国际标准

ISO/SAE 21434

第一版2021年8月

公路车辆网络安全工程

公路车辆—网络安全工程

参考编号
ISO/SAE 21434：
2021(E)

受版权保护的文档

ISO版权办公室

CP 401·Ch.de Blandonnet 8
CH-1214 Vernier，日内瓦

电话：+41227490111

Email:copyright@iso.org
Website:www.iso.org

SAE国际

400英联邦大道。
Warrendale, PA, USA15096

电话：877-606-7323（美国和加拿大境内）

电话：+1724-776-4970（美国以外）
Fax:724-776-0790
Email:CustomerService@sae.org
Website:www.sae.org

由ISO在瑞士出版，由SAE International在美国出版

前言

国际标准化组织（ISO）是全球各国标准机构(ISO成员机构）的联合体。国际标准的准备工作通常由ISO技术委员会承担。每个对已成立技术委员会的主题感兴趣的成员机构都有权派代表参加该委员会。国际组织，无论是政府还是非政府，在与ISO联络的情况下，也参与这项工作。ISO在所有电工标准化事务上与国际电工委员会（IEC）密切合作。

SAE国际是一个全球性的协会，拥有超过128,000名来自航空航天、汽车和商用车行业的工程师及相关技术专家。SAE国际的标准被用于推动全球的移动工程发展。SAE技术标准开发计划是该组织为其服务的航空航天、汽车和商用车行业提供的主要服务之一。这些工作由来自世界各地的9,000多名工程师和其他合格专业人士通过志愿努力授权、修订和维护。SAE主题专家作为个人参与标准制定过程，而不是其组织的代表。因此，SAE标准代表了在透明、开放和协作的过程中开发的最佳技术内容。

本文件的编制过程以及进一步维护的程序已在ISO/IEC指令第1部分和SAE技术标准委员会政策中描述。特别是，不同类型的ISO文件所需的不同审批标准应予以注意。本文件是根据ISO/IEC指令第2部分的编辑规则起草的（见www　org/directives).

请注意，本文件中的一些元素可能受专利权保护。ISO和SAE国际不负责识别任何或所有此类专利权。在文件开发过程中识别出的任何专利权详情将列于引言部分和/或ISO收到的专利声明列表中（参见www.iso.org/patents)。

SAE技术标准委员会规则规定：“本文件的发布旨在推进技术和工程科学的发展。使用本文件完全是自愿的，其适用性和适合性，包括由此产生的任何专利侵权，完全由用户负责。”

本文档中使用的任何商品名称都是为了方便用户而提供的信息，不构成认可。

有关标准的自愿性质、与符合性评估相关的ISO特定术语和表达方式的含义，以及ISO在技术性贸易壁垒（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 .

本文件由技术委员会ISO/TC 22，道路车辆，分委员会SC 32，电气和电子组件和一般系统方面，以及SAE TEVEES18A车辆网络安全系统工程委员会共同编写。

ISO/SAE 21434第1版取消并取代SAE J3061：2016[3Z]。

主要变更如下：

——内容和结构的全面修改。

有关本文件的任何反馈或问题应提交给用户所在国家的标准机构。这些机构的完整列表可参见<https://www.sae.org/standards/content/ISO/SAE1>.html。或者，若要对本文件提供反馈，请访问https://www.sae.org/standards/content/ISO/SAE 21434/。

介绍

本文件的目的

本文档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。通过确保适当考虑网络安全，本文档旨在使E/E系统的工程能够跟上最先进技术以及不断演变的攻击方法。

本文件提供了网络安全工程相关的词汇、目标、要求和指南，作为整个供应链中共同理解的基础。这使得组织能够：

一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。

本文件可用于实施包括网络安全风险管理在内的网络安全管理体系。

本文件的组织结构

图1给出了文档结构的概述。图1中的元素并不规定各个主题的执行顺序。

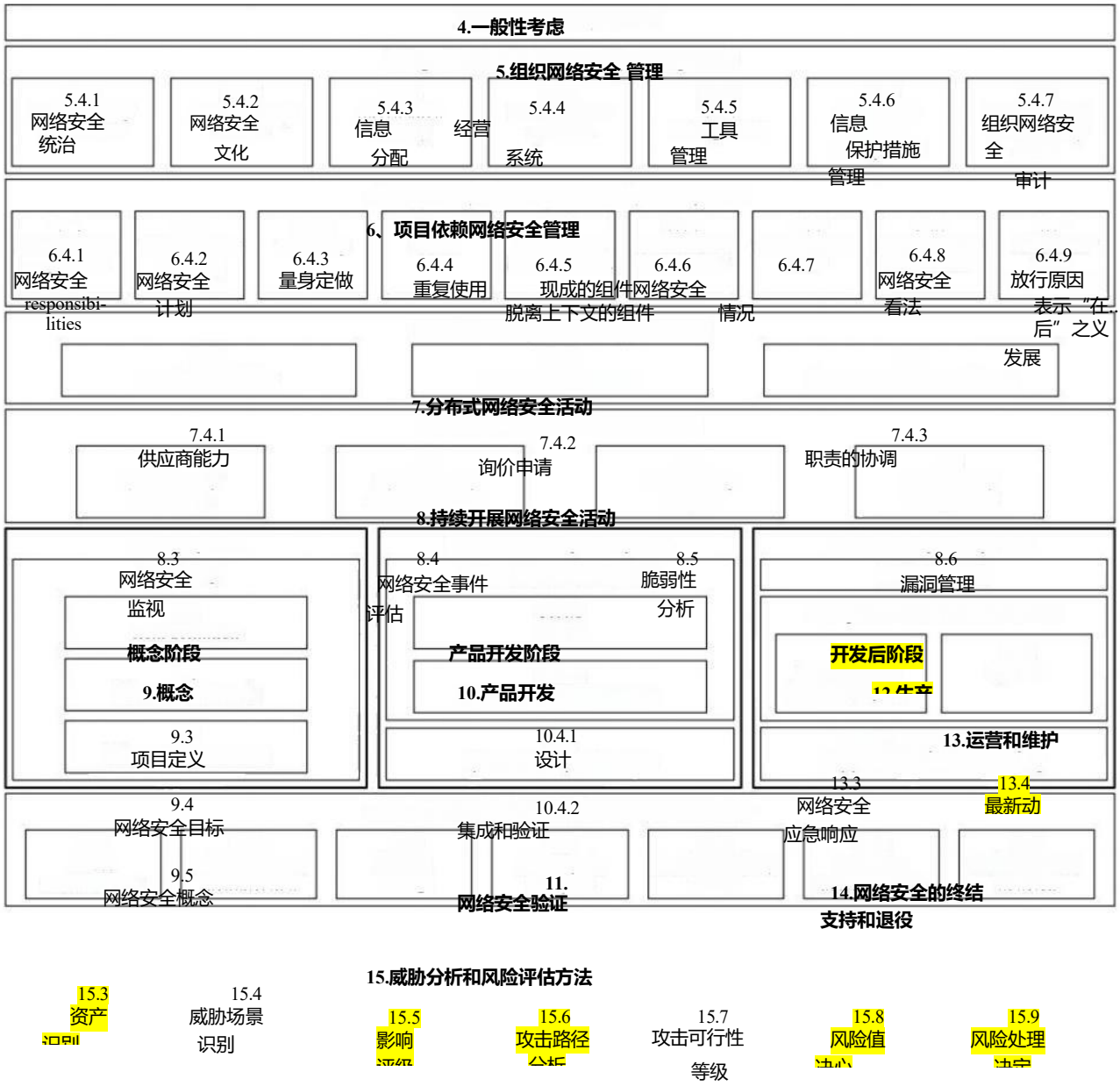


图1-本文件概述

第4条（一般考虑）是信息性的，包括本文档中所采用的道路车辆网络安全工程方法的背景和观点。

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（项目级网络安全管理）包括项目级的网络安全管理和网络安全活动。

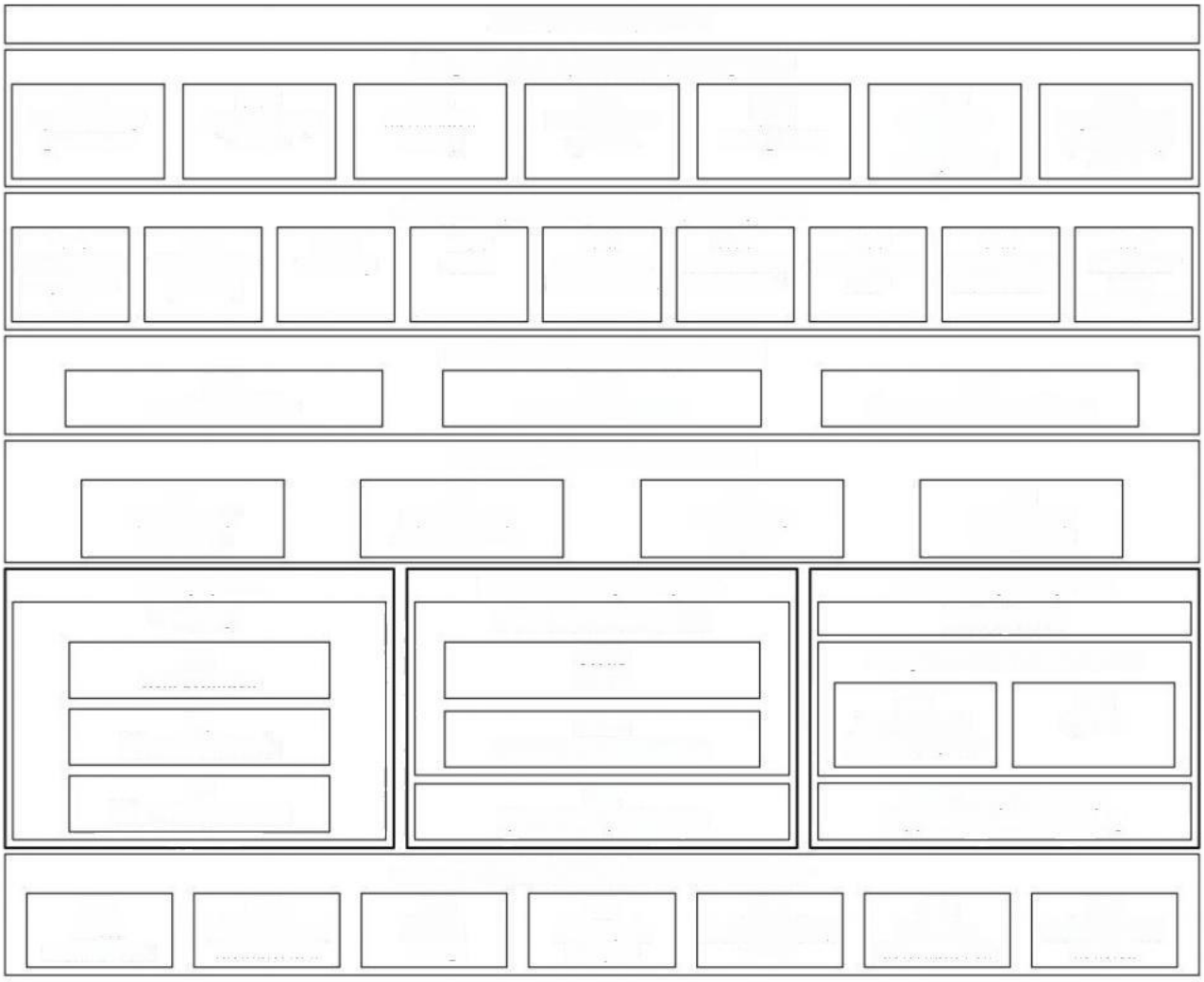
条款Z（分布式网络安全活动）包括客户和供应商之间分配网络安全活动责任的要求。

第8条（持续的网络安全活动）包括提供信息以进行持续风险评估的活动，并定义了E/E系统的漏洞管理，直至网络安全支持结束。

第9条（概念）包括确定网络安全风险、网络安全目标和项目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）包括在车辆级别对项目进行的网络安全验证，



第12条（生产）包括与网络安全相关的制造和组装项目或组件的方面。

第13条（操作和维护）包括与网络安全事件响应和更新项目或组件相关的活动。

第14条（网络安全支持结束和退役）包括对项目或组件支持结束和退役的网络安全考虑。

第15条（威胁分析和风险评估方法）包括用于分析和评估以确定网络安全风险程度的模块化方法，以便采取措施。

第5条至第15条有其自己的目标、provisions(i.e.requirements、建议、权限）和工作产品。工作产品是网络安全活动的结果，满足一个或多个相关要求。

“先决条件”是强制性输入，由前一阶段的工作产品组成。“其他支持信息”是可以考虑的信息，可由与网络安全活动负责人不同的来源提供。

网络安全活动和工作成果的总结见附录A。

条款和工作成果被分配了唯一的标识符，由两个字母缩写组成（“RQ”表示要求，“RC”表示建议，“PM”表示许可，“WP”表示工作成果），后面跟着两个数字，用连字符隔开。第一个数字指的是条款，第二个数字则表示该条款下连续序列中的顺序。例如，[RQ-05-14]指的是第5条中的第14项规定，这是一项要求。

公路车辆网络安全工程

1范围

本文件规定了道路车辆中电气和电子（E/E）系统概念、产品开发、生产、运行、维护和退役的网络安全风险管理工程要求，包括其组件和接口。

定义了一个框架，其中包括网络安全过程的要求和用于通信和管理网络安全风险的共同语言。

本文件适用于系列生产道路车辆电子/电气系统，包括其组件和接口，其开发或修改是在本文件发布之后开始的。

本文件未规定与网络安全相关的具体技术或解决方案。

2规范性引用文件

以下文件在本文中被引用，其部分内容构成本文件的要求。对于有日期的引用，仅适用所引用的版本。对于没有日期的引用，适用所引用文件的最新版本（包括任何修正案）。ISO 26262-3：2018，道路车辆—功能安全—第3部分：概念阶段

3术语、定义和缩略语

3.1术语和定义

本文件中，以下术语和定义适用。

ISO和IEC维护用于标准化的术语数据库，网址如下：ISO在线浏览平台：https://www

.org/obp

IEC Electropedia：可在https://www.electropedia.org/上获取

3.1.1
体系结构设计
允许识别组件（3.1.7）、其边界、接口和交互的表示

3.1.2
资产
具有价值或有助于价值的对象

条目注释1：资产具有一个或多个网络安全属性（3.1.20），其破坏可能导致一种或多种损害情形（3.1.22）。

3.1.3
攻击可行性
攻击路径属性（3.1.4）描述成功执行相应操作集的难易程度

3.1.4
攻击路径

攻击
为实现威胁场景（3.1.33）而采取的一系列蓄意行动

3.1.5
攻击者

执行攻击路径（3.1.4）的个人、团体或组织

3.1.6
审计

对过程进行检查，以确定在多大程度上实现了过程目标

[来源：ISO 26262-1：2018[1,3.5，修改——“关于”一词被替换为“确定程度”，并添加了“已实现”。]

3.1.7
组成部分

逻辑上和技术上可分离的部分

3.1.8
顾客

接受服务或产品的个人或组织

[来源：ISO 9000：2015[2]，3.2.4，修改——将短语“可能或已经收到”替换为“收到”，省略了短语“该人或组织打算或需要的”，并省略了条目中的示例和注释1。]

3.1.9
网络安全

公路车辆网络安全

资产（3.1.2）在威胁场景（3.1.33）中得到充分保护的状态（3.1.25）道路车辆、其功能及其电气或电子组件（3.1.Z）

条目注释1：为了简洁起见，本文件中使用网络安全一词代替道路车辆网络安全。

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，说明风险（3.1.29）是合理的

3.1.12
网络安全声明

关于风险的声明（3.1.29）

条目注释1：网络安全声明可以包括保留或共享风险的依据。

3.1.13
网络安全概念

项目网络安全要求（3.1.25）和操作环境要求（3.1.26），以及有关网络安全控制的相关信息（3.1.14）

3.1.14
网络安全控制
正在修改风险的措施（3.1.29）

[来源：ISO 31000：2018 [3,3.8，修改——“网络安全”一词被添加到术语中，“维护和/或”一词被删除，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.Z）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的概念级网络安全要求（3.1.33）

3.1.17
网络安全事件

现场情况可能涉及脆弱性（3.1.38）利用

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）和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
网络安全财产

值得保护的属性

条目注释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

网络安全要求和相应的体系结构设计（3.1.1）

3.1.22
损坏情况

涉及车辆或车辆功能并影响道路使用者的不良后果（3.1.31）

3.1.23
分散的网络安全活动

客户（3.1.8）和供应商之间分配了职责的项目（3.1.25）或组件（3.1.7）的网络安全活动

3.1.24
影响

损害情景（3.1.22）造成的损害或身体伤害程度的估计

3.1.25
条

在车辆级别上实现功能的组件或组件组（3.1.Z）

注1：如果系统在车辆级别实现功能，则可将其视为项目，否则为组件。

[来源：ISO 26262-1：2018[1,3.8，修改——术语“系统”已被“组件”取代，“ISO 26262适用的”和“或功能的一部分”短语被省略，并且条目中的注释1被替换。]

3.1.26

工作环境

考虑操作使用中的交互作用

注1：项目（3.1.25）或组件（3.1.Z）的操作使用可以包括在车辆功能、生产、和/或维修中的使用。

3.1.27
关联之外
未在特定项目（3.1.25）的背景下开发

示例：具有假设网络安全要求的处理单元，将集成到不同的项目中。

3.1.28
渗透测试

模拟真实世界攻击的网络安全测试，以识别破坏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（3.1.9），以攻击可行性（3.1.3）和影响（3.1.24）表示

3.1.30
风险管理
协调活动，以指导和控制组织的风险（3.1.29）[来源：ISO 31000：2018[3，3.2]

3.1.31
道路使用者
使用道路的人

示例乘客、行人、骑自行车者、机动车驾驶员或车辆所有者

3.1.32
裁缝，动词
与本文件中的描述相比，省略或以不同的方式执行某项活动

3.1.33
威胁场景
为实现损害情形（3.1.22）而破坏一个或多个资产（3.1.2）的网络安全属性（3.1.20）的潜在原因

3.1.34
分拣
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.Z）的相关性

3.1.35
扳机
分诊标准（3.1.34）

3.1.36
确认
通过提供客观证据，确认项目（3.1.25）的网络安全目标（3.1.16）是充分的，并已实现

[来源：ISO/IEC/IEEE 15288：2015 [4]，4.1.53，修改——“满足特定预期用途或应用的要求”一词已被“该物品的网络安全目标充分且已实现”所取代，条目注释1被省略。]

3.1.37
证明

通过提供客观证据，确认已满足特定要求

[来源：ISO/IEC/IEEE 15288：2015[4]，4.1.54，已修改——条目中的注释1已被省略。]

3.1.38
弱点

可作为攻击路径（3.1.4）的一部分加以利用的弱点（3.1.40）

[来源：ISO/IEC 27000：2018[5,3.77，修改——省略了“资产或控制”的短语；将“由一个或多个威胁”替换为“作为攻击路径的一部分”。]

3.1.39
脆弱性分析

漏洞的系统识别和评估（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：缺少要求或规格。

示例2建筑或设计缺陷，包括安全协议设计不正确。

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。

示例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使用过时或已弃用的函数，包括加密算法。

3.2简写术语

克　　网络安全保证等级

慢性静脉郁滞综合征　　通用脆弱性评分系统

E/E　　电气和电子

一般的　　电子控制单元

全方位距离导航系统　　车载诊断

石油乳状液泥浆　　原设备制造商

总理　　准许

克罗　　推荐

求矩　　要求

拉西克　　负责、问责、支持、知情、咨询

塔拉　　威胁分析和风险评估

网页　　工作成果

4一般注意事项

项目包括车辆中用于实现车辆level，e.g.braking特定功能的所有电子设备和软件（即其组件）。项目或组件与其运行环境相互作用。

本文件的应用仅限于系列生产道路车辆的网络安全相关项目和组件（即非原型），包括售后市场和服务部件。系统外部

出于网络安全目的，可考虑对车辆(e.g.back-end服务器）进行保护，但不在本文档的范围内。

本文档从单一项目的视角描述了网络安全工程。本文件未规定道路车辆电子电气架构中各项目功能的适当分配。对于整个车辆而言，可以考虑车辆的电子电气架构或其与网络安全相关的项目和组件的网络安全案例集。如果在项目和组件上执行了本文档中描述的网络安全活动，则会解决不合理的车辆网络安全风险。

本文档中描述的组织整体网络安全风险管理适用于整个生命周期阶段，如图2所示。

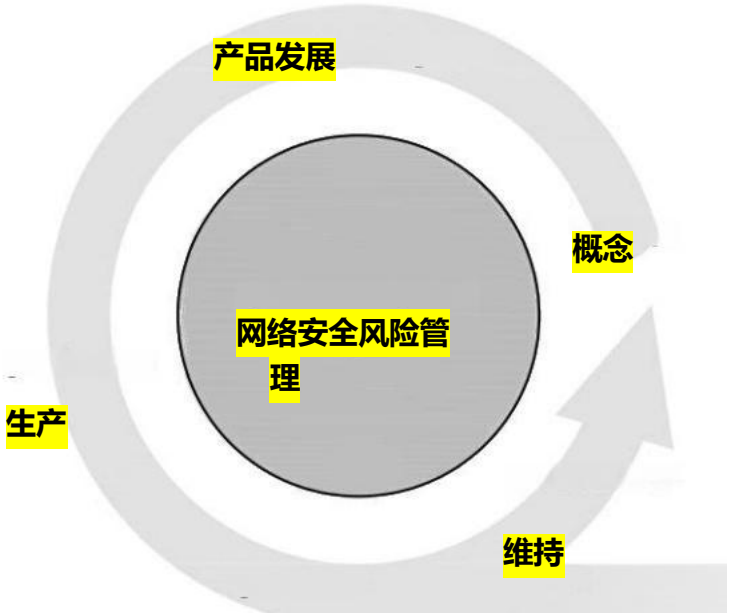


图2-网络安全风险管理总体情况

网络安全风险管理贯穿整个供应链，以支持网络安全工程。汽车供应链展示了多种合作模式。并非所有参与特定项目的组织都适用相同的网络安全活动。网络安全活动可以根据具体情况量身定制（见第6条）。特定项目或组件的开发合作伙伴就工作分配达成一致，以便执行相应的网络安全活动（见第7条）。

图3显示了项目、功能、组件和相关术语之间的关系。

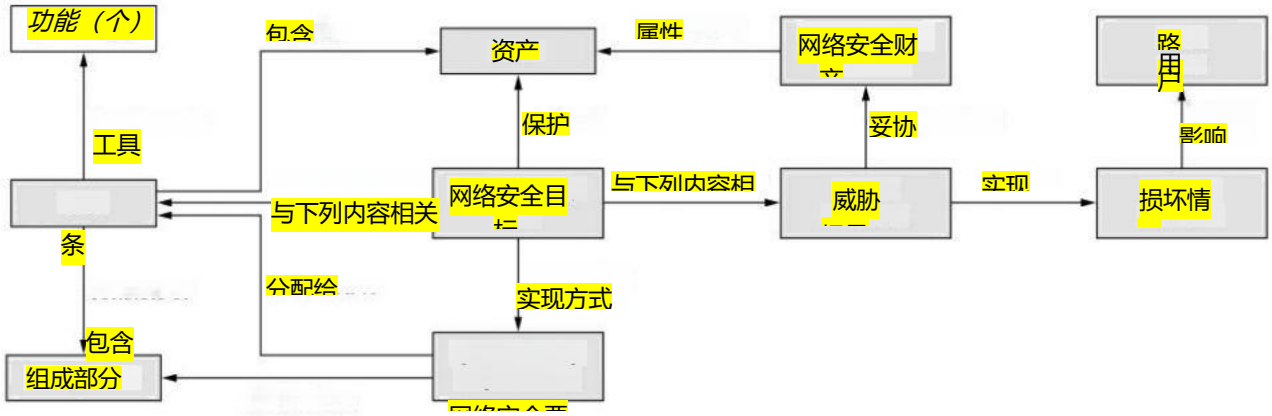


图3-项目、功能、组件和相关术语之间的关系

第15条描述了在其他条款所述网络安全活动中调用的评估网络安全风险的模块化方法。

网络安全工程中的分析活动旨在识别并探索抽象敌对行为者可能采取的恶意行动，以及这些行动可能导致车辆电子系统网络安全受损的程度。网络安全工程与其他学科的专业知识之间的协调，可以支持对特定网络安全风险的深入分析和缓解（参见ISO/TR 4804[6]）。网络安全监控、补救和事件响应活动作为应对措施，补充了概念和产品开发活动，承认环境条件的变化（例如新的攻击技术）以及持续识别和管理道路车辆电子系统中的弱点和漏洞的需求。

纵深防御方法可用于缓解网络安全风险。纵深防御方法利用多层网络安全控制来提高车辆的网络安全。如果攻击能够渗透或绕过一层，另一层可以帮助遏制攻击并保持资产的安全保护。

5组织网络安全管理

5.1概述

为了实现网络安全工程，组织制定并维护网络安全治理 和 a 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。这包括规定组织规则和流程，这些规则和流程将根据本文件的目标进行独立审计。

为支持网络安全工程，组织实施网络安全管理系统，包括管理工具和应用质量管理体系。

5.2目标

本条款的目的在于：

a）制定网络安全政策和网络安全的组织规则和流程；

b）分配执行网络安全活动所需的责任和相应权限；

c)支持网络安全的实施，包括提供资源和管理网络安全过程与相关过程之间的相互作用；

d)管理网络安全风险；

e）建立并保持网络安全文化，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共享；

g)建立和维护支持网络安全维护的管理体系；

h）提供证据证明工具的使用不会对网络安全产生不利影响；

i)执行组织网络安全审计。

5.3输入

5.3.1先决条件

没有一个

5.3.2进一步支持性资料

可考虑以下信息：

-符合支持质量管理标准的现有证据。

样例　　IATF 16949 [Z]与ISO 9001[B]、ISO 10007 [2]、汽车SPICE®1)相结合，ISO/IEC330xx系列标准[10]、ISO/IEC/IEEE15288 1和ISO/IEC/IEEE 12207[12]。

5.4要求和建议

5.4.1网络安全治理

[RQ-05-01]该组织应制定网络安全政策，包括：

a)承认道路车辆网络安全风险；以及

b）执行管理层对管理相应网络安全风险的承诺。

注1：网络安全政策可以包括组织目标和其他政策的链接。

注2网络安全政策可以包括关于组织产品或服务组合中通用威胁场景的风险处理的声明，考虑到外部或内部环境。

[RQ-05-02]本组织应制定并维护以下规则和流程：

a)使本文件的要求得以实施；以及

b）支持相应活动的执行。

示例1：过程定义、技术规则、指南、方法和模板。

注3：网络安全风险管理可包括活动的投入-收益考虑。

注4：规则和流程涵盖概念、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：漏洞披露的相关规则和流程，例如作为信息共享的一部分，可按照ISO 29147 [14]进行规定。

1）汽车香料®[13]是市面上可买到的合适产品的例子。提供此信息是为了方便本文件的使用者，并不构成ISO对这些产品的认可。

注释6图4概述了总体网络安全政策（见[RQ-05-01]）、组织特定的网络安全规则和流程（见[RQ-05-02]）、责任（见[RQ-05-03]）和资源（见[RQ-05-04])之间的关系。

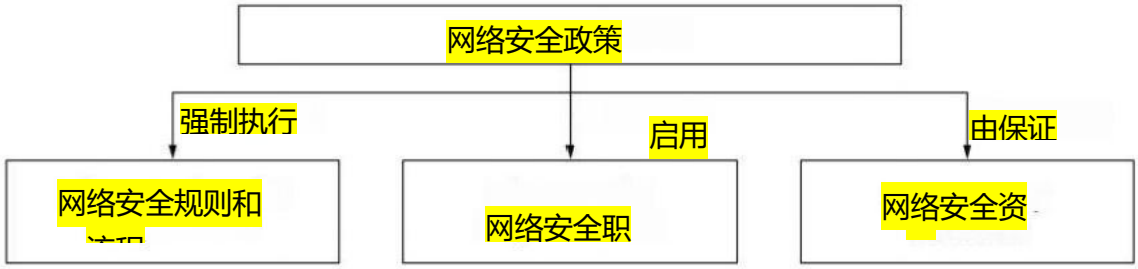


图4-网络安全治理

[RQ-05-03]组织应分配和传达实现和维护网络安全的责任和相应的组织权限。

注7：这涉及到组织活动和项目相关活动。

[RQ-05-04]本组织应提供资源以应对网络安全问题。

注释8资源包括负责网络安全风险管理、开发和事件管理。

示例2：执行网络安全活动的熟练人员和合适的工具。

[RQ-05-05]本组织应确定与网络安全相关或相互作用的学科，并在这些学科之间建立和维护沟通渠道，以便：

a]确定网络安全是否以及如何融入现有流程；

b）协调有关信息的交换。

注9：协调可以包括在学科之间共享流程以及使用策略和工具。

注10：学科包括信息技术安全、功能安全和隐私。

示例3：跨学科交流：

一威胁情景和危害（参见ISO 26262-1：2018[1]，3.75）信息；

一网络安全目标和安全目标（参见ISO 26262-1：2018[1,3.139）；和/或

一网络安全要求与功能安全要求冲突或相互竞争（参见ISO 26262- 1：20181,3.69）。

5.4.2网络安全文化

[RQ-05-06]本组织应培养和维护强大的网络安全文化。

注1：示例见附录B。

[RQ-05-07]组织应确保被分配网络安全角色和职责的人员具备履行这些职责的能力和意识。

注2：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；

—与网络安全相关的纪律的组织规则和流程，如功能安全和隐私；

一领域知识；

一系统工程；

一与网络安全相关的各种方法、工具和准则；和/或

一已知的攻击方法和网络安全控制。

[RQ-05-08]本组织应建立并保持持续改进过程。

示例持续改进过程，包括：

一从以往的经验中学习，包括通过网络安全监控和观察内部和外部网络安全相关信息收集的网络安全信息；

一从与网络安全相关的、在该领域具有类似应用的产品的信息中学习；

一为后续网络安全活动提供改进；

一将网络安全方面的经验教训传达给相关人员；以及

一根据[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需要、允许或禁止与网络安全相关的信息共享的情况。

注：分享信息的情况可基于：

一可以共享的信息类型；

一分享的审批流程；

一编辑信息的要求；

一源代码归属规则；

一为特定方提供的通信类型；

一漏洞披露程序（参见5.4.1中的注释5）；和/或

一收件方对处理高度敏感信息的要求。

[RC-05-10]组织应根据[RQ-05-09]，将其共享数据的信息安全管理与其他方保持一致。

示例：公共、内部、机密、第三方机密等安全分类级别的对齐。

5.4.4管理体系

[RQ-05-11]本组织应根据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，解决以下问题：

示例1 IATF 16949[Z]与ISO 9001[81]联合使用。

a)变更管理；

注1：网络安全中的变更管理范围是管理项目及其组件的变更，以便适用的网络安全目标和要求继续fulfilled，e.g.a根据生产控制计划对生产过程中的变更进行审查，以防止此类变更引入新的漏洞。

b)documentation 管理

注2：工作产品可以合并或映射到不同的文档存储库。

c)配置管理；以及

d)requirements 管理

[RQ-05-12]为维护现场产品网络安全所需配置信息应一直保留到产品网络安全支持结束，以便采取补救措施。

注3：存档构建环境有助于确保以后使用配置信息。

示例2：物料清单、软件配置。

[RC-05-13]应建立生产过程的网络安全管理系统，以支持第12条所述的活动。

EXAMPLE3 IEC624432-1 [15].

5.4.5工具管理

[RQ-05-14]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，例如基于模型的开发、静态检查器、验证工具。

示例2生产过程中使用的工具，如闪存写入器、生产线末端测试仪。

示例3用于维护的工具，例如车载诊断工具或重新编程工具。

注释 可通过以下方式建立此类管理：

一用户手册的使用说明及勘误表；

一防止意外使用或操作；

一对工具用户的访问控制；和/或

一工具的身份验证。

[RC-05-15]支持网络安全事件补救措施的适当环境（见13.3）应可重复，直至产品网络安全支持结束。

示例4测试、软件构建和开发环境，用于重现和管理漏洞。

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

[RC-05-16]应根据信息安全管理体系对工作成果进行管理。

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

[RQ-05-17]应独立进行网络安全审计，以判断是否组织流程实现本文件的目标。

注1：网络安全审计可以包括在或与根据质量标准进行的审计相结合管理体系standard，e.g.IATF 16949[Z]与ISO 9001[8.

注2：独立性可以基于ISO 26262系列[16。

注3：执行审核的人员可以是组织内部或外部的人员。

注4：为确保组织流程仍适合网络安全，可定期进行审核。

注5图Z说明了组织网络安全审计与其他网络安全活动的关系。

5.5工作产品

[WP-05-01]网络安全政策、规则和流程，由5.4.1至5.4.3的要求产生

[WP-05-02]能力管理、意识管理的证据，源自[RQ-05-07]和5.4.2中[RQ-05-08]的持续改进

[WP-05-03]证明组织管理体系的证据，根据5.4.4和5.4.6的要求

[WP-05-04]工具管理的证据，由5.4.5的要求产生

[WP-05-05]组织网络安全审计报告，根据5.4.7的要求

6项目依赖的网络安全管理

6.1概述

本条款描述了针对特定项目网络安全开发活动管理的要求。

项目依赖的网络安全管理包括责任分配（见6.4.1）和网络安全活动的规划（见6.4.2）。本文件以通用方式定义了要求，以便适用于各种项目和组件。此外，可以根据理由进行定制（见6.4.3），并在网络安全计划中定义。可以使用定制的例子包括：

—重复使用（见6.4.4)，

—组件脱离上下文（见6.4.5)，

—使用现成组件（见6.4.6)，—更新（见13.4)。

重复使用项目和组件是一种可能的发展策略，可以应用于项目、组件或其操作环境，无论是否进行修改。然而，修改可能会引入原本未考虑的漏洞。此外，已知攻击方式也可能发生变化，例如：

—攻击技术的演变，

—新出现的来自网络安全监控（见8.3)和/或网络安全事件评估（见8.4）的vulnerabilities，e.g.learned，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件开发的，则该项目或组件的重复使用基于现有工作产品。如果项目或组件不是根据本文件开发的，则重复使用可以基于现有文档和理由。

组件可以在假设的上下文中开发out-of-context，i.e.based。组织可以在与客户签订合同或商业协议之前，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做出假设。基于此，供应商可以推导出非上下文开发的需求。例如，微控制器可以进行非上下文开发。

现成组件是指不是为特定客户开发的组件，可以不经修改其设计或implementation，e.g.a第三方软件库而使用，即开源软件组件。现成组件不假定是按照本文件开发的。

图5显示，根据本文件，现成组件和非上下文组件都可以集成到项目或组件中。集成过程可能涉及类似于6.4.4节中的重用分析活动，如果需要修改以解决无效假设，则适用变更管理（见5.4.4)。这些变更可以针对旨在集成的组件，也可以针对作为集成目标的组件或项目。

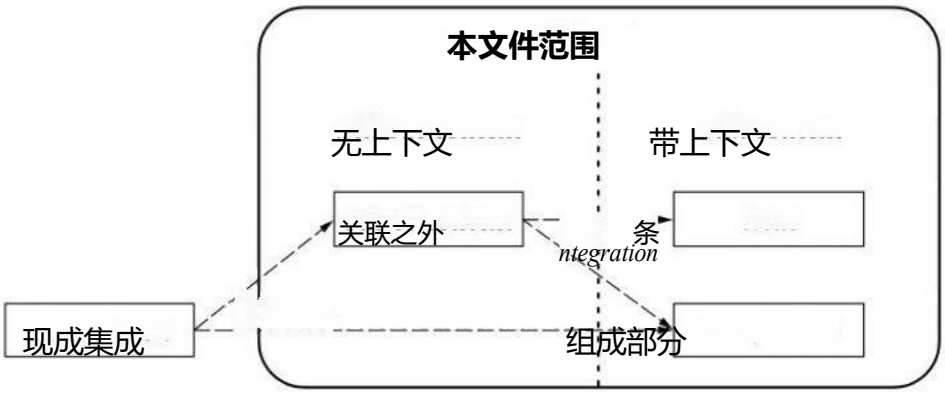


图5-现成组件和非上下文组件的集成

网络安全案例（见6.4.7）是网络安全评估和发布后开发的输入。

网络安全评估（见6.4.8）独立判断产品或组件的网络安全，是决定发布后开发的输入（见6.4.9)。

6.2目标

本条款的目的在于：

a）分配与项目网络安全活动相关的职责；

b)规划网络安全活动，包括定义定制网络安全活动；

c)创建网络安全案例；

d）如果适用，进行网络安全评估；以及

e)从网络安全的角度决定产品或组件是否可以发布到开发后。

6.3输入

6.3.1先决条件

没有一个

6.3.2进一步支持性资料

可考虑以下信息：

一组织网络安全审计报告[WP-05-03]；

一项目计划。

6.4要求和建议

6.4.1网络安全职责

[RQ-06-01]应根据[RQ-05-03]分配和传达与项目网络安全活动相关的责任。

注释　网络安全活动的责任可以转移，前提是必须进行沟通并且提供相关信息。

6.4.2网络安全规划

[RQ-06-02]为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)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：如果确定项目或组件与网络安全无关，则不存在网络安全活动，因此网络安全规划没有继续。

b）如果项目或组件与网络安全相关，那么该项目或组件是新开发的还是重复使用的；以及

C）是否采用6.4.3中的定制方法。

[RQ-06-03]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；

c)负责执行活动的人员；

d)执行活动所需资源；

e）活动的起始点或结束点，以及预期持续时间；

f）确定将要生产的工作产品。

[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网络安全活动进展的责任。

[RQ-06-05]网络安全计划应为：

a)项目开发计划中提及的；或

b）包含在项目计划中，使网络安全活动可区分。

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（另见[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，规定概念和产品开发阶段所需的网络安全活动。

[RQ-06-07]当确定了待执行活动的变更或细化时，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细化，例如，可根据网络安全活动的结果更新网络安全计划，如TARA（见第15条）。

[PM-06-08]根据15.8的分析确定的风险值为1的威胁场景，可省略第9.5、第10和第11条。

注5：这些威胁场景可能对网络安全产生影响，如果是这样，应对相应的风险，尽管可能不如本文件中规定的严格。

注6：根据网络安全案例中定义的原理，可以论证此类风险处理的充分性。该原理可以基于符合质量管理体系标准，例如IATF 16949[Z]与ISO 9001[8结合其他措施，例如：

—网络安全意识保障；

—质量人员的网络安全培训；和/或

—组织质量管理体系中定义的网络安全特定措施。

[RQ-06-09]网络安全计划中确定的工作产品应更新并维护，直至发布后开发阶段，以确保准确性。

[RQ-06-10]如果网络安全活动是分散的，客户和供应商应根据第7条各自定义与其各自的网络安全活动和接口有关的网络安全计划。

[RQ-06-11]网络安全计划应根据5.4.4进行配置管理和文档管理。

[RQ-06-12]网络安全计划中确定的工作产品应根据5.4.4进行配置管理、变更管理、需求管理和文档管理。

6.4.3定制

[PM-06-13]可以定制网络安全活动。

[RQ-06-14]如果网络安全活动是定制的，则应提供并审查定制是否充分且足以实现本文件相关目标的理由。

注：如果某项活动由供应链中的其他实体执行，则不视为定制，而是分布式网络安全活动（见第Z条）。但是，分布式网络安全活动可能导致联合定制（见7.4.3）。

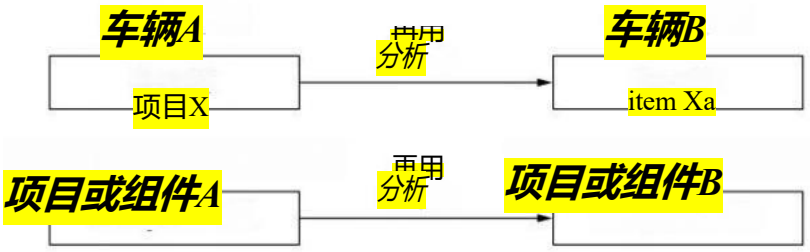
6.4.4重复使用

[RQ-06-15]如果已经开发了项目或组件，并且：则应进行重复使用分析：

a)计划进行修改；

b）计划在另一个操作环境中重复使用；或

示例1：由于现有项目或组件安装在新的操作环境中，或者由于与之交互的其他项目或组件升级而导致的环境修改（见图6）。



a可能因重复使用分析而改变。

图6-重复使用分析示例

c）计划在不作修改的情况下重复使用，且有关项目或组件的信息有相关变更。

示例2：已知攻击和漏洞的变化，或威胁场景的变化。

注1：在确定是否可以重复使用时，应考虑现有工作产品。

注2：修改可以包括设计修改和/或实施修改，其中：

—设计修改可以resultfromrequirementmodifications，e.g.functionalorperformance增强；

—实施修改可能源于软件的修正，或使用新的生产或维护tools，e.g.model-based开发。

注3：如果配置数据或校准数据的变更影响了产品的功能行为、资产或网络安全属性，则视为修改。

[RQ-06-16]项目或组件的重复使用分析应：

a）确定对项目或部件的修改以及对其运行环境的修改；

b)分析修改对网络安全的影响，包括对网络安全声明的有效性和先前做出的假设的影响；

示例3：对网络安全要求、设计和实施、运行环境、假设的有效性以及操作模式、维护、对已知攻击的易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 TARA考虑新资产或修改后的资产、威胁场景或风险值。

d）在网络安全计划中规定符合本文件要求的必要网络安全活动（见6.4.2)。

注4：这可能意味着定制（见6.4.3)。

[RQ-06-17]组件的重复使用分析应评估是否：

a）该组件能够满足其将要集成的项目或组件所分配的网络安全要求；以及

b）现有文件足以支持集成到一个项目或另一个组件中。

6.4.5组件脱离上下文

[RQ-06-18]应在相应工作产品中记录对脱离上下文开发的组件的预期用途和上下文的假设，包括外部接口。

[RQ-06-19]在开发组件时，网络安全要求应基于[RQ-06-18]中的假设。

[RQ-06-20]对于在非上下文中开发的组件的集成，应验证[RQ-06-18]中的网络安全声明和假设。

6.4.6现成组件

[RQ-06-21]在集成现成组件时，应收集和分析网络安全相关文档，以确定是否：

a）分配的网络安全要求可以得到满足；

b）该组件适用于预期用途的特定应用环境；以及

c）现有文件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件要求的网络安全活动。

示例：有关漏洞的文档不足。

注：这可能意味着定制（见6.4.3)。

6.4.7网络安全案例

[RQ-06-23]应创建网络安全案例，以提供项目或组件的网络安全论据，并由工作产品支持。

注1：如果论据的某部分从已编译的工作产品集中明显可见，则可以省略该论据的某部分）。

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，其中引用了各方生成的工作产品的证据。然后，项目的总体论点由各方的论据支持。
注3：网络安全案例考虑了开发后网络安全要求[WP-10-02]。

6.4.8网络安全评估

[RQ-06-24]应根据基于风险的方法制定理由，以决定是否对某项或某组件进行网络安全评估。

注1：依据可以是:

—TARA结果（见第15条）；

一待开发项目或组件的复杂性；和/或

一由组织规则和流程定义的标准（见5.4.1)。

注2：如果未进行网络安全评估，则可以在文件中记录理由
网络安全案例。

[RQ-06-25]应独立审查[RQ-06-24]的依据。

注3：独立性方案可基于ISO 26262系列[16]。

[RQ-06-26]网络安全评估应判断项目或组件的网络安全。

注4：可用证据由网络安全activities，i.e.the工作成果的文件化结果提供（见附录A）。

注5图Z说明了组织网络安全审计、项目级网络安全评估和其他网络安全活动之间的关系。

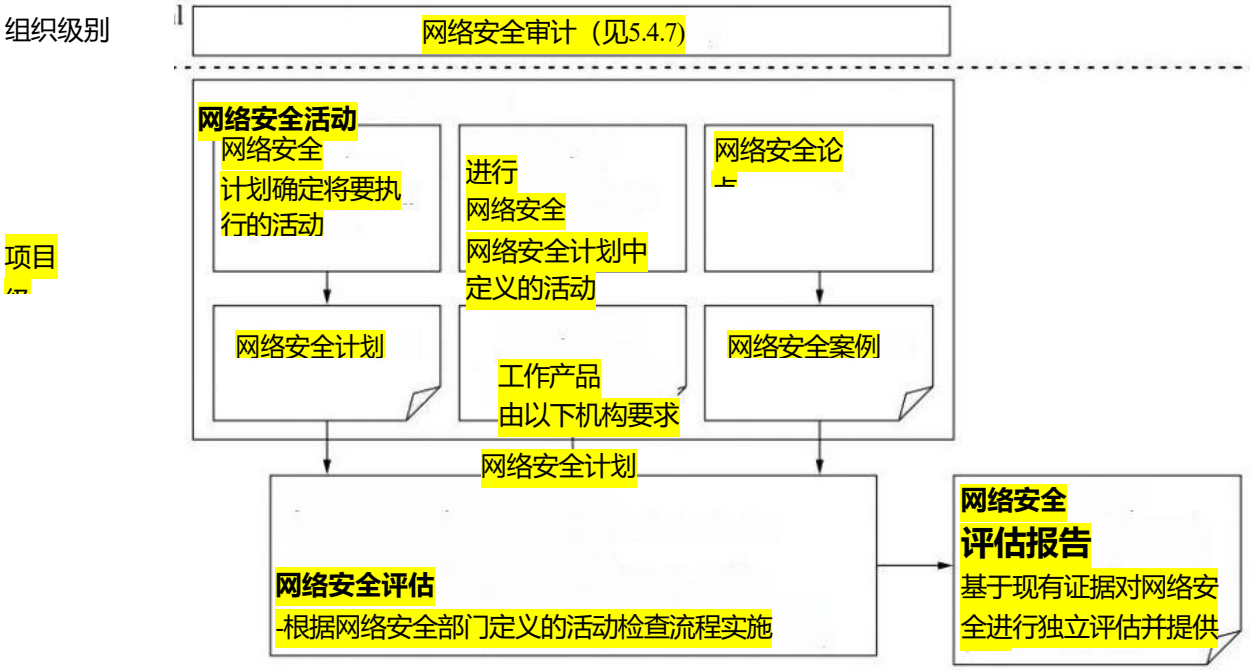


图7-网络安全评估与其他网络安全活动的关系

注6：可分步骤进行网络安全评估，以便尽早解决已识别的问题。

注7：如果先前的网络安全评估提供了否定建议，或者发现漏洞，则可重复或supplemented，e.g.due更改网络安全评估。

[RQ-06-27]应根据[RQ-06-01]任命负责独立规划和执行网络安全评估的人员。

注8：独立性方案可基于ISO 26262系列[16]。

样例　　来自组织内不同团队或部门的人员，如质量保证部，或独立组织的人员。

[RQ-06-28]执行网络安全评估的人员应具备：

a）获得相关信息和工具；

b）从事网络安全活动的人员的合作。

[PM-06-29]网络安全评估可基于是否实现本文件目标的判断。

[RQ-06-30]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措施和网络安全活动的适当性和有效性；以及

注9：可以通过使用先前的审查来判断其适当性和有效性用于验证目的。

d）如果提供了，证明实现本文件目标的理由。

注10：负责创建工作成果的人员可以提供理由，说明为何要实现本文档的相应目标，以便于进行网络安全评估，考虑[PM-06-13]。

注11：满足所有相应要求足以证明本文件的目标已实现。

[RQ-06-31]网络安全评估报告应包括对项目或组件的网络安全接受、有条件接受或拒绝的建议。

注12：评估报告也可以包括持续改进的建议。

[RQ-06-32]如果根据[RQ-06-31]提出有条件接受的建议，则网络安全评估报告应包括接受条件。

6.4.9发布后开发

[RQ-06-33]在发布后开发之前，应提供以下工作产品：

a)网络安全案例[WP-06-02]；

b）如适用，网络安全评估报告[WP-06-03]；以及

c）开发后网络安全要求[WP-10-02]。

[RQ-06-34]产品或组件的开发后放行应满足以下条件：

a)网络安全案例提供的网络安全论点是令人信服的；

b）如果适用，网络安全评估确认了网络安全情况；c）开发后阶段的网络安全要求被接受。

注释　　变更可能导致重新评估post-development，e.g.changes对网络安全声明的发布。

6.5工作产品

[WP-06-01]　网络安全计划，根据6.4.1至6.4.6的要求制定

[WP-06-02]　网络安全案例，由6.4.7的要求引起

[WP-06-03]　如适用，根据要求产生的网络安全评估报告　的6.4.8

[WP-06-04]　发布开发后报告，这是根据6.4.9的要求产生的

7个分布式网络安全活动

7.1概述

如果对某一项目或组件的网络安全活动分配了责任，则本条款适用。

本条款描述了分布式网络安全活动的管理，适用于：

a）分布式活动中开发的项目和组件；

b）客户与供应商之间的互动；以及

c）所有阶段，协议适用于客户/供应商接口。内部供应商可以与外部供应商以相同的方式进行管理。

例如，在开发过程中，一级组织可以是OEM的供应商，而在另一合同关系中，一级组织可以是二级组织的客户，以获得某个组件。如图8所示。

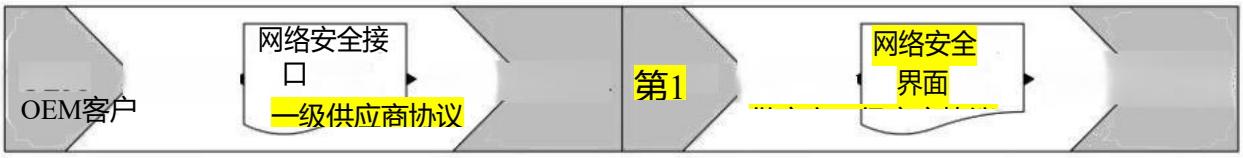


图8-供应链中客户/供应商关系的用例

7.2 目标

本条款的目的是定义交互、依赖和责任客户和供应商之间的分布式网络安全活动。

7.3输入

没有一个

7.4要求和建议

7.4.1供应商能力

[RQ-07-01]候选供应商开发和在适用情况下执行后评价的能力应评价根据本文件开展的开发活动。

注1：本评价支持供应商选择，可基于供应商符合本文件的能力，或基于对网络安全工程方面另一项国家或国际标准的先前实施的评价。

[RC-07-02]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记录。

注2：网络安全能力记录可包括：

一组织在网络安全方面的能力证据(e.g.cybersecurity开发、开发后、治理、质量和信息安全方面的最佳实践）；

一持续开展网络安全活动的证据（见第8条）和网络安全事件响应（见第13条）；以及

—以往网络安全评估报告的摘要。

7.4.2报价要求

[RQ-07-03]客户向候选供应商发出的报价请求应包括：

a）正式要求遵守本文件；

b）供应商按照第7.4.3条承担网络安全责任的预期；

c）网络安全目标和/或与供应商报价的项目或组件相关的网络安全要求。

样例　　与消息认证相关的网络安全要求。

7.4.3职责对齐

[RQ-07-04]客户和供应商应在网络安全接口协议中规定分布式网络安全活动，包括：

a）指定客户和供应商的网络安全联系点；

b）确定客户和供应商应分别执行的网络安全活动；

示例1：客户在车辆级别上执行的网络安全验证。

示例2：关于开发后网络安全活动的分布。

示例3关于由以下人员开发的组件或工作成果的网络安全评估

供应商可由第三方、客户或供应商执行。

c）如适用，根据第6.4.3条联合制定网络安全活动；

d）要共享的信息和工作成果；注1：共享的信息可以包括：

— 分发、审查和网络安全问题反馈机制；

— 漏洞和其他网络安全相关发现的信息交换程序，e.g.concerning风险；

— 确保客户与供应商之间兼容性的相关流程、方法和工具，例如正确处理数据以及保护用于传递数据的通信网络；

— 角色定义，

— 沟通和记录项目或组件变更的方法，包括可能重复TARA；

— 要求管理工具的一致性；和/或

— 网络安全评估结果。

e）分布式网络安全活动的里程碑；以及

f）项目或部件的网络安全支持结束定义。

[RC-07-05]客户和供应商应在分布式网络安全活动开始前就网络安全接口协议达成一致。

[RQ-07-06]如果存在需要按照[RQ-08-07]进行管理的已识别漏洞，客户和供应商应就这些行动以及对这些行动的责任达成一致。

[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，则客户和供应商应通知对方，以便采取适当的决策和行动。

[RC-07-08]责任应在责任分配矩阵中指定。

注2：ARASIC表可使用，见附录C。

7.5工作产品

[WP-07-01]网络安全接口协议，根据7.4.3的要求

8持续的网络安全活动

8.1概述

在整个生命周期的所有阶段都执行持续的网络安全活动，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，并根据定义的触发器分析网络安全信息，以便进行分类。

网络安全事件评估（见8.4）确定网络安全事件是否对项目或组件构成弱点。

漏洞分析（见8.5）检查弱点并评估特定弱点是否可被利用。

漏洞管理（见8.6）跟踪和监督项目和组件中已识别漏洞的处理，直至其网络安全支持结束。

8.2目标

本条款的目的在于：

a)监控网络安全信息，以识别网络安全事件；

b)评估网络安全事件，以识别弱点；

c)从弱点中识别漏洞；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：

-[WP-05-01]中包含的用于开发触发器的规则和流程。

8.3.1.2进一步支持性资料

可考虑以下信息：

—项目定义[WP-09-01]；

—网络安全声明[WP-09-04]；

—网络安全规范[WP-10-01]；—威胁场景[WP-15-03]；

—过去的脆弱性分析[WP-08-05]；

—从现场收到的信息。

示例漏洞扫描报告、修复信息、消费者使用信息。

8.3.2要求和建议

[RQ-08-01]应选择来源以收集网络安全信息。

注1：可选择内部和/或外部源。

注2：内部源可以包括8.3.1.2中列出的那些。

注3：外部来源可包括：

-研究人员；

—商业或非商业来源；

—组织的供应链；

—本组织的客户；和/或

—政府消息人士。

样例　　获取最先进的攻击方法。

[RQ-08-02]应定义和维护网络安全信息分类的触发器。

注4：触发器可以包括关键字、配置信息的参考、组件或供应商的名称。

[RQ-08-03]应收集网络安全信息并进行分类，以确定网络安全信息是否成为一种或多种网络安全事件。

8.3.3工作产品

[WP-08-01]网络安全信息来源，源自[RQ-08-01]

[WP-08-02]由[RQ-08-02]引发的触发器

[WP-08-03]网络安全事件，由[RQ-08-03]引起

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[WP-08-03]；

—适用的开发后网络安全要求[WP-10-02]；以及

—根据[RQ-05-12]的要求配置信息。

8.4.1.2进一步支持性资料

可考虑以下信息：

—项目定义[WP-09-01]；

—网络安全规范[WP-10-01]；—过去的漏洞分析[WP-08-05]。

8.4.2要求和建议

[RQ-08-04]应评估网络安全事件，以识别项目和/或组件中的弱点。

注1：此活动可与[RQ-08-03]的分诊相结合。

注2：如果存在漏洞并且有可用的补救措施（供应商为组件中的漏洞提供的e.g.a补丁），组织可以将补救措施（见8.6）视为假定漏洞，无需进行其他活动。

注3：威胁场景[WP-15-03]可根据本次评估的结果进行更新。

8.4.3工作产品

[WP-08-04] 网络安全事件导致的弱点，由[RQ-08-04]引起

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[WP-09-01]或网络安全规范[WP-10-01]。

注释 如果对项目执行漏洞分析，则使用该项目定义，且如果对组件执行漏洞分析，则使用网络安全规范。

8.5.1.2进一步支持性资料

可考虑以下信息：

一网络安全事件的弱点[WP-08-04]；

—在产品开发过程中发现的弱点[WP-10-05]；—过去的漏洞
分析[WP-08-05]；

—攻击路径[WP-15-05]；

—验证报告[WP-10-04]和[WP-10-07]；—来自过去
网络安全事件的信息。

8.5.2要求和建议

[RQ-08-05]应分析弱点，以确定漏洞。

注1：分析可包括：

架构一分析；

根据15.6进行一攻击路径分析；和/或

根据15.Z.对一攻击可行性进行评级。

注2：可进行根本原因分析，以确定可能导致弱点成为漏洞的任何潜在因素。

示例1攻击路径分析显示不存在攻击路径，因此，该弱点不被视为漏洞。

示例2：利用该弱点的攻击可行性评级非常低，因此，该弱点不被视为漏洞。
[RQ-08-06]应为未被确定为漏洞的弱点提供依据。

8.5.3工作产品

[WP-08-05]漏洞分析，源自[RQ-08-05]和[RQ-08-06]

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：

一漏洞分析[WP-08-05]。

8.6.1.2进一步支持信息

没有一个

8.6.2要求和建议

[RQ-08-07]应对漏洞进行管理，以便针对每个漏洞：

a）按照第15.9条对相应的网络安全风险进行评估和处理，以确保不存在任何不合理的风险；或

b）通过应用独立于TARA的可用补救措施消除漏洞。

样例　　开源软件补丁。

注1：如果漏洞管理导致项目或组件发生变更，则应根据[RQ-05-11]应用变更管理。

注2：漏洞信息可以在分布式网络安全活动的上下文中共享（参见Z.4.3，e.g.sharing对攻击路径的知识）并且可以与其他相关方共享（参见5.4.3）。

[RQ-08-08]如果根据第15.9条做出的风险处理决定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应用。

8.6.3工作产品

[WP-08-06]由[RQ-08-07]引起的受控漏洞证据

9概念

9.1概述

概念阶段涉及对车辆级功能的考虑，这些功能在项目中得以实现。在本条款中，项目及其运行环境被确定为“项目定义”（见9.3）。项目定义是后续活动的基础。

本条款还规定了项目网络安全目标（见第9.4条），这是最高级别的要求。为此，评估网络安全风险，通过使用第15条的方法来实现（另见附录H，图H.1）。此外，第9.4条还规定了网络安全声明，用于解释为什么认为保留或分担风险是适当的。

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，这两者均源自网络安全目标，并基于对项目的全面观点。

9.2目标

本条款的目的在于：

a)在网络安全的背景下定义项目、其运行环境及其相互作用；

b）规定网络安全目标和网络安全声明；以及

c)指定网络安全概念，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

没有一个

9.3.1.2进一步支持性资料

可考虑以下信息：

-有关项目和业务环境的现有信息。

样例　　车载电子/电子系统架构，包括车载网络、外部网络车辆；参考模型(s)和早期开发的文档。

9.3.2要求和建议

[RQ-09-01]应识别出关于该项目的以下信息：

a）项目边界；

注1：项目边界将项目与其操作环境区分开来。项目边界的描述可以包括与车辆内部其他项目和/或与车辆外部电子/电气系统的接口。

b)项功能；以及

注2：本说明描述了项目在生命周期阶段[e.g.product开发（测试）、生产、操作和维护、退役]期间的预期行为，并包括项目实现的车辆功能。

c）初步架构。

注3：初步架构的描述可以包括对项目组件的识别以及它们的连接和项目的外部接口。

注4：本文件中所述的项目定义，特别是项目边界，可能与根据ISO 26262系列l16的功能安全的其他discipline，e.g.such中的项目定义不同。注5：可以考虑有关约束和适用网络安全标准的信息。

注6：开发一个脱离上下文的组件（见6.4.5）可以基于对假定（通用）项目的定义和对项目内组件功能的描述。

[RQ-09-02]应描述与网络安全相关的项目操作环境信息。

注7：对作战环境及其与项目交互作用的描述，能够识别和/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assumptions，e.g.an假设项目所依赖的每个公钥基础设施证书颁发机构都得到适当管理。

9.3.3工作产品

[WP-09-01]　　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进一步支持性资料

可考虑以下信息：

一网络安全事件[WP-08-03]

9.4.2要求和建议

[RQ-09-03]应根据项目定义进行分析，包括：

a）按照15.3进行资产识别；

b）按照15.4识别威胁场景；

c)按照15.5规定的冲击等级；

d）按照15.6进行攻击路径分析；

e）按照15.7的规定进行攻击可行性评级；

f）按照15.8确定风险值。

注1：如果项目定义没有提供足够的分析信息，则可以假定这些信息。

[RQ-09-04]根据[RQ-09-03]的结果，应按照15.9为每个威胁场景确定风险处理选项。

注2：通过消除风险源来避免风险，可能会导致项目变更，因此需要按照变更管理进行变更（见5.4.4)。

[RQ-09-05]如果威胁场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网络安全目标是保护资产免受威胁场景影响的要求。

注4：如适用，可确定用于网络安全目标的CAL（见附录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。

[RQ-09-06]如果威胁场景的风险处理决策包括：

a）分担风险；或

b）如果由于在[RQ-09-03]分析过程中使用的一个或多个假设而保留风险，则应指定一个或多个相应的网络安全声明。

注6：可考虑将网络安全声明用于网络安全监控。

[RQ-09-07]应进行验证以确认：

a）关于项目定义，[RQ-09-03]的结果是否正确和完整；

b）[RQ-09-04]的风险处理决策与[RQ-09-03]的结果的完整性、正确性和一致性；

c）[RQ-09-05]的网络安全目标和[RQ-09-06]的网络安全声明与[RQ-09-04]的风险处理决策之间的完整性、正确性和一致性；以及

d）项目中[RQ-09-05]的所有网络安全目标和[RQ-09-06]的网络安全声明的一致性。

9.4.3工作产品

[WP-09-02] [WP-09-03]

[WP-09-04] TARA，源自[RQ-09-03]和[RQ-09-04]网络安全目标，源自[RQ-09-05]

网络安全声明，源自[RQ-09-06]

[WP-09-05]网络安全目标验证报告，源自[RQ-09-07]

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：

一项目定义[WP-09-01]；

一网络安全目标[WP-09-03]；以及

一网络安全声明[WP-09-04]。

9.5.1.2进一步支持性资料

可考虑以下信息：

一 TARA[WP-09-02].

9.5.2要求和建议

[RQ-09-08]应描述技术和/或操作网络安全控制及其相互作用，以实现网络安全目标，同时考虑：

a)项目功能之间的相互依赖关系；和/或

b)网络安全索赔。

注1：描述可以包括：

一实现网络安全的条件，包括对破坏的检测和监控，

—专门用于解决安全通信信道威胁scenarios，e.g.use的特定方面的功能。

注2：描述可用于评估设计和确定网络安全确认的目标。

[RQ-09-09]应根据[RQ-09-08]的描述，为网络安全目标定义项目和操作环境的网络安全要求。

注3网络安全要求可以取决于或包括项目的具体功能，例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之外实现，但它们包含在项目的网络安全确认中，以确认是否实现了相应的网络安全目标。

注5：作为运行环境一部分的其他项目的要求可以是网络安全要求。

[RQ-09-10]网络安全要求应分配给项目，如果适用，则应分配给一个或多个组件。

注6网络安全控制的描述补充了网络安全要求和对操作环境的要求的规范和分配，所有这些共同构成了网络安全概念。

[RQ-09-11]应验证[RQ-09-08]、[RQ-09-09]和[RQ-09-10]的结果，以确认：

a）与网络安全目标的完整性、正确性和一致性；以及

b)网络安全声明的一致性。

9.5.3工作产品

[WP-09-06]网络安全概念，源自[RQ-09-08]、[RQ-09-09]和[RQ-09-10]

[WP-09-07]网络安全概念验证报告，源自[RQ-09-11]

10产品开发

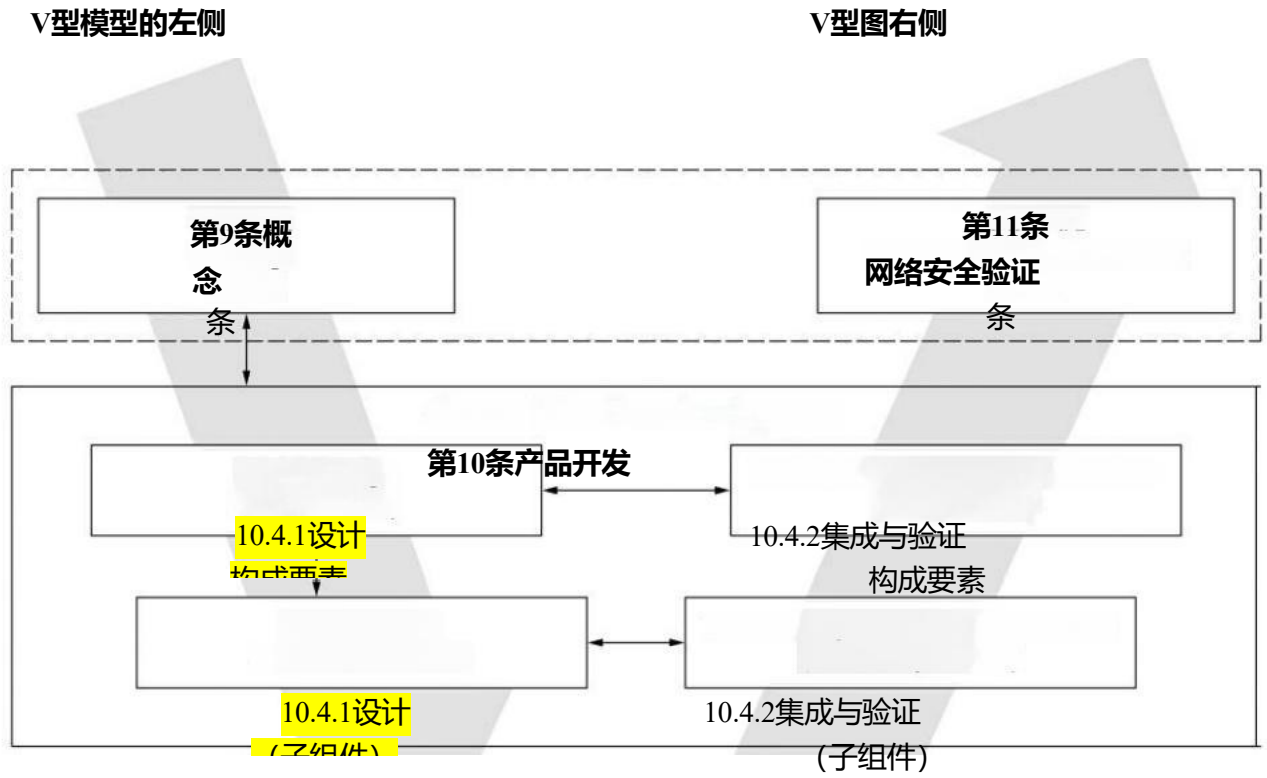
10.1概述

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，本条款描述了集成和验证活动（见10.4.2)。

这些网络安全活动会反复进行，直到不再需要进一步完善网络安全控制措施。网络安全规范是通过验证活动来定义和确认的，以确保网络安全概念的实现。

图9展示了如何将产品开发活动应用于基于V模型的工作流程，其中10.4.1对应V模型的左侧，10.4.2对应右侧。在这个例子中，在项目级别假设了两层抽象，即组件级别和子组件级别。此工作流可以扩展以涵盖任何级别的抽象。



钥匙

垂直双向箭头表示在设计过程中，根据10.4.1所述的网络安全规范，从更高层次的体系结构抽象进行验证。

水平双向箭头表示根据第10.4.2节所述网络安全规范对已实施和集成组件进行验证。

图9-V模型中的产品开发活动示例

可以应用不同于V-model(e.g.agile软件开发的开发方法或方法。

CAL可用于扩展本条款中活动的深度和严格程度以及用于这些活动的方法（见附录E）。

10.2目标

本条款的目的在于：

a)定义网络安全规范；

注1：这些可以包括不在中的网络安全相关组件的规范现有建筑设计。

b)验证定义的网络安全规范是否符合更高层次架构抽象的网络安全规范；

c）识别部件的弱点；

注2：漏洞分析和管理在第8条中进行了描述。

d）提供证据，证明组件的实施和集成结果符合网络安全规范。

10.3输入

10.3.1先决条件

应提供以下信息：

一来自更高层次的架构抽象的网络安全规范[WP-10-01]；

注1：这可以仅限于与正在开发的组件相关的信息，例如。

一分配给正在开发的组件的网络安全要求；

一正在开发的组件的外部接口规范；

一对开发中的组件的操作环境所作的假设信息。

注2：对于最高级别的架构抽象开发，使用项目网络安全概念[WP-09-06]和项目定义[WP-09-01]，而不是来自更高级别架构抽象的网络安全规范。

10.3.2进一步支持信息

可考虑以下信息：

一项目定义[WP-09-01]；

一网络安全概念[WP-09-06]；

一现有建筑设计；

-已经建立的网络安全控制；

-从重复使用的组件中发现的已知弱点和漏洞。

10.4要求和建议

10.4.1设计

[RQ-10-01]应根据以下内容定义网络安全规范：

a)来自更高层次的体系结构抽象的网络安全规范；

b）如果适用，选择实施的网络安全控制措施；以及

示例1：使用带有嵌入式硬件信任锚的独立微控制器来保护密钥存储功能和信任锚点对非安全外部连接的隔离。

注1：可以从可信目录中选择网络安全控制。

c）如适用，现有建筑设计。

注2：网络安全规范包括定义的架构设计相关子组件之间的接口规范，以满足定义的网络安全要求，包括其使用、静态和动态方面。

注3：在定义网络安全规范时，开发后阶段的网络安全影响可以是considered，e.g.secure密钥库管理；调试接口停用；删除个人身份信息的程序。

注4：网络安全规范可以包括与满足网络安全要求相关的配置和校准参数的识别，以及values，e.g.the正确配置的设置或允许范围，以便集成硬件安全模块。

注5：可考虑实施网络安全控制所必需的组件功能，例如。处理器性能，内存资源。

[RQ-10-02]定义的网络安全要求应分配给架构设计的组件。

[Q-10-03]如果适用，应规定确保组件开发后网络安全的程序。

示例2正确集成和初始化网络安全控制的程序，以及在整个生产过程中维护网络安全。

[RQ-10-04]如果使用设计、建模或编程符号或语言来描述网络安全规范或其实施，则在选择此类符号或语言时应考虑以下内容：

a)语法和语义上都明确且易于理解的定义；

b)支持实现模块化、抽象和封装；

c)支持使用结构化构造；

d)支持使用安全设计和实现技术；

e）整合现有组件的能力；以及

示例3：用另一种语言编写的库、框架和软件组件。

f)语言对因不当使用而产生的漏洞的恢复能力。

示例4：缓冲区溢出的容错能力。

注6：对于软件开发，实施包括使用编程语言进行编码。

[RQ-10-05]未在语言本身中解决的网络安全的合适设计、建模或编程语言的标准（见[RQ-10-04]）应由设计、建模和编码指南或开发环境涵盖。

示例5使用MISRAC：2012[17]或CERT C[18l在“C”编程语言中进行安全编码。

示例6适合的设计、建模和编程语言的标准：

一语言子集的使用；

一强类型化的实施；和/或

一使用防御性实施技术。

[RC-10-06]应采用已建立和信任的设计和实施原则，以避免或尽量减少引入弱点。

注7：网络安全架构设计原则示例见NIST特别出版物800-160第1卷[19J，附录F.1。

[RQ-10-07]应分析[RQ-10-01]中定义的架构设计，以识别弱点。注8：可考虑来自重复使用组件的已知弱点和漏洞。

注9：已识别的弱点将被分析为漏洞（见8.5），已识别的漏洞将被管理（见8.6)。但是，已识别的弱点可以通过对架构设计进行更改而得到解决，无需执行漏洞分析。

[RQ-10-08]应验证定义的网络安全规范，以确保其完整性、正确性和与更高层次架构抽象的网络安全规范的一致性。

注10：验证方法可包括：

—审查；

—分析；

—模拟；和/或

—原型设计。

10.4.2集成与验证

[RQ-10-09]集成和验证活动应验证组件的实现和集成是否符合规定的网络安全规范。

[RQ-10-10]应考虑以下因素，对[RQ-10-09]的集成和验证活动进行规定：

a)确定的网络安全规范；

b）如适用，适用于批量生产的配置；

c）具备足够的能力来支持定义的网络安全规范中规定的功能；以及

d）如适用，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：验证方法可包括：

—需求测试；

—接口测试；

—资源使用情况评估；

——控制流和数据流的验证；

—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，考虑以下因素：

—集成度水平，用于测试以实现验证目标；

—根据对选定测试的分析，在后续集成活动期间进行额外测试的必要性environment，e.g.due将目标处理器的数据字和地址字的不同位宽与处理器仿真或开发环境进行最终集成。

注4：测试用例的生成方法可以包括：

—需求分析；

—等价类的生成和分析；

—边界值分析；和/或

一基于知识或经验的错误猜测。

[RQ-10-11]如果采用测试验证，则应使用定义的测试覆盖率指标对测试覆盖率进行评估，以确定测试活动是否充分。

注5：标准测试覆盖范围指标可能不足以涵盖软件的cybersecurity，e.g.statement。

[RC-10-12]应进行测试，以确认组件中未识别的弱点和漏洞最小化。

注6：不必要的功能可能包含弱点。

注7：测试方法可包括：

—功能测试；

—漏洞扫描；

—粗略测试；和/或

—渗透测试。

注8：已识别的弱点将被分析为漏洞（见8.5），已识别的漏洞将被管理（见8.6)。但是，已识别的弱点可以通过对架构设计进行更改而得到解决，无需执行漏洞分析。

[RQ-10-13]如果未按照[RC-10-12]进行测试，则应提供理由。

注9：基本原理可包括以下考虑因素：

-访问组件攻击面的可行性；

—能够（直接或间接）访问组件并结合其他组件的损坏；和/或

—组件的简单性。

10.5工作产品

[WP-10-01]网络安全规范，源自[RQ-10-01]和[RQ-10-02]

[WP-10-02]开发后网络安全要求，由[RQ-10-03]产生

[WP-10-03]建模、设计或编程语言和编码的文档如适用，由[RQ-10-04]和[RQ-10-05]产生的指南

[WP-10-04]网络安全规范验证报告，源自[RQ-10-08]

[WP-10-05]产品开发过程中发现的弱点，由[RQ-10-07]和[RC-10-12]，如适用

[WP-10-06]集成和验证规范，源自[RQ-10-10]

[WP-10-07]集成和验证报告，由[RQ-10-09]、[RQ-10-11]和[RC-10- 12]产生

11网络安全验证

11.1概述

本条款描述了针对产品在车辆级的网络安全确认活动（见图9）。该产品在其操作环境中，与预期用于批量生产的配置一起，在车辆级进行考虑。

11.2目标

本条款的目的在于：

a)验证网络安全目标和网络安全声明；

b）确认项目实现网络安全目标；

c)确认不存在任何不合理风险。

11.3输入

11.3.1先决条件

应提供以下信息：

一项目定义[WP-09-01]；

一网络安全目标[WP-09-03]；以及

一适用的网络安全声明[WP-09-04]。

11.3.2进一步支持性资料

可考虑以下信息：

一网络安全概念[WP-09-06]；

一产品开发工作成果（见10.5)。

11.4要求和建议

[RQ-11-01]考虑系列生产配置的项目在车辆级别的确认活动应确认：

a）网络安全目标与威胁情景和相应风险的适当性；注1：如果在确认过程中发现网络安全目标未解决的任何风险，则可按照9.4进行解决。

b）实现本项网络安全目标；

C)网络安全声明的有效性；以及

d）如适用，操作环境要求的有效性。

注2：确认活动可包括：

一通过审查第9.5条和第10条的工作成果，确认实现网络安全目标；

一渗透测试，以证明网络安全目标的充分性和实现情况；和/或

一审查通过第9和第10条确定的所有受控风险。

注3：可使用注3 CAL来调整渗透测试的深度和严格程度（见附录E）。

注4：对[RQ-11-01]确认活动期间发现的弱点进行分析，以确定漏洞（参见8.5）并识别漏洞，进行管理（参见8.6)。

[RQ-11-02]应提供选择确认活动的依据。

11.5工作产品

[WP-11-01]确认报告，来源于[RQ-11-01]和[RQ-11-02]

12生产

12.1概述

生产涵盖产品或部件的制造和组装，包括车辆级别。创建生产控制计划以确保将开发后的网络安全要求应用于产品或部件，并确保在生产过程中不会引入漏洞。

12.2目标

本条款的目的在于：

a）将网络安全要求应用于开发后；以及

b）防止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：

—发布后开发报告[WP-06-04]；以及

—开发后网络安全要求[WP-10-02]。

12.3.2进一步支持性信息

没有一个

12.4要求和建议

[RQ-12-01]应创建生产控制计划，以应用开发后网络安全要求。

注1：生产控制计划可作为整体生产计划的一部分。

[RQ-12-02]生产控制计划应包括：

a）应用于开发后网络安全要求的一系列步骤；

b）生产工具、设备；

c）网络安全控制措施，以防止生产期间的未经授权的更改；以及

示例1防止对存放软件的生产服务器进行物理访问的物理控制。示例2应用加密技术和/或访问控制的逻辑控制。

d) 确认开发后网络安全要求得到满足的方法。

注2：方法可以包括检查和校准检查。

注3：制造产品或组件并安装硬件和软件时，生产过程可以使用特权访问。如果在生产后未经授权使用这种访问，则可能会在产品或组件中引入漏洞。

[RQ-12-03]应实施生产控制计划。

12.5工作产品

[WP-12-01]生产控制计划，来源于[RQ-12-01]和[RQ-12-02]

13运营和维护

13.1概述

本条款描述了网络安全事件响应（见13.3）以及对现场项目或组件的更新（见13.4）。

当组织将网络安全事件响应作为漏洞管理的一部分时，就会发生网络安全事件响应（请参阅第8.6节）。

更新是指在开发后对项目或组件进行的更改，可以包括额外的information，e.g.technical规范、集成手册和用户手册。组织可以针对各种reasons，e.g.addressing漏洞或安全问题发布更新，提供功能改进。与更新相关的工作产品作为其他条款的工作产品进行记录。

处于概念、产品开发或生产阶段的项目或组件的修改由变更管理（见5.4.4）涵盖，而不是本条款。

13.2目标

本条款的目的在于：

a）确定并实施网络安全事件的补救措施；以及

b）在生产后对项目或组件进行更新期间和之后，直至其网络安全支持结束，保持网络安全。

13.3网络安全事件响应

13.3.1输入

13.3.1.1先决条件

没有一个

13.3.1.2进一步支持性信息

可考虑以下信息：

一与导致网络安全事件的漏洞相关的网络安全信息

答复

—漏洞分析[WP-08-05]。

13.3.2要求和建议

[RQ-13-01]对于每起网络安全事件，应创建网络安全事件响应计划，其中包括：

a)补救措施；

注1：补救措施由第8.6节中的漏洞管理确定。

b)一份沟通计划；

注2：制定沟通计划可能涉及内部利益相关parties，e.g.marketing或公共关系、产品开发团队、法律、客户关系、质量管理、采购。

注3：沟通计划可以包括识别内部和外部沟通伙伴（e.g.development、研究人员、公众、当局）以及为这些受众开发特定信息。

c）分配补救措施的责任；注4：责任人可以有：

—对受影响项目或组件的专业知识，包括遗留项目和组件；

—组织的knowledge(e.g.business流程、沟通、采购、法律等）；和/或

—决策权。

d)记录与网络安全事件相关的新的网络安全信息的程序；注5：可根据8.3，e.g.information收集新的网络安全信息，包括：

—受影响的部件；

—相关事件和漏洞；

—法医数据，例如数据日志、碰撞传感器数据；和/或

—最终用户投诉。

e)确定进度的方法；

样例　　衡量进展的措施是：

— 得到补救的受影响项目或组件的百分比；和/或

— 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）关闭行动。

[RQ-13-02]应实施网络安全事件响应计划。

13.3.3工作产品

[WP-13-01]　　网络安全事件响应计划，源自[RQ-13-01]

13.4更新

13.4.1输入

13.4.1.1先决条件

应提供以下信息：

—发布后开发报告[WP-06-04]。

13.4.1.2其他支持性资料

可考虑以下信息：

—网络安全事件响应计划[WP-13-01]；

—与更新相关的开发后网络安全要求[WP-10-02]。

13.4.2要求和建议

[RQ-13-03]应根据本文件开发车辆内的更新和与更新相关的能力。

13.4.3工作产品

没有一个

14网络安全支持和退役结束

14.1概述

退役与网络安全支持结束不同。组织可以终止对某个项目或组件的网络安全支持，但该项目或组件仍可在现场按设计运行。退役和网络安全支持结束都可能带来网络安全影响，但这些影响被视为单独的事项。

退役可能在组织不知情的情况下发生，而且以无法强制执行退役程序的方式进行，因此，退役行为不在本文档的范围内。

在概念和产品开发阶段考虑网络安全支持的结束和退役。

14.2目标

本条款的目的在于：

a)通知网络安全支持结束；以及

b）能够对网络安全项目和组件进行退役。

14.3网络安全支持结束

14.3.1输入

没有一个

14.3.2要求和建议

[RQ-14-01]当组织决定终止对某项产品或组件的网络安全支持时，应创建一个程序与客户进行沟通。

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：可向车辆所有者发布通知。

14.3.3工作产品

[WP-14-01]与[RQ-14- 01]相关的网络安全支持结束的沟通程序

14.4停运

14.4.1输入

14.4.1.1先决条件

应提供以下信息：

—开发后网络安全要求[WP-10-02]。

14.4.1.2其他支持性资料

没有一个

14.4.2要求和建议

[RQ-14-02]应提供与退役相关的开发后网络安全要求。

注：与这些要求相关的适当documentation(e.g.instructions、用户手册）可使网络安全方面的停运成为可能。

14.4.3工作产品

没有一个

15威胁分析和风险评估方法

15.1概述

本条款描述了确定道路使用者受威胁情景影响程度的方法。这些方法及其成果统称为威胁分析与风险评估（TARA），是从受影响的道路使用者的角度进行的。本条款中定义的方法是通用模块，可以系统地调用，并且可以在项目或组件生命周期的任何阶段调用：

—资产识别（见15.3)；

-威胁情景识别（见15.4 ）；-影响评级（见15.5 ）；

一攻击路径分析（见15.6 ）；

一攻击可行性评级（见15.7Z);

-风险价值确定（见15.8）；以及-风险处

理决策（见15.9)。

由于这些是通用模块，本条款中定义的工作产品被记录为其他条款中产生的工作产品的组成部分。

有关这些方法的实例，请参见附录H。

可以应用特定于组织的冲击评级、攻击可行性评级和风险值确定量表，并将其映射到本文件中定义的相应量表。

15.2目标

本条款的目的在于:

a)识别资产、其网络安全属性和损坏场景;

b)确定威胁场景;

c)确定损坏情景的影响等级;

d)识别实现威胁场景的攻击路径;

e)确定攻击路径的利用难易程度;

f）确定威胁场景的风险值;

g）为威胁场景选择适当的风险处理选项。

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:

一项目定义[WP-09-01]。

15.3.1.2其他支持性资料

可考虑以下信息:

一网络安全规范[WP-10-01]

15.3.2要求和建议

[RQ-15-01]应确定损坏情况。

注1：损坏情况可包括：

-项目功能与不良后果之间的关系；

一对道路使用者的伤害描述；和/或

一相关资产。

[RQ-15-02]应识别具有网络安全属性的资产，其破坏会导致损害场景。

注2：资产的识别可基于：

—分析项目定义；

—进行冲击评级；

-从威胁场景中推导出资产；和/或

—使用预定义的目录。

示例1：资产是存储在信息娱乐系统中的个人信息（客户个人偏好），其网络安全属性是保密性。损坏场景是由于保密性的丧失而导致的未经客户同意披露个人信息。

示例2：资产为制动功能的数据通信，其网络安全属性为完整性，损坏场景为车辆高速行驶时意外全制动导致与后车发生碰撞（追尾）。

15.3.3工作产品

[WP-15-01] 由[RQ-15-01]导致的损坏情况

[WP-15-02]具有网络安全属性的资产，源自[RQ-15-02]

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其他支持性资料

可考虑以下信息：

—网络安全规范[WP-10-01]；

—损坏场景[WP-15-01]；

—具有网络安全属性的资产[WP-15-02]。

15.4.2要求和建议

[RQ-15-03]应识别威胁场景，包括：目标资产；

—损害资产的网络安全属性；以及——导致网络安全属性受损的原因。

注1：可以包括或与威胁scenario，e.g.damage情景、资产、攻击者、方法、工具和攻击面之间的技术相互依赖性相关联的更多信息。

注2：威胁情景识别方法可以采用小组讨论和/或系统方法，例如：

一从合理可预见的误用和/或滥用中引出恶意用例;

一基于frameworkssuchasEVITA[201，TVRA[211，PASTA[22，STRIDE（欺骗、篡改、否认、信息泄露、拒绝服务、提升权限）的威胁建模方法。

注3：一种损坏情形可以对应多种威胁情形，而一种威胁情形可导致多重损坏场景。

样例　对制动ECU的CAN消息进行欺骗会导致CAN消息的完整性丢失从而导致制动功能的完整性丧失。

15.4.3工作产品

[WP-15-03]　由[RQ-15-03]导致的威胁场景

15.5影响评级

15.5.1输入

15.5.1.1先决条件

应提供以下内容:

一损坏场景[WP-15-01]。

15.5.1.2其他支持性资料

可考虑以下信息:

一项目定义[WP-09-01];

一具有网络安全特性的资产[WP-15-02]。

15.5.2要求和建议

[RQ-15-04]应针对道路使用者在安全、财务、运营和隐私（S、F、O、P）影响类别中可能产生的不利后果，对损坏情景进行评估。

注1：本文件未提供不同影响类别之间的关系（e.g.weighting）。

注2：可考虑其他影响类别。

注3：如果考虑了其他影响类别，则应说明这些类别的依据和解释可按照第7条的规定在供应链中共享。

[RQ-15-05]应确定每个撞击类别的损坏情景的影响等级，如下所示:

一严重;

一主要;

-中度；或

-可忽略不计。

注4：财务、运营和隐私相关影响可根据下表进行评级附件F.

[RQ-15-06]应根据ISO 26262-3：2018,6.4.3得出安全相关影响等级。

注5：附录E中的表E.1可用于将安全影响标准映射到影响等级。

注6：功能安全评估可为此目的重复使用。

[PM-15-07]如果损害情景导致了影响等级，并且可以论证其他影响类别的所有影响都被认为是不那么关键的，那么可以省略对该其他影响类别的进一步分析。

示例：损坏情况的安全影响被评定为“严重”，因此，未进一步分析该损坏情况的财务影响。

15.5.3工作产品

[WP-15-04] 由[RQ-15-04]至[RQ-15-06]

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[WP-10-01]；以及

注意：如果对项目执行攻击路径分析，则使用该项目定义。如果对组件执行攻击路径分析，则使用网络安全规范。

—威胁场景[WP-15-03]。

15.6.1.2其他支持性资料

可考虑以下信息：

—网络安全事件的弱点[WP-08-04]；

—产品开发期间发现的弱点[WP-10-05]；—架构设计；

—如果可用，先前确定的攻击路径[WP-15-05]；

—漏洞分析[WP-08-05]。

15.6.2要求和建议

[RQ-15-08]应分析威胁场景，以确定攻击路径。

注1：攻击路径分析可基于：

-自上而下的方法，通过分析威胁场景可能的realised，e.g.attack树、攻击图的不同方式来推导攻击路径；和/或

—从上至下的方法，从已识别的漏洞构建攻击路径。

注2：如果部分攻击路径没有导致威胁场景的实现，则可以停止对该部分攻击路径的分析。

[RQ-15-09]应将攻击路径与攻击路径可实现的威胁场景相关联。

注3：在产品开发的早期阶段，攻击路径通常不完整或不精确，因为具体实现细节尚未确定，无法识别特定漏洞。在产品开发过程中，随着更多信息的获得，攻击路径可以更新为available，e.g.after漏洞分析。

样例

—威胁场景：对制动ECU的CAN消息进行欺骗，导致CAN消息的完整性丢失，从而导致制动功能的完整性丢失。

—实现上述威胁场景的攻击路径：

i.通过蜂窝接口，远程信息处理ECU受到破坏；

ii.通过来自远程信息处理ECU的CAN通信，网关ECU被破坏；

iii.网关ECU转发恶意制动请求信号（不想要的快速减速）。

15.6.3工作产品

[WP-15-05]　　攻击路径，由[RQ-15-08]和[RQ-15-09]得出

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其他支持性资料

可考虑以下信息：

—建筑设计；

—漏洞分析[WP-08-05]。

15.7.2要求和建议

[RQ-15-10]对于每条攻击路径，应按照下述内容确定攻击可行性评级：

表1.

表1-攻击可行性评级和相应描述

攻击可行性评级	描述
高	攻击路径可以利用低工作量完成。

中等	攻击路径可以利用中等努力完成。
低	攻击路径可以通过高工作量来实现。
极低	攻击路径的实现需要付出极大的努力。

[RC-15-11]应根据以下方法之一定义攻击可行性评级方法：

a)基于攻击潜力的方法；

b）基于CVSS的方法；或

c)基于攻击向量的方法。

注1：方法的选择可取决于生命周期中的阶段和可用信息。

[RC-15-12]如果采用基于攻击可能性的方法，应根据包括以下核心因素确定攻击可行性评级：

a)已经的时间；

b)专业技能；

c)产品或部件的知识；

d)机会之窗；以及

e)设备。

注2：核心攻击潜在因素可从ISO/IEC 18045[23]中得出

注3 G.2提供了基于攻击潜力确定攻击可行性的指南。

[RC-15-13]如果使用基于CVSS的方法，应根据基础度量组的可利用性度量确定攻击可行性评级，包括：

a)攻击向量；

b)攻击复杂性；

c)所需特权；以及

d)用户交互。

注4 G.3提供了基于CVSS方法确定攻击可行性的指南。

[RC-15-14]如果采用基于攻击向量的方法，应根据评估攻击路径的主要攻击向量（参见CVSS[24]2.1.1）来确定攻击可行性评级。注5 G.4提供了基于攻击向量方法确定攻击可行性的指南。注6在development(e.g.concept阶段的早期，当信息不足以识别具体攻击路径时，基于攻击向量的方法可以适合作为评估攻击可行性的手段。

15.7.3工作产品

[WP-15-06]攻击可行性评级，来源于[RQ-15-10]

15.8风险值确定

15.8.1输入

15.8.1.1先决条件

应提供以下信息：

一威胁场景[WP-15-03]；

—影响评级及其相关影响类别[WP-15-04]；以及—攻击可行性评级

[WP-15-06]。

15.8.1.2进一步支持性信息

没有一个

15.8.2要求和建议

[RQ-15-15]对于每个威胁场景，应根据相关损害场景的影响和相关攻击路径的攻击可行性确定风险值。

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产生影响，则可以为每个影响评级单独确定一个风险值。

注2：如果威胁场景对应于多个攻击路径，则可以适当aggregated，e.g.the威胁场景被分配相应攻击路径的攻击可行性评级的最大值。

[RQ-15-16]威胁场景的风险值应为1和5之间的值（包括1和5），其中1表示风险最小。

样例　　风险值确定方法：

-风险矩阵；

—风险公式。

15.8.3工作产品

[WP-15-07]　　风险值，由[RQ-15-15]和[RQ-15-16]得出

15.9风险处理决策

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]；

—威胁场景[WP-15-03]；以及

—风险值[WP-15-07]。

15.9.1.2其他支持性资料

可考虑以下信息：

—网络安全规范[WP-10-01]；

—项目或组件的先前风险处理决策，或类似项目或组件的先前风险处理决策；—影响评级和相关影响类别[WP-15-04]；

—攻击路径[WP-15-05]；

—攻击可行性评级[WP-15-06]。

15.9.2要求和建议

[RQ-15-17]对于每个威胁场景，考虑到其风险值，应确定以下一个或多个风险处理选项：

a)避免风险；

示例1：通过消除风险源，决定不开始或继续进行来避免风险产生风险的活动。

b)降低风险；

c)分担风险；

例如：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：保留风险和分担风险的理由被记录为网络安全索赔，并且应根据第8条接受网络安全监控和漏洞管理。

15.9.3工作产品

[WP-15-08]风险处理决策，源自[RQ-15-17]

附件A
提供信息的

网络安全活动和工作成果摘要

A.1概述

表A.1提供了网络安全活动及其相应工作成果的概要。这有助于组织管理这些活动，确保涵盖所有网络安全活动，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，这些活动的工作成果属于网络安全评估的范围。第15条列出的所有工作成果在其他条款中均作为工作成果记录。

A.2网络安全活动和工作成果概述

表A.1-本文件的网络安全活动和工作成果

子条款	工作产品
组织网络安全管理	
5.4.1Cybersecurity治理	[WP-05-01]网络安全政策、规则和流程
5.4.2网络安全文化	[WP-05-01]网络安全政策、规则和流程 [WP-05-02]能力管理、意识管理和持续改进的证据
5.4.3信息共享	[WP-05-01]网络安全政策、规则和流程
5.4.4管理体系	[WP-05-03]组织管理体系的证据
5.4.5工具管理	[WP-05-04]工具管理证据
5.4.6信息安全管理工作	[WP-05-03]组织管理体系的证据
5.4.Z组织网络安全审计	[WP-05-05]组织网络安全审计报告
项目依赖的网络安全管理	
6.4.1网络安全职责	[WP-06-01]网络安全计划
6.4.2网络安全规划	[WP-06-01]网络安全计划
6.4.3定制	[WP-06-01]网络安全计划
6.4.4重复使用	[WP-06-01]网络安全计划
6.4.5组件脱离上下文	[WP-06-01]网络安全计划
6.4.6现成组件	[WP-06-01]网络安全计划
6.4.Z网络安全案例	[WP-06-02]网络安全案例
6.4.8网络安全评估	[WP-06-03]网络安全评估报告
6.4.9发布后开发	[WP-06-04]发布后开发报告
分布式网络安全活动	
Z4.1供应商能力	没有一个

Z4.2报价请求	没有一个
7.4.3职责对齐	[WP-07-01]网络安全接口协议
持续的网络安全活动	

表A.1（续）

子条款	工作产品
8.3网络安全监控	[WP-08-01]网络安全信息来源[WP-08-02]触发因素 [WP-08-03]网络安全事件
8.4网络安全事件评估	[WP-08-04]网络安全事件的弱点
8.5漏洞分析	[WP-08-05]漏洞分析
8.6漏洞管理	[WP-08-06]管理漏洞的证据
概念阶段	
9.3项目定义	[WP-09-01]项目定义
9.4网络安全目标	[WP-09-02]TARA [WP-09-03]网络安全目标 [WP-09-04]网络安全声明 [WP-09-05]网络安全目标验证报告
9.5网络安全概念	[WP-09-06]网络安全概念 [WP-09-07]网络安全概念验证报告
产品开发阶段	
10.4.1设计	[WP-10-01]网络安全规范 [WP-10-02]开发后网络安全要求[WP-10-03]建模、设计或编程语言和编码准则 [WP-10-04]网络安全规范验证报告[WP-10-05]产品开发期间发现的弱点
10.4.2集成与验证	[WP-10-05]产品开发期间发现的弱点[WP-10-06]集成和验证规范 [WP-10-07]集成和验证报告
第11条网络安全确认	[WP-11-01]确认报告
开发后阶段	
第12条生产	[WP-12-01]生产控制计划
13.3网络安全事件响应	[WP-13-01]网络安全事件响应计划
13.4更新	没有一个
14.3网络安全支持结束	[WP-14-01]通报网络安全支持结束的程序
14.4停运	没有一个
威胁分析和风险评估方法	
15.3资产识别	[WP-15-01]损伤情景 [WP-15-02]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影响评级	[WP-15-04]影响评级和相关影响类别

15.6攻击路径分析	[WP-15-05]攻击路径
15.7攻击可行性评级	[WP-15-06]攻击可行性评级
15.8风险值确定	[WP-15-07]风险值
15.9风险处理决策	[WP-15-08]风险处理决策

附件B
提供信息的

网络安全文化实例

表B.1提供了弱和强网络安全文化的例子。

表B.1-弱和强网络安全文化的例子

表明a的示例 薄弱的网络安全文化	表明a的示例 强大的网络安全文化
与网络安全相关的决策的问责制是不可追溯的。	该过程确保与网络安全相关的决策的问责制是可追溯的。
（实施的功能或特性）的性能、成本或进度优先于网络安全	网络安全和安全是最重要的。
奖励制度更注重成本和时间安排，而不是网络安全。	奖励制度支持并激励有效实现网络安全，并惩罚那些采取危害网络安全的捷径的人。
网络安全人员强制要求严格遵守网络安全，而不考虑项目/活动的具体需求。	网络安全人员是榜样，他们对适当性和实际实施有良好的感觉，这使整个组织信任他们的行动。
评估网络安全及其管理过程的人员受到负责执行这些过程的人的不当影响。	该流程提供了充分的制衡，例如网络安全评估的适当独立性。
对网络安全的消极态度，例如： -在开发结束时对测试的严重依赖； 没有为现场可能出现的弱点或事故做好准备； 一管理只有在有时才作出反应 生产、现场的网络安全事件，或者媒体对竞争对手的产品给予了大量关注。	积极主动的网络安全态度，例如： 在产品生命周期的最初阶段发现并解决网络安全问题（网络安全设计）； 该组织准备对现场的漏洞或事件做出快速反应。
未分配网络安全所需资源	分配了网络安全所需的资源。 熟练人员应具备与所分配活动相称的能力。

表B.1（续）

表明a的示例 薄弱的网络安全文化	表明a的示例 强大的网络安全文化
“群体思维”确认bias(i.e.uncritical接受或符合主流观点）。 “在组建评审小组时，为了确保预期的结果而对deck“(i.e.choose成员进行排序）” 防止潜在的分歧。 持不同意见的人会被排斥或被贴上“不是团队player“(e.g.uncooperative、不妥协、有毒的人”的标签。 异议会对绩效评估产生负面影响。 少数派持不同意见者被贴上或被视为“麻烦制造者”、“不合作的团队成员”或“吹哨blower“(i.e.agitator、不受欢迎的人或告密者”。 表达担忧的员工会感到害怕 弹回	该过程利用多样性作为优势： 在所有过程中寻求、重视和整合知识多样性； 反对使用多样性的行为受到抑制和惩罚。 支持沟通和决策渠道存在，管理层鼓励使用： 鼓励自我披露； 任何人（内部或 鼓励外部）潜在的脆弱性； 在该领域、在制造和开发其他产品的过程中，发现和解决过程仍在继续。
没有系统持续改进流程、学习周期或其他形式的经验教训。	持续改进是所有流程的组成部分。
流程是临时的或隐性的。	遵循定义、可追溯和受控的过程。

附件C
提供信息的
网络安全接口协议模板示例

C.1概述

如果不同的组织参与分布式网络安全活动，重要的是在不同的组织之间就责任、信息披露水平和每个里程碑的实现水平达成一致。

本附录根据[RQ-07-04]提供网络安全接口协议的示例模板。该模板提供了客户和供应商之间分布式网络安全活动的角色和职责定义指南（图C.1）。

还可以向模板添加其他信息，例如联系点、目标里程碑、协作方法或工具。

C.2示例模板

此示例模板中的列条目包括：

a)阶段：本文件的阶段；

b)工作成果：与分布式活动接口相关的本文件的工作成果；

c)文件参考：本文件的相关条款；

d)供应商：RASIC规定的供应商责任；

e）客户：RASIC规定的客户责任；

注1：模板使用RASIC来说明特定工作的职责分配组织间的产品。RASIC可以按以下方式使用：

— R（责任方）：负责开展活动的组织；

— A（负责的）：指有权在活动完成后批准该活动的组织；

S（支持）：将帮助负责活动的组织的组织；

— 我方（被告知）：获知活动进展和所做决定的组织；以及

C（咨询）：提供咨询或指导，但不积极参与活动的组织。

f）保密程度：供应商和客户就每个工作产品的保密性达成一致；

注2：可能的保密级别可以是：

— 高度机密：只有创建工作产品的组织才被允许访问它；

— 机密：允许客户和供应商访问工作产品；

与第三方保密：根据第5.4.3条，允许将本工作成果与授权的外部方共享；以及

—— 公开：工作成果可以不受任何限制地共享。

g）注释：有关组织之间谈判和讨论结果的补充信息。

阶段	工作产品	医生 ref.	供应商					客户					级别 机密性	评论
			R	A	S	I	C	R	A	S	I	C		
概念	项目定义													
	治疗分析和风险看法													
	网络安全概念													
	验证报告 网络安全概念													
产品发展	网络安全规范													

图C.1-网络安全接口协议模板示例

附件D
提供信息的

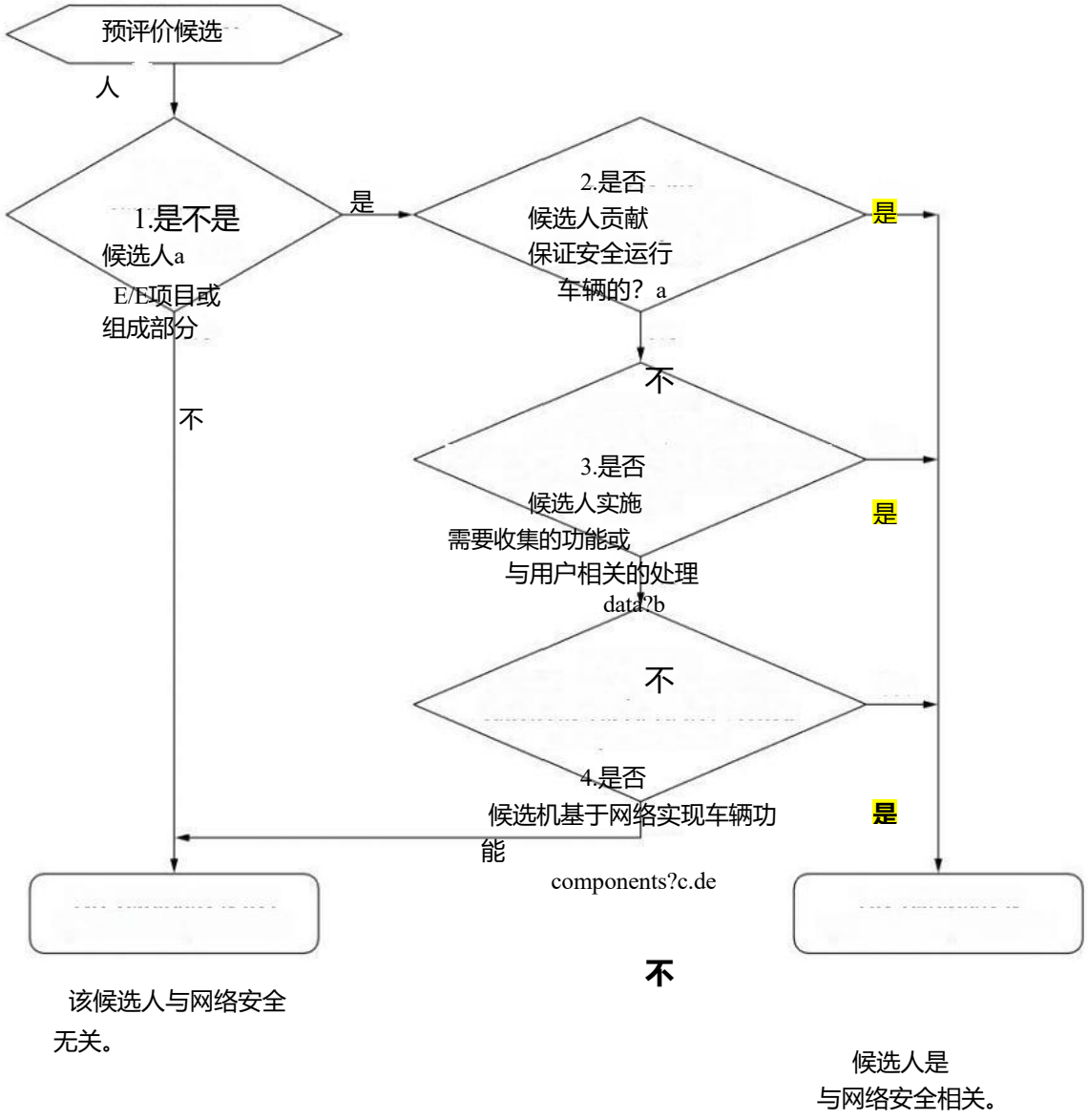
网络安全相关性-示例方法和标准

D.1概述

本附录提供了确定项目或组件是否与网络安全相关性的示例方法（参见[RQ-06-02]）。

D.2方法

可以使用图D.1中的决策图确定候选项目或组件的网络安全相关性，该决策图给出了示例标准。



一个例子　　运动控制模块和具有汽车安全完整性等级（ASIL）标识的模块。

b例　　与驾驶员或乘客有关的数据，或者与位置数据等潜在敏感信息有关的数据。

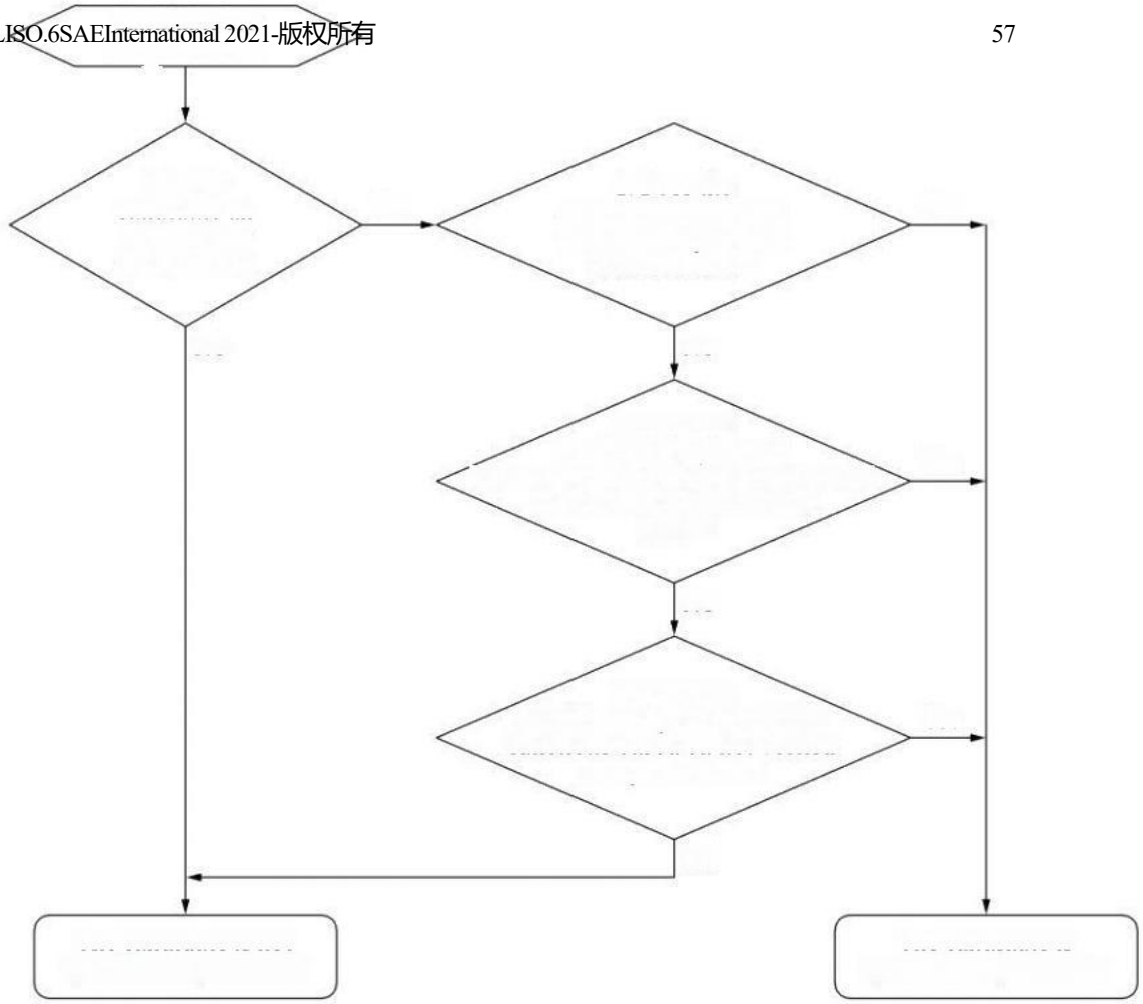
c例　　内部连接—CAN、以太网、媒体导向系统传输（MOST）、传输控制协议/互联网协议（TCP/IP）。

d示例　　外部连接——与后端服务器、蜂窝电信网络、车载的接口　　诊断（OBD-II）接口。

e例子　　无线　　连接传感器、执行器-远程无钥匙进入（RKE）、近场　　交流（NFC）、轮胎压力监测系统（TPMS）。

图D.1——网络安全相关性示例方法和标准

网络安全相关性也可以根据经验以及多位专家的判断来确定，包括e.g.involving安全专家和网络安全专家。



附件E
提供信息的

网络安全保证级别

E.1概述

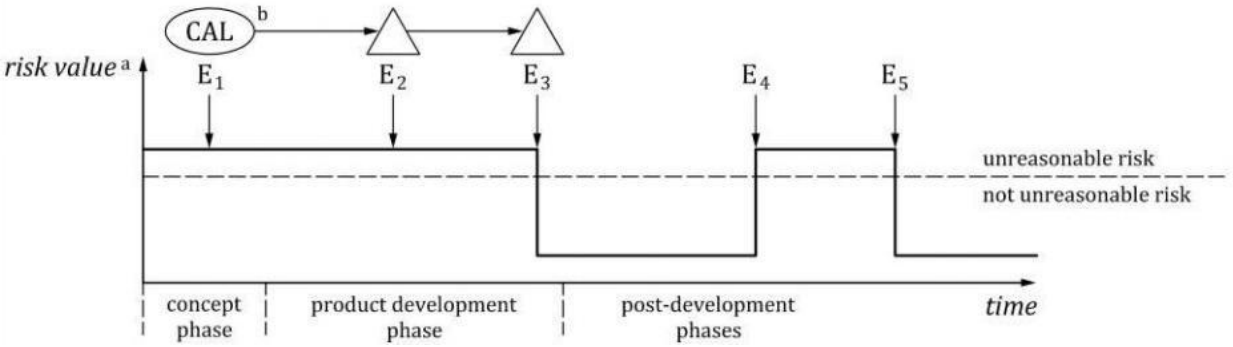
本附录描述了一种网络安全保证等级（CAL）分类方案，可用于规定和传达一组保证要求，以确保对项目或组件资产的保护措施已充分开发。此CAL分类方案不规定网络安全控制的技术要求，但可用于推动网络安全工程，为参与组织之间沟通网络安全保证要求提供共同语言。

CAL可由开发项目的组织确定，也可由在脱离上下文的情况下开发组件的组织假定。

一旦确定，CAL将规定后续产品开发活动所需的严格程度，以应对需要降低风险的威胁场景。这可以通过将CAL作为网络安全目标的一个属性来实现，该属性将被细化的网络安全要求所继承。

E.2确定CAL

CAL与风险间接相关；然而，它不能直接从风险值中确定。这是因为风险值是动态的，会随着时间的推移而变化，这取决于项目的规范、设计、实施和操作环境的演变，而CAL表示的是一个随时间保持不变的保证水平。因此，在开发初期的概念阶段可以使用预期在网络安全支持结束前一直稳定的参数来确定CAL，例如基于项目资产及其相关风险方面的参数，在考虑实施网络安全控制之前。CAL与相关风险之间的关系如图E.1所示。



钥匙

E1 事件1：规定了网络安全要求。

E2 事件2：实施网络安全控制。

E3 事件3：测试表明网络安全控制有效，事件4：现场发现漏洞。

E4 事件5：漏洞已修复。

E5 CALis应用于网络安全活动。

a 风险值是动态的，会根据当前规范、设计或实施情况而变化。

b 预期的保证水平atE1 given被保护资产的重要性规定了E2 、E3 后续网络安全活动的严格程度。

图E.1-CAL与风险之间的关系

CAL可以根据识别出的威胁场景（见15.4）来确定。表E.1给出了一个基于四个CAL的例子，每个CAL对应基于所使用的网络安全工程方法而增加的保证水平。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CAL。

表E.1-基于影响和攻击向量参数的示例CAL确定

		攻击向量b			
		物理	**本地**	**邻近**	**网络**
影响	严重	钙2	钙3	钙4	钙4
	主要的	钙1	钙2	钙3	钙4
	中度	钙1	钙1	钙2	钙3
	可忽略	--_a	---a	---a	---a
a见[PM-06-08]。 b攻击向量是攻击可行性的静态参数。					

在客户和供应商之间共享确定CAL的书面理由可以提高相互理解。CAL分类方案和确定的CAL也可以成为客户和供应商之间的网络安全接口协议的一部分。

可以将单个CAL分配给项目的所有网络安全目标，也可以将不同的CAL分配给每个网络安全目标。如果将网络安全目标组合在一起，则将最高级别的单个CAL分配给组合后的网络安全目标。

E.3使用CAL

E.3.1一般考虑

CAL分类方案可用于确定网络安全活动执行的严格程度，即提供所需保证所需的努力。

CAL可用于选择：

a）开发和验证所用的方法；

b）识别弱点和分析漏洞的方法；

c)网络安全评估方法。

表E.2提供了一些CAL的示例及其在概念和产品开发阶段使用时的指导。对于每次CAL的增加，相应的方法代表了设计、验证和网络安全评估对项目或组件保证的有意义提升。表E.2、E.3和E.4中的示例旨在让行业能够通过使用CAL来扩展本文档中描述的活动，从而获得实践经验。

表E.2-网络安全保证措施的CAL数量和预期严格度示例

克	**描述**	**a）提供网络安全活动以适当严谨性进行的信心的方法**	**b)提供对无人操作的信心的方法 已知漏洞不会持续存在**	**c）独立方案 提供信心 所执行的网络安全活动是否适当**
钙1	需要低至中等程度的网络安全保障	需求基础测试	基于已知信息进行漏洞搜索的分析和/或测试等活动	不需要
钙2	中度网络- 需要安全保证			网络安全评估由不同于发起人的人员执行
钙3	需要中等至高级的网络安全保障	对组件之间的所有相互作用进行测试	通过探索性方法进行分析和/或测试以查找漏洞的活动	网络安全评估由与发起人不同的团队的人员执行
钙4	需要高度的网络安全保障	对所有组件之间的相互作用组合进行试验		网络安全评估由独立于发起部门的人员进行，该人员不受管理、资源和发布权限的约束

E.3.2概念

本分条款提供了一个关于使用CAL分类方案以调整开发措施的严格性和范围的示例。

在概念阶段，随着网络安全概念的定义和网络安全要求分配到初步架构的组件，CAL可以作为[RQ-09-10]的扩展使用：

a)从网络安全目标派生的网络安全要求继承了该网络安全目标的CAL；

b)如果将从多个网络安全目标继承的、具有不同CAL的多个网络安全要求分配给一个体系结构组件，则该组件被分配的CAL为最高；

c)如果组件被确认为不受架构中其他组件的保护，则CAL根据理由，可以减少或取消分配给组件的任务。

E.3.3产品开发

在产品开发中应用CAL分类方案可以是使用依赖于CAL的方法和措施。

在产品开发中，如果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，则可以按照最高CAL为这些网络安全要求开发组件。

表E.3和E.4提供了如何将CAL应用于网络安全活动样本的示例；以类似方式可解决其他网络安全活动。

表E.3提供了一个例子，说明如何使用CAL来确定各自活动的独立性水平。

表E.3-网络安全活动独立性水平示例

活动	要求-ments	独立性水平适用于a				范围
		钙1	钙2	钙3	钙4	
网络安全概念和设计活动的验证	[RQ-09-11] [RQ-10-08]	I1	I1	I2	I2	在网络安全要求中应用最高CAL
验证组件的实现和集成	[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	12	I3	

符号定义如下：

一：未就该活动的独立性提出建议；

11：该活动由与负责创建所考虑工作产品(s)的人员相关的不同人员执行；

I2：该活动由独立于负责创建所考虑工作产品的团队的人员执行（s)，i.e.by向不同直接上级报告的人员；和

I3：该活动由一个独立于负责创建所考虑工作产品(s)的部门的人员执行，该人员在管理、资源和发布权限方面独立。

表E.4提供了如何使用CAL确定影响用于验证和确认的测试方法严格性的参数的示例。

表E.4—试验方法参数示例

活动	要求-ments	测试参数适用toa				范围
		钙1	钙2	钙3	钙4	
功能测试	[RC-10-12] [RQ-11-01]	T1	T1	T2	T2	适用于网络安全要求中的最高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	
渗透测试	[RC-10-12] [RQ-11-01]	—	—	T1	T2	

a符号定义如下：

一：未针对该活动的测试参数提出建议；

T1：测试参数集1：

—基于需求的功能测试；

—对已知漏洞进行漏洞扫描；

-对输入进行随机选择的模糊测试；

—penetration测试假设攻击者具有中等的专业知识、对项目或组件的了解和/或资源；T2：测试参数设置2：

—基于组件之间需求和交互的功能测试；

—对已知漏洞进行漏洞扫描；

-增加测试用例迭代次数和/或自适应选择输入的模糊测试；

—penetration测试假设攻击者具有更高的专业知识、对项目或组件的了解和/或资源

附件F
提供信息的
影响评级指南

F.1概述

本附录给出了涉及安全、财务、运营和隐私损害的损害场景影响评级标准（见15.5）的示例。本附录中的表格（见表F.1至表F.4）可用于影响评级。

关于损伤的可扩展性(i.e.impact在单一损伤场景中对多个道路使用者的影响）如何改变影响评级的考虑没有包含在给出的例子中，但可以根据需要添加到组织特定的评级标准中（e.g.Reference[20]，C.1.2，表4）。

F.2安全损坏影响等级

表F.1-安全影响等级标准示例

影响评级	安全性影响评级标准
严重	S3：危及生命的损伤（生存不确定），致命损伤
主要的	S2：严重和危及生命的损伤（可能存活）
中度	S1：轻度和中度损伤
可忽略	所以：无损伤a
SO的评级可基于ISO 26262-3：2018，表B.1。	

安全影响评级标准取自ISO 26262-3：2018。

如果提供了依据，也可根据ISO 26262-3：2018对可控性和暴露进行考虑，以评定其对安全性的影响。

F.3财务损失影响等级

表F.2-财务影响评级标准示例

影响评级	财务影响评级标准
严重	财务损失导致灾难性的后果，受影响的道路使用者可能无法克服。
主要的	财务损失将导致重大后果，受影响的道路使用者能够克服这些后果。
中度	财务损失导致不便的后果，受影响的道路使用者将能够用有限的资源克服。

可忽略	财务损失导致无影响、可忽略不计的后果或与道路使用者无关。

F.4操作损坏影响等级

表F.3-操作影响评级标准示例

影响评级	运营影响评级标准
严重	操作损坏导致核心车辆功能的丧失或受损。 示例1车辆无法工作或核心功能出现意外行为，例如启用故障恢复模式或自动驾驶至非预期位置。
主要的	操作损坏会导致重要车辆功能的损失或损坏。示例2：对驾驶员造成严重困扰：
中度	操作损坏导致车辆功能部分退化。示例3用户满意度受到负面影响。
可忽略	操作损坏不会导致车辆功能的任何损伤或不可察觉的损伤。

这些标准可能也有或没有安全后果。

F.5隐私损害影响等级

表F.4-隐私影响评级标准示例

影响评级	隐私影响评级标准
严重	隐私损害对道路使用者造成重大甚至不可逆转的影响，有关道路使用者的信息高度敏感且容易与PII主体关联。
主要的	隐私损害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，难以与PII主体联系起来；或 b)敏感且易于链接到PII主机。
中度	隐私损害给道路使用者带来了不便的后果。有关道路使用者的信息包括： a）敏感但难以与PII主体联系起来；或 b）不敏感，但容易与PII主体链接。
可忽略	隐私损害不会对道路使用者产生影响，或者产生的后果微不足道，或者与道路使用者无关。有关道路使用者的信息不敏感，且难以与个人身份信息主体联系起来。

个人可识别信息（PII）和PII主体可根据ISO/IEC 29100 [25]进行定义。

附件G
提供信息的

攻击可行性评级指南

G.1概述

本附录提供了如何应用以下方法进行攻击可行性评级的指南（见15.7)：

—基于攻击潜力；

—基于CVSS；以及

一基于攻击向量。

是否攻击有可能扩展（即，容易扩展到多个实例和目标）的考虑可以包括在攻击可行性评级中。

G.2基于攻击可能性的方法指南

G.2.1攻击可能性背景

ISO/IEC 18045 [23]将攻击潜力定义为攻击项目或组件所需付出的努力，以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：

—经过的时间；

一专家专长；

-对产品或部件的了解；

一机会之窗；以及设备。

本小节给出了定制和示例映射以攻击可行性的示例。

G.2.2参数调整示例

G.2.2.1已用时间的示例自定义

经过时间参数包括识别漏洞和开发并（成功）应用攻击所需的时间。因此，该评级基于评级时的专家知识状态，见表G.1。

表G.1-已用时间

≤1天
≤1周
≤1个月
≤6months
>6个月

G.2.2.2专家专业知识的示例定制

专业知识参数与攻击者的能力有关，相对于他们的技能和经验，参见表G.2。

表G.2-专家专业知识

门外汉 与专家或熟练人员相比，知识不足，没有特殊的专业技能。示例1：普通人员使用公开的逐步描述攻击。
熟练： 熟悉产品或系统类型的安全行为。 示例2：有经验的车主，普通技师，知道简单的和流行的攻击，如里程表调谐，安装假冒零件。
行家 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、产品类型中的经典攻击、攻击方法等在产品或系统类型中实现。 示例3：有经验的技术人员或工程师。
多位专家： 攻击的不同步骤需要不同领域的专家水平。 示例4多名具有不同领域专业知识的资深工程师，他们对于攻击的不同步骤来说是专家级的。

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关于项目或组件的信息量有关，参见表G.3。

表G.3-对项目或组件的了解

新闻资料： 与项目或component(e.g.as相关的公共信息（从互联网获得）。示例1：在产品主页或互联网论坛上发布的资讯和文档。

表G.3（续）

受限信息： 有关项目或受控于开发组织并根据保密协议与其他组织共享的component(e.g.knowledge的限制信息）。例如2：制造商和供应商之间共享的内部文档、要求和设计规范。
机密信息： 关于项目或组件的机密信息(e.g.knowledge在开发组织内的离散团队之间共享，仅限于指定团队的成员访问）。 示例3：防盗器相关信息、软件源代码。
严格保密信息： 关于产品或组件的严格保密信息（仅少数人知晓的e.g.knowledge，其访问权限受到严格控制，仅限于需要知道的人和个人）。 示例4：制造商和/或供应商内部记录的客户特定校准或存储器映射。

G.2.2.4机会窗口的示例定制

机会窗口参数与成功执行攻击的访问条件（时间、类型）有关。它结合了访问类型(e.g.logical和物理）和访问持续时间（e.g.unlimited和有限）。根据攻击类型的不同，这可能包括发现潜在目标、访问目标、在目标上利用漏洞、对目标进行攻击的时间、未被发现、规避检测和网络安全控制等（见表G.4）。

表G.4-机会之窗

无限制： 通过公共/不可信网络实现高可用性，无需任何时间limitation(i.e.asset始终可访问）。远程访问无需物理存在或时间限制，以及对项目或组件的无限物理访问。 示例1：远程attack(e.g.vehicle-to-anything或蜂窝接口）无需任何前提条件，所有者可无限次物理访问以进行芯片调谐。
简单： 高可用性和有限的访问时间。无需对项目或组件进行实际操作即可远程访问。 示例2：蓝牙配对时间、远程软件更新、需要车辆静止的远程攻击。
中度： 物品或组件的可用性较低。物理和/或逻辑访问受限。无需使用任何特殊工具即可对车辆内部或外部进行物理访问。 示例3：攻击者进入一辆未上锁的汽车，通过车载诊断端口获得了暴露的物理interface，e.g.phys-访问权限。
困难的 项目或组件的可用性极低。对项目或组件的访问级别不适宜进行攻击。 示例4：解封IC以提取信息，通过暴力破解加密密钥的速度比密钥旋转速度快。

G.2.2.5设备定制示例

设备参数与攻击者可用于发现漏洞和/或执行攻击的工具相关，参见表G.5。

表G.5-设备

标准的 攻击者可以很容易地获得设备。这些设备可以是产品本身的一部分（操作系统中的e.g.a调试器），也可以很容易地获得(e.g.internet源代码、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、烙铁、钳子）。
专业： 攻击者无法轻易获得设备，但可以不费吹灰之力获得。这包括购买中等数量的equipment(e.g.power分析工具，使用数百个 通过互联网连接的个人电脑将属于此类)，或开发更广泛的攻击脚本或程序。如果攻击的不同步骤需要使用由专门设备组成的明显不同的测试平台，则将被评定为定制。 示例2：专用硬件调试设备、车载通信设备（硬件在环测试台、高级示波器、信号发生器）、特殊化学品。
定制： 设备是专门生产的（例如，非常复杂的软件），public(e.g.black市场不容易获得，或者设备非常专业，其分销受到控制，甚至可能受到限制。或者，设备非常昂贵。 示例3：制造商限制的工具，电子显微镜。
多个定制： 引入了允许在攻击的不同步骤中需要不同类型的定制设备的情况。

G.2.2.6攻击可能性与攻击可行性之间的示例映射

对于每个参数，可以定义数值。根据ISO/IEC 18045[23，基于上述适应性，提出了以下量表，见表G.6。

表G.6-攻击潜力的示例聚合

已用时间		专家经验		知识来源项或成分 nent		机遇之窗		设备	
枚举	**价值**	**枚举**	**价值**	**枚举**	**价值**	**枚举**	**价值**	**枚举**	**价值**
≤1天	0	门外汉	0	平民	0	无限制	0	标准的	0
≤1周	1	熟练	3	受限	3	简易	1	专业	4
≤1个月	4	行家	6	机密的	7	中度	4	定制	7
≤6个月	17	多名专家	8	严格保密	11	困难 / 无	10	多发言	9
>6个月	19								

根据ISO/IEC 18045[23，攻击可能性对应于所有参数的添加。攻击可行性使用表G.Z进行映射，基于对ISO/IEC 18045[23的定制。

表G.7-示例攻击可能性映射

攻击可行性评级	对价值的看法
高	0-9
	10-13
中等	14-19
低	20-24
极低	≥25

G.3基于CVSS的方法指南

为了评估信息技术安全漏洞，可以使用由事件响应和安全团队论坛（第一）[24]维护的CVSS。在基础指标组中，可利用性指标（参见参考文献[24]，7.1）可用于评估攻击可行性。其他CVSS指标(e.g.impact指标）则涵盖此document，e.g.damage场景和影响评估的各个方面。

可利用性指标包括：

一攻击向量；

—攻击复杂性；

-所需特权；以及

一用户交互。

它们首先由first[24]描述。对CVSS指标进行评估后，每个指标都会在预定义范围内产生数值。总体可利用性值可以根据一个简单的公式计算得出：

E=8,22×V×C×P×U

在哪里

E是可利用性值；

V是与攻击向量相关的数值，范围为0.2至0.85；

C是与攻击复杂度相关的数值，范围从0.44到0.77；

P是与所需权限相关的数值，范围为0.27到0.85；U是与用户交互相关的数值，范围为0.62到

0.85。

因此，可利用性值介于0.12和3.89之间。

CVSS可利用性值与攻击可行性之间的映射示例如表G.8所示。这是等距离可利用性步骤的一个示例。

表G.8-示例CVSS可利用性映射

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

表G.8（续）

攻击可行性评级	CVSS漏洞可利用性值
极低	0,12-1,05

注意：仅使用可利用性指标作为更大范围的CVSS基础指标组的一部分，并不严格符合CVSS对指标的要求。为了根据本文件计算风险，缺失的影响指标可以通过本文件中的影响指标来弥补，详见附录F和参考文献[24]。

不改变可利用性指标值的情况下，可以补充其描述，以更好地指导组织的业务和正在开发的项目或组件，并减少在将描述应用于实际漏洞时可能出现的误解。这些补充可以是特定于组织的例子，添加到指标值描述中。

除了漏洞之外，CVSS可利用性度量还可以用于评估概念上的弱点、缺陷和差距。

G.4基于攻击向量的方法指南

基于攻击向量的方法反映了攻击路径利用的背景。攻击可行性评级越高，攻击者能够利用攻击路径的距离（逻辑上和物理上）就越远。假设是，通过互联网可以利用漏洞的潜在攻击者数量大于需要物理访问项目或组件才能利用攻击路径的潜在攻击者数量，见表G.9。

表G.9-基于攻击向量的方法

攻击可行性评级	标准
高	**网络** 潜在攻击路径不受任何限制，可直达网络堆栈。例如：蜂窝网络连接使ECU直接连接并可访问互联网。
中等	**相邻：** 潜在的攻击路径被限制在网络堆栈中，但是连接在物理上或逻辑上是有限制的。 示例2蓝牙接口，虚拟专用网络连接。
低	**本地** 潜在的攻击路径不局限于网络堆栈，威胁代理需要直接访问项目以实现攻击路径。 示例3：通用串行总线大容量存储设备、存储卡。
极低	**物理：** 威胁代理需要物理访问才能实现攻击路径。

附件H
提供信息的

TARA方法的应用实例-前照灯系统

H.1概述

本附录中提供的前照灯系统开发示例和相应工作产品仅用于说明目的，并不意味着任何特定的实际使用方法。

本附录通过提供威胁分析和风险评估（TARA）方法的应用示例，有助于理解本文档的要求。此示例仅用于说明TARA应用的概念阶段，并以抽象和简化的形式呈现。具体而言，它涉及：

—项目定义；以及

—塔拉。

TARA定义为模块化分析方法，每个模块可以按任意顺序进行，例如：

-资产识别→相应的损坏场景识别→影响评级→威胁场景识别→攻击路径分析→。

—从目录中选择损坏场景→影响评级→威胁场景识别→资产识别→...

本附录中的示例按以下顺序排列：

i.资产识别；

ii.影响评级；

iii.威胁场景识别；

iv.攻击路径分析；

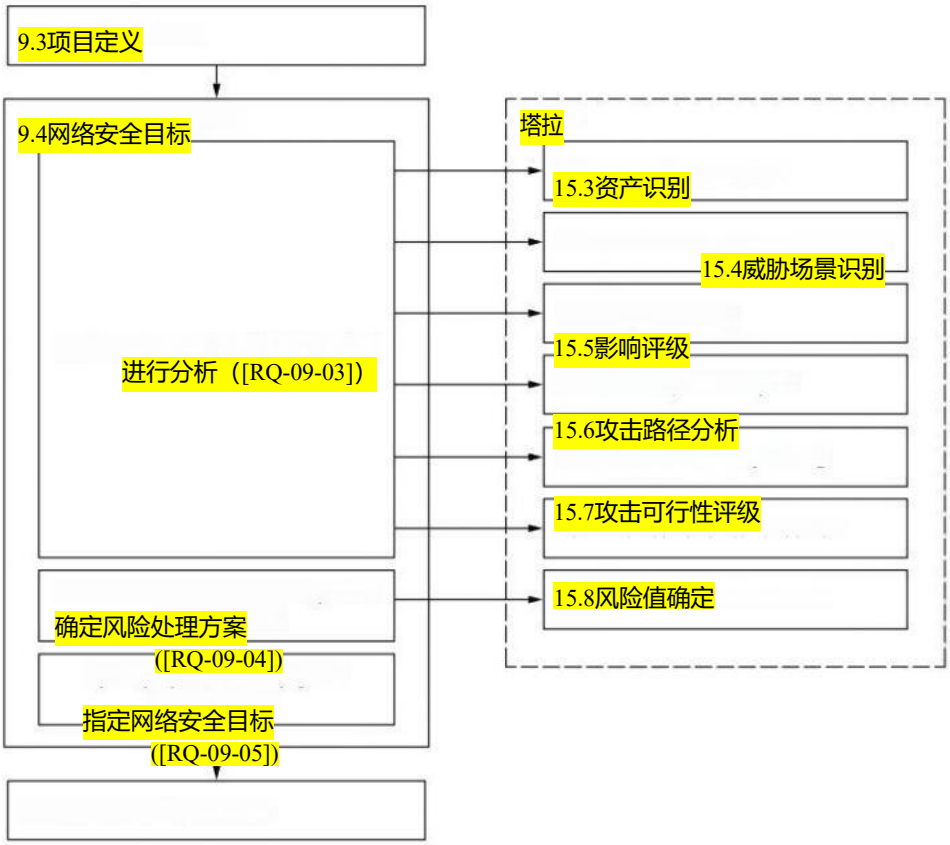
五、攻击可行性评级；

v.风险价值确定；

vii.风险处理决策。

在步骤v中，采用两种不同的方法对攻击可行性进行评级。一种方法采用基于攻击向量的方法（见[RC-15-14]），另一种方法采用基于攻击潜力的方法（见[RC-15-12]）。

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-概念阶段的交互作用

H.2前照灯系统概念阶段的示例活动

H.2.1项目定义

本小节显示了9.3的选定工作产品的示例。前照灯系统的一个示例项目定义如下：

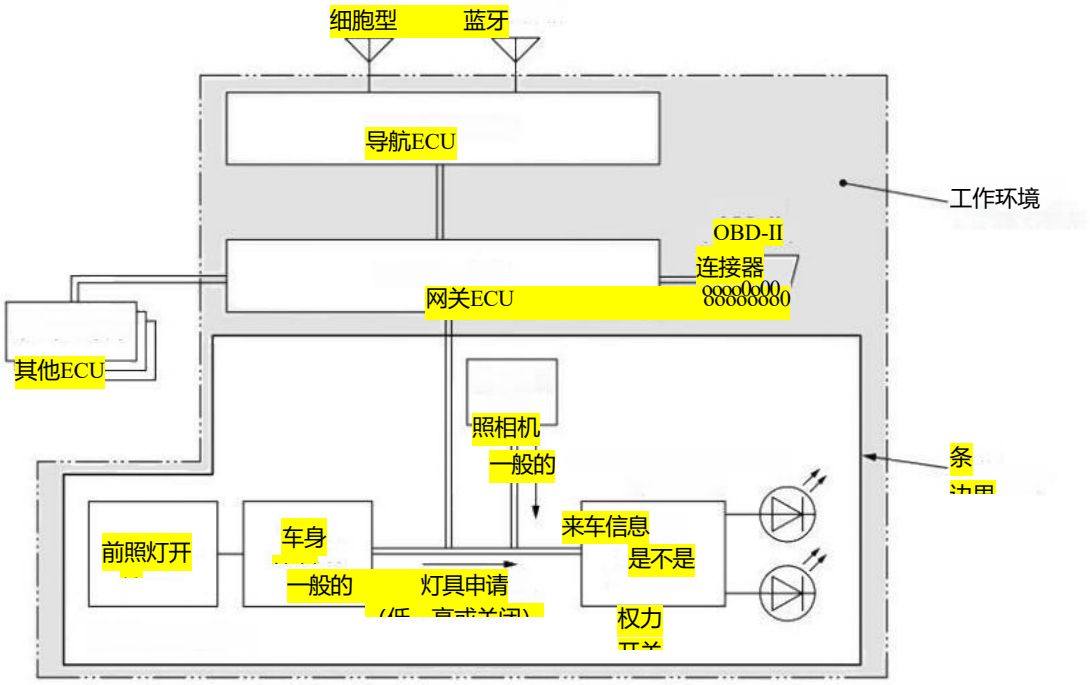
a)界面（见图H.2)；

b)项目功能；

一项目功能概述：前照灯系统根据驾驶员的需求通过开关开启或关闭前照灯。如果前照灯处于远光模式，当检测到迎面而来的车辆时，前照灯系统会自动切换到近光模式。如果不再检测到迎面而来的车辆，前照灯也会自动恢复到远光模式。

注：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-前照灯系统项目边界和初步架构示例

在项目定义期间，对项目的运行环境进行描述（见[RQ-09-02]）。运行环境为TARA的分析活动提供了补充信息。表H.1显示了本附录中使用的运行环境的示例描述。

表H.1-操作环境示例说明

该部件（前照灯系统）与网关ECU相连，网关ECU通过数据通信与导航ECU相连。
导航ECU具有外部通信接口： —Bluetooth; —cellular. 假设： —navigation ECU具有防火墙，以防止外部接口的无效数据通信。
Gateway ECU具有外部通信接口： — OBD-II. 假设： —gateway ECU具有强大的安全控制功能，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要求进行资产识别，以确定项目资产及其损坏情况。表H.2显示了资产识别的示例结果。

表H.2-资产和损坏情况示例清单

资产	网络安全财产			损坏情况
	C	I	A	
数据通信（灯请求）	—	X	X	车辆不能在夜间行驶，因为（驾驶员感觉到）停车时前照灯功能被抑制。
	—	X	–	在中速夜间行驶时，由于未预期的前照灯关闭导致与狭窄静止物体（e.g.atree）发生正面碰撞。
数据通信 （来车信息）	—	X	–	迎面而来的车辆驾驶员被眩光所遮挡，这是由于夜间驾驶时无法切换到近光灯造成的。
	—	—	X	自动远光灯故障引起 夜间驾驶时，前照灯始终保持在低光束。
车身控制ECU的固件	X	X	–	...

H.2.3影响等级

[RQ-09-03]还根据15.5对损害情景的影响进行评级。表H.3显示了影响评级的示例结果。

表H.3-损坏情景影响评级示例

损坏情况	影响种类	影响评级
车辆不能在夜间行驶，因为（驾驶员感觉到）停车时前照灯功能被抑制。	0	主要的
在中速夜间行驶时，由于未预期的前照灯关闭，导致与狭窄静止的object(e.g.a树发生正面碰撞。	S	重度（S3)
夜间行车时，前照灯始终处于近光状态，导致自动远光灯故障。	0	中度

H.2.4威胁场景识别

[RQ-09-03]还根据15.4节要求，对威胁场景进行识别。表H.4显示了威胁场景识别的示例结果。

表H.4-示例威胁场景

损坏情况	威胁场景
在中速夜间行驶时，由于意外关闭前照灯而与狭窄静止物体（例如树木）发生正面碰撞	信号欺骗会导致“灯请求”信号与电源开关执行器ECU之间的数据通信完整性丢失，可能会导致前照灯意外关闭。
	篡改车身控制ECU发送的信号会导致“灯请求”信号与电源开关致动器ECU之间的数据通信完整性丢失，可能会导致前照灯意外熄灭。
故障自动由头部引起的高光束灯始终亮着	资产：来车信息 网络安全财产：可用性 相关原因：否认到来车辆信息

夜间低光束 驾驶	

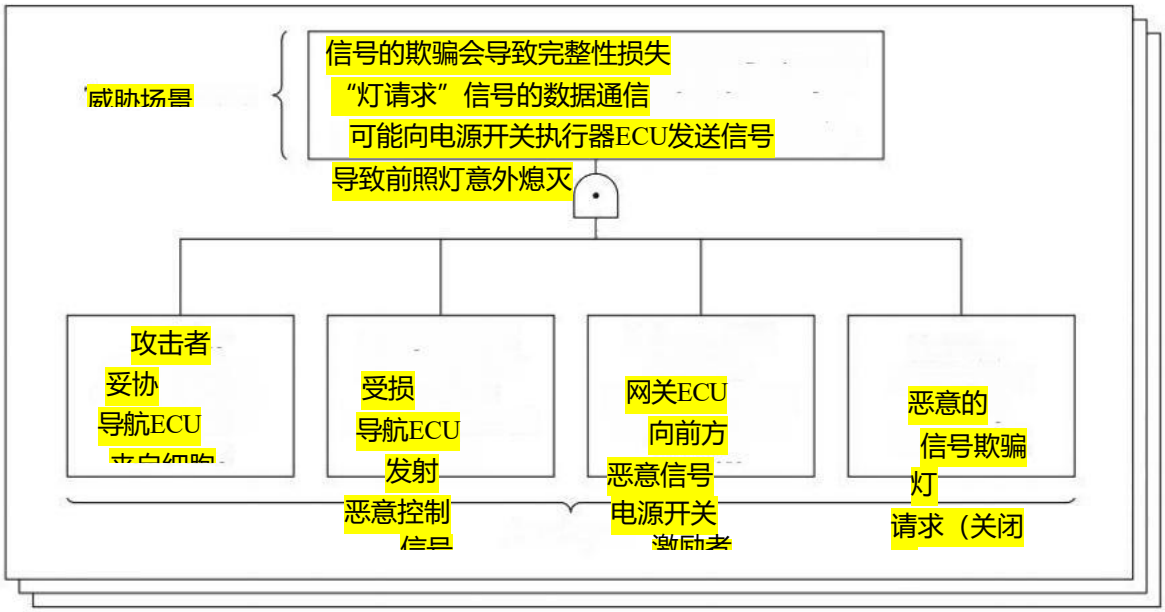
H.2.5攻击路径分析

[RQ-09-03]也称作攻击路径分析，依据15.6。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示例。

攻击路径的分析可以考虑假设。在本例中，根据假设，可以排除需要在物品内部进行物理访问的攻击路径，例如身体控制ECU的微控制器。

表H.5-威胁场景的示例攻击路径

威胁场景	攻击路径
欺骗分配器会导致“灯请求”信号与电源开关执行器ECU之间的数据通信完整性丢失，可能会导致前照灯意外关闭	i.攻击者通过蜂窝接口破坏导航ECU。 ii.被破坏的导航ECU发送恶意控制信号。ii.网关ECU将恶意信号转发至电源开关执行器。iv.恶意信号欺骗灯请求（关闭）。
	i.攻击者通过蓝牙接口破坏导航ECU。 ii.被破坏的导航ECU发送恶意控制信号。 iii.网关ECU将恶意信号转发至电源开关致动器。iv.恶意信号欺骗灯请求（关闭）。
	i.攻击者获得对OBD连接器的本地（参见表G.9）访问权。 ii.攻击者从OBD连接器发送恶意控制信号。 iii.网关ECU将恶意信号转发至电源开关致动器。iv.恶意信号欺骗灯请求（关闭）。
拒绝提供来车信息	i.攻击者通过蜂窝接口破坏导航ECU。 ii.被破坏的导航ECU传输恶意控制信号。 iii.网关ECU将恶意信号转发至电源开关执行器。 iv.攻击者用大量消息淹没通信总线。
	i.当车辆未上锁停放时，攻击者将一个支持蓝牙的OBD适配器连接到OBD接口上。 ii.攻击者利用蓝牙接口入侵司机的智能手机。 iii.攻击者通过智能手机和蓝牙适配器向网关ECU发送消息。 iv.网关ECU将恶意信号转发至电源开关执行器。 五、攻击者用大量消息淹没通信总线。



图H.3-通过攻击树分析得出的攻击路径示例

H.2.6攻击可行性评级

[RQ-09-03] 还根据15.7对每条攻击路径的攻击可行性评级进行了说明。

表H.7显示了根据G.4中所述的基于攻击向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G.2中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：基于攻击向量方法的攻击可行性评级示例

攻击路径	攻击可行性评级
i.攻击者通过蜂窝接口破坏导航ECU。 ii.被破坏的导航ECU发送恶意控制信号。 iii.网关ECU将恶意信号转发至电源开关致动器。iv.恶意信号欺骗灯请求（打开）。	高
i.攻击者通过蓝牙接口破坏导航ECU。 ii.被破坏的导航ECU传输恶意控制信号。 iii.网关ECU将恶意信号转发至电源开关致动器。iv.恶意信号欺骗灯请求（打开）。	中等
i.攻击者从OBD2接口发送恶意控制信号。 ii.网关ECU将恶意信号转发至电源开关致动器。iii.恶意信号欺骗灯请求（打开）。	低

注1：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到所有与项目相关的漏洞信息。

根据建议（见[RC-15-11]），也可以基于潜在攻击方法确定攻击可行性，表H.7中举例说明了该方法。

表H.7：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						
		乙	塞	科伊克	沃奥	平衡	价值	攻击可行性等级
拒绝服务地点迎面而来的因车信息-mation	i.攻击者破坏导航来自蜂窝接口的ECU。 ii.被破坏的导航ECU发送恶意控制信号 iii.网关ECU将恶意信号转发至电源开关执行器 四、攻击者用大量消息淹没通信总线	1	8	7	0	4	20	低
	i.当车辆停车时，攻击者将一个支持蓝牙的OBD适配器连接到OBD接口开锁 ii.攻击者破坏了驾驶员的带有蓝牙接口的智能手机。 iii.攻击者通过智能手机和蓝牙适配器发送消息到网关ECU。 iv.网关ECU传输恶意数据向电源开关致动器发送信号。 五、攻击者淹没通信带有大量消息的公交车	1	8	7	4	4	24	低
钥匙 ET已用时间 SE专家专业知识 KoIC对项目或组件的了解或Woo机会窗口 Eq设备								

注2：每个组织可以根据自己的政策对每个评级应用理由。例如，机会窗口被分配为4（中等，参见表G.4），用于第二攻击路径，因为需要物理访问。攻击可行性评级是根据所有可行性值综合考虑后确定的。

表G.7.

H.2.7风险值确定

[RQ-09-03]还根据15.8对每个威胁场景的风险确定进行了说明。风险值可以通过组织定义的风险矩阵来确定，该矩阵用于映射影响评级（见15.5）和攻击可行性（见15.7）与风险值的组合。表H8展示了一个示例风险矩阵，而表H.9则展示了使用表H8进行风险确定的结果示例。

表H.8-风险矩阵示例

		攻击可行性评级			
		极低	低	中等	高
影响评级	严重	2	3	4	5
	主要的	**1**	**2**	3	4
	中度	**1**	**2**	2	3
	可忽略	**1**	**1**	1	1

表H.9-确定的风险值示例

威胁场景	聚合攻击可行性等级	影响评级	风险值
欺骗信号导致“灯请求”信号的通信数据不完整，该信号用于电源开关执行器ECU	**高**	**严重**	**S:5**
拒绝提供来车信息	**低**	**中度**	**0:2**

风险值也可由组织定义的风险公式确定。下文的公式和表H.10中给出了一个示例。

$$R = I + I \times F$$

表H.10-影响和攻击可行性数值化翻译示例

影响等级	数值I，用于冲击
可忽略	0
中度	1
主要的	1,5

攻击可行性评级	数值F，用于攻击可行性
极低	0
低	1
中等	1,5
高	2

对于表H.9中显示的具体威胁场景，使用示例进行计算。表H.8和上述公式将导致相同的风险值。

H.2.8风险处理决策

[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-风险处理决策示例结果

威胁场景	风险值	风险处理选项
欺骗信号会导致“灯请求”信号的数据通信完整性丢失开关执行器ECU	S:5	降低风险
拒绝提供来车信息	0:2	降低风险

参考书目

[1] ISO 26262-1：2018，道路车辆功能安全第1部分：词汇

[2] ISO 9000：2015，质量管理体系—基础和词汇

[3] ISO 31000：2018，风险管理指南

[4] ISO/IEC/IEEE 15288：2015，系统和软件工程-系统生存周期过程

[5] ISO/IEC 27000：2018，信息技术-安全技术-信息安全管理系统-概述和词汇

[6] ISO/TR 4804，公路车辆-自动驾驶系统安全和网络安全-设计、验证和确认

[7] IATF 16949，汽车生产和相关服务零部件组织的质量管理体系要求

[8] ISO 9001，质量管理体系要求

[9] ISO 10007，质量管理-配置管理指南

[10] ISO/IEC 33001，信息技术过程评估概念和术语

[11] ISO/IEC/IEEE 15288，系统和软件工程-系统生存周期过程

[12]ISO/IEC/IEEE12207，系统和软件工程-软件生存周期过程

[13] VDA QMC工作组13/汽车SIG。汽车香料工艺评估/参考模型，第3.1版[在线]。柏林：VDA QMC，2017年11月。可从以下网址获取：http://www..automotivespice.com/fileadmin/software-download/AutomotiveSPICE.PAM.31.pdf

[14] ISO 29147，信息技术安全技术漏洞披露

[15] IEC 62443-2-1，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] ISO 26262（所有部分），道路车辆-功能安全

[17] MISRAC 2012，《C语言在关键系统中的使用指南》，第3版，第1次修订。英国诺顿：HORIBA Mira，2019年2月。ISBN（印刷版/电子版）：978-1-906400-21-7/978-1-906400-22-4。

[18] SEI C编码标准——开发安全、可靠和有保障的系统规则[在线]。宾夕法尼亚州匹兹堡：卡内基梅隆大学软件工程研究所，2016年[查看于2021-02-12]。可用at：https://resources.sei.cmu.edu/library/asset-view.cfm？assetid=454220

[19] ROSS Ron等（2018），《系统安全工程：多学科方法在可信安全系统工程中的考虑》[在线].（国家标准与技术研究院，马里兰州盖瑟斯堡），NIST特别出版物（SP）800-160，第1卷。2018年3月更新[查看于2021-02-16]。可获取于：https://doi.org/10.6028/NIST.SP.800-160v1

[20]电子安全车辆入侵防护应用（E-safety VEHICLE INTRUSION Protection，简称evita）基于暗面场景的车载网络交付D2.3：Security需求[在线]。由A. Ruddle等人编辑。2009年12月[查看日期：2021-01-17]。at：https://doi.org/10.5281/zenodo可获取
.1188418

[21] ETSI TS 102165-1，网络；方法和协议；第1部分：威胁、漏洞和风险分析（TVRA）方法和格式，版本5.2.3[在线]。2017年10月[查看于2021年1月19日]。可获取于：htt ps：//www.etsi.org/deliver/etsi ts/102100102199/10216501/05.02.0360/ts_10216501v050203p.pdf

[22]UcEDAVELEZ，Tony和MoRANA，Marco M.风险中心威胁建模：攻击模拟和威胁分析过程。新泽西州霍博肯：Wiley，2015年5月。ISBN：978-1-118-98835-0.

[23] ISO/IEC 18045，信息技术-安全技术-IT安全评估方法

[24]论坛，事件响应与安全团队（第一）。通用漏洞评分系统（CVSS），通用漏洞评分系统v3.1：Specification文档，[在线]。可获取于：https://www.first.org/cvss/v3.1/specification-document

[25] ISO/IEC 29100，信息技术-安全技术-隐私框架

[26] AUTOMOTIVE ISAC，汽车网络安全最佳实践[在线]。可从以下网址获取：https://www.automotiveisac.com/best-practices/

[27]事件响应与安全团队论坛（第一）。交通灯协议（TLP），第一版标准定义及使用指南-1.0，[在线]。可获取于：https://www ， first.org/tlp/

[28] ISO/IEC 23822），信息技术术语

[29]ISO/IEC15408（所有部分），信息技术-安全技术-IT安全评估准则

[30] ISO/IEC 27001，信息技术-安全技术-信息安全管理系统-要求

[31] ISO/IEC 27010，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/IEEE 26511，系统和软件工程——系统、软件和服务用户的信息管理者要求

[33]IEC31010，风险管理-风险评估技术

[34] IEC 61508-7，电气/电子/可编程电子安全相关系统功能安全—第7部分：技术与措施概述

[35]John JOHNSON Christopher等人（2016）《网络威胁信息共享指南》[在线]。（国家标准与技术研究院，马里兰州盖瑟斯堡），NIST特别出版物（SP）800-150,2016年10月[查看于2021-02-16]。可获取at：https://doi.org/10.6028/NIST.SP.800-150

[36]联合任务部队转型倡议2012），《风险评估指南》[在线]。（国家标准与技术研究院，马里兰州盖瑟斯堡），NIST特别出版物（SP）800-30，Rev.1.September 2012[查看日期：2021年2月16日]）。可从以下网址获取：http://dx.doi.org/10.6028/NIST.SP.800-30r1

[37]SAEJ3061，网络物理车辆系统网络安全指南

[38] SCARFONE Karen，et al.（2008），信息安全测试与评估技术指南[在线]。（美国国家标准与技术研究院，Gaithersburg，MD），NIST特别出版物（SP）800-115。2008年9月[查看日期：2021-02-16]。可从以下网址获取：https://doi.org/10.6028/NIST.SP.800-115

2）可用at：https://www.iso.org/obp/ui#iso：std：iso-iec：2382。

[39] TAKANEN Ari等.软件安全与质量保证中的模糊测试,第二版.马萨诸塞州波士顿/伦敦:Artech House,2018年1月.ISBN:978-1-60807-850-9.

ICS 43.040.15
基于81页的价格