ICS 43.040
CCS T 40

中华人民共和国国家标准

GB/T 46194—2025/ISO/SAE 21434:2021

道路车辆　信息安全工程

Road vehicles—Cybersecurity engineering

（ISO/SAE 21434:2021,IDT）

2025-10-05 发布　　2025-10-05 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件等同采用ISO/SAE 21434:2021《道路车辆　信息安全工程》。

本文件做了下列最小限度的编辑性改动:

——增加了关于汽车网关的威胁分析和风险评估(TARA)示例(见附录H),以帮助标准使用者更好地理解威胁分析和风险评估(TARA)方法。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会(SAC/TC 114)归口。

本文件起草单位:中国汽车技术研究中心有限公司、泛亚汽车技术中心有限公司、广州汽车集团股份有限公司、上海华为技术有限公司、北京航空航天大学、上海机动车检测认证技术研究中心有限公司、三六零数字安全科技集团有限公司、国汽(北京)智能网联汽车研究院有限公司、电子科技大学、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、梅赛德斯-奔驰(中国)投资有限公司、北京百度网讯科技有限公司、东软集团股份有限公司、沃尔沃汽车(亚太)投资控股有限公司、东风汽车集团股份有限公司、长城汽车股份有限公司、一汽-大众汽车有限公司、法雷奥汽车内部控制(深圳)有限公司。

本文件主要起草人:孙航、张亚楠、冯海涛、罗浩、李宝田、潘凯、杨世春、许瑞琛、严敏睿、郑继虎、罗蕾、王海均、朱科屹、吕明、刘健皓、陈静相、张云霞、龚诗祺、李晓阳、王博、朱燚。

道路车辆　信息安全工程

1　范围

本文件规定了道路车辆中电子电气(E/E)系统(包括其组件和接口)在概念、产品开发、生产、运营、维护和报废阶段的信息安全风险管理的工程要求。

本文件定义了一个包括信息安全过程要求以及沟通和管理信息安全风险的通用语言框架。

本文件适用于开发或改进量产道路车辆 E/E 系统,包括其组件和接口。

本文件未规定与信息安全有关的具体技术或解决方案。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 34590.3—2022　道路车辆　功能安全　第3部分:概念阶段(ISO 26262-3:2018,MOD)

注:GB/T 34590.3—2022 被引用的内容与 ISO 26262-3:2018 被引用的内容没有技术上的差异。

3　术语和定义、缩略语

3.1　术语和定义

下列术语和定义适用于本文件。

3.1.1

架构设计　architectural design

可识别组件(3.1.7)及其边界、接口和交互的表示方法。

3.1.2

资产　asset

具有价值或对价值做出贡献的对象。

注:资产具有一个或多个信息安全属性(3.1.20),当信息安全属性被违背时可能导致一个或多个危害场景(3.1.22)。

3.1.3

攻击可行性　attack feasibility

攻击路径(3.1.4)的属性,描述成功执行相应攻击活动的难易度。

3.1.4

攻击路径　attack path

攻击　attack

为实现威胁场景(3.1.33)的一组蓄意活动。

3.1.5

攻击者　attacker

执行攻击路径(3.1.4)的个人、团体或组织。

3.1.6

审核　audit

对过程进行检查，以确定过程目标的实现程度。

3.1.7

组件　component

逻辑上和技术上能分离的组成部分。

3.1.8

客户　customer

接受服务或产品的个人或组织。

3.1.9

信息安全　cybersecurity

道路车辆信息安全　road vehicle cybersecurity

使资产(3.1.2)处于受到充分保护的状态，免受道路车辆相关项(3.1.25)、其功能及其电气或电子组件(3.1.7)的威胁场景(3.1.33)的危害。

注：为简洁起见，本文件使用“信息安全”一词代替道路车辆信息安全。

3.1.10

信息安全评估　cybersecurity assessment

信息安全(3.1.9)状态的评价。

3.1.11

信息安全档案　cybersecurity case

有证据支持的结构化论证，表明风险(3.1.29)的合理性。

3.1.12

信息安全声明　cybersecurity claim

关于风险(3.1.29)的声明。

注：包括保留或分担风险的理由。

3.1.13

信息安全概念　cybersecurity concept

相关项(3.1.25)的信息安全需求和对操作环境(3.1.26)的要求以及有关信息安全控制(3.1.14)的相关信息。

3.1.14

信息安全控制　cybersecurity control

改变风险(3.1.29)的措施。

3.1.15

信息安全事态　cybersecurity event

与相关项(3.1.25)或组件(3.1.7)有关的信息安全信息(3.1.18)。

3.1.16

信息安全目标　cybersecurity goal

与一个或多个威胁场景(3.1.33)相关的概念级信息安全需求。

3.1.17

信息安全事件　cybersecurity incident

可能涉及漏洞(3.1.38)利用的情况。

3.1.18

信息安全信息　cybersecurity information

与信息安全(3.1.9)有关的信息,其相关性尚未确定。

3.1.19

信息安全接口协议　cybersecurity interface agreement

客户(3.1.8)和供应商之间关于分布式信息安全活动(3.1.23)的协议。

3.1.20

信息安全属性　cybersecurity property

值得保护的属性。

注:属性包括保密性、完整性和可用性。

3.1.21

信息安全规范　cybersecurity specification

信息安全需求和相应的架构设计(3.1.1)。

3.1.22

危害场景　damage scenario

涉及车辆或车辆功能且影响道路使用者(3.1.31)的不良后果。

3.1.23

分布式信息安全活动　distributed cybersecurity activities

相关项(3.1.25)或组件(3.1.7)的信息安全活动,其责任在客户(3.1.8)和供应商之间分配。

3.1.24

影响　impact

因危害场景(3.1.22)造成的损害程度或物理伤害程度的估计。

3.1.25

相关项　item

在车辆层面实现一个功能的组件(3.1.7)或组件集。

注:如果一个系统在车辆层面实现了一个功能,它就能成为一个相关项,否则就是一个组件。

3.1.26

操作环境　operational environment

在操作使用中考虑到相互作用的环境。

注:相关项(3.1.25)或组件(3.1.7)的操作使用,包括在车辆功能、生产、服务和修理中的使用。

3.1.27

独立于环境　out-of-context

未在特定相关项定义下的开发。

示例:基于假设信息安全需求的处理单元可集成到不同的相关项(3.1.25)中。

3.1.28

渗透测试　penetration testing

模拟真实攻击的信息安全测试,用以识别破坏信息安全目标(3.1.16)的方法。

3.1.29

风险　risk

信息安全风险　cybersecurity risk

道路车辆信息安全(3.1.9)不确定性的效果,用攻击可行性(3.1.3)和影响(3.1.24)表示。

3.1.30

风险管理　risk management

指导和控制组织的风险(3.1.29)的协调活动。

3.1.31

道路使用者　road user

参与道路交通活动的人员。

示例：乘客、行人、骑行人、车辆驾驶者、车辆拥有者。

3.1.32

裁剪　tailor

省略某项活动或者以与本文件中所描述的不同方式来执行某项活动。

3.1.33

威胁场景　threat scenario

为实现危害场景(3.1.22)，一个或多个资产(3.1.2)的信息安全属性(3.1.20)遭到破坏的潜在原因。

3.1.34

分类　triage

分析以确定信息安全信息(3.1.18)与某一相关项(3.1.25)或组件(3.1.7)的相关性。

3.1.35

触发器　trigger

用于分类(3.1.34)的准则。

3.1.36

确认　validation

通过提供客观证据以证明相关项(3.1.25)的信息安全目标(3.1.16)是否充分并已实现。

3.1.37

验证　verification

通过提供客观证据确认是否满足特定要求。

3.1.38

漏洞/脆弱性　vulnerability

能被利用的弱点(3.1.40)，作为攻击路径(3.1.4)的一部分。

3.1.39

漏洞分析　vulnerability analysis

系统地识别和评估漏洞(3.1.38)。

3.1.40

弱点　weakness

可导致非预期行为的缺陷或特征。

示例：如缺少需求或规范；架构或设计缺陷，包括安全协议的不正确设计；实现的弱点，包括硬件和软件的缺陷，安全协议的不正确的实现；操作过程或程序有缺陷，包括操作不当和用户培训不足；使用过时或弃用的功能，包括加密算法等。

3.2　缩略语

下列缩略语适用于本文件。

CAL：信息安全保障等级(Cybersecurity Assurance Level)

CVSS：通用漏洞评分系统(Common Vulnerability Scoring System)

ECU：电子控制单元（Electronic Control Unit）

E/E：电子电气（Electrical and Electronic）

OBD：车载诊断（On-Board Diagnostic）

OEM：原始设备制造商（Original Equipment Manufacturer）

PM：许可（Permission）

RASIC：责任、批准、支持、知情、咨询（Responsible，Accountable，Supporting，Informed，Consulted）

RC：建议（Recommendation）

RQ：要求（Requirement）

TARA：威胁分析和风险评估（Threat Analysis and Risk Assessment）

WP：工作成果（Work Product）

4 整体考虑

一个相关项包括车辆中实现整车级别特定功能（例如：制动）的所有电子设备和软件（组件）。一个相关项或一个组件与各自的操作环境相互作用。

本文件仅适用于批量生产的道路车辆（不是原型车）与信息安全相关的相关项和组件，包括售后和配套服务组件。出于信息安全目的可能考虑车辆的外部系统（例如：后端服务器），但不在本文件的范围内。

本文件从单个相关项的角度来描述信息安全工程。本文件未规定如何适当分配道路车辆 E/E 架构中相关项功能。对于车辆整体而言，可能考虑构建车辆 E/E 架构或其信息安全相关的相关项和组件的信息安全档案集。如果在相关项和组件上执行了本文件中描述的信息安全活动，将会解决车辆不合理的信息安全风险。如图 1 所示，本文件中描述的组织整体信息安全风险管理适用于全生命周期。

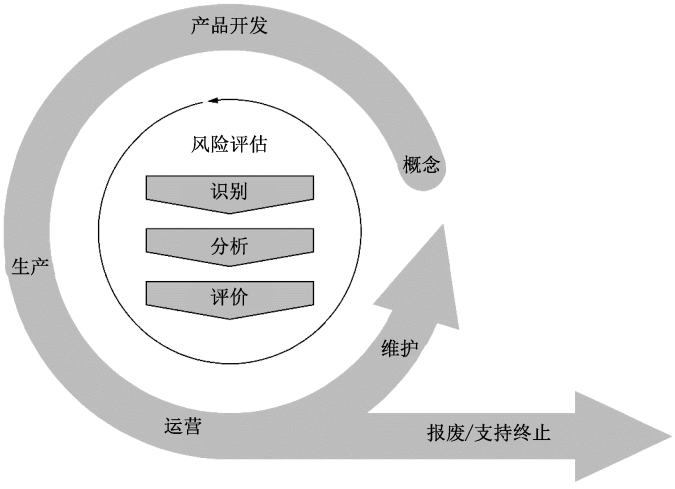


图 1 整体信息安全风险管理

信息安全风险管理适用于整个供应链，以支持信息安全工程。汽车供应链表现出多样化的合作模式，并非所有的信息安全活动都适用于与某个特定项目相关的所有组织，信息安全活动可根据具体情况的需要进行裁剪。某一特定相关项或组件的开发伙伴应就工作分工达成一致，以便执行适用的信息安全活动。图 2 显示了一个相关项、功能、组件和相关术语之间的关系。

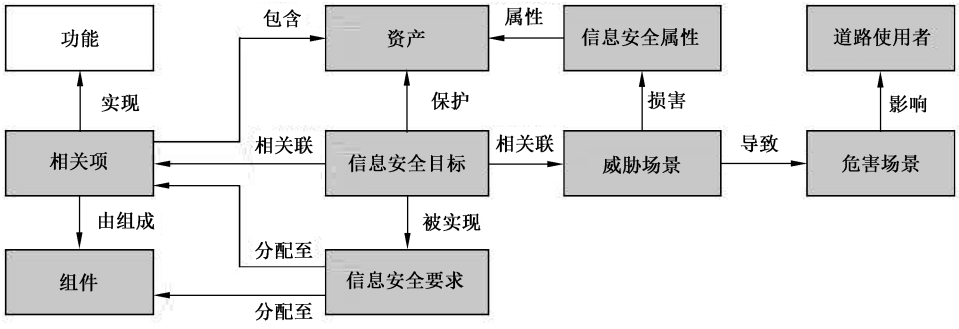


图 2　相关项、功能、组件和相关术语之间的关系

第 15 章描述了信息安全风险评估的模块化方法，这些方法在其他条款描述的信息安全风险活动中被引用。

在信息安全工程背景下的分析活动，可识别和探索恶意攻击者的潜在行为，以及车辆 E/E 系统的信息安全损害后可能产生的危害。信息安全工程和其他学科的专业知识之间的协调可支持深入分析并减轻具体的信息安全风险。信息安全监测、补救和事件响应活动作为概念和产品开发活动的补充，可作为一种被动的方法，确认环境中不断变化的条件（例如：新的攻击技术），需要持续地识别和管理道路车辆 E/E 系统的弱点和漏洞。

纵深防御的方法可用于减轻信息安全风险。纵深防御方法利用多层信息安全控制来提高车辆的信息安全性。如果攻击能够穿透或绕过一个层，另一个层能帮助抵御攻击并保持对资产的保护。

5　组织的信息安全管理

5.1　总则

为了实现信息安全工程，组织建立并维护包括信息安全意识管理、能力管理和持续改进在内的信息安全治理和信息安全文化。这涉及制定组织层面的规则和过程，并依据本文件中的目标进行独立审核。

为了支持信息安全工程，组织还建立了信息安全管理体系，包括工具的管理和质量管理体系的应用。

5.2　目的

本章的目的是：

a)　定义信息安全方针和组织层面的信息安全规则和过程；

b)　分配执行信息安全活动所需的职责和相应的权限；

c)　支持信息安全的实施，包括资源的提供和信息安全过程与其他相关过程之间相互作用的管理；

d)　管理信息安全风险；

e)　建立并维护信息安全文化，包括能力管理、意识管理和持续改进；

f)　支持并管理信息安全信息的共享；

g)　建立并维护支撑信息安全维护的管理体系；

h)　提供证据证明使用的工具不会对信息安全产生不利的影响；

i)　执行组织层面的信息安全审核。

5.3 输入

5.3.1 先决条件

无。

5.3.2 支持信息

可考虑以下信息：

符合质量管理标准的证据。

示例：IATF 16949 与其他标准的联合，例如：ISO 9001、ISO 10007、ISO/IEC 330××系列标准、ISO/IEC/IEEE 15288 和 ISO/IEC/IEEE 12207。

5.4 要求和建议

5.4.1 信息安全治理

[RQ-05-01]组织应定义信息安全方针，包含：

a) 对道路车辆信息安全风险的确认；

b) 高级管理层对相应信息安全风险进行管理的承诺。

注 1：信息安全方针与组织目标及其他方针相关联。

注 2：在考虑内部和外部环境的情况下，信息安全方针可能包括一项声明，说明对组织的产品或服务组合的一般威胁场景的风险处理。

[RQ-05-02]组织应建立并维护组织层面的规则和过程，以满足以下要求：

a) 能够实施本文件的要求；

b) 支持相应活动的执行。

示例 1：如过程定义、技术规则、指南、方法和模板。

注 3：信息安全风险管理包括活动的付出-收益的考虑。

注 4：这些规则和过程覆盖概念、产品开发、生产、运营、维护和报废，包括 TARA 的方法、信息共享、信息安全监测、信息安全事件响应和触发。

注 5：有关漏洞披露的规则和过程，例如：信息共享的一部分，依据 GB/T 30276—2020 或 ISO/IEC 29147 定义。

注 6：图 3 概述了总体的信息安全方针（见[RQ-05-01]）与具体组织的信息安全规则和过程（见[RQ-05-02]）、职责（见[RQ-05-03]）和资源（见[RQ-05-04]）之间的关系。

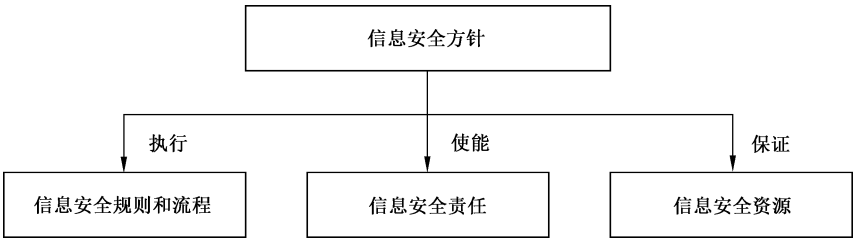


图 3 信息安全治理

[RQ-05-03] 组织应分配和传达实现信息安全的职责，并给予相应的组织权力。

注 7：既与项目层面的活动相关，也与组织层面的活动相关。

[RQ-05-04]组织应提供解决信息安全问题所需的资源。

注 8：资源包括负责信息安全风险管理、开发、事件管理的人员。

示例 2：熟练的人员和合适的工具来执行信息安全活动。

[RQ-05-05]组织应识别与信息安全有关或相互作用的专业领域，并在这些专业领域之间建立和维护沟通的渠道，以满足以下要求：

a) 确定是否要将信息安全融入现有过程中，以及如何融合；

b) 协调相关信息的交换。

注 9：协调包含各学科之间共享过程，以及策略和工具的使用。

注 10：学科包含信息技术安全、功能安全和隐私保护。

示例 3：跨学科的交换：

——威胁场景和危害信息；

——信息安全目标和功能安全目标；

——信息安全要求与功能安全要求的冲突或对抗。

5.4.2 信息安全文化

[RQ-05-06]组织应培养并维护强大的信息安全文化。

注 1：示例见附录 B。

[RQ-05-07]组织应确保被分配了信息安全角色和职责的人员具有履行这些角色和职责的能力和意识。

注 2：能力、意识和培训项目考虑以下范围：

——与信息安全相关的组织规则和过程，包括信息安全风险管理；

——与信息安全学科相关的信息安全规则和过程，例如：功能安全和隐私保护；

——领域知识；

——系统工程；

——信息安全有关的方法、工具、指南；

——已知的攻击手段和信息安全控制。

[RQ-05-08]组织应建立并维护持续改进过程。

示例：持续改进过程包括：

——从以前的经验中学习，包括通过信息安全监测和内外部信息安全相关信息观察而收集的信息安全信息；

——从领域中类似的应用产品的信息安全信息中学习；

——在后续的信息安全活动中进行改进；

——将信息安全经验教训传达给适当的人员；

——根据[RQ-05-02]检查组织规则和过程的充分性。

注 3：持续改进适用于本文件中的所有信息安全活动。

5.4.3 信息共享

[RQ-05-09]组织应界定在组织内部和外部要求、允许或禁止共享信息安全相关信息的情形。

注：共享信息的情况可能基于：

——共享的信息类型；

——共享的审批过程；

——信息的编辑要求；

——源头归属的规则；

——为特定方提供的通信类型；

——漏洞披露程序(见 5.4.1 的注 5)；

——面向接收方的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，将共享数据的信息安全管理与其他各方保持一致。

示例：公共、内部、机密和第三方机密的安全分类级别的一致。

5.4.4 管理体系

[RQ-05-11]组织应按国际标准或者同等标准建立和维护一个质量管理体系来支撑信息安全工程，包含：

示例 1：IATF 16949 与 GB/T 19001 或 ISO 9001 相结合。

a) 变更管理；

注 1：信息安全变更管理的范围是管理相关项及其组件的变更，以便继续满足适用的信息安全目标和要求。例如：根据生产控制计划评审生产过程的变更，以防止此类变更引入新的漏洞。

b) 文档管理；

注 2：一项工作成果被合并或映射到不同的文档库。

c) 配置管理；

d) 需求管理。

[RQ-05-12]用于维护在实地运行中的产品信息安全所需的配置信息应在产品信息安全支持结束前保持可用，以便能采取补救措施。

注 3：归档生成环境有助于确保配置信息的后续使用。

示例 2：物料清单、软件配置。

[RC-05-13]宜建立生产过程的信息安全管理体系，以便支持第 12 章的活动。

示例 3：GB/T 33007—2016 或 IEC 62443-2-1。

5.4.5 工具管理

[RQ-05-14] 应管理能够影响相关项或组件信息安全的工具。

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

示例 2：用于生产的工具，例如 Flash 刷写工具、EOL 测试工具。

示例 3：用于售后维修的工具，例如 OBD 工具或者重新编程工具。

注：这类管理可能通过以下方式确立：

——用户手册及勘误表的使用；

——对非预期的使用和操作进行防护；

——对工具使用者进行访问控制；

——对工具进行认证。

[RC-05-15]支持信息安全事件补救措施的合适环境宜是可复现的，直至产品的信息安全支持结束。

示例 4：用于复现和管理漏洞的测试、软件构建和开发环境。

示例 5：用于构建产品软件的工具链和编译器。

5.4.6 信息安全管理

[RC-05-16]工作成果宜按照信息安全管理体系进行管理。

示例：可将工作成果存储在文件服务器上，以防止未经授权的变更或删除。

5.4.7 组织层面的信息安全审核

[RQ-05-17]应独立进行信息安全审核以判断组织的过程是否达到了本文件的目标。

注 1：将信息安全审核纳入质量管理体系标准的审核中，或者与之相结合。例如：IATF 16949 与 GB/T 19001 或 ISO 9001 相结合。

注 2：独立性可能基于 GB/T 34590 系列标准。

注 3：执行审核的人员可能来自组织内部或者外部。

注 4：为了确保组织的过程始终适用于信息安全，可能周期性执行审核。

注 5：图 6 展示了组织的信息安全审核和其他信息安全活动间的关系。

5.5 工作成果

[WP-05-01]由 5.4.1～5.4.3 得出的信息安全方针、规则和过程。

[WP-05-02]由[RQ-05-07]得出的能力管理和意识管理的证据以及由 5.4.2 中[RQ-05-08]得出的持续改进的证据。

[WP-05-03]由 5.4.4 和 5.4.6 得出的组织管理体系的证据。

[WP-05-04]由 5.4.5 得出的工具管理的证据。

[WP-05-05]由 5.4.7 得出的组织层面的信息安全审核报告。

6 项目相关的信息安全管理

6.1 总则

本章描述了有关特定项目的信息安全开发活动的管理要求。

项目相关的信息安全管理包括职责分配和信息安全活动的计划。本文件以通用方式定义要求，以便能将其应用于各种相关项和组件。另外，能基于基本原理在信息安全计划中进行裁剪。能使用裁剪的示例包括：

——复用；

——独立于环境的组件；

——使用现成组件；

——更新。

无论相关项、组件或其操作环境是否发生变更，都能策略性地复用相关项和组件。但是，变更可能会引入原始相关项或组件尚未考虑的漏洞。此外，已知攻击可能发生了变化，例如：

——攻击技术的发展；

——新出现的漏洞，例如：从信息安全监测或信息安全事件评估中得知的漏洞；

——自初始开发以来资产的变化。

如果原始相关项或组件是根据本文件开发的，则基于现有的工作成果复用该相关项或组件。如果相关项或组件最初不是根据本文件开发的，则基于现有文件复用，并说明理由。

一个组件可独立于环境开发，例如：基于假设的环境。在与客户接触或达成商业协议之前，组织可为不同的应用和不同的客户开发通用组件。供应商可对环境和预期用途进行假设。基于此，供应商可得出独立于环境的开发需求。例如：独立于环境开发微控制器。

现成的组件是指不为特定客户开发的组件，能在不变更其设计或实施的情况下使用。例如：第三方软件库、开源软件组件。现成的组件不被认为是按照本文件要求开发的。

按照本文件，现成的组件和独立于环境开发的组件可被集成到一个相关项或组件中(见图 4)。集成可包含与 6.4.4 中复用分析类似的活动，如果为了解决无效的假设而进行变更，则适用于变更管理。可对准备集成的组件或以集成为目标的组件或相关项进行变更。

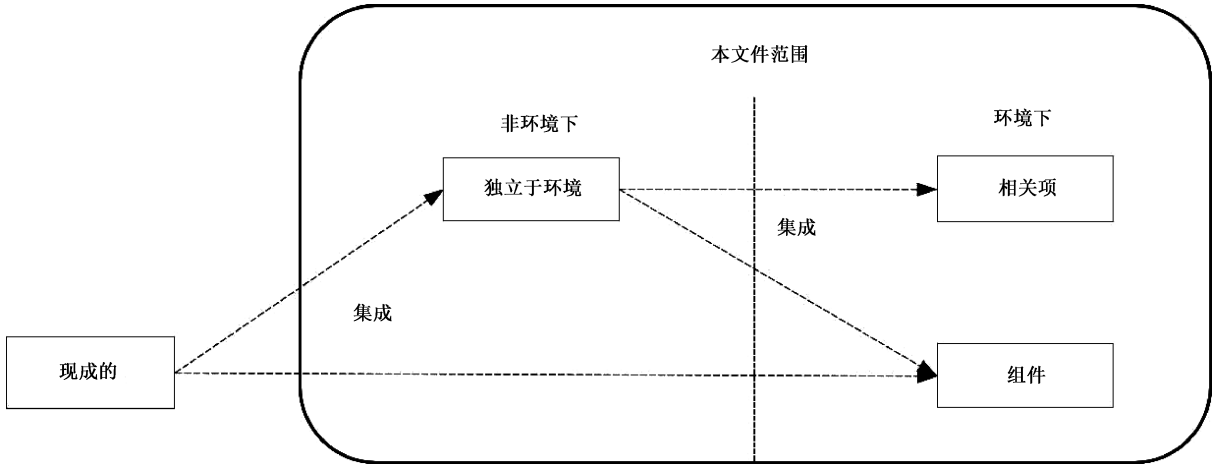


图 4　现成和独立于环境的组件的集成

信息安全档案是信息安全评估和后开发阶段发布的输入。

注：后开发阶段通常包括生产、运维、报废阶段。

信息安全评估可独立判断一个相关项或组件的信息安全，是决定后开发阶段发布的输入。

6.2　目的

本章的目的是：

a）　分配项目的信息安全活动职责；

b）　规划信息安全活动，包括定义裁剪的信息安全活动；

c）　创建一个信息安全档案；

d）　如果适用，执行信息安全评估；

e）　从信息安全的角度决定是否发布相关项或组件以用于后开发阶段。

6.3　输入

6.3.1　先决条件

无。

6.3.2　支持信息

可考虑以下信息：

——组织的信息安全审核报告[WP-05-03]；

——项目计划。

6.4　要求和建议

6.4.1　信息安全职责及其分配

[RQ-06-01]与项目信息安全活动有关的职责应根据[RQ-05-03]进行沟通和分配。

注：信息安全活动的责任可能转移，前提是要进行交流并移交相关信息。

6.4.2　信息安全计划

[RQ-06-02]为了决定相关项或组件的信息安全活动，应分析相关项或组件以确定：

a) 该相关项或组件是否与信息安全相关；

注 1：附录 D 提供了可用于评估信息安全相关性的方法和标准。

注 2：如果确定该相关项或组件与信息安全无关，则没有相关的信息安全活动，因此不会启动信息安全计划。

b) 如果该相关项或组件与信息安全有关，该相关项或部件是新开发还是复用；

c) 是否按照 6.4.3 进行裁剪。

[RQ-06-03]信息安全计划应包括：

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) 执行活动所需的资源；

e) 开始节点或终止节点以及预期持续时间；

f) 工作成果的标识。

[RQ-06-04]应根据[RQ-05-03]和[RQ-05-04]分配、开发和维护信息安全计划以及根据信息安全计划跟踪信息安全活动进度的职责。

[RQ-06-05]信息安全计划应满足以下至少一项：

a) 在开发项目计划中提及；

b) 包括在项目计划中，以使信息安全活动具有可区分性。

注 3：信息安全计划能在配置管理下包含与其他计划(例如：项目计划)的交叉引用(见[RQ-06-09])。

[RQ-06-06]信息安全计划应根据第 9 章、第 10 章、第 11 章和第 15 章的相关要求，指定与概念阶段和产品开发阶段所需要的信息安全活动。

[RQ-06-06]当进行的活动确定要发生更改或细化时，应更新信息安全计划。

注 4：信息安全计划能在开发过程中逐步完善。例如：信息安全计划能根据信息安全活动的结果进行更新，如 TARA(见第 15 章)。

[PM-06-08]对于根据 15.8 分析确定的风险值为 1 的威胁场景，可省略与 9.5、第 10 章、第 11 章的符合性。

注 5：如果这些威胁场景对信息安全产生影响，相应风险也会得到处理，尽管可能没有本文件中定义的那么严格。

注 6：可能根据信息安全档案中定义的理论依据来论证此类风险的处理是否充分，基于质量管理标准符合性的基本原理并结合其他措施，如 IATF 16949 与 GB/T 19001—2016 或 ISO 9001 相结合，例如：

——信息安全意识保证；

——质量人员的信息安全培训；

——组织的质量管理体系中规定的信息安全具体措施。

[RQ-06-09]信息安全计划中确定的工作成果应在后开发阶段发布之前和发布时进行更新并保持准确性。

[RQ-06-10]对于分布式信息安全活动，客户和供应商均应根据第 8 章为其各自的信息安全活动和接口定义信息安全计划。

[RQ-06-11]信息安全计划应按照 5.4.4 的规定，进行配置管理和文档管理。

[RQ-06-12]按照 5.4.4 的规定，信息安全计划中确定的工作成果，应进行配置管理、变更管理、需求管理和文档管理。

6.4.3 裁剪

[PM-06-13]信息安全活动可被裁剪。

[RQ-06-14]如果信息安全活动被裁剪了，应提供并审查裁剪的理由，用来证明可通过裁剪充分实

现本文件的相关目标。

注：因供应链中的另一实体执行而未执行的活动不被视为裁剪，被视为分布式信息安全活动。然而，信息安全活动的分布可能导致联合裁剪。

6.4.4 复用

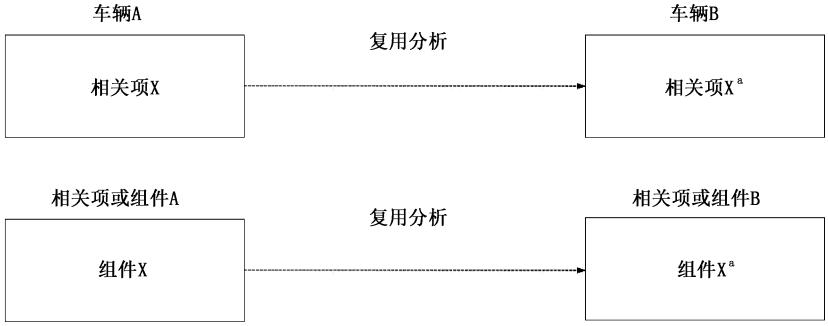
[RQ-06-15]如果一个相关项或组件完成开发，应开展复用分析：

a) 计划进行变更；

b) 计划在另一个操作环境中复用；

示例 1：由于在新的操作环境中安装了现有的相关项或组件，或者由于与之交互的其他相关项或组件的升级而使环境发生了变更(见图 5)。

c) 计划在不变更的情况下复用，并且有关相关项或组件的信息也有相应的变化。



[a] 可作为复用分析的结果而改变。

图 5 复用分析示例

示例 2：已知攻击和漏洞的变化，或威胁场景的变化。

注 1：在确定是否复用时，需考虑现有的工作成果。

注 2：变更可能包括设计变更、实施变更：

——设计变更可能来自需求变更，例如：功能或性能增强；

——软件修正或使用新的生产或维护工具，例如：基于模型的开发，可能会导致实施变更。

注 3：配置数据或校准数据的变更，如果影响现有相关项或组件的功能行为和资产或信息安全属性，则视为发生变更。

[RQ-06-16]相关项或组件的复用分析应：

a) 识别相关项或组件的变更和操作环境的变更；

b) 分析变更后的信息安全影响，包括对信息安全声明和先前假设的有效性的影响；

示例 3：对信息安全需求、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) 识别受影响或缺少的工作成果；

示例 4：TARA 考虑新的或变更的资产、威胁场景或风险值。

d) 在信息安全计划中指定符合本文件所需的信息安全活动。

注 4：可能产生裁剪。

[RQ-06-17]组件的复用分析应评估：

a) 该组件能够满足其要集成的相关项或组件所分配的信息安全要求；

b) 现有文档是否足以支持该组件集成到一个相关项或另一个组件中。

6.4.5 独立于环境的组件

[RQ-06-18]应在相应的工作成果中记录独立于环境开发的组件对预期用途和环境的假设，包括外部接口。

[RQ-06-19]对于独立于环境的组件的开发，信息安全需求应基于[RQ-06-18]的假设。

[RQ-06-20]对于独立于环境开发的组件的集成，应验证[RQ-06-18]的信息安全声明和假设。

6.4.6 现成组件

[RQ-06-21]当集成现成组件时，应收集和分析与信息安全相关的文件，以确定：

a) 满足分配的信息安全需求；

b) 组件适合于预期的特定应用环境；

c) 现有的证明文件是否足以支持信息安全活动。

[RQ-06-22]如果现有的证明文件不足以支持现成组件的集成，那么应识别并执行符合本文件的信息安全活动。

示例：有关漏洞的文件不充分。

注：这可能意味着裁剪。

6.4.7 信息安全档案

[RQ-06-23]应创建一个信息安全档案，为相关项或组件的信息安全提供证据，并有工作成果加以支持。

注 1：可能省略证据(例如：如果从已编译的工作成果集看出该证据，则可能省略该证据)。

注 2：在分布式开发中，相关项的信息安全档案可能是客户和供应商的信息安全档案的组合，其中引用各方产生的工作成果的证据。相关项的整体证据由各方的证据共同支持。

注 3：信息安全档案需考虑后开发的信息安全需求[WP-10-02]。

6.4.8 信息安全评估

[RQ-06-24]应采用基于风险的基本原理决定是否对相关项或组件进行信息安全评估。

注 1：基本原理可能基于：

——TARA 分析结果；

——待开发相关项或组件的复杂性；

——组织规则和过程所规定的标准。

注 2：如果不进行信息安全评估，可能将基本原理记录在信息安全档案中。

[RQ-06-25]应独立评审[RQ-06-24]的基本原理。

注 3：独立方案能基于 GB/T 34590 系列标准。

[RQ-06-26]信息安全评估应判断相关项或组件的信息安全。

注 4：现有证据由信息安全活动的记录结果提供，如工作成果(见附录 A)。

注 5：图 6 说明组织信息安全审核、项目级信息安全评估和其他信息安全活动之间的关系。

注 6：信息安全评估能逐步进行，以尽早解决已发现的问题。

注 7：信息安全评估可能重复或补充。例如：由于变更，之前的信息安全评估提供了否定建议或发现了漏洞。

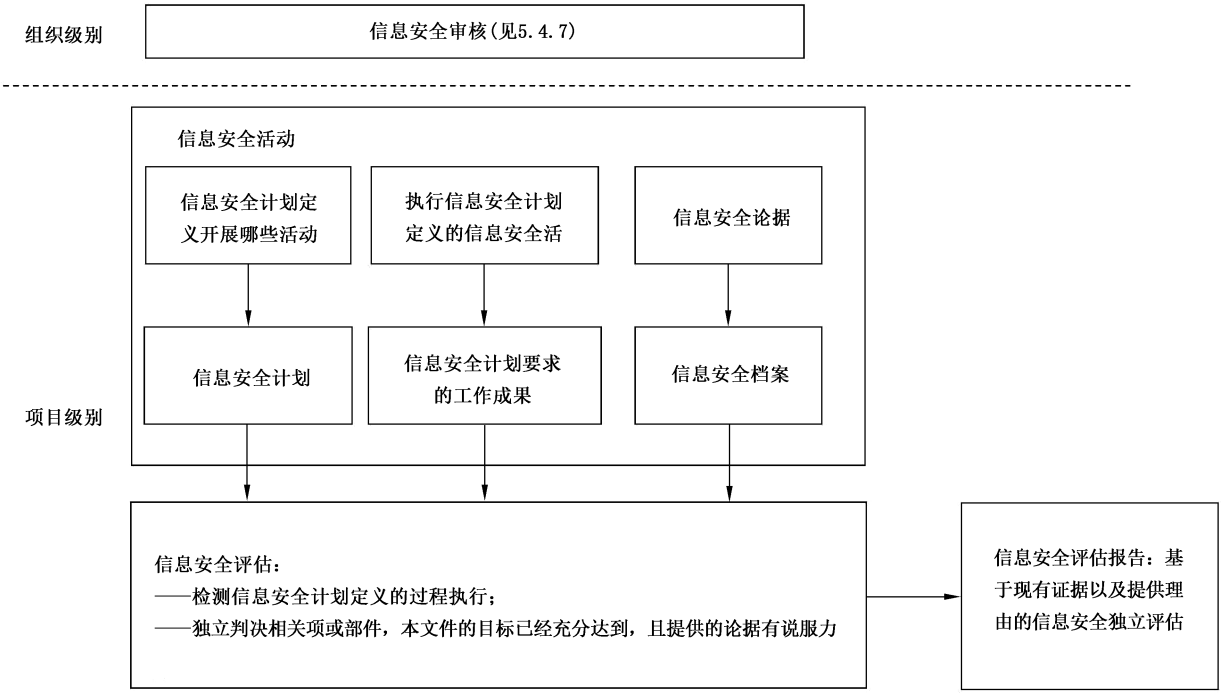


图 6　与其他信息安全活动有关的信息安全评估

[RQ-06-27]应根据[RQ-06-01],任命负责计划和独立进行信息安全评估的人员。

注 8：独立方案能基于 GB/T 34590 系列标准。

示例：来自组织内不同团队或部门的人员,如质量保证部门,来自独立组织的人员。

[RQ-06-28]进行信息安全评估的人员应：

a)　有权获得相关信息和工具；

b)　获得执行信息安全活动的人员的合作。

[PM-06-29]可基于对是否达到本文件目标的判断进行信息安全评估。

[RQ-06-30]信息安全评估的范围应包括：

a)　信息安全计划和信息安全计划要求的所有工作成果；

b)　对信息安全风险的处理；

c)　项目实施的信息安全控制和信息安全活动的适当性和有效性；

注 9：合理性和有效性可能通过使用前期为验证而进行的评审来判断。

d)　如果提供,证明已达到本文件目标的基本原理。

注 10：考虑到[PM-06-13],工作成果的创建负责人能提供一个基本原理,解释为什么要实现本文件的相应目标以促进信息安全评估。

注 11：符合所有相应要求是实现本文件目的充分基本原理。

[RQ-06-31]信息安全评估报告应包括接受,带条件接受或拒绝该相关项或组件的信息安全建议。

注 12：评估报告也可能包括持续改进建议。

[RQ-06-32]如果提出了根据[RQ-06-31]的带条件接受建议,则信息安全评估报告应包括接受条件。

6.4.9　后开发的发布

[RQ-06-33]以下工作成果应在后开发阶段的发布之前可用：

——信息安全档案[WP-06-02]；

——如果适用，信息安全评估报告[WP-06-03]；

——后开发阶段的信息安全需求[WP-10-02]。

[RQ-06-34]相关项或组件在后开发的发布应满足以下条件：

a) 信息安全档案提供了充分的证据证明信息安全；

b) 如果适用，通过信息安全评估确认信息安全档案；

c) 后开发阶段的信息安全需求被接受。

6.5 工作成果

[WP-06-01]由 6.4.1～6.4.6 得出的信息安全计划。

[WP-06-02]由 6.4.7 得出的信息安全档案。

[WP-06-03]如果适用，由 6.4.8 得出的信息安全评估报告。

[WP-06-04]由 6.4.9 得出的后开发阶段的发布报告。

7 分布式信息安全活动

7.1 总则

如果相关项或组件信息安全活动的责任是分布式的，则本条适用。本章描述了分布式信息安全活动的管理，并且适用于以下情况：

a) 在分布式信息安全活动中开发的相关项和组件；

b) 客户与供应商间的交互；

c) 客户与供应商接口协议适用的所有阶段。

内部供应商和外部供应商可采用同样的方式进行管理。

示例：一个 1 级供应商(tier-1)是某 OEM 开发过程中的供应商，在另一个组件供应的合同关系中它是某 2 级供应商(tier-1)的客户，这在图 7 中进行了说明。

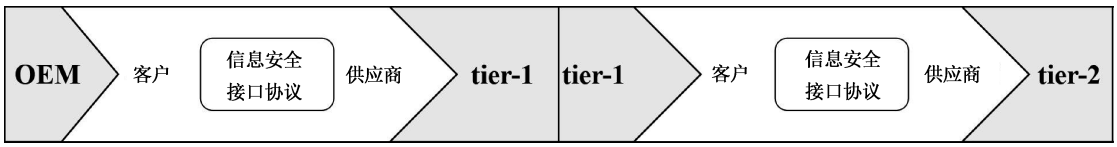


图 7 供应链中客户/供应商关系的示例

7.2 目的

本章的目的是定义客户和供应商在信息安全活动中的交互、依赖和职责。

7.3 输入

无。

7.4 要求和建议

7.4.1 供应商的能力

[RQ-07-01]如果适用，应按本文件评价潜在供应商在开发以及后开发活动方面的能力。

注 1：该评价能用来支持供应商的选择，可能依据本文件要求的能力，也可能依据其他国家或国际的信息安全工程标准的实施情况进行评价。

[RC-07-02]供应商宜提供信息安全能力记录，来支持客户对供应商能力的评价。

注 2：信息安全能力记录包含：

——组织关于信息安全能力的证据（例如：在开发、后开发、治理、质量和传统信息安全等方面的信息安全最佳实践）；

——开展可持续的信息安全活动（见第 8 章）和信息安全事件响应（见第 13 章）的证据；

——以往信息安全评估报告的总结。

7.4.2 询价

[RQ-07-03]客户向潜在供应商发出的报价请求应包含：

a) 符合本文件的正式要求；

b) 7.4.3 中对供应商履行信息安全职责的预期；

c) 与供应商报价的相关项或组件有关的信息安全目标或信息安全需求集。

示例：关于消息认证的信息安全需求。

7.4.3 职责的协调

[RQ-07-04]客户和供应商应在信息安全接口协议中规定分布式信息安全活动，包含：

a) 任命信息安全相关的客户和供应商的联络人；

b) 识别需要由客户和供应商各自实施的信息安全活动；

示例 1：客户执行整车层面的信息安全确认。

示例 2：后开发阶段的信息安全活动的分布。

示例 3：供应商、客户或者第三方可就供应商开发的组件或工作成果进行信息安全评估。

c) 如果适用，按照 6.4.3 共同对信息安全活动进行裁剪；

d) 应共享信息和工作成果；

注 1：共享的信息可能包含：

——分发、评审和发生信息安全问题时的反馈机制；

——漏洞和其他信息安全相关发现的信息交换流程，例如风险相关信息；

——接口相关的过程、方法和工具，用来确保客户和供应商对接的兼容性，例如对于数据的恰当处理和对传输数据的通信网络的安全防护；

——角色的定义；

——沟通和记录相关项或组件变更的方法，包含 TARA 潜在重复使用；

——需求管理工具的统一；

——信息安全评估的结果。

e) 分布式信息安全活动的里程碑；

f) 相关项或组件的信息安全支持终止的定义。

[RC-07-05]信息安全接口协议应在客户和供应商开始分布式活动前共同商定。

[RQ-07-06]如果根据[RQ-08-07]识别的漏洞需要管理，则客户和供应商应对采取的行动及行动的职责达成共识。

[RQ-07-07]如果需求不清楚、不可行或与其他信息安全需求或相关领域的需求相冲突，则客户和供应商应互相通知对方，以便做出适当的决定并采取行动。

[RC-07-08]在职责分配矩阵中规定职责。

注 2：能使用 RASIC 表，见附录 C。

7.5 工作成果

[WP-07-01]由 7.4.3 得出的信息安全接口协议。

8 持续的信息安全活动

8.1 总则

本章包括以下内容：

a) 持续的信息安全活动可在全生命周期的每一个阶段进行，也可在项目之外进行；
b) 信息安全监测收集信息安全情报并根据已定义的触发器进行分类；
c) 信息安全事态评估帮助确定信息安全事件是否展现了相关项和组件的脆弱性；
d) 漏洞分析检查弱点，并评估该弱点是否可被用于发动攻击；
e) 漏洞管理跟踪并监督相关项和组件中的漏洞处理，直至信息安全支持结束。

8.2 目的

本章的目的是：

a) 监控信息安全情报从而识别信息安全事态；
b) 评估信息安全事态从而识别弱点；
c) 识别来自脆弱性的漏洞；
d) 管理已识别的漏洞。

8.3 信息安全监测

8.3.1 输入

8.3.1.1 先决条件

应提供以下信息：

在[WP-05-01]中用于开发触发器的规则和过程。

8.3.1.2 支持信息

可考虑以下信息：

——相关项定义[WP-09-01]；
——信息安全声明[WP-09-04]；
——信息安全规范[WP-10-01]；
——威胁场景[WP-15-03]；
——以往的漏洞分析结果[WP-08-05]；
——现场收集的信息。

示例：漏洞扫描报告、修复信息、顾客使用信息。

8.3.2 要求和建议

[RQ-08-01]应选择信息安全情报收集的来源。

注 1：能选择外部、内部的来源。

注 2：内部来源可能包括列在 8.3.1.2 的来源。

注 3：外部来源可能包括：

——信息安全研究员；

——商业或非商业的来源；

——组织的供应链；

——组织的客户；

——政府来源。

示例：最先进的攻击方法的来源。

[RQ-08-02]应该定义和维护触发器，以便进行信息安全情报分类。

注 4：触发器可能包括关键字、配置信息的参考文件、组件或供应商的名称。

[RQ-08-03]应收集和分类信息安全情报，并确定是否成为一个或多个信息安全事态。

8.3.3 工作成果

[WP-08-01]由[RQ-08-01]得出的信息安全情报来源。

[WP-08-02]由[RQ-08-02]得出的触发器。

[WP-08-03]由[RQ-08-03]得出的信息安全事态。

8.4 信息安全事态评估

8.4.1 输入

8.4.1.1 先决条件

应提供以下信息：

——信息安全事态[WP-08-03]；

——如有后开发阶段的信息安全需求；

——对应[RQ-05-12]的配置信息。

8.4.1.2 支持信息

可考虑以下信息：

——相关项定义[WP-09-01]；

——信息安全规范[WP-10-01]；

——以往的漏洞分析结果[WP-08-05]。

8.4.2 要求和建议

[RQ-08-04]应评估信息安全事态，以识别相关项或组件中的弱点。

注 1：此活动可与[RQ-08-03]中的分类相结合使用。

注 2：如果存在弱点并且有对应的补救措施(例如：供应商为组件中的漏洞提供了修补程序)，则组织可能将该补救措施作为无需任何其他活动的漏洞来处理。

注 3：能根据此评估结果更新威胁场景[WP-15-03]。

8.4.3 工作成果

[WP-08-04]由[RQ-08-04]得出的信息安全事态的弱点。

8.5 漏洞分析

8.5.1 输入

8.5.1.1 先决条件

应提供以下信息：

相关项定义[WP-09-01]或信息安全规范[WP-10-01]。

注：如果对相关项进行漏洞分析，则使用相关项的定义；如果对组件进行漏洞分析，则使用信息安全规范。

8.5.1.2 支持信息

可考虑以下信息：

——信息安全事态中的弱点[WP-08-04]；

——产品开发过程中发现的弱点[WP-10-05]；

——以往的漏洞分析结果[WP-08-05]；

——攻击路径[WP-15-05]；

——验证报告[WP-10-04]和[WP-10-07]；

——以往的信息安全事件。

8.5.2 要求和建议

[RQ-08-05]应分析弱点以识别漏洞。

注 1：该分析可能包括：

——架构分析；

——根据 15.6 进行的攻击路径分析；

——根据 15.7 进行的攻击可行性定级。

注 2：通过执行根本原因分析，来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，则该弱点不被视为漏洞。

示例 2：利用弱点的攻击可行性评级非常低，则该弱点不被视为漏洞。

[RQ-08-06]如果弱点未被确定为漏洞，应提供理由。

8.5.3 工作成果

[WP-08-05]由[RQ-08-05]和[RQ-08-06]得出的漏洞分析结果。

8.6 漏洞管理

8.6.1 输入

8.6.1.1 先决条件

应提供以下信息：

漏洞分析结果[WP-08-05]。

8.6.1.2 支持信息

无。

8.6.2 要求和建议

[RQ-08-07]应对漏洞进行管理，以对每个漏洞开展以下工作：

a) 相应的信息安全风险按照 15.9 进行评估和处理，以便消除不合理的风险；

b) 通过应用独立于 TARA 的补救措施来消除漏洞，例如：开源软件的补丁。

注 1：如果漏洞管理导致相关项和组件变更，则根据[RQ-05-11]进行变更管理。

注 2：有关漏洞的信息可能在分布式信息安全活动的相关环境中共享（例如：攻击路径信息的分享），也可能分享给其他相关方。

[RQ-08-08]如果根据 15.9 的风险处置决策需要进行信息安全事件响应，则应参照 13.3。

注 3：信息安全事件响应流程可能独立于 TARA。

8.6.3 工作成果

[WP-08-06]由[RQ-08-07]得出的漏洞管理证据。

9 概念阶段

9.1 总则

概念阶段涉及整车级别功能在相关项中的实施。在本章中，相关项及其操作环境被识别为“相关项定义（见 9.3）”，相关项定义构成了后续活动的基础。

本章还规定了相关项的信息安全目标（见 9.4）这一最高级别的要求。为此，通过第 15 章（见附录 H 的图 H.1）的方法完成信息安全风险评估。此外，9.4 规定了信息安全声明，用于解释风险保留和分担的充分性。

信息安全概念（见 9.5）由信息安全需求和对操作环境的要求组成，两者都源于信息安全目标，并基于对该相关项的全面看法。

9.2 目的

本章的目的是：

a) 定义相关项、操作环境和在信息安全上下文中的相互影响；

b) 明确信息安全目标和信息安全声明；

c) 明确实现信息安全目标的信息安全概念。

9.3 相关项定义

9.3.1 输入

9.3.1.1 先决条件

无。

9.3.1.2 支持信息

可考虑以下信息：

有关该相关项和操作环境的现有信息。

示例：车内 E/E 系统架构，包括车内网络、车外网络、参考模型和前期开发文档。

9.3.2 要求和建议

[RQ-09-01]在相关项中应确定以下信息：

a) 相关项边界；

注 1：相关项边界将相关项与其操作环境区分开来。相关项边界的描述可能包括与车辆内部其他相关或与车辆外部 E/E 系统的接口。

b) 相关项功能；

注 2：相关项功能描述了相关项在生命周期各阶段[例如：产品研发(测试)、生产、运营和维护、报废]的预期行为，包括相关项实现的车辆功能。

c) 初步架构：

注 3：初步架构的描述包括识别相关项的组成部分及其连接，以及相关项的外部接口。

注 4：本文件中的相关项定义，特别是相关项边界，可能与其他学科的相关项定义不同。例如：参考 GB/T 34590 系列标准。

注 5：考虑限制因素和使用的信息安全标准。

注 6：开发一个独立于环境的组件可能基于对一个假定的(通用)相关项的定义和对该相关项内组件功能的描述。

[RQ-09-02]应描述与信息安全有关的相关项的操作环境信息。

注 7：通过描述操作环境及其与相关项之间的交互，可能识别或分析相关的威胁情景和攻击路径。

注 8：相关信息可能包括假设。例如：假设该相关项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]由 9.3.2 得出的相关项定义。

9.4 信息安全目标

9.4.1 输入

9.4.1.1 先决条件

应提供以下信息：

相关项定义[WP-09-01]。

9.4.1.2 支持信息

可考虑以下信息：

信息安全事态[WP-08-03]。

9.4.2 要求和建议

[RQ-09-03]应根据相关项定义进行分析，其中包括：

a) 根据 15.3 进行资产识别；

b) 根据 15.4 进行威胁场景识别；

c) 根据 15.5 进行影响评级；

d) 根据 15.6 进行攻击路径分析；

e) 根据 15.7 对攻击可行性进行评级；

f) 根据 15.8 确定风险值。

注 1：如果相关项定义没有为分析提供足够的信息，可能假设这些信息。

[RQ-09-04]根据[RQ-09-03]的结果，应按照 15.9 的规定为每种威胁场景确定风险处置方案。

注 2：通过消除风险源来避免风险，可能导致按照变更管理对该相关项进行变更。

[RQ-09-05]如果一个威胁场景的风险处置决策包括减少风险，那么应指定一个或多个相应的信息安全目标。

注 3：信息安全目标是保护资产免受威胁场景的要求。

注 4：如果适用，能为信息安全目标确认一个 CAL(见附录 E)。

注 5：能为相关项的任何生命周期阶段指定信息安全目标。

[RQ-09-06]如果一个威胁场景的风险处置决策包括以下情况，则应指定一个或多个相应的信息安全声明：

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。

注 6：信息安全声明能被考虑用于信息安全监测。

[RQ-09-07]应进行验证，以确认满足以下要求：

a) [RQ-09-03]的结果在相关项定义方面的正确性和完整性；

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

c) [RQ-09-05]的信息安全目标和[RQ-09-06]的信息安全声明与[RQ-09-04]风险处置决策之间的完整性、正确性和一致性；

d) [RQ-09-05]的信息安全目标和[RQ-09-06]的信息安全声明的一致性。

9.4.3 工作成果

[WP-09-02]由[RQ-09-03]和[RQ-09-04]得出的 TARA。

[WP-09-03]由[RQ-09-05]得出的信息安全目标。

[WP-09-04]由[RQ-09-06]得出的信息安全声明。

[WP-09-05]由[RQ-09-07]得出的信息安全目标的验证报告。

9.5 信息安全概念

9.5.1 输入

9.5.1.1 先决条件

应提供以下信息：

——相关项定义[WP-09-01]；

——信息安全目标[WP-09-03]；

——信息安全声明[WP-09-04]。

9.5.1.2 支持信息

可考虑以下信息：

威胁分析和风险评估[WP-09-02]。

9.5.2 要求和建议

[RQ-09-08]应考虑以下因素，描述达成信息安全目标而采取的技术上、运营上的信息安全控制措施，及其相互关系：

a) 相关项功能的依赖性；

b) 信息安全声明。

注 1：描述可能包括：

——达成信息安全目标的条件。例如：对损害的预防、探测与监控；

——处理威胁场景特定方面的专用功能。例如：使用安全的通信通道。

注 2：这些描述能用来评估设计，并确定信息安全确认的目标。

[RQ-09-09]应按照[RQ-09-08]的描述，为信息安全目标定义相关项的信息安全需求及操作环境的信息安全需求。

注 3：信息安全需求可能取决于相关项的特定功能。例如：升级能力或在运营时获得用户许可的能力。

注 4：对操作环境的需求，是在相关项以外实现的，但是被包括在相关项的信息安全确认内，以确定相应的信息安全目标是否达成。

注 5：对于作为操作环境一部分的其他相关项的需求，可能作为这些相关项的信息安全需求。

[RQ-09-10]信息安全需求应被分配到相关项。如果适用，分配到一个或者多个组件。

注 6：信息安全控制的描述补充了信息安全需求和操作环境需求的规范和分配，这些都构成了信息安全概念。

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

a) 完整性、正确性及其与信息安全目标的一致性；

b) 与信息安全声明的一致性。

9.5.3 工作成果

[WP-09-06]由[RQ-09-08]、[RQ-09-09]和[RQ-09-10]得出的信息安全概念。

[WP-09-07]由[RQ-09-11]得出的信息安全概念验证报告。

10 产品研发

10.1 总则

本章描述了信息安全需求和架构设计的规范，以及集成与验证活动(见 10.4.1)。

这些信息安全活动需迭代执行，直到信息安全控制不需要进一步细化(见 10.4.2)。需要定义信息安全规范并通过验证活动，确认是否实现信息安全概念。为实现信息安全概念，需要通过验证活动定义并通过验证活动确认信息安全规范。

图 8 阐明了基于 V 模型的工作流程中，如何进行产品研发活动的示例。10.4.1 对应 V 模型的左侧，10.4.2 对应 V 模型的右侧。在此示例中，相关项层面下，假定了两个抽象层，即组件级和子组件级。本工作流程可被扩展以覆盖所有抽象层。

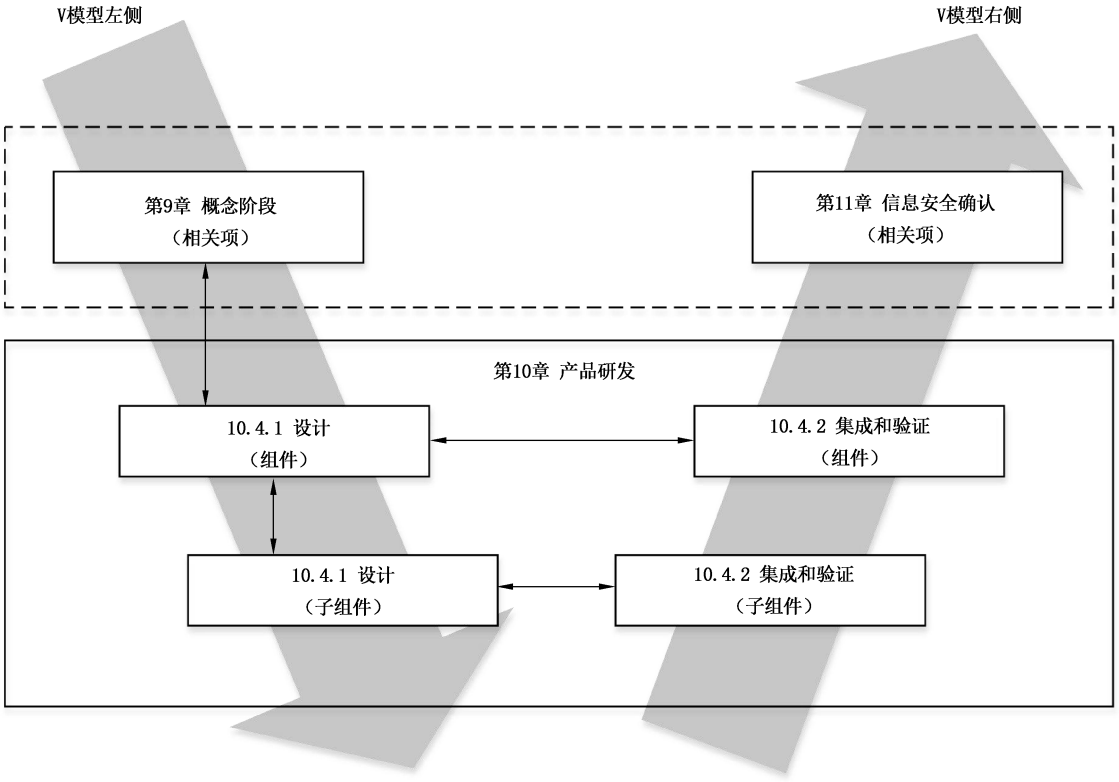


图 8　模型中的产品开发示例

纵向双向箭头指明，按照 10.4.1 的描述，在设计过程中，对于更高层级的抽象架构，针对信息安全规范进行的验证。

横向双向箭头指明，按照 10.4.2 的描述，对于已执行并已集成的组件，针对信息安全规范进行的验证。

可应用不同于 V 模型的开发方法，例如：敏捷软件开发。

可按照 CAL 调节本章活动的深度和严格程度，以及使用的方法（见附录 E）。

10.2　目的

本章的目的是：

a）　定义信息安全规范；

注 1：这些可能包括现有架构设计中不存在的信息安全相关组件的规范。

b）　验证定义的信息安全规范是否符合更高级别的抽象架构的信息安全规范；

c）　识别组件的弱点；

注 2：漏洞分析与管理的描述见第 8 章。

d）　提供证据证明组件的实施和集成结果符合信息安全规范。

10.3　输入

10.3.1　先决条件

应提供以下信息：

更高层级抽象架构的信息安全规范［WP-10-01］。

注 1：仅限于与正在开发的组件相关的信息，例如：

——分配给正在开发的组件的信息安全需求；

——正在开发的组件的外部接口规范；

——关于正在开发的组件的操作环境的假设信息。

注 2：对于最高层级抽象架构的开发，使用相关项的信息安全概念[WP-09-06]和相关项定义[WP-09-01]，而不是更高层级抽象架构的信息安全规范。

10.3.2 支持信息

可考虑以下信息：

——相关项定义[WP-09-01]；

——信息安全概念[WP-09-06]；

——现有架构设计；

——已建立的信息安全控制；

——复用件中已知的弱点和漏洞。

10.4 要求和建议

10.4.1 设计

[RQ-10-01]应基于以下信息制定信息安全规范：

a) 更高层级抽象架构的信息安全规范；

b) 如果适用，选择实施的信息安全控制；

示例 1：使用带有嵌入式硬件信任锚的单独微控制器来实现安全密钥存储功能，并隔离与非安全外部连接相关的信任锚。

注 1：从受信任目录中选择信息安全控制。

c) 如果适用，现有的架构设计。

注 2：信息安全规范覆盖定义的架构设计中的子组件之间的接口规范，包括其使用、静态和动态方面，这些架构设计和满足定义的信息安全需求相关。

注 3：在定义信息安全规范时，可能考虑后开发阶段的信息安全影响，如密钥库的安全管理、停用调试接口、删除个人身份信息的程序。

注 4：信息安全规范可能包括识别满足信息安全需求相关的配置和校准参数，以及它们的设置或允许的范围值。例如：集成硬件安全模块的正确配置。

注 5：可能考虑实施信息安全控制所需组件的能力。例如：处理器性能、内存资源。

[RQ-10-02]定义的信息安全需求应分配给架构设计的组件。

[RQ-10-03]如果适用，应制定在组件开发完成后确保信息安全的程序。

示例 2：正确集成和启动信息安全控制的程序，以及在整个生产过程中维护信息安全的程序。

[RQ-10-04]如果信息安全规范或实施中使用设计、建模或编程符号或语言，则在选择此类符号或语言时应考虑以下内容：

a) 一个在语法和语义上都清晰易懂的定义；

b) 支持实现模块化、抽象和封装；

c) 支持使用结构化构造；

d) 支持使用安全的设计和实现技术；

e) 能够集成现有组件；

示例 3：用另一种语言编写的库、框架、软件组件。

f) 针对由于语言使用不当而导致的漏洞，语言的恢复能力。

示例 4：对缓冲区溢出的恢复能力。

注 6：对于软件开发，实现包括使用编程语言进行编码。

[RQ-10-05]如果语言本身并未涉及适用于信息安全的设计、建模或编程语言的标准(见[RQ-10-04])，则标准应包含在设计、建模和编码指南或开发环境中。

示例 5：在 C 语言中使用 MISRA C:2012 或 CERTC 进行安全编码。

示例 6：适用于设计、建模和编程语言的标准：

——语言子集的使用；

——强类型的强制执行；

——使用防御性实现技术。

[RC-10-06]宜采用已确立且可信的设计和实施原则，以避免或尽量减少引入弱点。

注 7：NIST 特别出版物 800-160 第 1 卷 F.1 中给出了信息安全架构设计的设计原则示例。

[RQ-10-07]应分析[RQ-10-01]中定义的架构设计以识别弱点。

注 8：可能考虑来自复用件的已知弱点和漏洞。

注 9：对已识别的弱点进行漏洞分析(见 8.5)并管理识别的漏洞(见 8.6)。但是，可能通过更改架构设计来解决已识别的弱点，而无需执行漏洞分析。

[RQ-10-08]应验证定义的信息安全规范以确保完整性、正确性以及与更高层级抽象架构的信息安全规范的一致性。

注 10：验证方法可能包括：

——评审；

——分析；

——模拟；

——原型法。

10.4.2 集成和验证

[RQ-10-09]集成和验证活动应验证组件的执行和集成符合定义的信息安全规范。

[RQ-10-10]制定[RQ-10-09]的集成和验证活动应考虑：

a) 定义的信息安全规范；

b) 如果适用，用于批量生产的配置；

c) 足够的能力来支持定义的信息安全规范中指定的功能；

d) 如果适用，符合[RQ-10-05]的建模、设计和编码指南。

注 1：可能包括车辆的集成和测试。

注 2：验证方法可能包括：

——基于需求的测试；

——接口测试；

——资源使用评估；

——控制流和数据流的测试；

——动态分析；

——静态分析。

注 3：如果采用测试进行验证，选择测试用例和测试环境可能考虑：

——实现验证目标的集成测试级别；

——基于对所选测试环境的分析，在后续集成活动中需要额外的测试。例如：由于与处理器仿真或开发环境相比，用于最终集成的目标处理器的数据字和地址字的位宽不同。

注 4：派生测试用例的方法可能包括：

——对需求的分析；

——等价类的生成与分析；

——临界值的分析；

——基于知识或经验的错误猜测。

[RQ-10-11]如果采用测试进行验证，应使用定义的测试覆盖率度量标准来评估测试覆盖率，以确定测试活动的充分性。

注 5：标准测试覆盖率度量可能不足以应对信息安全。例如：软件的语句覆盖率。

[RC-10-12]应执行测试以确认组件中剩余的未识别弱点和漏洞已最小化。

注 6：非必需的功能可能包含一个弱点。

注 7：测试方法可能包括：

——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漏洞分析(见 8.5)并管理已识别的漏洞(见 8.6)。然而，已识别的弱点可能通过更改架构设计来解决，而无需执行漏洞分析。

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

注 9：理由包括以下因素：

——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危害；

——组件的简单性。

10.5 工作成果

[WP-10-01]由[RQ-10-01]到[RQ-10-02]得出的信息安全规范。

[WP-10-02]由[RQ-10-03]得出的后开发阶段的信息安全需求。

[WP-10-03]如果适用，由[RQ-10-04]和[RQ-10-05]得出的建模、设计或编程语言和编码指南的文件。

[WP-10-04]由[RQ-10-08]得出的信息安全规范的验证报告。

[WP-10-05]如果适用，由[RQ-10-07]到[RC-10-12]得出的产品开发过程中发现的弱点。

[WP-10-06]由[RQ-10-10]得出的集成和验证规范。

[WP-10-07]由[RQ-10-09]、[RQ-10-11]、[RC-10-12]得出的集成和验证报告。

11 信息安全确认

11.1 总则

本章描述了在整车级别对该相关项进行信息安全确认的活动(见图 8)。考虑该相关项在整车级别中的操作环境以及用于批量生产的配置。

11.2 目的

本章的目的是：

a) 确认信息安全目标和信息安全声明；

b) 确定该相关项实现的信息安全目标；

c) 确定不存在不合理的风险。

11.3 输入

11.3.1 先决条件

应提供以下信息：

——相关项定义[WP-09-01]；

——信息安全目标 [WP-09-03]；

——如果适用，信息安全声明[WP-09-04]。

11.3.2 支持信息

可提供以下信息：

——信息安全概念[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]考虑量产配置状态下，相关项在整车级别的确认活动中应确认：

a) 在威胁场景和相关风险方面的信息安全目标充分性；

注 1：如果在确认过程中发现有任何风险未被信息安全目标解决，则可能按照 9.4 解决。

b) 实现该相关项的信息安全目标；

c) 信息安全声明的有效性；

d) 如果适用，操作环境要求的有效性。

注 2：确认活动可包括：

——通过审查 9.5 和第 10 章的工作成果确认信息安全目标的实现；

——执行渗透测试验证信息安全目标的充分性和得到实现；

——审查通过第 9 章和第 10 章的所有已识别管理风险。

注 3：使用 CAL 能够扩展渗透测试的深度和严谨度(见附录 E)。

注 4：在[RQ-11-01]的确认活动期间，对已识别弱点进行漏洞分析(见 8.5)并管理已识别的漏洞(见 8.6)。

[RQ-11-02]应提供选择确认活动的理由。

11.5 工作成果

[WP-11-01]由[RQ-11-01]和[RQ-11-02]得出的确认报告。

12 生产

12.1 总则

生产涵盖了相关项或组件及其整车级的制造、装配。制定生产控制计划是为了确保针对相关项或组件在后开发阶段的信息安全需求能够被落实，并确保生产过程不会引入漏洞。

12.2 目的

本章的目的是：

a) 落实后开发阶段的信息安全需求；

b) 防止在生产过程中引入新的漏洞。

12.3 输入

12.3.1 先决条件

应提供以下信息：

——已发布的后开发阶段报告(见[WP-06-04])；

——后开发阶段的信息安全需求(见[WP-10-02])。

12.3.2 支持信息

无。

12.4 要求和建议

[RQ-12-01]应制定生产控制计划，以满足后开发阶段的信息安全需求。

注 1：生产控制计划可作为总体生产计划的一部分。

[RQ-12-02]生产控制计划应包括：

a) 应用后开发阶段信息安全需求的一系列步骤；

b) 生产工具和装备；

c) 在生产阶段防止未授权改动的信息安全控制；

示例 1：防止对运行软件的生产服务器进行物理访问的物理控制。

示例 2：运用密码学技术、访问控制的逻辑控制。

d) 确认满足后开发阶段信息安全需求的方法。

注 2：方法包括检查和校准检查。

注 3：制造相关项或组件和安装软件或硬件时，生产过程可能使用特权访问；如果在生产阶段之后以未授权的方式访问，可能会在相关项或组件中引入漏洞。

[RQ-12-03]应实施生产控制计划。

12.5 工作成果

[WP-12-01]由[RQ-12-01]和[RQ-12-02]得出的生产控制计划。

13 运营和维护

13.1 总则

本章描述了信息安全事件响应(见 13.3)和对既定领域的相关项或组件的更新(见 13.4)。

当一个组织将信息安全事件响应作为漏洞管理的一部分来调用时，就会发生信息安全事件响应(见 8.6)。

更新是在开发后对一个相关项或组件所做的改变，可包括额外的信息，如技术规范、集成手册、用户手册。组织可出于各种原因发布更新信息，例如：解决漏洞或安全问题，提供功能改进。有关更新的工作成果被记录为其他章的工作成果。

处于概念、产品开发或生产阶段的相关项或组件的修改，由变更管理进行规定，不属于本章范围。

13.2 目的

本章的目的是：

a) 确定并实施信息安全事件的补救措施；

b) 从生产后直到信息安全支持结束期间，对于相关项或组件在更新时和更新后进行信息安全的维护。

13.3 信息安全事件响应

13.3.1 输入

13.3.1.1 先决条件

无。

13.3.1.2 支持信息

可考虑以下信息：

——与引起信息安全事件响应的漏洞有关的信息安全情报；

——漏洞分析报告[WP-08-05]。

13.3.2 要求和建议

[RQ-13-01]对于每个信息安全事件，应制定信息安全事件响应计划，包括：

a) 补救措施；

注 1：补救措施由 8.6 中的漏洞管理来决定。

b) 沟通计划；

注 2：沟通计划的建立可能涉及内部各相关方。例如：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：沟通计划可能包括确定内部和外部的沟通伙伴（例如：开发、研究人员、公众、管理机构），并为这些群体共享具体信息。

c) 为补救措施分配责任；

注 4：负责的人应有：

——与受影响的相关项或组件相关的专业知识，包括遗留的相关项和组件；

——组织知识（例如：业务流程、沟通、采购、法律）；

——决定权。

d) 记录与信息安全事件有关的新信息安全情报的程序；

注 5：能根据 8.3 收集新的信息安全情报。例如以下信息：

——受影响的组件；

——相关的事件和漏洞；

——佐证数据，例如数据日志、碰撞传感器数据；

——终端用户投诉。

e) 确定进度的方法；

示例：衡量进度的方法如下：

——受影响的相关项或组件被修复的百分比；

——受补救措施影响的相关项或组件的百分比。

f) 关闭信息安全事件响应的标准；

g) 关闭操作。

[RQ-13-02]应执行信息安全事件响应计划。

13.3.3 工作成果

[WP-13-01]由[RQ-13-01]得出的信息安全事件响应计划。

13.4 更新

13.4.1 输入

13.4.1.1 先决条件

应提供以下信息：
发布的后开发阶段报告[WP-06-04]。

13.4.1.2 支持信息

可考虑以下信息：
——信息安全事件响应计划[WP-13-01]；
——与更新相关的后开发阶段的信息安全需求[WP-10-02]。

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 信息安全支持终止和报废

14.1 总则

报废与信息安全支持的终止是不同的。组织可终止对一个相关项或组件的信息安全支持，但该相关项或组件仍然可在实地中按设计运行。报废和信息安全支持的终止都会带来信息安全方面的影响，但这些影响要分开考虑。

报废可在组织不知情的情况下发生，在这种情况下报废程序无法被组织强制执行，因此报废行为不属于本文件的范围。

报废可能在组织不知情的情况下发生，也可能未按程序执行，因此此类报废行为不属于本文件的范围。

信息安全支持终止和报废应在概念和产品开发阶段中考虑。

14.2 目的

本章的目的是：

a) 信息安全支持终止的沟通；
b) 使与信息安全相关的相关项和组件能够报废。

14.3 信息安全支持终止

14.3.1 输入

无。

14.3.2 要求和建议

[RQ-14-01]应建立一个程序，以便在组织决定对某一相关项或组件终止信息安全支持时与客户沟通。

注 1：这些沟通可能根据供应商和客户之间的合同要求进行处理。

注 2：可能通过公告的方式向客户传达信息。

14.3.3 工作成果

[WP-14-01]由[RQ-14-01]得出的信息安全支持终止沟通程序。

14.4 报废

14.4.1 输入

14.4.1.1 先决条件

应提供以下信息：

后开发阶段的信息安全需求[WP-10-02]。

14.4.1.2 支持信息

无。

14.4.2 要求和建议

[RQ-14-02]应提供后开发阶段有关报废的信息安全需求。

注：与此类需求相关的适当文件(例如：操作说明、用户手册)，能用于在报废过程中实现信息安全。

14.4.3 工作成果

无。

15 威胁分析和风险评估方法

15.1 总则

本章描述了判定威胁场景对道路使用者影响程度的方法。这些方法及其工作成果从受影响的道路使用者角度进行开展，统称为 TARA，从受影响的道路使用者角度执行。本章中定义的方法是通用模块，可在相关项或组件的生命周期中任何节点进行系统地调用：

——资产识别(见 15.3)；

——威胁场景识别(见 15.4)；

——影响评级(见 15.5)；

——攻击路径分析(见 15.6)；

——攻击可行性评级(见 15.7)；

——风险值计算(见 15.8)；

——风险处置决策(见 15.9)。

由于这些是通用模块，所以在此阶段中定义的工作成果记录在其他章节工作成果中。附录 H 提供了示例说明。组织可应用用于影响评级、攻击可行性评级和风险值计算的特定等级，并映射到本文件中

定义的相应等级。

15.2 目的

本章的目的是：

a) 识别资产、资产的信息安全属性和资产的危害场景；
b) 识别威胁场景；
c) 计算危害场景的影响等级；
d) 识别实现威胁场景的攻击路径；
e) 确定攻击路径可被利用的容易程度；
f) 计算威胁场景的风险值；
g) 对威胁场景选择合适的风险处置方案。

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：

相关项定义[WP-09-01]。

15.3.1.2 支持信息

可考虑以下信息：

信息安全规范[WP-10-01]。

15.3.2 要求和建议

[RQ-15-01]应识别危害场景。

注 1：危害场景包含：

——相关项的功能与不良后果之间的关系；
——对道路使用者的危害说明；
——相关资产。

[RQ-15-02]应识别因信息安全属性被破坏而导致危害场景的资产。

注 2：识别资产可能基于：

——分析相关项定义；
——执行影响评级；
——从威胁场景中提取资产；
——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)，该资产的信息安全属性为保密性。危害场景是由于该资产失去保密性，在未经客户同意的情况下，披露客户个人信息。

示例 2：资产是制动功能的通信数据，该资产的信息安全属性是完整性。危害场景是车辆高速行驶时，因非预期的全力制动而与跟随车辆发生碰撞(追尾碰撞)。

15.3.3 工作成果

[WP-15-01]由[RQ-15-01]得出的危害场景。

[WP-15-02]由[RQ-15-02]得出的具有信息安全属性的资产。

15.4 威胁场景识别

15.4.1 输入

15.4.1.1 先决条件

应提供以下信息：

相关项定义[WP-09-01]。

15.4.1.2 支持信息

可考虑以下信息：

——信息安全规范[WP-10-01]；

——危害场景[WP-15-01]；

——具有信息安全属性的资产[WP-15-02]。

15.4.2 要求和建议

[RQ-15-03]应识别威胁场景，威胁场景包含：

——目标资产；

——资产被破坏的信息安全属性；

——信息安全属性被破坏的原因。

注 1：进一步的信息能被威胁场景包含或与威胁场景关联。例如：危害场景与资产、攻击者、攻击方法、攻击工具及攻击面之间的依赖关系。

注 2：威胁场景识别方法可能使用小组讨论、系统方法。例如：

——引发由合理可预见的误用或滥用导致的恶意案例；

——基于 EVITA、TVRA、PASTA、STRIDE(欺骗、篡改、否认、信息披露、拒绝服务、提升特权)等框架的威胁建模方法。

注 3：一个危害场景能对应多个威胁场景，一个威胁场景能导致多个危害场景。

示例：从制动 ECU 方面分析，CAN 消息欺骗会导致 CAN 消息的完整性缺失，从而导致制动功能的完整性缺失。

15.4.3 工作成果

[WP-15-03]由[RQ-15-03]得出的威胁场景。

15.5 影响评级

15.5.1 输入

15.5.1.1 先决条件

应提供以下信息：

危害场景[WP-15-01]。

15.5.1.2 支持信息

可考虑以下信息：

——相关项定义[WP-09-01]；

——具有信息安全属性的资产[WP-15-02]。

15.5.2 要求和建议

[RQ-15-04]根据对道路使用者的潜在不利影响，分别从安全、财务、操作和隐私(S、F、O、P)的影响类别对危害场景进行评估。

注 1：本文件不提供不同影响类别之间的关系(例如：权重)。

注 2：也能考虑其他影响类别。

注 3：如果考虑其他影响类别，则根据第 7 章在供应链中分享这些类别的基本原理和解释。

[RQ-15-05]应确定每个危害场景的影响等级，每个影响类别应为以下影响等级之一：

——严重；

——重大；

——中等；

——忽略。

注 4：财务、操作和隐私相关影响根据附录 F 中提供的表格进行评级。

[RQ-15-06]与安全相关的影响等级应来自 GB/T 34590.3—2022 中 6.4.3 规定的内容。

注 5：附录 F 中的表 F.1 能用于将安全影响准则映射到影响等级。

注 6：功能安全评估能为此目的重复使用。

[PM-15-07]若一个危害场景导致了一个影响等级，并且其他影响类别的影响可被认为是不那么关键的，那么可省略对其他影响类别的进一步分析。

示例：危害场景的安全影响被评定为“严重”，因此，该危害场景的财务影响可不用进一步分析。

15.5.3 工作成果

[WP-15-04]由[RQ-15-04]至[RQ-15-06]得出的相关影响类别的影响等级。

15.6 攻击路径分析

15.6.1 输入

15.6.1.1 先决条件

应提供以下信息：

——相关项定义[WP-09-01]或信息安全规范[WP-10-01]；

注：如果对相关项执行攻击路径分析，则使用相关项定义；如果对组件执行攻击路径分析，则使用信息安全规范。

——威胁场景[WP-15-03]。

15.6.1.2 支持信息

可考虑以下信息：

——信息安全事态的弱点[WP-08-04]；

——产品开发过程中发现的弱点[WP-10-05]；

——架构设计；

——如果适用，前期已识别的攻击路径[WP-15-05]；

——漏洞分析[WP-08-05]。

15.6.2 要求和建议

[RQ-15-08]应分析威胁场景从而识别攻击路径。

注 1：攻击路径分析可能基于：

——自上而下的方法：通过分析实现威胁场景的不同方式（例如：攻击树、攻击图）来推断攻击路径；

——自下而上的方法：通过已识别的漏洞构建攻击路径。

注 2：如果部分攻击路径不会导致威胁场景的实现，则可能停止对该部分攻击路径的分析。

[RQ-15-09]应把攻击路径和可由该攻击路径所实现的威胁场景进行关联。

注 3：在产品开发的早期阶段，由于具体的实施细节尚不清楚，攻击路径通常不完整或不精确，无法识别具体的漏洞。在产品开发过程中，攻击路径可能随着更多信息的可用而更新，例如在漏洞分析之后。

示例：

——威胁场景：欺骗制动 ECU 的 CAN 消息，导致 CAN 消息的完整性缺失，从而导致制动功能的完整性缺失。

——实现上述威胁场景的攻击路径：

1） 利用蜂窝接口损害远程通信 ECU；

2） 利用远程通信 ECU 的 CAN 通信损害网关 ECU；

3） 网关 ECU 转发恶意制动请求信号（非预期的快速减速）。

15.6.3 工作成果

[WP-16-05]由[RQ-16-08]和[RQ-16-09]得出的攻击路径。

15.7 攻击可行性评级

15.7.1 输入

15.7.1.1 先决条件

应提供以下信息：

攻击路径[WP-15-05]。

15.7.1.2 支持信息

可考虑以下信息：

——架构设计；

——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，应按表 1 所述确定攻击可行性等级。

表 1 攻击可行性等级和相应描述

攻击可行性等级	描述
高	攻击路径可用低工作量完成
中	攻击路径可通过中等工作量完成
低	攻击路径可用高工作量完成
非常低	攻击路径可用非常高的工作量来完成

[RC-15-11]攻击可行性评级方法宜根据以下方法之一确定：

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：方法的选择取决于产品生命周期中的阶段和可用信息。

[RC-15-12]如果使用基于攻击潜力的方法，则宜根据核心要素确定攻击可行性等级，包括：

a) 操作时间；

b) 专业知识；

c) 相关项或组件的知识；

d) 机会窗口；

e) 设备。

注 2：核心攻击潜在因素能从 ISO/IEC 18045 中得出。

注 3：G.2 提供了基于攻击潜力来确定攻击可行性等级的指南。

[RC-15-13]如果使用基于 CVSS 的方法，则应根据基本度量组的可利用性度量确定攻击可行性等级，包括：

a) 攻击矢量；

b) 攻击复杂性；

c) 所需特权；

d) 用户交互，

注 4：G.3 提供基于 CVSS 来确定攻击可行性等级的指南。

[RC-15-14]如果使用基于攻击向量的方法，则宜根据评估攻击路径的主要攻击向量确定攻击可行性等级。

注 5：G.4 提供了基于攻击向量来确定攻击可行性等级的指南。

注 6：在开发的早期阶段(例如：概念阶段)，当没有足够的信息来识别特定的攻击路径时，基于攻击向量的方法适用于评估攻击的可行性等级。

15.7.3 工作成果

[WP-15-06]由[RQ-15-10]得出的攻击可行性等级。

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：

——威胁场景[WP-15-03]；

——相关影响类别的影响等级[WP-15-04]；

——攻击可行性等级[WP-15-06]。

15.8.1.2 支持信息

无。

15.8.2 要求和建议

[RQ-15-15]对于每个威胁场景，应根据危害场景的影响等级和攻击路径的攻击可行性等级计算风险值。

注 1：如果一个威胁场景对应于多个危害场景或一个危害场景具有多个影响类别的影响，则可能为每个影响等级分

别确定单独的风险值。

注 2：如果一个威胁场景对应于多条攻击路径，则可能适当聚合相关的攻击可行性评级。例如：某威胁场景被分配了相应攻击路径中的最大攻击可行性等级。

[RQ-15-16]威胁场景的风险值应介于(包括)1 和 5 之间。其中，值 1 表示最小风险。

示例：风险值计算方法：

——风险矩阵；

——风险计算公式。

15.8.3 工作成果

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

15.9 风险处置决策

15.9.1 输入

15.9.1.1 先决条件

应提供以下信息：

——相关项定义[WP-09-01]；

——威胁场景[WP-15-03]；

——风险值[WP-15-07]。

15.9.1.2 支持信息

可考虑以下信息：

——信息安全规范[WP-10-01]；

——相关项或组件或类似相关项或组件的先前风险处置决策；

——影响类别的影响等级[WP-15-04]；

——攻击路径[WP-15-05]；

——攻击可行性等级[WP-15-06]。

15.9.2 要求和建议

[RQ-15-17]对于每个威胁场景，考虑到威胁场景的风险值，应确定以下一种或多种风险处置决策：

a) 避免风险；

示例 1：消除风险源，决定不开始或停止会产生风险的活动。

b) 降低风险；

c) 分担风险；

示例 2：通过合同分担风险或通过购买保险转移风险。

d) 保留风险。

注：保留风险和分担风险的理由记录为信息安全声明，并根据第 8 章进行信息安全监测和漏洞管理。

15.9.3 工作成果

[WP-15-08]由[RQ-15-17]得出的风险处置决策。

附 录 A
（资料性）
信息安全活动和工作成果摘要

A.1 综述

表 A.1 提供了信息安全活动及其相应工作成果的摘要。这可帮助组织管理这些活动，确保信息安全活动的覆盖面，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信息安全计划中确定的。因此，这些活动的工作成果都在信息安全评估的范围内。第 15 章列出的所有工作成果在其他章节中被记录为工作成果。

A.2 信息安全活动和工作成果摘要

表 A.1 本文件的信息安全活动和工作成果

子章	工作成果
组织的信息安全管理	
5.4.1 信息安全治理	[WP-05-01]信息安全方针、规则和过程
5.4.2 信息安全文化	[WP-05-01]信息安全方针、规则和过程 [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]信息安全方针、规则和程序
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]工具管理的证据
5.4.6 信息安全管理	[WP-05-03]组织管理体系的证据
5.4.7 组织层面的信息安全审核	[WP-05-05]组织层面的信息安全审核报告
项目相关的信息安全管理	
6.4.1 信息安全职责及其分配	[WP-06-01]信息安全计划
6.4.2 信息安全计划	[WP-06-01]信息安全计划
6.4.3 裁剪	[WP-06-01]信息安全计划
6.4.4 复用	[WP-06-01]信息安全计划
6.4.5 独立于环境的组件	[WP-06-01]信息安全计划
6.4.6 现成组件	[WP-06-01]信息安全计划
6.4.7 信息安全档案	[WP-06-02]信息安全档案
6.4.8 信息安全评估	[WP-06-03]信息安全评估报告
6.4.9 后开发的发布	[WP-06-04]后开发阶段的发布报告

表 A.1　本文件的信息安全活动和工作成果（续）

子章	工作成果
分布式信息安全活动	
7.4.1 供应商的能力	无
7.4.2 询价	无
7.4.3 职责的协调	[WP-07-01]信息安全接口协议
持续的信息安全活动	
8.3 信息安全监测	[WP-08-01]信息安全情报来源 [WP-08-02]触发器 [WP-08-03]信息安全事态
8.4 信息安全事态评估	[WP-08-04]来自信息安全事态的弱点
8.5 漏洞分析	[WP-08-05]漏洞分析的结果
8.6 漏洞管理	[WP-08-06]漏洞管理证据
概念阶段	
9.3 相关项定义	[WP-09-01]相关项定义
9.4 信息安全目标	[WP-09-02]TARA [WP-09-03]信息安全目标 [WP-09-04]信息安全声明 [WP-09-05]信息安全目标的验证报告
9.5 信息安全概念	[WP-09-06]信息安全概念 [WP-09-07]信息安全概念的验证报告
产品开发阶段	
10.4.1 设计	[WP-10-01]信息安全规范 [WP-10-02]开发后的信息安全需求 [WP-10-03]建模、设计或编程语言和编码指南的文件 [WP-10-04]信息安全规范的验证报告 [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
11 信息安全确认	[WP-11-01]确认报告
后开发阶段	
12 生产	[WP-12-01]生产控制计划

表 A.1　本文件的信息安全活动和工作成果（续）

子章	工作成果
13.3 信息安全事件响应	[WP-13-01]信息安全事件响应计划
13.4 更新	无
14.3 信息安全支持终止	[WP-14-01]信息安全支持终止沟通程序
14.4 报废	无
威胁分析和风险评估方法	
15.3 资产识别	[WP-15-01]危害场景 [WP-15-02]具有信息安全属性的资产
15.4 威胁场景识别	[WP-15-03]威胁场景
15.5 影响评级	[WP-15-04]相关影响类别的影响等级
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]攻击可行性等级
15.8 风险值确定	[WP-15-07]风险值
15.9 风险处置决策	[WP-15-08]风险处置决策

附 录 B
（资料性）
信息安全文化示例

表 B.1 提供了一个薄弱的信息安全文化示例和强大的信息安全文化示例。

表 B.1 薄弱的和强大的信息安全文化示例

表明信息安全文化薄弱的示例	表明信息安全文化强大的示例
与信息安全相关的决策责任不可追溯	有过程确保信息安全的决策责任是可追溯的
性能（所实施的功能或特性）、成本或进度优先于信息安全	信息安全和功能安全具有最高优先权
相较于信息安全，奖励制度更偏向于成本和进度	奖励制度支持和鼓励有效实现信息安全，并处罚因走捷径而危害信息安全的人
信息安全人员强制对信息安全进行不适用的、非常严格的遵守，而不考虑项目/活动的特殊需求	信息安全人员以身作则，以良好的适用性和实际执行力获取整个组织对其行为的信任
评估信息安全及其管理过程受到执行过程人员的不当影响	过程提供了适当的制衡，例如：信息安全评估中适度的独立性
应对信息安全的消极态度，例如： ——严重依赖研发结束时的测试； ——没有为在用车上潜在的弱点或事件做好准备； ——只有当在产车、在用车发生信息安全事件，或当媒体对竞争对手的产品给与大量关注时，管理层才会做出反应	应对信息安全的积极态度，例如： ——在产品生命周期的最初阶段就能发现和解决信息安全问题（设计中的信息安全）； ——组织已准备好对在用车的漏洞和事件做出快速反应
信息安全所需的资源未进行分配	信息安全所需的资源已分配。 技术资源拥有与指定活动相对应的能力
应对信息安全的薄弱现象，例如： ——“群体思维”确认偏差（即不加批判地接受或遵从主流观点）； ——组建审查小组时“暗中布局”（即选择成员以确保预期结果），以防止可能出现的异议； ——排斥提出异议的人或将贴上“没有团队精神”的标签（例如：不合作、不妥协、有害的人）； ——提出异议会对绩效评估产生负面影响； ——少数提出异议的人被视作或被贴上“麻烦制造者”“没有团队精神”或“内部举报者”（即煽动者、不受欢迎者或告密者）的标签； ——员工害怕因为表达担忧而受到影响	过程利用了多样性优势： ——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是被阻止和惩罚的。 存在相应的沟通和决策渠道，并且管理层鼓励使用： ——鼓励自我披露； ——鼓励任何人（内部或外部）负责任的披露潜在的漏洞； ——在用、在产和开发其他产品中持续进行发现和解决过程
没有成体系的持续改进过程、学习周期或者其他形式的经验总结	持续改进是所有过程的必要条件
过程是临时的或不明确的	遵循明确的、可追踪的和可控的过程

附 录 C
（资料性）
信息安全接口协议模板示例

C.1 目的

不同组织在参与分布式信息安全活动时，各组织对相互之间的责任、信息披露程度和每个里程碑的实现程度达成一致很重要。

本附录按照[RQ-07-04]提供了一个信息安全接口协议模板的示例。模板对如何定义在客户和供应商之间的分布式信息安全活动的角色和责任给出了指导。

模板也可加入其他信息，例如联系人、目标里程碑、协作方法和工具等。

C.2 示例模板

本示例模板列项包括：

a) 本文件的阶段；

b) 工作成果：本文件与分布式活动接口相关的工作成果物；

c) 参考章：本文件的相关章节；

d) 供应商：供应商按照责任矩阵 RASIC 所承担的责任；

e) 客户：客户按照 RASIC 所承担的责任；

注 1：模板使用 RASIC 来表示组织之间具体工作成果的责任分配。责任矩阵的使用方法如下：

——R(负责)：对开展活动负责的组织；

——A(批准)：完成后，有权批准活动的组织；

——S(支持)：帮助负责活动组织的组织；

——I(通知)：被告知活动进展和正在做出的所有决定的组织；

——C(咨询)：提供建议或指导但不主动参与活动的组织。

f) 保密等级：供应商和客户就每个工作成果的保密性达成一致；

注 2：可能的保密等级是：

——高度保密：仅允许创建工作成果的组织访问；

——保密：允许客户和供应商访问工作成果；

——第三方受信：根据 5.4.3 规定，允许与被授权的外部各方共享工作成果；

——公开：允许不受任何限制地共享工作成果。

g) 备注：关于各组织之间谈判和讨论结果的补充信息。

表 C.1　信息安全接口协议模板示例

阶段	工作成果	参考章节	供应商					客户					保密等级	备注
			负责	批准	支持	通知	咨询	负责	批准	支持	通知	咨询		
概念	相关项定义													
	威胁分析和风险评估													
	信息安全概念													
	信息安全概念的验证报告													
产品开发	信息安全规范													
……	……													

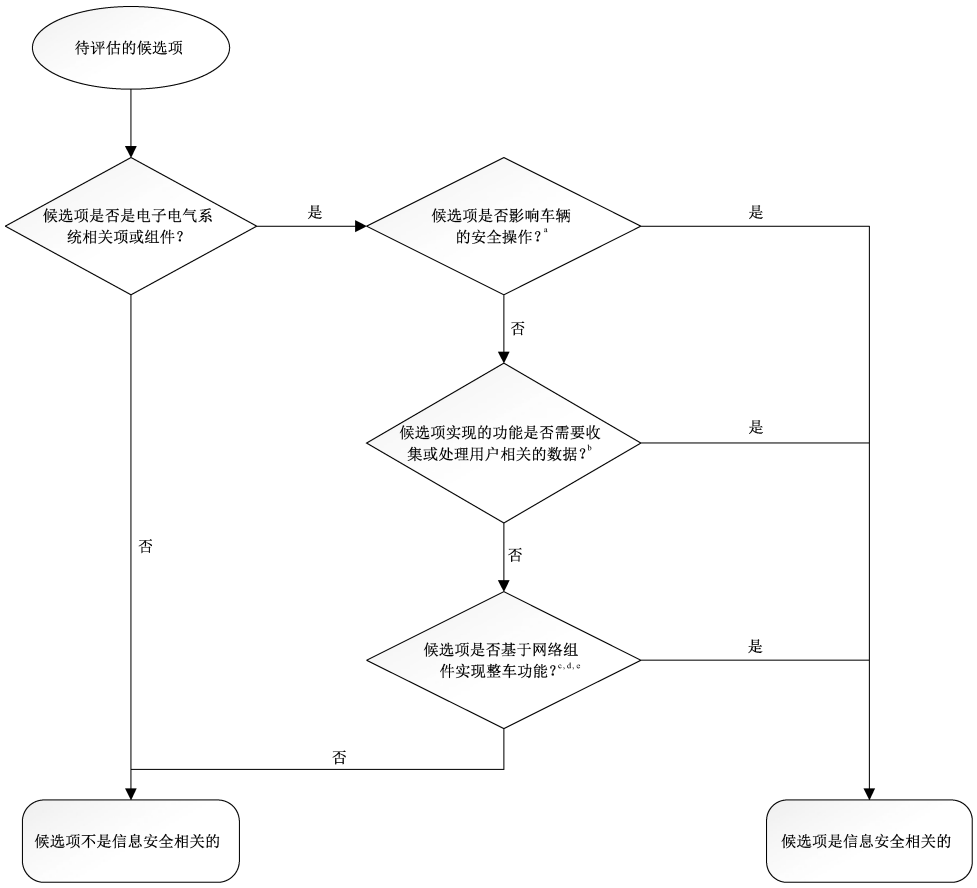
附 录 D
（资料性）
信息安全的相关性——判定方法和准则示例

D.1 目的

本附录提供了确定一个相关项或组件是否与信息安全相关（见[RQ-06-02]）的示例方法。

D.2 方法

通过图 D.1 中的决策图可确定候选相关项或组件的信息安全相关性，图 D.1 给出了示例的判定准则。



[a] 示例：运动控制模块和具有汽车安全完整性等级（ASIL）的模块。

[b] 示例：与驾驶员或乘客有关，或与潜在敏感信息（如位置数据）有关的数据。

[c] 示例：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] 示例：外部连接——与后端服务器的功能接口；蜂窝通信网络、车载自动诊断系统（OBD-II）接口。

[e] 示例：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）、胎压监测系统（TPMS）。

图 D.1 信息安全相关性判定方法

信息安全的相关性也可根据经验和多领域专家的判断来确定。例如：功能安全专家和信息安全专家。

附 录 E
（资料性）
信息安全保障等级

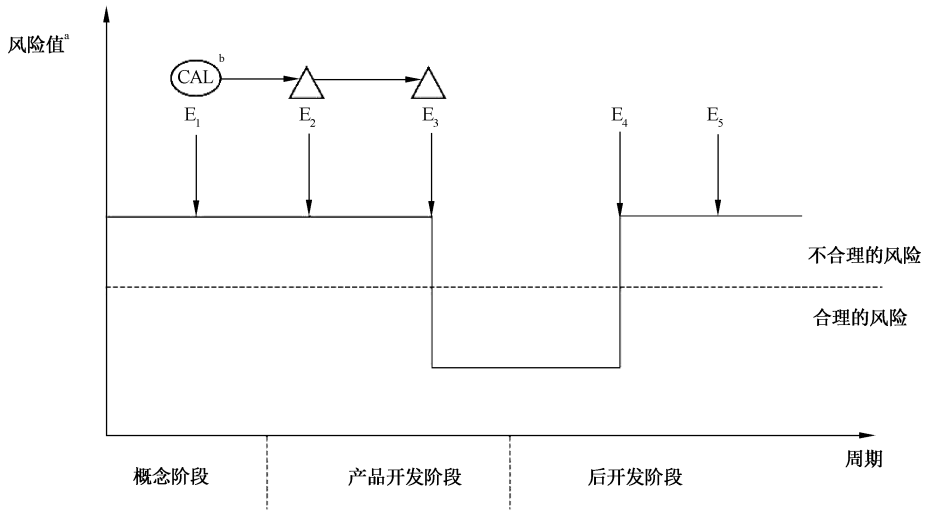
E.1 总则

本附录描述了一个信息安全保障级别（CAL）的分类方案，该方案可用于规定和传达一套保障要求，其严格程度可确保相关项或组件的资产得到充分保护。这个 CAL 分类方案没有规定信息安全控制的技术要求，但是它可用来推动信息安全工程，为相关组织之间交流信息安全保证要求提供一种共同语言。

CAL 可由开发相关项的组织确定，或是由开发独立于环境的组件的组织进行假设。一旦确定，CAL 将指定后续产品开发活动中所需的严格程度，以处理涉及风险的威胁场景。这可通过将 CAL 作为信息安全目标的一个属性来实现，这种属性可被细化的信息安全需求所继承。

E.2 确定一个 CAL

CAL 与风险间接相关，但它不能直接从风险值中确定。因为风险值是动态的，随着时间的推移而变化，取决于相关项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，不会随着时间推移发生变化。因此，在考虑实施信息安全控制之前，可在概念阶段的开发之初使用预计在信息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。



标引说明：

E_1 ——事件 1：信息安全要求被明确；

E_2 ——事件 2：信息安全控制得到实施；

E_3 ——事件 3：测试表明信息安全控制是有效的；

E_4 ——事件 4：在运营阶段发现漏洞；

E_5 ——事件 5：漏洞被修复；

◯ ——CAL 被确定和分配；

△ ——CAL 被应用于信息安全活动中。

[a] 风险值是动态的，可根据当前的规范、设计或实施而变化。

[b] 鉴于需要保护的资产的重要性，在 E_1 确定的预期保证水平规定了 E_2、E_3 的后续信息安全活动的严格程度。

图 E.1 CAL 和风险之间的关系

可根据对已确定的威胁场景的考虑来确定 CAL(见 15.4)。表 E.1 给出了一个基于四个 CAL 的示例，每个 CAL 依次对应着基于所使用的信息安全工程方法的递增的保证水平。该示例展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确定 CAL 的示例

影响	攻击路径[b]			
	物理	本地	近场	网络
十分严重的	CAL2	CAL3	CAL4	CAL4
严重的	CAL1	CAL2	CAL3	CAL4
普通的	CAL1	CAL1	CAL2	CAL3
忽略不计	…[a]	…[a]	…[a]	…[a]

[a] 见[PM-06-08]。

[b] 攻击向量是攻击可行性的一个静态参数。

在客户和供应商之间分享确定 CAL 的书面理由可增进相互理解。CAL 分类方案和确定的 CAL 也可成为客户和供应商之间信息安全接口协议的一部分。

可为一个项目的所有信息安全目标分配一个 CAL，也可为每个信息安全目标分配不同的 CAL。如果信息安全目标被合并，单个 CAL 中的最高值将被分配给合并的信息安全目标。

E.3 使用 CAL

E.3.1 整体考虑

CAL 分类方案可用于确定信息安全活动的严格程度，即提供所需保证的必要要素。

可用 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) 信息安全评估的方法。

表 E.2 提供了一些 CAL 的示例，以及它们在概念和产品开发阶段的使用指南。对于 CAL 值的每一次增加，相应的方法代表了设计、验证和信息安全评估对相关项或组件保证的有意义的增加。表 E.2、表 E.3 和表 E.4 中的示例是为了使行业在使用 CAL 来扩展本标准中描述的活动中获得经验。

表 E.2 CAL 数值和信息安全保障措施中预期严格程度的示例

CAL	描述	a)提供确保信息安全活动以适当的严格度执行的方法	b)提供确保不存在未管理的漏洞的方法	c)独立计划，以确保所开展的信息安全活动是适当的
CAL1	低、中等级信息安全保障	基于需求的测试	通过分析、测试等基于已知信息来发现漏洞的活动	不需要
CAL2	中等级信息安全保障			信息安全评估由非发起人执行
CAL3	中、高等级信息安全保障	组件之间的所有相互作用都经过测试	通过分析、测试等探索性方法来发现漏洞的活动	信息安全评估由与发起人不同的团队中的人进行的
CAL4	高等级信息安全保障	所有组件之间的相互作用组合都经过测试		信息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

本条提供了一个示例，说明如何使用 CAL 分类方案来调整开发方案的严格程度和范围。

在概念阶段，随着信息安全概念的定义以及将信息安全需求分配给初步架构的组成部分，可通过如下方式可作为 CAL 在[RQ-09-10]的延伸：

a) 来自信息安全目标的信息安全要求继承了该信息安全目标的 CAL；

b) 如果从多个信息安全目标继承的具有不同 CAL 的多个信息安全要求被分配给一个架构组件，则将最高的 CAL 分配给该组件；

c) 如果确认该组件受到架构中其他组件的保护，则可根据合理理由减少或放弃不必要的 CAL 使用。

E.3.3 产品开发

CAL 分类方案在产品开发中的应用可是使用依赖 CAL 的方法和度量。

在产品开发中,如果信息安全需求被分配到组件中,并且无法确认是否与其他组件隔离,那么就可按照这些信息安全需求的最高 CAL 来开发组件。

表 E.3 和表 E.4 提供了如何将 CAL 应用于信息安全活动的示例;可用类似的方式处理更多的信息安全活动。

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

表 E.3 信息安全活动的独立程度示例

活动	要求	独立性水平适用[a]				范围
		CAL1	CAL2	CAL3	CAL4	
验证信息安全的概念和设计活动	[RQ-09-11] [RQ-10-08]	I1	I1	I2	I2	适用于信息安全要求中最高的 CAL
验证组件的实施和整合	[RQ-10-09]	I1	I1	I2	I2	
信息安全确认	[RQ-11-01]	I1	I1	I2	I2	
信息安全评估	[RQ-06-27]	—	I1	I2	I3	

[a] 符号定义如下:

—:对这项活动的独立性没有建议;

I1:该活动是由一个不同于负责创建及考虑此工作产品的人来进行的;

I2:该活动是由一个独立于负责创建及考虑此工作产品的团队的人执行的,例如:由一个向不同的直接上级报告的人执行。

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及考虑该工作产品的部门的人执行。

表 E.4 提供了一个示例,以说明如何利用 CAL 值来确定影响用于验证和确认的测试方法严格程度的参数。

表 E.4 测试方法的参数示例

活动	要求	测试参数适用[a]				范围
		CAL1	CAL2	CAL3	CAL4	
功能测试	[RC-10-12] [RQ-11-01]	T1	T1	T2	T2	适用于信息安全需求中最高的 CAL 值
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	

表 E.4　测试方法的参数示例（续）

活动	要求	测试参数适用[a]				范围
		CAL1	CAL2	CAL3	CAL4	

[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、相关项或组件的知识和资源适中。

T2:测试参数设置 2：

——基于需求和组件之间相互作用的功能测试；

——对已知漏洞进行漏洞扫描；

——通过增加测试用例的迭代次数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、相关项或组件的知识或资源更高。

附 录 F
（资料性）
影响评级的准则

F.1 综述

本附录举例说明了影响评级的标准（见 15.5），涉及安全、财务、操作和隐私的损害情况。本附录中的表格（见表 F.1～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示例中，但可酌情添加到具体组织的评级标准中。

F.2 安全损害的影响评级

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
十分严重的	S3：威胁生命的伤害（不确定是否幸存），致命的伤害
严重的	S2：严重的和有生命危险的伤害（可能生存）
普通的	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 GB/T 34590.3—2022 中表 B.1。	

安全影响评级标准取自 GB/T 34590.3—2022。如果提供理由，也可考虑按照 GB/T 34590.3—2022 的可控性和暴露概率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
十分严重的	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
严重的	导致经济上的大量损失，受影响的道路使用者将能够克服这些后果
普通的	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
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 操作影响评级标准示例

影响评级	操作影响评级的标准
十分严重的	操作上的损坏导致了车辆核心功能的丧失或受损 **示例 1**：车辆不工作或出现核心功能的意外行为，例如启用跛行回家模式或自主驾驶到一个非预期的位置。
严重的	操作上的损坏导致了车辆重要功能的丧失或受损 **示例 2**：给驾驶员带来重大困扰。
普通的	操作上的损坏导致了车辆功能的部分退化 **示例 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

这些标准可能会产生安全后果。

F.5 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
十分严重的	隐私损害导致对道路使用者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，很容易与个人可识别信息主体联系起来
严重的	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： 高度敏感且难以与个人可识别信息主体联系起来
普通的	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： a) 敏感但难以与个人可识别信息主体联系起来； b) 不敏感，但很容易与个人可识别信息主体联系起来
可忽略不计	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。有关道路使用者的信息并不敏感，很难与个人可识别信息主体联系起来

个人可识别信息和个人可识别信息主体可根据 ISO/IEC 29100 来定义。

附 录 G
（资料性）
攻击可行性评级指南

G.1 总则

本附录提供了如何使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；

——基于攻击向量。

攻击可行性评级中可包括攻击是否具有扩展潜力（即容易扩展到多个实例和目标）的考虑因素。

G.2 基于攻击潜力的方法指南

G.2.1 攻击潜力的背景

ISO/IEC 18045 将攻击潜力定义为攻击一个相关项或组件所花费的精力的度量，用攻击者的专业知识和资源表示。攻击潜力取决于五个核心参数：

——经历时长；

——专家的专业知识；

——相关项或组件的知识；

——机会窗口；

——设备。

本条给出了自定义示例和攻击可行性示例的映射。

G.2.2 参数适配示例

G.2.2.1 自定义经历时长示例

经历时长参数包括识别漏洞、开发和（成功地）应用漏洞的时间。因此，该等级是基于评级时专家知识的状态，见表 G.1。

表 G.1 经历时长

经历时长
≤1 天
≤1 周
≤1 个月
≤6 个月
>6 个月

G.2.2.2 自定义专家的专业知识示例

专业知识参数与攻击者的能力、技能和经验有关，见表 G.2。

表 G.2　专家的专业知识

专家的专业知识
外行： 与专家或专业人士相比缺乏知识，没有特别的专长 **示例 1**：普通人使用公开的攻击的逐步描述。
精通： 熟悉产品或系统类型的安全行为 **示例 2**：有经验的人员、了解简单和流行攻击（例如：里程表调整、安装假冒零件）的普通技术人员。
专家： 熟悉底层算法、协议、硬件、结构、安全行为、使用的安全原理和概念、定义新攻击的技术和工具、密码学、产品类型的经典攻击、在产品或系统类型中实现的攻击方法等 **示例 3**：有经验的技术人员或工程师。
多名专家： 一个攻击的不同步骤需要专家级别的不同专业知识 **示例 4**：一个攻击的不同步骤需要多名经验丰富的、拥有不同领域专业知识的工程师。

G.2.2.3　相关项或组件的自定义知识示例

相关项或组件的知识参数与攻击者获得的关于相关项或组件的信息的数量有关，见表 G.3。

表 G.3　相关项或组件的知识

相关项或组件的知识
公共信息： 关于该相关项或组件的公共信息。例如：从互联网上获得的 **示例 1**：在产品主页或互联网论坛上发布的信息和文档。
受限制的信息： 关于相关项或组件的受限制的信息。例如：在开发组织内部控制的知识，并在保密协议下与其他组织共享的知识 **示例 2**：制造商和供应商之间共享的内部文档、需求和设计规范。
机密信息： 关于相关项或组件的机密信息。例如：在开发人员组织中的离散团队之间共享的知识，只有特定团队的成员才能访问这些知识 **示例 3**：防盗控制系统相关信息、软件源代码。
严格保密的信息： 关于相关项或组件的严格保密的信息。例如：只有少数人知道的知识，根据严格的知情需要和个人承诺，对这些知识的获取实行严格控制 **示例 4**：由制造商、供应商在内部记录的特定客户的校准或内存映射。

G.2.2.4　自定义机会窗口示例

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（例如：逻辑和物

理)和访问持续时间(例如:无限和有限)。根据攻击的类型,这可能包括:发现可能的目标、访问目标、对目标开展工作、对目标进行攻击的时间、保持未被发现、规避检测和信息安全控制等(见表 G.4)。

表 G.4 机会窗口

机会窗口
无限制: 通过公共/不受信任的网络的高可用性,没有任何时间限制(例如:资产总是可访问的)。对相关项或组件实施没有物理存在或时间限制的远程访问,以及无限制物理访问 **示例 1**:无任何先决条件的远程攻击(例如:车联网或蜂窝接口)、所有者无限制访问芯片调试。
容易: 高可用性和有限的访问时间。对相关项或组件实施没有物理存在的远程访问 **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。
中等: 相关项或组件的可用性低。有限的物理、逻辑访问。不使用任何特殊工具直接进入车辆内部或外部 **示例 3**:攻击者进入一辆未上锁的汽车,访问暴露的物理接口。例如:通过车载诊断端口进行物理访问。
困难: 相关项或组件的可用性非常低。执行攻击需要对相关项或组件实施不切实际的访问 **示例 4**:对集成电路进行解密以提取信息,以比密钥旋转更快的速度暴力破解密钥。

G.2.2.5 自定义设备示例

设备参数与攻击者用来发现漏洞或执行攻击的工具有关,见表 G.5。

表 G.5 设备

设备
标准设备: 攻击者随时可获得设备。该设备可以是产品本身的一部分(例如:操作系统中的调试器),或者很容易获得(例如:网络资源、协议分析器或简单的攻击脚本) **示例 1**:笔记本电脑、CAN 适配器、车载诊断软件保护器、普通工具(例如:螺丝刀、烙铁、钳子)。
专业设备: 攻击者不容易获得设备,但不需要过度的努力就可获得。这可能包括购买适量的设备(例如:电源分析工具、使用数百台联网的个人电脑),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不同的由专门设备组成的测试台,这将被认为是定制设备 **示例 2**:专业硬件调试设备、车载通信设备(例如:环内硬件试验台、高档示波器、信号发生器)、特殊化学品。
定制设备: 设备是专门生产的(例如:非常复杂的软件)、公众不容易获得(例如:黑市)或者设备非常专业,以至于其分销受到控制,甚至可能受到限制。另外,这些设备非常昂贵 **示例 3**:厂家限制的工具、电子显微镜。
多种定制设备: 引入多种定制设备是为了考虑到攻击的不同步骤需要不同类型的定制设备的情况

G.2.2.6 攻击潜力和攻击可行性映射示例

对于每个参数，可定义数值。根据 ISO/IEC 18045，基于上述适配标准，提出以下量表，见表 G.6。

表 G.6 攻击潜力聚合示例

经历时长		专家的专业知识		相关项或组件的知识		机会窗口		设备	
列举	值	列举	值	列举	值	列举	值	列举	值
≤ 1 天	0	外行	0	公共信息	0	无限	0	标准设备	0
≤ 1 周	1	精通	3	受限制的信息	3	容易	1	专业设备	4
≤ 1 个月	4	专家	6	机密信息	7	中等	4	定制设备	7
≤ 6 个月	17	多个专家	8	严格保密的信息	11	困难/没有	10	多种定制设备	9
＞ 6 个月	19								

根据 ISO/IEC 18045，攻击潜力对应于所有参数的相加。基于 ISO/IEC 18045 的自定义，攻击可行性使用表 G.7 映射。

表 G.7 攻击潜力映射示例

攻击可行性评级	数值
高	0～9
	10～13
中	14～19
低	20～24
非常低	≥25

G.3 基于 CVSS 的方法指南

可使用 CVSS 评估信息技术安全的漏洞。在基本度量组中，可利用性度量可用于评估攻击的可行性。其他 CVSS 度量(例如：影响度量)被本文件覆盖，例如：危害场景和影响评估。

可利用性的度量如下：

a) 攻击向量；

b) 攻击复杂性；

c) 权限要求；

d) 用户交互。

CVSS 度量的评估为每一个度量在预定义的范围内生成一个数值。整体可利用性度量值可用一个简单的公式来计算：

$$E = 8.22 \times V \times C \times P \times U \qquad \cdots\cdots\cdots\cdots\cdots\cdots (G.1)$$

式中：

E ——可利用性值；

V ——与攻击向量相关的数值，范围为 0.2～0.85；

C ——与攻击复杂性相关的数值，范围为 0.44～0.77；

P ——与权限要求相关的数值，范围为 0.27～0.85；

U ——与用户交互相关的数值，范围为 0.62～0.85。

因此，可利用性度量值的范围在 0.12 和 3.89 之间。

表 G.8 给出了一个 CVSS 可利用性度量值到攻击可行性映射的示例。这是等距可利用性步骤的示例。

表 G.8 CVSS 可利用性映射示例

攻击可行性评级	CVSS 可利用性度量值
高	2.96～3.89
中	2.00～2.95
低	1.06～1.99
非常低	0.12～1.05

注：仅使用可利用性度量作为更大的 CVSS 基础度量组的一部分并不严格符合 CVSS 对度量的要求。根据本文件计算风险时，缺失的影响度量可能通过本文件的度量指标进行代替，见附录 F。

在不改变可利用性度量值的情况下，可对其描述进行补充，从而更好地指导组织的业务和正在开发的相关项或组件，并在应用于实际漏洞时减少误解的可能性。这些补充可是添加到度量值描述中的特定于组织的示例。

除了漏洞之外，CVSS 可利用性度量还可用于评估概念级的弱点、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可能利用攻击路径的环境。攻击可行性等级越高，攻击者利用攻击路径的距离（逻辑上和物理上）就越远。其假设是，能够利用互联网漏洞的潜在攻击者的数量大于能够利用需要物理访问相关项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

攻击可行性评级	标准
高	网络： 潜在攻击路径被无任何限制绑定到网络栈 **示例 1**：蜂窝网络连接使 ECU 可直接连接并在互联网上访问。
中	邻近： 潜在攻击路径绑定到网络栈；然而，连接在物理上或逻辑上是有限的 **示例 2**：蓝牙接口、虚拟专用网络连接。
低	本地： 潜在攻击路径不绑定到网络栈，威胁代理需要直接访问相关项来实现攻击路径 **示例 3**：通用串行总线海量存储设备、内存卡。
非常低	物理： 威胁代理需要物理访问来实现攻击路径

附 录 H
（资料性）
TARA 方法的应用示例——前照灯系统以及网关

H.1 总则

本附录中的前照灯系统以及网关的开发和相应的工作成果示例仅用于说明目的，并未暗示任何实际应用的特定做法。

本附录通过提供 TARA 方法的应用示例来帮助理解本文件的要求。该示例仅介绍了概念阶段 TARA 的应用，并以抽象、简化的方式呈现。具体说明了：

——相关项定义；

——TARA。

TARA 被定义为用于分析的模块化方法，且每个模块可按任意顺序进行，例如：

——资产识别→相应的危害场景识别→影响评级→威胁场景识别→攻击路径分析→……

——从目录中选择危害场景→影响评级→威胁场景识别→资产识别→……

本附录示例遵从以下顺序：

1） 资产识别；

2） 影响评级；

3） 威胁场景识别；

4） 攻击路径分析；

5） 攻击可行性评级；

6） 风险值确定；

7） 风险处置决策。

在步骤 5 中，应用了两种不同的方法来对攻击可行性评级。一种使用基于攻击向量（见[RC-15-14]）的方法，另一种使用基于攻击潜力（见[RC-15-12]）的方法。图 H.1 提供了第 9 章和第 15 章之间的交互概况。

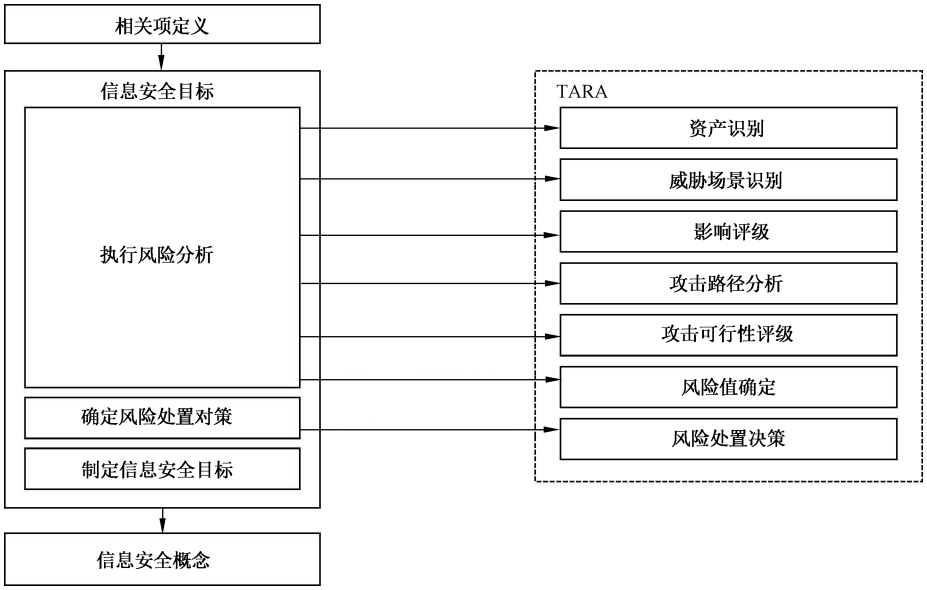


图 H.1 概念阶段的交互

H.2 前照灯系统概念阶段的示例活动

H.2.1 相关项定义

本条展示了 9.3 中指定的工作成果示例。前照灯系统的示例相关项定义如下。

——相关项的边界（见图 H.2）。

——相关项的功能；

相关项的功能概述：前照灯系统根据驾驶员的开关操作以打开或关闭前照灯。如果前照灯处于远光灯模式，当检测到对向驶来的车辆时，该系统自动将前照灯切换至近光灯模式。当未检测到对向驶来的车辆时，自动将前照灯切换回远光灯模式。

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。

——初步的系统架构（见图 H.2）。

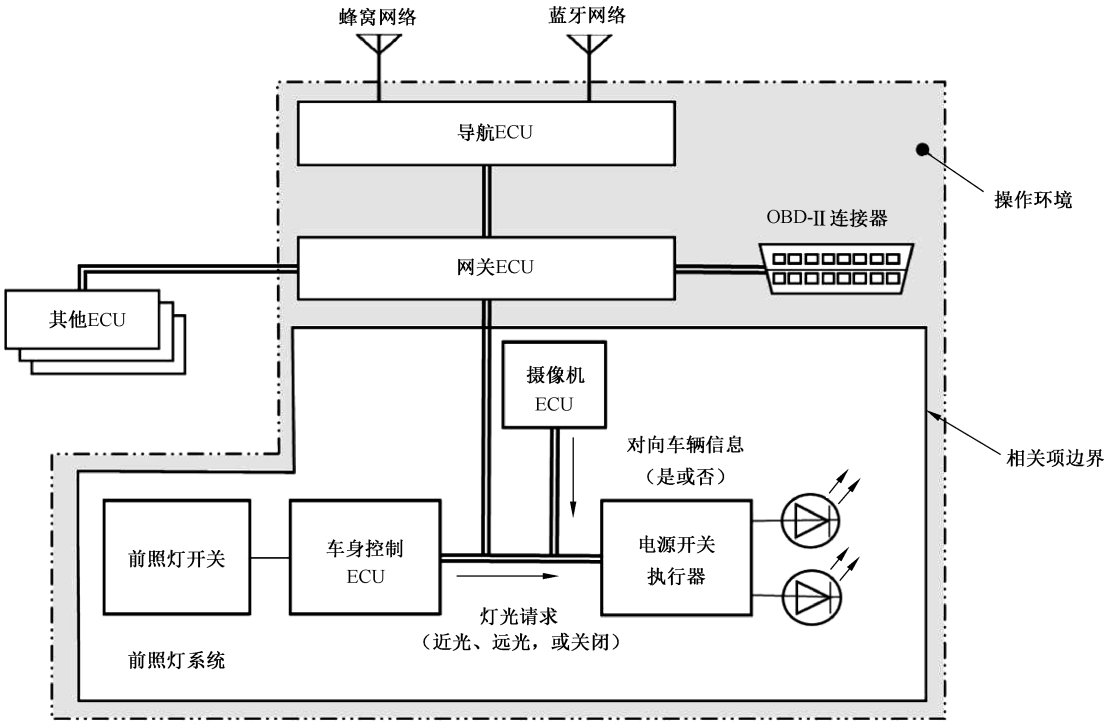


图 H.2　前照灯系统的相关项边界及初步系统架构示例

在相关项定义期间，需描述相关项的操作环境（见[RQ-09-02]）。操作环境为 TARA 的分析活动提供补充信息。操作环境描述的示例如表 H.1 所示。

表 H.1　操作环境描述的示例

序号	操作环境描述的示例
1	该相关项（前照灯系统）与网关 ECU 连接，网关 ECU 和导航 ECU 通过数据通信连接
2	导航 ECU 具有如下外部通信接口： ——蓝牙网络； ——蜂窝网络。 假设：导航 ECU 配置了防火墙以阻止来自外部接口的无效数据通信
3	网关 ECU 具有如下外部通信接口： ——OBD-Ⅱ。 假设：网关 ECU 配置了强健的信息安全控制，包括防火墙功能（以 CAL4 来开发）

H.2.2　资产识别

[RQ-09-03]要求按照 15.3 进行资产识别，以识别相关项的资产以及它们对应的危害场景。资产识别的示例结果如表 H.2 所示。

表 H.2　资产和危害场景列表的示例

序号	资产	安全属性			危害场景
		C	I	A	
1	数据通信（前灯请求）	—	X	X	车辆不能夜间行驶，因为（驾驶员感知到）前灯功能在停车时是被禁止的
		—	X	—	因夜间以中速行驶时不小心关掉前灯而造成的与一个狭窄静止物体的正面碰撞（比如树）
2	数据通信（对向车辆信息）	—	X	—	因为在夜间驾驶时不能切换到低光束而造成对向车辆司机不能看见
		—	—	X	夜间驾驶时，前灯总是处于低光束状态，导致自动远光灯出现故障
3	车身控制 ECU 的固件	X	X	—	……

H.2.3　影响评级

[RQ-09-03]要求按照 15.5 进行影响评级，以评定危害场景的影响。影响评级的示例结果如表 H.3 所示。

表 H.3　危害场景影响评级的示例

序号	危害场景	影响分类	影响评级
1	车辆不能夜间行驶，因为（驾驶员感知到）前灯功能在停车时是被禁止的	O	严重的
2	因夜间以中速行驶时不小心关掉前灯而造成的与一个狭窄静止物体的正面碰撞（比如树）	S	十分严重的（S3）
3	夜间驾驶时，前灯总是处于低光束状态，导致自动远光灯出现故障	O	普通的

H.2.4　威胁场景识别

[RQ-09-03]要求按照 15.4 进行威胁场景识别。威胁场景识别的示例结果如表 H.4 所示。

表 H.4　威胁场景的示例

序号	危害场景	威胁场景
1	因夜间以中速行驶时不小心关掉前灯而造成的与一个狭窄静止物体的正面碰撞（比如树）	信号的欺骗会破坏与电源开关执行器 ECU 的“前灯请求”信号的数据通信的完整性，可能导致前灯在无意中关闭
2		篡改由车身控制 ECU 发送的信号会导致会破坏与电源开关执行器 ECU 的“前灯请求”信号的数据通信的完整性，可能导致前灯在无意中关闭

表 H.4 威胁场景的示例（续）

序号	危害场景	威胁场景
3	夜间驾驶时，前灯总是处于低光束状态，导致自动远光灯出现故障	资产：对向车辆的信息。 信息安全属性：可用性。 相关原因：对向车辆的拒绝服务攻击

H.2.5 攻击路径分析

[RQ-09-03]要求按照 15.6 进行攻击路径分析。攻击路径分析的示例结果如表 H.5 所示，基于攻击树进行攻击路径分析的示例结果如图 H.3 所示。

攻击路径的分析可考虑假设。在本示例中，可根据假设排除需要物理访问相关项内部的攻击路径。例如：车身控制 ECU 的微控制器。

表 H.5 威胁场景的攻击路径示例

序号	威胁场景	攻击路径
1	伪装信号导致发送至电源开关控制器的“灯光请求”信号的数据通信完整性丢失，可能造成前照灯意外关闭	1） 攻击者通过蜂窝网络接口入侵了导航 ECU； 2） 被入侵的导航 ECU 发送恶意控制信号； 3） 网关 ECU 转发恶意控制信号至电源开关执行器； 4） 恶意信号伪装成灯光请求（关灯）
2		1） 攻击者通过蓝牙网络接口入侵了导航 ECU； 2） 被入侵的导航 ECU 发送恶意控制信号； 3） 网关 ECU 转发恶意控制信号至电源开关执行器； 4） 恶意信号伪装成灯光请求（关灯）
3		1） 攻击者可本地访问 OBD 连接器； 2） 攻击者通过 OBD 连接器发送恶意控制信号； 3） 网关 ECU 转发恶意信号至电源开关执行器； 4） 恶意信号伪装成灯光请求（关灯）
4	拒绝提供对向车辆信息的服务	1） 攻击者通过蜂窝网络接口入侵了导航 ECU； 2） 被入侵的导航 ECU 发送恶意控制信号； 3） 网关 ECU 转发恶意控制信号至电源开关执行器； 4） 攻击者用大量消息泛洪攻击通信总线
5	拒绝提供对向车辆信息的服务	1） 当车辆停车未锁时，攻击者将支持蓝牙的 OBD 加密狗连接至 OBD 连接器； 2） 攻击者通过蓝牙网络接口入侵了驾驶员的智能手机； 3） 攻击者通过智能手机和蓝牙加密狗向网关 ECU 发送消息； 4） 网关 ECU 转发恶意信号至电源开关执行器； 5） 攻击者用大量消息泛洪攻击通信总线

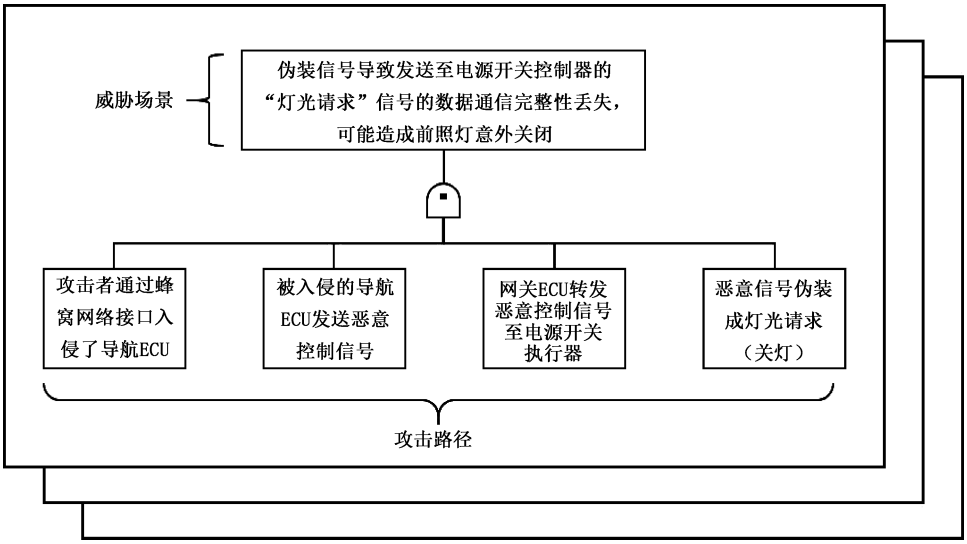


图 H.3　基于攻击树进行攻击路径分析的示例

H.2.6　攻击可行性评级

[RQ-09-03]要求按照 15.7 进行攻击可行性评级。根据 G.4 所述的基于攻击向量的方法进行攻击可行性评级的示例结果如表 H.6 所示。根据 G.2 所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如表 H.7 所示。

表 H.6　基于攻击向量的方法进行攻击可行性评级的示例

序号	攻击路径	攻击可行性评级
1	1）　攻击者通过蜂窝网络接口入侵了导航 ECU； 2）　被入侵的导航 ECU 发送恶意控制信号； 3）　网关 ECU 转发恶意控制信号至电源开关执行器； 4）　恶意信号伪装成灯光请求(开灯)	高
2	1）　攻击者通过蓝牙网络接口入侵了导航 ECU； 2）　被入侵的导航 ECU 发送恶意控制信号； 3）　网关 ECU 转发恶意控制信号至电源开关执行器； 4）　恶意信号伪装成灯光请求(开灯)	中
3	1）　攻击者通过 OBD-II 连接器发送恶意控制信号； 2）　网关 ECU 转发恶意信号至电源开关执行器； 3）　恶意信号伪装成灯光请求(开灯)	低

注：基于攻击向量的方法适合于概念阶段。因为在概念阶段，无法搜集所有和漏洞信息有关的相关项。

根据建议(见[RC-15-11])，攻击可行性也可使用基于攻击潜力的方法来确定，如表 H.7 所示。

表 H.7　基于攻击潜力的方法进行攻击可行性评级的示例

序号	威胁场景	攻击路径	攻击可行性评估						
			ET	SE	KoIC	WoO	Eq	数值	攻击可行性评级
1	拒绝提供对向车辆信息的服务	1）攻击者通过蜂窝网络接口入侵了导航 ECU； 2）被入侵的导航 ECU 发送恶意控制信号； 3）网关 ECU 转发恶意控制信号至电源开关执行器； 4）攻击者用大量消息泛洪攻击通信总线	1	8	7	0	4	20	低
2	拒绝提供对向车辆信息的服务	1）当车辆停车未锁时，攻击者将支持蓝牙的 OBD 加密狗连接至 OBD 连接器； 2）攻击者通过蓝牙网络接口入侵驾驶员的智能手机； 3）攻击者通过智能手机和蓝牙加密狗向网关 ECU 发送消息； 4）网关 ECU 转发恶意信号至电源开关执行器； 5）攻击者用大量消息泛洪攻击通信总线	1	8	7	4	4	24	低
关键字： ET——经历时长； SE——专家的专业知识； KoIC——相关项或组件的知识； WoO——机会窗口； Eq——设备。									

注：各组织可依据各自的政策来制定每个评级的原则。例如：因为需要物理访问，第二条攻击路径的机会窗口被赋值为 4（中等，见表 G.4）。攻击可行性评级是考虑基于表 G.7 的所有可行性值来确定的。

H.2.7　风险值确定

[RQ-09-03]要求按照 15.8 对每个威胁场景的风险值进行确定。风险值可使用组织定义的风险矩阵来确定，将影响评级（见 15.5）和攻击可行性评级（见 15.7）组合映射到风险值。风险矩阵的示例如表 H.8 所示，使用表 H.8 进行风险值确定的示例结果如表 H.9 所示。

表 H.8　风险矩阵的示例

影响评级	攻击可行性评级			
	非常低	低	中	高
十分严重的	2	3	4	5
严重的	1	2	3	4
普通的	1	2	2	3
可忽略不计	1	1	1	1

表 H.9　风险值确定的示例

序号	威胁场景	综合的攻击可行性评级	影响评级	风险值
1	伪装信号导致发送至电源开关控制器的“灯光请求”信号的数据通信完整性丢失	高	十分严重的	S:5
2	拒绝提供对向车辆信息的服务	低	中等	O:2

风险值也可由组织定义的风险计算公式来确定，一个示例如公式(H.1)和表 H.10 所示。

$$R = 1 + I \times F \qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (H.1)$$

式中：

R ——风险值；

I ——影响的数值；

F ——攻击可行性的数值。

表 H.10　将影响和攻击可行性转换为数值的示例

影响评级	影响的数值 I
可忽略	0
中等	1
重大	1.5
严重	2

攻击可行性评级	攻击可行性的数值 F
极低	0
低	1
中	1.5
高	2

对于表 H.9 中展示的特定威胁场景，使用表 H.8 中给出的示例和上述公式计算，将得出相同的风险值。

H.2.8　风险处置决策

[RQ-09-04] 要求按照 15.9 选择风险处置方案。风险处置决策的示例结果如表 H.11 所示。

表 H.11　风险处置决策的示例结果

序号	威胁场景	风险值	风险处置方案
1	伪装信号导致发送至电源开关控制器的“灯光请求”信号的数据通信完整性丢失	S:5	降低风险
2	拒绝提供对向车辆信息的服务	O:2	降低风险

H.3　汽车网关概念阶段的示例活动

H.3.1　相关项定义

本条展示了 9.3 中指定的工作成果示例。汽车网关(以下简称“网关”)的示例相关项定义如下：

——相关项的边界(见图 H.4)；

——相关项的功能；

相关项的功能概述：网关的基础功能为在不同的通信协议和不同的传输速度的模块之间进行通信时，建立连接和信息解码，并将数据传输给其他系统。

——初步的系统架构(见图 H.4)。

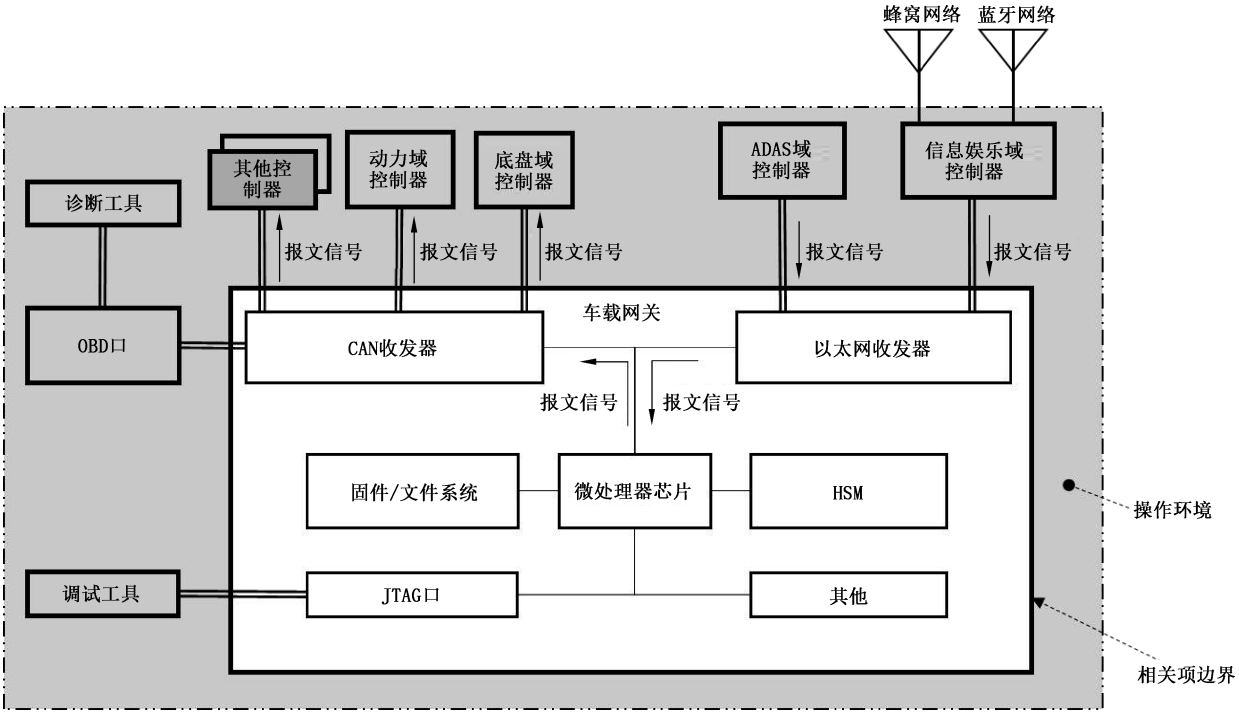


图 H.4　网关的相关项边界及初步系统架构示例

在相关项定义期间，需描述相关项的操作环境(见[RQ-09-02])。操作环境为 TARA 的分析活动提供补充信息。操作环境描述的示例结果如表 H.12 所示。

表 H.12　操作环境描述的示例

序号	操作环境描述的示例
1	操作环境中的其他控制器(例如:ADAS 域控制器等)可通过 CAN 和车载以太网等与网关建立通信
2	操作环境中的其他控制器(例如:信息娱乐域控制器等)存在 USB、WLAN、蓝牙、蜂窝网络等对外通信方式。这些控制器也支持诊断和调试工具的接入
3	操作环境中的诊断工具可通过 OBD 口对网关进行诊断
4	操作环境中的调试工具可通过 JTAG 口对网关进行调试和刷写

操作环境信息应该包括假设(见[RQ-09-02])。假设的示例结果如表 H.13 所示。

表 H.13　假设的示例

序号	假设的示例
1	假设操作环境中的其他控制器实施了安全控制措施,入侵技术无法轻易扩展
2	假设操作环境中的其他控制器使用了适当的硬件安全模块和软件安全协议或算法
3	假设操作环境中对外连接的控制器(例如:信息娱乐域控制器等)具有身份认证机制
4	假设操作环境中对外连接的控制器(例如:信息娱乐域控制器等)对应的 PKI 是安全可信的

H.3.2　资产识别

[RQ-09-03]要求按照 15.3 进行资产识别,以识别相关项的资产以及它们对应的危害场景。资产识别的示例结果如表 H.14 所示。

表 H.14　资产和危害场景示例

序号	资产	安全属性			危害场景
		C	I	A	
1	网关固件	—	X	—	由于网关固件的完整性被破坏,可能存在车辆被未授权打开车门、启动引擎的风险
2	日志服务软件	—	X	—	由于日志服务软件完整性被破坏,可能存在网关日志服务无法正常使用,影响安全问题分析造成的风险
3	系统配置文件	X	—	—	由于系统配置文件数据机密性被破坏,可能存在网关的系统配置信息泄露的风险
4	微处理器芯片	—	X	—	由于微处理器芯片的完整性被破坏,可能存在网关基础功能异常运行的风险
		—	—	X	由于微处理器芯片的可用性被破坏,可能存在网关联网/定位/数字钥匙等功能无法正常使用的风险

对于网关的其他资产,可采用相同的方式进行资产识别和危害场景识别。

H.3.3 影响评级

[RQ-09-03]要求按照 15.5 进行影响评级，以评定危害场景的影响。根据附录 F 所述的方法进行影响评级的示例结果如表 H.15 所示。

表 H.15 危害场景影响评级的示例

序号	危害场景	S	F	O	P	影响评级
1	由于网关固件的完整性被破坏，可能存在车辆被未授权打开车门、启动引擎的风险	十分严重的	严重的	严重的	可忽略不计	十分严重的
2	由于日志服务软件完整性被破坏，可能存在网关日志服务无法正常使用的风险	可忽略不计	普通的	普通的	可忽略不计	普通的
3	由于系统配置文件数据机密性被破坏，可能存在网关的系统配置信息泄露的风险	可忽略不计	普通的	可忽略不计	严重的	严重的
4	由于微处理器芯片的完整性被破坏，可能存在网关基础功能异常运行的风险	十分严重的	严重的	严重的	可忽略不计	十分严重的
5	由于微处理器芯片的可用性被破坏，可能存在网关联网/定位/数字钥匙等功能无法正常使用的风险	严重的	普通的	严重的	可忽略不计	严重的

对危害场景所造成的影响从安全、财务、操作、隐私(SFOP)四个方面进行分析，并得出每个影响的指标值。选取危害场景四个指标中的最高值作为其影响评级。

以危害场景“由于网关固件的完整性被破坏，可能存在车辆被未授权打开车门、启动引擎的风险”为例：

——安全(S)：十分严重的，因为该危害场景在特定场景下(例如：高速情况下)，可能导致驾乘人员受到威胁生命的伤害，且不确定是否幸存；

——财务(F)：严重的，因为该危害场景可能让车主无法定位到网关存在完整性破坏问题，而去更换车门、引擎等多个车辆模块，会导致经济上的大量损失，即使这些损失通常是可克服的；

——操作(O)：十分严重的，因为该危害场景可能导致车辆核心功能的丧失或受损；

——隐私(P)：可忽略不计，因为该危害场景不会造成隐私层面的影响。

最终影响评级可选取四个指标中的最高值，在此情况下，影响评级为：十分严重的。

注：各组织依据各自的策略来制定评级的度量和原则。

H.3.4 威胁场景识别

[RQ-09-03]要求按照 15.4 进行威胁场景识别。威胁场景识别的示例结果如表 H.16 所示。

表 H.16 威胁场景的示例

序号	危害场景	威胁场景
1	由于网关固件的完整性被破坏,可能存在车辆被未授权打开车门、启动引擎的风险	攻击者可能通过篡改网关的固件,导致网关无法对恶意数据进行拦截,从而帮助攻击者进行进一步跨域攻击
2	由于日志服务软件完整性被破坏,可能存在网关日志服务无法正常使用的风险	攻击者可能通过篡改网关的日志服务软件,导致读取日志时获取错误信息
3	由于系统配置文件数据机密性被破坏,可能存在网关的系统配置信息泄露的风险	攻击者可能通过网关的调试口进入文件系统,获取系统配置信息
4	由于微处理器芯片的完整性被破坏,可能存在网关基础功能异常运行的风险	攻击者可能通过篡改微处理器芯片的引脚配置,导致网关功能异常运行
5	由于微处理器芯片的可用性被破坏,可能存在网关联网功能/定位/数字钥匙等功能无法正常使用的风险	攻击者可能通过篡改微处理器芯片的外围电路,导致网关无法对数据进行正确的转发

H.3.5 攻击路径分析

[RQ-09-03]要求按照 15.6 进行攻击路径分析。攻击路径分析的示例结果如表 H.17 所示,基于攻击树进行攻击路径分析的示例结果如图 H.5 所示。

攻击路径的分析可考虑假设。在本示例中,可根据假设排除需要物理访问相关项内部的攻击路径。例如:车身控制 ECU 的微控制器。

表 H.17 威胁场景的攻击路径示例

序号	威胁场景	攻击路径
1	攻击者可能通过篡改网关的固件,导致网关无法对恶意数据进行拦截,从而帮助攻击者进行进一步跨域攻击	1) 攻击者获得网关 PCB 并可物理访问; 2) 攻击者提取网关固件; 3) 攻击者对固件进行逆向分析并篡改内容; 4) 攻击者获取网关的固件的刷写权限; 5) 攻击者对网关进行固件重新刷写
2	攻击者可能通过篡改网关的日志服务软件,导致读取日志时获取错误信息	1) 攻击者获得网关软件包并进行篡改; 2) 攻击者连接车辆诊断接口; 3) 攻击者破解 UDS 协议的安全访问权限控制[种子和密钥机制(Seed and Key)]以提升权限,或仿冒已授权的节点; 4) 攻击者使用 UDS 协议将错误的软件包刷写至网关
3	攻击者可能通过网关的调试口进入文件系统,获取系统配置信息	1) 攻击者通过物理访问,使用工具连接网关调试口; 2) 攻击者检索各个文件系统,尝试连接所有系统资源; 3) 攻击者从系统资源中查询并提取需要的系统配置信息

表 H.17　威胁场景的攻击路径示例（续）

序号	威胁场景	攻击路径
4	攻击者可能通过篡改微处理器芯片的引脚配置，导致网关功能异常运行	1）　攻击者获得网关 PCB 并可物理访问； 2）　攻击者篡改芯片的启动模式引脚配置，以改变启动策略； 3）　芯片启动恶意固件，导致网关功能异常运行
5	攻击者可能通过篡改微处理器芯片的外围电路，导致网关无法对数据进行正确的转发	1）　攻击者获得网关 PCB 并可物理访问； 2）　攻击者篡改芯片的外围电路，以造成其运行异常； 3）　芯片运行异常，导致网关合法功能丢失

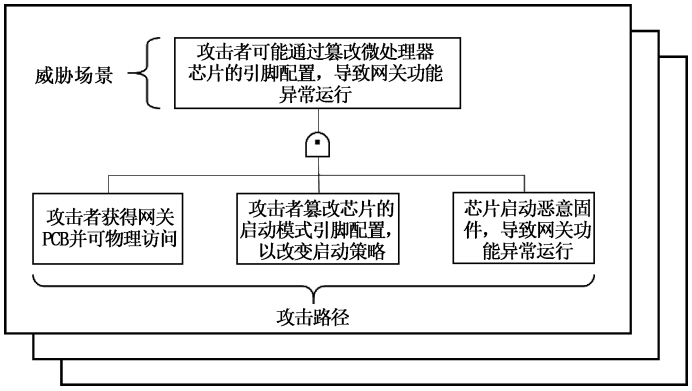


图 H.5　基于攻击树进行攻击路径分析的示例

H.3.6　攻击可行性评级

[RQ-09-03]要求按照 15.7 进行攻击可行性评级。本节展示了采用两种不同的方法进行攻击可行性评级的示例结果。根据 G.4 节所述的基于攻击向量的方法进行攻击可行性评级的示例如表 H.18 所示。根据 G.2 所述的基于攻击潜力的方法进行攻击可行性评级的示例如表 H.19 所示。

表 H.18　基于攻击向量的方法进行攻击可行性评级的示例

序号	攻击路径	攻击可行性评级
1	1）　攻击者获得网关 PCB 并可物理访问； 2）　攻击者提取网关固件； 3）　攻击者对固件进行逆向分析并篡改内容； 4）　攻击者获取网关的固件的刷写权限； 5）　攻击者对网关进行固件重新刷写	非常低
2	1）　攻击者获得网关软件包并进行篡改； 2）　攻击者连接车辆诊断接口； 3）　攻击者破解 UDS 协议的安全访问权限控制（Seed and Key 机制）以提升权限，或仿冒已授权的节点； 4）　攻击者使用 UDS 协议将错误的软件包刷写至网关	中

表 H.18 基于攻击向量的方法进行攻击可行性评级的示例（续）

序号	攻击路径	攻击可行性评级
3	1） 攻击者通过物理访问，使用工具连接网关调试口； 2） 攻击者检索各个文件系统，尝试连接所有系统资源； 3） 攻击者从系统资源中查询并提取需要的系统配置信息	非常低
4	1） 攻击者获得网关 PCB 并可物理访问； 2） 攻击者篡改芯片的启动模式引脚配置，以改变启动策略； 3） 芯片启动恶意固件，导致网关功能异常运行	非常低
5	1） 攻击者获得网关 PCB 并可物理访问； 2） 攻击者篡改芯片的外围电路，以造成其运行异常； 3） 芯片运行异常，导致网关合法功能丢失	非常低

注：基于攻击向量的方法适合于概念阶段。因为在概念阶段，无法搜集所有和漏洞信息有关的相关项。

根据建议（见[RC-15-11]），攻击可行性也可使用基于攻击潜力的方法来确定，如表 H.19 所示。

表 H.19 基于攻击潜力的方法进行攻击可行性评级的示例

序号	威胁场景	攻击路径	攻击可行性评估						
			ET	SE	KoIC	WoO	Eq	数值	攻击可行性评级
1	攻击者可能通过篡改网关的固件，导致网关无法对恶意数据进行拦截，从而帮助攻击者进行进一步跨域攻击	1） 攻击者获得网关 PCB 并可物理访问； 2） 攻击者提取网关固件； 3） 攻击者对固件进行逆向分析并篡改内容； 4） 攻击者获取网关的固件的刷写权限； 5） 攻击者对网关进行固件重新刷写	4	6	7	10	7	34	非常低
2	攻击者可能通过篡改网关的日志服务软件，导致读取日志时获取错误信息	1） 攻击者获得网关软件包并进行篡改； 2） 攻击者连接车辆诊断接口； 3） 攻击者破解 UDS 协议的安全访问权限控制（Seed and Key 机制）以提升权限，或仿冒已授权的节点； 4） 攻击者使用 UDS 协议将错误的软件包刷写至网关	1	3	3	4	0	11	高

表 H.19　基于攻击潜力的方法进行攻击可行性评级的示例（续）

序号	威胁场景	攻击路径	攻击可行性评估						
			ET	SE	KoIC	WoO	Eq	数值	攻击可行性评级
3	攻击者可能通过网关的调试口进入文件系统，获取系统配置信息	1）攻击者通过物理访问，使用工具连接网关调试口； 2）攻击者检索各个文件系统，尝试连接所有系统资源； 3）攻击者从系统资源中查询并提取需要的系统配置信息	1	3	3	10	4	22	低
4	攻击者可能通过篡改微处理器芯片的引脚配置，导致网关功能异常运行	1）攻击者获得网关 PCB 并可物理访问； 2）攻击者篡改芯片的启动模式引脚配置，以改变启动策略； 3）芯片启动恶意固件，导致网关功能异常运行	4	6	7	10	4	31	非常低
5	攻击者可能通过篡改微处理器芯片的外围电路，导致网关无法对数据进行正确的转发	1）攻击者获得网关 PCB 并可物理访问； 2）攻击者篡改芯片的外围电路，以造成其运行异常； 3）芯片运行异常，导致网关合法功能丢失	4	6	7	10	4	31	非常低
关键字： ET——经历时长 SE——专家的专业知识 KoIC——相关项或组件的知识 WoO——机会窗口 Eq——设备									

注：各组织依据各自的策略来制定每个评级的度量和原则。

H.3.7　风险值确定

[RQ-09-03]要求按照 15.8 对每个威胁场景的风险值进行确定。风险值可使用组织定义的风险矩阵来确定，将影响评级（见 15.5）和攻击可行性评级（见 15.7）组合映射到风险值。风险矩阵的示例如表 H.20 所示，使用表 H.20 进行风险值确定的示例结果如表 H.21 所示。

在本节中，攻击可行性评级采用表 H.19 基于攻击潜力的方法评估得到的结果。

表 H.20　风险矩阵示例

影响评级	攻击可行性评级			
	非常低	低	中	高
十分严重的	2	3	4	5
严重的	1	2	3	4
普通的	1	2	2	3
可忽略不计	1	1	1	1

表 H.21　风险值确定的示例(基于风险矩阵)

序号	威胁场景	综合的攻击可行性评级	影响评级	风险值
1	攻击者可能通过篡改网关的固件,导致网关无法对恶意数据进行拦截,从而帮助攻击者进行进一步跨域攻击	非常低	十分严重的	2
2	攻击者可能通过篡改网关的日志服务软件,导致读取日志时获取错误信息	高	普通的	3
3	攻击者可能通过网关的调试口进入文件系统,获取系统配置信息	低	严重的	2
4	攻击者可能通过篡改微处理器芯片的引脚配置,导致网关功能异常运行	非常低	十分严重的	2
5	攻击者可能通过篡改微处理器芯片的外围电路,导致网关无法对数据进行正确的转发	非常低	严重的	1

风险值也可由组织定义的风险计算公式来确定,一个示例如公式(H.2)和表 H.22 所示。

$$R = 1 + I \times F \qquad \cdots\cdots\cdots\cdots\cdots\cdots (H.2)$$

式中:

R ——风险值,

I ——影响的数值,

F ——攻击可行性的数值。

表 H.22　将影响和攻击可行性转换为数值的示例

影响评级	影响的数值 I
可忽略不计	0
普通的	1
严重的	1.5
十分严重的	2

攻击可行性评级	攻击可行性的数值 F
非常低	0.5
低	1
中	1.5
高	2

一个依据风险计算公式确定风险值的示例如表 H.23 所示。

表 H.23　风险值确定的示例(基于风险计算公式向下取整)

序号	威胁场景	F	I	R
1	攻击者可能通过篡改网关的固件,导致网关无法对恶意数据进行拦截,从而帮助攻击者进行进一步跨域攻击	0.5	2	2
2	攻击者可能通过篡改网关的日志服务软件,导致读取日志时获取错误信息	2	1	3
3	攻击者可能通过网关的调试口进入文件系统,获取系统配置信息	1	1.5	2
4	攻击者可能通过篡改微处理器芯片的引脚配置,导致网关功能异常运行	0.5	2	2
5	攻击者可能通过篡改微处理器芯片的外围电路,导致网关无法对数据进行正确的转发	0.5	1.5	1

对于表 H.21 中展示的特定威胁场景,使用表 H.20 中给出的示例和上述公式计算,将得出相同的风险值。

注:各组织根据各自的策略定义风险矩阵和风险计算公式,或采用其他方法确定风险值。

H.3.8　风险处置决策

[RQ-09-04]要求按照 15.9 选择风险处置方案。风险处置决策的示例结果如表 H.24 所示。

表 H.24　风险处置决策的示例结果

序号	威胁场景	风险值	风险处置方案
1	攻击者可能通过篡改网关的固件,导致网关无法对恶意数据进行拦截,从而帮助攻击者进行进一步跨域攻击	2	降低风险
2	攻击者可能通过篡改网关的日志服务软件,导致读取日志时获取错误信息	3	降低风险
3	攻击者可能通过网关的调试口进入文件系统,获取系统配置信息	2	降低风险
4	攻击者可能通过篡改微处理器芯片的引脚配置,导致网关功能异常运行	2	降低风险
5	攻击者可能通过篡改微处理器芯片的外围电路,导致网关无法对数据进行正确的转发	2	保留风险

H.3.9　制定信息安全目标

[RQ-09-05]要求按照 9.4 制定信息安全目标。信息安全目标的示例结果如表 H.25 所示。

表 H.25　信息安全目标的示例结果

序号	威胁场景	风险处置方案	信息安全目标
1	攻击者可能通过篡改网关的固件，导致网关无法对恶意数据进行拦截，从而帮助攻击者进行进一步跨域攻击	降低风险	保护网关固件，防止攻击者篡改固件
2	攻击者可能通过篡改网关的日志服务软件，导致读取日志时获取错误信息	降低风险	保护网关日志服务软件，防止攻击者篡改软件
3	攻击者可能通过网关的调试口进入文件系统，获取系统配置信息	降低风险	保护网关的调试口，防止攻击者非授权访问
4	攻击者可能通过篡改微处理器芯片的引脚配置，导致网关功能异常运行	降低风险	保护微处理器芯片，防止其引脚配置被恶意篡改
5	攻击者可能通过篡改微处理器芯片的外围电路，导致网关无法对数据进行正确的转发	保留风险	无

[RQ-09-06]要求对于选择保留风险的威胁场景，应提供相应的信息安全声明。信息安全声明的示例结果如表 H.26 所示。

表 H.26　信息安全声明的示例结果

威胁场景	风险处置方案	信息安全声明
攻击者可能通过篡改微处理器芯片的外围电路，导致网关无法对数据进行正确的转发	保留风险	由于该威胁场景需要攻击者破坏 PCB 板的电路实现攻击，其攻击可行性极低，从而风险值低。因此可选择保留风险

参 考 文 献

[1] GB/T 19001 质量管理体系 要求

[2] GB/T 30276 信息安全技术 网络安全漏洞管理规范

[3] GB/T 33007 工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序

[4] GB/T 34590(所有部分) 道路车辆 功能安全

[5] ISO/TR 4804 Road vehicles—Safety and cybersecurity for automated driving systems—Design，verification and validation

[6] ISO 9000:2015 Quality management systems—Fundamentals and vocabulary

[7] ISO 9001 Quality management systems—Requirements

[8] ISO 10007 Quality management—Guidelines for configuration management

[9] ISO 26262-1:2018 Road vehicles—Functional safety—Part 1: Vocabulary

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

[11] ISO 31000:2018 Risk management—Guidelines

[12] ISO/IEC 2382 Information technology—Vocabulary

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

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

[15] ISO/IEC 27000:2018 Information technology—Security techniques—Information security management systems—Overview and vocabulary

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

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

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

[19] ISO/IEC 29147 Information technology—Security techniques—Vulnerability disclosure

[20] ISO/IEC 33001 Information technology—Process assessment—Concepts and terminology

[21] ISO/IEC/IEEE 15288 Systems and software engineering—System life cycle processes

[22] ISO/IEC/ IEEE 12207 Systems and software engineering—Software life cycle processes

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

[24] IEC 31010 Riskmanagement—Risk assessment techniques

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

[26] IEC 62443-2-1 Industrial communication networks—Network and system security—Part 2-1:Establishing an industrial automation and control system security program

[27] IATF 16949 Quality management system requirements for automotive production and relevant service parts organizations

[28] SAE J3061 Cybersecurity Guidebook for Cyber—Physical Vehicle Systems

[29] ETSI TS 102165-1 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]

[30] AUTOMOTIVE，ISAC，Automotive Cybersecurity Best Practices [online]

[31] 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]

[32] FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS（FIRST）. Common Vulnerability Scoring System（CVSS），Common Vulnerability Scoring System v3.1：Specification Document [online]

[33] FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS（FIRST）. Traffic Light Protocol（TLP）FIRST Standards Definitions and Usage Guidance—Version 1.0[online]

[34] JOHNSON Christopher，et al.（2016）Guide to Cyber Threat Information Sharing [online].(National Institute of Standards and Technology，Gaithersburg，MD)，NIST Special Publication（SP)800150，October 2016 [viewed 2021-02-16]

[35] 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]

[36] 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)：978-1-906400-21-71978-1-906400-22-4

[37] 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]

[38] SCARFONE Karen，et al.(2008)，Technical Guie 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].

[39] SE1 CERT C Coding Standard—Rules for developing safe，reliable and secure systems [online]Pittsburgh，Pennsylvania：Software Engineering Institute，Carnegie Mellon University，2016 [viewed2021-02-12]

[40] TAKANEN Ari et al. Fuzzing for Software Security and Quality Assurance，Second Edition. Boston Massachusetts/London：Artech House，January 2018. ISBN：978-1-60807-850-9

[41] 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

[42] VDA OMC WORKING GROUP 13/AUTOMOTIVE SIG. Automotive SPICE Process Assessment Reference Model，Version 3.1[online]. Berlin：VDA QMC，November 2017