文件名	入侵规范 检测系统协议
文档所有者	AUTOSAR
文件责任	AUTOSAR
证件编号981	

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	· 改进的协议解释 字段 · 提高了之间的一致性 概览和详细表格 · 帧尺寸计算的更正
2020-11-30 R20-11		AUTOSAR 释放 管理	· 初始发行

免责声明

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

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

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

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

AUTOSAR 一词和 AUTOSAR 标志是注册商标。

目录

1 简介和概述

本协议要求规范定义了 AUTOSAR 协议入侵检测系统(IDS) 的格式、消息序列和语义。

文档 RS IntrusionDetectionSystem [1]描述了分布式入侵检测系统(IDS) 的元素。有关IDS元素的概述,请参阅[1] 。

PRS IDS通过提供将合格的安全事件(QSEv)从入侵检测系统管理器(IdsM)实例传输到入侵检测系统报告器 (IdsR) 实例的协议来为 IDS做出贡献。

1.1 协议目的和目标

如[1]中所述， QSEv可以本地保存在安全事件被限定的ECU上。或者,可以将QSEv发送到IdsR。 IDS 协议涵盖了从IdsM实例向IdsR实例发送QSEv 。

1.2 协议的适用性

IDS 协议支持QSEv的推送接口。 IdsM实例推送相应配置到 IdsR 的QSEv 。此协议未涵盖拉取接口。它可以通过将 QSEv 本地存储在适当的组件中,然后通过常规诊断接口访问本地存储的QSEv来实现。

1.2.1 约束和假设

使用IDS 协议没有特定的假设和限制。它被设计为适用于所有总线系统。软件堆栈必须能够发送和接收I-PDU。IdsM 不支持接收 QSEv。

1.2.2 限制

没有为上下文数据大小定义限制。建议将完整的单个QSEv的限制设置为 16 kByte。

1.3 依赖

1.3.1 对其他协议层的依赖

经典平台上的IdsM实例使用PDU 路由器通过IDS 协议传输QSEv 。

1.3.2 对其他标准和规范的依赖

如果SOC需要， IDS 协议的元素可以通过IdsR映射到 syslog 格式。

1.3.3 对应用层的依赖

IDS 协议不依赖于应用层。应用层组件可以使用IdsM的API来发布安全事件。

2 用例

AUTOSAR IDS 架构和功能在[1] 中进行了描述。因此，本章是该协议用例的简要总结。

ID	姓名	描述
0001	QSEv的传输	将合格的安全事件从 IdsM 实例传输到 IdsR 实例

表 2.1：IDS 协议的用例

2.1 UC_0001“将合格的安全事件传播给 IdsR

IDS 协议的主要用例是将合格的安全事件QSEv以独立于ECU类型或使用的通信机制的方式传播到IdsR 。 IdsM实例可以分配给与安全相关的车辆架构的所有节点。该决定通常基于对车辆 E/E 架构的安全分析。因此， IdsM实例可以通过许多不同的总线系统间接连接到IdsR ，如图 2.1 所示。

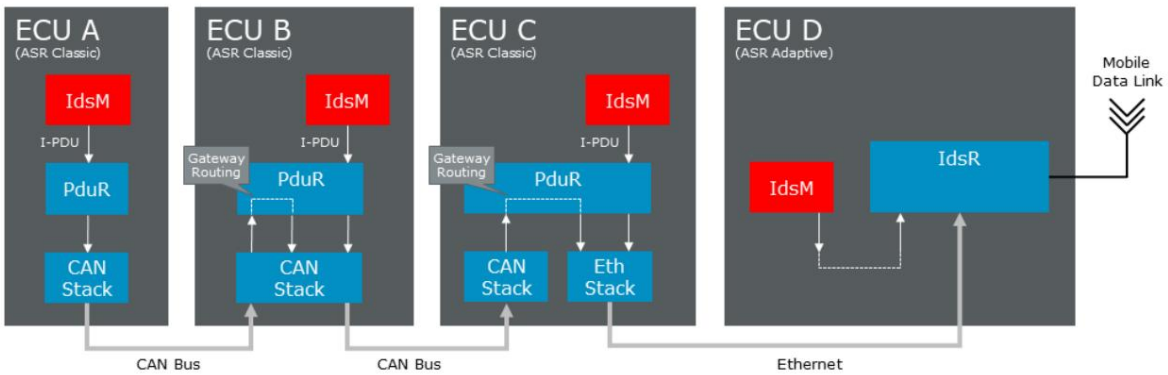


图 2.1：IDS 协议用例

3 协议要求

3.1 需求追溯

下表引用了 IDS 要求规范[1]中指定的要求,并链接到这些要求的实现。

要求	描述	满意
[RS_Ids_00502]	事件时间戳	[PRS_Ids_00400] [PRS_Ids_00401]
[RS_Ids_00503]	时间戳源	[PRS_Ids_00404]
[RS_Ids_00505]	QSEv 的真实性	[PRS_Ids_00600] [PRS_Ids_00601]
[RS_Ids_00510]	IdsM 应允许传输 QSEv 到 IdsR	[PRS_Ids_00001]
[RS_Ids_00820]	IdsM 安全事件	[PRS_Ids_00720]

4 术语和缩写词的定义

4.1 首字母缩略词

首字母缩略词	描述：
自适应平台	AUTOSAR 自适应平台
BSW	标准化的 AUTOSAR 软件模块,提供电子控制单元通常需要的基本功能。
具有灵活数据速率的控制器局域网/控制器局域网	一种汽车网络通信协议。
上下文数据	SEv的相关信息。它是提供了一个可选数据 更广泛地了解安全事件（例如,损坏的 数据）。上下文数据的内容和编码是外部的 由传感器定义,IdsM 模块未知。
经典平台	AUTOSAR 经典平台
上下文数据缓冲区	可变大小的缓冲区以适应上下文数据的需要 SEvs。
电子控制单元	提供电子功能的电子控制单元 汽车的系统,例如制动系统或车窗升降器。
事件缓冲区	用于临时存储报告的 SEv 的缓冲区。
事件框架	IDS协议主框架,包含基本信息 像安全事件 ID。
过滤链	一组应用于安全事件的连续过滤器。 输出是合格的安全事件。
弹性射线	一种汽车网络通信协议。
通用 I-Pdu	通用交互层协议数据单元。
入侵侦测系统	入侵检测系统是一种安全控制,可检测 并处理安全事件。
入侵检测系统协议	IDS 协议指定了被使用的消息格式 身份识别系统。
入侵侦测系统 信息	IdsM 使用 IDS 协议发送的消息。
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。
I-PDU 多路复用器	一个 AUTOSAR 基本软件模块,它指定了将多个 Pdus 与一个协议控制信息进行复用的协议。
林	本地互连网络:用于连接传感器和执行器的串行通信总线。
协议数据单元路由器	负责消息路由的 AUTOSAR 组件 独立于底层通信网络。
协议要求规范入侵检测系统	描述所有元素的规范文档 IDS 协议。
合格的安全事件 (QSEv) 通过过滤链的安全事件被视为	合格的安全事件并发送到配置的接收器。
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	板载安全事件由 BSW、CDD、SWC 或 IdsM 的其他软件组件或应用程序。

首字母缩略词	描述：
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	BSW、CDD、SWC 或其他软件组件或应用程序 向 IdsM 报告安全事件。
安全事件和事件 管理	收集、关联和分析事件中的安全性以检测威胁的技术概念。
传感器	报告身份，通知 IdsM 模块有关 SEv 的信息。它 可以是 BSW 模块、专有 CDD 或 SWC 应用程序。
安全运营中心	安全运营中心是IDS的后端 可以处理和分析数据。
插座适配器	Socket Adapter 是 AUTOSAR 的一个基础软件模块，它 在基于 Pdu 的服务通信之间创建接口 基于级别和套接字的 TCP/IP

表 4.1：首字母缩略词

4.2 缩写

缩写	描述：
美联社	AUTOSAR 自适应平台
API	应用程序接口
BSW	基础软件
能够	控制器局域网
CAN FD	具有灵活数据速率的控制器局域网
客户尽职调查	复杂设备驱动程序
CP	AUTOSAR 经典平台
电子控制单元	电子控制单元
ID	标识符
身份识别系统	入侵侦测系统
I-PDU	交互层协议数据单元
身份证件	入侵检测系统管理器
IdsR	入侵检测系统报告器
林	本地互连网络
小姐	毫秒
N-PDU	网络层协议数据单元
OEM	原始设备制造商
PDU	协议数据单元路由器
PRS 身份证	协议需求规范入侵检测系统
QSEv	合格的安全事件
SecXT	安全提取
SEv	安全事件
扫描电镜	安全事件记忆
SIEM	安全事件和事件管理
一些/IP	IP上可扩展的面向服务的中间件
SOC	安全运营中心
SWC	软件组件

表 4.2：缩写

5 协议规范

[PRS_Ids_00001] d IDS 协议的主要目的是将合格的安全事件(QSEv)从入侵检测系统管理器(IdsM)实例传输到入侵检测系统报告器(IdsR)实例。c(RS_Ids_00510)

5.1 IDS消息格式

IDS 协议如图 5.1 所示。

图 5.1:包含签名的 IDS 消息

[PRS_Ids_00002] dIDS协议由标准事件框架和最多三个可选字段组成。它提供了几个选项来仅发送合格安全事件QSEv的最少数据或使用更多详细信息扩展此数据。

除了带有时间戳或上下文数据的扩展外,还可以选择通过向每个QSEv 添加签名来保护数据传输。下面的列表显示了配置示例并解释了选项。 C ()

所有选项都可以相互独立地配置或关闭,因此所有选项的子集或组合都是可能的。

1. [PRS_Ids_00003] dStandard Qualified Security Event QSEv ,无需进一步数据.c()
2. [PRS_Ids_00400] dQualified Security Event QSEv with Timestamp: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。
   该选项必须通过协议头中的相应配置位设置。c (RS_Ids_00502) (参考5.1.5 Timestamp)
3. [PRS_Ids_00500] dQualified Security Event QSEv with Context Data:上下文数据包括仅转发到接收器的传感器特定信息。 IdsM不了解这些数据的内容或结构。

   该选项必须通过协议header.c()中相应的配置位来设置（参考5.1.6 Context Data）
4. [PRS_Ids_00600] dQualified Security Event QSEv with Signature:如果需要更安全的安全事件通信,则可以将签名添加到每个QSEv。

   该选项必须通过协议头中的相应配置位来设置。c（RS_Ids_00505） （参考5.1.8签名）

5.1.1 IDS 协议概述

在图 5.2中,您可以找到IDS 协议的所有元素的概述。

字段名长度		数据说明
协议 版本	4位	IdsM 协议的版本
协议 标题	4位	IdsM 协议头信息: 位 [0]:0 - 不包括上下文数据,1 - 包括上下文数据 Bit[1]:0 - 不包括时间戳,1 - 包括时间戳 位 [2]:0 - 不包括签名,1 - 包括签名 位[3]:保留
身份证件 实例 ID	10位	发送 IdsMinstance 的唯一标识符 0-1023
模块 实例 ID	6位	标识符在模块的多个实例之间有所不同
事件 ID	16 位	安全事件的唯一标识符: AUTOSAR 内部 ID 范围:0…0x7FFF 客户特定 ID 的范围:0x8000…0xFFFF
数数	16 位	处理后导致当前事件的 IdsM 调用数 配置的过滤器,例如EventAggregation
预订	8位	留作将来使用
时间戳8 字节		检测到事件时的时间戳/Tickstamp:(可选) Byte[0] Bit[7]=0:AUTOSAR 标准,Byte[0] Bit[6]:保留 Byte[0] Bit[7]=1:OEM 特定/自定义时间戳 以毫秒为单位的分辨率。可能不是每个事件类型都需要。 如果未设置,则字段由 IdsR 填充。如果不是真实时间,IdsR 可能会 重新计算时间并插入新值
上下文数据 长度	1 或 4 字节	上下文数据的长度信息。仅在存在上下文数据时可用。 (选项) 第一个字节上下文数据的最高有效位表示如果 上下文数据长度以 7 位或 31 位编码: Context Data Byte[0] Bit[7]=0:长度编码为 7 位 - 字节[0] 位[0..6] - 有效值:1..127 字节 Context Data Byte[0] Bit[7]=1:长度编码为 31 位 - Byte[0] Bit[0..6], Byte[1..3] Bit[0..7] - 有效值:1..(2^31) - 1 Bytes 1…(2^31)-1
上下文数据1…(2^31) -1字节		传感器附加的二进制 blob:(可选)
签名 长度	2 字节	签名的长度信息。仅在签名存在时可用。 (选修的) 签名字节[0..1]:签名长度 1..65535 字节
签名	1..65535 字节	安全事件认证签名:(可选) 签名计算与 Eventframe + 可选时间戳 + 可选上下文数据 签名字节[2..n]:签名数据 - 可通过 MetaModel 配置

图 5.2:入侵检测系统协议概述

5.1.2 字节序 字节顺序

[PRS_Ids_00004] dIDS协议使用大字节序作为字节顺序,也称为
作为摩托罗拉格式。这等于网络字节顺序,例如由以太网使用。
在本节的表格和说明中,字节数以相同的方式增加
字节在IDS消息中传输,从 0 开始。

第一个字节是最高有效字节 (MSB),通常是字节 0
最后一个字节是最低有效字节（LSB）。
位数减少,字节的最高有效位 (msb) 为位 7
和最低有效位 (lsb) 0.c()

5.1.3 通讯接口的独立性

[PRS_Ids_00005] dIDS协议独立于使用的硬件和
底层通信接口（例如 CAN、以太网、FlexRay）。它经过优化
以适应标准 CAN 总线通信,所需信息最少
安全事件。以太网通信也适用。c()

5.1.4 IDS 事件框架

图 5.3显示了IDS协议的Event Frame 。

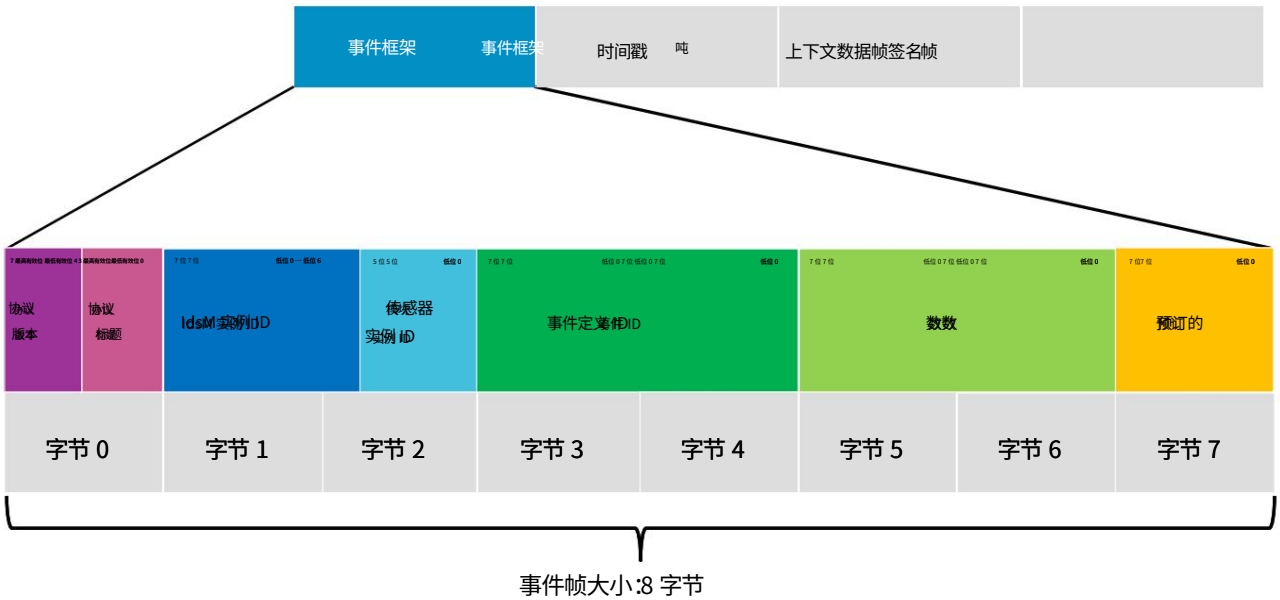


图 5.3:IDS 事件框架

[PRS_Ids_00006] dIDS事件帧由 8 个字节组成,如上所述。c()

5.1.4.1 协议版本和头

字节 0							
位 7	位 6	位 5	位 4	位 3	位 2	位 1	位 0
协议版本				协议头			
				预订的	西格纳真的	时间戳	语境数据

表 5.1:协议版本和标头的布局

5.1.4.1.1 协议版本

[PRS_Ids_00008] dIDS协议的版本信息：

- 位[7..4]:0-15

计算公式：

协议版本 = (BYTE0 & 0xF0) >> 4

本 IDS 协议规范使用的版本号应为 1.c()

5.1.4.1.2 协议头

[PRS_Ids_00009] dIDS 协议头信息,包括配置位
打开或关闭特定功能：

- 位[0]:包含上下文数据

  0:不包括上下文数据

  1:包含上下文数据

- Bit[1]:包含时间戳

  0:不包括时间戳

  1:包括时间戳

- 位[2]:包括签名

  0:不包括签名

  1:包括签名

- 位[3]:保留

计算公式：

ProtocolHeader = (BYTE0 & 0x0F)c()

注意：
[PRS_Ids_00010] d仅当时间戳、上下文数据或签名可用时，相应的协议头位设置为 1。

永远不会使用 Length=0.c() 传输上下文数据或签名

[PRS_Ids_00011] dReserved Bits 应预设为值 0。在接收器端应忽略这些位。c()

5.1.4.2 IdsM Instance ID 和 Sensor Instance ID

[PRS_Ids_00012] dTable 5.2显示了组合元素 IdsM 和传感器实例 ID.c()

字节 1								字节 2							
位 7	位 6	位 5	位 4	位 3	位 2	位 1	位 0	位 7	位 6	位 5	位 4	位 3	位 2	位 1	位 0
IDS 实例 ID								传感器实例 ID							

表 5.2：IdsM 实例 ID、传感器实例 ID

5.1.4.2.1 IdsM 实例 ID

[PRS_Ids_00013] d发送安全事件的IdsM实例的唯一标识符。

IdsM 实例 ID 范围：0-1023。
通常一个 ECU 中有一个IdsM实例。对于带有经典和自适应组件的复杂ECU ，例如多控制器或多分区设备，可能存在多个IdsM。经典平台中的一个IdsM和自适应平台中的一个IdsM 。在这样的星座中，两个IdsM都必须配置不同的 IDS Instance ID。

计算公式： IdsM Instance ID
(10 Bits) = ((BYTE2 & 0xC0) >> 6) |((BYTE1 << 2))c()

5.1.4.2.2 传感器实例 ID

[PRS_Ids_00014] dIdentifier 用于区分同种传感器模块的多个实例。

传感器实例 ID 范围：0-63 例如，一个ECU
中的多个 CanDrv可以发出“相同”的安全事件。为了区分这些，使用了传感器实例 ID。

如果配置中只有一个传感器实例，则传感器实例 ID 的值默认设置为 0。

笔记：

Sensor Instance ID 应在相应的基本软件模块的配置中设置。

计算公式：
传感器实例 ID（6 位）= (BYTE2 & 0x3F)c()

5.1.4.3 事件定义ID

事件定义 ID 如表 5.3 所示。

字节 3	字节 4
事件定义 ID	

表 5.3：事件定义 ID

[PRS_Ids_00015] d事件定义 ID 是安全事件的唯一标识符。它描述了安全事件的类型。c()

[PRS_Ids_00016] d如果传感器生成多个相同类型的安全事件，则称为 Event instance.c()

[PRS_Ids_00017] d 事件定义 ID 的范围分为三个范围：

1. AUTOSAR 内部 ID：0-0x7FFF（最多 32768 个安全事件）
2. 客户特定 ID：0x8000-0xFFFE（最多 32767 个安全事件）
3. 无效 ID：0xFFFF

c ()

5.1.4.4 计数

表 5.4显示了 IDS 元素计数。

字节 5	字节 6
数数	

表 5.4：计数

[PRS_Ids_00018] d 计数表示导致当前合格安全事件的IdsM API调用数。当一个事件被创建时，它的计数被初始化为 1。然而，像事件聚合这样的过滤器可以将几个事件组合成一个事件。此事件的计数设置为所有聚合事件的计数之和。如果安全事件是由已经过滤和预设计数值的智能传感器发送的，则该预设只是添加到IdsM的计数中。所以最终的计数是传感器的计数和IdsM processing.c()的结果之和

5.1.4.5 保留

保留字节如表 5.5 所示。

字节 7
预订的

表 5.5:保留

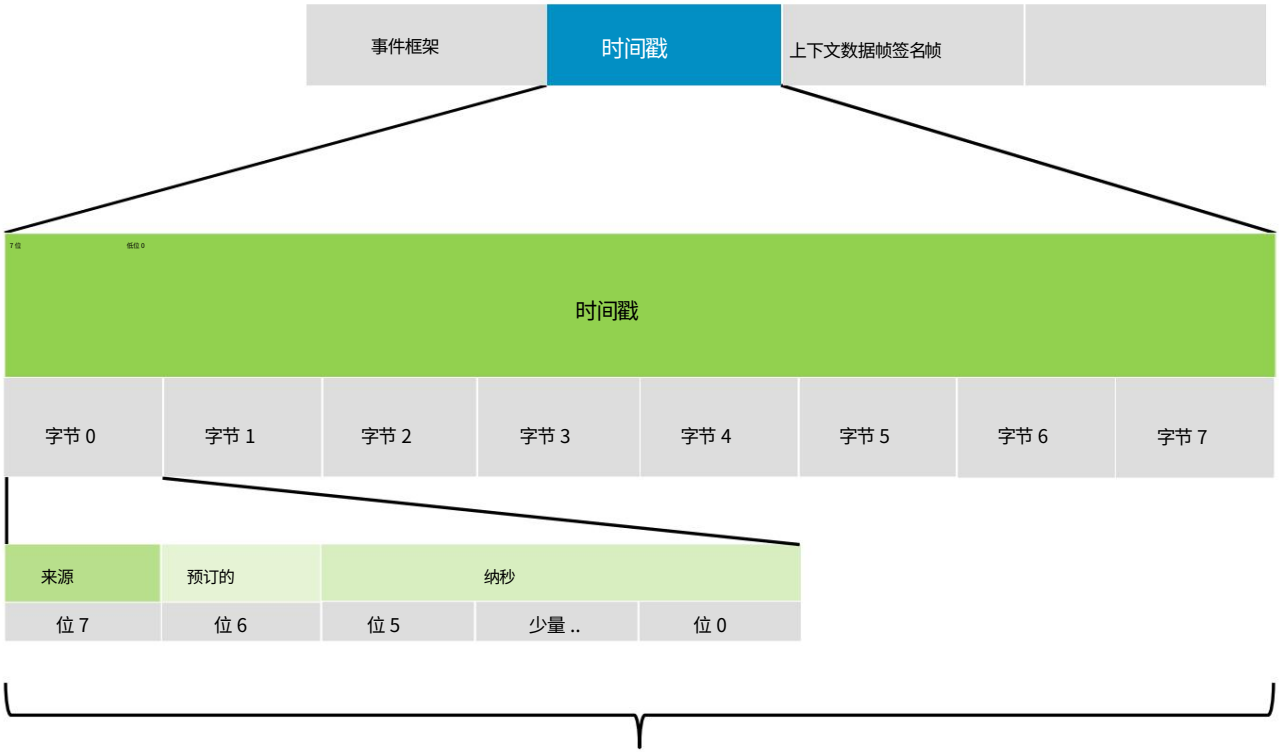
[PRS_Ids_00019] dIDS协议的Event Frame的Byte[7]保留供将来使用.c()

注意：

[PRS_Ids_00020] dReserved Bytes 应预设为值 0。在接收方应忽略这些字节。c()

5.1.5 时间戳

时间戳的详细信息如图 5.4 所示。



时间戳帧图 5.4:时间戳

[PRS_Ids_00401] dIDS协议提供时间戳作为可配置选项。c(RS_Ids_00502)

[PRS_Ids_00402] d它在第一次检测到安全事件时记录
（第一次出现）.c()

[PRS_Ids_00403] dResolution in ms 是必需的。时间戳应被编码
总共 64 位以适合单个 CAN frame.c()

[PRS_Ids_00404] d不同来源的时间戳可以在IDS中配置
协议。

- Bit[7]:时间戳来源

  0:AUTOSAR 标准 CP:StbM - AP:ara::tsync

  1:辅助/OEM 特定时间戳

- 位[6]:保留

c(RS_Ids_00503)

5.1.5.1 时间戳AUTOSAR

时间戳				
字节 0			字节 1	字节 2	字节 3
位 7	位 6	位 5 .. 0			
[illegible]	[illegible]	纳秒			

表 5.6:时间戳源和纳秒

时间戳			
字节 4	字节 5	字节 6	字节 7
秒			

表 5.7:时间戳秒

[PRS_Ids_00405] d对于IDS 协议AUTOSAR 时间格式结合了
30 位纳秒和 32 位秒的时间戳.c()

5.1.5.1.1 纳秒

[PRS_Ids_00406] dFor 纳秒只需要 30 位来编码 0..999 999
999 ns = 10-9秒.c()

笔记：

AUTOSAR 时间同步协议（例如 CP 中的 stbm)将 32 位用于纳秒。 IDS 协议的纳秒截断不限制分辨率

的时间戳。

5.1.5.1.2 秒

[PRS_Ids_00407] dSeconds 用 32 位编码,导致大约
127年决议.c()

笔记：

详情请参考时间同步协议 SWS-TimeSynchronisation
[2]

5.1.5.2 时间戳代工

时间戳				
字节 0		字节 1	字节 2	字节 3
位 7	位 6 .. 0			
	OEM 时间戳			

表 5.8:OEM 时间戳格式

[PRS_Ids_00408] dOEM时间源提供使用其他时间协议的选项。这
长度限制为 63 位。需要与OEM应用程序的接口。准确度是
由OEM.c()定义

5.1.6 上下文数据

[PRS_Ids_00501] dIDS协议提供了一个可选功能来丰富
在事件框架中传输的标准安全事件以及更详细的信息。因此可以添加上下文数据。它是传感器附加的二进制 blob。

这些数据包括有关安全事件的具体详细信息,可以
由SOC用于改进对安全事件的分析,例如格式错误的
通信传感器检测到的消息。
IdsM不了解这些数据的内容或结构。只有发行
传感器和后端或SOC知道它。c()

上下文数据有两种不同大小的变体:

5.1.6.1 上下文数据 - 大小 Long

图 5.5显示了具有 4 字节长度字段的“Context Data Size Long”。

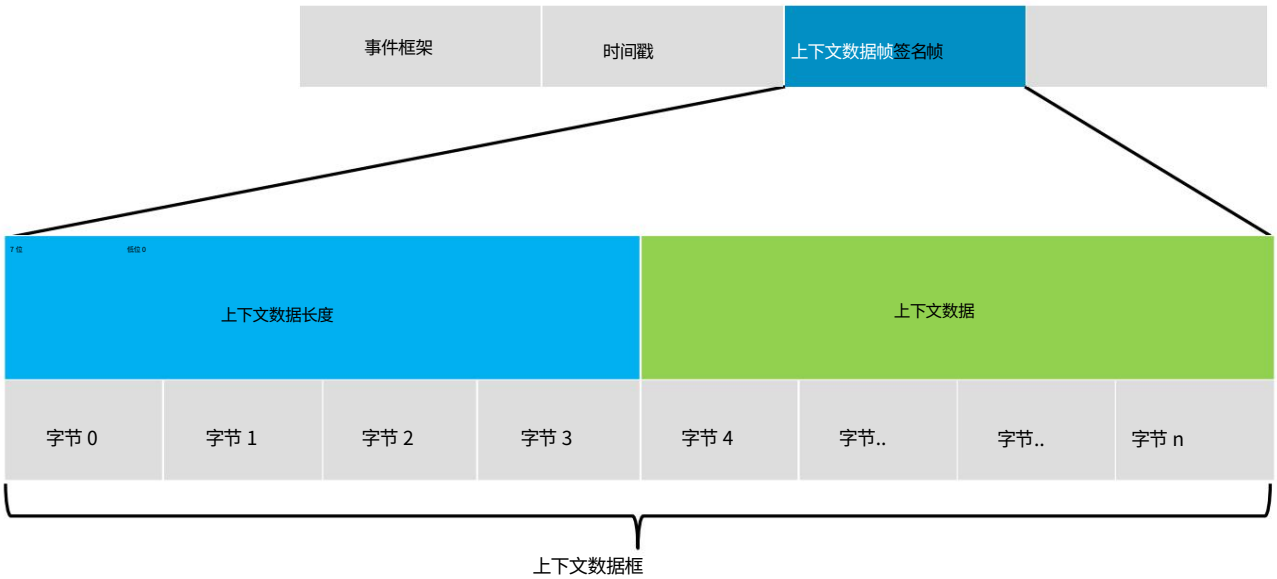


图 5.5:上下文数据大小长

[PRS_Ids_00502] d“上下文数据大小长”包括一个 4 字节长度字段。向上
可以传输到231-1上下文数据字节。c()

5.1.6.2 上下文数据 - 短尺寸

在图 5.6中显示了替代版本“Context Data Size Short”。

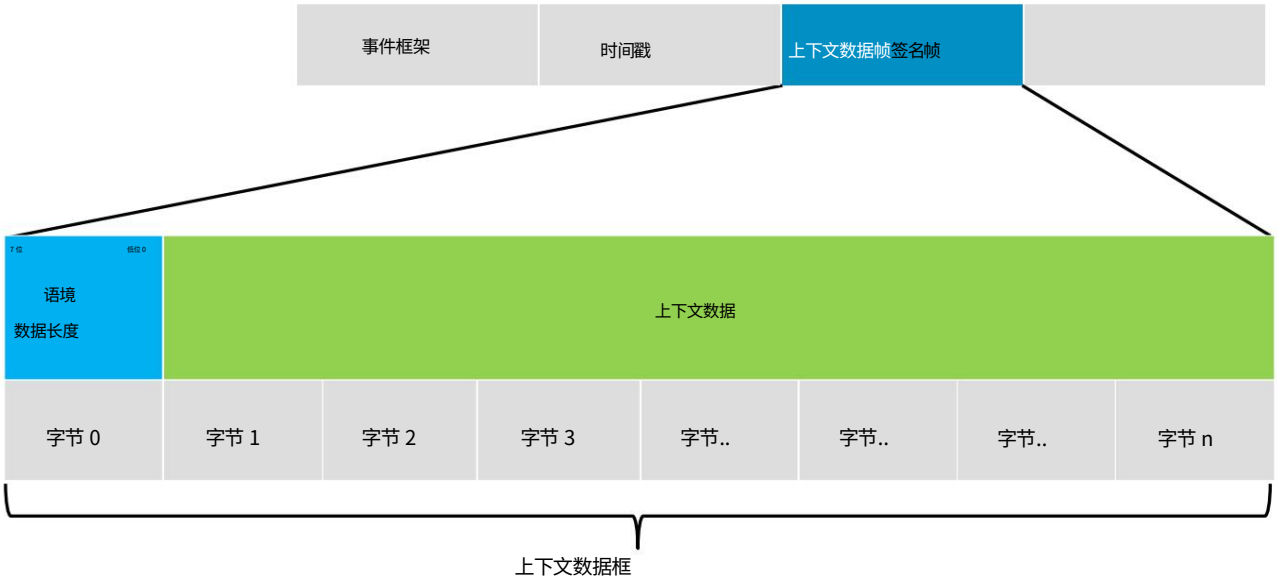


图 5.6:上下文数据大小短

[PRS_Ids_00503] d“上下文数据大小短”是 1 字节的替代版本
最大长度字段127 字节上下文数据.c()

5.1.7 上下文数据长度编码

上下文数据							
字节 0							
位 7	位 6	位 5	位 4	位 3	位 2	位 1	位 0
长度 格式	上下文数据长度						

表 5.9:上下文数据

[PRS_Ids_00504] d在表 5.9中显示了上下文数据长度的编码。

- 上下文数据字节[0]位[7]

  0:7位长度信息编码在上下文数据字节[0]位[0..6]:1-127
  字节

  1:在上下文数据字节[0..3]位[0..30]中编码的31位长度信息:
  1..(231-1)字节

如果长度以 7 位（1 字节)或 31 位（4 字节)编码,则第一个字节上下文数据 (MSB) 的最高有效位 (msb) 发出信号。c()

5.1.8 签名

[PRS_Ids_00601] dIDS协议提供了一个可选功能,使
QSEv的传输更安全。可以将数字签名添加到IDS 消息中。它可用于确保真实性以及证明签名的完整性

来自IdsM的消息通过所有通信系统直到到达后端
或SOC (End2End-Security).c(RS_Ids_00505)

图 5.7显示了IDS 协议的签名选项。

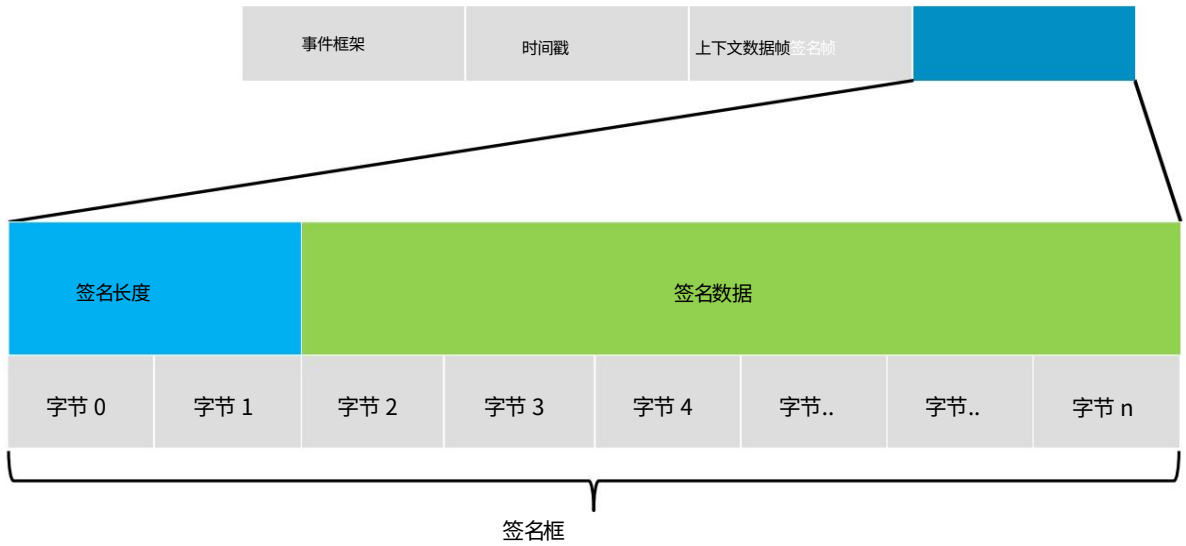


图 5.7:签名

5.1.8.1 签名长度

[PRS_Ids_00602] d

- 签名长度以 2 个字节编码:
  签名长度字节[0..1]:签名长度 1..65535

C ()

5.1.8.2 签名数据

签名							
字节 2	字节 3	字节 4	字节 5 字节 5签名		字节..	字节..	字节 n
数据							

表 5.10:签名

表 5.10显示了签名数据。 [PRS_Ids_00603] d

- 签名数据字节[2..65537]:签名数据

安全事件签名的加密值是用
序列化数据:
事件框架 + 可选时间戳 + 可选上下文数据。
使用哪种加密算法取决于系统。
IDS 协议没有规定任何特定的算法,也没有规定 format.c( )
（另请参阅5.1.4事件框架、 5.1.5时间戳和5.1.6上下文数据。）

5.1.9 IDS消息分离

[PRS_Ids_00800] d 在以太网上,IDS 消息分隔标头是强制性的。它
用于明确地处理IDS 消息。除了传输一个
单条IDS 消息通过以太网,可收集和发送多条IDS 消息
在单个以太网 frame.c() 中

[PRS_Ids_00801] d一个唯一的以太网端口地址应该用于IDS通信.c()

[PRS_Ids_00802] dSOME/IP和IDS消息不应在同一端口上混合
因为 receiver.c() 无法正确区分它们]

笔记:

IdsR通常通过以太网连接。但正如已经提到的其他
支持汽车通信总线和协议。关于留言
分离标题应考虑以下内容:

- CAN FD: I-Pdu-Multiplexer [3]支持在一条消息中收集多个IDS消息。由于CAN的尺寸限制

  I-Pdu-Multiplexer 通常使用短标头或无标头选项。所以
  IDS 消息分离头通常不用于CAN总线。
- FlexRay: PDU 打包功能支持收集多个IDS
  一条消息中的消息。它不使用分隔标题,但
  更新位以识别可用部件。
  有关详细信息,请参阅 SWS FlexRay 接口[4]。
- CAN (标准) :在没有 IDS 消息分隔头的情况下传输。
- LIN:在没有 IDS 消息分隔头的情况下传输。

5.1.9.1 IDS 消息分离头

图 5.8显示了 IDS 消息分离头。

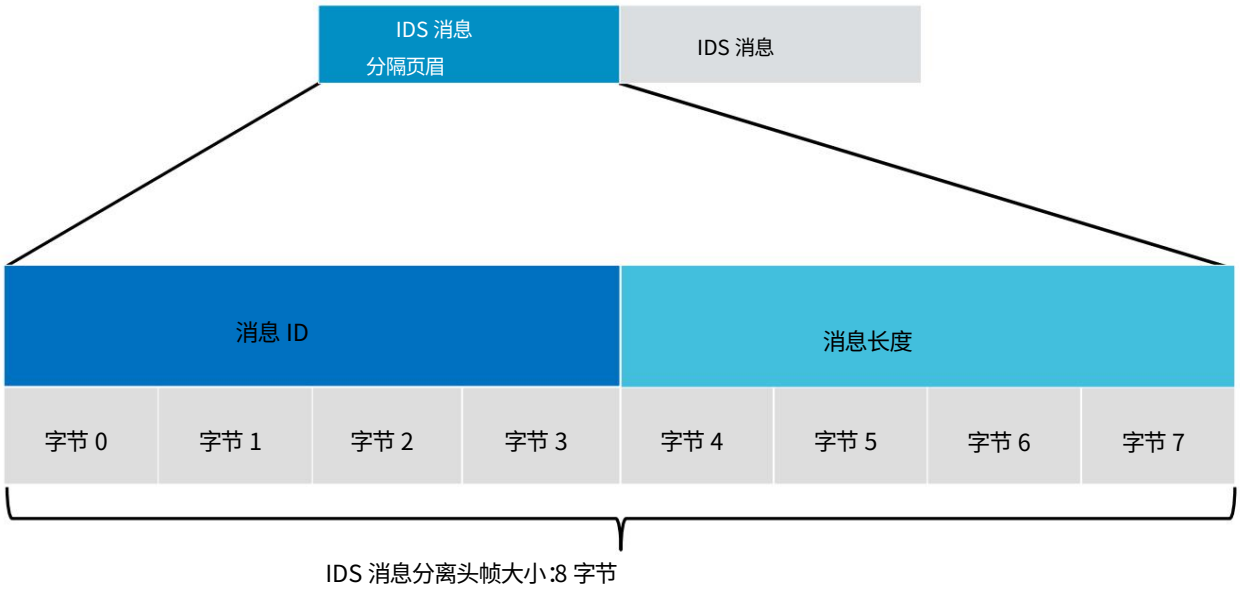


图 5.8:IDS 消息分隔标头

[PRS_Ids_00803] d
IDS 消息分离报头由一个 4 字节ID字段组成,用于在接收器处进行唯一标识,以及一个 4 字节长度字段指定数据长度。两者都大
字节序.c()

5.1.9.2 IDS消息分离头ID

[PRS_Ids_00804] dIDS 消息分隔标头 ID 以 4 字节编码。这是
任意数字,最好是 0.c()

笔记:
在 AUTOSAR CP中,IDS 消息分隔标头 ID 应在配置时设置
插座适配器和 I-PDU 多路复用器。
有关详细信息,请参阅 SWS-Socket Adapter [5]和 SWS-IPDUMultiplexer [3]。

5.1.9.3 IDS消息分离头长度

[PRS_Ids_00805] dIDS 消息分离头长度由下式计算
添加IDS消息长度和静态IDS消息分离头长度（8
字节）。它以 4 个字节编码。
可能的范围是:

消息长度字节[0..3]:16.. 2.147.549.212 Bytes.c()
最小长度为 16 字节:IDS 消息分隔头（8 字节)加上最小的IDS 消息,即事件帧（8 字节）,没有配置任何选项。

另请参阅5.1.11.2具有最小大小的示例 IDS 消息。

最大长度取决于配置的选项。
如果所有选项都配置了最大大小并且使用了 IDS 消息分隔头,则消息的总大小为 2.147.549.212 字节。
有关详细信息,请参阅5.1.11.1最大大小的 IDS 消息示例。

笔记：
AUTOSAR 平台：

- CP： IDS 消息分离头对应于SocketAdaptor/I-PDU-Multiplexer [5] / [3]支持的N-PDU机制。
- AP： IDS Message Separation Header 必须由IdsM 生成。

5.1.10 PDU 类型

注意：
在CP 中,IDS 协议使用IDS类型的GeneralPurposeIPdu （交互层协议数据单元)来传输合格的安全事件 QSEv。
详见系统模板[6],通讯一章。

5.1.11 IDS 消息示例

5.1.11.1 具有最大大小的示例 IDS 消息

[PRS_Ids_00900] d 配置最大大小的 IDS 协议的所有选项：

- 选项时间戳 AUTOSAR 已配置。
- Option Context Data Size Long 已配置。
- 选项签名已配置。

事件帧:8 字节时间
戳:8 字节上下文数
据大小长： 231-1字节 = 2.147.483.647 字节上下文数
据大小长长度编码:4 字节签名:65535 字节签名长度编码：
2 字节IDS 消息 = 8 + 8 + 2.147 .483.647 + 4 + 65535 +
2 = 2.147.549.204 字节

对于 CAN 总
线:CAN TP = 232 -1 = 4.294.967.295的最大消息大小

对于以太网:IDS
消息分隔头必须添加 8 个字节:带 IDS 分隔头的最大 IDS 消息:8 字节 +
2.147.549.204 字节 = 2.147.549.212 字节

IDS 消息分离头可以用 4 字节编码的最大大小:4 字节 = 232 = 4.294.967.296

这确保了最大尺寸的 IDS 消息可以通过标准汽车总线系统传输!c()

5.1.11.2 最小尺寸的示例 IDS 消息

[PRS_Ids_00901] d没有配置 IDS 协议选项 - 最小大小:

事件帧:8 字节
IDS 消息 = 8 Bytesc()

5.2 消息类型

目前不用于IDS 协议。

5.3 服务/命令

目前不用于IDS 协议。

5.4 序列（下层）

目前不用于IDS 协议。

5.5 错误信息

IDS 协议不发送特定的错误消息。

[PRS_Ids_00720] d如果出现特定于 IdsM 的内部错误
合格的安全事件被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于处理事件。

2. 上下文数据缓冲区溢出：没有更多的上下文数据缓冲区可用于存储上下文数据。

3. 流量限制溢出：当前流量超过配置的限制。

c(RS_Ids_00820)
注意：
这些事件的 ID 来自安全提取(SecXT)。有关详细信息，请参阅安全提取模板[7]。

6 配置参数

目前不用于IDS 协议。

7 协议使用和指南

目前不用于IDS 协议。

参考

[1] 入侵检测系统要求
AUTOSAR_RS_IntrusionDetectionSystem

[2] 时间同步规范
AUTOSAR_SWS_TimeSynchronization

[3] I-PDU多路复用器规范
AUTOSAR_SWS_IPDUMultiplexer

[4] FlexRay 接口规范
AUTOSAR_SWS_FlexRayInterface

[5] 插座适配器规格
AUTOSAR_SWS_SocketAdaptor

[6] 系统模板
AUTOSAR_TPS_SystemTemplate

[7] 安全提取模板
AUTOSAR_TPS_SecurityExtractTemplate