关系的定义。
理由：	应该可以配置给定的应用程序报告给定的安全事件。
用例：	报告给定应用程序的安全事件
依赖关系： -	
配套材料：	

c(RS_Main_00514)

[RS_SECXT_00006]{DRAFT}支持安全事件的持久存储

描述：	安全提取应支持给定安全事件的持久性配置。
理由：	应该可以配置一组给定的安全事件永久存储在已检测到的 ECU 上。
用例：	将安全事件存储在已检测到的 ECU 上
依赖关系： -	
配套材料：	

c(RS_Main_00514)

[RS_SECXT_00007]{DRAFT}安全默认报告模式的定义
活动d

描述：	安全提取应支持为安全事件配置具有不同详细级别的默认报告模式。
用例：	报告具有不同详细级别的安全事件
依赖关系： -	
配套材料：	

c(RS_Main_00514)

[RS_SECXT_00018]{DRAFT}支持在映射时定义严重性级别
安全事件d

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

理由：	应该可以根据安全事件到 IdsM 实例的映射来配置安全事件的严重性级别。
用例：	报告带有其他严重性级别信息的安全事件
依赖关系： -	
配套 材料：	

c(RS_Main_00514)

2.2 与 IdsM 实例相关的要求

[RS_SECXT_00013]{DRAFT} IdsM 实例的可选配置d

描述：	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。
理由：	除了安全事件之外,安全提取还应部分有助于 IdsM 实例的配置 可选地定义和部分配置 IdsM 实 例依赖关系： –支持材料：
用例：	

c(RS_Main_00514)

[RS_SECXT_00014]{DRAFT}时间戳配置的可选配置d

描述：	安全提取应支持配置 IdsM 实例是否为报告的安全事件提供时间戳信息,如果提供,该时间戳信息是否 为 AUTOSAR 标准化格式。
理由：	IdsM 实例是否将时间戳信息添加到其报告的安全事件中应该是可配置的。
用例：	可选择报告安全事件的时间戳信息
依赖关系： -	
配套 材料：	

c(RS_Main_00514)

[RS_SECXT_00015]{DRAFT}时间戳格式的配置d

描述：	当向报告的安全事件添加时间戳信息时，安全提取应支持 IdsM 使用的配置格式。时间戳格式可能是 AUTOSAR 标准化的、由其他机构标准化的、公司标准化的或任意定义的。
理由：	不同的公司和项目预计对报告的安全事件使用不同的时间戳格式 具有可配置格式的报告时间戳信息
用例：	
依赖关系： -	
配套材料：	

c(RS_Main_00514)

[RS_SECXT_00016]{DRAFT}为安全事件消息提供身份验证的可选配置d

描述：	对于 AUTOSAR 经典平台和自适应平台，安全提取应支持可选配置，即要求 IdsM 实例将身份验证信息（即签名）添加到它发送到网络上的所有安全事件消息中。
理由：	安全提取应在网络配置方面支持 IdsM 实例配置。
用例：	可选择在 Adaptive Platform 上定义和部分配置 IdsM 实例
依赖关系： -	
配套材料：	

c(RS_Main_00514)

[RS_SECXT_00017]{DRAFT}网络配置与 IdsM 的关联实例d

描述：	对于 AUTOSAR 经典平台和自适应平台，安全提取模板应描述如何定义 IdsM 实例与其网络配置的关联。
理由：	安全提取应在网络配置方面支持 IdsM 实例配置。
用例：	可选择定义和部分配置 IdsM 实例
依赖关系： -	
配套材料：	

c(RS_Main_00514)

2.3 与 AUTOSAR 方法相关的要求

[RS_SECXT_00019]{DRAFT}支持定义 IDS 范围和系统边界d

描述：	安全摘录应支持设计和实施的 IDS 范围（即系统边界)的定义。
理由：	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。
用例：	IDS 的系统级描述
依赖关系： -	
配套材料：	

c(RS_Main_00514)

[RS_SECXT_00020]{DRAFT}支持部分和完整的安全交换提取定义d

描述：	安全摘录应支持开发合作伙伴之间对其定义的部分和完整交换。
理由：	为了实现 IDS 的分布式开发,多个开发合作伙伴贡献了一个描述整个 IDS 设计的安全提取文件。这些贡献者需要能够在 IDS 设计允许的情况下独立于其他人指定他们的安全提取部分。
用例：	IDS的分布式开发
依赖关系： -	
配套材料：	

c(RS_Main_00514)

[RS_SECXT_00010]{DRAFT}推导相关ECU-C参数d

描述：	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。
理由：	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。
用例：	为 IdsM 导出 ECU-C 配置参数
依赖关系： -	

配套 材料：	

c(RS_Main_00514)

[RS_SECXT_00011]{DRAFT} AUTOSAR 标准化安全规范
活动d

描述：	安全提取应支持 AUTOSAR 标准化安全事件的规范。
理由：	随着入侵检测系统管理器的引入，AUTOSAR 还将为现有的 BSW 模块（经典平台）或功能集群（自适应平台）提供标准化的安全事件。这些标准化的安全事件应使用安全提取模板指定，以启用文档生成的自动处理（单一来源原则）。
用例：	指定 AUTOSAR 标准化安全事件依赖项： –支持材料：

c(RS_Main_00514)

约束和规范项的历史

A.1 根据 AUTOSAR,本文档的约束历史 R20-11

A.1.1 在 R20-11 中添加了 Traceables

数字	标题
[RS_SECXT_00001]安全事件	
[RS_SECXT_00002]安全事件过滤	
[RS_SECXT_00003]安全事件与 Ecu 的关联	
[RS_SECXT_00004]安全事件与通信总线的关联	
[RS_SECXT_00005]支持安全事件的持久化存储	
[RS_SECXT_00006]支持不同的安全事件上报模式	
[RS_SECXT_00007]安全事件与基本软件模块的关联	

表 A.1:在 R20-11 中添加的 Traceables

A.1.2 R20-11 中更改的可追溯性

没有任何

A.1.3 R20-11 中删除的 Traceables

没有任何