国际/sae
标准 21434

第一版
2021-08

道路车辆。网络安全工程

网络安全的知识

参考编号
ISO/SAE21434：2021(E)

ISO 版权办公室
CP401•Ch.de Blandonnet8
维尔尼尔 CH-1214；日内瓦
电话：+4122 749 01 11
电子邮件：copyright@iso.org
网站：www.iso.org

SAE 国际
400 英联邦博士。
美国宾夕法尼亚州沃伦代尔 15096
电话：877-606-7323（在美国和加拿大境内）
电话：+1724-776-4970（美国境外）
Fax：724-776-0790
电子邮件：CustomerService@sae.org
网站：www.sae.org

瑞士 ISO 出版，美国 SAE 国际出版

前言

ISO（国际标准化组织）是一个由国家标准机构（ISO 成员机构）组成的全球联合会。编制国际标准的工作通常由 ISO 技术委员会进行。对已设立技术委员会的问题感兴趣的每个成员机构都有权在该委员会中担任代表。国际组织、政府组织和非政府组织也参与了这项工作。ISO 与国际电工委员会(IEC)就所有电工标准化问题密切合作。

SAE 国际是一个由超过 128,000 名航空航天、汽车和商用车行业的工程师和相关技术专家组成的全球协会。来自 SAE 国际的标准被用于推进世界各地的移动工程。SAE 技术标准开发计划是该组织为航空航天、汽车和商用车提供服务的移动行业的主要条款之一。这些工作由来自 9000 多名工程师和世界各地其他合格专业人员的志愿者努力授权、修订和维护。SAE 主题专家在标准过程中充当个人，而不是作为其组织的代表。因此，SAE 标准代表了在一个透明、开放和协作的过程中开发的最佳技术内容。
ISO/IEC 指令第 1 部分和 SAE 技术标准委员会的程序。特别是，应注意对不同类型的 ISO 文件所需的不同批准标准。本文件根据 ISO/IEC 指令第 2 部分的编辑规则起草（见 www.iso、org/指令）。
我们提请注意，本文件的某些要素可能是专利权的主题。ISO 和 SAE 国际不负责识别任何或所有此类专利权。在文件开发过程中确定的任何专利权的细节将在介绍和/或收到的 ISO 清单中(见 www。iso，org/patents)。

SAE 技术标准委员会的规则规定：“本文件的发布是为了推进技术和工程科学的状态。本文件的使用完全是自愿的，其适用性和适用性，包括由此产生的任何专利侵权，是用户的唯一责任。”
本文件中使用的任何商品名称均为为方便用户而提供的信息，不构成背书。

有关标准的自愿性质、ISO 与一致性评估相关的具体术语和表达的含义，以及关于 ISO 在技术贸易壁垒(TBT)中遵守世界贸易组织(WTO)原则的信息，请参见 www。iso，org/iso/foreword.html.

本文件是由技术委员会 ISO/TC22、道路车辆、小组委员会 SC32、电气和电子部件和一般系统方面以及 SAE、TEVEES18A 车辆网络安全系统工程委员会共同编写的。
本第一版的 ISO/SAE21434 取消并取代了 SAEJ3061：2016 也]。
主要变化如下：
-完成内容和结构的返工。
关于本文件的任何反馈或问题都应直接指向用户的国家标准机构。这些尸体的完整清单可以在 www 上找到。iso，org/members.或者，要提供关于本文档的反馈，请访问 https://www。sae.org/standards/content/ISO/SAE21434/。.

介绍

本文件的目的
本文件阐述了道路车辆内电气和电子（E/E）系统工程中的网络安全视角。通过确保对网络安全的适当考虑，本文件旨在使 E/E 系统的工程能够跟上最先进的技术和不断发展的攻击方法。
本文档提供了与网络安全工程相关的词汇、目标、需求和指导方针，作为整个供应链常识的基础。这使组织能够：

— 定义网络安全政策和流程；

— 管理网络安全风险；以及
— 培养网络安全文化。
本文档可用于实现网络安全管理系统，包括网络安全风险管理。

本文件的组织
图 1 给出了对文档结构的概述。图 1 中的元素并没有规定单个主题的执行序列。

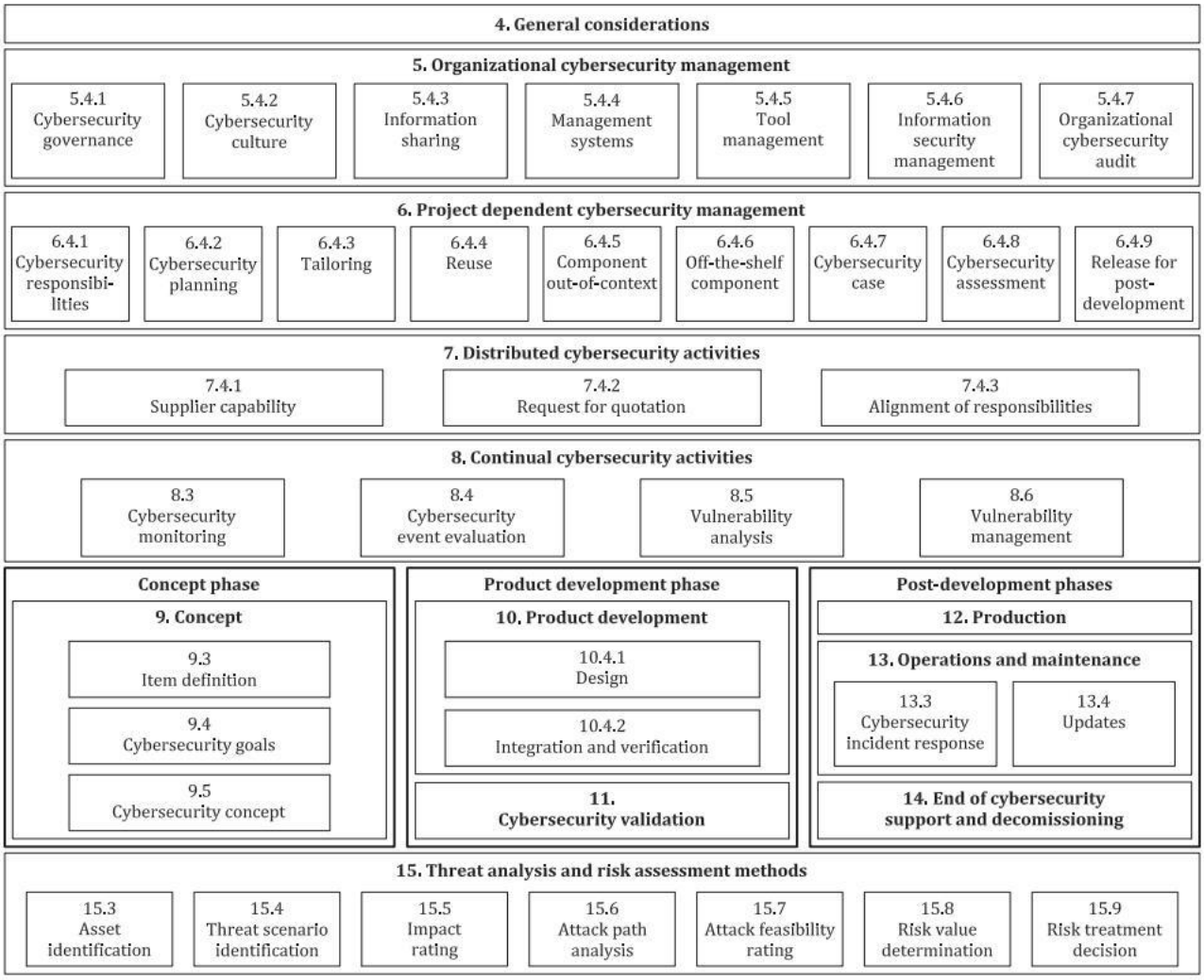


图 1-本文档的概述

第 4 条（一般考虑】是信息性，包括本文件中采用的道路车辆网络安全工程方法的上下文和观点。

第 5 条(组织网络安全管理]包括网络安全管理和组织网络安全政策、规则和流程的规范。
第 6 条(项目依赖的网络安全管理]包括项目级的网络安全管理和网络安全活动。
第 7 条（分布式网络安全活动）包括在客户和供应商之间分配网络安全活动责任的要求。
第 8 条（持续的网络安全活动）包括为正在进行的风险评估提供信息，并定义机电系统的漏洞管理，直到网络安全支持结束。

第 9 条[概念]包括确定网络安全风险、网络安全目标和网络安全要求的活动。
第 10 条(产品开发]包括定义网络安全规范、实施和验证网络安全要求的活动。
第 11 条（网络安全验证）包括车辆级项目的网络安全验证。第 12 条[生产]包括项目或部件的制造和组装中与网络安全相关的方面。
第 13 条（操作和维护）包括与网络安全事件响应和对项目或组件的更新相关的活动。
第 14 条（网络安全支持和退役）包括项目或组件支持和退役的网络安全考虑。
第 15 条（威胁分析和风险评估方法）包括模块化的分析和评估方法，以确定网络安全风险的程度，以便能够进行治疗。
第 5 至第 15 条有其自己的目标、规定（即要求、建议、许可）和工作产品。工作产品是满足一个或多个相关要求的网络安全活动的结果。

“先决条件”是由前一阶段的工作产品组成的强制性输入。进一步的支持信息”是可以考虑的信息，可以由不同于负责网络安全活动的人的来源提供。
关于网络安全活动和工作产品的总结可以在附件 A 中找到。

条款和工作产品被分配了唯一的标识符，包括两个字母的缩写(“RQ”表示要求，“RC”表示推荐，“PM”表示许可，“WP”)，后面是两个数字，用连字符分隔。第一个数字是指该条款，第二个数字分别给出了该条款的连续条款顺序或工作产品的顺序。例如，[RQ-05-14]是指第 5 条中的第 14 条规定，这是一项要求。

道路车辆。网络安全工程

1 范围

本文件规定了网络安全风险管理的概念、产品开发，生产、操作、维护和退役的工程要求，包括其部件和接口。
定义了一个框架，包括对网络安全过程的要求和对通信和管理网络安全风险的通用语言。

本文件适用于系列生产道路车辆机电系统，包括其部件和接口，并在本文件发布后开始开发或修改。

本文件没有规定与网络安全相关的具体技术或解决方案。

2 归一化引用

以下文件在文中被提及，其部分或全部内容构成了本文件的要求。对于有日期的参考文献，只有被引用的版本适用。对于未注明日期的参考文件，适用参考文件的最新版本（包括任何修订）。

ISO26262-3：2018，道路车辆。功能安全。第 3 部分：概念阶段

3 术语、定义和缩写术语

3.1 术语和定义

对于本文件的目的，适用以下术语和定义。

ISO 和 IEC 在以下地址维护术语数据库以用于标准化：
ISO 在线浏览平台：可在 https:〃www.iso.org/obp 上获得
IEC 电子百科：可在 https:〃www.clectropedia.org/上获得

3.1.1
建筑设计
允许识别组件的表示法(3.1.71。它们的边界、接口和相互作用

3.1.2
资产
具有值或贡献于价值的对象
输入注 1：资产具有一个或多个网络安全属性（3.1.20），其妥协可能导致一个或多个损坏场景（3.1.22）。

3.1.3
攻击可行性
攻击路径的属性（3.1.4）描述成功执行相应操作集的方便性

3.1.4
攻击路径
攻击
为实现威胁场景而采取的一套蓄意行动（3.1.33）

3.1.5
攻击者
执行攻击路径的人员、组或组织（3.1.4）

3.1.6
审计
检查过程，以确定过程目标的实现程度

[来源：ISO26262-1：2018 叫 3.5，修改-“关于”改为“以确定”和“实现”的程度。]

3.1.7
组件
在逻辑上和技术上都是可分离的部分

3.1.8
客户
接收服务或产品的个人或组织

【来源：ISO9000：2015 図，3.2.4，修改——“可以或确实接收”改为“接收”，忽略了“此人或组织有意或要求”，省略了示例和注释 1。】

3.1.9
网络安全
道路车辆网络安全
资产（3.1.2）对道路车辆（3.1.251（3.1.251 及其电气或电子部件）的威胁情况（3.1.33）
入口注 1：在本文件中，为了简洁起见，我们使用网络安全这个术语来代替道路车辆的网络安全。

3.1.10
网络安全评估
网络安全判断（3.1.9）

3.1.11
网络安全案例
有证据支持的结构化论点表明，风险（3.1.29）并非不合理

3.1.12
网络安全索赔
关于风险声明（3.1.29）

进入注 1：网络安全索赔可以包括保留或分担风险的理由。

3.1.13
网络安全概念
该项目的网络安全要求（3.1.251 和对运行环境的要求（3.1.261。与网络安全控制的相关信息（3.1.14）

3.1.14
网络安全控制
正在修改风险的度量标准（3.1.29）
[资料来源：ISO31000：2018 风 3.8，修改-单词“网络安全”被添加到术语中，短语“维护和/或”被删除，条目注释被删除。]

3.1.15
网络安全事件
与项目（3.1.25）或组件（3.1.7）相关的网络安全信息（3.1.18）

3.1.16
网络安全目标
与一个或多个威胁场景相关联的概念级网络安全需求（3.1.33）

3.1.17
网络安全事件
可能涉及漏洞的情况（3.1.38）

3.1.18
网络安全信息
尚未确定相关性的网络安全信息（3.1.9）

3.1.19
网络安全接口协议
客户（3.1.8）与供应商之间关于分布式网络安全活动的协议（3.1.23）

3.1.20
网络安全属性
这可以是值得保护的属性

项目注 1：属性包括机密性、完整性和/或可用性。

3.1.21
网络安全规范
网络安全要求及相应的架构设计（3.1.1）

3.1.22
损坏情况
涉及车辆或车辆功能和影响道路使用者的不利后果（3.1.31）

3.1.23
分布式网络安全活动
其职责在客户（3.1.8）和供应商之间分配的项目（3.1.25）或组件（3.1.7）的网络安全活动

3.1.24
影响
估计场景造成的伤害或物理伤害的估计（3.1.22）

3.1.25
项目
在车辆级别上实现功能的组件或组件集（3.1.7）

注意 1：如果系统在车辆级别实现功能，它可以是一个项目，否则它是一个组件。【来源：ISO26262-1：2018 叫 3.8，修改-术语“系统”已被“组件”取代，“ISO26262 应用的短语”和“或函数的一部分”已被省略，注释 1 已被替换。】

3.1.26
操作环境
在操作使用中考虑交互作用的上下文
入口注 1：项目（3.1.25）或组件（3.1.7）的操作使用可包括在车辆功能、生产和/或服务和维修中的使用。

3.1.27
上下文外
未在特定项目的上下文中开发（3.1.25）

将假定网络安全要求集成到不同项目中的处理单元。

3.1.28
渗透试验
在网络安全测试中，模拟真实世界的攻击，以确定危及网络安全目标的方法（3.1.16）

3.1.29
风险
网络安全风险
不确定性对道路车辆网络安全的影响（3.1.91，表示为攻击可行性（3.1.3）和影响（3.1.24）

3.1.30
风险管理
协调指导和控制风险组织的活动（3.1.29）
[资料来源：ISO31000：2018 风 3.2]

3.1.31
道路使用者
使用道路的人

例如乘客、行人、骑自行车者、司机或车主。

3.1.32
量身定制，动词
以与本文档中的描述不同的方式省略或执行一个活动

3.1.33
威胁场景
为了实现一个或多个资产（3.1.2）的网络安全属性（3.1.20）妥协的潜在原因（3.1.22）

3.1.34
分诊
分析以确定网络安全信息（3.1.18）与项目（3.1.25）或组件（3.1.7）的相关性

3.1.35
触发器
分诊标准（3.1.34）

3.1.36
验证
通过提供客观证据，确认该项目（3.1.251 的网络安全目标(3.1.16）已足够，并已实现
[来源：iso/iec/iee15288：2015[4]，4.1.53，修改-“特定预期用途或应用的要求”已被“项目的网络安全目标足够并已实现”取代，注释 1 已被省略。]

3.1.37
验证
通过提供客观证据，确认已满足了规定的要求
[来源：iso/iec/iee15288：2015[4]修改的注释 1 被省略。

3.1.38
漏洞
弱点（3.1.40）可作为攻击路径的一部分（3.1.4）

【来源：ISO/IEC27000：2018㈤，3.77，修改-“资产或控制”被省略；“被一个或多个威胁”被“作为攻击路径的一部分”取代。】

3.1.39　　漏洞分析
系统识别和评估漏洞（3.1.38）

3.1.40
软弱
可能导致不良行为的缺陷或特征

示例 1 缺少要求或规范。

示例 2 架构或设计缺陷，包括安全协议的不正确设计。
示例 3 实现弱点，包括硬件和软件缺陷、安全协议的错误实现。

例如 4 操作过程或程序中的缺陷，包括误用和用户培训不足。

示例 5　　使用过时或弃使用的函数，包括加密算法。

3.2 缩写术语
cal　　网络安全保证级别
cvss　　常见的漏洞评分系统
E/E　　电气和电子
ECU　　电子控制单元
obd　　车载诊断

OEM　　原设备制造商
下午　　许可
中华人民共和国　　建议

RQ　　要求
流氓　　负责、负责、支持、知情、咨询
塔拉　　威胁分析和风险评估
惠普　　工作产品

4 一般考虑

项目包括涉及在车辆级实现特定功能的车辆中的所有电子设备和软件(即其组件]，例如制动。项目或组件与其操作环境进行交互。
本文件的应用仅限于与网络安全相关的项目和零部件（即不是原型），包括售后市场和服务部件。外部系统

对于车辆（例如后端服务器），可以考虑用于网络安全的目的，但不在本文档的范围内。
本文档从单个项目的角度描述了网络安全工程。本文件中未规定对道路车辆机电体系结构中项目的适当功能分配。对于车辆作为整体，可以考虑车辆机电架构或其网络安全相关项目和组件的网络安全案例集。如果本文档中描述的网络安全活动是对项目和组件进行的，则将解决不合理的车辆网络安全风险。
本文档中描述的组织的整体网络安全风险管理适用于整个所有生命周期阶段，如图 2 所示。

图 2-整体网络安全风险管理

网络安全风险管理应用于整个供应链，以支持网络安全工程。汽车供应链表现出不同的合作模式。并非所有的网络安全活动都适用于参与特定项目的所有组织。网络安全活动可以根据特定情况的需要进行定制（见第 6 条）。特定项目或组件的开发合作伙伴就工作分割达成一致，以便执行适用的网络安全活动（见第 7 条）。
图 3 显示了项目、函数、组件和相关术语之间的关系。

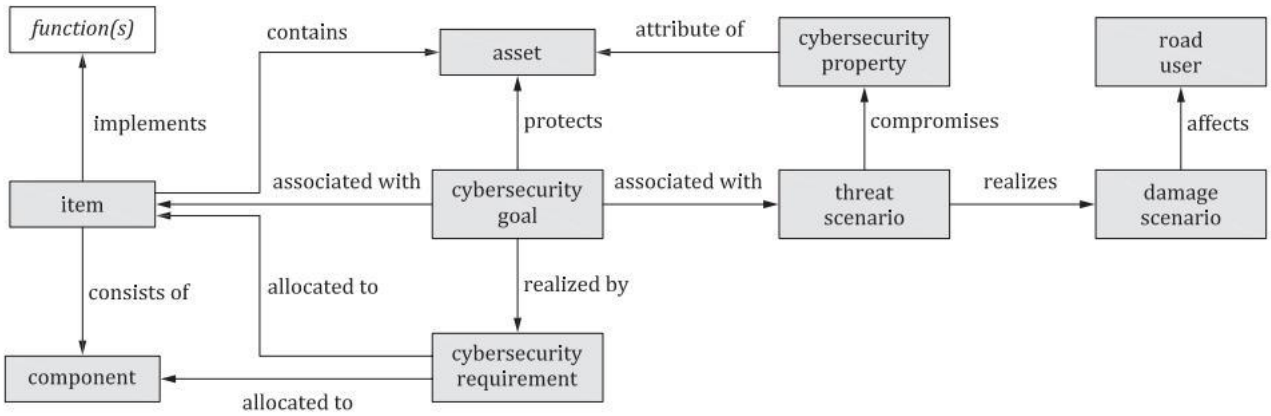


图 3-项目、功能、组件及相关术语之间的关系

第 15 条描述了在其他条款中描述的网络安全活动中调用的评估网络安全风险的模块化方法。
网络安全工程背景下的分析活动，识别并探索具有恶意的抽象对抗行为者所执行的潜在行动，以及车辆机电系统网络安全的损害可能造成的损害。网络安全工程和其他学科的专业知识之间的协调可以支持特定的深入分析和减轻网络安全风险(cf。ISO/TR4804 回)。网络安全监控、补救和事件响应活动补充了概念和产品开发活动，作为一种反应性方法，承认环境条件的变化（例如新的攻击技术），以及识别和管理道路车辆机电系统的弱点和弱点的持续需求。
一种深入的防御方法可以用来减轻网络安全风险。深入防御方法利用网络安全控制来提高车辆的网络安全。如果攻击能够穿透或绕过其中一层，那么另一层可以帮助控制攻击并保持对资产的保护。

5. 组织网络安全管理

5.1 一般来说

为了使网络安全工程成为可能，该组织建立并维护网络安全治理和网络安全文化，包括网络安全意识管理、能力管理和持续改进。这包括指定根据本文档的目标进行独立审计的组织规则和流程。

为了支持网络安全工程，该组织实施了网络安全的管理系统，包括管理工具和应用质量管理系统。

5.2 目标

本条款的目的是：

a) 定义网络安全政策和网络安全的组织规则和流程；

b) 指定执行网络安全活动所需的职责和相应的主管部门；

c) 支持网络安全的实施，包括提供资源和管理网络安全流程与相关流程之间的交互；

d) 管理网络安全风险；

e) 建立和维护网络安全文化，包括能力管理、意识管理和持续改进；

f) 支持和管理网络安全信息的共享；

g) 建立和维护支持网络安全维护的管理系统；

h) 提供证据证明使用工具不会对网络安全产生不利影响；和

i) 执行组织网络安全审计。

5.3 输入

5.3.1 先决条件

没有。

5.3.2 进一步支持信息

可以考虑以下信息：

-符合支持质量管理的标准的现有证据。

[1]示例 IATF16949 0 结合 ISO9001[8]，ISO10007[也，汽车香料®)，ISO/IEC330xx 系列标准[10]1，ISO/IEC/IEEE15288[11]ISO/IEC/IEEE12207[12].

5.4 要求和建议

5.4.1 网络安全治理

该组织应定义一个网络安全政策，其中包括：

a) 承认道路车辆的网络安全风险；以及

b) 执行管理层承诺管理相应的网络安全风险。

注 1 网络安全策略可以包括与组织的目标和其他策略的链接。
注 2 网络安全政策可以包括关于关于组织产品或服务组合的一般威胁场景的风险处理的声明，考虑到外部或内部的上下文。

本组织应建立和维护以下规则和流程：

I汽车香料®[13]是一个合适产品的例子。本信息是为方便本文档的用户而提供的，并不构成 ISO 对这些产品的认可。

a) 能够实现本文件的要求；以及

b) 支持相应活动的执行。

示例 1 流程定义、技术规则、指南、方法和模板。

注 3 网络安全风险管理可以包括活动的努力-效益考虑。

注 4 规则和流程包括概念、产品开发、生产、操作、维护和退役，包括 TARA 方法、信息共享、网络安全监控、网络安全事件响应和触发器。
注 5 关于漏洞披露的规则和流程，例如作为信息共享的一部分，可以根据 ISO29147 进行规定[14].

注 6 图 4 概述了总体网络安全策略（参见 RQ05-01]）与特定组织的网络安全规则和流程（参见 RQ05-02）、职责（参见 RQ05-03）和资源（参见 RQ05-04]之间的关系。

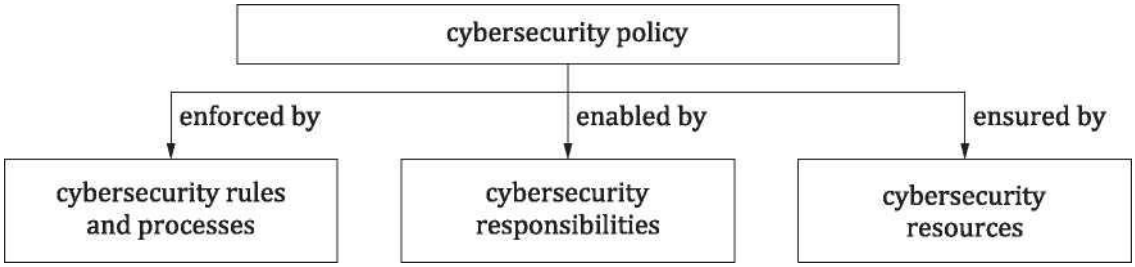


图 4-网络安全治理

[RQ-05-03]组织应分配和沟通实现网络安全的职责和相应的组织权限来实现和维护网络安全。

注 7.这与组织活动和与项目相关的活动有关。

该组织应提供解决网络安全问题的资源。
注 8：资源包括负责网络安全风险管理、开发和事件管理的人员。

例如 2.执行网络安全活动的熟练人员和适当的工具。
[RQ-05-05]该组织应确定与网络安全相关或与其互动的学科，并建立和维护这些学科之间的沟通渠道，以便：

a) 确定网络安全是否以及如何集成到现有流程中；以及

b) 协调相关信息的交流。

注 9 协调可以包括共享流程以及在学科之间使用策略和工具。

注 10.各学科包括信息技术安全、功能安全和隐私。

示例 3 中的跨学科交流：

— 威胁场景和危险(cf。ISO26262-1：2018 叫 3.75]信息；

— 网络安全目标和安全目标(cf。ISO26262-1：2018 叫 3.139)；和/或
— 网络安全要求与功能安全要求相冲突或相互竞争(cf。ISO262621：2018[1]，3.69)。

5.4.2 网络安全文化

该组织应培养和保持强大的网络安全文化。
注 1 例如，详见附件 B。

该组织应确保被分配给网络安全角色和职责的人有能力和意识。

注 2A 的能力、意识和培训计划可包括：

— 关于网络安全的组织规则和流程，包括网络安全风险管理；

— 与网络安全相关的学科相关的组织规则和流程，如功能安全和隐私；

领域知识；

-系统工程；

— 与网络安全相关的方法、工具和指导方针；和/或
— 已知的攻击方法和网络安全控制。

该组织应建立并保持一个持续的改进过程。

例如，持续改进过程，包括：

— 借鉴以往经验，包括网络安全监控和网络安全内外部网络安全相关信息收集的网络安全信息；

— 从网络安全相关信息中学习该领域类似应用的产品；

— 获得将在后续网络安全活动中应用的改进；

— 向相关人员传达有关网络安全的经验教训；以及

— 根据[RQ-05-02]检查组织规则和流程的充分性。
注 3 持续改进适用于本文档中的所有网络安全活动。

5.4.3 信息共享

[RQ-05-09]组织应定义组织内部或外部要求、允许或禁止与网络安全相关的信息共享的情况。
注意：共享信息的情况可以基于：

— 可以共享的信息类型；

— 共享审批流程；

— 对编辑信息的要求；

— 源归因规则；

— 针对特定各方的通信类型；

— 漏洞披露程序（见 5.4.1 中的注释 5）：和/或

— 对接收方关于处理高度敏感信息的要求。

该组织应根据[RQ-05-09]，将其对共享数据的信息安全管理与其他各方保持一致。

样例 调整公共、内部、机密、第三方机密的安全分类级别。

5.4.4 管理系统

该组织应按照国际标准或同等标准建立和维护质量管理体系，以支持网络安全工程，解决：

例如 1IATF16949 凶结合 ISO9001 陛

a) 变更管理；
注 1 网络安全变更管理的范围是管理项目及其组件的变化，以便继续满足适用的网络安全目标和要求，例如根据生产控制计划审查生产过程的变化，以防止此类变化引入新的漏洞。

b) 文件管理；

注 2 一个工作产品可以组合或映射到不同的文档存储库。

c) 配置管理；和

d) 要求管理。

[RQ-05-12]现场维护产品网络安全所需的配置信息应保留，直至产品网络安全支持结束，以便采取补救行动。

注 3 归档构建环境有助于确保以后使用配置信息。

示例 2 材料清单，软件配置。
应建立一个针对生产过程的网络安全管理系统，以支持第 12 条的活动。

示例 3IEC624432-1

5.4.5 工具管理

应管理能够影响项目或组件网络安全的工具。

示例 1 用于概念或产品开发的工具，如基于模型的开发、静态检查器、验证工具。

示例 2 在生产过程中使用的工具，如闪存写入器、端线测试器。

示例 3 用于维护的工具，如车载诊断工具或重编程工具。
注意：此类管理可通过以下方式建立：

— 应用于带有勘误数据的用户手册；

— 防止意外使用或行动的保护；

— 对工具用户的访问控制
— 工具的身份验证。
[RC-05-15]支持网络安全事件补救措施的适当环境（见 13.3）。
示例 4 用于复制和管理漏洞的测试、软件构建和开发环境。

示例 5 用于构建产品软件的工具链和编译器。

5.4.6 信息安全管理

工作产品应按照信息安全管理系统进行管理。
例如，工作产品可以存储在文件服务器上，以保护它们免受未经授权的更改或删除。

5.4.7 组织网络安全审计

网络安全审计应独立进行，以判断组织过程是否实现了本文件的目标。
注 1 网络安全审计可以包含在符合质量管理体系标准的审计中，或与之结合，例如 IATF16949[Z]与 ISO9001[81]。

注 2：独立性可以基于，例如，ISO26262 系列壁]。

注 3 执行审计的人员可以是组织的内部或外部。
注 4 为确保组织流程仍然适用于网络安全，可以定期进行审计。

注 5 图 7 说明了与其他网络安全活动相关的组织网络安全审计。

5.5 工作产品

网络安全政策、规则和流程，由 5.4.1 至 543 的要求制定

能力管理、意识管理和持续改进的证据为 5.4.2
由 544 的要求和 546 的要求所产生的组织管理系统的证据

工具管理的证据

[WP-05-05]根据 5.4.7 的要求提出的组织网络安全审计报告

6、项目依赖的网络安全管理

6.1 一般来说

本条款描述了关于对特定项目的网络安全开发活动的管理的要求。
与项目相关的网络安全管理包括职责的分配（见 6.4.1）和网络安全活动的规划（见 6.4.21。本文档以一种通用的方式定义了需求，以便它可以应用于各种项和组件。此外，还可以应用基于网络安全计划中定义的理论原理的定制方法(见 6.4.3]。何时可以使用裁剪的例子包括：
— 重用（见 6.4.4）。

-组件断章取用（请参见 645），
— 使用现成的组件（见 6.4.6）。
— 更新（见 13.4）。

项目和组件的重用是一种可能的开发策略，可以对项目、组件或其操作环境进行修改。但是，修改可能会引入可能没有考虑到的原始项目或组件的漏洞。此外，已知的攻击可能也发生了变化，例如：

— 一种攻击技术的发展，
— 新出现的漏洞，例如来自网络安全监控（见 8.3）和/或网络安全事件评估（见 8.4）。或
— 自原始开发以来资产的变化。

如果原始项目或组件是根据本文档开发的，则该项目或组件的重用是基于现有的工作产品。如果项目或组件最初不是按照本文档开发的，那么重用可以基于现有文档。

一个组件可以脱离上下文进行开发，即基于一个假定的上下文。在与客户达成接触或商业协议之前，组织可以为不同的应用程序和不同的客户开发通用组件。供应商可以对上下文和预期用途作出假设。在此基础上，供应商可以获得离义开发的需求。例如，一个微控制器可以开发脱离上下文。

一个现成的组件是一个不代表特定客户开发的组件，可以在不修改其设计或实现的情况下使用，例如一个第三方软件库、一个开源软件组件。假定没有按照本文档开发出现成的组件。

图 5 显示，现成组件和上下用组件都可以根据本文档集成到项目或组件中。该集成可以涉及类似于 644 中的重用分析的活动，如果进行了更改以解决无效的假设，则更改管理(请参见____)应用程序。可以对打算要集成的组件和/或作为集成目标的组件或项进行更改。

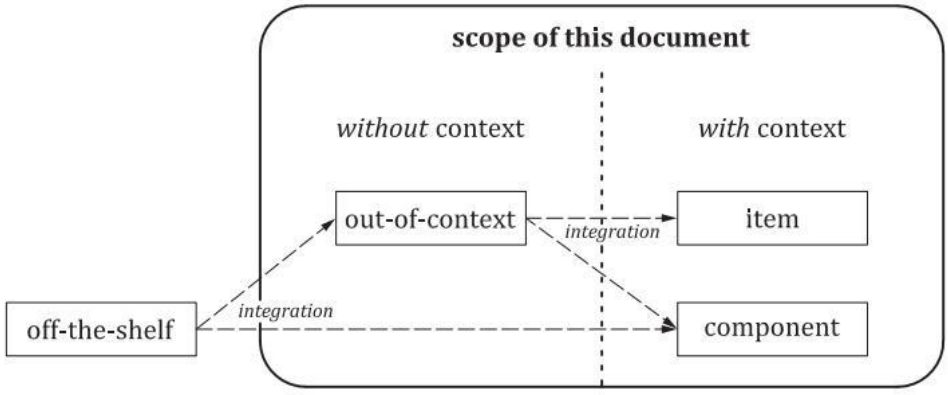


图 5-现成组件和非上下文组件的集成

网络安全案例（见 6.4.7）是对网络安全评估和开发后发布的输入。
网络安全评估（见 6.4.8）独立判断项目或组件的网络安全，是开发后发布决策的输入（见 6.4.9）。

6.2 目标

本条款的目的是：

a) 指定有关项目网络安全活动的职责；

b) 规划网络安全活动，包括量身定制的网络安全活动的定义；

c) 创建一个网络安全案例；

d) 如果适用，应进行网络安全评估；以及
e) 从网络安全的角度决定是否可以发布该项目或组件以进行后开发。

6.3 输入

6.3.1 先决条件
没有。

6.3.2 进一步支持信息
可以考虑以下信息：

-组织网络安全审计报告；
-项目计划。

6.4 要求和建议

6.4.1 网络安全责任
有关项目网络安全活动的责任应按照[RQ-05-03]进行分配和沟通。
注：网络安全活动的职责可以转移网络安全活动的责任。

6.4.2 网络安全规划
[RQ-06-02]为了决定项目或组件所需的网络安全活动，应分析项目或组件以确定：

a) 该项目或组件是否与网络安全相关；
注 1 附录 D 提供了一种可用于评估网络安全相关性的方法和标准。

注 2 如果该项目或组件被确定为与网络安全无关，则没有网络安全活动，因此网络安全计划不继续。

b) 如果该项目或组件与网络安全相关，则该项目或组件是新开发还是重用；以及
c) 是否按照 643 进行裁剪。
网络安全计划应包括：

a) 活动的目标；

b) 对其他活动或信息的依赖性；

c) 负责开展活动的人员；

d) 执行活动所需的资源；

e) 起点或终点，以及活动的预期持续时间；以及

f) 识别要生产的工作产品。
[RQ-06-04]应根据[RQ-05-03]和[RQ-05-04]分配制定和维护网络安全计划以及跟踪针对网络安全计划的网络安全活动进展的职责。
网络安全计划应包括：

a) 项目计划中引用的；

b) 包括在项目计划中，以便网络安全活动是可区分的。
注 3 网络安全计划可以包含对其他计划（例如，项目计划）的交叉引用，这些计划也处于配置管理之下（也请参见[RQ-06-09]]。

[RQ-06-06]网络安全计划应根据第 9、10.11 和 15 条的相关要求，规定在概念和产品开发阶段进行网络安全所需的活动。

当确定了要执行的活动的更改或改进时，应更新网络安全计划。

注 4 网络安全计划可以在开发过程中逐步进行细化。例如，网络安全计划可以根据网络安全活动的结果进行更新，如 TARA（见第 15 条）。
[PM-06-08]对于根据 15.8conformity 第 9.5 条第 10 条和第 11 条的分析确定的风险值 1 的威胁场景，可以省略。. .

注 5 这些威胁场景可能会对网络安全产生影响，如果是这样，将处理相应的风险，尽管可能没有本文档中定义的那么严格。

注 6 此类风险处理的充分性可以根据网络安全案例中定义的理由进行论证。其基本原理可以基于符合质量管理标准，如 IATF16949 和 ISO9001[8]，并结合其他措施，例如：

— 网络安全意识的保证；

— 对质量人员的网络安全培训

— 组织质量管理体系中定义的网络安全具体措施。
[RQ-06-09]网络安全计划中确定的工作产品应进行更新和维护，以保持准确性。
[RQ-06-10]如果将网络安全活动分发，客户和供应商各自应根据第 Z 条制定有关各自网络安全活动和接口的网络安全计划
网络安全计划应按照第 544 条的规定进行配置管理和文件管理。

[RQ-06-12]网络安全计划中确定的工作产品应按照 544 年的标准进行配置管理、变更管理、需求管理和文档管理。

6.4.3 尾矿
网络安全活动可以量身定制。

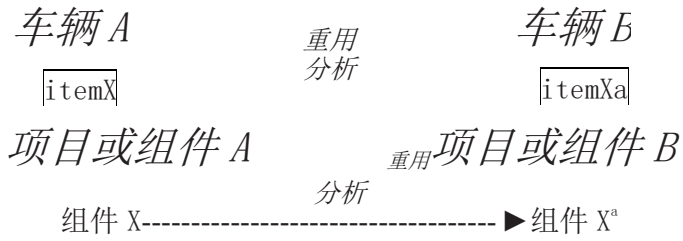
[RQ-06-14]如果定制了网络安全活动，则应提供并审查为什么定制活动足以实现本文件的相关目标的理由。
注意：由于供应链中的另一个实体执行而未执行的活动不被视为定制活动，而是分布式网络安全活动（见第 7 条）。然而，网络安全活动的分发可能会导致联合定制（见 7.4.3）。

6.4.4 重新使用
如果开发了项目或部件，应进行重用分析：

a) 计划进行修改；

b) 是否计划在其他操作环境中重复使用；或

示例 1 由于在新的操作环境中安装现有项目或组件，或由于与之交互的其他项目或组件的升级而导致的对环境的修改（请参见图 6）。



[a]可以由于重用分析而进行更改。

图 6-重用分析示例

c) 计划不经修改就重复使用，有关项目或组件的信息有相关更改。

示例 2 已知攻击和漏洞的更改，或威胁场景的更改。

注 1 在确定是否可能重用时，考虑现有的工作产品。

注 2：修改可包括设计修改和/或实施修改：

— 设计的修改可能来自于需求的修改，例如功能或性能的增强；

— 实现修改可以源于对软件的修正，或使用新的生产或维护工具，例如基于模型的开发。

注 3 如果对配置数据或校准数据的更改影响了项目或组件的功能行为、资产或网络安全属性，则被视为一种修改。
对项目或部件的重用分析应：

a) 确定对项目或组件的修改以及对其操作环境的修改；

b) 分析修改对其产生的网络安全影响，包括对网络安全索赔有效性和先前假设的影响；

示例 3 对网络安全需求、设计和实现、操作环境、假设和操作模式的有效性、维护、对已知攻击的敏感性和已知漏洞或资产的暴露的影响。

c) 识别受影响或缺失的工作产品；以及

示例 4 考虑新资产或修改资产、威胁场景或风险价值的 TARA。

d) 在网络安全计划中指定符合本文件所需的网络安全活动（见 642）。

注 4 这可能意味着裁剪（请参见 6.4.3）。
对组件的重用分析应评估是否：

a) 组件能够满足要集成的项目或组件所分配的网络安全要求；以及
b) 现有的文档足以支持集成到项目或其他组件中。

6.4.5 组件上下文外

[RQ-06-18]相应的工作产品中应记录对外部开发的组件的预期用途和上下文的假设，包括外部接口。

对于断章取义地开发组件，网络安全要求应基于[RQ-06-18]的假设。

对于集成上下文开发的组件，其的网络安全声明和假设应得到验证。

6.4.6 现成组件

在集成一个现成的组件时，应收集并分析与网络安全相关的文档，以确定是否：

a) 可以满足已分配的网络安全要求；

b) 该组件适用于预期用途的特定应用程序上下文；以及

c) 现有的文档足以支持网络安全活动。

[RQ-06-22]如果现有文档不足以支持现成组件的集成，则应识别并执行符合本文档的网络安全活动。

示例：有关漏洞的文档不足。
注意：这可能意味着裁剪（见 6.4.3）。

6.4.7 网络安全案例

应创建一个网络安全案例，以为有工作产品支持的项目或组件的网络安全提供依据。
注 1 参数的部分可以是隐式的（例如，如果参数的一部分从编译的工作产品集中明显，那么可以省略）。

注 2 在分布式开发中，项目的网络安全案例可以是客户和供应商的网络安全案例的组合，它们引用了来自双方生成的工作产品的证据。然后，来自各方的论据支持项目的整体论点。

注 3 网络安全案例考虑了网络安全案例对开发后的网络安全要求。

6.4.8 网络安全评估

是否对某一项目或组件进行网络安全评估的决定应采用基于风险的方法的理由支持。
注 1：其基本原理可以基于：
— TARA 结果（见第 15 条）：

— 待开发的项目或组件的复杂性
— 由组织规则和流程定义的标准（见 5.4.1）。
注 2 如果没有进行网络安全评估，其理由可以记录在网络安全案例中。

研究结果表明，对其基本原理应进行独立审查。
注 3 该独立方案可基于 ISO26262 系列壁]。
网络安全评估应对项目或组件的网络安全进行判断。
注 4 现有证据由网络安全活动的记录结果，即工作产品（见附件 A）提供。

网络安全评估和其他网络安全活动。

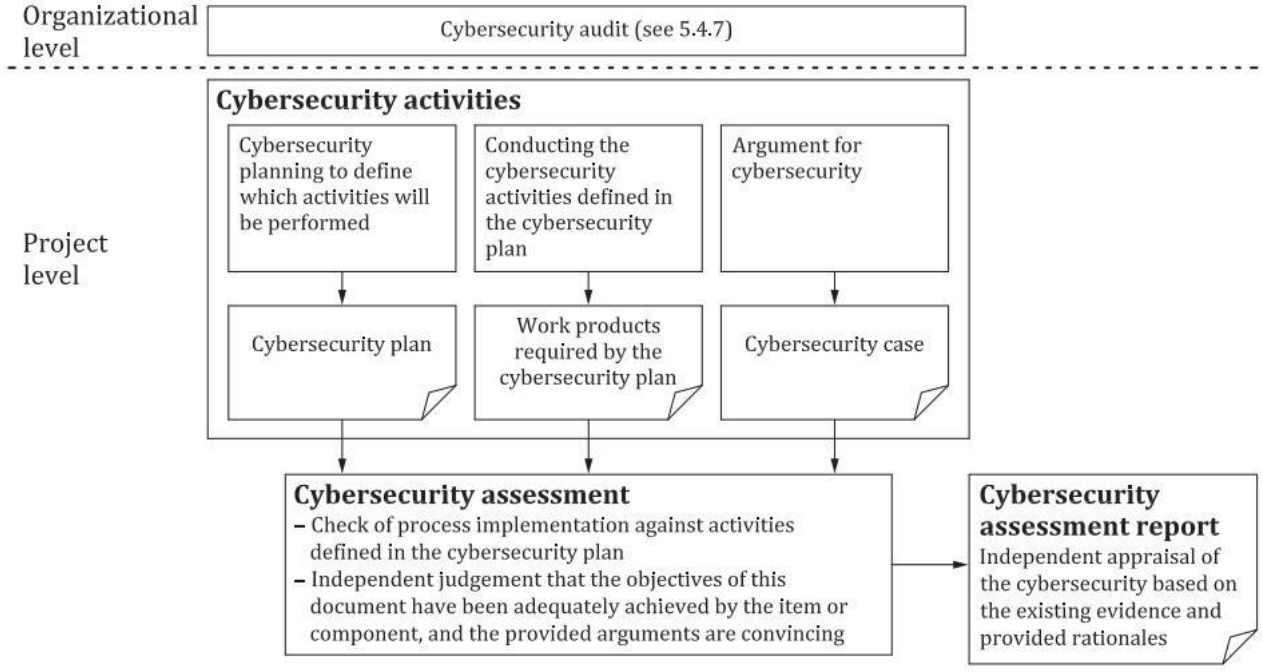


图 7-与其他网络安全活动相关的网络安全评估

注 6A 网络安全评估可以逐步进行，以促进早期解决已确定的问题。

注 7 网络安全评估可以重复或补充，例如，由于更改，当以前的网络安全评估提供了负面建议时，或当发现了一个漏洞时。
应根据[RQ-06-01]的规定指定负责计划和独立计划和执行网络安全评估的人员。

注 8：独立方案可基于 ISO26262 系列

例如，来自组织内不同团队或部门的人员，如质量保证，来自独立组织的人员。
进行网络安全评估的人员应具备：

a) 获取相关信息和工具；以及
b) 开展网络安全活动的人员的合作。
网络安全评估可能是基于对本文件的目标是否已实现的判断。
网络安全评估的范围应包括：

a)网络安全计划和网络安全计划中确定的所有工作产品；

b) 网络安全风险的处理；
c) 为项目实施的网络安全控制和网络安全活动的适当性和有效性；以及

注 9 其适当性和有效性可以通过使用为验证目的而事先进行的审查来判断。

d) 如果提供了证明实现本文件目标的理由。
注 10 负责创建工作产品的人员可以提供为什么实现本文档的相应目标，以促进网络安全评估[PM-06-13]。
注 11 满足所有相应的要求是实现本文件目标的充分依据。

网络安全评估报告应包括对项目或组件的接受、有条件接受或拒绝网络安全的建议。
注 12.评估报告还可以包括关于持续改进的建议。
如果根据[RQ-06-31]提出了有条件验收的建议，则网络安全评估报告应包括验收条件。

面向开发后的 6.4.9 发布
以下工作产品应在开发前发布：

a) 网络安全案例；

b) 如果适用，请发布网络安全评估报告；以及

c) 开发后的网络安全要求。
项目或部件开发后发布，应满足以下条件：

a) 网络安全案例所提供的关于网络安全的论证是令人信服的；

b) 网络安全案件经网络安全评估确认；

c) 接受开发后阶段的网络安全要求。

注 更改可能导致重新评估开发后的发布，例如网络安全的更改
索赔。

6.5 工作产品
[WP-06-01] 网络安全计划，由 641 年至 646 年的要求而产生

[WP-06-02] 网络安全案例，由 647 年的要求而产生

网络安全评估报告，如适用，由要求
648

根据 649 的要求，发布开发后报告

7. 分布式网络安全活动

7.1 一般来说

如果一个项目或组件的网络安全活动的责任被分配，则适用本条款。
本条款描述了对分布式网络安全活动的管理，并适用于：

a) 在分布式活动中开发的项目和组件；

b) 客户和供应商之间的互动；以及
c) 协议适用于客户/供应商接口的所有阶段。

内部供应商可以以与外部供应商相同的方式进行管理。

例如，一级组织可以在开发期间可以是 OEM 的供应商，在另一个合同关系中，一级组织可以是组件的二级组织的客户。这一点如图 8 所示。

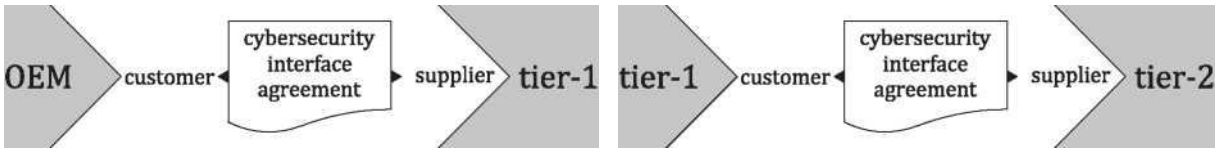


图 8—关于供应链中的客户/供应商关系的用例

7.2 目标

本条款的目的是定义客户和供应商之间的分布式网络安全活动的交互、依赖关系和责任。

7.3 输入

没有。

7.4 要求和建议

7.4.1 供应商能力

应评估候选供应商开发并在适用时根据本文件进行开发后活动的能力。
注 1 本评估支持供应商的选择，可以基于供应商符合本文件的能力，或基于对之前实施的关于网络安全工程的其他国家或国际标准的评估。
为了支持客户对供应商能力的评估，供应商应提供一份网络安全能力的记录。
注 2A 关于网络安全能力的记录可包括：

— 该组织关于网络安全能力的证据（例如，来自开发、开发后、治理、质量和信息安全的网络安全最佳实践]；
— 持续网络安全活动（见第 8 条）和网络安全事件响应（见第 13 条）；以及

-对以前的网络安全评估报告的摘要。

7.4.2 报价请求

客户向候选供应商提出的报价请求应包括：

a) 符合本文件的正式要求；
b) 期望供应商根据第 743 条的规定承担网络安全责任；以及

c) 与供应商所报价的项目或组件相关的网络安全目标和/或网络安全要求集。

示例与消息认证相关的网络安全要求。

7.4.3 责任比对

客户和供应商应在网络安全接口协议中指定分布式网络安全活动，包括：

a) 预约客户和供应商关于网络安全的联系点；

b) 识别将分别由客户和供应商执行的网络安全活动；

示例 1 由客户执行的车辆级别上的网络安全验证。

示例 2 关于开发后的网络安全活动的分发。

示例 3 关于供应商开发的零部件或工作产品的网络安全评估可以由第三方、客户或供应商执行。

c) 如果适用，根据第 643 条联合定制网络安全活动；

d) 要共享的信息和工作产品；
注 1 所共享的信息可包括：

— 发布、审查和网络安全问题反馈机制；

— 漏洞的信息交换程序和其他与网络安全相关的发现，例如有关风险；

— 与接口相关的过程、方法和工具，以确保客户和供应商之间的兼容性，如正确处理数据和确保通信用于传递这些数据的网络；

— 角色定义，

— 沟通和记录项目或组件中变化的方法，包括 TARA 的潜在重复；

— 对需求管理工具的一致性
— 网络安全评估的结果。

e) 有关分布式网络安全活动的里程碑；和

f) 对项目或组件的网络安全支持结束的定义。
在分布式网络安全活动开始之前，网络安全接口协议应在客户和供应商之间共同达成协议。

如果存在需要根据[RQ-08-07]进行管理的确定漏洞，客户和供应商应就这些行动的行动和责任达成一致。

[RQ-07-07]如果要求不明确、不可行，或与其他网络安全要求或其他学科的要求相冲突，则客户和供应商应相互通知对方，以便作出适当的决策和行动。

职责应在责任分配矩阵中加以规定。
注 2：可使用 RASIC 表，见附件 C。

7.5 工作产品

网络安全接口协议，由要求 743 产生

8. 持续的网络安全活动

8.1 一般来说

持续的网络安全活动将在生命周期的所有阶段进行，并且可以在特定项目之外进行。
网络安全监控（见 8.3）收集网络安全信息，并根据已定义的触发器分析网络安全信息进行分类。
网络安全事件评估（见 8.4）确定网络安全事件是否存在项目或组件的弱点。
脆弱性分析（见 8.5）检查弱点，并评估是否可以利用特定的弱点。
漏洞管理（见 8.6）跟踪并监督项目和组件中已识别漏洞的处理，直到其网络安全支持结束。

8.2 目标

本条款的目的是：

a) 监控网络安全信息，识别网络安全事件；

b) 评估网络安全事件，以识别弱点；

c) 从弱点中识别出弱点；以及

d) 管理已识别的漏洞。

8.3 网络安全监控

8.3.1 输入

8.3.1.1 先决条件

应提供以下信息：

-用于开发触发器的规则和流程。

8.3.1.2 进一步支持信息

可以考虑以下信息：

项目定义[WP-09-01]；

-网络安全索赔要求；

-网络安全规范；

威胁场景[WP-15-03]；

— 过去的漏洞分析；

— 从该字段收到的信息。

例如，漏洞扫描报告、修复信息、消费者使用信息。

8.3.2 要求和建议

网络安全信息的收集应选择信息来源。

注 1 可以选择内部和/或外部来源。
注 2 内部来源可以包括 8.3.L2 中列出的那些来源。

注 3：外部资料来源可以包括：

—researchers；

— 商业性或非商业性的资料来源；

— 组织供应链；

— 本组织的客户；和/或
-政府来源。

最先进的攻击方法的示例来源。

对于网络安全信息的分类，应定义和维护触发器。
注 4 触发器可以包括关键字、配置信息的参考资料、组件或供应商的名称。
[RQ-08-03]应收集并试用网络安全信息，以确定该网络安全信息是否成为一个或多个网络安全事件。

8.3.3 工作产品

网络安全信息的来源，来自于网络安全信息的来源

触发器，由 RQ-08.02]产生的触发器

网络安全事件，由此造成的网络安全事件

8.4 网络安全事件评估

8.4.1 输入

8.4.1.1 先决条件

应提供以下信息：

-网络安全事件；

— 开发后的网络安全要求[WP-10-02]，如果适用；以及

— 配置信息符合 RQ-05-12]。

8.4.1.2 进一步支持信息

可以考虑以下信息：

项目定义[WP-09-01]；

-网络安全规范；

-过去的漏洞分析。

8.4.2 要求和建议

应对网络安全事件进行评估，以识别项目和/或组件中的弱点。

注 1 该活动可与[RQ-08-03]的分类相结合。
注 2 如果存在缺陷并且存在可用的补救措施（例如供应商为组件中的漏洞提供的补丁），组织可以将补救措施（参见 8、6）处理为假定的漏洞，而不需要任何其他活动。

注 3 威胁场景可根据此评估结果[WP-15-03]进行更新。

8.4.3 工作产品

网络安全事件造成的弱点，由网络安全事件造成的弱点

8.5 漏洞分析

8.5.1 输入

8.5.1.1 先决条件

应提供以下信息：

-项目定义，或网络安全规范。

注意：如果在项目上执行漏洞分析，则使用项目定义，如果在组件上执行漏洞分析，则使用网络安全规范。

8.5.1.2 进一步支持信息

可以考虑以下信息：

— 网络安全事件造成的弱点；

— 在产品开发过程中发现的弱点；

— 过去的漏洞分析；

— 攻击路径[WP-15-05]

— 验证报告和验证报告；
— 来自过去网络安全事件的信息。

8.5.2 要求和建议

应分析漏洞，以识别漏洞。
注 1 该分析可包括：

— 架构分析；
— 根据 15.6：和/或要求进行的攻击路径分析
— 攻击的可行性等级符合第 15.7 节的标准。
注 2 可以执行根本原因分析来确定导致弱点可能成为漏洞的任何潜在因素。
示例 1 攻击路径分析显示没有攻击路径存在，因此，该弱点不被视为漏洞。
例子 2 利用弱点的攻击可行性评级非常低，因此，弱点不被视为漏洞。

对于未被确定为漏洞的弱点，应提供一个理论依据。

8.5.3 工作产品

脆弱性分析，由 RQ 和 RQ-08-06]得出

8.6 漏洞管理

8.6.1 输入

8.6.1.1 先决条件
应提供以下信息：

-漏洞分析。

8.6.1.2 进一步支持信息
没有。

8.6.2 要求和建议
应对漏洞进行管理，以便针对每个漏洞：
a) 相应的网络安全风险按照 15.9 进行评估和处理，以便不存在不合理的风险；或
b) 通过应用独立于 TARA 的可用补救措施来消除该漏洞。

开源软件的示例修补程序示例。

注 1 如果漏洞管理导致对项目或组件的变更，则按照[RQ-05-11]应用变更管理。
注 2 关于漏洞的信息可以在分布式网络安全活动的上下文中共享（见 743，例如共享攻击路径的知识)和其他相关方(见 5.4.3）。
[RQ-08-08]如果根据第 15.9 条规定的风险处理决策需要网络安全事件响应，则应应用第 13.3 条。
注 3 网络安全事件响应过程可以独立于 TARA 进行应用。

8.6.3 工作产品

受管理漏洞的证据

9 概念

9.1 一般来说

概念阶段涉及到考虑车辆级的功能，如在项目中实现的那样。在本条款中，项目及其操作环境被标识为“项目定义”（见 9.3）。项目的定义构成了后续活动的基础。

本条款还指定了该项目的网络安全目标（见 9.4）。这是最高级别的要求。为此，网络安全风险被评估，这是通过使用 Cleus 的方法来实现的。15(另见附件 H，图 H.11。此外，9,4 指定了网络安全索赔，用来解释为什么风险保留或共享被认为是足够的。
网络安全概念（见 9.5）包括网络安全要求和对操作环境的要求，这两者都来自网络安全目标，并基于对项目的全面视图。

9.2 目标

本条款的目的是：

a) 在网络安全领域定义项目及其操作环境及其相互作用；

b) 明确网络安全目标和网络安全声明；以及
c) 明确网络安全概念，以实现网络安全目标。

9.3 项目定义

9.3.1 输入

9.3.1.1 先决条件

没有。

9.3.1.2 进一步支持信息

可以考虑以下信息：

-有关项目和操作环境的现有信息。

例如车载机电系统架构，包括车载网络、车辆外部网络、参考模型）和早期开发的文档。

9.3.2 要求和建议

应确定有关该项目的以下信息：

a) 项目边界；
注 1 项目边界将项目与操作环境区分开来。项目边界的描述可以包括与车辆内部的其他项目的接口和/或与车辆外部的 E/E 系统的接口。

b) 项目功能；和
注 2 这描述了项目在生命周期阶段的预期行为（例如，产品开发（测试）、生产、操作和维护、退役】，并包括由项目实现的车辆功能。
c) 初步架构。

注 3 对初步体系结构的描述可以包括项目的组件及其连接的标识，以及项目的外部接口。
注 4 本文档中描述的项目定义，特别是项目边界，可能与其他学科的项目定义不同，例如根据 ISO26262series 壁的功能安全]。

注 5 可以考虑关于约束条件和适用的网络安全标准的信息。
注 6 断章上下文的组件开发（见 6.4.5）可以基于假设的（通用）项目的定义和项目内组件功能的描述。
应描述与网络安全相关的项目的操作环境的信息。

注 7 对操作环境的描述及其与项目的交互作用可以帮助识别和/或分析相关的威胁场景和攻击路径。

注 8 相关信息可以包括假设，例如，假设该项目所依赖的每个公钥基础设施证书颁发机构都得到了适当的管理。

9.3.3 工作产品

项目定义，由 9.3.2 的要求产生

9.4 网络安全目标

9.4.1 输入

9.4.1.1 先决条件

应提供以下信息：

-项目定义[WP-09-01]。

9.4.1.2 进一步支持信息

可以考虑以下信息：

-网络安全事件。

9.4.2 要求和建议

应执行根据项目定义进行的分析，包括：

a) 根据第 15.3 条规定进行的资产标识：

b) 根据第 15.4 条规定进行的威胁情景识别：
c) 符合第 15.5 条规定的冲击等级：
d) 根据 15.6 标准进行的攻击路径分析：
e) 根据第 15.7 条规定的攻击可行性等级；以及
f) 根据 15.8 确定风险价值。

注 1 如果项目定义没有为分析提供足够的信息，则可以假定这类信息。

根据 RQ-09-03]的结果，应根据 159 确定每个威胁情景的风险治疗方案

注 2 通过删除风险源来避免风险，可能会导致项目根据变更而进行的变更管理（见 5.4.4）。

如果威胁情景的风险处理决策包括降低风险，则应指定一个或多个相应的网络安全目标。

注 3 网络安全目标是一种保护资产免受威胁场景影响的要求。
注 4 如果适用，可确定网络安全目标的 CAL（见附件 E）。

注 5 可以为项目的任何生命周期阶段指定网络安全目标。

如果威胁情景的风险治疗决策包括：

a) 分享风险；或

b) 由于分析过程中使用的一个或多个假设而保留的风险，

然后，应指定一个或多个相应的网络安全索赔。

注 6 网络安全索赔可以考虑进行网络安全监控。

应进行验证，以确认：

a) RQ-09-03]关于项目定义结果的正确性和完整性；

b) 结果的风险治疗决策的完整性、正确性和一致性；

c) 的网络安全目标和 RQ-09-04]关于风险处理决策的网络安全声明的完整性、正确性和一致性；以及
d) 该项的所有网络安全目标与该项的网络安全声明的一致性。

9.4.3 工作产品 TARA，由 RQ 和 RQ-09-04]产生

网络安全目标，源自[RQ-09 月 05 日]

网络安全索赔，源自[RQ-09-06]

关于网络安全目标的验证报告

9.5 网络安全概念

9.5.1 输入

9.5.1.1 先决条件

应提供以下信息：

项目定义[WP-09-01]；

-网络安全目标；以及

-网络安全索赔。

9.5.1.2 进一步支持信息

可以考虑以下信息：

—TARA[WP-09-02]。

9.5.2 要求和建议

应描述实现网络安全目标的网络安全技术和/或操作网络安全控制及其交互，并考虑到：

a) 项目功能之间的依赖关系
b) 网络安全索赔。

注 1 该描述可包括：

— 实现网络安全目标的条件，例如防止妥协，发现和监测妥协，
— 专门用于解决威胁场景的特定方面的功能，例如使用安全通信信道。

注 2 该描述可用于评估设计和确定网络安全验证的目标。

[RQ-09-09]应根据[RQ-09-08]的描述，定义项目的网络安全要求和对运营环境的要求。

注 3 网络安全要求可以取决于或包括项目的特定功能，如更新
能力或在操作期间获得用户同意的能力。

注 4 对操作环境的要求在项目外实现，但它们包含在项目的网络安全验证中，以确认是否实现了相应的网络安全目标。

注 5 作为操作环境的一部分，对其他项目的要求可以是对这些项目的网络安全要求。
网络安全要求应分配给该项目，如果适用于其一个或多个组件。

注 6 对网络安全控制的描述补充了网络安全需求和操作环境需求的规范和分配，这些需求共同构成了网络安全的概念。

对 RQ0908、RQ0909 和 RQ0910]的结果应进行验证以确认：

a) 关于网络安全目标的完整性、正确性和一致性；以及

b) 与网络安全声明有关的一致性。

9.5.3 工作产品

网络安全概念，由 0908、0909 和 0910]产生

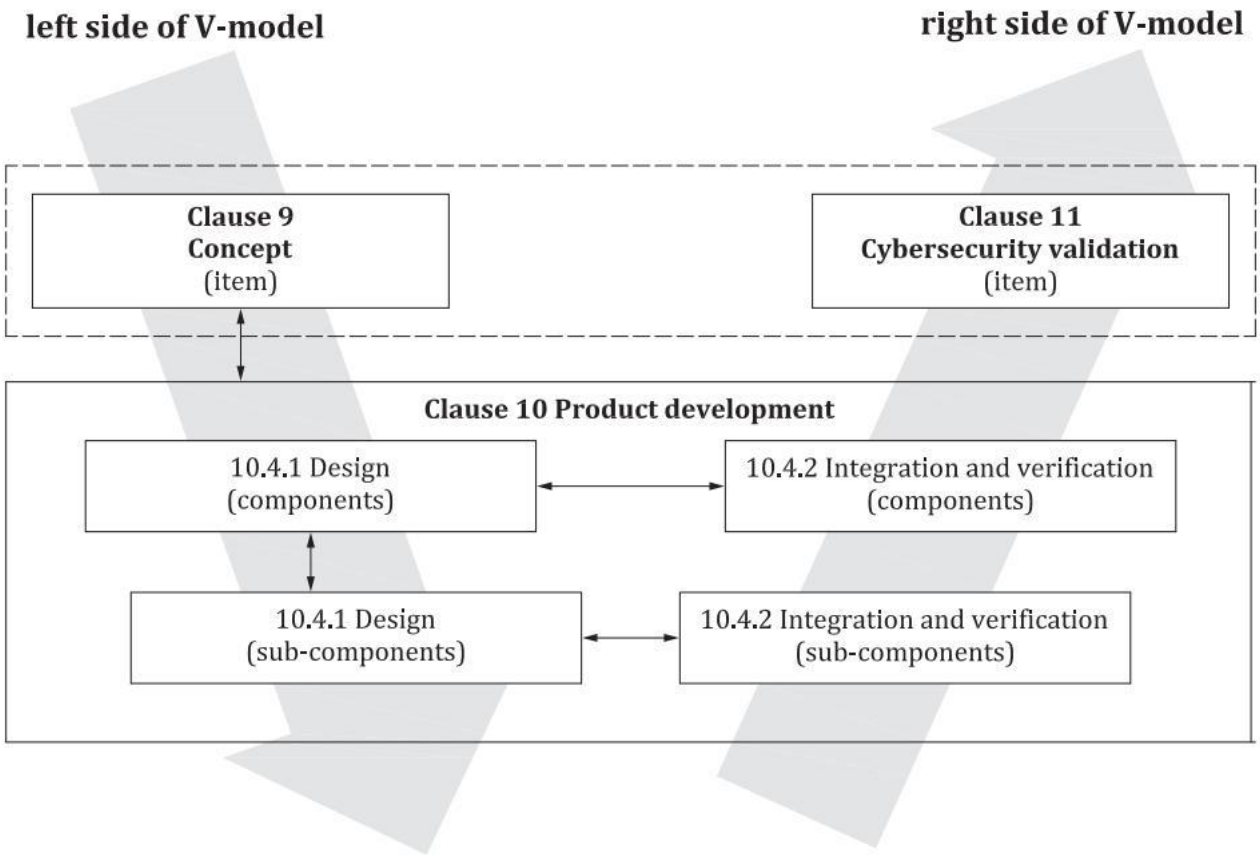
关于网络安全概念的验证报告

10 产品开发

10.1 一般来说

本条款描述了网络安全要求和体系结构设计的规范（见 10.4.1）。
此外，本条款还描述了集成和验证活动（请参见 10.4.2）。

这些网络安全活动将迭代执行，直到不需要进一步改进网络安全控制。网络安全规范的定义是通过验证活动来定义和确认，以实现网络安全概念。
图 9 说明了一个如何将产品开发活动应用于基于 v 模型的工作流程的示例，其中 1041 对应于 v 模型的左侧，1042 对应于右侧。在本例中，假设项目级别下有两层抽象，即组件级别和子组件层。此工作流可以扩展到覆盖任何级别的抽象。



*如 1041 中所述的设计过程中的架构抽象级别。
水平双向箭头描述了根据 10.4.2 中所述的网络安全规范对已实现和集成组件的验证。

图 9-V 型模型中的产品开发活动的示例

可以应用不同于 v 模型的开发方法或方法（例如，敏捷软件开发）。
CAL 可用于衡量本条款中活动的深度和严谨性，以及它们所使用的方法（见附件 E）。

10.2 目标

本条款的目的是：

a) 定义网络安全规范；

注 1 这些可以包括现有体系结构设计中不存在的网络安全相关组件的规范。

b) 验证定义的网络安全规范符合更高级的架构抽象网络安全规范；

c) 识别组件中的弱点；以及
注 2 第 8 条描述了漏洞分析和管理。

d) 提供了证明组件的实现和集成的结果符合网络安全规范的证据。

10.3 输入

10.3.1 先决条件

应提供以下信息：

— 来自更高级的体系结构抽象层次的网络安全规范；

注 1：这可能仅限于与正在开发的组件相关的信息，例如。

— 分配给正在开发的组件的网络安全要求；

— 正在开发的组件的外部接口规范；
— 关于正在开发的组件的操作环境的信息。

注 2 对于最高级别架构抽象的开发，使用项目的网络安全概念[WP09-06]和项目定义[WP-09-01]，而不是来自高级架构抽象的网络安全规范。

10.3.2 进一步支持信息

可以考虑以下信息：

项目定义[WP-09-01]；

— 网络安全概念；

— 现有建筑设计；

— 已经建立好的网络安全控制系统；
— 来自可重用组件的已知弱点和漏洞。

10.4 要求和建议

10.4.1 设计

网络安全规范应根据以下原则进行定义：

a) 来自更高层次的体系结构抽象化的网络安全规范；

b) 选择要实施的、如适用的网络安全控制；以及

示例 1 使用带有嵌入式硬件信任锚的单独微控制器用于安全密钥存储功能，并与非安全外部连接的信任锚隔离。
注 1 网络安全控制可以从受信任的目录中选择。

c) 现有的建筑设计，如果适用。

注 2 网络安全规范包括与满足已定义的网络安全需求相关的已定义架构设计的子组件之间的接口规范，包括它们的使用、静态和动态方面。

注 3 在定义网络安全规范时，可以考虑开发后阶段的网络安全影响，例如对密钥存储的安全管理；调试接口的停止激活；删除个人身份信息的程序。

注 4 网络安全规范可包括识别与满足网络安全要求相关的配置和校准参数，以及其设置或允许的值范围，例如，硬件安全模块集成的正确配置。

注 5 可以考虑实现网络安全控制所需的组件的能力，例如处理器性能、内存资源。
所定义的网络安全要求应分配给架构设计的组成部分。

如果适用，[RQ-10-03]应规定确保组件开发后的网络安全的程序。
示例 2 正确集成和初始化网络安全控制，以及在整个生产过程中维护网络安全的程序。

[RQ-10-04]如果网络安全规范或其实现使用了设计、建模或编程符号或语言，则在选择该符号或语言时应考虑以下事项：

a) 在语法和语义中有明确和可理解的定义；

b) 支持模块化、抽象和封装的实现；

c) 支持使用结构化结构；

d) 支持使用安全的设计和实施技术；

e) 能够集成已存在的组件；以及

示例 3　　用另一种语言编写的库、框架、软件组件。

f) 该语言对由于使用不当而产生的漏洞的弹性。

示例 4 对缓冲区溢出的弹性。

注 6 对于软件开发，实现包括使用编程语言进行编码。

[RQ-10-05]标准（参见[RQ-10-04]]针对网络安全的合适设计、建模或编程语言应由设计、建模和编码指南或开发环境涵盖。

示例 5 使用 MISRAC：2012M1 或 CERTC 用“C”编程语言进行安全编码。

示例 6 适合的设计、建模和编程语言的标准：

— 语言子集的使用；

— 强打字技术的执行

— 使用防御性实施技术。

应采用已建立的和值得信赖的设计和实施原则，以避免或尽量减少弱点的引入。

注 7 网络安全建筑设计的设计原则示例见 NIST 特别出版物 800-160Voll*]，附录 F.1。

应分析 RQ-10-01]中定义的建筑设计，以确定其弱点。

注 8 可以考虑来自重用组件的已知弱点和漏洞。

注 9 对已识别的弱点进行漏洞分析（见 8.5），并对已识别的漏洞进行管理（见 8.6）。但是，已识别出的弱点可以通过更改架构设计来解决，而无需执行漏洞分析。

[RQ-10-08]应验证已定义的网络安全规范，以确保来自高级架构抽象的网络安全规范的完整性、正确性和一致性。

注 10：验证方法可包括：

—review;

—analysis;

—simulation; and/or

—prototyping.

10.4.2 集成和验证

集成和验证活动应验证组件的实现和集成是否符合已定义的网络安全规范。

[RQ-10-09]的集成和验证活动应考虑：

a) 已定义的网络安全规范；

b) 适用于系列生产的配置，如果适用；

c) 有足够的能力来支持已定义的网络安全规范中指定的功能；以及

d) 如果适用，符合 RQ-10-05]的建模、设计和编码指南。

注 1 这可以包括车辆集成和验证。

注 2：进行验证的方法可包括：

-基于要求的测试；

-接口测试；

— 资源使用评估；

— 控制流程和数据流的验证；

— 动态分析；和/或
-静态分析。

注 3 如果采用测试验证，可选择测试用例和测试环境，并考虑：

— 可进行测试的集成水平，以达到验证目标；

— 在后续的集成活动中，需要根据对所选的测试环境的分析进行其他测试，例如，与处理器仿真或开发环境相比，目标处理器的数据字和地址字的位宽不同。

注 4：推导测试用例的方法可包括：

— 要求分析；

— 等价类的生成和分析；

— 边界值分析；和/或

— 根据知识或经验进行错误猜测。

如果采用测试验证，应使用定义的测试覆盖度量对测试覆盖率进行评估，以确定测试活动的充分性。
注 5 标准测试覆盖指标可能不足以满足网络安全，例如软件的语句覆盖。

应进行测试，以确认组件中剩余的未知弱点和漏洞已被最小化。

注 6 不必要的功能可能包含一个弱点。

注 7：测试方法可包括：

-功能测试；

-漏洞扫描；

— fuzz 测试；和/或
-渗透测试。
注 8 对确定的弱点进行漏洞分析（见 8.5），并对确定的漏洞进行管理（见 8.6）。但是，已识别出的弱点可以通过更改架构设计来解决，而无需执行漏洞分析。
如果没有按照[RC-10-12]进行测试，则应提供理论依据。

注 9：其基本原理可包括以下注意事项：

— 进入组件攻击面的可行性；
— ）（直接或间接地访问组件的能力；和/或
— 组件的简单性。

10.5 工作产品

网络安全规范，来自 1001 和 1002 的网络安全规范

开发后的网络安全要求

如果适用，由[RQ-10-04]和[RQ-10-05]产生的建模、设计或编程语言和编码指南的文件

由[RQ-10-08]得出的网络安全规范的验证报告

如果适用的话，在产品开发期间由和 RC10-12 造成的弱点

集成和验证规范，源自
集成和验证报告、RQ-10 和 RC-1012 产生的集成和验证报告

11 网络安全验证

11.1 一般来说

本条款描述了该项目在车辆级别进行网络安全验证的活动（见图 9）。该项目包括在车辆层面的操作环境和系列生产的配置。

11.2 目标

本条款的目的是：

a) 验证网络安全目标和网络安全主张；

b) 确认项目达到网络安全目标；

c) 确认仍不存在不合理的风险。

11.3 输入

11.3.1 先决条件

应提供以下信息：

项目定义[WP-09-01]；

— 网络安全目标；以及

— 网络安全索赔，如果适用的话。

11.3.2 进一步支持信息

可以考虑以下信息：

— 网络安全概念；
— 产品开发中的工作产品（见 10.5）。

11.4 要求和建议

考虑到系列生产配置的项目的车辆一级的验证活动应确认：

a) 网络安全目标符合威胁场景的网络安全目标和相应的风险；
注 1 如果在验证过程中发现了网络安全目标没有解决的任何风险，它们可以按照 9 进行解决±4.

b) 实现本项目的网络安全目标；

c) 网络安全索赔的有效性；以及

d) 对操作环境的要求的有效性，如果适用。

注 2：验证活动可包括：
— 通过审查第 23 条和第 10 条的工作产品，确认网络安全目标的实现；

— 渗透测试，以证明网络安全目标的充分性和实现性；和/或
— 审查通过第 9 条和第 10 条确定的所有管理风险。

注 3CAL 可用于测量渗透试验的深度和严密度（见附件 E）。
注 4：对[RQ-11-01]验证活动中发现的漏洞进行漏洞分析（见 8.5），并对识别出的漏洞进行管理（见 8.6）。
应提供选择验证活动的理由。

11.5 工作产品

验证报告，由 RQ11 月 01 日和 11 月 02 日得出的结果

12 生产

12.1 一般来说

生产包括一个项目或部件的制造和组装，包括车辆水平。创建一个生产控制计划，以确保后开发的网络安

全要求应用于项目或组件，并确保在生产过程中不会引入漏洞。

12.2 目标
本条款的目的是：

a) 在开发后应用网络安全要求；
b) 防止在生产过程中引入漏洞。

12.3 输入

12.3.1 先决条件
应提供以下信息：

— 开发后报告；

— 开发后的网络安全要求。

12.3.2 进一步支持信息
没有。

12.4 要求和建议
应制定一个生产控制计划，适用于开发后的网络安全要求。
注 1 生产控制计划可作为整体生产计划的一部分纳入。
生产控制计划应包括：

a) 将网络安全要求应用于开发后的阶段的步骤序列；

b) 生产工具和设备；

c) 网络安全控制，防止生产过程中未经授权的变更；

示例 1 阻止物理访问持有软件的生产服务器的物理控件。

示例 2 应用加密技术和/或访问控制的逻辑控件。

d) 确认满足网络开发安全要求的方法。

注 2：方法可包括检查和校准检查。

注 3 要制造项目或组件并安装硬件和软件，生产过程可以使用特权访问权限。如果在生产后以未经授权的方式使用，这种访问可能会在项目或组件中引入漏洞。
应实施生产控制计划。

12.5 工作产品

生产控制计划，由 RQ 和 RQ12 所产生的生产控制计划

13 操作和维护

13.1 一般来说
本条款描述了对字段中的项目或组件的网络安全事件响应（参见 13.3）和更新（参见 13.4）。
当组织将其作为漏洞管理的一部分调用时，就会发生网络安全事件响应（请参见 8.6）。
更新是在开发后对项目或组件所做的更改，可以包括其他信息，如技术规范、集成手册、用户手册。组织可以因为各种原因发布更新，例如解决漏洞或安全问题，提供功能改进。有关更新的工作产品被记录为其他条款的工作产品。
在概念、产品开发或生产阶段的项目或组件的修改包括变更管理（见 5.4.4），而不是本条款。

13.2 目标

本条款的目的是：

a) 确定并实施针对网络安全事件的补救措施；以及
b) 在生产后更新项目或组件期间和之后维护网络安全，直到其网络安全支持结束。

13.3 网络安全事件响应

13.3.1 输入

13.3.1.1 先决条件

没有。

13.3.1.2 进一步支持信息

可以考虑以下信息：
-与导致网络安全事件响应的漏洞相关的网络安全信息；

-漏洞分析。

13.3.2 要求和建议

对于每一个网络安全事件，都应创建一个网络安全事件响应计划，其中包括：

a) 补救措施；
注 1 补救措施由 8.6 中的漏洞管理决定。

b) 沟通计划；

注 2 沟通计划的创建可能涉及内部利益相关方，例如市场营销或公共关系、产品开发团队、法律、客户关系、质量管理、采购。

注 3A 沟通计划可以包括识别内部和外部沟通伙伴（例如，开发、研究人员、一般公众、当局），以及为这些受众开发具体信息。

c) 指定的补救行动的责任；
注 4：各项责任人员可以拥有：

— 在受影响的项目或组件方面的专业知识，包括遗留的项目和组件；

— 组织知识（例如，业务流程、沟通、采购、法律）；和/或
— 决策权。

d) 记录与网络安全事件相关的新网络安全信息的程序；
注 5 可根据 8.3 收集新的网络安全信息，例如以下信息：

— 受影响的组件；

— 相关事件和漏洞；

— 法医数据，如数据日志， 碰撞传感器数据；和/或
— 最终用户投诉。

e) 一种确定进度的方法；

样例 进度措施如下：

— 被修正的受影响项目或组件的百分比
— 受补救措施影响的项目或组件的百分比。

f) 关闭网络安全事件响应的标准；以及

g) 关闭的操作。
应实施网络安全事件响应计划。

13.3.3 工作产品

网络安全事件响应计划，由

13.4 更新

13.4.1 输入

13.4.1.1 先决条件
应提供以下信息：

— 开发后报告。

13.4.1.2 进一步支持信息
可以考虑以下信息：

— 网络安全事件响应计划；

— 与更新相关的后开发方面的网络安全要求。

13.4.2 要求和建议
车辆内与更新和更新相关的能力应根据本文件进行开发。

13.4.3 工作产品
没有。

14 结束网络安全支持和退役

14.1 一般来说

退役不同于网络安全支持。组织可以结束对项目或组件的网络安全支持，但该项目或组件仍然可以按照该领域中的设计运行。网络安全支持的退役和结束都可能带来网络安全的影响，但这些影响是单独考虑的。

退役可以在组织不知情的情况下发生，因此不能强制执行退役程序，因此退役行为超出了本文件的范围。在概念和产品开发阶段，将考虑结束网络安全支持和退役。

14.2 目标
本条款的目的是：

a) 沟通网络安全支持的终结；以及
b) 使与网络安全有关的项目和组件能够退役。

14.3 网络安全支持结束

14.3.1 输入
没有。

14.3.2 要求和建议
当一个组织决定终止对某个项目或组件的网络安全支持时，应创建一个程序来与客户进行沟通。
注 1 这些通信可以在供应商和客户之间的合同要求下处理。
注 2 可通过公告的方式与车主进行沟通。

14.3.3 工作产品
负责对网络安全支持的终端进行沟通的程序

14.4 解码

14.4.1 输入

14.4.1.1 先决条件
应提供以下信息：

— 开发后的网络安全要求。

14.4.1.2 进一步支持信息
没有。

14.4.2 要求和建议
应提供关于退役的后开发的网络安全要求。
注意：与此类要求相关的适当文件(例如说明、用户手册]可以使网络安全能够退役。

14.4.3 工作产品
没有。

15.威胁分析和风险评估方法

15.1 一般来说
本条款描述了确定道路用户可能受到威胁场景的影响程度的方法。这些方法及其工作产品统称为威胁分析和风险评估(TARA)，并从受影响的道路使用者的角度来执行。本子句中定义的方法是可以系统地调用的通用模块，从项目或组件生命周期中的任何时间点开始：

-资产识别（见 15.31：

— 威胁情景识别（见 15.4）：
-冲击等级（见 15.51：
— 攻击路径分析（见 15.61：

— 攻击可行性等级（见 15.71：
— 风险价值确定（见 15.81：和
— 风险治疗决策（见 15.9）。
因为这些都是通用模块，所以本子句中定义的工作产品被记录为其他子句生产的工作产品的一部分。
通过实例说明这些方法，请见附件 H。

可以应用影响评级、攻击可行性评级和风险值确定的组织特定量表，并映射到本文档中定义的相应量表。

15.2 目标
本条款的目的是：

a) 识别资产、其网络安全属性及其损害情况；

b) 识别威胁场景；

c) 确定损坏场景的影响等级；

d) 识别能够实现威胁场景的攻击路径；

e) 确定利用攻击路径的容易程度；

f) 确定威胁情景的风险值；以及
g) 为威胁场景选择适当的风险治疗方案。

15.3 资产识别

15.3.1 输入

15.3.1.1 先决条件
应提供以下信息：

-项目定义[WP-09-01]。

15.3.1.2 进一步支持信息
可以考虑以下信息：

-网络安全规范。

15.3.2 要求和建议

应确定损坏情况。
注 1A 损坏情况可能包括：

— 项目的功能与不良后果之间的关系；

— 对道路使用者造成伤害的描述
— 相关资产。

应识别具有网络安全属性的资产，其妥协会导致损害的情况。

注 2 资产的识别可依据：

— 分析项目定义；

— 执行影响评级；

— 从威胁情景中获取资产的方法

— 使用预定义的目录。

例如 1 该资产是存储在信息娱乐系统中的个人信息(客户个人偏好]，其网络安全属性为保密性。损害情况是由于失去保密性而未经客户同意而泄露个人信息。
实例 2 该资产是制动功能的数据通信，其网络安全特性是完整性。损坏情况是与车辆在高速行驶时意外完全制动造成的后续车辆发生碰撞（追尾碰撞）。

15.3.3 工作产品

由 RQ-15-01]造成的损害情况

具有网络安全属性的资产，由

15.4 威胁场景识别

15.4.1 输入

15.4.1.1 先决条件
应提供以下内容：

-项目定义[WP-09-01]。

15.4.1.2 进一步支持信息

可以考虑以下信息：

-网络安全规范；

-损伤情况[WP-15-01]；

— 具有网络安全属性的资产。

15.4.2 要求和建议

应确定威胁情景，并包括：

目标资产；

— 损害了该资产的网络安全财产；以及
— 造成网络安全财产妥协的原因。

注 1 进一步的信息可以包括或与威胁场景相关联，例如损坏场景、资产、攻击者、方法、工具和攻击表面之间的技术相互依赖性。

注 2 威胁场景识别的方法可使用小组讨论和/或系统的方法，例如：

— 引起合理可预见的滥用和/或滥用导致的恶意使用案例；
— 基于 evita 等框架的威胁建模方法[201，TVRA[2[1]]，意大利面[22]，大步(欺骗，篡改，否认，信息披露，拒绝服务，提高特权]。

注 3A 损伤场景可能对应于多个威胁场景，而一个威胁场景可能导致多个损伤场景。
例如，为制动 ECU 欺骗 CAN 消息会导致 CAN 消息的完整性丧失，从而失去制动功能的完整性。

15.4.3 工作产品

由 RQ-15-03]产生的威胁情景

15.5 影响等级

15.5.1 输入

15.5.1.1 先决条件

应提供以下内容：

-损伤情况[WP-15-01]。

15.5.1.2 进一步支持信息

可以考虑以下信息：

项目定义[WP-09-01]；

— 具有网络安全属性的资产。

15.5.2 要求和建议

[RQ-15-04]损害情况应分别针对安全、财务、运营和隐私等影响类别（S、F、O、P）对道路使用者造成的潜在不利后果进行评估。

注 1 本文档不提供不同影响类别之间的关系（例如，权重）。
注 2 可以考虑其他的影响类别。
注 3 如果考虑了其他影响类别，则可根据第 7 条的规定在供应链中共享这些类别的基本原理和解释。

应确定每个影响类别的损坏场景的影响等级为以下因素之一：

—severe；

—major；

-中度；或
—negligible.
注 4 与财务、运营和隐私相关的影响可以根据附件 F 中的表进行评级。

与安全相关的影响等级应来自 ISO26262-3：2018,6.4.3。
注 5　　附件 F 中的表 F.1 可用于绘制安全影响标准和影响等级。

注 6.功能安全评估可重复用于此目的。
[PM-15-07]如果一个损害场景导致了一个影响评级，并且可以认为另一个影响类别的每个影响都不那么关键，那么可以省略对该其他影响类别的进一步分析。
例如，损坏场景的安全影响被评为“严重”，因此没有进一步分析该损坏场景的财务影响。

15.5.3　工作产品

与相关影响类别相关的影响评级，由 RQ15 至 06 得出的影响评级

15.6　攻击路径分析

15.6.1　输入

15.6.1.1　先决条件
应提供以下信息：

-项目定义[WP-09-01]或网络安全规范]；以及

注意：如果对项目执行攻击路径分析，则使用项目定义，如果在组件上执行攻击路径分析，则使用网络安全规范。

-威胁场景[WP-15-03]。

15.6.1.2　进一步支持信息
可以考虑以下信息：

— 网络安全事件造成的弱点；

— 在产品开发过程中发现的弱点；

-建筑设计；

— 先前确定的攻击路径，WP-15-05]，如果可用；

-漏洞分析。

15.6.2　　要求和建议
应分析威胁情景，以识别攻击路径。
注 1 攻击路径分析可以基于：
— 通过分析实现威胁场景的不同方法，推断自上而下的攻击路径，例如攻击树、攻击图；和/或

— 从识别出的漏洞中构建攻击路径的自下而上的方法。
注 2 如果部分攻击路径不能导致实现威胁场景，则可以停止对该部分攻击路径的分析。

攻击路径应与攻击路径可以实现的威胁场景相关联。

注 3 在产品开发的早期阶段，攻击路径往往不完整或不精确，因为具体的实现细节还无法识别特定的漏洞。在产品开发过程中，随着更多信息可用，攻击路径可以更新，例如在漏洞分析之后。

样例
— 威胁场景：欺骗制动 ECU 的 CAN 消息会导致 CAN 消息的完整性丧失，从而导致制动功能的完整性丧失。

— 实现上述威胁场景的攻击路径：

i. 远程信息通信 ECU 通过蜂窝接口中断；

ii. 网关 ECU 通过远程通信 ECU 的 CAN 通信中断；

iii. 网关 ECU 转发恶意制动请求信号（不必要的快速减速）。

15.6.3 工作产品

攻击路径，由 15 和 05 产生的攻击路径

15.7 攻击可行性评级

15.7.1 输入

15.7.1.1 先决条件

应提供以下信息：

— 攻击路径[WP-15-05]。

15.7.1.2 进一步支持信息

可以考虑以下信息：

-建筑设计；

-漏洞分析。

15.7.2 要求和建议

对于每个攻击路径，攻击可行性等级应按照表 1 所述确定。

表 1-攻击的可行性等级和各自的说明

攻击可行性评级	描述
高	攻击路径可以通过低努力完成。
介质	攻击路径可以通过中等程度的努力来完成。
低	攻击路径可以通过高努力完成。
非常低	攻击路径可以通过非常高的努力来完成。

攻击可行性评级方法应根据以下方法之一进行定义：

a) 攻击潜在的方法；

b) 基于 CVSS 的方法；或

c) 基于攻击向量的方法。

注 1 该方法的选择可能取决于生命周期中的阶段和可用信息。

如果使用基于攻击潜力的方法，应根据核心因素确定攻击可行性等级，包括：

a) 经过的时间；

b) 专业知识；

c) 有关该项目或零部件的知识；

d) 机会之窗；和

e) 设备。

注 2 核心攻击的潜在因素可以从 ISO/IEC18045 中得出

注 3 $G_{\pm}2$ 提供了基于攻击潜力来确定攻击可行性的指导方针。

如果使用基于 CVSS 的方法，应根据基本度量组的可利用性指标来确定攻击的可行性评级，包括：

a) 攻击向量；

b) 攻击复杂性；

c) 所需的特权；和
d) 用户交互。
注 4 G.3 提供了关于基于基于 CVSS 的方法确定攻击可行性的指南。
如果使用基于攻击向量的方法,应基于评估主要的攻击向量来确定攻击的可行性评级(cf。CVSS[24]2.1.1)的攻击路径。
注 5 G±4 提供了基于基于攻击向量的方法来确定攻击可行性的指导方针。

注 6 在开发的早期阶段（例如概念阶段），当没有足够的信息时
识别特定的攻击路径，一种基于攻击向量的方法可以用于估计攻击的可行性。

15.7.3 工作产品

由 RQ-15-10]得出的攻击可行性评级

15.8 风险价值的确定

15.8.1 输入

15.8.1.1 先决条件
应提供以下信息：

威胁场景[WP-15-03]；

— 具有相关影响类别的影响评级；以及

-攻击的可行性等级。

15.8.1.2 进一步支持信息
没有。

15.8.2 要求和建议
对于每个威胁情景，风险值应从相关损伤情景的影响和相关攻击路径的攻击可行性来确定。
注 1 如果威胁场景对应于多个损害场景和/或相关损害场景在多个影响类别中存在影响,则可以为每个影响评级分别确定一个单独的风险值。

注 2 如果威胁场景对应于多个攻击路径，则可以适当地聚合相关的攻击可行性评级，例如，为威胁场景分配了相应攻击路径的攻击可行性评级的最大值。
威胁情景的风险值应为（包括）1 和 5 之间，其中值为 1 代表最小风险。

风险值的确定方法：

风险矩阵；
-风险公式。

15.8.3 工作产品

风险值 1515 和 1516 产生的风险值

15.9 风险治疗决策

15.9.1 输入

15.9.1.1 先决条件
应提供以下信息：

项目定义[WP-09-01]；

-威胁情景，以及

风险值[WP-15-07]。

15.9.1.2 进一步支持信息

可以考虑以下信息：

-网络安全规范；

— 项目或组件，或类似项目或组件的先前风险处理决定；

— 具有相关影响类别的影响等级；

攻击路径[WP-15-05]；

-攻击的可行性等级。

15.9.2 要求和建议

对于每个威胁情景，考虑到其风险值，应确定以下一种或多种风险治疗方案(s)：

a) 避免风险；
例如 1 通过消除风险源，决定不开始或继续进行导致风险的活动来避免风险。

b) 降低风险；

c) 分享风险；

示例 2 通过合同分担风险或通过购买保险转移风险。

d) 保留风险。

注意：保留风险和分担风险的理由被记录为网络安全声明，并根据第 8 条进行网络安全监控和漏洞管理。

15.9.3 工作产品

风险治疗的决定

NexA
（信息）

网络安全活动和工作产品的总结

A.1 一般

表 A.1 总结了网络安全活动及其相应的工作产品。这可以帮助组织管理这些活动，确保网络安全活动的覆盖范围，并了解项目的潜在工作量。概念和产品开发阶段的活动在网络安全计划中定义。因此，这些活动的工作产品都在网络安全评估的范围内。第 15 条中列出的所有工作产品在其他条款中被记录为工作产品。

A.2 网络安全活动和工作产品概述

表 A.1-本文件的网络安全活动及工作产品

子条款	工作产品
组织网络安全管理	
5.4.1 网络安全治理	网络安全政策、规则和流程
5.4.2 网络安全文化	网络安全政策、规则和流程 能力管理、意识管理和持续改进的证据
5.4.3 信息共享	网络安全政策、规则和流程
5.4.4 管理系统	组织管理系统的证据
5.4.5 工具管理	工具管理的证据
546.信息安全管理	组织管理系统的证据
5.4.7 组织网络安全审计	组织网络安全审计报告
项目依赖性的网络安全管理	
641.网络安全责任	网络安全计划
642 网络安全规划	网络安全计划
643 尾矿	网络安全计划
644 重复使用	网络安全计划
645 组件上下文外	网络安全计划
646 现成组件	网络安全计划
647 网络安全案例	网络安全案例
648 网络安全评估	网络安全评估报告
649 发布后开发	开发后报告的发布
分布式网络安全活动	
741 供应商能力	没有
742 报价请求	没有
743.责任的调整	网络安全接口协议
持续的网络安全活动	

表 A.1（继续）

子条款	工作产品
8.3 网络安全监控	网络安全信息的来源 Trigers 网络安全事件
8.4 网络安全事件评估	网络安全事件的弱点
8.5 漏洞分析	漏洞分析
8.6 漏洞管理	被管理漏洞的证据
概念阶段	
9.3 项目定义	项目定义
9.4 网络安全目标	2002 年 9 月 9 日 网络安全目标 网络安全索赔 关于网络安全目标的验证报告
9.5 网络安全概念	网络安全概念 网络安全概念的验证报告
产品开发阶段	
1041 设计	网络安全规范 开发后的网络安全要求 建模、设计或编程语言和编码指南的文档 网络安全规范的验证报告 在产品开发过程中发现的弱点
1042.集成与验证	在产品开发过程中发现的弱点 集成和验证规范 集成和验证报告
第十一条网络安全验证	[WP-11-01]验证报告
开发后阶段	
第 12 条生产	生产控制计划
13.3 网络安全事件响应	网络安全事件响应计划
13.4 更新	没有
14.3 网络安全支持	沟通网络安全支持终端的程序
14.4 解码	没有
威胁分析与风险评估方法	
15.3 资产识别	[WP-15-01]损坏情况 具有网络安全属性的资产
15.4 威胁场景识别	[WP-15-03]威胁场景
15.5 影响等级	具有相关影响类别的影响评级
15.6 攻击路径分析	攻击路径
15.7 攻击可行性评级	攻击可行性评级
15.8 风险价值确定	[WP-15-07]风险值
15.9 风险治疗决策	风险治疗决策

附件 B
（信息）

网络安全文化的例子

表 B.1 提供了弱网络安全文化的例子。

表 B.1 网络安全文化的例子

表明网络安全文化薄弱的例子	表明一个强大的网络安全文化的例子
对与网络安全相关的决策的责任是无法追踪的。	该过程确保了对与网络安全相关的决策的问责制是可追溯的。
性能（已实现的功能或特性）、成本或进度优先于网络安全。	网络安全和安全处于最高优先位。
奖励系统有利于成本和时间表，而不是网络安全。	奖励系统支持并激励网络安全的有效实现，并惩罚那些采取危及网络安全的捷径的人。
网络安全人员在不考虑项目/活动的具体需求的情况下，强制不适当和非常严格地遵守网络安全。	网络安全人员作为具有适当性和实际实施意识的榜样，导致整个组织对其行动的信任。
评估网络安全及其管理流程的人员会受到负责执行流程的人员的过度影响。	该过程提供了充分的制衡，例如在网络安全评估中具有适当的独立程度。
对网络安全的被动态度，例如。： — 严重依赖于开发结束时的测试； — 未为现场潜在的弱点或事件做好准备； — 管理层只有在生产中出现网络安全事件或媒体大量关注竞争对手产品时，才会做出反应。	对网络安全的积极态度。： — 网络安全问题从产品生命周期的最早阶段就被发现和解决（通过设计的网络安全）； — 该组织准备对现场的漏洞或事件做出快速反应。
没有分配网络安全所需的资源。	已分配了网络安全所需的资源。 熟练的资源具有与所分配的活动相称的能力。

表 B.1（继续）

表明网络安全文化薄弱的例子	表明一个强大的网络安全文化的例子
—“集团认为“确认偏差(即不关键” 接受或符合主流观点）。 —“堆放甲板”(即选择成员以确保 当形成审查小组时 防止潜在的异议。 -持异议者被排斥或被贴上“不是团队”的标签 “玩家”（例如不合作、不妥协、有毒人员）。 -异议会对表现产生负面影响 审查。 -少数民族持不同意见者被贴上标签或被视为 a “麻烦制造者”，“不是团队球员”或“哨子” “鼓风机”（即搅拌器，不可取的或告密者）。 -表达担忧的员工会担心 反应。	该过程利用多样性的优势： -寻求知识多样性、有价值和知识多样性 集成在所有过程中； -对抗多样性使用的行为是 不鼓励和惩罚。 具有支持性的沟通和决策能力 漏斗存在，管理层鼓励其使用： -鼓励进行自我表露； -任何人负责披露(内部或 鼓励外部因素存在潜在的脆弱性； -发现和解决过程继续进行 该领域，在制造和发展中 其他产品。
没有系统的持续改进过程，学习周期或其他形式的经验教训学习。	持续改进是所有过程不可或缺的部分。
进程是特殊的或隐式的。	我们将遵循已定义、可跟踪和受控制的过程。

附件 C
（信息）

网络安全接口协议模板的示例

CSUB1 通用

如果不同的组织参与了分布式网络安全活动，那么就不同组织之间的责任、信息披露水平和每个里程碑的成就水平达成一致是很重要的。

本附件提供了根据[RQ-07-04]规定的网络安全接口协议的示例模板。本模板提供了关于如何定义客户和供应商之间的分布式网络安全活动的角色和职责的指导(图 C.1)。
其他信息也可以添加到模板中，如联系点、目标里程碑、协作的方法或工具。

CSUB2 示例模板

此示例模板中的列条目包括：
a) 各阶段：本文件的各个阶段；
b) 工作产品：本文档中与分布式活动接口相关的工作产品；
c) 文件参考文件：本文件的相关条款；
d) 供应商：RASIC 规定的供应商责任；
e) 客户：由 RASIC 提供的客户责任；

注 1 该模板使用 RASIC 来演示组织之间特定工作产品的职责分配。RASIC 的使用方法如下：

— 负责开展活动的组织；

— 活动完成后有权批准活动的组织；

— 支持机构：将帮助负责该活动的组织的组织；

— 本人告知：了解活动进展和正在做出决定的组织；
— 咨询]：提供建议或指导但不积极开展活动的组织。
f) 保密级别：供应商和客户对各工作产品的保密性达成一致；以及

注 2：可能的保密级别可为：

— 高度机密：只有创建工作产品的组织才能访问它；

— 保密信息：客户和供应商均可以访问工作产品；

-与第三方保密：根据 5.4.3 与授权外部方共享：

公共：工作产品可以共享，没有任何限制。

g)评论：关于组织之间谈判和讨论结果的附加信息。

阶段	工作产品	博士参考	供应商					客户					保密水平	评论
			R	A	S	I	C	R	A	S	I	C		
概念	项目定义													
	治疗分析和风险评估													
	网络安全概念													
	网络安全概念验证报告													
产品开发	网络安全规范													
L——— ▮	-----	—								— - ,				

图 C.1-网络安全接口协议模板的示例

附件 D
（信息）

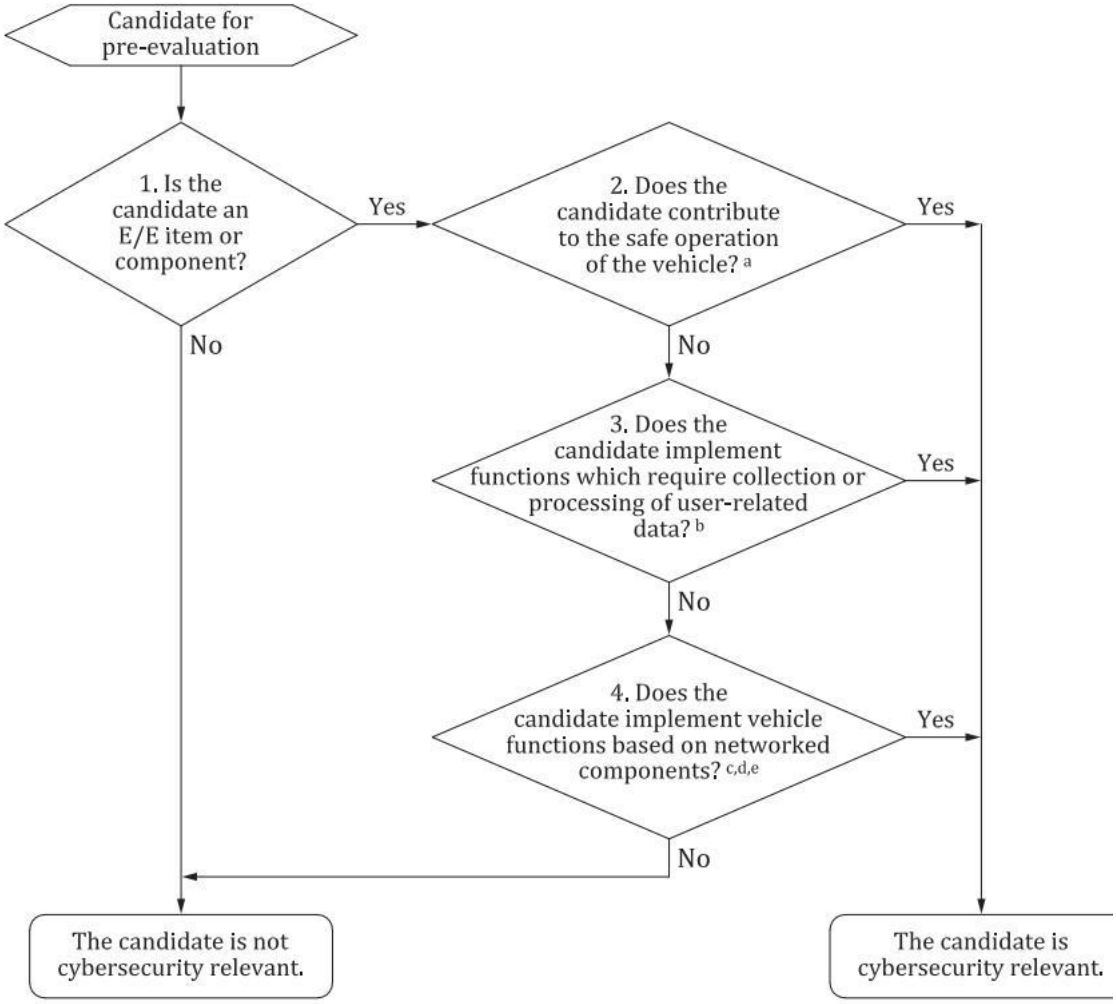
网络安全相关性-示例、方法和标准

DSUR1 通用

本附件提供了确定一个项目或组件是否与网络安全相关的示例方法（请参见[RQ-06-02]]。

DSUB2 方法

候选项目或组件的网络安全相关性可以使用图示例标准的 d.1 中的决策图来确定。



gnations.例如与司机或乘客相关的数据，或与潜在的敏感信息，例如位置数据。

例如内部连接——CAN、以太网、面向媒体的系统传输(MOST)、传输控制协议/互联网协议（TCP/IP）。

示例外部连接——到后端服务器的功能接口；蜂窝电信网络、机载诊断（OBD-II）接口。

样例　　无线连接的传感器或执行器-远程无钥匙入口(RKE)，近场通信(NFC)、轮胎压力监测系统(TPMS)。

图 D.1-网络安全相关性示例的方法和标准

网络安全的相关性也可以根据经验和多种专家的判断来确定，例如，涉及安全专家和网络安全专家。

附件 E
（信息）

网络安全保证级别

E.1 一般

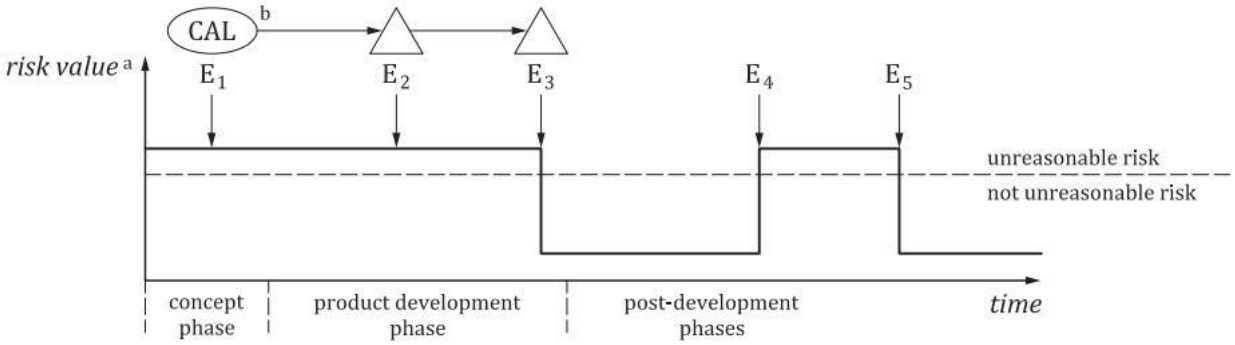
本附件描述了一种网络安全保证级别(CAL)分类方案，可用于指定和传达一套保证要求，以提供对项目或组件的资产保护得到充分发展的信心。该 CAL 分类方案没有指定网络安全控制的技术要求，但它可以用于驱动网络安全工程，为相关组织之间通信网络安全保证要求提供了一种通用语言。

CAL 可以由开发项目的组织确定，也可以由断章上下义开发组件的组织假设。

一旦确定，CAL 将指定后续产品开发活动中所需的严格性，以解决需要降低风险所需的威胁场景。这可以通过将 CAL 作为网络安全目标的属性来实现，该目标由改进的网络安全要求继承。

E.2 确定 CAL

CAL 与风险间接相关；然而，它不能直接从风险价值来确定。这是因为风险价值是动态的，随时间变化的项目或组件的规范、设计、实现和操作环境而变化，而 CAL 表示了随时间保持固定的保证水平。因此，在概念阶段的开发开始时，可以使用预计在网络安全支持结束之前保持稳定的参数，例如在考虑网络安全控制的实施之前，基于一个项目的资产及其相关风险的方面的参数。CAL 与相关风险之间的关系如图 e.1 所示。



Ei

E2 事件 2：实施网络安全控制。

E3 事件 3：测试显示网络安全控制有效。

E4

E5 事件 4：在该字段中发现了一些漏洞。事件 5：漏洞已被修复。

CAL。

CAL 被应用于网络安全活动中。

a 风险价值是动态的，可根据当前的规范、设计或实施而有所不同。

鉴于被保护资产的临界性，E1 确定的预期保证水平规定了 E？，E3 后续网络安全活动的严格性。

图 E.1-CAL 与风险之间的关系

可根据考虑到已确定的威胁场景来确定 CAL（见 15.4）。表 E.1 给出了一个基于四个 cal 的例子，每个 cal 对应于基于所使用的网络安全工程方法的保证水平。该示例显示了根据相关威胁场景的最大影响和攻击向量分配的呼叫器。

表 E.1-基于冲击和攻击矢量参数的 CAL 确定示例

		攻击向量 [b]			
		物理	**本地**	**相邻**	**网络**
影响	严重	cal2	cal3	卡尔 4	卡尔 4
	少校	cal1	cal2	cal3	卡尔 4
	中等	cal1	cal1	cal2	cal3
	不可避免的	___a	___a	___a	___a
请参阅 2008 年 6 月 6 日下午。 [b]攻击向量是攻击可行性的一个静态参数。					

在客户和供应商之间共享确定 CAL 的文档化基本原理可以增进相互理解。CAL 分类方案和确定的 CAL 也可以是客户和供应商之间的网络安全接口协议的一部分。

单个 CAL 可以分配给一个项目的所有网络安全目标，或者不同的 CAL 可以分配给每个网络安全目标。如果网络安全目标被合并，最高的个人呼叫将被分配给合并的网络安全目标。

ESBAR3 使用 CAL

E.3.1 一般考虑

CAL 分类方案可用于确定执行网络安全活动的严格程度，以满足提供所需保证所需的努力。

CAL 可用于选择：

a) 用于开发和验证的方法；

b) 识别弱点和分析漏洞的方法；以及
c) 网络安全评估的方法。
表 E.2 提供了一些 cal 的例子和关于在概念和产品开发阶段使用它们的指导。对于 CAL 的每一次增加，相应的方法都代表了通过设计、验证和网络安全评估对项目或组件的保证的显著增加。提供了表 E.2E.3 和 E4 中的示例，以便在使用 CALs 来扩展本文档中描述的活动时获得行业经验。

表 E.2-呼叫的示例数和网络安全保证的预期严格性措施

cal	描述	a)方法提供网络安全活动以适当严格执行的信心	使用 b)方法来提供对非托管漏洞不继续存在的信心	c)独立计划，以提供对网络安全活动是适当的信心
cal1	需要提供较低到中等程度的网络安全保证	基于需求的测试	基于已知信息搜索漏洞的分析和/或测试等活动	不需要
cal2	需要提供适度的网络安全保证			网络安全评估是由与发起者不同的人进行的
cal3	需要中到高的网络安全保证	我们测试了组件之间的所有相互作用	通过探索性方法对漏洞进行分析和/或测试等活动	网络安全评估是由一个不同于发起者的团队中的人进行的
卡尔 4	需要很高的网络安全保证	测试了组件之间相互作用的所有组合		网络安全评估由原始部门关于管理、资源和发布权限的独立人员进行

E.3.2 概念

本子条款提供了一个关于使用 CAL 分类方案来适应开发措施的严谨性和范围的示例。

在概念阶段，随着网络安全概念的定义和网络安全需求分配到初步架构的组件，CALs 可作为[RQ-09-10]的扩展：

a) 来自网络安全目标的网络安全要求继承了来自该网络安全目标的 CAL；

b) 如果将从多个网络安全目标中继承的具有不同 CAL 的多个网络安全要求分配给一个架构组件，则将最高的 CAL 分配给该组件；

c) 如果确认组件为不受体系结构中其他组件的保护，则根据基本原理，分配给组件的 CAL 可以减少或变得不必要。

E.3.3 产品开发

CAL 分类方案在产品开发中的一个应用可以是使用依赖于 CAL 的方法和度量。

在产品开发中，如果将网络安全要求分配给组件，并且无法确认与其他组件的隔离，则可以根据这些网络安全要求的最高 CAL 开发组件。
表 E.3 和 E4 提供了如何将 CAL 应用于网络安全活动示例的示例；进一步的网络安全活动也可以以类似的方式加以解决。
表 E.3 提供了一个如何使用 CAL 来确定执行各自活动的独立性级别的示例。

表 E.3-网络安全活动的独立性水平示例

活动	要求	独立性的程度适用于[a]				范围
		cal1	cal2	cal3	卡尔	
验证网络安全的概念和设计活动	[RQ-09-11]	I1	I1	I2	I2	适用于网络安全要求中最高的 CAL
验证组件的实现和集成的情况	[RQ-10-09]	I1	I1	I2	I2	
网络安全验证	[RQ-11-01	I1	I1	I2	I2	
网络安全评估	[RQ-06-27	—	I1	I2	I3	

a 这些符号的定义如下：

-：没有关于该活动的独立性的建议；
I1：该活动由不同的人就负责创建所考虑的工作产品的人来执行；
I2：活动是由独立于负责创建所考虑的工作成果的团队中的人员执行的），即由向不同的直接上级报告的人员报告；和
13：该活动由有关管理、资源和发布权限的独立人员执行，并由负责创建所考虑的工作产品的部门执行。

表 E.4 提供了一个示例，说明了如何使用 cal 来确定影响用于验证和验证的测试方法的严格性的参数。

表 E.4-测试方法的参数示例

活动	要求	测试参数适用于[a]				范围
		cal1	cal2	cal3	卡尔	
功能测试	[RC-10-12] [RQ-11-01]	T1	T1	T2	T2	适用于网络安全要求中最高的 CAL
漏洞扫描	[RC-10-12] [RQ-11-01]	T1	T1	T1	T1	
模糊测试	[RC-10-12] [RQ-11-01]	—	T1	T2	T2	
渗透试验	[RC-10-12] [RQ-11-01]	—	—	T1	T2	

[a]这些符号的定义如下：

-：没有关于此活动的测试参数的建议；

T1：测试参数集 1：

-根据要求进行的功能测试；

-进行漏洞扫描，以查找已知的漏洞；

-使用随机选择的输入数据进行的模糊测试；

渗透测试，假设攻击者专业知识、项目或组件知识和/或资源；

T2：测试参数集 2：

-基于需求和组件之间的交互作用的功能测试；

-进行漏洞扫描，以查找已知的漏洞；

-具有增加测试用例迭代和/或输入的自适应选择次数的模糊测试；

-渗透测试，假设攻击者具有更高的专业知识、项目或组件的知识和/或资源。

附件 F
（信息）

影响评级指南

F.1 一般

本附件给出了影响等级标准的示例（涉及安全、财务、运营和隐私损害的损害情况见 15.51。本附件中的表（见表 F.1 至表 F.4）可用于影响等级。

关于损害的可伸缩性(即在单一损害场景中对多个道路用户的影响]如何修改影响评级的考虑没有包括在给出的示例中，但可以酌情添加到特定于组织的评级标准中(如参考[20]。C.1.2，表 4）。

F.2 冲击等级或安全损坏

表 F.1-安全影响等级标准的示例

影响等级	安全冲击等级标准
严重	S3：危及生命的伤害（生存率不确定），致命的伤害
少校	S2：严重和危及生命的伤害（有可能存活）
中等	S1：轻度和中度伤害
不可避免的	S0：无伤害 [a]
[a]S0 的评级可基于 ISO26262-3：2018，表 B.1。	

安全影响等级标准取自 ISO26262-3：2018。

如果提供了一个理由，符合 ISO26262-3：2018 的控制性和暴露性也可以被考虑为对安全性的评级影响。

F.3 对财务损害的影响等级

表 F.2-财务影响评级标准的示例

影响等级	财务影响评级的标准
严重	经济损失会导致受影响的道路使用者可能无法克服的灾难性后果。
少校	经济损害会导致受影响的道路使用者将能够克服的重大后果。
中等	经济损害会造成不方便的后果，受影响的道路使用者将能够通过有限的资源来克服这些后果。
不可避免的	经济损失不会造成任何影响，后果可以忽略不计，或与道路使用者无关。

F.4 操作损坏的冲击等级

表 F.3-操作影响评级标准的示例

影响等级	运行影响等级的标准
严重	操作损坏会导致核心车辆功能的损失或损坏。 示例 1 车辆不工作或显示核心功能的意外行为，如启用软行家庭模式或自动驾驶到意外位置。
少校	操作损坏会导致重要车辆功能的损失或损坏。例子 2 是司机的重大烦恼。
中等	操作损坏会导致车辆功能的部分退化。示例 3 会对用户满意度产生负面影响。
不可避免的	操作损坏不会导致车辆功能的损害或不可感知的损坏。

这些标准可能也有安全后果，也可能没有安全后果。

F.5 对隐私损害的影响等级

表 F.4-隐私影响评级标准的示例

影响等级	关于隐私影响等级的标准
严重	隐私损害会对道路使用者造成重大甚至不可逆转的影响。 有关道路用户的信息非常敏感，并且很容易链接到 PII 负责人。
少校	隐私方面的损害会对道路使用者造成严重影响。有关道路使用者的信息包括： a) 高度敏感，难以连接到 PII 校长；或 b) 敏感且易于链接到 PII 主体。
中等	隐私方面的损害会给道路使用者造成不便的后果。 有关道路使用者的信息包括： a) 敏感但难以链接到 PII 主体；或 b) 不敏感，但很容易链接到 PII 主体。
不可避免的	隐私损害不会造成任何影响，或可忽略不计的后果，或与道路使用者无关。 有关道路用户的信息并不敏感，也难以链接到 PII 负责人。

个人身份信息(PII)和 PII 主体可根据 ISO/IEC29100[匹]进行定义。

附件 G
（信息）

攻击可行性等级指南

GSBUR1 通用

本附件提供了关于如何将以下方法应用于攻击可行性评级的指导方针（见 15.7）：

-攻击潜在的；

-CVSS-based；和
-基于攻击向量的。
考虑一个攻击是否有扩展的潜力（即很容易扩展到多个实例和目标），可以包括在攻击可行性的评级中。

G.2 关于基于攻击潜力的方法的指南

G.2.1 关于攻击潜力的背景

攻击潜力在 ISO/IEC18045㈤中定义为为攻击项目或组件所花费的努力的度量，用攻击者的专业知识和资源来表示。攻击潜力依赖于五个核心参数：

-过去的时间；

-专业知识；

— 有关项目或零部件的知识；

— 机会之窗；和

—equipment.

此子句给出了定制的示例和攻击可行性的映射示例。

G.2.2 参数自适应示例

G.2.2.1 经过时间的定制示例

所经过的时间参数包括识别漏洞并开发和（成功）应用漏洞的时间。因此，该评级是基于评级时的专家知识状态，见表 G.1。

表 G.1-所用时间

<1 天
<1 周
<1 个月
<6 个月
>6 个月

G.2.2.2 专家专长的示例定制

专业知识参数与攻击者的能力相关，相对于他们的技能和经验，见表 G.2。

表 G.2-专业知识

平面图：	
与专家或熟练人士相比，知识不足，没有特别的专业知识。	
	示例 1 普通人使用公开的攻击的逐步描述。
专业人员：	
了解到他们熟悉产品或系统类型的安全行为。 例如 2 经验丰富的业主，普通技术人员知道简单和流行的攻击，如里程计调谐，安装假冒部件。	
专家：	
熟悉底层算法、协议、硬件、结构、安全行为、所采用的安全原则和概念、定义新攻击的技术和工具、密码学、产品类型的经典攻击、攻击方法等。在产品或系统类型中实现。	
例子 3：经验丰富的技术人员或工程师。	
多位专家：	

对于不同的攻击步骤，在专家层面上需要不同的专业知识领域。

例如 4 多个经验丰富的工程师，他们具有不同领域的专业知识，并且是专家级别的不同攻击步骤所必需的。

G.2.2.3 项目或组件知识的示例定制

项目或组件参数的知识与攻击者获得的有关项目或组件的信息量有关，请参见表 G.3。

表 G.3-有关项目或组件的知识

公共信息： 有关项目或组件的公共信息（例如从互联网上获得）。
示例 1 在产品主页或互联网论坛上发布的信息和文档。

表 G3（继续）

受限信息：
有关项目或组件的受限信息（例如，在开发人员组织内受控制并根据保密协议与其他组织共享的知识]。 示例 2 制造商和供应商之间共享的内部文档、需求和设计规范。
机密信息：
关于项目或组件的机密信息（例如，开发人员组织中离散团队之间共享的知识，其访问权限仅限于指定团队的成员）。
示例 3 与固定器相关信息，软件源代码。 **严格保密的信息：**
关于项目或部件的严格机密信息（例如，只有少数人知道的知识，获取受到严格需要了解基础和个人事业的严格控制）。 示例 4 由制造商和/或供应商内部记录的客户特定的校准或内存地图。

G.2.2.4 机会窗口的定制示例

机会窗口参数与成功执行攻击的访问条件（时间、类型）相关。它将访问类型（例如逻辑和物理）和访问持续时间（例如无限制和有限）相结合。根据攻击类型的不同，这可能包括发现可能的目标、对目标的访问、对目标的利用工作、对目标执行攻击的时间、保持未被发现、绕过检测和网络安全控制等等。（详见表 G.4）。

表 G.4：机会之窗

无限制：
通过公共/不受信任网络实现的高可用性，没有任何时间限制（即资产始终可访问）。没有物理存在或时间限制的远程访问，以及对项目或组件的无限物理访问。 示例 1 在没有任何先决条件的情况下进行远程攻击(例如车辆到任何东西或蜂窝接口]，由所有者对芯片调优的无限物理访问。
简单：
高可用性和有限的访问时间。不存在对项目或组件的远程访问。 例如 2 蓝牙配对时间，远程软件更新，远程攻击，要求车辆静止不动。
中度：
项目或组件的可用性较低。有限的物理和/或逻辑访问。无需使用任何特殊工具，即可实际进入车辆内部或外部。 示例 3 攻击器进入一个已解锁的汽车，并可以访问暴露的物理接口，例如通过车载诊断端口进行物理访问。
困难：
项目或组件的可用性非常低。对执行项目或组件的攻击的访问级别。 示例 4 封装 IC 以提取信息，以超过旋转密钥的速度破解加密密钥。

G.2.2.5 设备定制实例

设备参数与攻击者可以发现漏洞和/或执行攻击的工具相关，见表 G.5。

表 G.5 设备

标准：	
	攻击者很容易获得设备。该设备可以是产品本身的一部分（例如，操作系统中的调试器），也可以很容易地获得(例如，互联网源、协议分析器或简单的攻击脚本）。 示例 1 笔记本电脑、CAN 适配器、车载诊断适配器、普通工具（螺丝刀、焊铁、钳子）。
专业人员：	
	攻击者不容易获得设备，但可以毫不费力地获取设备。这可能包括购买适量的设备(例如，功率分析工具，使用数百台通过互联网连接的个人电脑将属于这一类]，或开发更广泛的攻击脚本或程序。如果不同的攻击步骤需要明显不同的测试台组成的专门设备，这将被评为定制的。 例如 2 专用硬件调试设备、车载通信设备（回路试验台硬件、高级示波器、信号发生器）、特种化学品。
定制：	
	设备是专门生产的（例如非常复杂的软件]，不容易向公众获得(例如黑市），或者设备是如此专业，其分销受到控制，甚至可能受到限制。或者，这些设备也非常昂贵。
	例子 3，受制造商限制的工具，电子显微镜。
多个定制：	
	引入是允许一种情况，即不同的攻击步骤需要不同类型的定制设备。

G.2.2.6 攻击潜力和攻击可行性之间的示例映射

对于每个参数，都可以定义数值。根据 ISO/IEC18045㈤，根据上面提出的适应性，提出了以下量表，见表 G.6。

表 G.6-攻击潜力的示例聚合

经过的时间		专家专业知识		对项目或组件的知识		机会之窗		设备	
枚举	**价值**	**枚举**	**价值**	**枚举**	**价值**	**枚举**	**价值**	**枚举**	**价**
<1 天	0	莱曼	0	公众	0	无限	0	标准	0
<1 周	1	熟练的	3	受限	3	简单	1	专业	4
<1 个月	4	专家	6	机密	*7*	中等	4	定制	*7*
<6 个月	17	多位专家	8	严格保密	11	困难/ 没有	10	多个定制	9
>6 个月	19								

根据 ISO/IEC18045[23]，攻击势对应于所有参数的增加。基于 ISO/IEC18045 的自定义，使用表 G.7 绘制了攻击的可行性[23].

表 G.7-攻击潜在映射的示例

攻击可行性评级	值
高	0-9
	10 - 13
介质	14-19
低	20 - 24
非常低	>25

基于 CVSS 的方法的 G3 指南

为了对信息技术安全漏洞进行评级，可以使用事件响应论坛和安全团队（首先）[24]维护的 CVSS。在基本度量组中，可利用性度量(cf。参考[24]。7.1]可用于评估攻击的可行性。其他 CVSS 指标（如影响

指标）由本文档的各个方面涵盖，如损害场景和影响评估。

可利用性指标为：

-攻击向量；

-攻击复杂性；

-所需的特权；和
-用户交互。
首先描述[24]。对 CVSS 度量的评估会根据预定义的范围内产生每个度量的数值。总体可利用性值可以根据一个简单的公式进行计算：

E=8,22x “CxPxU
在哪里

E 为可利用性值；

V 是与攻击向量相关的数值，范围为 0、2 到 0、85；

C 是与攻击复杂度相关的数值，范围从 0、44 到 0、77；

P 是与所需特权相关联的数值，范围为 0、27 到 0、85；和

U 是与用户交互相关的数值，范围从 0、62 到 0、85。

因此，可利用性值的范围在 0、12 到 3、89 之间。
表 G.8 给出了一个关于 CVSS 可利用性值来攻击可行性的示例映射。这是等距离可利用性步骤的一个例子。

表 G.8-CVSS 可利用性映射示例

攻击可行性评级	CVSS 可利用性值
高	2,96-3,89
介质	2,00-2,95
低	1,06 -1,99

表 G.8（继续）

攻击可行性评级	CVSS 可利用性值
非常低	0,12-1,05

注意：仅使用可利用性度量作为较大的 CVSS 基本度量组的一部分的过程并不严格符合 CVSS 对度量的要求。要根据本文档计算风险，缺失的影响度量可以通过本文档的影响度量来补偿，请参见 AocexF 和参考[24]。

在不改变可利用性度量值的情况下，可以补充它们的描述，以便就组织的业务和正在开发的项目或组件提供更好的指导，并减少在将描述应用于实际漏洞时出现误解的可能性。这些补充可以是添加到度量值描述中的特定于组织的示例。

除了漏洞之外，CVSS 的可利用性度量还可以用于评估概念上的缺陷、缺陷和差距。

G4 关于基于攻击矢量的方法的指导方针

基于攻击向量的方法反映了攻击路径的上下文。攻击者为了利用攻击路径，距离越远（逻辑上和物理上），攻击的可行性等级就会越高。假设可以利用互联网利用漏洞的潜在攻击者的数量大于可以利用需要物理访问项目或组件的攻击路径的潜在攻击者的数量，见表 G9

表 G.9-基于攻击向量的方法

攻击可行性评级	标准
高	**网络：** 潜在的攻击路径被绑定到网络堆栈上，而没有任何限制。 示例 1 蜂窝网络连接，使 ECU 直接连接并在互联网上访问。
介质	**相邻：** 潜在的攻击路径被绑定到网络堆栈；但是，连接在物理上或逻辑上都受到限制。 示例 2：蓝牙接口，虚拟专用网连接。
低	**本地：** 潜在的攻击路径不绑定到网络堆栈，威胁代理需要直接访问该项目才能实现攻击路径。 例如 3：通用串行总线大容量存储设备，存储卡。
非常低	**物理：** 威胁代理需要物理访问才能实现攻击路径。

附件 H
（信息）

TARA 方法-前照灯系统的应用实例

HSUB1 总干事

本附件中前照灯系统开发的示例和各自的工作产品仅为说明性目的而提供，并不打算暗示任何实际使用的特定方法。

本附件可以通过介绍威胁分析和风险评估(TARA)方法的应用实例，来帮助理解本文件的要求。本示例只展示了说明 TARA 应用程序的概念阶段，并以抽象、简化的方式呈现。特别是它解决了：

-项目定义；和
—TARA.

TARA 被定义为模块化的分析方法，每个模块都可以按任何顺序进行，例如：

— 资产识别相应损害场景的识别影响等级威胁场景识别攻击路径分析。

— 从目录中选择损害场景，影响评级，影响场景识别，资产识别。

本附件中的例子的顺序如下：

i. 资产鉴定；

ii. 影响等级；

iii. 威胁场景识别；

iv. 攻击路径分析；

v. 攻击可行性评价；

vi. 风险价值确定；
vii. 风险治疗决策。

在步骤 v 中，采用了两种不同的方法来评价攻击的可行性。一种方法使用基于攻击矢量的方法（参见[RC-15-14]]，另一种方法使用基于攻击潜力的方法）。
图 H.1 概述了第 9 条和第 15 条之间的各种相互作用。

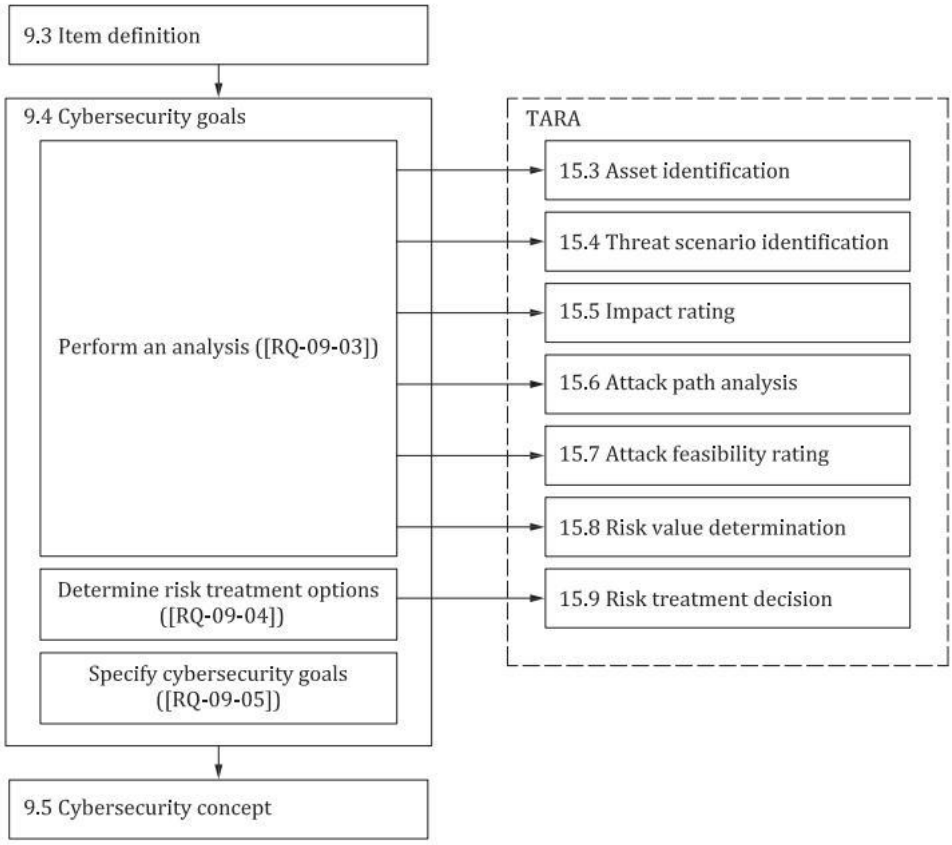


图 H.1-概念阶段的相互作用

H2 前照灯系统概念阶段的示例活动

H.2.1 项目定义

. 本条款显示了 9.3 所选工作产品示例，前照灯系统示例项目定义如下：

a) 项目边界（见图 H.2）：

b) 项目功能；

-项目功能概述：前照灯系统根据开关开启/关闭前照灯。如果前照灯处于远光灯模式，则当检测到迎面而来的车辆时，前照灯系统会将前照灯自动切换到近光灯模式。如果不再检测到即将到来的车辆，它也会将前照灯自动返回到远光灯模式。

注意关于前照灯的功能，前照灯系统不依赖于导航 ECU 和网关 ECU。

c) 初步架构（见图 H.2）。

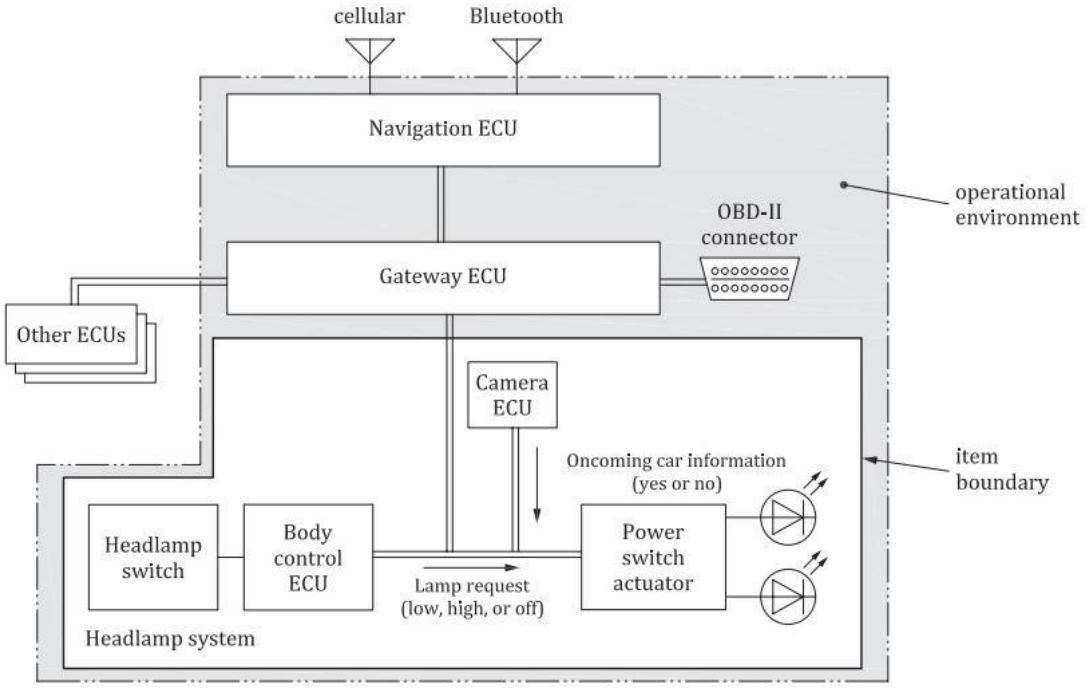


图 H.2-前照灯系统的项目边界及初步架构示例

在项目定义期间，将描述项目的操作环境（请参见[RQ-09-02]]。操作环境为 TARA 的分析活动提供了补充信息。表 H.1 显示了本附件中使用的操作环境的示例说明。

表 H.1-操作环境的示例说明

项目（前照灯系统）与网关 ECU 连接，网关 ECU 通过数据通信与导航 ECU 连接。 导航 ECU 具有外外部通信接口： —Bluetooth； —cellular. 假设： — 导航 ECU 有一个防火墙，以防止来自外部接口的无效数据通信。 网关 ECU 具有外部通信接口： —OBD-II. 假设： — 网关 ECU 具有很强的安全控制能力，包括防火墙功能(开发为 CAL4)。

H.2.2 资产识别

[RQ-09-03]根据 15.3 的要求进行资产识别，以识别项目的资产及其损坏情况。表 H.2 为资产识别的示例结果。

表 H.2-资产和损坏情况的示例列表

资产	网络安全属性			损坏情况
	C	I	A	
数据通信（指示灯请求）	—	X	X	车辆不能在夜间驾驶，因为（驾驶员感知到）前照灯功能在停车时被抑制。
	—	X	—	夜间中速行驶时，前照灯与狭窄的静止物体（例如一棵树）发生碰撞。
数据通信（未来的汽车信息）	—	X	—	迎面而来的车辆的司机是盲的，这是由于夜间驾驶无法转向近光灯。
	—	—	X	夜间驾驶时前照灯始终保持近光灯造成的自动远光灯故障。
车身控制 ECU 固件	X	X	—	

H.2.3 冲击等级

[RQ-09-03]还根据 15.5 的要求使用影响等级来评价损坏场景的影响。表 H.3 显示了影响等级的示例结果。

表 H.3-损坏场景的影响等级示例

损坏情况	影响类别	影响等级
车辆不能在夜间驾驶，因为（驾驶员感知到）前照灯功能在停车时受到抑制。	O	少校
夜间中速行驶时，前照灯与狭窄的静止物体（例如一棵树）发生碰撞。	S	严重 (S3)
夜间驾驶时前照灯始终保持近光灯造成的自动远光灯故障。	O	中等

H.2.4 威胁场景识别

[RQ-09-03]还根据“54 表 H.4 显示了威胁方案识别的示例结果”来调用威胁方案识别。

表 H.4-威胁场景的示例

损坏情况	威胁场景
由于夜间中速行驶时意外关闭前照灯，与狭窄的静止物体（例如一棵树）发生前碰撞	信号的欺骗导致“灯请求”信号与电源开关执行器 ECU 的数据通信的完整性丧失，可能导致前照灯无意中关闭。
	篡改车身控制 ECU 发送的信号，导致“灯请求”信号与电源开关执行器 ECU 的数据通信的完整性丧失，可能导致前照灯无意中关闭。
夜间驾驶时，前照灯始终保持在近光灯造成的自动远光灯故障	资产：迎面而来的汽车信息 网络安全属性：可用性 相关原因：拒绝提供迎面而来的汽车信息的服务

H.2.5 攻击路径分析

. [RQ-09-03]还根据 15.6 调用攻击路径分析。表 H.5 显示了攻击路径分析的示例结果，图 H.3 显示了通过攻击树分析的攻击路径分析的示例。

对攻击路径的分析可以考虑到假设。在本例中，可以根据假设排除需要在项目内部进行物理访问的攻击路径，如身体控制 ECU 的微控制器。

表 H.5-威胁场景的攻击路径示例

威胁场景	攻击路径
信号的欺骗导致“灯请求”信号与电源开关执行器 ECU 的数据通信的完整性丧失，可能导致前照灯无意中关闭	i. 攻击器从蜂窝接口损害导航 ECU。 ii. 受损的导航 ECU 发送恶意控制信号。 iii. 网关 ECU 将恶意信号转发到电源开关执行器。 iv. 恶意信号欺骗灯请求（关闭）。
	i. 攻击器从蓝牙接口损害导航 ECU。 ii. 受损的导航 ECU 发送恶意控制信号。 iii. 网关 ECU 将恶意信号转发到电源开关执行器。 iv. 恶意信号欺骗灯请求（关闭）。
	i. 攻击器将获得对 OBD 连接器的本地访问权限（见表 G.9）。 ii. 攻击器从 OBD 连接器发送恶意控制信号。 iii. 网关 ECU 将恶意信号转发到电源开关执行器。 iv. 恶意信号欺骗灯请求（关闭）。
拒绝提供迎面而来的汽车信息	i. 攻击器从蜂窝接口损害导航 ECU。 ii. 受损的导航 ECU 发送恶意控制信号。 iii. 网关 ECU 将恶意信号转发到电源开关执行器。 iv. 攻击者用通信总线淹没了大量的信息。
	i. 当车辆停车解锁时，攻击器会将启用蓝牙的 OBD 适配器连接到 OBD 连接器上。 ii. 攻击者通过蓝牙接口损害了司机的智能手机。 iii. 攻击者通过智能手机和蓝牙适配器向网关 ECU 发送信息。 iv. 网关 ECU 将恶意信号转发到电源开关执行器。 v. 攻击者用通信总线淹没了大量的信息。

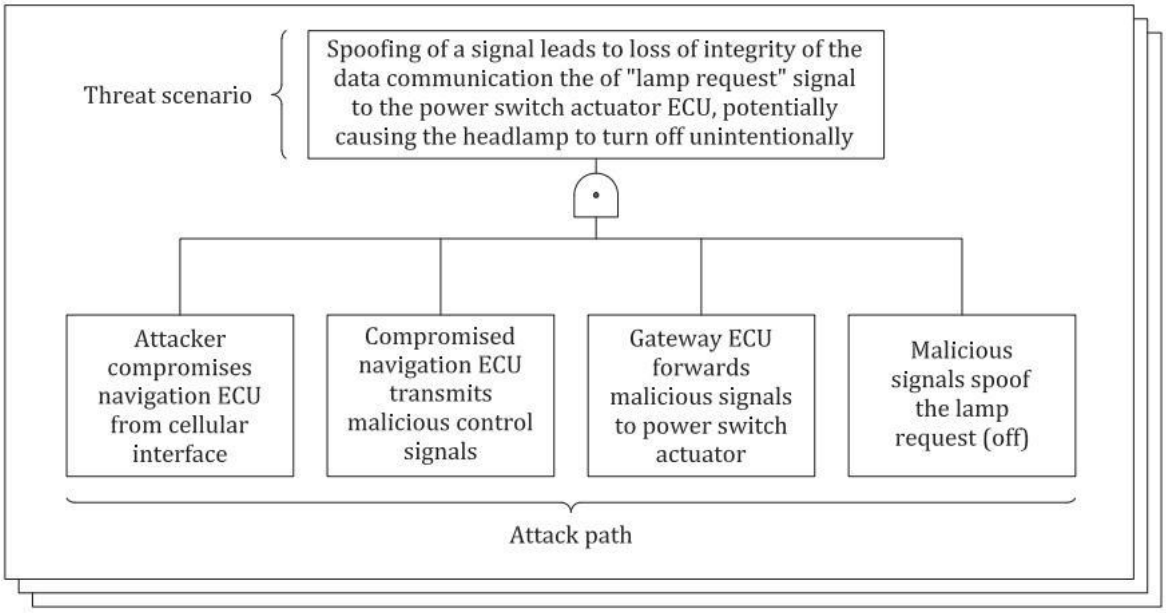


图 H.3-通过攻击树分析导出的攻击路径的示例

H.2.6 攻击可行性评级

. . [RQ-09-03]还根据 15.7 表呼叫每个攻击路径的攻击可行性评级。6 显示了根据 G4 所述的基于攻击矢量的方法的攻击可行性评级的示例结果。表 H.7 显示了根据 G2 所述的基于攻击潜力的方法的攻击可行性评级的示例结果。

表 H.6-使用基于攻击矢量的方法的攻击可行性评价示例

攻击路径	攻击可行性评级
i. 攻击器从蜂窝接口损害导航 ECU。 ii. 受损的导航 ECU 发送恶意控制信号。 iii. 网关 ECU 将恶意信号转发到电源开关执行器。 iv. 恶意信号欺骗灯请求（打开）。	高
i. 攻击器从蓝牙接口损害导航 ECU。 ii. 受损的导航 ECU 发送恶意控制信号。 iii. 网关 ECU 将恶意信号转发到电源开关执行器。 iv. 恶意信号欺骗灯请求（打开）。	介质
i. 攻击器从 OBD2 连接器发送恶意控制信号。 ii. 网关 ECU 将恶意信号转发给电源开关执行器。 iii. 恶意信号欺骗灯请求（打开）。	低

注 1 该基于攻击向量的方法适用于概念阶段。因为在概念阶段，不可能收集所有与漏洞信息相关的项目。

根据推荐（见[RC-15-11]]，攻击的可行性也可以基于基于攻击潜力的方法来确定，这如表 H.7 中的示例所示。

表 H.7-使用基于攻击潜力的方法的攻击可行性评级示例

威胁场景	攻击路径	攻击可行性评估						
		等	se	KoIC	WoO	Eq	价值	攻击可行性评级
拒绝提供迎面而来的汽车信息	i. 攻击器从蜂窝接口损害导航 ECU。 ii. 受损的导航 ECU 发送恶意控制信号。 iii. 网关 ECU 将恶意信号转发到电源开关执行器。 iv. 攻击者用通信总线淹没了大量的信息。	1	8	*7*	0	4	20	低
	i. 当车辆停车解锁时，攻击器会将启用蓝色的 OBD 适配器连接到 OBD 连接器上。 ii. 攻击者妥协 司机的智能手机 与 蓝牙接口。 iii. 攻击者通过智能手机和蓝牙适配器向网关 ECU 发送信息。 iv. 网关 ECU 将恶意信号转发到电源开关执行器。 v. 攻击者用通信总线淹没了大量的信息。	1	8	*7*	4	4	24	低
密钥 ET 经过的时间 SE 专家专业知识 KoIC 对项目或组件的知识 WoO 机会窗口 Eq 设备								

注 2 每个组织都可以根据自己的政策对每个评级应用基本依据。例如，为第二个攻击路径分配了机会窗口 4（中等，请参见表 G.4），因为需要物理访问。根据表 G.7，考虑所有可行性值，确定攻击可行性等级。

H.2.7 风险价值确定

[RQ-09-03]还要求根据 15.8 要求对每个威胁场景进行风险确定。风险值可以利用组织定义的风险矩阵来确定，以便将影响评级（见 15.5）和攻击可行性（见 15.7）的组合映射到风险值。表 H.8 显示了一个示例风险矩阵，表 H.9 显示了使用表 H.8 确定风险的示例结果。

表 H.8-风险矩阵示例

		攻击可行性评级			
		非常低	低	介质	高
影响等级	严重	2	3	4	5
	少校	1	2	3	4
	中等	1	2	2	3
	不可避免	1	1	1	1

表 H.9-已确定的风险值的示例

威胁场景	综合攻击的可行性等级	影响等级	风险价值
信号欺骗导致电源开关执行器 ECU“灯请求”信号数据通信完整性丧失	高	严重	S：5
拒绝提供迎面而来的汽车信息	低	中等	0：2

风险值也可以由组织定义的风险公式来确定。以下公式和表 H.10 显示了一个示例。

影响等级	表示影响的数值 I
不可避免	0
中等	1
少校	1,5
严重	2

攻击可行性评级	攻击可行性的数值 F
非常低	0
低	1
介质	1,5
高	2

表 H.10-影响和攻击可行性与数值之间的示例转换

对于表 H.9 中所示的特定威胁场景，使用表 H.8 中给出的示例和上述公式的计算将导致相同的风险值。

H.2.8 风险治疗决策

[RQ-09-04]要求根据 15.9 选择治疗方案。表 H.11 显示了风险治疗决策的示例结果。.

表 H.11-风险治疗决策的示例结果

威胁场景	风险价值	风险治疗选择
信号欺骗导致电源开关执行器 ECU“灯请求”信号数据通信完整性丧失	S：5	降低风险
拒绝提供迎面而来的汽车信息	0：2	降低风险

参考书目

[1] *ISO26262-1：2018，道路车辆。功能安全。第 1 部分：词汇*

[2] *ISO9000：2015，质量管理体系-基础和词汇表*

[3] ISO31000：2018，风险管理-指南

[4] *ISO/IEC/IEEE15288：2015，系统和软件工程-系统生命周期过程*

[5] *ISO/IEC27000：2018，信息技术。安全技术。信息安全管理系统。概述和词汇表*

[6] *ISO/TR4804，道路车辆。自动驾驶系统的安全和网络安全。设计、验证和验证*

[7] *IATF16949，对汽车生产和相关服务部件组织的质量管理体系要求*

[8] *ISO9001，质量管理体系。要求*

[9] *ISO10007，质量管理-配置管理指南*

[10] *ISO/IEC33001，信息技术。过程评估。概念和术语*

[11] *ISO/IEC/IEEE15288，系统和软件工程。系统生命周期过程*

[12] *ISO/IEC/IEEE12207，系统和软件工程。软件生命周期过程*

[13] Vdaqmc 工作组 13/汽车股份有限公司。汽车香料工艺评估/参考模型，3.1 版[在线。柏林：VDAQMC，2017 年 11 月 。网址是：http://www.automotivespice.com/fileadmin/software-download/AutomotiveSPICEPAM_31.pdf

[14] *ISO29147，信息技术。安全技术。漏洞披露*

[15] *IEC62443-2-1，工业通信网络。网络和系统安全。第 2-1 部分：建立工业自动化和控制系统安全程序*

[16] ISO26262（所有零部件），道路车辆-功能安全

[17] *MISRAC2012，关键系统中 C 语言的使用指南，3rd 版，1st* 修订。英国努尼顿：HORIBAMira，2019 年 2 月。ISBN（印刷/电子）：978-1-906400-21-7/978-1-906400-22-4。

[18] SEICERTC 编码标准-开发安全、可靠和安全系统的规则。宾夕法尼亚州匹兹堡：卡耐基梅隆大学软件工程研究所，2016 年[查看 2021-02-12]。查询网址为：https://resources.sei.cmu.edu/library/asset-view.cfm? assetid=454220

[19] ROSSRon 等人。（2018），系统安全工程：对可信安全系统工程中多学科方法的考虑[在线]。（国家标准与技术研究所，盖瑟斯堡，医学博士），NIST 特别出版物(SP)800-160，Vol。 1.更新于 2018 年 3 月[查看 2021 年 02 月 16 日]。可在：https://doi.org/10.6028/NIST.SP.800 上获得-160v1

[20] 电子安全车辆入侵保护应用程序(evita)可交付 D2.3：基于黑暗面场景的汽车车载网络的安全要求。由 A.Ruddle 等人编辑。2009 年 12 月[浏览 2021 年 01 月 17 日]。可在：https://doi.org/10.5281/zenodo 上获得.1188418

[21] *ETSITS102165-1，cyber；方法和协议：第 1 部分：威胁、漏洞、风险分析(TVRA)，5.2.3 版[在线]。2017 年 10 月[观看 2021-01 月 19 日]。购买网址为：https://www.etsi.org/deliver/etsi_ts/102100102199/10216501/05.02.0360/ts 10216501v050203p.pdf*

[22] 尤西达维勒斯，托尼和莫拉纳，马可 M。*风险中心威胁建模：攻击模拟和威胁分析的过程*。新泽西州，霍博肯：威利，2015 年 5 月。编号编号：978-1-118-988350。

[23] *ISO/IEC18045，信息技术安全技术。IT 安全评估的方法*

[24] 事件响应论坛和安全小组（第一）。常见漏洞评分系统(CVSS)，常见漏洞评分系统 v3，1：规范文件，[联机]。可在：https://www.first 上获得。Org/cvss/v3.1/specification-document

[25] *ISO/IEC29100，信息技术。安全技术。隐私框架*

[26] *汽车 ISAC，汽车网络安全最佳实践[在线]。网址是：https:www.automotiveisac.com/best-practices/*

[27] 事件响应论坛和安全小组（第一）。红绿灯协议(TLP)，第一标准定义和使用指南-版本 1、0，[在线]。网址是：https://www.first.org/tlp/

[28] [2]*ISO/IEC2382，信息技术。词汇表*

[29] *ISO/IEC15408（所有部件），信息技术。安全技术。IT 安全评价标准*

[30] *ISO/IEC27001，信息技术。安全技术。信息安全管理系统。要求*

[31] *ISO/IEC27010，信息技术。安全技术。部门间和组织间通信的信息安全管理*

[32] *ISO/IEC/IEEE26511，系统和软件工程-对系统、软件和服务用户的信息管理人员的要求*

[33] *IEC31010，风险管理-风险评估技术*

[34] *IEC61508-7，电气/电子/可编程电子安全相关系统的功能安全。第 7 部分：技术和措施概述*

[35] 约翰逊·克里斯托弗等人。（2016）网络威胁信息共享指南[在线]。（国家标准与技术研究所，盖瑟斯堡，医学博士），NIST 特别出版物(SP)800150,2016 年 10 月[查看 2021-02-16]。可在：https://doi.org/10.6028/NIST.SP.800-150 上获得

[36] 2012 年联合任务部队转型计划]，进行风险评估的指南[在线]。（国家标准与技术研究所，盖瑟斯堡，医学博士），NIST 特别出版物(SP)800-30，版。1.2012 年 9 月[观看 2021 年 02 月 16 日]。可在：http://dx.doi.org/10.6028/NIST.SP.800-30r1 上获得

[37] *SAEJ3061，网络物理车辆系统的网络安全指南*

[38] 围巾，凯伦等人。（2008），信息安全测试和评估技术指南[在线]。（国家标准与技术研究所，盖瑟斯堡，医学博士），NIST 特别出版物(SP)800-115。2008 年 9 月[浏览 2021 年 02 月 16 日]。可在：https://doi.org/10.6028/NIST.SP.800-115 上获得

[39]takanenAri 等人。为软件安全和质量保证的融合，第二版。马萨诸塞州波士顿/伦敦：艺术科技之家，2018 年 1 月。编号编号：978-1-60807-850-9。

2可在：https://www.iso 获得。Org/obp/ui#iso：std：iso-iec：2382.

ICS43.040.15
价格基于 81 页