

目录

前言.....	6
简介.....	8
1 范围.....	13
2 规范性参考文件	14
3 术语、定义和缩略语	15
3.1 术语和定义.....	15
3.2 缩略语.....	19
4 整体考虑	21
5 组织网络安全管理	23
5.1 综述	23
5.2 目标	23
5.3 输入	23
5.4 要求和建议	24
5.5 工作成果	28
6 依靠项目的网络安全管理	30
6.1 综述.....	30
6.2 目标.....	31
6.3 输入.....	31
6.4 要求和建议	32
6.5 工作成果	39
7 分布式网络安全活动	40

7.1 综述	40
7.2 目标	40
7.3 输入	40
7.4 要求和建议	40
7.5 工作成果	42
8 持续的网络安全活动	43
8.1 综述	43
8.2 目标	43
8.3 网络安全监测	43
8.4 网络安全事件评估	44
8.5 脆弱性分析	45
8.6 漏洞管理	46
9 概念	48
9.1 综述	48
9.2 目标	48
9.3 项目定义	48
9.4 网络安全目标	49
9.5 网络安全概念	51
10 产品开发	53
10.1 综述	53
10.2 目标	54
10.3 输入	54

10.4 要求和建议	55
10.5 工作成果	58
11 网络安全验证	60
11.1 综述	60
11.2 目标	60
11.3 输入	60
11.4 要求和建议	60
11.5 工作成果	61
12 生产	62
12.1 综述	62
12.2 目标	62
12.3 输入	62
12.4 要求和建议	62
12.5 工作成果	63
13 运营和维护	64
13.1 综述	64
13.2 目标	64
13.3 网络安全事件应对	64
13.4 更新	66
14 结束网络安全支持和停用工作	67
14.1 综述	67
14.2 目标	67

14.3 网络安全支持的结束	67
14.4 停用	67
15 威胁分析和风险评估方法	69
15.1 综述	69
15.2 目标	69
15.3 资产识别	70
15.4 威胁情景识别	71
15.5 影响评级	72
15.6 攻击路径分析	73
15.7 攻击可行性等级	74
15.8 风险值的确定	76
15.9 风险处理决定	77
附件 A	79
附件 B	83
附件 C	85
附件 D	87
附件 E	89
E.1 综述	89
E.2 确定一个 CAL	89
E.3 使用 CAL	91
附件 F	95
F.1 综述	95

F.2 安全损害的冲击等级.....	95
F.3 财务损失的影响评级.....	95
F.4 操作损害的影响等级.....	96
F.5 对隐私损害的影响等级.....	96
附件 G.....	98
G.1 综述.....	98
G.2 基于攻击潜力的方法的准则.....	98
G.3 基于 CVSS 方法的准则.....	103
G.4 基于攻击矢量的方法的准则.....	104
附件 H.....	106
TARA 方法的应用实例--大灯系统.....	106
H.1 综述.....	106
H.2 大灯系统概念阶段的活动实例.....	107
参考文献.....	117



微信搜一搜

Q 轩辕实验室

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。

制定国际标准的工作通常是通过 ISO 技术委员会进行的。每个对某一主题有意向的成员机构都有权派代表参加技术委员会。对已成立的技术委员会有意向的每个成员机构都有权派代表参加该委员会。国际组织，政府和非政府组织与 ISO 联络，也参与这项工作。国际标准化组织与国际电工委员会（IEC）就所有的电工标准化问题进行了密切的合作。

国际汽车工程师学会是一个由超过 128,000 名在航空航天、汽车和商用车行业的工程师和相关技术专家组成的全球性协会。国际汽车工程师学会的标准被用于推动全世界的交通工程。SAE 的技术标准开发项目是该组织对那些移动行业的主要规定之一，它服务于航空航天、汽车和商业车辆。这些工作由来自世界各地的 9000 多名工程师及其他合格的专业人员的自愿努力来授权、修订和维护。SAE 主题专家在标准制定过程中以个人身份行事，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的技术内容。

用于制定本文件的程序及旨在进一步维护本文件的程序在 ISO/IEC 指令第 1 部分和 SAE 技术标准委员会政策中有所描述。特别要注意的是，不同类型的 ISO 文件所需的不同批准标准。本文件是根据 ISO/IEC 指令第 2 部分的编辑规则起草的（见 www.iso.org/directives）。

请注意，本文件中的一些内容可能涉及专利权问题。ISO 和 SAE 国际将对识别任何或所有此类专利权不负有责任。在本文件开发过程中发现的任何专利权的细节将出现在导言中或 ISO 专利清单上（见 www.iso.org/patents）。

SAE 技术标准委员会规则规定：“本文件的出版是为了推动技术和工程科学的发展。本文件的使用完全是自愿的，其对任何特定用途的适用性和适宜性，包括由此产生的任何专利侵权行为，完全由用户负责。”

本文件中使用的任何商品名称是为方便用户而提供的信息，并不构成对其的认可。

关于标准的自愿性质的解释，和与符合性评估有关的 ISO 特定术语和表达方式的含义，

以及 ISO 坚持的关于世界贸易组织 (WTO) 在技术性贸易壁垒 (TBT) 方面的原则, 见 www.iso/foreword.html。本文件由 ISO/TC 22 道路车辆技术委员会、SC 32 电气和电子元件及分委员会, 以及 SAE TEVEES18A 车辆网络安全系统工程委员会联合编写。

该 ISO/SAE 21434 的第一版取消并取代了 SAE J3061: 2016[37]。

主要变化如下:

——对内容和结构进行了全面的重写。

关于本文件的任何反馈或问题都应直接提交给用户的国家标准机构。这些机构的完整清单可以在 www.iso.org/members.html 上找到。另外, 要对本文件提供反馈意见, 请访问 [https://www.sae.org/standards/content/ISO/ SAE 21434/](https://www.sae.org/standards/content/ISO/SAE%2021434/)。

简介

本文件的目的

此文件论述了道路车辆内电气和电子（E/E）系统工程中的网络安全问题。通过确保对网络安全的适当考虑，此文件旨在使 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。

该文件提供了与网络安全工程相关的词汇、目标、要求和指导方针，作为整个供应链共同理解的基础。这使企业能够：

- 确定网络安全政策和流程；
- 管理网络安全风险；
- 培养一种网络安全文化。

该文件可用于实施网络安全管理系统，包括网络安全风险管理。风险管理。

本文件的组织结构

图 1 给出了本文件的结构概述。图 1 中的元素没有规定各个主题的执行顺序。

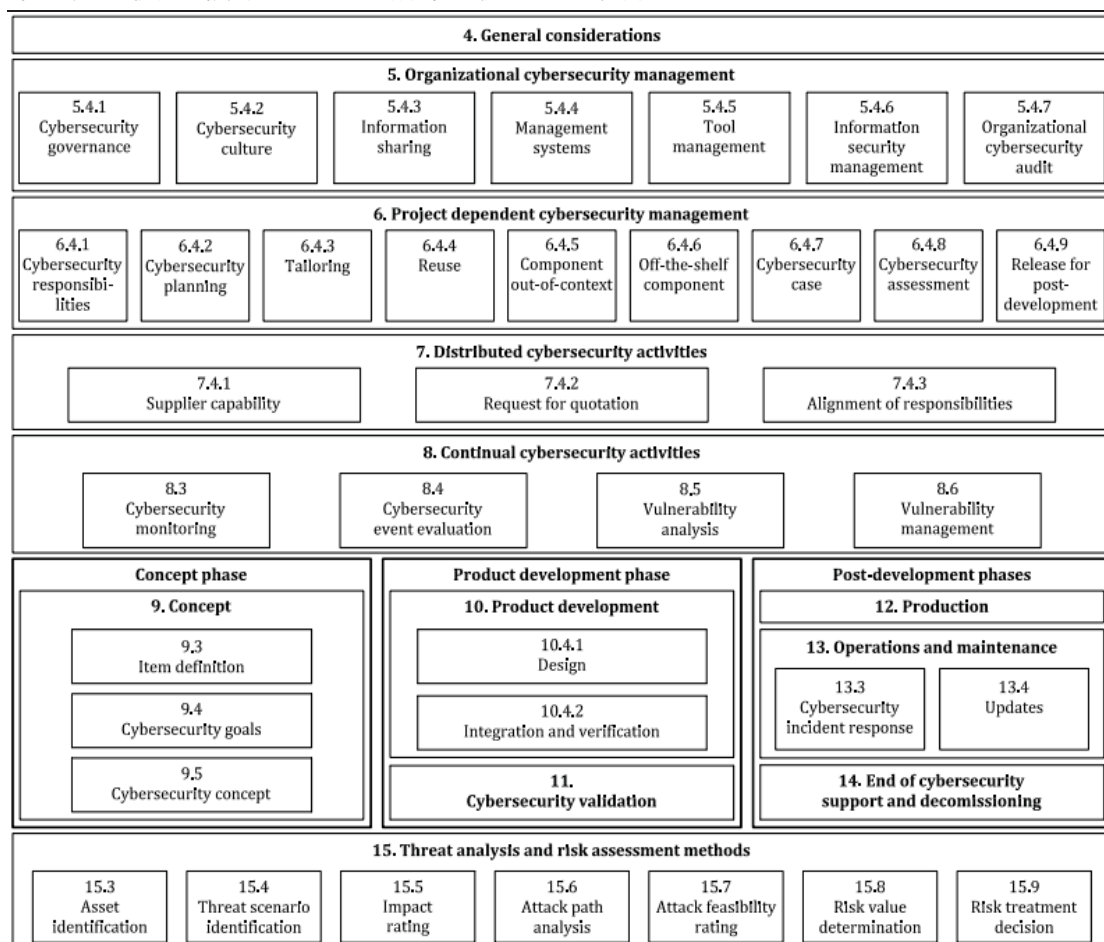


图 1 本文件概述

- 注：4. 总体考虑
5. 组织化网络安全管理
- 5.4.1 网络安全治理
- 5.4.2 网络安全文化
- 5.4.3 信息共享
- 5.4.4 管理系统
- 5.4.5 工具管理
- 5.4.6 信息安全管理
- 5.4.7 组织化网络安全审查
6. 依托项目的网络安全管理
- 6.4.1 网络安全责任性

- 6.4.2 网络安全计划
- 6.4.3 裁剪
- 6.4.4 再次使用
- 6.4.5 上下文无关的组件
- 6.4.6 成品组件
- 6.4.7 网络安全案例
- 6.4.8 网络安全评估
- 6.4.9 后续开发的发布
- 7. 分布式网络安全活动
 - 7.4.1 供应方能力
 - 7.4.2 询价书
 - 7.4.3 责任一致
- 8. 持续的网络安全活动
 - 8.3 网络安全监测
 - 8.4 网络安全事件评估
 - 8.5 漏洞分析
 - 8.6 漏洞管理
- 9. 概念
 - 9.3 项目定义
 - 9.4 网络安全目标
 - 9.5 网络安全概念
- 10. 产品开发
 - 10.4.1 设计
 - 10.4.2 集成和验证
- 11. 网络安全验证
- 12. 产品

- 13. 运营和维护
 - 13.3 网络安全事故责任
 - 13.4 更新
- 14. 网络安全支持和停用的终端
- 15. 威胁分析和风险评估方法
 - 15.3 资产确认
 - 15.4 威胁情况确认
 - 15.5 影响等级
 - 15.6 攻击路径分析
 - 15.7 攻击可行等级
 - 15.8 风险值确认
 - 15.9 风险处理决定

第 4 条(总体考虑) 是信息性化的，包括本文件中对道路车辆网络安全工程所采取的背景和观点。本文件所采取的道路车辆网络安全工程方法的背景和观点。

第 5 条（组织化网络安全管理）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（依托项目的网络安全管理）包括项目层面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的责任的要求。

第 8 条（持续的网络安全活动）包括为持续的风险评估提供信息的活动，并定义了 E/E 系统的脆弱性管理，直到网络安全支持的结束。

第 9 条（概念）包括确定网络安全风险、网络安全目标和项目的网络安全要求的活动。术语，包括确定项目的网络安全风险、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的活动，以及实施和验证网络安全要求。实施和验证网络安全要求。

第 11 条（网络安全验证）包括在车辆层面对一个项目进行网络安全验证。

第 12 条（生产）包括物品或组件的制造和组装的网络安全相关方面。

第 13 条（运营和维护）包括与网络安全事件响应和项目或组件更新有关的活动。

第 14 条（网络安全支持的结束和退役）包括网络安全考虑因素终止支持和停用的项目或组件的网络安全考虑。

第 15 条（威胁分析和风险评估方法）包括分析和评估的模块方法，以确定网络安全的程度，从而进行处理。

第 5 条至第 15 条有各自的目标、规定（即要求、建议、许可）和工作产品。工作产品是网络安全活动的结果，它满足了一个或多个相关要求。

“先决条件”是由前一阶段的工作产品组成的强制性投入。“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，这些信息可以由负责不同网络安全活动的人员的提供来源。

网络安全活动和工作产品的摘要可在附件 A 中找到。

规定和工作产品被分配了独特的标识符，包括一个双字母的缩略语（“RQ”表示要求，“RC”表示建议，“PM”表示许可，“WP”表示工作成果产品），后面是两个数字，用连字符分开。第一个数字指的是条款，而第二个数字分别表示该条款的规定或工作成果的连续顺序。例如，[RQ-05-14]指的是第 5 条中的第 14 条规定，这是一项要求。

1 范围

本文件规定了网络安全风险管理的工程要求，内容涉及道路车辆中概念、产品开发、生产、运行、电气和电子(E/E)系统维护和停用，包括其部件和接口。

定义了一个包括对网络安全流程的要求和通用语言的框架用于沟通和管理网络安全风险。

本文件适用于系列化生产的道路车辆 E/E 系统，包括其组件和接口。

本文件不规定与网络安全有关的具体技术或解决方案。

2 规范性参考文件

以下文件在文本中被提及, 其部分或全部内容构成本文件的要求。对于过时的参考文献, 只适用于所引用的版本。对于未注明日期的参考文件, 适用于所参考文件的最新版本 (包括任何修正案)。

ISO 26262-3:2018, 道路车辆-功能安全-第三部分: 概念阶段

轩辕实验室 XYLab

3 术语、定义和缩略语

3.1 术语和定义

在本文件中，适用以下术语和定义：

ISO 和 IEC 在以下地址维护术语数据库，供标准化工作使用。

ISO 在线浏览平台：可在 <https://www.iso.org/obp>

IEC Electropedia：可在 <https://www.electropedia.org/>

3.1.1 architectural design(架构设计)

可以识别组件（3.1.7）、其边界、接口和交互的表示方法

3.1.2 asset(资产)

具有价值或对价值有贡献的物体

注 1：一项资产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害情况（3.1.22）。

3.1.3 attack feasibility(攻击可行性)

攻击路径的属性（3.1.4），描述成功执行相应的一组行动的难易程度的行动。

3.1.4 attack path(攻击路径)

实现威胁场景的蓄意行动集（3.1.33）

3.1.5 attacker(攻击者)

执行攻击路径的个人、团体或组织（3.1.4）

3.1.6 audit(审核)

对过程进行审核检查，以确定实现过程目标的程度

[来源：ISO 26262-1:2018[1]，第 3.5 条，修改-将“关于”一词替换为“确定”和“达到”的程度]

3.1.7 component(组件)

逻辑上和技术上可分离的组成部分

3.1.8 customer(消费者)

接受服务或产品的客户、个人或组织

[来源: ISO 9000:2015[2], 3.2.4, 修改-短语“能够或确实接收”被替换为“接收”，短语“该人员或组织打算或要求的”被省略，条目示例和注释 1 被省略。]

3.1.9 cybersecurity(网络安全)

网络安全道路车辆网络安全状态，在该状态下，资产（3.1.2）受到充分保护，免受道路车辆项目（3.1.25）、其功能及其电气或电子部件（3.1.7）的威胁场景（3.1.33）

注 1：为简洁起见，本文件使用“网络安全”一词代替道路车辆网络安全。

3.1.10 cybersecurity assessment(网络安全评估)

网络安全评估-网络安全判断（3.1.9）

3.1.11 cybersecurity case(网络安全案例)

网络安全案例结构化论证，有证据证明风险（3.1.29）并非不合理

3.1.12 cybersecurity claim(网络安全声明)

关于风险的网络安全索赔声明（3.1.29）

注 1：网络安全索赔可包括保留或分担风险的理由。

3.1.13 cybersecurity concept(网络安全概念)

网络安全概念项目（3.1.25）的网络安全要求和操作环境要求（3.1.26），以及网络安全控制的相关信息（3.1.14）

3.1.14 cybersecurity control(网络安全控制)

修改风险的网络安全控制措施（3.1.29）

[来源: ISO 31000:2018[3], 3.8, 修改-在术语中添加了“网络安全”一词，删除了短语“维护和/或”，删除了条目注释。]

3.1.15 cybersecurity event(网络安全事件)

与项目（3.1.25）或部件（3.1.7）有关的网络安全信息（3.1.18）。

3.1.16 cybersecurity goal(网络安全目标)

与一个或多个威胁情景相关的概念级网络安全要求（3.1.33）。

3.1.17 cybersecurity incident(网络安全事故)

可能涉及脆弱性的实地情况 (3.1.38) 开发

3.1.18 cybersecurity information(网络安全信息)

与网络安全有关的信息 (3.1.9) , 其相关性尚未确定。

3.1.19 cybersecurity interface agreement(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 cybersecurity property(网络安全财产)

可以值得保护的属性。

注: 属性包括保密性、完整性和/或可用性。

3.1.21 cybersecurity specification(网络安全规范)

网络安全要求和相应的架构设计 (3.1.1) 。

3.1.22 damage scenario(损害情况)

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 distributed cybersecurity activities(分布式网络安全活动)

项目 (3.1.25) 或部件 (3.1.7) 的网络安全活动, 其责任在客户 (3.1.8) 和供应商之间分配。

3.1.24 impact(影响)

对损害情况下的损害或身体伤害程度的估计 (3.1.22) 。

3.1.25 item(项目)

在车辆层面实现一个功能的组件或组件集 (3.1.7) 。

注 1:如果一个系统在车辆层面实现了一个功能, 它就可以成为一个项目, 否则就是一个部件。

[资料来源:ISO 26262-1:2018^[1], 3.8, 修改 - 术语 "系统 "已被 "组件 "取代, 短语 "适用于 ISO 26262 "和 "或部分功能 "已被省略, 条目注 1 已被替换。]

3.1.26 operational environment (业务环境)

考虑到业务使用中的相互作用的背景

注 1：一个物品（3.1.25）或一个部件（3.1.7）的操作使用可以包括在车辆功能、生产和/或服务与维修中的使用。

3.1.27 out-of-context(上下文无关)

没有在具体项目的背景下开发（3.1.25）。

举例说明具有假定的网络安全要求的处理单元将被集成到不同的项目中。

3.1.28 penetration testing(渗透测试)

网络安全测试，模拟真实世界的攻击，以确定破坏的方式。

网络安全目标(3.1.16)

3.1.29 risk(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 risk management(风险管理)

在风险方面指导和控制组织的协调活动（3.1.29）[资料来源：ISO 31000:2018 [3], 3.2]。ISO 31000:2018 [3], 3.2]。

3.1.31 road user(道路使用者)

使用道路的人

例子：乘客、行人、骑车人、驾车人或车主。

3.1.32 tailor (裁剪)

以与本文件描述不同的方式省略或执行某项活动

3.1.33 threat scenario(威胁情况)

一个或多个资产（3.1.2）的网络安全属性（3.1.20）受到损害的潜在原因，以实现损害情况（3.1.22）。

3.1.34 triage(分流)

分析以确定网络安全信息（3.1.18）与某一项目（3.1.25）的相关性，或

组成部分(3.1.7)

3.1.35 trigger(触发器)

分流的标准 (3.1.34)

3.1.36 validation(验证)

通过提供客观证据，确认具有合乎需要可实现的项目的网络安全目标 (3.1.16)。

[资料来源：ISO/IEC/IEEE 15288:2015[4]，4.1.53，修改后--"特定用途或应用的要求已得到满足"改为"项目的网络安全目标充分且已实现"条目，注释1已被省略。]

3.1.37 verification(核查)

通过提供客观证据，确认特定要求已得到满足

[SOURCE:ISO/IEC/IEEE 15288:2015[4]，4.1.54，修改后--条目的注1被省略。]

3.1.38 vulnerability(脆弱性)

可作为攻击路径 (3.1.4) 的一部分被利用的弱点 (3.1.40)。

[资料来源：ISO/IEC 27000:2018[5]，3.77，修改后--省略了"资产或控制的"这句话；"被一个或多个威胁"这句话被"作为攻击路径的一部分"取代。]

3.1.39 vulnerability analysis(脆弱性分析)

系统地识别和评估脆弱性 (3.1.38)。

3.1.40 weakness(弱点)

可导致不良行为的缺陷或特征

例子 1 缺少要求或规范。

例子 2 建筑或设计缺陷，包括安全协议的不正确设计。

例子 3 实施弱点，包括硬件和软件缺陷，不正确地实施安全协议。

例子 4 操作过程或程序中的缺陷，包括误操作和用户培训不足。

例子 5 使用过期或废弃的功能，包括加密算法。

3.2 缩略语

CAL	网络安全保障等级
CVSS	常见漏洞评分系统
E/E	电气和电子
ECU	电子控制单元
OBD	车载诊断仪
OEM	原始设备制造商
PM	许可
RC	建议
RQ	要求
RASIC	责任、批准、支持、知情、咨询
TARA	威胁分析和风险评估
WP	工作成果

4 整体考虑

一个项目包括车辆中所有的电子设备和软件（即其组件），这些设备和软件参与实现车辆层面上的特定功能，例如制动。一个项目或一个部件与它的运行环境相互作用。

本文件的应用仅限于系列化生产的道路车辆（即不是原型车）的网络安全相关项目和部件，包括售后和服务部件。外部系统为了网络安全的目的,可以考虑对车辆（如后端服务器）的安全保护，但不在本文件的范围内。

本文件从单个项目的角度来描述网络安全工程。本文件没有规定在道路车辆的 E/E 架构中对项目进行适当的功能分配。对于车辆整体而言，可以考虑车辆 E/E 架构或其网络安全相关项目和组件的网络安全案例集。如果本文件中描述的网络安全活动是在项目和部件上进行的，那么不合理的车辆网络安全风险就会得到解决。

如图 2 所示，本文件中描述的一个组织的整体网络安全风险管理适用于所有生命周期阶段。

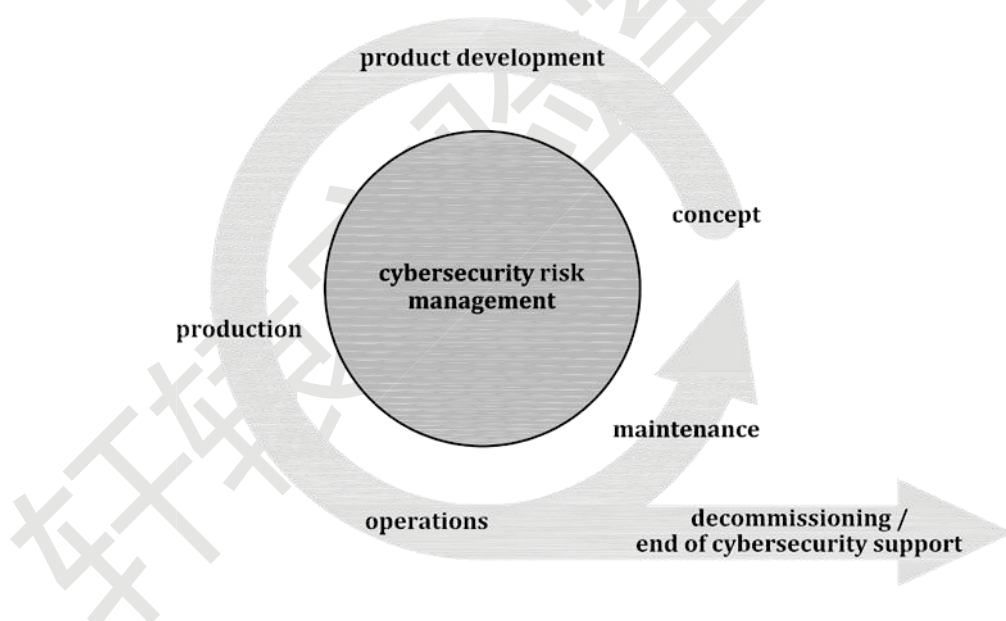


图 2 - 整体网络安全风险管理

网络安全风险管理适用于整个供应链，以支持网络安全工程。汽车供应链表现出多样化的合作模式。并非所有的网络安全活动都适用于参与某个特定项目的所有组织。网络安全活动可以根据具体情况的需要进行调整（见第 6 条）。某一特定项目或部件的开发伙伴就工作分工达成一致，以便开展适用的网络安全活动（见第 7 条）。

图 3 显示了一个项目、功能、组件和相关术语之间的关系。

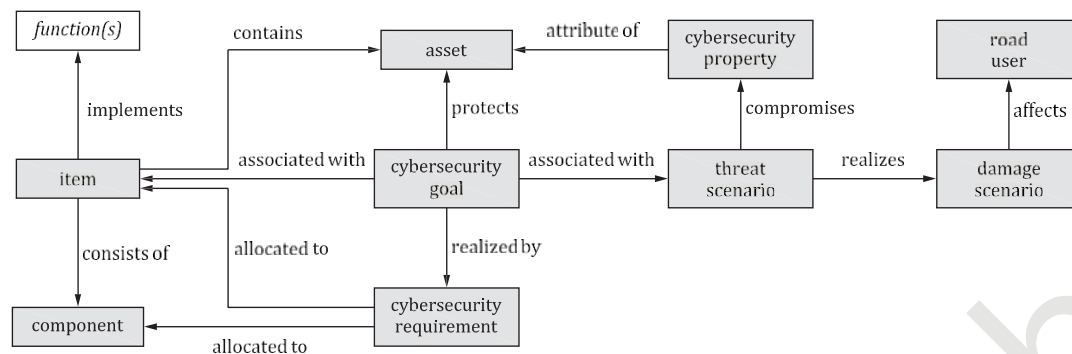


图 3 - 项目、功能、组件和相关术语之间的关系

第 15 条描述了评估网络安全风险的模块方法，这些方法在其他条款所述的网络安全活动中被援引。

在网络安全工程方面的分析活动，确定和探索具有恶意的抽象对手行为者所采取的潜在行动，以及车辆 E/E 系统的网络安全遭到破坏后可能产生的损害。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深入分析和减轻具体的网络安全风险（参见 ISO/TR 4804 [6]）。网络安全监测、补救和事件响应活动是对概念和产品开发活动的补充，作为一种被动的方法，承认环境中不断变化的条件（如新的攻击技术）和不断需要识别和管理道路车辆 E/E 系统的弱点和漏洞。

深度防御的方法可用于减轻网络安全风险。深度防御方法利用各层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一个层，另一个层可以帮助遏制攻击并保持对资产的保护。

5 组织网络安全管理

5.1 综述

为了实现网络安全工程，该组织建立并维持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。这涉及到规定组织规则和程序，并根据本文件的目标进行独立审计。

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体系。

5.2 目标

本条款的目标是：

- a) 确定网络安全政策以及网络安全的组织规则和程序。
- b) 指定开展网络安全活动所需的责任和相应的权限。
- c) 支持网络安全的实施，包括提供资源和管理网络安全进程与相关进程之间的相互作用。
- d) 管理网络安全风险。
- e) 建立并维持一种网络安全文化，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) 建立和维护支持维护网络安全的管理制度。
- h) 提供证据表明工具的使用不会对网络安全产生不利影响；以及
- i) 进行组织网络安全审计。

5.3 输入

5.3.1 先决条件

无

5.3.2 进一步的支持信息

可以考虑以下信息：

——符合支持质量管理的标准的现有证据。

例子：IATF 16949[7]与 ISO 9001[8]、ISO 10007[9]、Automotive SPICE®(汽车 SPICE® [13]是商业上可获得的合适产品的一个例子。这些信息是为了方便本文件的用户而提供的，并不构成 ISO 对这些产品的认可)、ISO/IEC 330xx 系列标准[10]、ISO/IEC/IEEE 15288[11]和 ISO/IEC/IEEE 12207[12]相结合。

5.4 要求和建议

5.4.1 网络安全治理

[RQ-05-01] 组织应确定网络安全政策，包括：

- a)承认道路车辆网络安全风险；
- b)执行管理层对管理相应的网络安全风险的承诺；

注 1 网络安全政策可以包括与组织的目标和其他政策的链接。

注 2 网络安全政策可以包括一项声明，说明对组织的产品或服务组合的一般威胁情况的风险处理，考虑到外部或内部的情况。

[RQ-05-02] 组织应建立并维持规则和程序来：

- a)能够实施本文件的要求；
- b)支持相应活动的执行；

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以包括活动的付出-收益考虑。

注 4 规则和流程涵盖概念、产品开发、生产、运营、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 有关漏洞披露的规则和流程，例如作为信息共享的一部分，可以按照 ISO 29147[14]进行规定。

注 6 图 4 概述了总体网络安全政策（见[RQ-05-01]）与具体组织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。

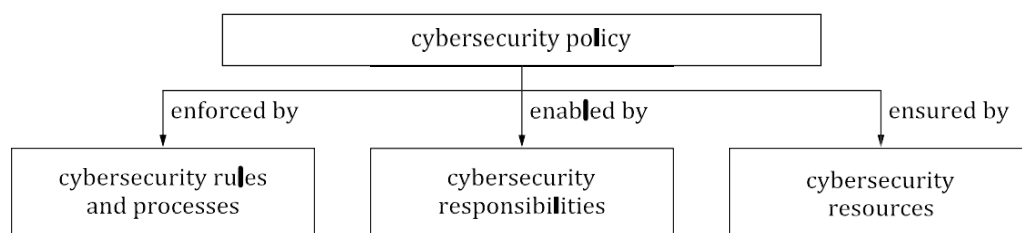


图 4 - 网络安全的进展情况

[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力。

注 7 这涉及到组织活动以及依赖项目的活动。

[RQ-05-04] 本组织应提供解决网络安全的资源。

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 2 熟练的人员和合适的工具来进行网络安全活动。

[RQ-05-05] 组织应确定与网络安全相关或互动的学科，并在这些学科之间建立和保持沟通渠道，以便：

- a) 确定是否以及如何将网络安全纳入现有流程；
- b) 协调相关信息的交流；

注 9 协调可以包括在各学科之间分享流程和使用策略和工具。

注 10 学科包括信息技术安全、功能安全和隐私。

例 3 跨学科的交流：

- 威胁情况和危险（参见 ISO 26262-1:2018[1], 3.75）信息；
- 网络安全目标和安全目标（参见 ISO 26262-1:2018 [1], 3.139）；
- 网络安全要求与功能安全要求冲突或竞争（参见 ISO 26262- 1:2018 [1], 3.69）。

5.4.2 网络安全文化

[RQ-05-06] 组织应培养和维持一种强大的网络安全文化。

注 1 例子见附件 B。

[RQ-05-07] 组织应确保被指派网络安全角色和责任的人员具备履行这些角色和责任的能力和意识。

注 2 能力、意识和培训计划可以包括：

- 关于网络安全的组织规则和程序，包括网络安全风险管理；
- 与网络安全相关的学科的组织规则和程序，如功能安全和隐私；
- 领域知识；
- 系统工程；
- 与网络安全有关的方法、工具和准则；
- 已知的攻击方法和网络安全控制。

[RQ-05-08] 组织应建立并保持一个持续改进过程。

例 持续改进过程，包括：

——从以前的经验中学习，包括通过网络安全监测和观察内部和外部的网络安全相关信息来收集网络安全信息。

- 学习与网络安全有关的信息，了解该领域内类似应用的产品。
- 得出改进意见，以便在以后的网络安全活动中加以应用。
- 向适当的人传达有关网络安全的经验教训。
- 根据[RQ-05-02]检查组织规则和程序的适当性。

注 3 持续改进适用于本文件中的所有网络安全活动。

5.4.3 信息共享

[RQ-05-09] 组织应界定在哪些情况下需要、允许或禁止在组织内部或外部共享与网络安全有关的信息。

注 共享信息的情况可以基于以下几点：

- 可以共享的信息类型；
- 共享的批准程序；
- 对编辑信息的要求；
- 源头归属的规则；
- 为特定当事方提供的通信类型；
- 漏洞披露程序（见 5.4.1 的注 5）；

——对接收方处理高度敏感信息的要求。

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

例 公共、内部、机密、第三方机密等安全分类级别的调整。

5.4.4 管理系统

[RQ-05-11] 该组织应按照国家或同等标准建立一个质量管理体系，以支持网络安全工程，其中包括：

例 1 IATF 16949[7]与 ISO 9001[8]相结合

a) 变革管理

注 1 网络安全中的变更管理的范围是管理项目及其组成部分的变更，以便继续实现适用的网络安全目标和要求，例如，对照生产控制计划审查生产过程的变更，以防止这种变更带来新的漏洞。

b) 文件管理

c) 配置管理

d) 要求管理

[RQ-05-12] 为维护现场产品的网络安全所需的配置信息应保持可用，直到对产品的网络安全支持结束，以便能够采取补救行动。

注 3 归档构建环境对确保以后使用配置信息很有用。

例 2 材料清单，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 条的活动。

例 3 IEC 62443 2-1 [15]

5.4.5 工具管理

[RQ-05-14] 应管理能够影响项目或部件网络安全的工具。

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。

例 2 在生产过程中使用的工具，如闪存写入器、生产线末端测试器。

例 3 用于维护的工具，如板载诊断工具或重新编程工具。注意这种管理可以通过

以下方式建立:

- 应用的用户手册与勘误表;
- 防止非故意的使用或行动;
- 工具用户的访问控制;
- 对该工具的认证;

[RC-05-15] 支持网络安全事件补救行动的适当环境 (见 13.3) 应该是可重复的, 直到产品的网络安全支持结束。

例 4 用于再现和管理漏洞的测试、软件构建和开发环境。

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

[RC-05-16] 工作产品应按照信息安全管理系统进行管理。

例 工作成果可以存储在一个文件服务器上, 以保护它们不被擅自更改或删除。

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, 以判断组织程序是否达到本文件的目标。

注 1 网络安全审计可以包括在根据质量管理体系标准进行的审计中, 或与之相结合, 例如 IATF 16949[7]与 ISO 9001[8]相结合。

注 2 独立性可以基于, 例如, ISO 26262 系列[16]。

注 3 执行审计的人员可以是组织的内部或外部人员。

注 4 为确保组织流程仍然适合网络安全, 可以定期进行审计。

注 5 图 7 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 工作成果

[WP-05-01] 根据 5.4.1 至 5.4.3 的要求制定的网络安全政策、规则和流程

[WP-05-02] 5.4.2 的[RQ-05-07]产生的能力管理、意识管理和[RQ-05-08]产生的持续改进的证据

[WP-05-03] 根据 5.4.4 和 5.4.6 的要求产生的组织管理系统的证据

[WP-05-04] 工具管理的证据，源于 5.4.5 的要求

[WP-05-05] 根据 5.4.7 的要求产生的组织网络安全审计报告

轩辕实验室 XYLab

6 依靠项目的网络安全管理

6.1 综述

本条款描述了关于特定项目的网络安全开发活动管理的要求。

依靠项目的网络安全管理包括责任的分配（见 6.4.1）和网络安全活动的规划（见 6.4.2）。本文件以通用的方式定义了需求，因此它可以应用于各种项目和组件。此外，还可以根据网络安全计划中定义的理由，进行定制（见 6.4.3）。可以使用裁剪的例子包括：

- 再利用（见 6.4.4）
- 组件脱离背景（见 6.4.5）
- 使用一个现成的组件（见 6.4.6）
- 更新（见 13.4）

物品和部件的再利用是一种可能的发展战略，无论是否对物品、部件或其操作环境进行修改，都可以应用。然而，修改可能会引入原始项目或组件可能没有考虑到的漏洞。此外，可能在已知的攻击中出现了变化，例如：

- 攻击技术的演变
- 新出现的漏洞，例如从网络安全监测（见 8.3）和/或网络安全事件评估（见 8.4）

中得知的漏洞

- 自最初开发以来，资产的变化

如果最初的项目或组件是按照本文件开发的，那么该项目或组件的再利用是基于现有的工作产品。如果该项目或组件最初不是按照本文件开发的，则可以在现有文件的基础上进行再利用，并说明理由。

一个组件可以被开发出来，即基于一个假设的环境。一个组织可以在与客户接触或达成商业协议之前，为不同的应用和不同的客户开发通用组件。供应商可以对背景和预期用途做出假设。在此基础上，供应商可以推导出对环境外开发的要求。例如，一个微控制器可以被开发出来。

现成的组件是指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，第三方软件库、开放源码软件组件。现成的组件不被认为是按照本文件的要求开发的。

图 5 显示，根据本文件，现成的组件和非现成的组件都可以被集成到一个项目或组件中。集成可以涉及到与 6.4.4 中的重用分析类似的活动，如果为了解决无效的假设而进行修改，则适用于变更管理（见 5.4.4）。可以对打算集成的部件和/或作为集成目标的部件或项目进行修改。

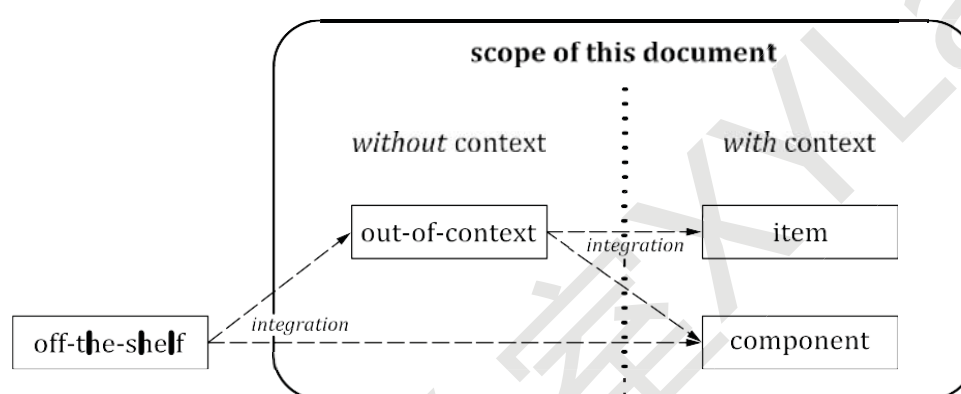


图 5 - 现成的和非现成的组件的整合

网络安全案例（见 6.4.7）是对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）独立判断一个项目或组件的网络安全，是决定释放后开发（见 6.4.9）的一个输入。

6.2 目标

本条款的目标是：

- 指定有关项目网络安全活动的责任；
- 计划网络安全活动，包括定义专门的网络安全活动；
- 创建一个网络安全案例；
- 进行网络安全评估（如适用）；
- 从网络安全的角度决定该项目或组件是否可以释放后开发；

6.3 输入

6.2.1 先决条件

无

6.3.2 进一步的支持信息

可以考虑以下信息：

——组织网络安全审计报告[WP-05-03]

——项目计划

6.4 要求和建议

6.4.1 网络安全责任

[RQ-06-01]应根据[RQ-05-03]分配和通报有关项目网络安全活动的责任。

注：网络安全活动的责任可以转移，前提是要进行沟通并提供相关信息。

6.4.2 网络安全规划

[RQ-06-02] 为了决定项目或部件所需的网络安全活动，应分析该项目或部件以确定：

a)该项目或组件是否与网络安全有关；

注 1 附件 D 提供了一个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，那么就没有网络安全活动，因此不继续进行网络安全规划；

b)如果该项目或部件与网络安全有关，则该项目或部件是新开发还是重复使用；

c)是否按照 6.4.3 的规定进行了裁剪；

[RQ-06-03] 网络安全计划应包括：

a)一项活动的目标；

b)对其他活动或信息的依赖性；

c)负责执行一项活动的人员；

d)执行一项活动所需的资源；

e)起始点或终结点，活动预期的持续周期；

f)确定要产生的工作产品；

[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根据网络安全计划跟踪网络安全活动进展的责任。

[RQ-06-05] 网络安全计划应是：

- a)在开发项目计划中提及的；
- b)包括在项目计划中，从而使网络安全活动可以区分开来；

注 3 网络安全计划可以纳入与其他计划（如项目计划）的交叉引用，这些计划也属于配置管理（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，规定在概念和产品开发阶段需要进行的网络安全活动。

[RQ-06-07] 当确定要进行的活动发生变化或细化时，应更新网络安全计划。

注 4 网络安全计划可以在发展过程中逐步完善。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 15.8 的分析确定的风险值为 1 的威胁情景，可以省略与 9.5、条款 10 和条款 11 符合性。

注 5 这些威胁情况可能会对网络安全产生影响，如果是这样，就会对相应的风险进行处理，尽管可能没有本文件中定义的那么严格。

注 6 可以根据网络安全案例中定义的理由来论证对此类风险的处理是否充分，该理由可以基于符合质量管理标准，如 IATF 16949[7]与 ISO 9001[8]相结合，并结合其他措施，例如：

- 网络安全意识保证
- 质量人员的网络安全培训
- 组织的质量管理体系中规定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在开发后发布之前和发布时进行更新并保持准确性。

[RQ-06-10] 如果网络安全活动是分布式的，客户和供应商应根据条的 7 规定，就各自的网络安全活动和接口各自确定一个网络安全计划。

[RQ-06-11] 网络安全计划应按照 5.4.4 的规定，接受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 5.4.4 的规定，接受配置管理、变更管理、需求管理和文档管理。

6.4.3 裁剪

[PM-06-13] 一项网络安全活动可能是量身定做的。

[RQ-06-14] 如果一项网络安全活动是有针对性的，那么应提供并审查为什么这种针对性足以实现本文件的相关目标的理由。

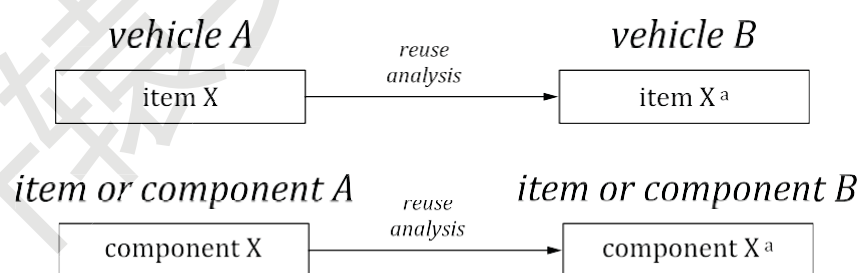
注 由于由供应链中的另一实体执行而未执行的活动不被视为量身定制，而是被视为分布式网络安全活动（见条 7）。然而，网络安全活动的分布可以导致联合定制（见 7.4.3）。

6.4.4 再利用

[RQ-06-15] 如果一个项目或组件已经开发出来且：

- a) 计划进行修改
- b) 计划在另一个操作环境中重新使用

例 1 在新的操作环境中安装现有的项目或部件，或升级与之相互作用的其他项目或部件而导致的环境的修改（见图 6）。



a 可以作为再利用分析的结果而改变

图 6 - 重复使用分析示例

c) 计划不加修改地重新使用，并且有关该项目或组件的信息有相关的变化。

例 2 已知攻击和漏洞的变化，或威胁情景的变化。

注 1 在确定是否可以重用时，要考虑现有的工作产品。

注 2 修改可以包括设计上的修改或实施上的修改，其中：

——设计修改可以来自于需求的修改，例如功能或性能的提升。

——实施的修改可能来自对软件的修正，或使用新的生产或维护工具，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到物品或部件的功能行为、资产或网络安全属性，则被视为修改。

[RQ-06-16] 对一个项目或部件的再利用分析应：

- a) 确定对该项目或部件的修改以及对其操作环境的修改。
- b) 分析修改的网络安全影响，包括对网络安全主张的有效性和以前作出的假设的影响。

例 3 对网络安全要求、设计和实施、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) 确定受影响或丢失的工作成果；

例 4 TARA 考虑新的或修改的资产、威胁情景或风险值。

- d) 在网络安全计划中明确规定符合本文件的必要网络安全活动（见 6.4.2）。

注 4 这可能意味着裁剪（见 6.4.3）。

[RQ-06-17] 一个组件的再利用分析应评估是否：

- a) 该组件能够满足将被集成的项目或组件所分配的网络安全要求；
- b) 现有的文件足以支持整合到一个项目中，或整合到另一个组件中；

6.4.5 组件脱离背景

[RQ-06-18] 对开发的非情境组件的预期用途和情境的假设，包括外部接口，应在相应的工作产品中予以记录。

[RQ-06-19] 对于开发一个脱离背景的组件，网络安全要求应基于[RQ-06-18]的假设。

[RQ-06-20] 对于整合一个在背景之外开发的组件，应验证[RQ-06-18]的网络安全主张和假设。

6.4.6 现成的组件

[RQ-06-21] 在集成一个现成的组件时，应收集和分析与网络安全有关的文件，以确定是否：

- a) 分配的网络安全要求可以得到满足；
- b) 该部件适用于预期用途的具体应用环境；
- c) 现有文件足以支持网络安全活动。

[RQ-06-22] 如果现有文件不足以支持现成组件的集成，那么应确定并执行符合本文件的网络安全活动。

例 有关漏洞的文件不充分。

注 这可能意味着量身定做（见 6.4.3）。

6.4.7 网络安全案例

[RQ-06-23] 应创建一个网络安全案例，为该项目或组件的网络安全提供论据，并由工作产品加以支持。

注 1 部分论据可以是隐含的（例如，如果部分论据从汇编的工作成果中可以看出，那么这部分论据可以省略）。

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，其中引用了各方产生的工作产品的证据。项目的整体论证由所有各方的论证来支持。

注 3 网络安全案例考虑了开发后的网络安全要求[WP-10-02]。

6.4.8 网络安全评估

[RQ-06-24] 在决定是否对某一项目或部件进行网络安全评估时，应以基于风险的方法为依据说明理由。

注 1 理由可以基于以下几点：

- TARA 结果（见条 15）
- 待开发的项目或部件的复杂性
- 组织规则和程序所规定的标准（见 5.4.1）

注 2 如果不进行网络安全评估，可将理由记录在网络安全案例中。

[RQ-06-25] 应独立审查[RQ-06-24]的基本原理。

注 3 独立计划可以基于 ISO 26262 系列[16]。

[RQ-06-26] 网络安全评估应判断该项目或组件的网络安全情况。

注 4 现有的证据是由网络安全活动的记录结果，即工作产品（见附件 A）提供的。

注 5 图 7 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。

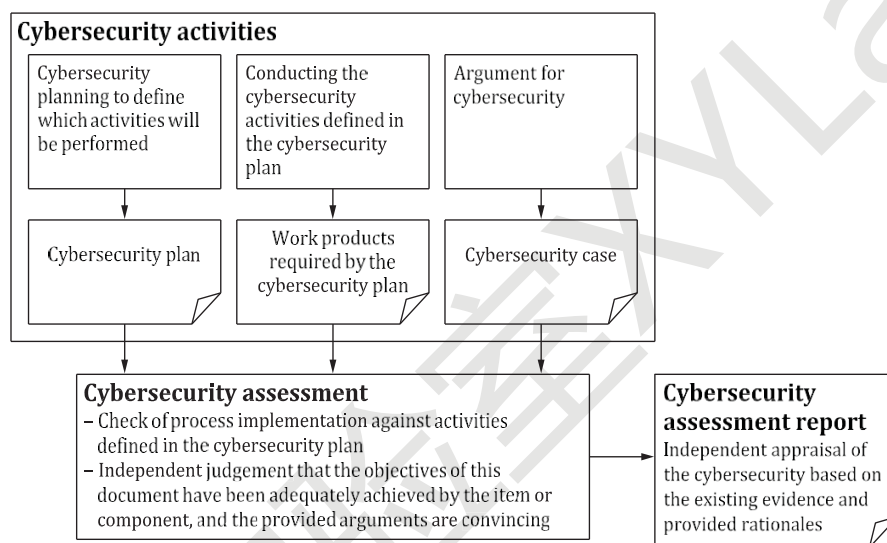


图 7 - 网络安全评估与其他网络安全活动的关系

注 6 网络安全评估可以分步骤进行，以促进尽早解决所发现的问题。

注 7 网络安全评估可以重复或补充，例如，由于变化，以前的网络安全评估提供了一个负面的建议或发现了一个漏洞。

[RQ-06-27] 应根据[RQ-06-01]任命一名负责计划和独立进行网络安全评估的人员。

注 8 独立计划可以基于 ISO 26262 系列[16]。

例 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。

[RQ-06-28] 进行网络安全评估的人应具备：

- a) 获得相关信息和工具；
- b) 执行网络安全活动的人员的合作。

[PM-06-29] 网络安全评估可基于对是否实现本文件的目标的判断。

[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) 对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;

注 9 适当性和有效性可以通过使用为验证目的而进行的先前审查来判断。

- d) 如果提供了理由, 证明实现了本文件的目标。

注 10 负责创建工作产品的人可以提供一个理由, 说明为什么要实现本文件的相应目标, 以促进网络安全评估, 考虑[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理由。

[RQ-06-31] 网络安全评估报告应包括对该项目或部件的网络安全的接受、有条件接受或拒绝的建议。

注 12 评估报告还可以包括持续改进的建议。

[RQ-06-32] 如果按照[RQ-06-31]提出有条件接受的建议, 那么网络安全评估报告应包括接受的条件。

6.4.9 后续开发的发布

[RQ-06-33] 以下工作成果应在发布前提供给开发后的人:

- a) 网络安全案[WP-06-02];
- b) 如果适用, 网络安全评估报告[WP-06-03];
- c) 开发后的网络安全要求[WP-10-02]。

[RQ-06-34] 项目或部件开发后的发布应满足以下条件:

- a) 网络安全案例为网络安全提供的论据是令人信服的;
- b) 网络安全评估确认了网络安全案例 (如适用) ;
- c) 开发后阶段的网络安全要求被接受。

注 变化可能会导致对开发后的版本进行重新评估, 例如对网络安全要求的变化。

6.5 工作成果

[WP-06-01] 网络安全计划，由 6.4.1 至 6.4.6 的要求产生

[WP-06-02] 网络安全案例，源于 6.4.7 的要求

[WP-06-03] 根据 6.4.8 的要求产生的网络安全评估报告（如适用）

[WP-06-04] 根据 6.4.9 的要求，发布开发后报告

轩辕实验室 XYLab

7 分布式网络安全活动

7.1 综述

如果项目或组件的网络安全活动的责任被分配，本条款适用。

本条款描述了对分布式网络安全活动的管理适用于：

- a) 在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；
- c) 在协议适用于客户/供应商界面的所有阶段。内部供应商可以用与外部供应相同的方式进行管理。

例如，在开发过程中，一级组织可以是原始设备制造商的供应商，而在另一种合同关系中，一级组织可以是二级组织的客户，以获得某个部件。这在图 8 中得到了说明。

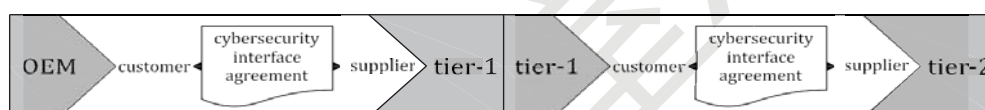


图 8 - 供应链中客户/供应商关系的用例

7.2 目标

本条款的目的是定义客户和供应商之间分布式网络安全活动的互动、依赖和责任。

7.3 输入

无

7.4 要求和建议

7.4.1 供应商能力

[RQ-07-01] 应评估候选供应商按照本文件规定进行开发和（如适用）进行后期开发活动的能力。

注 1 该评价支持供应商的选择，可以基于供应商符合本文件的能力，也可以基于对另一国家或国际标准在网络安全工程方面的先前实施情况的评价。

[RC-07-02] 为了支持客户对供应商能力的评估，供应商应提供网络安全能力的记

录。

注 2 网络安全能力的记录可以包括：

——组织有关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

安全的网络安全最佳做法）；

——持续的网络安全活动（见第 8 条）和网络安全事件响应（见第 13 条）的证据；

——以前的网络安全评估报告摘要。

7.4.2 要求报价

[RQ-07-03] 客户向候选供应商发出的报价请求应包括：

a) 正式要求符合本文件的规定；

b) 预计供应商将按照 7.4.3 的规定承担网络安全责任；

c) 与供应商报价的项目或部件有关的网络安全目标和/或网络安全要求集；

例 与信息验证有关的网络安全要求。

7.4.3 职责的统一

[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) 指定客户和供应商在网络安全方面的联络点；

b) 确定由客户和供应商分别开展的网络安全活动；

例 1 由客户进行车辆层面的网络安全验证。

例 2 关于开发后的网络安全活动的分布。

例 3 关于供应商开发的部件或工作产品的网络安全评估可由第三方、客户或供应商进行。

c) 如果适用的话，根据 6.4.3 的规定，共同制定网络安全活动；

d) 将要分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流程序；例如，关于风险。

——与接口有关的流程、方法和工具，以确保客户和供应商之间的兼容性，如适当处理数据和确保用于传递该数据的通信网络的安全；

——角色的定义；

——沟通和记录项目或部件的变化的方法，包括可能的 TARA 的重复；

——在需求管理工具上保持一致；

——网络安全评估的结果。

e)关于分布式网络安全活动的里程碑；

f)对该项目或组件的网络安全支持结束的定义。

[RC-07-05] 网络安全接口协议应在分布式网络安全活动开始前由客户和供应商共同商定。

[RQ-07-06] 如果存在需要根据[RQ-08-07]进行管理的已识别的漏洞，客户和供应商应就行动和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，那么客户和供应商应各自通知对方，以便做出适当的决定和行动。

[RC-07-08] 应在责任分配矩阵中规定责任。

注 2 可以使用 RASIC 表，见附件 C。

7.5 工作成果

[WP-07-01] 网络安全接口协议，由 7.4.3 的要求产生。

8 持续的网络安全活动

8.1 综述

持续的网络安全活动是在生命周期的所有阶段进行的，可以在特定项目之外进行。

网络安全监测（见 8.3）收集网络安全信息，并分析网络安全信息，根据定义的触发器进行分流。

网络安全事件评估（见 8.4）确定网络安全事件是否为某一项目或组件带来弱点。

脆弱性分析（见 8.5）检查弱点，评估某一特定弱点是否可以被利用。

漏洞管理（见 8.6）跟踪和监督对项目或组件中已发现的漏洞的处理，直到它们的网络安全支持结束。

8.2 目标

本条款的目标是：

- a) 监测网络安全信息以确定网络安全事件；
- b) 评估网络安全事件，以确定薄弱环节；
- c) 从弱点中识别脆弱性；
- d) 管理已查明的漏洞。

8.3 网络安全监测

8.3.1 输入

8.3.1.1 先决条件

应提供以下信息：

——触发器开发的规则和流程包括在[WP-05-01]中。

8.3.1.2 进一步的支持信息

可以考虑以下信息：

——项目定义[WP-09-01]

——网络安全索赔[WP-09-04]

——网络安全规范[WP-10-01]

——威胁情况[WP-15-03]

——过去的脆弱性分析[WP-08-05]

——从外地收到的信息

例 漏洞扫描报告、维修信息、消费者使用信息

8.3.2 要求和建议

[RQ-08-01] 应选择收集网络安全信息的来源。

注 1 可以选择内部和/或外部来源。

注 2 内部来源可以包括 8.3.1.2 中列出的那些。

注 3 外部来源可以包括:

——研究人员

——商业或非商业来源

——组织的供应链

——组织的客户

——政府来源

例 最先进的攻击方法的来源。

[RQ-08-02] 应定义并维护触发器，以便对网络安全信息进行分类。

注 4 触发器可以包括关键词、配置信息的参考、组件或供应商的名称。

[RQ-08-03] 应收集和分流网络安全信息，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 工作成果

[WP-08-01] 网络安全信息的来源，源于[RQ-08-01]

[WP-08-02] 触发器，产生于[RQ-08-02]

[WP-08-03] 网络安全事件，由[RQ-08-03]引起的网络安全事件

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[WP-08-03]
- 开发后的网络安全要求[WP-10-02]
- 根据[RQ-05-12]的规定，配置信息

8.4.1.2 进一步的支持信息

可以考虑以下信息：

- 项目定义[WP-09-01]
- 网络安全规范[WP-10-01]
- 过去的脆弱性分析[WP-08-05]。

8.4.2 要求和建议

[RQ-08-04] 应评估网络安全事件，以确定项目和/或组件的弱点。

注 1 这项活动可以与[RQ-08-03]的分流相结合。

注 2 如果存在一个弱点，并且有可用的补救措施（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（见 8.6）作为一个假定的漏洞来处理，而无需任何其他活动。

注 3 威胁情景[WP-15-03]可根据该评估的结果进行更新。

8.4.3 工作成果

[WP-08-04] 网络安全事件带来的弱点，源于[RQ-08-04]。

8.5 脆弱性分析

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 如果对一个项目进行脆弱性分析，则使用项目定义；如果对一个部件进行脆弱

性分析，则使用网络安全规范。

8.5.1.2 进一步的支持信息

可以考虑以下信息：

- 网络安全事件中的弱点[WP-08-04]
- 在产品开发过程中发现的弱点[WP-10-05]
- 过去的脆弱性分析[WP-08-05]
- 攻击路径[WP-15-05]
- 核查报告[WP-10-04]和[WP-10-07]
- 过去网络安全事件的信息

8.5.2 要求和建议

[RQ-08-05] 应分析弱点以确定脆弱性

注 1 该分析可包括：

- 对架构的分析
- 按照 15.6 的规定进行攻击路径分析
- 根据 15.7 的规定，攻击可行性等级

注 2 可以进行根本原因分析，以确定导致弱点成为漏洞的可能性的任何潜在因素。

例 1 攻击路径分析显示不存在攻击路径，因此，该弱点不被当作漏洞处理。

例 2 利用该弱点的攻击可行性等级很低，因此，该弱点不被视为漏洞。

[RQ-08-06] 对于未被确定为漏洞的弱点应提供理由。

8.5.3 工作成果

[WP-08-05] 漏洞分析，源于[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：

——脆弱性分析[WP-08-05]

8.6.1.2 进一步的支持信息

无

8.6.2 要求和建议

[RQ-08-07] 漏洞的管理应做到对每个漏洞。

a) 对相应的网络安全风险进行评估，并按照 15.9 的规定进行处理，使之不存在不合理的风险

b) 通过应用独立于 TARA 的可用补救措施来消除该漏洞

例 开源软件的补丁

注 1 如果脆弱性管理导致项目或部件的变更，则按照[RQ-05-11]进行变更管理。

注 2 有关漏洞的信息可以在分布式网络安全活动范围内（见 7.4.3，如分享攻击路径的知识）和向其他有关各方（见 5.4.3）分享。**[RQ-08-08]** 如果根据 15.9 作出的风险处理决定需要进行网络安全事件应对，则应适用 13.3。

注 3 网络安全事件响应过程可以独立于 TARA 而应用。

8.6.3 工作成果

[WP-08-06] 有管理的漏洞的证据，产生于[RQ-08-07]

9 概念

9.1 综述

概念阶段涉及对项目中实施的车辆级功能的考虑。在本条款中，项目及其运行环境被确定为“项目定义”（见 9.3）。项目定义构成了后续活动的基础。

本条款还规定了项目的网络安全目标（见 9.4），这是最高级别的要求。为此对网络安全风险进行了评估，这是通过使用第 15 条的方法实现的（另见附件 H，图 H.1）。此外，9.4 规定了网络安全要求，用于解释为什么认为风险保留或分担是充分的。

网络安全概念（见 9.5）由网络安全要求和对操作环境的要求组成，两者都来自于网络安全目标并基于对该项目的全面看法。

9.2 目标

本条款的目标是：

- a) 在网络安全的背景下，定义项目、其运行环境和它们的相互作用；
- b) 明确网络安全目标和网络安全要求；
- 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

无

9.3.1.2 进一步的支持信息

可以考虑以下信息：

——有关该项目和操作环境的现有信息。

例 车内 E/E 系统结构，包括车内网络、车外网络、参考模型和早期开发的文件。

9.3.2 要求和建议

[RQ-09-01] 应确定物品的下列信息：

- a) 项目边界

注 1 项目边界将项目与它的运行环境区分开来。项目边界的描述可以包括与车辆内部其他项目和与车辆外部 E/E 系统的接口。

b)项目功能

注 2 这描述了项目在生命周期各阶段[如产品开发（测试）、生产、运营、维护和停用]的预期行为，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识别项目的组成部分及其连接，以及项目的外部接口。

注 4 本文件中描述的项目定义，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 ISO 26262 系列[16]的功能安全。

注 5 可以考虑有关制约因素和适用的网络安全标准的信息。

注 6 开发一个脱离背景的组件（见 6.4.5）可以基于对一个假定的（通用）项目的定义和对该项目内组件功能的描述。

[RQ-09-02] 应描述与网络安全有关的项目的操作环境信息。

注 7 对操作环境及其与项目的相互作用的描述，可以识别或分析相关的威胁情景和攻击路径。

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机构都得到了适当的管理。

9.3.3 工作成果

[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 进一步的支持信息

可以考虑以下信息:

——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, 其中包括:

- a) 根据 15.3 的规定进行资产鉴定
- b) 按照 15.4 的规定进行威胁情景识别
- c) 根据 15.5 的规定, 冲击等级
- d) 根据 15.6 的规定, 进行攻击路径分析
- e) 根据 15.7 的规定, 对攻击的可行性进行评级
- f) 按照 15.8 的规定确定风险值

注 1 如果项目定义没有为分析提供足够的信息, 可以假设这些信息。

[RQ-09-04] 根据[RQ-09-03]的结果, 应按照 15.9 的规定为每种威胁情况确定风险处理方案。

注 2 通过消除风险源来避免风险, 可导致按照变更管理 (见 5.4.4) 对该项目进行变更。

[RQ-09-05] 如果一个威胁情景的风险处理决定包括减少风险, 那么应规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的要求。注 4 如果适用, 可以为网络安全目标确定一个 CAL (见附件 E) 。

注 5 可以为项目的任何生命周期阶段规定网络安全目标。

[RQ-09-06] 如果一个威胁情景的风险处理决定包括:

- a) 分担风险;
- b) 保留由于[RQ-09-03]分析过程中使用的一个或多个假设而产生的风险, 则应规定一个或多个相应的网络安全索赔;

注 6 网络安全索赔可被考虑用于网络安全监测。

[RQ-09-07] 应进行核查以确认：

- a) RQ-09-03]的结果在项目定义方面的正确性和完整性；
- b) RQ-09-04]的风险处理决定对[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]的网络安全主张与[RQ-09-04]的风险处理决定之间的完整性、正确性和一致性；
- d) 该项目[RQ-09-05]的所有网络安全目标和[RQ-09-06]的网络安全要求的一致性。

9.4.3 工作成果

[WP-09-02] TARA，由[RQ-09-03]和[RQ-09-04]产生

[WP-09-03] 网络安全目标，源于[RQ-09-05]

[WP-09-04] 网络安全要求，产生于[RQ-09-06]

[WP-09-05] 网络安全目标的核查报告，产生于[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：

- 项目定义[WP-09-01]
- 网络安全目标[WP-09-03]
- 网络安全索赔[WP-09-04]

9.5.1.2 进一步的支持信息

可以考虑以下信息：

- TARA[WP-09-02]

9.5.2 要求和建议

[RQ-09-08] 应描述技术或操作性网络安全控制措施及其相互作用，以实现网络安全目标，同时考虑到：

a)项目的功能之间的依赖性;

b)网络安全索赔;

注 1 说明中可以包括:

——实现网络安全目标的条件, 如预防入侵、检测和监控入侵。

——专门用于处理威胁情况的具体方面的功能, 例如使用安全通信渠道。

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, 为网络安全目标确定项目的网络安全要求和对运行环境的要求。

注 3 网络安全要求可以取决于或包括项目的具体特征, 如更新能力或在操作中获得用户同意的能力。

注 4 对运行环境的要求是在项目之外实现的, 但它们包括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 对作为运行环境一部分的其他项目的要求可以是对这些项目的网络安全要求。

[RQ-09-10] 网络安全要求应分配给该项目, 并在适用时分配给其一个或多个组成部分。

注 6 网络安全控制的描述是对网络安全要求和操作环境要求的具体化和分配的补充, 它们共同构成了网络安全概念。

[RQ-09-11] [RQ-09-08]、[RQ-09-09]和[RQ-09-10]的结果应得到核实以确认。

a)与网络安全目标有关的完整性、正确性和一致性;

b)在网络安全索赔方面的一致性。

9.5.3 工作成果

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

[WP-09-07] 网络安全概念的核查报告, 产生于[RQ-09-11]

10 产品开发

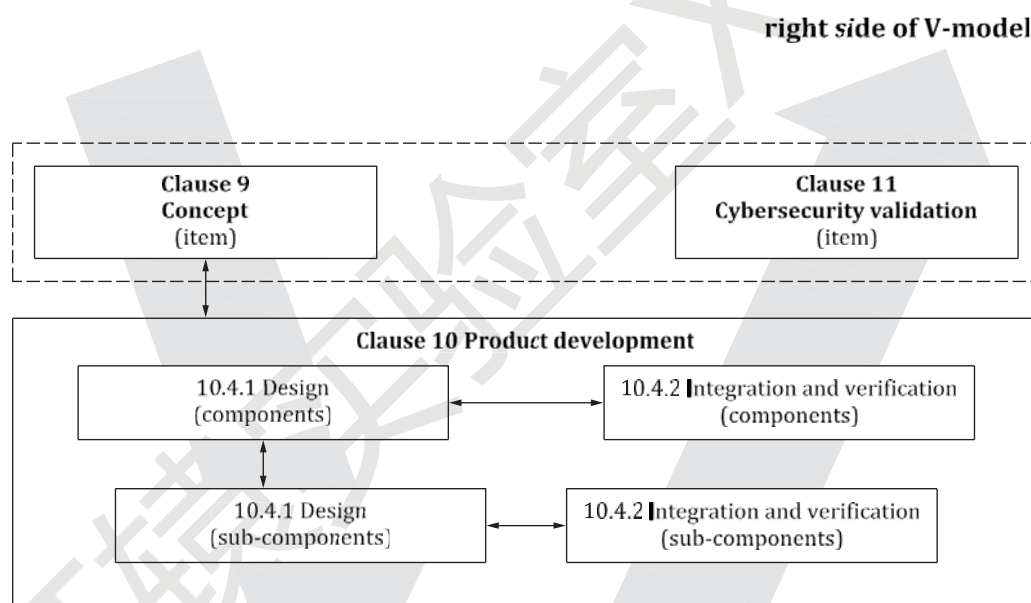
10.1 综述

本条款描述了网络安全要求和架构设计的规范（见 10.4.1）。

此外，本条款描述了集成和验证活动（见 10.4.2）。

这些网络安全活动是反复进行的，直到不需要进一步完善网络安全控制。网络安全规范被定义，并通过验证活动确认网络安全概念的实现。

图 9 说明了如何将产品开发活动应用于基于 V 模型的工作流的例子，其中 10.4.1 对应于 V 模型的左侧，10.4.2 对应于 右侧。在这个例子中，在项目层面下假设了两个抽象层，即组件层和子组件层。这个工作流程可以扩展到涵盖任何抽象层次。



垂直双向箭头描述了在设计期间从更高的架构抽象层面对网络安全规范进行验证，如 10.4.1 所述。

水平双向箭头描述了根据 10.4.2 中描述的网络安全规范对已实施和集成的组件进行验证。

图 9 - V 型模型中产品开发活动的例子

可以采用不同于 V 型模式的开发方式或方法（如敏捷软件开发）。

CAL 可以用来衡量本条款中活动的深度和严密性以及用于这些活动的方法（见附件 E）。

10.2 目标

本条款的目标是：

a)定义网络安全规范；

注 1 这些可以包括现有架构设计中不存在的网络安全相关组件的规范；

b)验证所定义的网络安全规范是否符合更高层次的架构抽象中的网络安全规范；

c)确定该部分的弱点；

注 2 脆弱性分析和管理的在条款 8 中描述；

d)提供证据表明组件的实施和整合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：

——从更高层次的架构抽象中获得网络安全规范[WP-10-01]。

注 1 这可以局限于与正在开发的组件有关的信息，例如：

——分配给开发中的组件的网络安全要求。

——开发中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假设信息。

注 2 对于最高级别的架构抽象的开发，使用项目的网络安全概念[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 进一步的支持信息

可以考虑以下信息：

——项目定义[WP-09-01]；

——网络安全概念[WP-09-06]；

——现有的建筑设计；

——已经建立的网络安全控制；

——从重复使用的组件中找出已知的弱点和漏洞。

10.4 要求和建议

10.4.1 设计

[RQ-10-01] 网络安全规范的定义应基于：

a)网络安全规范来自于更高层次的架构抽象

b)选择实施的网络安全控制措施

例 1 使用带有嵌入式硬件信任锚的独立微控制器来实现安全密钥存储功能，并将信任锚与非安全的外部连接隔离。

注 1 网络安全控制可以从受信任的目录中选择。

c)现有的架构设计，如果适用的话

注 2 网络安全规范包括所定义的架构设计中与满足所定义的网络安全要求有关的子组件之间的接口规范，包括其使用、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：密钥存储的安全管理；调试接口的停用；删除个人身份信息的程序。

注 4 网络安全规范可以包括确定与满足网络安全要求有关的配置和校准参数，以及它们的设置或允许的数值范围，例如为整合硬件安全模块的正确配置。

注 5 可以考虑实施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。

[RQ-10-02] 应将定义的网络安全要求分配给架构设计的组成部分。

[RQ-10-03] 如果适用，应规定在开发组件后确保网络安全的程序。

例 2 正确整合和初始化网络安全控制的程序，以及在整个生产过程中保持网络安全。

[RQ-10-04] 如果设计、建模或编程符号或语言被用于网络安全规范或其实施，在选择这种符号或语言时，应考虑以下几点：

a)在语法和语义上都有一个明确的、可理解的定义

b)支持实现模块化、抽象化和封装化

c)支持使用结构化的构造

d)支持使用安全设计和实施技术

e)整合现有组件的能力

例 3 用另一种语言编写的库、框架、软件组件

f)语言的复原力, 防止因使用不当而出现漏洞

例 4 对缓冲区溢出的复原力

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] 适合网络安全的设计、建模或编程语言的标准 (见[RQ-10-04]), 如果语言本身没有涉及, 则应由设计、建模和编码指南或开发环境涵盖。

例 5 使用 MISRA C:2012 [17]或 CERT C[18], 在 "C" 编程语言中进行安全编码。

例子 6 适合设计、建模和编程语言的标准。

——使用语言子集

——实施强类型化

——使用防御性执行技术

[RC-10-06] 应采用既定的、可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 NIST 特别出版物 800-160 卷[19], 附录 F.1 中给出了网络安全架构设计原则的例子。

[RQ-10-07] 应分析[RQ-10-01]中定义的架构设计, 以确定其弱点。

注 8 可以考虑重复使用的组件的已知弱点和漏洞。

注 9 对已识别的弱点进行脆弱性分析 (见 8.5), 对已识别的弱点进行管理 (见 8.6)。然而, 已识别的弱点可以通过改变架构设计来解决, 而无需进行脆弱性分析。

[RQ-10-08] 应验证所定义的网络安全规范, 以确保其完整性、正确性以及与来自更高架构抽象级别的网络安全规范的一致性。

注 10 核查方法可以包括:

——审查

——分析

——模拟

——原型设计

10.4.2 集成和验证

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

[RQ-10-10] 应考虑规定[RQ-10-09]的整合和验证活动。

a) 既定的网络安全规范

b) 拟用于批量生产的配置，如果适用

c) 有足够的力量来支持所定义的网络安全规范中规定的功能

d) 符合[RQ-10-05]的建模、设计和编码准则

注 1 这可以包括车辆集成和验证

注 2 核查的方法可以包括：

——基于要求的测试

——接口测试

——资源使用评估

——验证控制流和数据流

——动态分析

——静态分析

注 3 如果采用测试验证，可以选择测试用例和测试环境，考虑：

——测试的整合程度，以实现验证目标。

——根据对所选测试环境的分析，例如，由于最终集成的目标处理器的数据字和地址的位宽与处理器仿真或开发环境不同，在随后的集成活动中进行额外测试的必要性。

注 4 推导测试用例的方法可以包括：

——对需求的分析

- 等价类的生成和分析
- 边界值分析
- 基于知识或经验的错误猜测

[RQ-10-11] 如果采用测试验证，应使用定义的测试覆盖率指标评估测试覆盖率，以确定测试活动的充分性。

注 5 标准的测试覆盖率指标对网络安全来说可能是不够的，例如，软件的声明覆盖率。

[RC-10-12] 应进行测试，以确认组件中剩余的未识别的弱点和漏洞被最小化。

注 6 不必要的功能可能包含一个弱点

注 7 测试方法可以包括：

- 功能测试
- 漏洞扫描
- 模糊测试
- 渗透测试

注 8 对已识别的弱点进行脆弱性分析（见 8.5），对已识别的弱点进行管理（见 8.6）。然而，已识别的弱点可以通过改变架构设计来解决，而无需进行脆弱性分析。

[RQ-10-13] 如果不按照[RC-10-12]进行测试，则应提供理由。

注 9 理由可以包括以下考虑：

- 读取组件的攻击面的可行性；
- 有能力（直接或间接地）结合对其他组件的破坏来访问该组件；
- 组件的简单性；

10.5 工作成果

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

[WP-10-02] 开发后的网络安全要求，产生于[RQ-10-03]

[WP-10-03] 根据[RQ-10-04]和[RQ-10-05]产生的建模、设计或编程语言和编码

准则的文件

[WP-10-04] 网络安全规范的验证报告，源于[RQ-10-08]

[WP-10-05] 在产品开发过程中发现的弱点，由[RQ-10-07]和[RC-10-12]产生，
如果适用的话。

[WP-10-06] 集成和验证规范，产生于[RQ-10-10]

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

11 网络安全验证

11.1 综述

本条款描述了该项目在车辆层面的网络安全验证活动（见图 9）。该项目在车辆级别的操作环境中与打算批量生产的配置一起被考虑。

11.2 目标

本条款的目标是：

- a)验证网络安全目标和网络安全主张；
- b)确认该项目实现了网络安全的目标；
- c)确认没有不合理的风险存在；

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[WP-09-03]
- 网络安全索赔[WP-09-04]，如果适用的话

11.3.2 进一步的支持信息

可以考虑以下信息：

- 网络安全概念[WP-09-06]
- 产品开发的工作成果（见 10.5）

11.4 要求和建议

[RQ-11-01] 考虑到批量生产的配置，该项目在车辆层面的验证活动应确认：

- a)在威胁情况和相应的风险方面，网络安全目标是否充分

注 1 如果在验证过程中发现有任何网络安全目标没有解决的风险，可以按照 9.4 来解决。

- b)实现该项目的网络安全目标

c)网络安全索赔的有效性

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 9.5 条和第 10 条的工作成果，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

——对通过第 9 条和第 10 条确定的所有管理风险进行审查

注 3 CAL 可以用来衡量渗透测试的深度和严格程度（见附件 E）

注 4 对[RQ-11-01]验证活动中发现的弱点进行漏洞分析（见 8.5），对发现的漏洞进行管理（见 8.6）。

[RQ-11-02] 应提供选择审定活动的理由。

11.5 工作成果

[WP-11-01] 验证报告，由[RQ-11-01]和[RQ-11-02]产生。

12 生产

12.1 综述

生产涵盖了一个项目或部件的制造和组装，包括车辆层面。建立生产控制计划是为了确保开发后的网络安全要求适用于项目或组件，并确保在生产过程中不能引入漏洞。

12.2 目标

本条款的目标是：

- a) 适用于开发后的网络安全要求；
- 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：

- 发布发展后报告[WP-06-04]
- 开发后的网络安全要求[WP-10-02]

12.3.2 进一步的支持信息

无

12.4 要求和建议

[RQ-12-01] 应建立一个生产控制计划，适用于开发后的网络安全要求

注 1 生产控制计划可以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) 适用于开发后的网络安全要求的步骤顺序
- b) 生产工具和设备
- c) 网络安全控制，以防止生产过程中出现未经授权的更改

例 1 防止对持有软件的生产服务器进行物理访问的物理控制。

例 2 应用加密技术和/或访问控制的逻辑控制。

- d) 方法来确认开发后的网络安全要求得到满足。

注 2 方法可以包括检查和校准检查。

注 3 为了制造一个项目或部件并安装硬件和软件，生产过程中可以使用特权访问。

如果在生产后以未经授权的方式使用，这种访问会给项目或部件带来漏洞。

[RQ-12-03] 应执行生产控制计划；

12.5 工作成果

[WP-12-01] 生产控制计划，产生于[RQ-12-01]和[RQ-12-02]

13 运营和维护

13.1 综述

本条款描述了网络安全事件响应 (见 13.3) 和对现场项目或部件的更新 (见 13.4) 。当一个组织将网络安全事件响应作为脆弱性管理的一部分来调用时，就会发生网络安全事件响应 (见 8.6) 。

更新是在开发后对一个项目或组件所做的改变，可以包括额外的信息，如技术规范、集成手册、用户手册。组织可以出于各种原因发布更新，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。

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

13.2 目标

本条款的目标是：

- a) 确定并实施网络安全事件的补救行动；
- b) 在生产后的项目或组件的更新期间和更新后保持网络安全，直到其网络安全支持结束。

13.3 网络安全事件应对

13.3.1 输入

13.3.1.1 先决条件

无

13.3.1.2 进一步的支持信息

可以考虑以下信息：

- 与引起网络安全事件响应的漏洞有关的网络安全信息
- 脆弱性分析[WP-08-05]

13.3.2 要求和建议

[RQ-13-01] 对于每个网络安全事件，应制定网络安全事件应对计划，包括：

a)补救行动

注 1 补救措施由 8.6 中的脆弱性管理来决定。

b)一个沟通计划

注 2 沟通计划的建立可以涉及内部有关各方，如市场或公共关系、产品开发团队、法律、客户关系、质量管理、采购。

注 3 沟通计划可以包括确定内部和外部的沟通伙伴（如发展、研究人员、公众、当局），并为这些受众开发具体信息。

c)为补救行动分配的责任。

注 4 负责的人应有：

- 受影响的项目或部件，包括遗留项目和部件的专业知识；
- 组织知识（如业务流程、通信、采购、法律）；
- 决定权；

d)记录与网络安全事件有关的新网络安全信息的程序

注 5 可以根据 8.3 收集新的网络安全信息，例如以下信息：

- 受影响的部件
- 相关的事件和漏洞
- 法证数据，如数据日志、碰撞传感器数据
- 终端用户投诉

e)一种确定进展的方法

例 衡量进展的标准是：

- 受影响的项目或组件被修复的百分比
- 受补救行动影响的项目或部件的百分比

f)结束网络安全事件响应的标准

g)采取行动进行关闭。

[RQ-13-02] 应执行网络安全事件应对计划。

13.3.3 工作成果

[WP-13-01] 网络安全事件应对计划，源于[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：

——发布开发后报告[WP-06-04]。

13.4.1.2 进一步的支持信息

可以考虑以下信息：

——网络安全事件应对计划[WP-13-01]

——开发后的网络安全要求[WP-10-02]与更新有关

13.4.2 要求和建议

[RQ-13-03] 车辆内的更新和与更新有关的能力应按照本文件的规定开发。

13.4.3 工作成果

无

14 结束网络安全支持和停用工作

14.1 综述

停用与网络安全支持的结束是不同的。一个组织可以结束对一个项目或组件的网络安全支持，但该项目或组件仍然可以在现场按设计运行。停用和结束网络安全支持都会带来网络安全方面的影响，但这些影响要分开考虑。

停用可以在组织不知情的情况下发生，而且停用程序无法执行，因此停用行为不属于本文件的范围。

在概念和产品开发阶段考虑结束网络安全支持和停用问题。

14.2 目标

本条款的目标是：

- a)传达网络安全支持的结束；
- b)使得在网络安全方面的项目和部件退役；

14.3 网络安全支持的结束

14.3.1 输入

无

14.3.2 要求和建议

[RQ-14-01] 应建立一个程序，以便在一个组织决定结束对某一项目或组件的网络安全支持时向客户通报。

注 1 这些通信可以根据供应商和客户之间的合同要求进行处理。

注 2 可以通过公告的方式向车主传达信息。

14.3.3 工作成果

[WP-14-01] 沟通网络安全支持结束的程序，源于[RQ-14-01]。

14.4 停用

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[WP-10-02]。

14.4.1.2 进一步的支持信息

无

14.4.2 要求和建议

[RQ-14-02] 应提供开发后有关停用的网络安全要求。

注 与这些要求有关的适当文件（如说明、用户手册）可以使网络安全方面的停用工作得以进行。

14.4.3 工作成果

无

15 威胁分析和风险评估方法

15.1 综述

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。这些方法及其工作成果被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进行。本条款中定义的方法是通用模块，可以从项目或部件的生命周期的任何一点系统地调用。

- 资产识别（见 15.3）
- 威胁情景识别（见 15.4）
- 冲击等级（见 15.5）
- 攻击路径分析（见 15.6）
- 攻击可行性等级（见 15.7）
- 风险值的确定（见 15.8）
- 风险治疗决定（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所产生的工作产品的一部分。

关于这些方法的说明，见附件 H，其中有一个实际例子。

组织的影响评级、攻击可行性评级和风险值确定的具体尺度可以应用并映射到本文中定义的相应尺度。

15.2 目标

本条款的目标是：

- a) 确定资产、其网络安全属性和其损害情况
- b) 确定威胁情况
- c) 确定损害情景的影响等级
- d) 确定实现威胁情景的攻击路径
- e) 确定攻击路径被利用的难易程度
- f) 确定威胁情景的风险值

g)为威胁情况选择适当的风险处理方案

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 进一步的支持信息

可以考虑以下信息：

——网络安全规范[WP-10-01]

15.3.2 要求和建议

[RQ-15-01] 应确定损害情况

注 1 损坏情况可以包括：

——项目的功能与不良后果之间的关系

——描述对道路使用者的伤害

——相关资产

[RQ-15-02] 应确定具有网络安全特性的资产，其妥协导致损害情况的发生。

注 2 资产的识别可以基于以下几点：

——对项目定义进行分析

——进行影响评级

——从威胁情景中推导出资产

——使用预定义的目录

例 1 资产是存储在信息娱乐系统中的个人信息（客户的个人喜好），其网络安全属性是保密性。损害情况是，由于保密性的丧失，在未经客户同意的情况下，个人信息被披露。

例 2 资产是制动功能的数据通信，其网络安全属性是完整性。损害情况是在车辆

高速行驶时，由于非故意的完全制动而与后面的车辆发生碰撞（追尾碰撞）。

15.3.3 工作成果

[WP-15-01] 损害情况，由[RQ-15-01]引起的

[WP-15-02] 具有网络安全属性的资产，由[RQ-15-02]产生

15.4 威胁情景识别

15.4.1 输入

15.4.1.1 先决条件

应具备以下条件：

——项目定义[WP-09-01]

15.4.1.2 进一步的支持信息

可以考虑以下信息：

——网络安全规范[WP-10-01]

——损害情况[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]应确定威胁情况并包括：

——目标资产

——资产的网络安全属性受到损害

——导致网络安全财产受损的原因

注 1 进一步的信息可以包括或与威胁情景相关联，例如损害情景、资产之间的技术相互依赖性、攻击者、方法、工具和攻击面。

注 2 威胁情景识别的方法可以使用小组讨论和/或系统方法，例如：

——诱发因合理的可预见的误用或滥用而产生的恶意用例。

——基于 EVITA[20]、TVRA[21]、PASTA[22]、STRIDE（欺骗、篡改、拒付、信息披露、拒绝服务、提升权限）等框架的威胁建模方法。

注 3 一个损害情景可以对应多个威胁情景，一个威胁情景可以导致多个损害情景。

例 欺骗制动 ECU 的 CAN 信息导致 CAN 信息的完整性丧失，从而导致制动功能的完整性丧失。

15.4.3 工作成果

[WP-15-03] 威胁情况，由[RQ-15-03]产生的威胁情况

15.5 影响评级

15.5.1 输入

15.5.1.1 先决条件

应具备以下条件：

——损害情况[WP-15-01]

15.5.1.2 进一步的支持信息

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[WP-15-02]

15.5.2 要求和建议

[RQ-15-04]应根据安全、财务、运营和隐私（S、F、O、P）等影响类别中对道路使用者的潜在不利后果分别评估损害情景。

注 1 本文件不提供不同影响类别之间的关系（如加权）。

注 2 可以考虑其他影响类别。

注 3 如果考虑到额外的影响类别，那么这些类别的理由和解释可以根据条 7 在供应链中共享。

[RQ-15-05] 损害情景的影响等级应按每个影响类别确定为以下之一：

——严重的

——主要的

——中等的

——可以忽略不计的

注 4 财务、运营和隐私方面的影响可根据附件 F 中的表格进行评级。

[RQ-15-06] 与安全有关的影响等级应来自 ISO 26262-3:2018, 6.4.3。

注 5 附件 F 中的表 F.1 可用于将安全影响标准映射到影响等级。

注 6 用于功能安全的评估可以重新用于此目的。

[PM-15-07] 如果一个损害情景导致了一个影响等级，并且可以提出一个论点，即另一个影响类别的每一个影响都被认为是不太重要的，那么对该另一个影响类别的进一步分析可以省略。

例 损坏情况的安全影响被评为“严重”，因此该损坏情况的财务影响不作进一步分析。

15.5.3 工作成果

[WP-15-04] 由[RQ-15-04]至[RQ-15-06]产生的影响评级及相关影响类别。

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]；

注 如果对一个项目进行攻击路径分析，则使用项目定义；如果对一个组件进行攻击路径分析，则使用网络安全规范。

——威胁情况[WP-15-03]；

15.6.1.2 进一步的支持信息

可以考虑以下信息：

——网络安全事件中的弱点[WP-08-04]

——在产品开发过程中发现的弱点[WP-10-05]

——建筑设计

——以前确定的攻击路径[WP-15-05]，如果有的话

——脆弱性分析[WP-08-05]

15.6.2 要求和建议

[RQ-15-08] 应分析威胁情景，以确定攻击路径。

注 1 攻击路径分析可以基于以下几点：

——自上而下的方法，通过分析威胁情景的不同实现方式来推断攻击路径，例如攻击树、攻击图；

——自下而上的方法，从确定的漏洞中建立攻击路径。

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

[RQ-15-09] 一个攻击路径应与该攻击路径可实现的威胁情景相关。

注 3 在产品开发的早期阶段，攻击路径往往是不完整或不精确的，因为具体的实施细节还不知道，无法识别具体的漏洞。在产品开发过程中，随着更多信息的出现，例如在漏洞分析之后，攻击路径可以被更新。

例

——威胁情况：对制动 ECU 的 CAN 信息进行欺骗，导致 CAN 信息的完整性丧失，从而导致制动功能的完整性丧失。

——实现上述威胁情景的攻击路径。

(1) 远程信息处理 ECU 通过蜂窝接口被破坏。

(2) 网关 ECU 通过来自远程信息处理 ECU 的 CAN 通信受到影响。

(3) 网关 ECU 转发恶意的制动请求信号（不必要的快速减速）。

15.6.3 工作成果

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

15.7 攻击可行性等级

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 进一步的支持信息

可以考虑以下信息：

——建筑设计

——脆弱性分析[WP-08-05]

15.7.2 要求和建议

[RQ-15-10] 对于每个攻击路径，应按表 1 所述确定攻击可行性等级

攻击可行性等级	描述
高	攻击路径可以利用低的努力来完成。
中型	攻击路径可以利用中等程度的努力来完成。
低	攻击路径可以利用高度努力来完成。
非常低	攻击路径可以利用非常高的努力来完成。

[RC-15-11] 攻击可行性评级方法应根据以下方法之一来定义：

- a)基于攻击潜力的方法；
- b)基于 CVSS 的方法；
- c)基于攻击向量的方法；

注 1 方法的选择可能取决于生命周期中的阶段和可用的信息。

[RC-15-12] 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)专家的专业知识
- c)对该项目或组件的了解
- d)机会窗口

e)设备

注 2 核心攻击潜力因素可以从 ISO/IEC 18045 [23]中得出。

注 3 G.2 提供了关于根据攻击潜力确定攻击可行性的准则。

[RC-15-13] 如果使用基于 CVSS 的方法，应根据基础指标组的可利用性指标来确定攻击可行性等级，包括：

a)攻击矢量

b)攻击的复杂性

c)需要的特权

d)用户互动

注 4 G.3 提供了根据基于 CVSS 的方法确定攻击可行性的准则。

[RC-15-14] 如果使用基于攻击矢量的方法，应根据评估攻击路径的主要攻击矢量（参见 CVSS [24] 2.1.1）来确定攻击可行性等级。

注 5 G.4 提供了基于攻击矢量的方法确定攻击可行性的准则。

注 6 在开发的早期阶段（如概念阶段），当没有足够的信息来确定具体的攻击路径时，基于攻击矢量的方法可以适合估计攻击的可行性。

15.7.3 工作成果

[WP-15-06] 攻击的可行性评级，产生于[RQ-15-10]

15.8 风险值的确定

15.8.1 输入

15.8.1.1 先决条件

应提供以下信息：

——威胁情况[WP-15-03]；

——影响评级与相关的影响类别[WP-15-04]；

——攻击可行性评级[WP-15-06]。

15.8.1.2 进一步的支持信息

无

15.8.2 要求和建议

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

注 1 如果一个威胁情景对应一个以上的损害情景或一个相关的损害情景在一个以上的影响类别中具有影响，可以为每个影响等级单独确定一个风险值。

注 2 如果威胁情景与一个以上的攻击路径相对应，相关的攻击可行性评级可以适当汇总，例如威胁情景被赋予相应攻击路径的攻击可行性评级的最大值。

[RQ-15-16] 威胁情景的风险值应在 1 和 5 之间（包括 1 和 5），其中 1 的值代表最小风险。

例 确定风险值的方法：

——风险矩阵

——风险公式

15.8.3 工作成果

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

15.9 风险处理决定

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]

——威胁情况[WP-15-03]

——风险值[WP-15-07]

15.9.1.2 进一步的支持信息

可以考虑以下信息：

——网络安全规范[WP-10-01]

——该项目或部件，或类似项目或部件的先前风险处理决定

——含有相关影响类别的影响评级[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] 对于每种威胁情况，考虑到其风险值，应确定以下一种或多种风险处理方案：

a) 避开风险

例 1 通过消除风险源来避免风险，决定不开始或继续进行引起风险的活动。

b) 减少风险

c) 分担风险

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 保留风险和分担风险的理由被记录为网络安全索赔，并按照条 8 规定接受网络安全监测和脆弱性管理。

15.9.3 工作成果

[[WP-15-08]] 风险处理决定，产生于[RQ-15-17]

附件 A

(资料性)

网络安全活动和工作成果摘要

A.1 综述

表 A.1 提供了网络安全活动及其相应工作产品的摘要。这可以帮助组织管理这些活动，确保网络安全活动的覆盖面，并了解项目的潜在工作量。概念和产品开发阶段的活动是在网络安全计划中确定的。因此，这些活动的工作产品都在网络安全评估的范围内。从第条 15 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和工作成果

子条款	工作成果
组织网络安全管理	
5.4.1 网络安全治理	[WP-05-01] 网络安全政策、规则和程序
5.4.2 网络安全文化	[WP-05-01] 网络安全政策、规则和程序 [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、规则和程序
5.4.4 管理系统	[WP-05-03] 组织管理制度的证据
5.4.5 工具管理	[WP-05-04] 工具管理的证据
5.4.6 信息安全管理	[WP-05-03] 组织管理制度的证据
5.4.7 组织网络安全审计	[WP-05-05] 组织网络安全审计报告
依靠项目的网络安全管理	
6.4.1 网络安全责任	[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 裁剪	[WP-06-01] 网络安全计划
6.4.4 再利用	[WP-06-01] 网络安全计划
6.4.5 超出背景的组件	[WP-06-01] 网络安全计划
6.4.6 现有组件	[WP-06-01] 网络安全计划
6.4.7 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 后续开发的发布	[WP-06-04] 开发后报告的发布
分布式网络安全活动	
7.4.1 供应商能力	无
7.4.2 报价要求	无
7.4.3 责任的统一	[WP-07-01] 网络安全接口协议
持续的网络安全活动	
8.3 网络安全监测	[WP-08-01] 网络安全信息 的来源 [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] 来自网络安全事件的弱点
8.5 脆弱性 分析	[WP-08-05] 漏洞分析
8.6 脆弱性 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] 网络安全要求 [WP-09-05] 网络安全目标的核查报告

9.5 网络安全概念	[WP-09-06] 网络安全概念 [WP-09-07] 网络安全概念的核查报告
产品开发阶段	
10.4.1 设计	[WP-10-01] 网络安全规范 [WP-10-02] 开发后的网络安全要求 [WP-10-03] 建模、设计或编程语言和编码准则的文件化 [WP-10-04] 网络安全规范的核查报告 [WP-10-05] 产品开发过程中发现的弱点
10.4.2 集成和验证	[WP-10-05] 产品开发过程中发现的弱点 [WP-10-06] 集成和验证规范 [WP-10-07] 集成和验证报告
第 11 条 网络安全的验证	[WP-11-01] 审定报告
开发后阶段	
第 12 条 生产	[WP-12-01] 生产控制计划
13.3 网络安全事件应对	[WP-13-01] 网络安全事件应对计划
13.4 更新	无
14.3 结束网络安全支持	[WP-14-01] 交流网络安全支持结束的程序
14.4 停用	无
威胁分析和风险评估方法	
15.3 资产识别	[WP-15-01] 损害方案 [WP-15-02] 具有网络安全属性的资产
15.4 威胁情景识别	[WP-15-03] 威胁情况
15.5 冲击等级	[WP-15-04] 带有相关影响类别的影响评级
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 风险值的确定	[WP-15-07] 风险值
15.9 风险处理决定	[WP-15-08] 风险处理决定

轩辕实验室 XYLab

附件 B

(资料性)

网络安全文化的例子

表 B.1 提供了薄弱和强大的网络安全文化的例子。

表 B.1--薄弱和强大的网络安全文化的例子

表明网络安全文化薄弱的例子	表明强大的网络安全文化的例子
与网络安全有关的决定的责任是无法追溯的。	该程序确保与网络安全有关的决定的责任是可追溯的。
性能（所实施的功能或特性）、成本或时间表优先于网络安全。	网络安全和安全具有最高优先权。
奖励制度偏向于成本和进度，而不是网络安全。	奖励制度支持和激励有效实现网络安全，并惩罚那些走捷径、危害网络安全的人。
网络安全人员不考虑项目/活动的具体需要，就强行对网络安全进行不适当的、非常严格的遵守。	网络安全人员作为榜样，具有良好的适当性和实际执行力，导致整个组织对其行动的信任。
评估网络安全及其管理程序的人员受到负责执行程序的人员的不当影响。	该程序提供了充分的制衡，例如，网络安全评估中适当的独立程度。
对网络安全的被动态度，如： ——严重依赖开发结束时的测试。 ——没有为实地的潜在弱点或事件做好准备。 ——只有在生产中、现场发生网络安全事件时，或者媒体对竞争对手的产品给予大量关注时，管理层才会做出反应。	对网络安全采取积极主动的态度，如： ——在产品生命周期的最早阶段就发现并解决网络安全问题（设计中的网络安全）。 ——组织准备好对现场的漏洞或事件作出快速反应。

<p>——“群体思维”的确认偏见（即不加批判地接受或顺应流行的观点）。</p> <p>——在组建审查小组时，要“堆满甲板”（即选择成员以确保预期结果），以防止潜在的异议。</p> <p>——异议者被排斥或被贴上“不是团队成员”的标签（如不合作、不妥协、有毒的人）。</p> <p>——不同意见对绩效评估有负面的影响。</p> <p>——少数民族的异议者被贴上“麻烦制造者”、“非团队成员”或“告密者”（即煽动者、不受欢迎者或告密者）的标签或被视为“麻烦制造者”。</p> <p>——表达关切的员工害怕受到打击。</p>	<p>这个过程利用了多样性的优势</p> <p>——在所有过程中寻求、重视和整合知识多样性。</p> <p>——反对使用多样性的行为被阻止并受到惩罚。</p> <p>支持沟通和决策的渠道是存在的，而且管理层鼓励使用这些渠道。</p> <p>——鼓励自我披露。</p> <p>——我们鼓励任何人（内部或外部）负责地披露潜在的漏洞。</p> <p>——发现和解决的过程在现场、在制造和开发其他产品中继续进行。</p>
<p>没有系统的持续改进过程、学习周期或其他形式的经验总结。</p>	<p>持续改进是所有过程的组成部分。</p>
<p>流程是临时性的或隐性的。</p>	<p>遵循确定的、可追踪的和受控的流程。</p>
<p>没有为网络安全分配所需的资源。</p>	<p>为网络安全分配所需的资源。</p> <p>熟练的资源具有与分配的活动相称的能力。</p>

附件 C

(资料性)

网络安全接口协议模板的例子

C.1 综述

如果不同的组织参与了分布式网络安全活动，那么在不同的组织之间就责任、信息披露程度以及每个里程碑的实现程度达成一致是非常重要的。

本附件根据[RQ-07-04]提供了一个网络安全接口协议的示例模板。该模板对如何定义客户和供应商之间分布式网络安全活动的角色和责任提供了指导（图 C.1）。

其他信息也可以添加到模板中，如联络点、目标里程碑、合作的方法或工具。

C.2 示例模板

本例模板中的栏目条目是：

a)阶段：本文件的阶段。

b)工作产品：本文件中与分布式活动的接口有关的工作产品。

c)文件编号：本文件的相关条款。

d)供应商：RASIC 的供应商责任。

e)客户：由 RASIC 负责的客户。

注 1 本模板使用 RASIC 来展示组织间特定工作产品的责任分配。RASIC 可按以下方式使用：

—R（负责的）：负责开展该活动的组织

—A（负责的）：活动结束后，有权批准该活动的组织

—S（支持）：将帮助负责该活动的组织的组织

—我（知情）：被告知活动进展和正在作出的任何决定的组织

—C（咨询）：提供建议或指导的组织，但不积极从事该活动

f)保密程度：供应商和客户就每个工作成果的保密性达成一致；

注 2 可能的保密级别可以是：

- 高度机密：只有创造工作成果的组织才被允许访问它
- 保密：客户和供应商都被允许访问工作成果
- 与第三方保密：根据 5.4.3 的规定，该工作成果允许与授权的外部各方共享
- 公开：工作成果可以不受任何限制地分享

g) 评论：关于各组织之间谈判和讨论结果的补充信息。

Phase	Work product	Doc ref.	Supplier					Customer					Level of confidentiality	Comment
			R	A	S	I	C	R	A	S	I	C		
Concept	Item definition													
	Treat analysis and risk assessment													
	Cybersecurity concept													
	Verification report of cybersecurity concept													
Product develop- ment	Cybersecurity specification													

图 C.1 - 网络安全接口协议模板的例子

附件 D

(资料性)

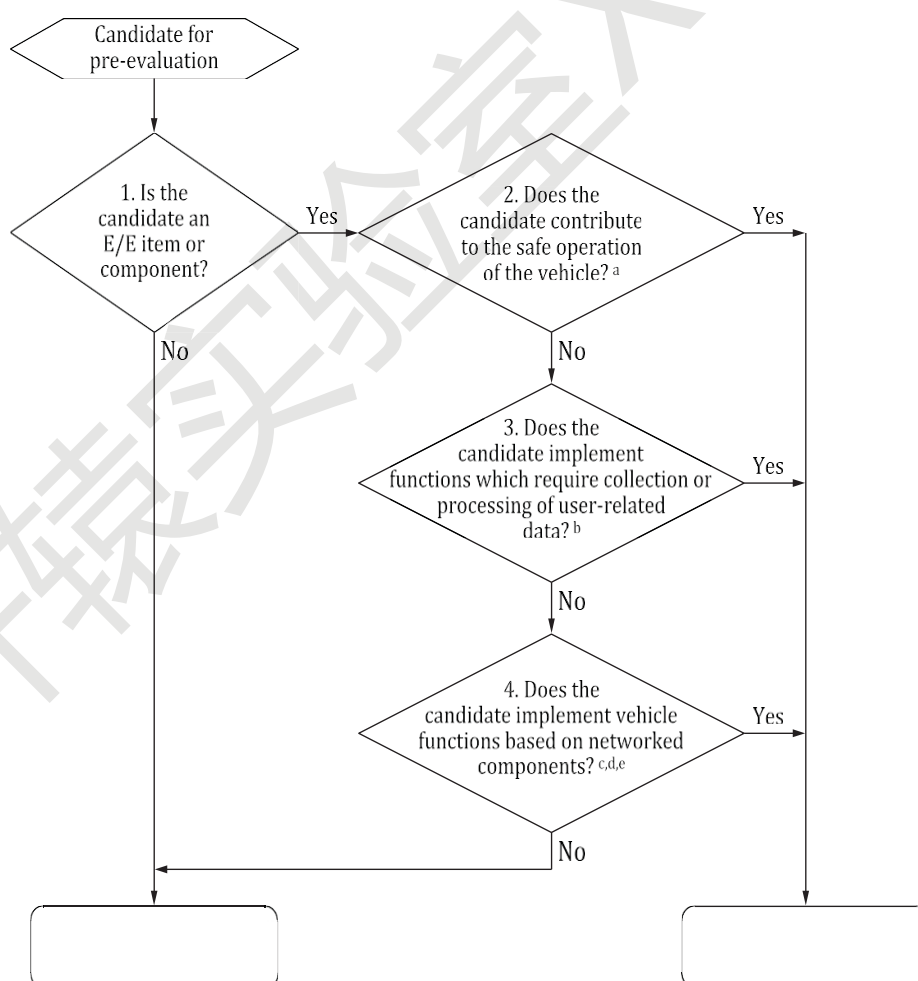
网络安全的相关性--方法和标准的例子

D.1 综述

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

D.2 方法

候选项目或组件的网络安全相关性可以通过图 D.1 中的决策图来确定，该图给出了示例标准。



- a 例子 运动控制模块和具有汽车安全完整性等级 (ASIL) 称号的模块。
- b 例子 与司机或乘客有关的数据，或与潜在的敏感信息（如位置数据）有关的数据。
- c 例子 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) 。
- d 例子 外部连接 - 与后端服务器的功能接口；蜂窝电信网络，车载诊断 (OBD-II) 接口。
- e 例子 无线连接的传感器或执行器--远程无钥匙进入 (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方法和标准

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

附件 E

(资料性)

网络安全保障水平

E.1 综述

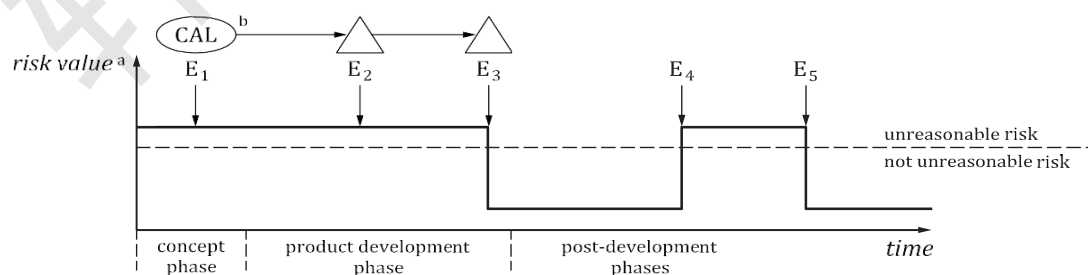
本附件描述了一个网络安全保证级别（CAL）的分类方案，可用于指定和交流一套保证要求，在严格程度上提供对某一项目或组件的资产保护得到充分发展的信心。这个 CAL 分类方案没有规定网络安全控制的技术要求，但是它可以用来推动网络安全工程，为相关组织之间交流网络安全保证要求提供一种共同语言。

CAL 可以由开发项目的组织确定，也可以由开发组件的组织断章取义。

一旦确定，CAL 规定了后续产品开发活动所需的严格程度，以解决需要降低风险的威胁情况。这可以通过将 CAL 作为网络安全目标的一个属性来实现，该目标由完善的网络安全要求继承。

E.2 确定一个 CAL

CAL 与风险间接相关；但是，它不能直接从风险值中确定。这是因为风险值是动态的，随着时间的推移而变化，取决于项目或组件不断变化的规格、设计、实施和操作环境，而 CAL 表达的是一种保证水平，将在一段时间内保持固定。因此，在考虑实施网络安全控制之前，可以在概念阶段的开发之初使用预计在网络安全支持结束之前保持稳定的参数来确定 CAL，例如基于项目资产及其相关风险的参数。图 E.1 说明了 CAL 和相



关风险之间的关系。



- E1 事件 1：网络安全要求被明确。
- E2 事件 2：网络安全控制得到实施。
- E3 事件 3：测试表明网络安全控制是有效的。
- E4 事件 4：在现场发现漏洞。
- E5 事件 5：漏洞被修复。
-  CAL 被确定和分配。
-  CAL 被应用于网络安全活动中。
- a 风险值是动态的，可以根据当前的规格、设计或实施而变化。
- b 鉴于需要保护的资产的关键性，在 E1 确定的预期保证水平规定了 E2、E3 的后续网络安全活动的严格程度。

图 E.1 - CAL 和风险之间的关系

可以根据对已确定的威胁情况的考虑来确定 CAL（见 15.4）。表 E.1 给出了一个基于四个 CAL 的例子，每个 CAL 都对应着基于所使用的网络安全工程方法的递增的保证水平。该例子显示了根据相关威胁情景的最大影响和攻击矢量分配的 CAL。

表 E.1--基于影响和攻击矢量参数的 CAL 确定示例

		Attack vector ^b			
		Physical	Local	Adjacent	Network
Impact	Severe	CAL2	CAL3	CAL4	CAL4
	Major	CAL1	CAL2	CAL3	CAL4
	Moderate	CAL1	CAL1	CAL2	CAL3
	Negligible	---a	---a	---a	---a
^a See [PM-06-08]. ^b Attack vector is a static parameter of attack feasibility.					

在客户和供应商之间分享确定 CAL 的书面理由可以增进相互理解。CAL 分类计划和确定的 CAL 也可以成为客户和供应商之间网络安全接口协议的一部分。

可以为一个项目的所有网络安全目标分配一个 CAL，也可以为每个网络安全目标分配不同的 CAL。如果网络安全目标被合并，单个 CAL 中的最高值将被分配给合并的网络安全目标

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的严格程度，即提供所需保证的必要努力。
可以用 CAL 来选择:

- a)用于开发和验证的方法。
- b)确定弱点和分析脆弱性的方法
- c)网络安全评估的方法。

表 E.2 提供了一些 CAL 的例子，以及它们在概念和产品开发阶段的使用指南。对于 CAL 的每一次增加，相应的方法代表了设计、验证和网络安全评估对项目或部件保证的有意义的增加。表 E.2、E.3 和 E.4 中的例子是为了使行业在使用 CAL 来扩展本文件中描述的活动中获得经验。

表 E.2--网络安全保障措施中 CAL 的示例数量和预期严格程度

CAL	描述	a) 提供信任的方法，以适当的严格程度开展网络安全活动。	b) 提供信心的方法，以确保未成年人的漏洞不存在。	c) 独立计划，以提供对所进行的网络安全活动适当的信心
CAL 1	需要低到中度的网络安全保障	基于需求的测试	分析和/或测试等活动，根据已知信息搜索漏洞	不需要
CAL 2	需要有适度的网络安全保障			网络安全评估是由不同于发起人的人进行的

CAL 3	需要中度至高度的网络安全保障	组件之间的所有相互作用都经过测试	分析和/或测试等活动，通过探索性的方法寻找漏洞	网络安全评估是由与发起人不同的团队中的人进行的
CAL 4	需要高度的网络安全保障	所有组件之间的相互作用组合都经过测试。		网络安全评估是由一个在管理、资源和发布权限方面独立于原部门的人进行的。

E.3.2 概念

本小节提供了一个例子，说明如何使用 CAL 分类方案来调整发展措施的严格程度和范围。

在概念阶段，随着网络安全概念的定义以及将网络安全要求分配给初步架构的组成部分，CAL 可以作为[RQ-09-10]的延伸，使用如下方式：

- a)来自网络安全目标的网络安全要求继承了该网络安全目标的 CAL。
- b)如果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被分配给一个架构组件，则将最高的 CAL 分配给该组。
- c)如果该组件被确认为受结构中其他组件的保护，则可以根据理由减少或不需要分配给该组件的 CAL。

E.3.3 产品开发

CAL 分类方案在产品开发中的应用可以是使用依赖于 CAL 的方法和措施。
在产品开发中，如果网络安全要求被分配到组件中，并且无法确认与其他组件的隔离，那么就可以按照这些网络安全要求的最高 CAL 来开发组件。

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例子；可以用类似的方式处理更多的网络安全活动。

表 E.3 提供了一个例子，说明如何利用 CAL 来确定执行各自活动的独立程度。

表 E.3--网络安全活动的独立程度示例

活动	要求	独立性水平适用				范围
		CAL	CAL	CAL	CAL4	
		1	2	3		
核实网络安全概念和设计活动	[RQ-09-11] [RQ-10-08]	I1	I1	I2	I2	适用于网络安全要求中最高 的 CAL
核实组件的实施和整合	[RQ-10-09]	1	I1	I2	I2	
网络安全验证	[RQ-11-01]	1	I1	I2	I2	
网络安全评估	[RQ-06-27]	—	I1	I2	I3	
<p>a 符号定义如下；</p> <p>-：对这项活动的独立性没有建议；</p> <p>I1：该活动是由一个不同的人进行的，与负责创造所考虑的工作产品的人相比；</p> <p>I2：该活动是由一个独立于负责创造所考虑的工作产品的团队的人执行的，即由一个向不同的直接上级报告的人执行；</p> <p>I3：该活动是由一个在管理、资源和发布权限方面独立于负责创建所考虑的工作产品的部门的人执行。</p>						

表 E.4 提供了一个例子，说明如何利用 CAL 来确定影响用于验证和确认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				范围
		CAL1	CAL2	CAL3	CAL4	
功能测试	[RC-10-12]	T1	T1	T2	T2	适用于网络安全要求中

	[RQ-11-01]					最高的 CAL
漏洞扫描	[RC-10-12]	T1	T1	T1	T1	
	[RQ-11-01]					
毛刺测试	[RC-10-12]	—	T1	T2	T2	
	[RQ-11-01]					
渗透测试	[RC-10-12]	—	—	T1	T2	
	[RQ-11-01]					

a 符号定义如下

对该活动的测试参数没有建议；

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。
- 随机选择输入的模糊测试。
- 渗透测试假定攻击者的专业知识、项目或组件的知识和/或资源适中；

T2：测试参数设置 2：

- 基于需求和组件之间的相互作用的功能测试。
- 对已知漏洞进行漏洞扫描。
- 通过增加测试案例的迭代次数和/或自适应选择输入来进行模糊测试。
- 渗透测试假定攻击者的专业知识、项目或组件的知识和/或资源更高。

附件 F

(资料性)

影响评级的准则

F.1 综述

本附件举例说明了影响评级的标准（见 15.5），涉及安全、财务、运营和隐私损害的损害情况。本附件中的表格（见表 F.1 至表 F.4）可用于影响评级。

关于损害的可扩展性(即在单一损害情况下对多个道路使用者的影响)如何修改影响评级的考虑没有包括在给出的例子中，但可以酌情添加到特定组织的评级标准中(例如参考文献[20]，C.1.2，表 4)。

F.2 安全损害的冲击等级

表 F.1--安全影响评级标准示例

影响评级	安全影响评级的标准
严重的	S3:威胁生命的伤害（生存不确定），致命的伤害
主要的	S2：严重的和有生命危险的伤害（可能生存）
中等水平	S1：轻度和中度伤害
忽略不计	S0：没有受伤 a
a S0 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。

如果提供理由，也可以考虑按照 ISO 26262-3:2018 的可控性和暴露度对安全的影响进行评级。

F.3 财务损失的影响评级

表 F.2 - 财务影响评级标准示例

影响评级	财务影响评级的标准
严重的	经济损失导致的灾难性后果，受影响的道路使用者可能无法克服。

主要的	经济上的损失导致了大量的后果，受影响的道路使用者将能够克服这些后果。
中等水平	经济损失导致不便的后果，受影响的道路使用者将能用有限的资源来克服。
可忽略不计	经济损失导致的影响不大，后果可忽略不计，或与道路使用者无关。

F.4 操作损害的影响等级

表 F.3 - 业务影响评级标准示例

影响评级	业务影响评级的标准
严重的	操作上的损坏导致了车辆核心功能的丧失或受损。 例子 1 车辆不工作或显示核心功能的意外行为，如启用跛行回家模式或自动驾驶到一个非预期的位置。
主要的	操作上的损坏导致了车辆重要功能的丧失或受损。 例子 2 司机的重大烦扰。
中等水平	操作上的损坏导致了车辆功能的部分退化。 例子 3 用户满意度受到负面影响。
可忽略不计	操作上的损坏导致车辆功能没有损害或无法感知的损害。

这些标准可能会或可能不会产生安全后果。

F.5 对隐私损害的影响等级

表 F.4--隐私影响评级标准示例

影响评级	隐私影响评级的标准
严重的	隐私损害导致对道路使用者产生重大甚至不可逆转的影响。 有关道路使用者的信息是高度敏感的，很容易与 PII 主体联系起来。
主要的	隐私的损害导致了对道路使用者的严重影响。有关道路使用者的信息是： a) 高度敏感且难以与 PII 主体联系起来； b) 敏感且容易与 PII 主体相联系。

中等水平	<p>隐私的损害导致了道路使用者的不便后果。有关道路使用者的信息是。</p> <p>a) 敏感但难以与 PII 主体联系起来；</p> <p>b) 不敏感，但很容易与 PII 主体联系起来。</p>
可忽略不计	<p>隐私损害导致没有影响或，后果可忽略不计或与道路使用者无关。</p> <p>有关道路使用者的信息并不敏感，很难与 PII 主体联系起来。</p>

个人可识别信息（PII）和 PII 委托人可以根据 ISO/IEC 29100[25]来定义。

附件 G

(资料性)

攻击可行性评级的准则

G.1 综述

本附件提供了关于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 的

—基于攻击矢量

考虑一个攻击是否有可能扩展（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 基于攻击潜力的方法的准则

G.2.1 攻击潜力的背景

攻击潜力在 ISO/IEC 18045[23]中被定义为衡量攻击一个项目或组件所要花费的努力，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

—专家的专业知识

—对该项目或组件的了解

—机会窗口

—设备

本子条款给出了定制化的例子和攻击可行性的例子映射。

G.2.2 参数调整的例子

G.2.2.1 例行定制的耗时

经过的时间参数包括识别漏洞以及开发和（成功）应用漏洞的时间。因此，这个评级是基于评级时的专家知识状况，见表 G.1。

表 G.1 - 经过的时间

≤1 天
≤1 周
≤1 个月
≤6 个月
超过 6 个月

G.2.2.2 专业知识的实例定制

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，见表 G.2。

表 G.2-专家

<p>门外汉</p> <p>与专家或精通的人相比，不了解情况，没有特别的专长。</p> <p>例子 1 普通人使用公开的攻击步骤描述。</p>
<p>精通</p> <p>知识渊博，即他们熟悉产品或系统类型的安全行为。</p> <p>例 2 有经验的车主，普通技术人员知道简单和流行的攻击，如里程表的调整，安装假冒的零件。</p>
<p>专家</p> <p>熟悉底层算法、协议、硬件、结构、安全行为、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、产品或系统类型中实施的攻击方法等。</p> <p>例 3 有经验的技术员或工程师。</p>
<p>多位专家</p> <p>攻击的不同步骤需要专家级别的不同领域的专业知识。</p> <p>例子 4 多个经验丰富的工程师，他们在不同的领域都有专长，而且在攻击的不同步骤中都需要专家级别。</p>

G.2.2.3 项目或组件的知识实例定制

对物品或组件参数的了解与攻击者获得的有关该物品或组件的信息量有关，见表

G.3。

表 G.3 - 对项目或部件的了解程度

<p>公共信息</p> <p>有关该项目或组件的公共信息（如从互联网上获得的信息）。</p> <p>例子 1 在产品主页或互联网论坛上发布的信息和文件。</p>
<p>限制性信息</p> <p>有关项目或组件的限制性信息（例如，在开发者组织内部控制的知识，并根据保密协议与其他组织共享）。</p> <p>例 2 制造商和供应商之间共享的内部文件，要求和设计规范。</p>
<p>机密信息</p> <p>关于项目或组件的机密信息（例如，在开发者组织内的不同团队之间共享的知识，只限定团队的成员才能访问这些信息）。</p> <p>例子 3 与防盗器有关的信息，软件源代码。</p>
<p>严格的保密信息</p> <p>关于项目或部件的严格保密信息（例如，只有少数人知道的知识，在严格的需要知基础上，对其访问进行非常严格的控制，并由个人承担）。</p> <p>例子 4 由制造商和/或供应商内部记录的客户特定的校准或记忆图。</p>

G.2.2.4 机会窗口的定制实例

机会窗口参数与成功实施攻击的访问条件（时间、类型）有关。它结合了访问类型（如逻辑和物理）和访问时间（如无限和有限）。根据攻击的类型，这可能包括发现可能的目标，进入目标，利用目标的工作，对目标进行攻击的时间，保持不被发现，规避检测和网络安全控制，等等。(见表 G.4)。

表 G.4-机会窗口

<p>无限的</p> <p>通过公共/不信任的网络，没有任何时间限制的高可用性（即资产总是可以访问）。没有实际存在或时间限制的远程访问，以及对物品或组件的无限制实际访问。</p> <p>例子 1 远程攻击（如车辆到任何东西或手机接口），没有任何先决条件，车主无限制的物理访问，进行芯片调整。</p>
<p>容易</p> <p>高可用性和有限的访问时间。远程访问，无需亲自到项目或组件处。</p> <p>例子 2 蓝牙的配对时间，远程软件更新，需要车辆静止的远程攻击。</p>
<p>适度的</p> <p>项目或组件的低可用性。有限的物理和/或逻辑访问。在不使用任何特殊工具的情况下对车辆内部或外部进行物理访问。</p> <p>例子 3 攻击者进入一辆未上锁的汽车，并获得了暴露的物理接口，例如通过车载诊断端口的物理访问。</p>
<p>困难的</p> <p>该物品或组件的可用性非常低。对该项目或组件的访问程度不实际，无法实施攻击。</p> <p>例 4 解除集成电路的盖子以提取信息，用蛮力破解密码钥匙，其速度比钥匙旋转的速度快。</p>

G.2.2.5 设备定制的例子

设备参数与攻击者可用来发现漏洞和/或执行攻击的工具有关，见表 G.5。

表 G.5-设备

<p>标准</p> <p>设备对攻击者来说是现成的。这种设备可以是产品本身的一部分（如操作系统中的调试器），或者可以很容易地得到（如互联网资源、协议分析器或简单的攻击脚本）。</p> <p>例 1 笔记本电脑、CAN 适配器、板载诊断加密狗、普通工具（螺丝刀、电烙铁、钳子）。</p>

<p>专攻</p> <p>攻击者不容易得到设备，但可以不费吹灰之力获得。这可以包括购买适量的设备（例如电力分析工具，使用数百台连接在互联网上的个人电脑就属于这个类别），或开发更广泛的攻击脚本或程序。如果一个攻击的不同步骤需要由专门设备组成的明显不同的测试台，这将被评为定制的。</p> <p>例 2 专门的硬件调试设备，车载通信设备（硬件在环测试台，高档示波器，信号发生器），特殊化学品。</p>
<p>定制</p> <p>设备是专门生产的（如非常复杂的软件），不容易向公众提供（如黑市），或者设备非常专业，其分配受到控制，甚至有可能受到限制。或者，该设备非常昂贵。</p> <p>例子 3 制造商限制的工具，电子显微镜。</p>
<p>多次定制</p> <p>引入这个概念是为了考虑到在攻击的不同步骤中需要不同类型的定制设备的情况。</p>

G.2.2.6 攻击潜力和攻击可行性之间的映射实例

对于每个参数，可以定义数值。基于 ISO/IEC 18045[23]，在上面提出的适应性基础上，提出了以下尺度，见表 G.6。

表 G.6-攻击潜力的汇总示例

经过的时间		专业经验		对该项目或组件的了解		机会窗口		装备	
列举	价值	列举	价值	列举	价值	列举	价值	列举	价值
≤1 天	0	外行	0	公众	0	无限制	0	标准	0
≤1 周	1	精通	3	受限制的	3	顺利	1	专业的	4
≤1 个月	4	专家	6	保密性	7	中等水平	4	订制	7
≤6 个月	17	多个前雇员	8	严格保密	11	有困难/没有	10	多次发言	9

超过 6 个月	19
---------	----

根据 ISO/IEC 18045[23]，攻击潜力对应于所有参数的增加。根据 ISO/IEC 18045 [23]的定制，使用表 G.7 对攻击可行性进行映射。

表 G.7-攻击潜力映射示例

攻击可行性等级	价值观
高	0 - 9
	10 - 13
中型	14 - 19
低	20 - 24
非常低	≥ 25

G.3 基于 CVSS 方法的准则

为了评定信息技术安全漏洞，可以使用由事件响应和安全团队论坛（FIRST）[24] 维护的 CVSS。在基本指标组中，可利用性指标（参见参考文献[24]，7.1）可以用来评定攻击的可行性。其他 CVSS 指标（如影响指标）由本文的某些方面所涵盖，如破坏情景和影响评估。

可利用性指标是：

- 攻击矢量
- 攻击的复杂性
- 需要的特权
- 用户互动

它们由 FIRST[24]描述。对 CVSS 指标的评估，根据预先定义的范围，为每个指标产生数字值。总的可利用性值可以根据一个简单的公式来计算。

$$e = 8,22 \times v \times c \times p \times u$$
 其中：

- E* 是可利用性值。
- V* 是与攻击矢量相关的数值，范围从 0.2 到 0.85。
- C* 是与攻击复杂性相关的数值，范围从 0.44 到 0.77。
- P* 是与所需特权相关的数值，范围从 0.27 到 0.85；
- U* 是与用户互动相关的数值，范围从 0.62 到 0.85。

因此，可利用性数值在 0.12 和 3.89 之间。

表 G.8 给出了 CVSS 可利用性值与攻击可行性的映射实例。这是一个等距可利用性步骤的例子。

表 G.8 - 例 C VSS 可利用性映射

攻击可行性等级	CVSS 可利用性值
高	2,96 - 3,89
中型	2,00 - 2,95
低	1,06 - 1,99
非常低	0,12 - 1,05

注 只使用可利用性指标作为更大的 CVSS 基本指标组的一部分的程序并不严格符合 CVSS 对指标的要求。为了按照本文的要求计算风险，缺失的影响度量可以用本文的影响度量进行补偿，见附件 F 和参考文献[24]。

在不改变可利用性度量值的情况下，可以对其描述进行补充，以便对组织的业务和正在开发的项目或组件提供更好的指导，并在将描述应用于实际漏洞时减少误解的可能性。这种补充可以是组织特定的例子，添加到度量值的描述中。

除了漏洞，CVSS 的可利用性指标也可以用来评价概念性的弱点、缺陷和差距。

G.4 基于攻击矢量的方法的准则

基于攻击矢量的方法反映了攻击路径可能被利用的背景。攻击者为了利用攻击路径，可以在越远的地方（逻辑上和物理上）进行攻击，攻击可行性等级就越高。假设可以利

用互联网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 G.9。

表 G.9-基于攻击向量的方法

攻击可行性等级	标准
高	网络 潜在的攻击路径是与网络堆栈绑定的，没有任何限制。 例子 1 蜂窝网络连接，使 ECU 直接连接并在互联网上访问。
中型	毗邻 潜在的攻击路径与网络堆栈绑定；但是，连接在物理上或逻辑上受到限制。 例子 2 蓝牙接口，虚拟专用网络连接。
低	当地 潜在的攻击路径不受网络堆栈的约束，威胁代理需要直接访问该项目以实现攻击路径。 实例 3 通用串行总线大容量存储设备，存储卡。
非常低	躯干 威胁代理需要物理访问以实现攻击路径。

附件 H

(资料性)

TARA 方法的应用实例--大灯系统

H.1 综述

本附件中的大灯系统开发实例和各自的工作成果仅用于说明，并不意味着实际使用的任何特定方法。

本附件通过介绍威胁分析和风险评估 (TARA) 方法的应用实例，可以帮助理解本文件的要求。这个例子只介绍了说明 TARA 应用的概念阶段，并以抽象的、简化的方式呈现。特别是，它涉及到：

—项目定义

—TARA

TARA 被定义为模块化的分析方法，每个模块可以按照任何顺序进行，例如：

—识别资产→识别相应的损害情况→影响评级→识别威胁情况→攻击路径分析
→.....

—从目录中选择损害情景→影响评级→威胁情景识别→资产识别→ ...

本附件中的例子遵循以下顺序：

(1)资产识别

(2)冲击等级

(3)威胁情景识别

(4)攻击路径分析

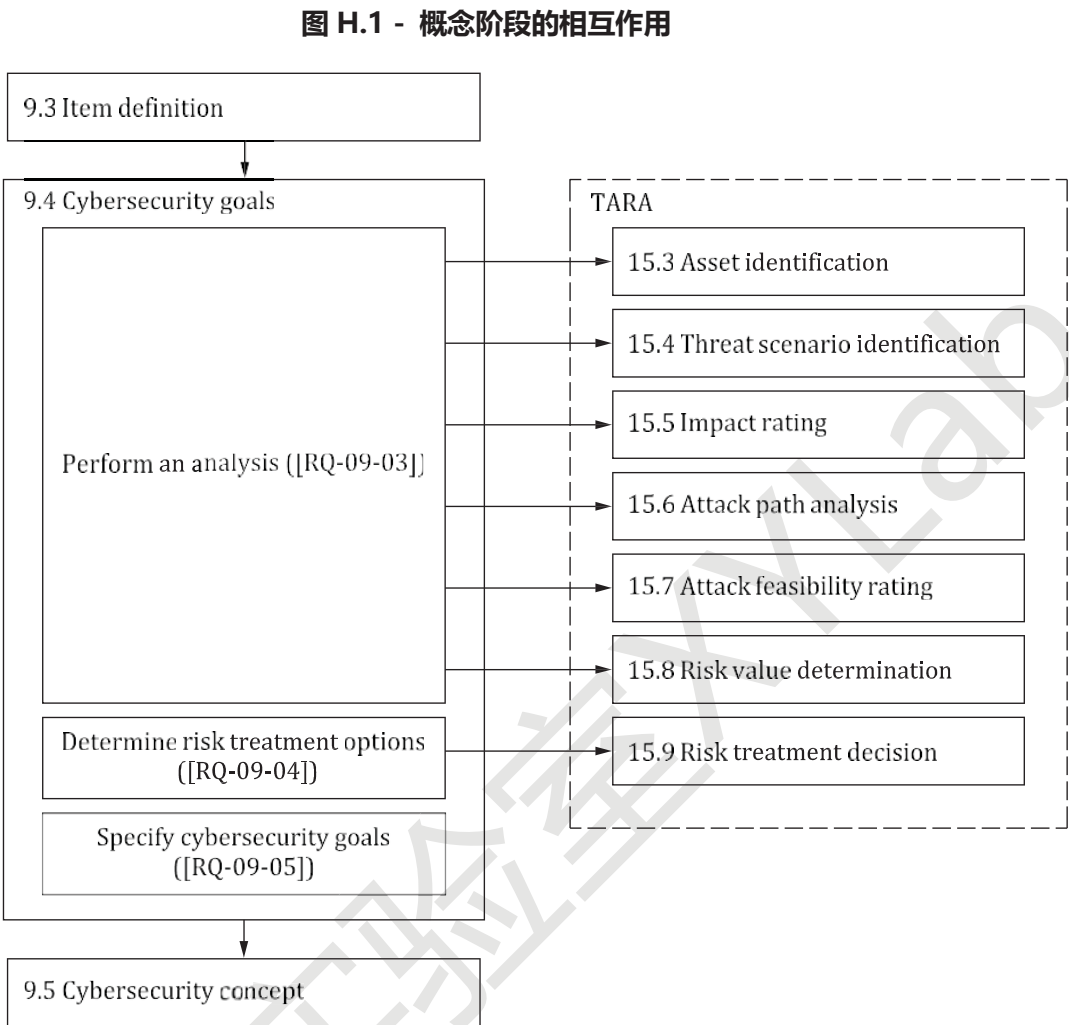
(5)攻击的可行性评级

(6)风险值的确定

(7)风险治疗决定

在第五步，采用两种不同的方法对攻击可行性进行评级。一种方法使用基于攻击矢量的方法（见[RC-15-14]），另一种方法使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。



H.2 大灯系统概念阶段的活动实例

H.2.1 项目定义

本子条款显示了 9.3 的部分工作产品的例子。下面给出了大灯系统的一个项目定义的例子

- a)项目边界 (见图 H.2)
- b)项目功能

- 该项目的功能概述：大灯系统根据驾驶员的需求，按照开关打开/关闭大灯。如果大灯处于高光模式，当检测到迎面而来的车辆时，大灯系统自动将大灯切换到低光模式。如果不再检测到迎面而来的车辆，它也会将大灯自动恢复到高光模式。

注 关于大灯的功能，大灯系统不依赖于导航 ECU 和网关 ECU。

c)初步架构 (见图 H.2)

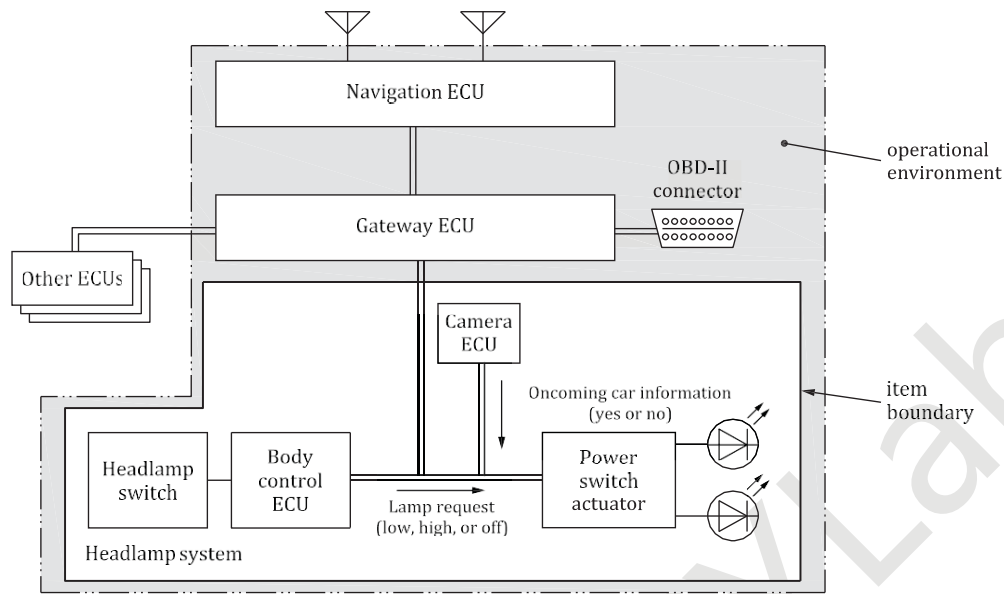


图 H.2 - 大灯系统的项目边界和初步结构实例

在项目定义过程中，对项目的运行环境进行了描述（见[RQ-09-02]）。操作环境为 TARA 的分析活动提供补充信息。表 H.1 显示了本附件中使用的操作环境的描述示例。

表 H.1 - 业务环境的充分描述

该项目（大灯系统）与网关 ECU 相连，而网关 ECU 通过数据通信与导航 ECU 相连	
导航 ECU 有外部通信接口	
— 蓝牙	
— 单元格	
假设	
— 导航 ECU 有一个防火墙，防止来自外部接口的无效数据通信。	
网关 ECU 有外部通信接口	
— OBD-II	
假设	
— 网关 ECU 具有强大的安全控制，包括防火墙功能（作为 CAL4 开发）	

H.2.2 资产识别

[RQ-09-03]根据 15.3 调用资产识别,以识别该物品的资产及其损坏情况。表 H.2 显

示了资产识别的示例结果。

表 H.2--资产和损害情况的实例列表

资产	网络安全财产			损失情况
	C	I	A	
数据通信（灯的要求	-	X	X	车辆不能在夜间行驶，因为（驾驶员认为）大灯功能在停放时被抑制了。
	-	X	-	在夜间以中速行驶时，由于非故意关闭大灯，导致前面与狭窄的静止物体（如树）相撞。
数据通信（来往车辆信息）	-	X	-	迎面而来的车辆的司机被蒙蔽了，这是由于在夜间驾驶时不能改用近光灯造成的。
	-	-	X	夜间驾驶时，大灯总是停留在近光灯下，导致自动远光灯功能失常。
车身控制 ECU 的固件	X	X	-	...

H.2.3 影响评级

[RQ-09-03]还按照 15.5 要求进行影响评级，以评定损坏情况的影响。表 H.3 显示了影响评级的例子结果。

表 H.3 - 损坏情况下的影响评级示例

损失情况	影响类别	影响评级
车辆不能在夜间行驶，因为（驾驶员认为）大灯功能在停放时被抑制。	O	主要的
在夜间以中速行驶时，由于非故意关闭大灯，导致前面与狭窄的静止物体（如树）相撞。	S	严重 (S3)

夜间驾驶时，大灯总是停留在近光灯下，导致自动远光灯功能失常。	O	中等水平
--------------------------------	---	------

H.2.4 威胁情景识别

[RQ-09-03]还根据 15.4 要求进行威胁情景识别。表 H.4 显示了威胁情景识别的示例结果。

表 H.4--威胁情况示例

损失情况	威胁情况
夜间以中速行驶时，因大灯意外关闭而导致正面与一排静止的物体（如树）相撞。	欺骗信号会导致 "灯请求 "信号与电源开关执行器 ECU 的数据通信失去完整性，有可能导致大灯意外关闭。
	篡改车身控制 ECU 发出的信号会导致 "车灯请求 "信号与电源开关执行器 ECU 的数据通信失去完整性，可能导致大灯意外关闭。
夜间行车时头灯始终保持在近光灯下，导致自动远光灯失灵	资产：来往车辆信息 网络安全财产：可用性 相关原因：对来车信息的拒绝服务

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进行攻击路径分析的示例。

对攻击路径的分析可以考虑到假设。在这个例子中，需要对物品内部进行物理访问的攻击路径，如车身控制 ECU 的微控制器，可以根据假设排除。

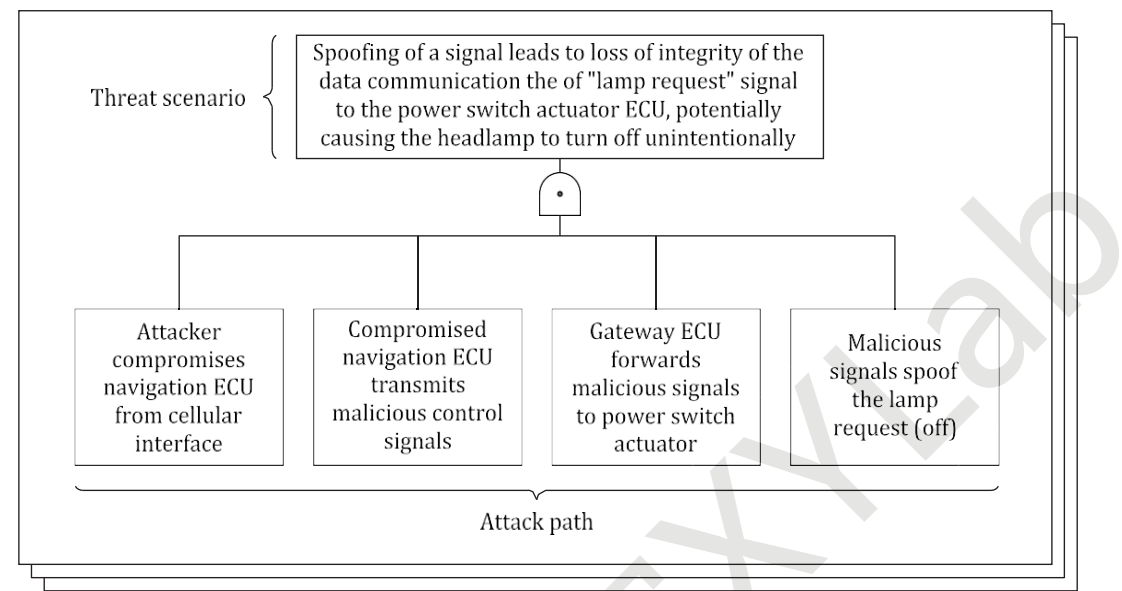
表 H.5 - 威胁情况下的攻击路径示例

威胁情况	攻击路径	
欺骗信号导致"灯请求 "信号与电源开关执	(1)	攻击者从手机接口入侵导航 ECU
	(2)	被入侵的导航 ECU 传输恶意的控制信号
	(3)	网关 ECU 将恶意信号转发给电源开关执行器

行器 ECU 的数 据通信失去完 整性,可能导致 大灯无意中关 闭。	(4)	恶意信号欺骗灯的请求 (关闭)
	(1)	
	(2)	
	(3)	攻击者从蓝牙接口破坏了导航 ECU
	(4)	被破坏的导航 ECU 传输恶意的控制信号
	(1)	网关 ECU 将恶意信号转发给电源开关执行器
	(2)	恶意信号欺骗灯的请求 (关闭)
	(3)	攻击者获得对 OBD 连接器的本地 (见表 G.9) 访问
	(4)	攻击者从 OBD 连接器发送恶意的控制信号
		网关 ECU 将恶意信号转发给电源开关执行器
拒绝提供来往 车辆信息的服 务	(1)	攻击者从手机接口入侵了导航 ECU
	(2)	被破坏的导航 ECU 传输恶意的控制信号
	(3)	网关 ECU 将恶意信号转发给电源开关执行器
	(4)	攻击者用大量的信息充斥着通信总线
	(1)	攻击者在车辆停车解锁时, 将一个支持蓝牙的 OBD 加密狗 连接到 OBD 连接器
	(2)	攻击者用蓝牙接口破坏了司机的智能手机
	(3)	攻击者通过智能手机和蓝牙加密狗向网关 ECU 发送信息
	(4)	网关 ECU 将恶意信号转发给电源开关执行器
	(5)	攻击者用大量的信息充斥着通信总线

H.2.6 攻击可行性等级

[RQ-09-03]还根据 15.7 要求对每个攻击路径进行攻击可行性评级。表 H.6 显示了按照 G.4 中描述的基于攻击矢量的方法进行攻击可行性评级的示例结果。表 H.7 显示了



按照 G.2 中描述的基于攻击潜力的方法进行攻击可行性评级的示例结果。

图 H.3 - 通过攻击树分析得出的攻击路径实例

表 H.6--基于攻击矢量方法的攻击可行性评级实例

攻击路径	攻击可行性等级
(1) 攻击者 从手机接口 入侵了导航 ECU (2) 被破坏的导航 ECU 传输恶意的控制信号 (3) 网关 ECU 将恶意信号转发给电源开关执行器 (4) 恶意信号欺骗了灯的请求 (ON)	高
(1) 攻击者 从蓝牙接口 破坏了导航 ECU (2) 被破坏的导航 ECU 传输恶意的控制信号 (3) 网关 ECU 将恶意信号转发给电源开关执行器 (4) 恶意信号欺骗了灯的请求 (ON)	中型
(1) 攻击者 从 OBD2 连接器 发送恶意的控制信号 (2) 网关 ECU 将恶意的信号转发给电源开关执行器	低

(3) 恶意信号欺骗了灯的请求 (ON)	
----------------------	--

注 1 基于攻击矢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有关的信息。

根据建议（见[RC-15-11]），也可以根据基于攻击潜力的方法确定攻击可行性，表 H.7 中的例子说明了这一点。

H.7--基于攻击潜力的方法的攻击可行性评级实例

威胁情况	攻击路径	攻击可行性评估						
		ET	SE	KoIC	WoO	Eq	价值	攻击可行性等级
拒绝为来往车辆提供信息服务	(1) 攻击者从手机接口入侵了导航 ECU (2) 被破坏的导航 ECU 传输恶意的控制信号 (3) 网关 ECU 将恶意信号转发给电源开关执行器 (4) 攻击者用大量的信息充斥着通信总线	1	8	7	0	4	20	低

	<p>(1) 攻击者在车辆停车解锁时，将支持蓝牙的 OBD 加密狗接入 OBD 连接器</p> <p>(2) 攻击者用蓝牙接口破坏了司机的智能手机</p> <p>(3) 攻击者通过智能手机和蓝牙加密狗向网关 ECU 发送信息</p> <p>(4) 网关 ECU 将恶意信号转发给电源开关执行器。</p> <p>(5) 攻击者用大量的信息充斥着通信总线。</p>	1	8	7	4	4	24	低
<p>关键</p> <p>ET 经过的时间</p> <p>SE 专家的专业知识</p> <p>KoIC 对该项目或组件的了解</p> <p>WoO 机会窗口</p> <p>Eq 设备</p>								

注 2 每个组织都可以根据自己的政策对每个评级采用合理的理由。例如，第二条攻击路径的机会之窗被定为 4 (适度, 参考表 G.4)，因为需要物理访问。考虑到基于表 G.7 的所有可行性值，确定攻击的可行性等级。

H.2.7 风险值的确定

[RQ-09-03]还要求根据 15.8 对每个威胁情景进行风险确定。可以利用组织定义的风险矩阵来确定风险值，将影响（见 15.5）和攻击可行性（见 15.7）的评级组合映射到风险值。表 H.8 显示了一个风险矩阵的例子，表 H.9 显示了使用表 H.8 确定风险的例子结果。

表 H.8--风险矩阵分析

		攻击可行性等级			
		非常低	低	中型	高
影响评级	严重的	2	3	4	5
	主要的	1	2	3	4
	中等水平	1	2	2	3
	可忽略不计	1	1	1	1

表 H.9 - 确定的风险值的例子

威胁情况	汇总攻击可行性等级	影响评级	风险值
欺骗信号导致电源开关执行器 ECU 的 "灯请求" 信号的数据通信的完整性丧失。	高	严重的	S: 5
拒绝提供来往车辆信息的服务	低	中等水平	O: 2

风险值也可以由组织定义的风险公式来确定。下面的公式和表 H.10 中显示了一个例子， $R = I + F$

表 H.10--将影响和攻击可行性转化为数值的例子

影响评级	数值 I 以求影响	攻击可行性等级	攻击可行性的数值 F
可忽略不计	0	非常低	0
中等水平	1	低	1
主要的	1,5	中型	1,5
严重的	2	高	2

对于表 H.9 中显示的具体威胁情况, 使用表 H.8 中的例子和上述公式的计算将导致相同的风险值。

H.2.8 风险处理决定

[RQ-09-04]要求按照 15.9 的规定选择处理方案。表 H.11 显示了风险处理决策的示例结果。

表 H.11 - 风险处理决定的检验结果

威胁情况	风险值	风险处理方案
欺骗信号导致电源开关执行器 ECU 的 "灯请求" 信号的数据通信失去完整性	S: 5	减少风险
拒绝提供来往车辆信息的服务	O: 2	减少风险

参考文献

- [1]ISO 26262-1:2018, Road vehicles — Functional safety — Part 1: Vocabulary
- [2]ISO 9000:2015, Quality management systems — Fundamentals and vocabulary
- [3]ISO 31000:2018, Risk management — Guidelines
- [4]ISO/IEC/IEEE 15288:2015, Systems and software engineering — System life cycle processes
- [5]ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary
- [6]ISO/TR 4804, Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation
- [7]IATF 16949, Quality management system requirements for automotive production and relevant service parts organizations
- [8]ISO 9001, Quality management systems — Requirements
- [9]ISO 10007, Quality management — Guidelines for configuration management
- [10]ISO/IEC 33001, Information technology — Process assessment — Concepts and terminology
- [11]ISO/IEC/IEEE 15288, Systems and software engineering — System life cycle processes
- [12]ISO/IEC/IEEE 12207, Systems and software engineering — Software life cycle processes
- [13]VDA QMC WORKING GROUP 13 / AUTOMOTIVE SIG. Automotive SPICE Process Assessment / Reference Model, Version 3.1 [online]. Berlin: VDA QMC,

November

2017.Available

at:http://www.automotivespice.com/fileadmin/software-download/AutomotiveSPICE_PAM_31.pdf

[14]ISO 29147, Information technology — Security techniques — Vulnerability disclosure

[15]IEC 62443-2-1, Industrial communication networks — Network and system security — Part 2-1:

Establishing an industrial automation and control system security program

[16]ISO 26262 (all parts), Road vehicles — Functional safety

[17]MISRA C 2012, Guidelines for the use of the C language in critical systems, 3rd Edition, 1st Revision.

Nuneaton, England: HORIBA MIRA, February 2019. ISBN (print/electronic): 978-1-906400-21-7/ 978-1-906400-22-4.

[18]SEI CERT C Coding Standard – Rules for developing safe, reliable and secure systems [online]. Pittsburgh, Pennsylvania: Software Engineering Institute, Carnegie Mellon University, 2016 [viewed 2021-02-12]. Available at: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=454220>

[19]ROSS Ron, et al. (2018), Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [online]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1. Updated March 2018 [viewed 2021-02-16]. Available at: <https://doi.org/10.6028/NIST.SP.800-160v1>

[20]E-SAFETY VEHICLE INTRUSION PROTECTED APPLICATIONS (EVITA) Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios [online]. Edited by A. Ruddle et al. December 2009 [viewed 2021-01-17]. Available at: <https://doi.org/10.5281/zenodo.1188418>

[21]ETSI TS 102 165-1, CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA), Version 5.2.3 [online]. October 2017[viewed 2021-01-19].Available at: https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf

[22]UcedaVélez, Tony and Morana, Marco M. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. Hoboken, New Jersey: Wiley, May 2015. ISBN: 978-1-118-98835- 0.

[23]ISO/IEC 18045, Information technology — Security techniques — Methodology for IT security evaluation

[24]FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST). Common Vulnerability Scoring System (CVSS), Common Vulnerability Scoring System v3.1: Specification Document, [online]. Available at: <https://www.first.org/cvss/v3.1/specification-document>

[25]ISO/IEC 29100, Information technology — Security techniques — Privacy framework

[26]Automotive ISAC, Automotive Cybersecurity Best Practices [online]. Available at: <https://www.automotiveisac.com/best-practices/>

[27]FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST). Traffic Light Protocol (TLP),FIRST Standards Definitions and Usage Guidance - Version 1.0, [online]. Available at: <https://www.first.org/tlp/>

[28]ISO/IEC 23822), Information technology — Vocabulary

[29]ISO/IEC 15408 (all parts), Information technology — Security techniques — Evaluation criteria for IT security

[30]ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[31]ISO/IEC 27010, Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

[32]ISO/IEC/IEEE 26511, Systems and software engineering — Requirements for managers of information for users of systems, software, and services

[33]IEC 31010, Risk management — Risk assessment techniques

[34]IEC 61508-7, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures

[35]JOHNSON Christopher, et al. (2016) Guide to Cyber Threat Information Sharing [online]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-150, October 2016 [viewed 2021-02-16]. Available at: <https://doi.org/10.6028/NIST.SP.800-150>

[36]JOINT TASK FORCE TRANSFORMATION INITIATIVE 2012), Guide for Conducting Risk Assessments [online]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. September 2012 [viewed 2021-02-16]. Available at: <http://dx.doi.org/10.6028/NIST.SP.800-30r1>

[37]SAE J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

[38]SCARFONE Karen, et al. (2008), Technical Guide to Information Security Testing and Assessment [online]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. September 2008 [viewed 2021-02-16]. Available at: <https://doi.org/10.6028/NIST.SP.800-115>

[39]TAKANEN Ari et al. Fuzzing for Software Security and Quality Assurance,

ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering (2021)

中文译文版权归轩辕实验室 XYLab 所有，仅供业内学习参阅



Second Edition. Boston, Massachusetts/London: Artech House, January 2018.

ISBN: 978-1-60807-850-9.

轩辕实验室 XYLab