国际/sae
标准 21434

第一版
2021-08

道路车辆、网络安全工程

网络安全的知识

参考编号
ISO/SAE21434：2021(E)

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 21434:2021《道路车辆 信息安全工程》。

本文件与ISO 21434:2021的主要内容差异及其原因如下：

增加了资料性附录H中关于汽车网关的威胁分析和风险评估（TARA）示例， 以帮助标准的使用者更好的理解威胁分析和风险评估（TARA）方法的应用。

本文件对国际标准的表述进行了编辑性修改。

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/TC114）归 口。

本文件为首次发布。

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、运行、维护和报废阶段的信息安全风险管理的工程要求。

本文件定义了一个框架，其中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。

本文件适用于在本文件发布后开发或修改的批量生产的道路车辆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 第三部分：概念阶段

3 术语和定义

下列术语和定义适用于本文件。

3.1

架构设计 architectural design

可以识别组件、边界、接口和交互的表示方法。

3.2

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，未达到要求时可能导致一个或多个危害场景。

3.3

攻击可行性 attack feasibility

攻击路径的属性，描述成功执行相应攻击活动的难易度。

3.4

攻击路径 attack path

为实现威胁场景的一组攻击活动。

3.5

攻击者 attacker

执行攻击路径的个人、团体或组织。

3.6

审核 audit

对过程进行检查， 以确定过程目标的实现程度。

3.7

组件 component
逻辑上和技术上可分离的组成部分。

3.8

客户 customer
接受服务或产品的个人或组织。

3.9

道路车辆信息安全 cybersecurity
使资产受到充分保护，免受道路车辆相关项、其功能及其电气或电子组件的威胁场景的危害。
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。

3.10

信息安全评估 cybersecurity assessment
信息安全状态的评价。

3.11

信息安全档案 cybersecurity case
有证据支持的结构化论证，表明风险的合理性。

3.12

信息安全声明 cybersecurity claim
关于风险的信息安全索赔声明。
注： 信息安全声明可包括保留或分担风险的理由。

3.13

信息安全概念 cybersecurity concept
相关项的信息安全需求和对操作环境的要求以及有关信息安全控制的相关信息。

3.14

信息安全控制 cybersecurity control
改变风险的措施。

3.15

信息安全事态 cybersecurity event
与相关项或组件有关的信息安全信息。

3.16

信息安全目标 cybersecurity goal
与一个或多个威胁情景相关的概念级信息安全需求。

3.17

信息安全事件 cybersecurity incident
可能涉及漏洞利用的情况。

3.18

信息安全信息 cybersecurity information
与信息安全有关的信息,其相关性尚未确定。

3.19

信息安全接口协议 cybersecurity interface agreement
客户和供应商之间关于分布式信息安全活动的协议。

3.20

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/或可用性。

3.21

信息安全规范 cybersecurity specification
信息安全需求和相应的架构设计。

3.22

危害场景 damage scenario
涉及车辆或车辆功能并影响道路使用者的不良后果。

3.23

分布式信息安全活动 distributed cybersecurity activities
相关项或组件的信息安全活动，其责任在客户和供应商之间分配。

3.24

影响 impact
对危害场景下的损害程度或物理伤害程度的估计。

3.25

相关项 item
在车辆层面实现一个功能的组件或组件集。
注： 如果一个系统在车辆层面实现了一个功能，它就可以成为一个相关项，否则就是一个组件。

3.26

操作环境 operational environment
在操作使用中考虑到相互作用的环境。
注： 相关项或组件的操作使用，包括在车辆功能，生产，和/或服务和修理中的使用。

3.27

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中。

3.28

渗透测试 penetration testing
模拟实际攻击的信息安全测试，用以识别破坏信息安全目标的方法。

3.29

风险 risk
信息安全风险，道路车辆信息安全不确定性的影响，可用攻击可行性和影响表示。

3.30

风险管理 risk management
指导和控制组织风险的协调活动。

3.31

道路使用者 road user
参与道路交通活动的人员。

3.32

裁剪 tailor
以与本文件描述不同的方式省略或执行某项活动。

3.33

威胁场景 threat scenario
为实现危害场景，一个或多个资产的信息安全属性遭到破坏的潜在原因。

3.34

分类 triage
分析以确定信息安全信息与某一相关项或组件的相关性。

3.35

触发器 trigger
用于分类的准则。

3.36

确认 validation
通过提供客观证据以证明相关项的信息安全目标是否充分并已实现。

3.37

验证 verification
通过提供客观证据确认是否满足特定要求。

3.38

脆弱性或漏洞 vulnerability
能被利用的弱点，可作为攻击路径的一部分。

3.39

漏洞分析 vulnerability analysis
系统地识别和评估漏洞。

3.40

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。

4 缩略语

CAL： 信息安全保障等级（Cybersecurity Assurance Level）
CVSS： 常见漏洞评分系统（Common Vulnerability Scoring System）
E/E： 电子电气（Electrical and Electronic）
ECU： 电子控制单元（Electronic Control Unit）
OBD: 车载诊断（On-Board Diagnostic）
OEM： 原始设备制造商（Original Equipment Manufacturer）
PM： 许可（Permission）
RC： 建议（Recommendation）
RQ： 要求（Requirement）
WP： 工作成果（Work Product）
RASIC： 责任、批准、支持、知情、咨询（Responsible, Accountable, Supporting, Informed, Consulted）
TARA： 威胁分析和风险评估（Threat Analysis and Risk Assessment）

5 整体考虑

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

本文件仅适用于批量生产的道路车辆（即不是原型车）与信息安全相关的相关项和组件，包括售后件和服务件。车辆的外部系统（如后端服务器）出于信息安全的目的可以考虑，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。本文件没有规定如何进行道路车辆E/E架构中相关项功能的适当分配。对于车辆整体而言，可以考虑构建车辆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。如果本文件中描述的信息安全活动是在相关项和组件上进行的，那么将会解决不合理的车辆信息安全风险。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。

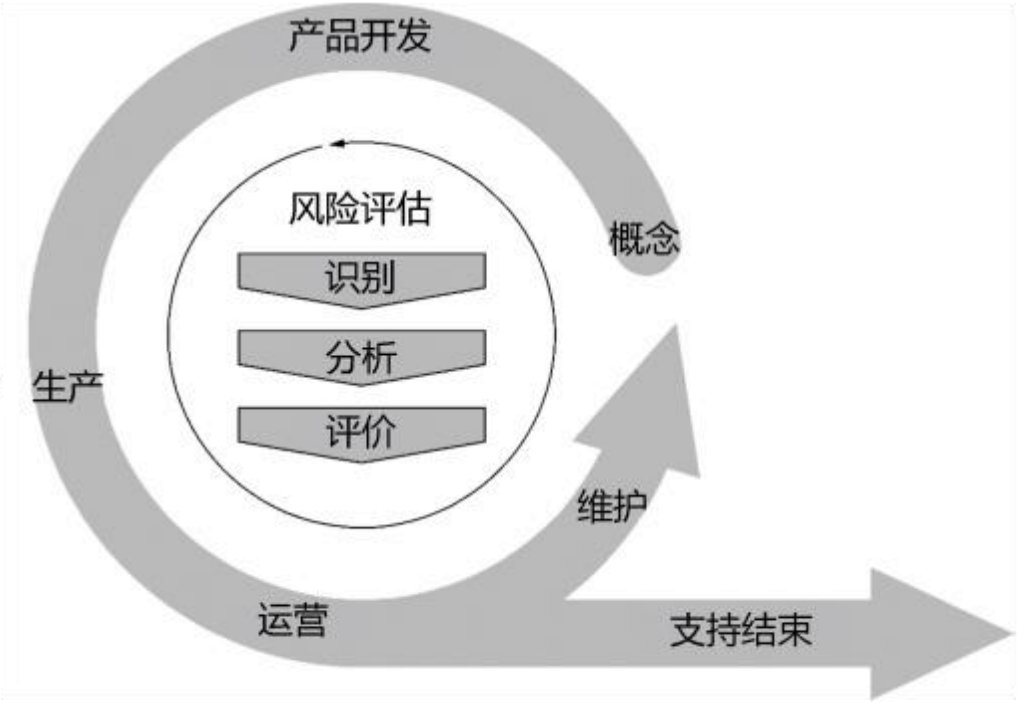

图 1　整体信息安全风险管理

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。信息安全活动可以根据具体情况的需要进行裁剪。某一特定相关项或部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。

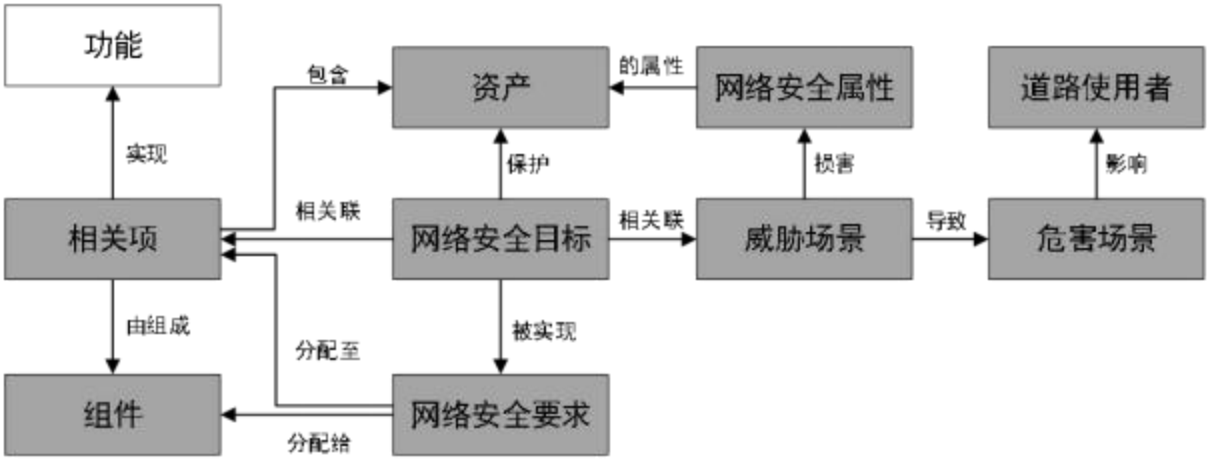

图 2　相关项、功能、组件和相关术语之间的关系

第16章描述了信息安全风险评估的模块化方法，这些方法会在其他章节所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，可识别和探索具有恶意意图的抽象敌对行为者的潜在行为，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以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，可以作为一种被动的方法，确认环境中不断变化的条件（如新的攻击技术），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。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。

6 组织的信息安全管理

6.1 总则

为了实现信息安全工程，组织应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。这涉及到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，组织还应为信息安全建立管理体系，包括工具的管理和质量管理体系的应用。

6.2 目标

本章的目标是：

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。

6.3 输入

无。

6.3.1 先决条件

无。

6.3.2 更多支持信息

可以考虑以下信息：

- 符合质量管理标准的证据。

例如：IATF 16949与其他标准的联合，如：ISO 9001，Automotive SPICE,ISO/IEC 330XX系列标准,ISO/IEC/IEEE 15288和ISO/IEC/IEEE 12207。

6.4 要求和建议

6.4.1 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) 最高管理层对相应信息安全风险进行管理的承诺。

注1：信息安全方针可以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：信息安全风险管理能包括活动的付出-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，可以依据ISO 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]组织应分配实现与维护信息安全的职责，并给予相应的组织权力。

注7：这既关系到项目层面的活动也关系到组织层面的活动。

[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完成信息安全活动。

[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到现有过程中， 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的冲突或对抗；

-信息安全要求与功能安全要求的冲突或对抗。

6.4.2　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。

6.4.3 信息共享

［RQ-05-09］组织应界定在哪些情况下，要求、允许或者被禁止组织内部和外部共享信息安全相关的信息。
注：共享信息的情况可以基于：
-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；
-为特定方提供的通讯类型；
-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。

6.4.4 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 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 2：一项工作成果可以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］用于维护该领域内产品信息安全的配置信息应保持可用，直至产品的网络安全支持结束， 以便能采取补救措施。
注 3：归档构建环境有助于确保配置信息的后续使用。
例 2：物料清单、软件配置。
［RC-05-13］应建立生产过程的信息安全管理体系，以便支持12章的活动。
例 3：IEC 62443 2-1。

6.4.5 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，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，如 Flash 写入、EOL 测试工具。
示例3：用于售后维修的工具，如 OBD 工具或者重新编程工具。
注：这类管理可以通过以下方式确立：
-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应该是可复现的，直至产品的信息安全支持结束。
例 4：用于复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。

6.4.6 信息安全管理

[RC-05-16]工作成果应按照信息安全管理体系进行管理。

例：可以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。

6.4.7 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：信息安全审核可以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 ISO 9001 相结合。

注 2：独立性可以基于，例如，GB/T 34590 系列标准。

注 3：执行审核的人员可以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，审核可以周期性执行。

注 5：图 7 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。

6.5 工作成果

[WP-05-01] 信息安全方针、规则和过程，依据 6.4.1 至 6.4.3 的要求。

[WP-05-02] 能力管理和意识管理的证据，依据[RQ-05-07]的要求；持续改进的证据，依据[RQ-05-08]的要求。

[WP-05-03] 组织管理体系的证据，依据 6.4.4 和 6.4.6 的要求。

[WP-05-04] 工具管理的证据，依据 6.4.5 的要求。

[WP-05-05] 组织层面的信息安全审核报告，依据 6.4.7 的要求。

7 项目相关的信息安全管理

7.1 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，以便可以将其应用于各种相关项和组件。另外，可以基于原理在信息安全计划中进行裁剪。可以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，相关项和组件的复用是可以应用的开发策略。 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，则可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，则可以基于现有文件复用，并说明理由。

一个组件可以独立于环境开发，例如基于假设的环境。在与客户接触或达成商业协议之前，组织可以为不同的应用和不同的客户开发通用组件。 供应商可以对环境和预期用途进行假设。 基于此，供应商可以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，可以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以被集成到一个相关项或组件中（见图4）。集成可包含与 7.4.4 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。

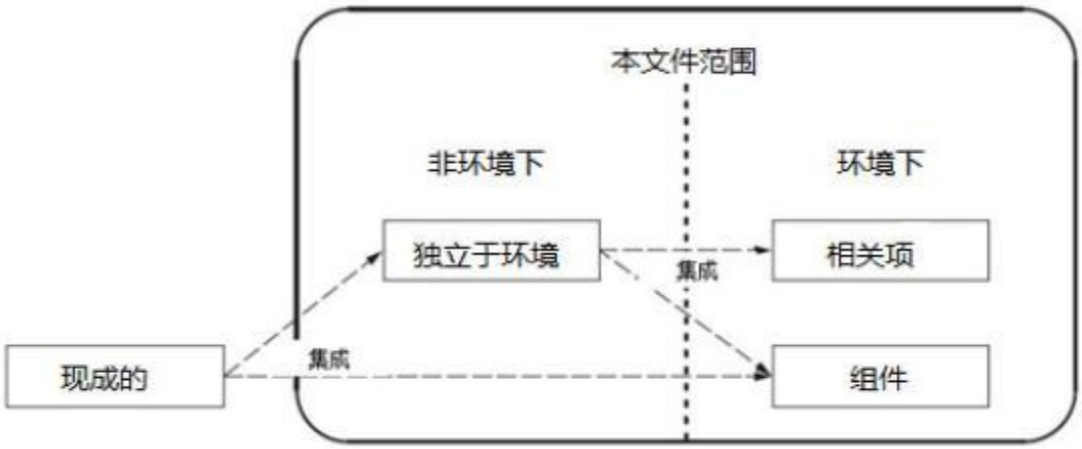

图 4　现成和独立于环境的组件的集成

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，是决策后开发阶段发布的输入。

7.2　目标

本章的目标是：

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）执行信息安全评估，如果适用；

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。

7.3　输入

7.3.1　先决条件

无。

7.3.2　更多支持信息

可以考虑以下信息：

-组织的信息安全审核报告[WP-05-03]；

-项目计划。

7.4　要求和建议

7.4.1　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以转移，前提是要进行交流并移交相关信息。

7.4.2　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 ）该模块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 7.4.3 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：

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：信息安全计划可以在配置管理下包含与其他计划（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、10、11 和 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-06-07]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：信息安全计划可以在开发过程中逐步完善。例如，信息安全计划可以根据信息安全活动的结果进行更新，如 TARA（见第 16 章）。

[PM-06-08]对于根据本文件 16.8 的分析确定的风险值为 1 的威胁场景，可以省略与 10.5、11 和 12 章的符合性。

注 5：威胁情况可能会对信息安全产生影响，如果产生影响，则对相应的风险进行处理。

注 6：可以根据信息安全档案中定义的基本原理来论证对此类风险的处理是否充分，基本原理可以基于质量管理标准的符合性，如 IATF 16949 与 ISO 9001 相结合，并结合其他措施，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 16 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 6.4.4 的规定，接收配置管理和文件管理。

[RQ-06-12]按照 6.4.6 的规定，信息安全计划中确定的工作成果，应接受配置管理、变更管理、需求管理和文件管理。

7.4.3 裁剪

[PM-06-13]信息安全活动可以被裁剪。

[RQ-06-14]如果信息安全活动被裁剪了，应提供并审查基本原理，用来证明可以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以导致联合裁剪。

7.4.4 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），A 可作为复用分析的结果而改变。

图 5　复用分析示例

c）计划在不变更的情况下复用，并且有关模块或组件的信息也有相应的变化，

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：变更可以包括设计变更和/或实施变更：

-设计变更可以来自需求变更，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。

7.4.5　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。

7.4.6　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）适合于预期用途的特定应用环境；

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。

7.4.7 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论据，并有工作成果加以支持。

注 1：证据可以隐含的（例如，如果从已编译的工作成果集中可以看出该证据，则可以省略这部分证据）。

注 2：在分布式开发中，相关项的信息安全档案可以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。相关项的整体论据由各方的论据共同支持。

注 3：信息安全档案需考虑后开发的信息安全需求[WP-10-02]。

7.4.8 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，可将基本原理记录在信息安全档案中。

[RQ-06-25] [RQ-06-24]的基本原理应独立评审。

注 3：独立方案可基于 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 说明了组织信息安全审核、项目级信息安全评估和其他信息安全活动之间的关系。

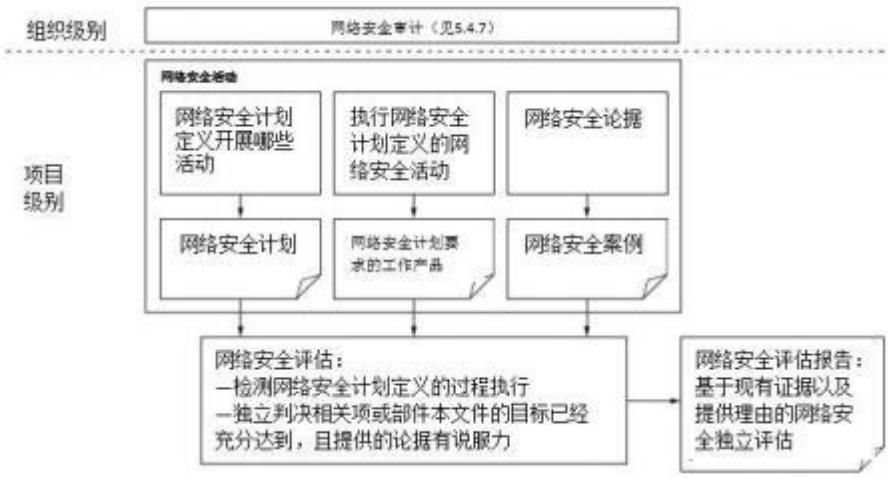

图 6 与其他信息安全活动有关的信息安全评估

注 6：信息安全评估可以逐步进行，以尽早解决已发现的问题。

注 7：信息安全评估可以重复或补充；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。

[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：独立方案可基于 GB/T 34590 系列标准。

例：来自于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：合理性和有效性可以通过使用先前为验证目的而进行的评审来判断。

d）证明已达到本文件目标的基本原理（如果提供）；

注 10：考虑到[PM-06-13]，工作成果的创建负责人可以提供一个基本原理，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：评估报告也可以包括持续改进建议。

[RQ-06-32]如果提出了根据[PM-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。

7.4.9 后开发的发布

[RQ-06-33]下列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）通过信息安全评估确认信息安全档案，如果适用；

b）后开发阶段的信息安全需求被接受。

7.5 工作成果

[WP-06-01]根据 7.4.1 至 7.4.6 的要求制定的信息安全计划。

[WP-06-02]根据 7.4.7 的要求制定的信息安全档案。

[WP-06-03]根据 7.4.8 的要求得出的信息安全评估报告（如适用）。

[WP-06-04]根据 7.4.9 的要求得出的用于后开发阶段的发布报告。

8 分布式信息安全活动

8.1 总则

如果相关项或组件信息安全活动的责任是分布式的，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-供应商间的交互；

c) 客户-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以采用同样的方式进行管理。

示例：一个 1 级供应商是某 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。

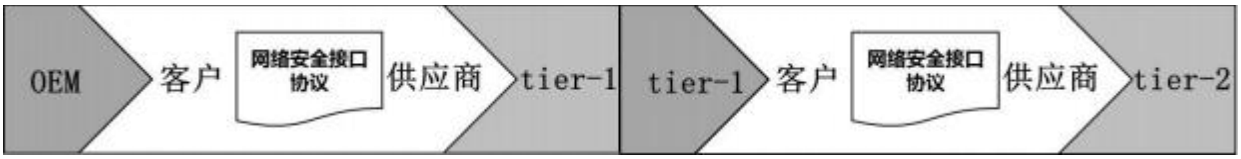

图 7　供应链中客户/供应商关系的用例

8.2　目标

本章的目标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。

8.3　输入

无。

8.4　要求和建议

8.4.1　供应商的能力

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

注 1：该评价可用来支持供应商的选择，可以依据本文要求的能力，也可以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] 供应商应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 9 章）和信息安全事件响应（见第 14 章）的证据；

-以往信息安全评估报告的总结。

8.4.2　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。

例：关于消息认证的信息安全需求。

8.4.3　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；

例 1：客户执行整车层面的信息安全确认。

例 2：后开发阶段的信息安全活动的分布。

例 3：供应商、客户或者第三方可以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：共享的信息可以包含：

-分发、评审和发生信息安全问题时的反馈机制；

-信息共享策略；

-漏洞和其他信息安全相关发现的信息交换流程，例如，关于风险；

-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讯网络的安全防护；

-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：可以使用 RASIC 表，参见附录 C。

8.5 工作成果

[WP-07-01]由 8.4.3 的要求产生的信息安全接口协议。

9 持续的信息安全活动

9.1 总则

持续的信息安全活动可以在全生命周期的每一个阶段进行，也可以在项目之外进行。

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。

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。

漏洞分析检查弱点，并评估该弱点是否可被用于发动攻击。

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。

9.2 目的

本章节的目的包括：

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。

9.3 信息安全监测

9.3.1 输入

9.3.1.1 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。

9.3.1.2 附加支持资料

可以考虑以下信息：

-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]；
-过去的漏洞分析结果[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。

9.3.2 要求和建议

[RQ-08-01]应选择信息安全情报收集的来源。
注 1:可以选择外部和/或内部的来源；
注 2:内部来源可以包括列在 9.3.1.2 的来源；
注 3:外部来源可以包括：
-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:触发器可以包括关键字、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。

9.3.3 工作成果

[WP-08-01]来自[RQ-08-01]的信息安全情报来源。
[WP-08-01]来自[RQ-08-02]的触发器。
[WP-08-03]来自[RQ-08-03]的信息安全事态。

9.4 信息安全事态评估

9.4.1 输入

9.4.1.1 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。

9.4.1.2 附加支持资料

可以考虑以下信息：
-相关项定义[WP-09-01]；
-信息安全规范[WP-10-01]；
-过去的漏洞分析结果[WP-08-05]；

9.4.2 要求和建议

[RQ-08-04]应评估信息安全事态， 以识别相关项和/或组件中的弱点。
注 1：此活动可与[RQ-08-03]中的触发器相结合使用；
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），则组织可以将该补救措施作为无需任何其他活动的漏洞来处理。
注 3:可根据此评估结果更新威胁场景[WP-15-03]。

9.4.3 工作成果

[WP-08-04]由[RQ-08-04]产生的信息安全事态的弱点。

9.5 漏洞分析

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]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。

9.5.1.2 附加支持资料

可以考虑以下信息：

—[WP-08-04]信息安全事态中的弱点。

—产品开发[WP-10-05]过程中发现的弱点。

—过去的漏洞分析结果[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。

9.5.2 要求和建议

[RQ-08-05]应分析弱点以识别漏洞。

注 1：该分析可包括：

—架构分析；

—根据 16.6 进行的攻击路径分析

—根据 16.7 进行的攻击可行性定级

注 2：可以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。

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。

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。

9.5.3 工作成果

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

9.6 漏洞管理

9.6.1 输入

9.6.1.1 先决条件

应提供以下信息：

-漏洞分析结果[WP-08-05]；

注：如果对相关项执行脆弱性分析，则使用相关项的定义;如果对组件执行脆弱性分析，则使用网络安全规范。

9.6.1.2 附加支持资料

无。

9.6.2 要求和建议

[RQ-08-07]应对漏洞进行管理，以便针对每个漏洞开展以下工作：

a) 相应的信息安全风险按照 16.9 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，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:有关漏洞的信息可以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），也可以分享给其他相关方。

[RQ-08-08]如果根据 16.9 的风险处置决策需要进行信息安全事件响应，则应参照 14.3。

注 3:信息安全事件响应流程可以独立于 TARA。

9.6.3 工作成果

[WP-08-06]由[RQ-08-07]产生的漏洞管理证据。

10 概念阶段

10.1 总则

概念阶段涉及到整车级别功能在相关项中实施的考虑。在本章节中，相关项及其操作环境被识别为“相关项定义”，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，这是最高级别的要求。为此，通过第 16 章（见附录 H，图 H.1）的方法完成信息安全风险评估。此外，10.4 规定了信息安全声明，用于解释风险保留和分担的充分性。

信息安全概念由信息安全需求和对操作环境的要求组成，基于信息安全目标以及相关项而形成。

10.2 目的

本章节的目的是：

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。

10.3 相关项定义

10.3.1 输入

10.3.1.1先决条件

无。

10.3.1.2进一步的支持信息

考虑信息如下：

-有关该相关项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，参考模型和前期开发文档。

10.3.2 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：相关项边界将项目与其操作环境区分开来。相关项边界的描述可包括与车辆内部其他相关和/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[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 功能安全系列标准。

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以基于对一个假定的（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，可以识别或分析相关的威胁情景和攻击路径。

注 8：相关信息包括假设，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。

10.3.3 工作成果

[WP-09-01]相关项定义， 由 10.3.2 的要求得出。

10.4 信息安全目标

10.4.1 输入

10.4.1.1先决条件

应提供以下信息：

-相关项定义[WP-09-01]。

10.4.1.2进一步的支持信息

可考虑以下信息：

-信息安全事态[WP-08-03]。

10.4.2 要求和建议

[RQ-09-03]应根据相关项定义进行分析，其中包括：

根据 16.3 的规定进行资产识别；

a）根据 16.4 的规定进行威胁场景识别；

b）根据 16.5 的规定，影响评级；

c）根据 16.6 的规定，进行攻击路径分析；

d）根据 16.7 的规定，对攻击可行性进行评级；

e）根据 16.8 的规定，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 的规定为每种威胁场景确定风险处理方案。

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，可以为信息安全目标确认一个 CAL（见附录 E）。

注 5：可以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：

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，则应指定一个或多个相应的信息安全声明；

注 6：信息安全声明可被考虑用于信息安全监测。

[RQ-09-07] 应进行验证以确认满足下列要求：

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）该相关项[RQ-09-05]的所有信息安全目标和[RQ-09-06]的信息安全声明的一致性。

10.4.3 工作成果

[WP-09-02]由[RQ-09-03]和[RQ-09-04]的要求得出 TARA。

[WP-09-03]由[RQ-09-05]的要求得出信息安全目标。

[WP-09-04]由[RQ-09-06]的要求得出信息安全声明。

[WP-09-05]由[RQ-09-07]的要求得出信息安全目标的验证报告。

10.5 信息安全概念

10.5.1 输入

10.5.1.1先决条件

应获得下列信息：

-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]。

10.5.1.2进一步的支持信息

可考虑下列信息：

-威胁分析和风险评估[WP-09-02]。

10.5.2 要求及推荐

[RQ-09-08] 应考虑以下因素，描述达成信息安全目标而采取的信息安全控制和/或运行控制措施，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：这些描述可用来评估设计， 并确定信息安全确认的目标。

[RQ-09-09] 相关项的信息安全需求及操作环境需求，应按照[RQ-09-08]的描述，为实现信息安全目标而进行定义。

注 3：信息安全需求取决于并包括：相关项的特定功能，例如： 升级能力或在运行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它相关项的需求，可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，分配到其一个或者多个组件。

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] and [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。

10.5.3 工作成果

[WP-09-06]来自[RQ-09-08], [RQ-09-09] 和 [RQ-09-10]的信息安全概念。

[WP-09-07]由[RQ-09-11]产生的信息安全概念验证报告。

11　产品研发

11.1　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。

迭代执行这些信息安全活动，直到信息安全控制不需要进一步细化。通过验证活动定义并确认信息安全规范，以实现信息安全概念。

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。

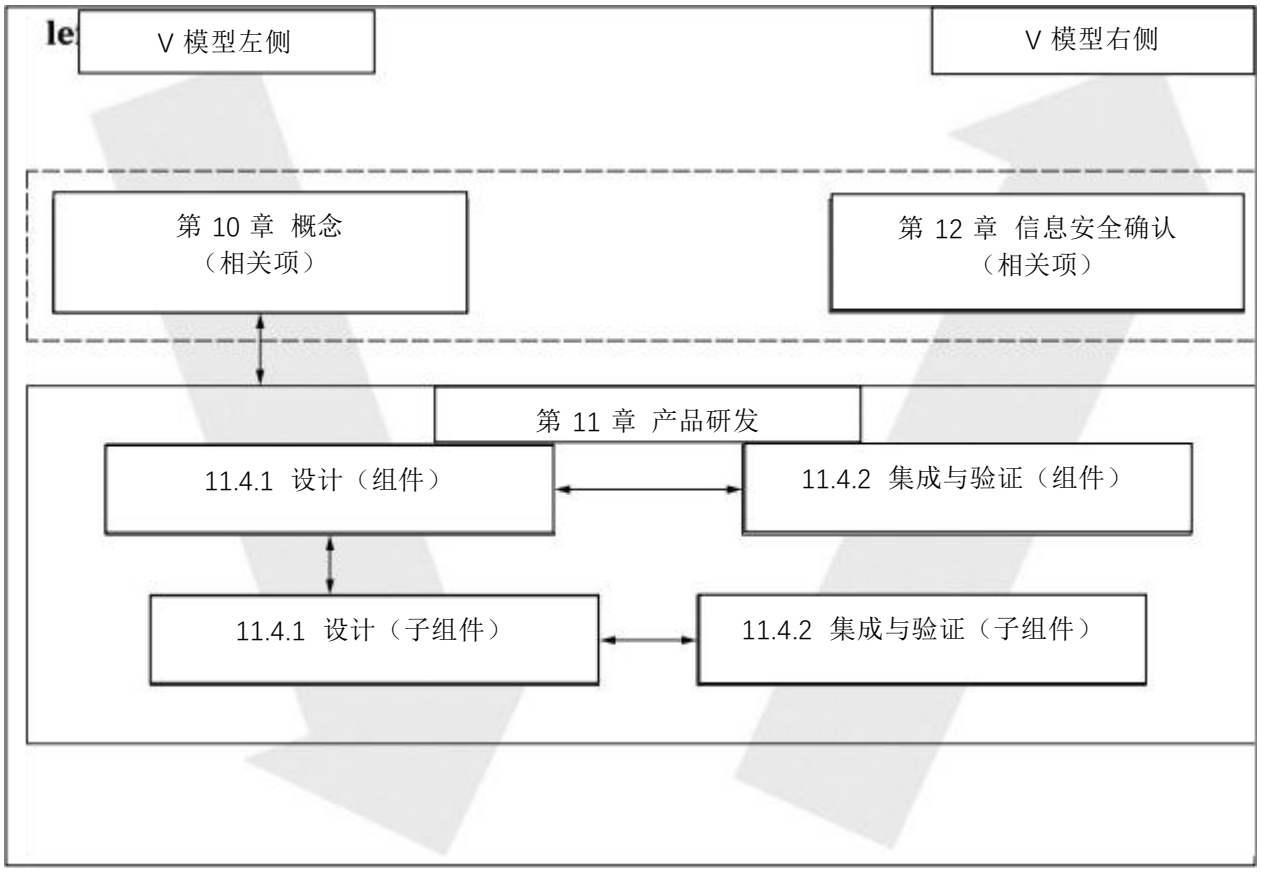

图 8　V 模型中的产品开发示例

纵向双向箭头指明，按照 11.4.1 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 11.4.2 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，也可应用不同于 V 模型的开发方法，如：敏捷软件开发。

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

11.2　目标

本章目标如下：

a) 定义信息安全规范；

注：这些可以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；

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。

11.3 输入

11.3.1 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：这可以仅限于与正在开发的组件相关的信息，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。

11.3.2 更多支持信息

可以考虑以下信息：

—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。

11.4 要求和建议

11.4.1 设计

[RQ-10-01] 定义信息安全规范应基于：

a）更高层级抽象架构的信息安全规范；

b）选择实施的信息安全控制（如果适用）；

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：可以从受信任目录中选择信息安全控制。

C）现有的架构设计，如果适用。

注 2：信息安全规范覆盖所定义的架构设计与所定义的信息安全需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：在定义信息安全规范时，可以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：信息安全规范可以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值范围，例如硬件安全模块的正确配置。

注 5：可以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，应指定组件开发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其实施使用设计、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，以及

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] 适用于信息安全的设计、建模或编程语言的标准（见[RQ-10-04]），语言本身并未涉及，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 CERT C 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] 应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 卷附录 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：可以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并管理识别的漏洞。 但是，可以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：验证方法可以包括：

—评审；

—分析；

—模拟；

—原型法。

11.4.2 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] 指定[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) 用于批量生产的配置，如果适用；

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) 符合[RQ-10-05]的建模、设计和编码指南，如果适用。

注 1：可以包括车辆的集成和测试。

注 2：验证方法可以包括：

—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以考虑：

—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以包括：

—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，已识别的弱点可以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；和/或

—组件的简单性。

11.5 工作成果

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

[WP-10-02] 由[RQ-10-03]产生的后开发阶段的信息安全需求。

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

[WP-10-04] 由[RQ-10-08]产生信息安全规范的验证报告。

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

[WP-10-06] 由[RQ-10-10]产生的集成和验证规范。

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

12 信息安全确认

12.1 概述

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。应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。

12.2 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。

12.3 输入

12.3.1 先决条件

应提供下列信息:

—相关项定义(参阅[WP-09-01])；

—信息安全目标 (参阅[WP-09-03])；

—信息安全声明(参阅[WP-09-04])，如果适用。

12.3.2 进一步的支持信息

应提供下列信息：

—信息安全概念(参阅[WP-09-06])；

—产品开发的工作成果（见 10.5）。

12.4 要求和建议

[RQ-11-01] 考虑批量生产配置状态下，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信息安全目标未解决任何风险,则可以按照 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) 操作环境要求的有效性，如果适用。

注 2：确认活动应包括：

—通过审查 9.5 和 10 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 9 和10 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并管理已识别的漏洞。

[RQ-11-02] 应提供选择确认活动的理由。

12.5 工作成果

[WP-11-01] 由[RQ-11-01]和[RQ-11-02]产生的确认报告。

13 生产

13.1 总则

生产包括了相关项或组件在整车级的制造、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。

13.2 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。

13.3 输入

13.3.1 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])。

13.3.2 进一步的支持信息

无。

13.4 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；

例 1：可以防止对运行软件的生产服务器进行物理访问的物理控制。

例 2：可以运用密码学技术和/或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：方法可以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，生产过程可以使用特权访问；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。

13.5 工作成果

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

14 运行和维护

14.1 总则

本章描述了信息安全事件响应和对既定领域的相关项或组件的更新。

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。

更新是在开发后对一个相关项或组件所做的改变，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而不是本章涵盖。

14.2 目标

本章的目标是：

a）确定并实施信息安全事件的补救措施；

b）在生产后的相关项或组件的更新期间和更新后保持信息安全，直到其信息安全支持结束。

14.3 信息安全事件响应

14.3.1 输入

14.3.1.1先决条件

无。

14.3.1.2进一步的支持信息

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]。

14.3.2 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：沟通计划的建立可以涉及内部各相关方，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（如开发、研究人员、公众、当局），并为这些群体共享具体信息。

c）为补救措施分配的责任；

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（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：可以根据 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，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。

14.3.3 工作成果

[WP-13-01]由[RQ-13-01]产生的信息安全事件响应计划。

14.4 更新

14.4.1 输入

14.4.1.1先决条件

应提供以下信息：

—发布的后开发阶段报告[WP-06-04]。

14.4.1.2进一步的支持信息

可以考虑以下信息：

—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]。

14.4.2 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。

14.4.3 工作成果

无。

15 信息安全支持终止和报废

15.1 综述

报废与信息安全支持终止是不同的。组织可以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以在既定领域按设计运行。报废和信息安全支持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。

报废可以在组织不知情的情况下发生，而且报废程序无法执行，因此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。

15.2 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。

15.3 信息安全支持终止

15.3.1 输入

无。

15.3.2 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客户传达信息。

15.3.3 工作成果

［WP-14-01］由［RQ-14-01］产生的信息安全支持终止沟通程序。

15.4 报废

15.4.1 输入

应提供以下信息:

—后开发阶段的信息安全需求［WP-10-02］。

15.4.1.1进一步的支持信息

无。

15.4.2 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(如操作说明、用户手册)，可以使信息安全方面的报废得以进行。

15.4.3 工作成果

无。

16 威胁分析和风险评估方法

16.1 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。本章中描述的方法和工作成果统称为威胁分析和风险评估(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，可以从相关项或组件生命周期中的任何节点系统地调用：

—资产识别；

—威胁场景识别；

—影响评级；

—攻击路径分析；

—攻击可行性评级；

—风险值计算；

—风险处置决策。

由于这些是通用模块，本章中定义的工作成果被记录在由其他章产生的工作成果中的一部分。参见附录 H 提供了这些方法的实例说明。组织用于影响评级、攻击可行性评级和风险值计算的特定等级可以应用并映射到本文件中定义的相应等级。

16.2 目标

本章的目标：

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)确定攻击路径可以被利用的容易程度；

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；

16.3 资产识别

16.3.1 输入

16.3.1.1先决条件

应提供以下信息：

—相关项定义[WP 09-01]。

16.3.1.2附加支持资料

参考以下信息：

—信息安全规范[WP-10-01]。

16.3.2 要求和建议

[RQ-15-01] 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] 识别具有信息安全属性的资产，资产的信息安全属性达不到标准将导致危害场景。

注 2：确定资产可以基于：

— 分析相关项定义；
— 执行影响评级；
— 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），资产的信息安全属性为保密性。危害场景是由于资产失去保密性，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，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）。

16.3.3 工作成果

[WP-15-01] 由[RQ-15-01]产生的危害场景；

[WP-15-02] 由[RQ-15-02]产生的具有信息安全属性的资产。

16.4 威胁场景识别

16.4.1 输入

16.4.1.1先决条件

应提供以下信息：

—相关项定义[WP-09-01]。

16.4.1.2附加支持资料

参考以下信息：

—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]。

16.4.2 要求和建议

[RQ-15-03]识别威胁场景，威胁场景包含：

—目标资产；

—资产受损害的信息安全属性；

—信息安全属性受损害缺失的原因；

注 1：附加信息可以包含或与威胁场景相关联，例如威胁场景、危害场景、资产、攻击者、方法、工具和攻击面之间的技术依赖关系。

注 2：威胁场景识别方法可以使用小组讨论或系统方法，例如：

—引发由合理可预见的滥用或滥用导致的恶意使用案例：

—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 3：一个危害场景可以对应多个威胁场景，一个威胁场景可以导致多个危害场景。

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。

16.4.3 工作成果

[WP-15-03] 由[RQ-15-03]产生的威胁场景。

16.5 影响评级

16.5.1 输入

16.5.1.1先决条件

应提供以下信息：

—危害场景[WP-15-01]。

16.5.1.2 **附加支持资料：**

参考以下信息：

—相关项定义[WP-09-01]:

—具有信息安全属性的资产[WP-15-02]。

16.5.2 **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、运营和隐私（S,F,0,P）等方面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（如权重）。

注 2：其他影响类别也可以参考。

注 3：如果参考其他影响类别，则可根据第 7 条在供应链中分享这些类别的基本原理和解释。

[RQ-15-05] 危害场景的影响等级应确定为以下影响等级之一：

—严重；

—重大；

—中等；

—忽略。

注 4：财务、运营和隐私相关影响可根据附录 F 中提供的表格进行评级。

[RQ-15-06] 安全相关影响评级来自 GB/T 34590.3-2022，6.4.3

注 5：附录 F 中的表 F.1 可用于将安全影响准则映射到影响等级。

注 6：功能安全评估可为此目的重复使用。

[PM-15-07] 若一个危害场景导致了一个影响等级，并且可以认为另一个影响不重要，则可以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，不进一步分析该危害场景的财务影响。

16.5.3 **工作成果**

[WP-15-04]由[RQ-15-04]至[RQ-15-06]产生的具有相关影响类别的影响评级。

16.6 **攻击路径分析**

16.6.1 **输入**

16.6.1.1**先决条件**

提供以下信息：

—相关项定义[WP-09-01]或者信息安全规范[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]；

16.6.1.2 **附加支持资料：**

参考以下信息：

—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;

—前期已识别的攻击路径[WP-15-05]，如果可用；

—漏洞分析[WP-08-05]

16.6.2 **要求和建议**

[RQ-15-08] 分析威胁场景，确定攻击路径。

注 1：攻击路径分析基于：

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

—自下而上的方法，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，则可以停止对该部分攻击路径的分析。

[RQ-15-09] 攻击路径与可实现攻击路径的威胁场景相关联。

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。在产品开发的早期阶段，还无法识别特定的漏洞，攻击路径通常是不完整或不精确的，因为具体的实现细节尚不清楚。在产品开发过程中，攻击路径可以随着更多信息的可用而更新，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：

ⅰ.利用蜂窝接口损害远程通信 ECU：

ii.利用远程通信 ECU 的 CAN 通信损害网关 ECU；

iii.网关 ECU 转发恶意制动请求信号（不必要的快速减速）。

16.6.3 工作成果

[WP-15-05] 由[RQ-15-08]和[RQ-15-09]产生的攻击路径。

16.7 攻击可行性评级

16.7.1 输入

16.7.1.1先决条件

提供以下信息：

—攻击路径[WP-15-05].

16.7.1.2附加支持资料

参考以下信息：

—架构设计；

—漏洞分析[WP-08-05]；

16.7.2 要求和建议

[RQ-15-10] 对于每条攻击路径，攻击可行性等级应按表 1 所述确定。

表 1-攻击可行性评级和相应描述

攻击可行性评级	描述
高	攻击路径可以用低工作量完成。
中	攻击路径可以通过中等工作量完成。
低	攻击路径可以用高工作量完成
非常低	攻击路径可以用非常高的工作量来完成

[RC-15-11] 攻击可行性评级方法应根据以下方法之一确定：

a）基于攻击潜力的方法；

b) 基于 CVSS 方法；

C）基于攻击向量方法；

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，则应根据核心要素确定攻击可行性等级，包括：

a) 运行时间；

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:核心攻击潜在因素可以从 ISO/IEC 18045 中得出。

注 3 附录 G.2 提供了基于攻击潜力来确定攻击可行性的指南。

[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：附录 G.3 提供基于 CVSS 的方法来确定攻击可行性的指南。

[RC-15-14] 如果使用基于攻击向量的方法，则应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：附录 G.4 提供了基于攻击矢量的方法来确定攻击可行性的指南。

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，一种基于攻击矢量的方法可以适合于估计攻击的可行性。

16.7.3 工作成果

[WP-15-06] 由[RQ-15-10]产生的攻击可行性评级。

16.8 风险值确定

16.8.1 输入

16.8.1.1先决条件

提供以下信息

—威胁场景[WP-15-03]；

—具有相关影响类别的影响评级[WP-15-04]；

—攻击可行性评级[WP-15-06]。

16.8.1.2附加支持资料

无。

16.8.2 要求和建议

[RQ-15-15] 对于每个威胁场景，应根据相关危害场景的影响和相关攻击路径的攻击可行性计算风险值。

注 1：如果威胁场景对应于多个危害场景或相关危害场景具有多个影响类别的影响，则可以为每个影响等级分别确定单独的风险值。

注 2：如果威胁场景对应于多条攻击路径，则可以适当聚合相关的攻击可行性评级，例如，威胁场景被分配了相应攻击路径的最大攻击可行性评级。

[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。

16.8.3 工作成果

[WP-15-07] 由[RQ-15-15] 和[RQ-15-16]产生的风险值。

16.9 风险处置决策

16.9.1 输入

16.9.1.1先决条件

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]。

16.9.1.2附加支持资料

参考以下信息：
—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；
—具有影响类别的影响评级[WP-15-04]；
—攻击路径[WP-15-05]；
—攻击可行性等级[WP-15-06]。

16.9.2 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，确定一个或多个风险处置决策：

a) 避免风险；

示例 1：消除风险源避开风险，决定不开始或不继续增加风险的活动。

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 条进行信息安全监测和漏洞管理。

16.9.3 工作成果

[WP-15-08] 由[RQ-15-17]产生的风险处置决策。

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产品的摘要。这可以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，这些活动的工作产品都在信息安全评估的范围内。第 15 章列出的所有工作产品在其他章节中被记录为工作产品。

A.2 信息安全活动和工作产品概述

表 A.1 -本文件的信息安全活动和工作成果

子章	工作成果
组织信息安全管理	
6.4.1 信息安全治理	[WP-05-01]信息安全政策、规则和程序
6.4.2 信息安全文化	[WP-05-01]信息安全政策、规则和程序 [WP-05-02]能力管理、意识管理和持续改进的证据
6.4.3 信息共享	[WP-05-01]信息安全政策、规则和程序
6.4.4 管理系统	[WP-05-03]组织管理制度的证据
6.4.5 工具管理	[WP-05-04]工具管理的证据
6.4.6 信息安全管理	[WP-05-03]组织管理制度的证据
6.4.7 组织信息安全审计	[WP-05-05]组织信息安全审计报告
依靠项目的信息安全管理	
7.4.1 信息安全责任	[WP-06-01]信息安全计划
7.4.2 信息安全规划	[WP-06-01]信息安全计划
7.4.3 裁剪	[WP-06-01]信息安全计划
7.4.4 再利用	[WP-06-01]信息安全计划
7.4.5 超出背景的组件	[WP-06-01]信息安全计划
7.4.6 现有组件	[WP-06-01]信息安全计划
7.4.7 信息安全案例	[WP-06-02]信息安全案例
7.4.8 信息安全评估	[WP-06-03]信息安全评估报告
7.4.9 后续开发的发布	[WP-06-04]开发后报告的发布
分布式信息安全活动	
8.4.1 供应商能力	无
8.4.2 报价要求	无
8.4.3 责任的统一	[WP-07-01]信息安全接口协议
持续的信息安全活动	
9.3 信息安全监测	[WP-08-01]信息安全信息的来源 [WP-08-02]触发器 [WP-08-03]信息安全事态
9.4 信息安全事件评估	[WP-08-04]来自信息安全事态的弱点
9.5 脆弱性分析	[WP-08-05]漏洞分析
9.6 脆弱性管理	[WP-08-06]管理漏洞的证据
概念阶段	
10.3 项目定义	[WP-09-01]相关项定义
10.4 信息安全目标	[WP-09-02]TARA

	[WP-09-03]信息安全目标 [WP-09-04]信息安全要求 [WP-09-05]信息安全目标的验证报告
10.5 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	
11.4.1 设计	[WP-10-01] 信息安全规范 [WP-10-02] 开发后的信息安全要求 [WP-10-03] 建模、设计或编程语言和编码准则的文件化 [WP-10-04] 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
11.4.2 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
12 信息安全的确认	[WP-11-01] 确认报告
开发后阶段	
13 生产	[WP-12-01] 生产控制计划
14.3 信息安全事件应对	[WP-13-01] 信息安全事件响应计划
14.4 更新	无
15.3 结束信息安全支持	[WP-14-01] 信息安全支持终止沟通程序
15.4 停用	无
威胁分析和风险评估方法	
16.3 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
16.4 威胁情景识别	[WP-15-03] 威胁场景
16.5 冲击等级	[WP-15-04] 具有影响类别的影响评级
16.6 攻击路径分析	[WP-15-05] 攻击路径
16.7 攻击可行性评级	[WP-15-06]攻击可行性等级
16.8 风险值的确定	[WP-15-07]风险值
16.9 风险处置决策	[WP-15-08]风险处置决策

附 录 B
（资料性附录）
信息安全文化示例

表 B.1- 信息安全文化薄弱和强大的示例

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，并处罚走因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当地、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， 以良好的适当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； 没有为在用车市场上潜在的弱点或事件做好准备； 只有当生产中、在用车市场上发生信息安全事件，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市场上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。
“群体思维 ”确认偏差（即不加批判的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； 在在用车市场、制造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。
过程是临时的或含蓄的。	遵循明确的、可追踪的和可控的过程。

附 录 C
（资料性附录）
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。

本附件按照[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。

模板还加入了其他信息，如联系人、 目标里程碑、协作方法和工具等。

C.2 示例模板

本示例模板中的列项包括:

a)阶段：本文件的阶段；

b)工作成果：本文档与分布式活动接口相关的工作成果物；

c)参考章：在本文档中的相关章；

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 6.4.3 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。

阶段	工作成果	参考章	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	项目定义													
	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													

图 C.1 信息安全接口协议模版示例

附 录 D
（资料性附录）
信息安全的相关性—判定方法和准则示例

D.1 目的

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

D.2 方法

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

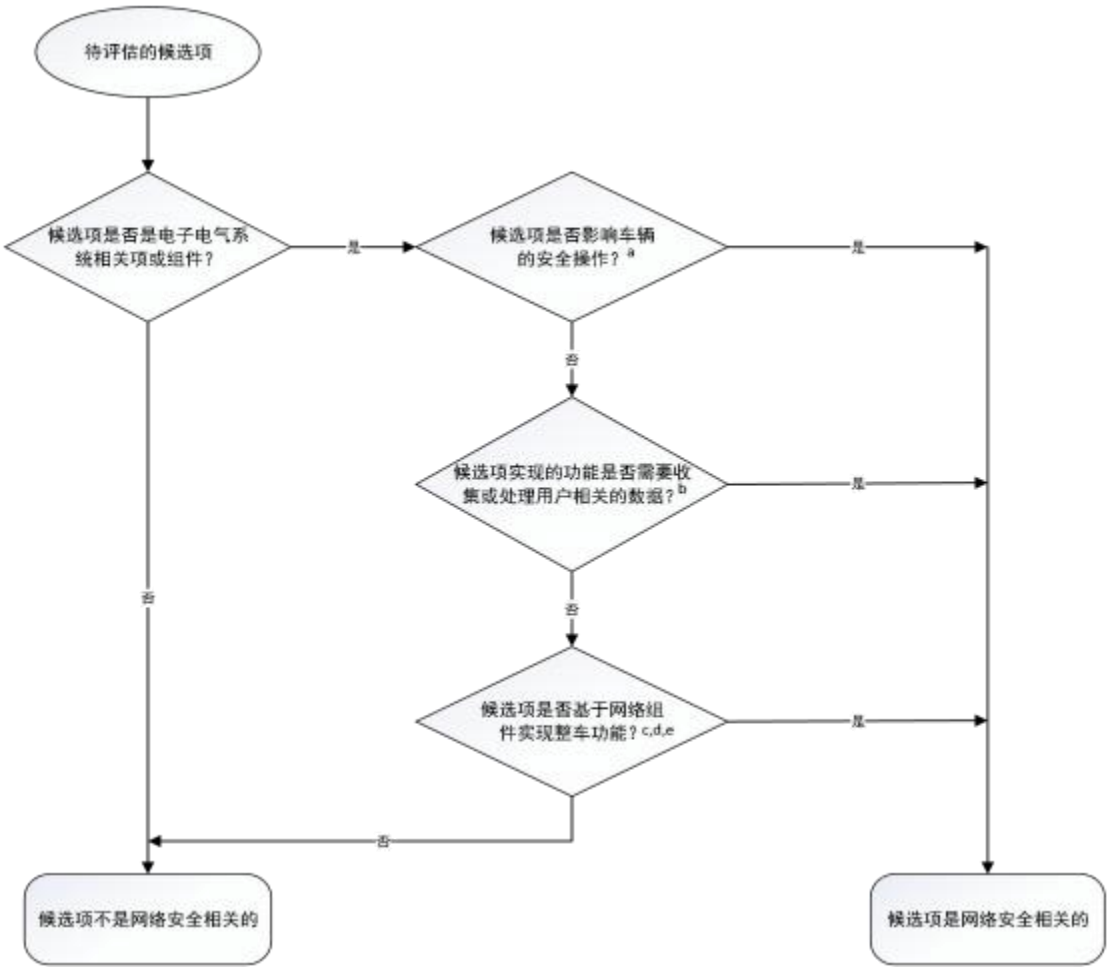

图 D.1 信息安全相关性判定方法

准则示例如下：

a)运动控制模块和具有汽车安全完整性等级(ASIL)的模块。

b)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)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)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)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)。

信息安全的相关性也可以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
（资料性附录）
信息安全保障等级

E.1 总则

本附件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，但是它可以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 可以由开发项目的组织确定，也可以由开发组件的组织另行假设。

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。这可以通过将 CAL 作为信息安全目标的一个属性来实现，这种属性可以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，将在一段时间内保持固定。因此，在考虑实施信息安全控制之前，可以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。

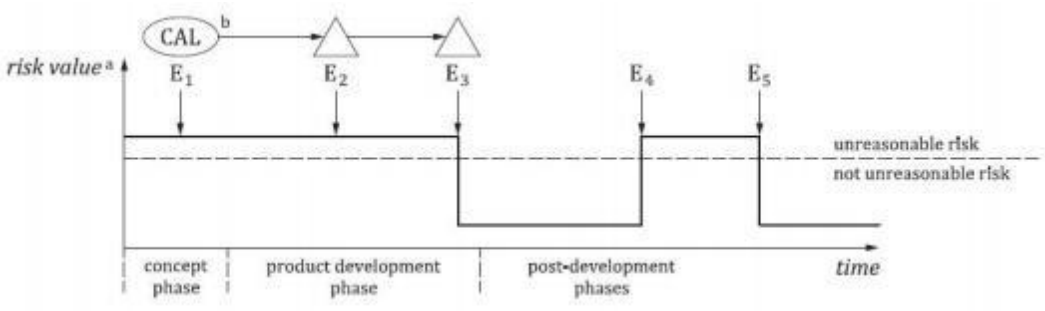

图 E.1 CAL 和风险之间的关系

关键要素

E1 事件 1:信息安全要求被明确。

E2 事件 2:信息安全控制得到实施。

E3 事件 3:测试表明信息安全控制是有效的。

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 被应用于信息安全活动中。

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 的后续信息安全活动的严格程度。

可以根据对已确定的威胁场景的考虑来确定 CAL（见 16.4）。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信息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 分类方案和确定的 CAL 也可以成为客户和供应商之间信息安全接口协议的一部分。

可以为一个项目的所有信息安全目标分配一个 CAL,也可以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 一般考虑

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）信息安全评估的方法。

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、E.3 和 E.4 中的例子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-信息安全保障措施中 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， 以确保未成年的漏洞不存在。	c）独立计划， 以提供对所进行的信息安全活动适当的信心

CAL1	需要低到中度信息安全保障	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
CAL2	需要有适度的信息安全保障			信息安全评估是由不同于发起人的人进行的
CAL3	需要中度至高度的信息安全保障	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	信息安全评估是由与发起人不同的团队中的人进行的
CAL4	需要高度的信息安全保障	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

本小节提供了一个例子,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；

c）如果该组件被确认为受架构中其他组件的保护，则可以根据理由减少或放弃不必要的 CAL 使用在该组件上。

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 CAL 的方法和度量。

在产品开发中，如果信息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信息安全要求的最高 CAL 来开发组件。

表 E.3 和 E.4 提供了如何将 CAL 应用于信息安全活动的例子；可以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--信息安全活动的独立程度示例

活动	要求	独立性水平适用				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造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造及考虑此工作产品的团队的人执行的，如：由一个向不同的直接上级报告的人执行； 以及 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] [RQ-11-01]	T1	T1	T2	T2	适用于信息安全要求中最高的 CAL
漏洞扫描	[RC-10-12] [RQ-11-01]	T1	T1	T1	T1	
模糊测试	[RC-10-12] [RQ-11-01]	——	T1	T2	T2	
渗透测试	[RC-10-12] [RQ-11-01]	——	——	T1	T2	

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/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、相关项或组件的知识和/或资源更高。

附 录 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 16.5）,涉及安全、财务、运营和隐私的损害情况。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，但可以酌情添加到具体组织的评级标准中。

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
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：S0 的评级可基于 GB/T 34590.3-2022,表 B.1。	

安全影响评级标准取自 GB/T 34590.3-2022。

如果提供理由，也可以考虑按照 GB/T 34590.3-2022 的可控性和暴光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
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 -业务影响评级标准示例

影响评级	业务影响评级的标准
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。 例 1 车辆不工作或出现核心功能的意外行为，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。 例 2 司机的重大烦扰。
普通的	操作上的损坏导致了车辆功能的部分退化。 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
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 PII 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: 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。
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 PII 主体联系起来； b）不敏感，但很容易与 PII 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 PII 主体联系起来。

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

附 录 G
（资料性附录）
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 16.7）：
—基于攻击潜力；
—基于 CVSS；
—基于攻击向量。
攻击可行性评级中可以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。
本节给出了一些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，该评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

≤ 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有关，与他们的技能和经验有关，见表 G.2。

表 G.2 — 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。

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。 例 2：有经验的业主，普通技术人员知道简单和流行的攻击，如里程表调整，安装假冒零件。
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。 例 3：有经验的技术人员或工程师。
多个专家： 一个攻击的不同步骤需要专家级别的不同专业知识。 例 4：多名经验丰富的工程师，他们在不同领域拥有专业知识，一个攻击的不同步骤需要他们的专业知识。

G.2.2.3 自定义相关项或组件的知识示例

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

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）。 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）。 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）。 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，访问是非常严格的控制在一个严格的需要知道的基础和个人许诺上）。 例 4：由制造商和/或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（如逻辑和物理）和访问持续时间（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、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

无限：

通过公共/不受信任的网络的高可用性，没有任何时间限制。（即，资产总是可访问的）。 没有物理存在或时间限制的远程访问，以及对相关项或组件的无限物理访问。 例 1：无任何先决条件的远程攻击（例如，车联网或蜂窝接口），所有者对芯片调试的无限物理访问。
容易： 高可用性和有限的访问时间。没有物理存在的远程访问相关项或组件。 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。有限的物理和/或逻辑访问。不使用任何特殊工具直接进入车辆内部或外部。 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。对执行攻击的相关项或组件的不切实际的访问。 例 4：破解 IC 以提取信息，暴力破解密钥的速度比密钥旋转的速度快。

G.2.2.5 自定义设备示例

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

标准设备： 攻击者随时可以获得设备。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）。 例 1：笔记本电脑，CAN 适配器，车载诊断软件保护器，普通工具（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以获得。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就属于这一类），或开发更广泛的攻击脚本或程序。如果攻击的不同步骤需要不同的由专门设备组成的测试台，这将被认为是定制设备。 例 2：专业硬件调试设备、车载通信设备（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(如非常复杂的软件)，公众不容易获得(如黑市)，或者设备非常专门化，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。 例 3：厂家限制的工具，电子显微镜。
多种定制设备： 引入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，可以定义数值。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	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

为了评估信息技术安全的漏洞，可以使用事件响应与安全团队论坛（FIRST）维护的 CVSS。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（如影响度量）有本文档的各个方面覆盖，如危害场景和影响评估。

可利用性度量是：

a) 攻击向量；

b) 攻击复杂性；

c) 权限要求；

d) 用户交互。

它们由 FIRST 描述。CVSS 度量的评估根据预先定义的范围为每个度量产生数值。整体可利用性值可以用一个简单的公式来计算：

$E = 8.22 \times V \times C \times P \times U$

其中，

E 为可利用性值；

V 为与攻击向量相关的数值，范围从 0.2 到 0.85；

C 为与攻击复杂性相关的数值，范围从 0.44 到 0.77；

P 是与权限要求相关的数值，范围从 0.27 到 0.85；

U 是与用户交互相关的数值，范围从 0.62 到 0.85。

因此，可利用性值的范围在 0.12 和 3.89 之间。

表 G.8 给出了一个 CVSS 可利用性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的过程并不严格符合 CVSS 对度量的要求。根据本文计算风险时，缺失的影响度量可以通过本文的影响指标进行补偿，见附录 F。

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，从而更好地指导组织的业务和正在开发的相关项或组件，并在将描述应用于实际漏洞时减少误解的可能性。这些补充可以是添加到度量值描述中的特定于组织的示例。

除了漏洞之外，CVSS 可利用性度量还可用于评估概念上的弱点、缺陷和差距。

G.4 基于攻击向量的方法指南

基于攻击向量的方法反映了攻击路径利用的上下文。为了利用攻击路径，攻击者离得越远（逻辑上和物理上），攻击可行性评级就越高。假设是可使用互联网来利用漏洞的潜在攻击者的数量大于可以利用需要物理访问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。 例 1：蜂窝网络连接，使 ECU 直接连接并可在互联网上访问。
中	邻近： 潜在攻击路径绑定到网络栈；然而链接在物理上或逻辑上是有限的。 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。 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
（资料性附录）
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。

本附录通过提供威胁分析和风险评估 (TARA) 方法的应用示例来帮助理解本标准的要求。该示例仅介绍了概念阶段，用以说明 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，且每个模块可以按任意顺序进行，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：

i.资产识别

ii.影响评级

iii.威胁场景识别

iv.攻击路径分析

v.攻击可行性评级

vi.风险值确认

vii.风险处置决策

在步骤 v 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 (参见 [RC-15-14]) 的方法，另一种使用基于攻击潜力 (参见 [RC-15-12]) 的方法。图 H.1 提供了 9 和 15 之间的交互概况。

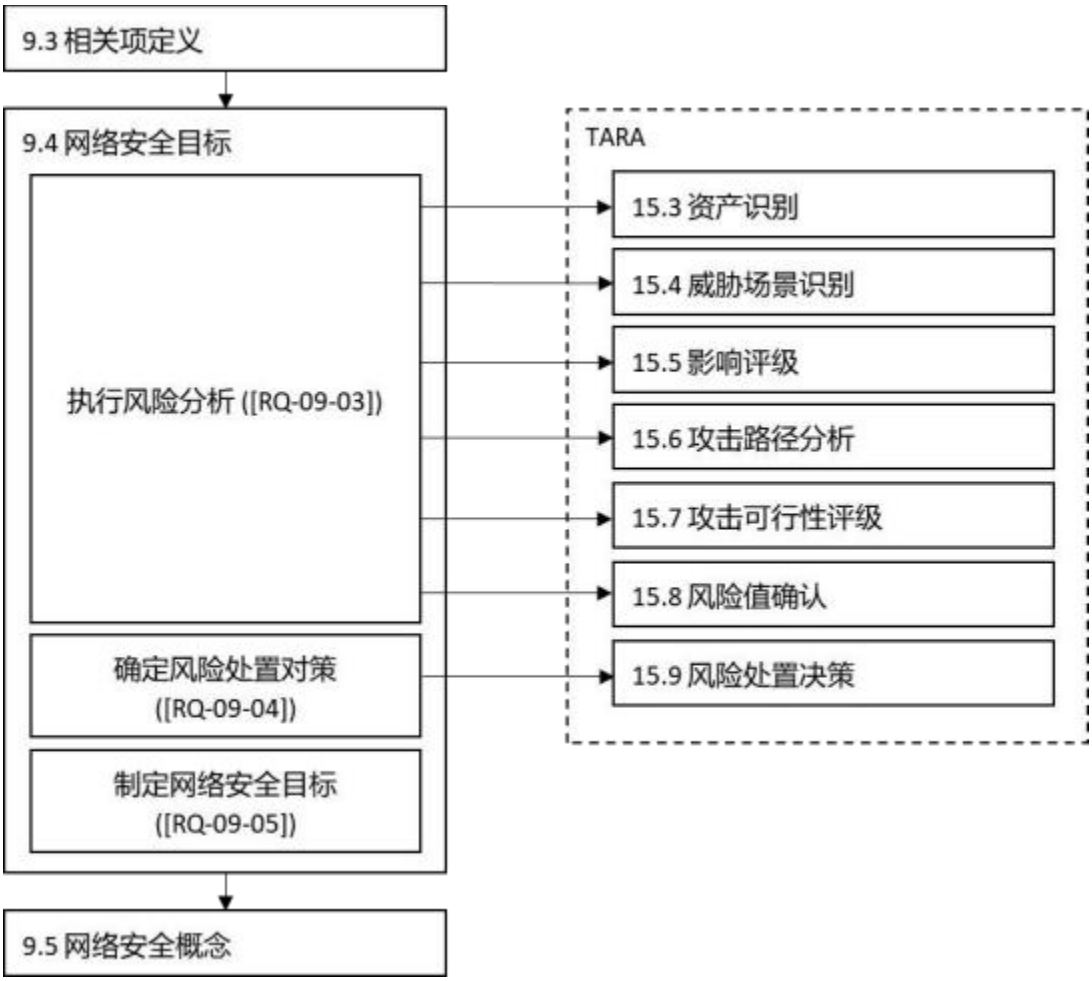

图 H.1 - 概念阶段的交互

H.2 前照灯系统概念阶段的示例活动

H.2.1 相关项定义

本节展示了 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：

a)相关项的边界 (参见图 H.2)

b)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/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。

c)初步的系统架构 (参见图 H.2)

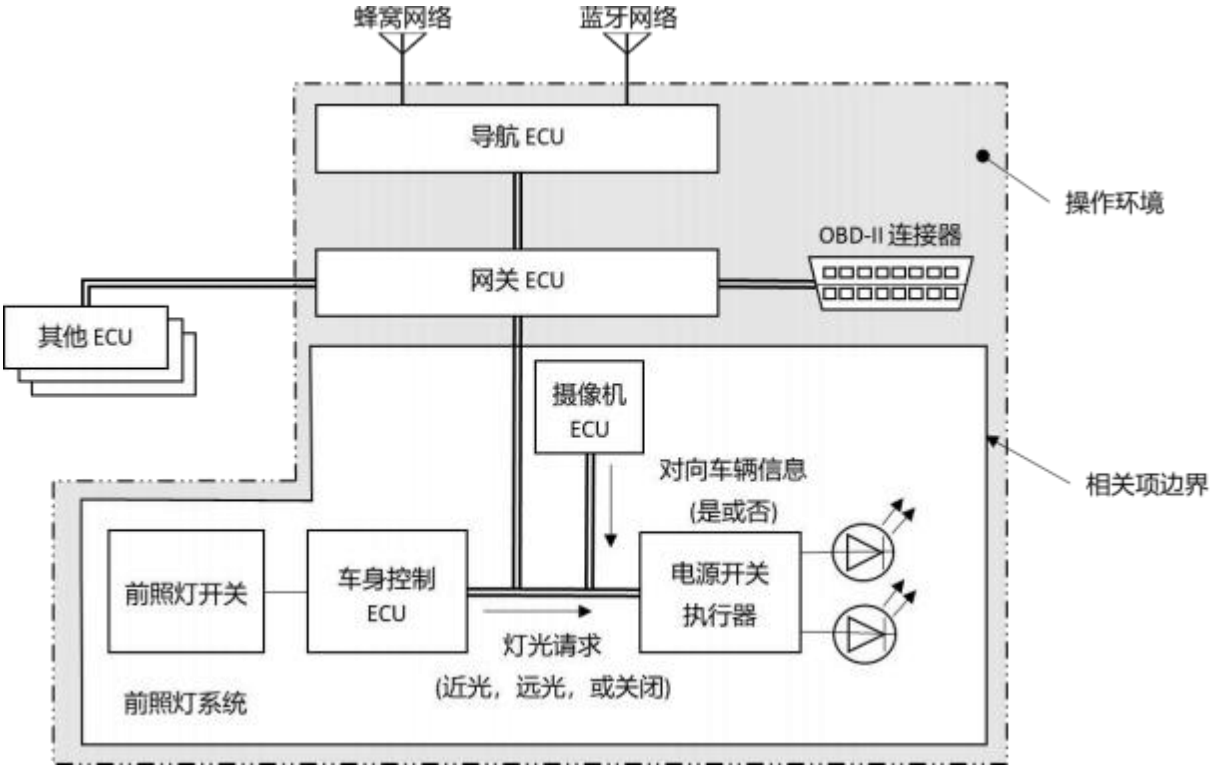

图 H.2 - 前照灯系统的相关项边界及初步系统架构示例

在相关项定义期间，需描述相关项的操作环境 (参见 [RQ-09-02])。操作环境为 TARA 的分析活动提供补充信息。表 H.1 展示了本附录中使用的操作环境的示例描述。

表 H.1 - 操作环境的示例描述

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。
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。
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] 按照 15.3 节要求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

资产	安全属性			危害场景
	C	I	A	
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）。
数据通信（迎面而来的汽车信息）	—	X	—	因为在夜间驾驶时不能切换到低光束而造成迎面驶来的车辆的司机不能看见。
	—	—	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。
车身控制 ECU 的固件	X	X	—	…

H. 2. 3 影响评级

[RQ-09-03] 也按照 15.3 节要求进行影响评级来为危害场景的影响评分。影响评级的示例结果如表 H.4 所示。

表 H.3 - 危害场景影响评级的示例

危害场景	影响分类	影响级别
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
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	重要 (S3)
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	中等

H. 2. 4 威胁场景识别

[RQ-09-03] 也按照 15.4 节要求进行威胁场景识别。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

危害场景	威胁场景
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。
	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。
夜间驾驶时，前灯总是处于低光束状态，导致自动远光灯出	资产：迎面驶来的车辆的信息。 信息安全性质：可用性。

现故障。	相关原因：迎面驶来的车辆的拒绝服务攻击。

H.2.5 攻击路径分析

[RQ-09-03] 也要求按照 16.6 进行攻击路径分析。表 H.5 展示了攻击路径分析的示例结果，图 H.3 展示了基于攻击树进行攻击路径分析的示例。

攻击路径的分析可以考虑假设。在本示例中，可以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

威胁场景	攻击路径
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	i. 攻击者通过蜂窝网络接口入侵了导航 ECU。 ii. 被入侵的导航 ECU 发送恶意控制信号。 iii. 网关 ECU 转发恶意控制信号至电源开关执行器。 iv. 恶意信号伪装成灯光请求 (关灯) 。
	i. 攻击者通过蓝牙网络接口入侵了导航 ECU。 ii. 被入侵的导航 ECU 发送恶意控制信号。 iii. 网关 ECU 转发恶意控制信号至电源开关执行器。 iv. 恶意信号伪装成灯光请求 (关灯) 。
	i. 攻击者可以本地访问 OBD 连接器。 ii. 攻击者通过 OBD 连接器发送恶意控制信号。 iii. 网关 ECU 转发恶意信号至电源开关执行器。 iv. 恶意信号伪装成灯光请求 (关灯) 。
拒绝提供对向车辆信息的服务	i. 攻击者通过蜂窝网络接口入侵了导航 ECU。 ii. 被入侵的导航 ECU 发送恶意控制信号。 iii. 网关 ECU 转发恶意控制信号至电源开关执行器。 iv. 攻击者用大量消息泛洪攻击通信总线。
	i. 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。 ii. 攻击者通过蓝牙网络接口入侵了驾驶员的智能手机。 iii. 攻击者通过智能手机和蓝牙加密狗向网关 ECU 发送消息。 iv. 网关 ECU 转发恶意信号至电源开关执行器。 v. 攻击者用大量消息泛洪攻击通信总线。

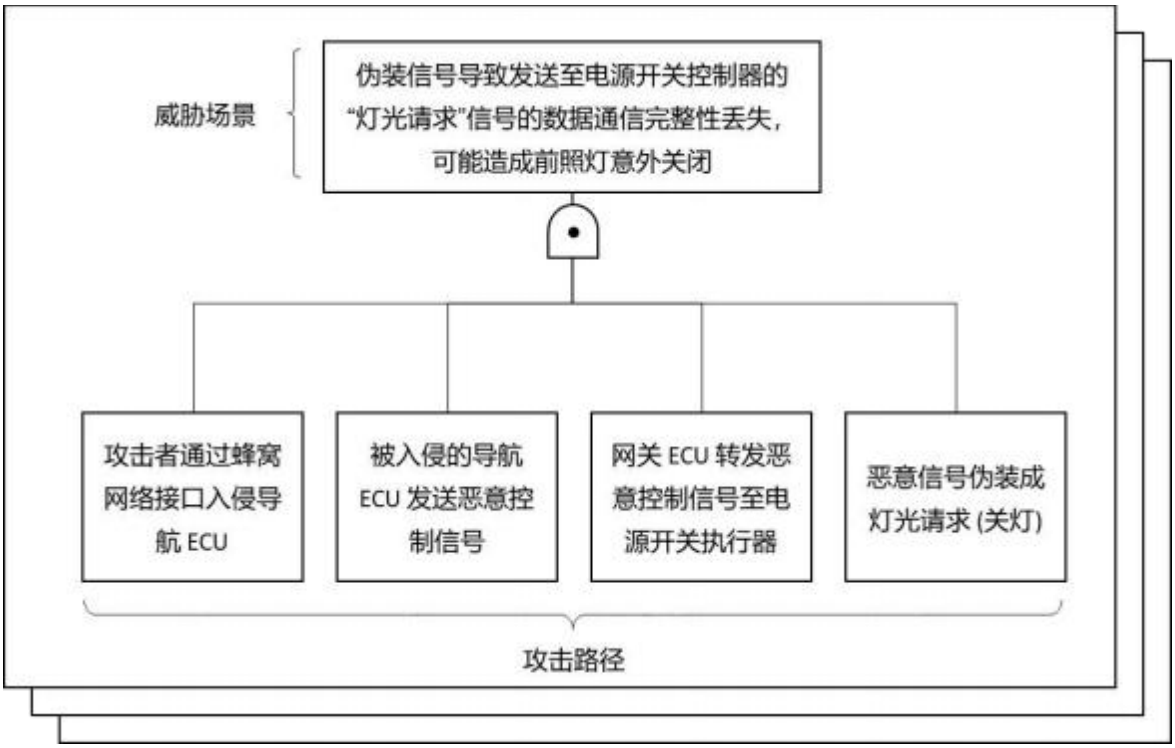

图 H.3 基于攻击树进行攻击路径分析的示例

H. 2. 6 攻击可行性评级

[RQ-09-03] 也要求按照 15.7 章进行攻击可行性评级。表 H.6 展示了根据 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。表 H.7 展示了根据 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。

表 H.6 基于攻击向量的方法进行攻击可行性评级的示例

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

注 1：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 (参见 [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

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
拒绝提供对向车辆信息的服务	i.攻击者通过蜂窝网络接口入侵了导航 ECU。 i.被入侵的导航 ECU 发送恶意控制信号。 i.网关 ECU 转发恶意控制信号至电源开关执行器。 v.攻击者用大量消息泛洪攻击通信总线。	1	8	7	0	4	20	低
	v.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。 vi.攻击者通过蓝牙网络接口入侵了驾驶员的智能手机。 i.攻击者通过智能手机和蓝牙加密狗向网关 ECU 发送消息。 i.网关 ECU 转发恶意信号至电源开关执行器。 x.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 2：各组织可以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，参见表 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] 也要求按照 15.8 章对每个威胁场景的风险值进行确定。风险值可以使用组织定义的风险矩阵来确定，用于将影响和攻击可行性的评级组合，映射到风险值。表 H.8 展示了一个风险矩阵示例，表 H.9 展示了使用表 H.8 进行风险值确定的示例结果。

表 H.8 风险矩阵示例

		攻击可行性评级			
		极低	低	中	高
影响评级	严重	2	3	4	5
	重大	1	2	3	4

	中等	1	2	2	3
	可忽略	1	1	1	1

表 H.9 风险值确定的示例

威胁场景	综合的攻击可行性评级	影响评级	风险值
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	严重	S:5
拒绝提供对向车辆信息的服务	低	中等	O:2

风险值也可以由组织定义的风险计算公式来确定。如以下公式和表 H.10 所示：$R = 1 + I \times F$

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 16.9 选择处置方案。表 H.11 展示了风险处置决策的示例结果。

表 H.11 风险处置决策的示例结果

威胁场景	风险值	风险处置方案
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
拒绝提供对向车辆信息的服务	O: 2	降低风险

H.3 网关TARA方法的应用示例

本附录中的网关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。

H.3.1 网关系统概念阶段的示例活动

本节展示了9.3 中指定的工作成果示例。网关的示例相关项定义如下：

相关项的边界（参见图 H.2）

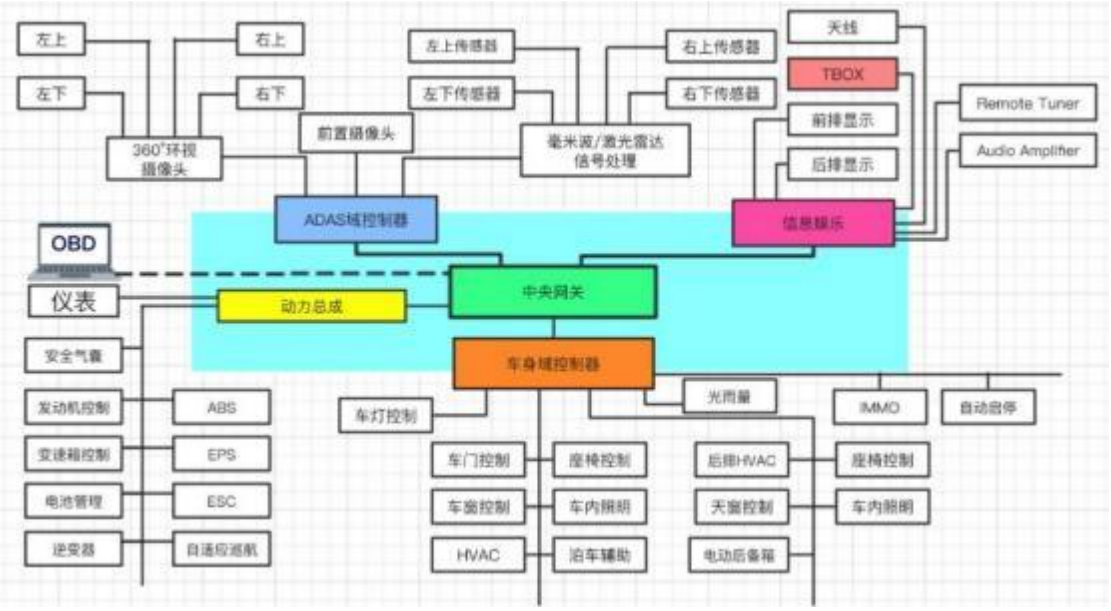

图 H.4 网关相关项的边界

a)相关项的功能

-相关项的功能概述：网关的作用就是为在不同的通信协议和不同的传输速度的计算机或模块之间进行通信时，建立连接和信息解码，并讲数据传输给其他系统。

b)相关项需定义的初步的框架(参见表 H.1)

表 H.12 网关相关项定义的初步框架

资产类别		示例
硬件	功能芯片	包括 Flash、EEPROM、看门狗等
	外部（以网关硬件为边界）接口	包括 JTAG、串口等
	内部接口	CAN 收发器、以太网收发器
软件	驱动层	驱动层：BSP 驱动、传感器驱动、控制模块驱动等
	固件	包括 Uboot 、Bootloader、HEX 二进制等
	操作系统（包括内核层）	包括 AutoSar
	应用程序	包括诊断服务（诊断协议）、路由服务、应用服务（通信协议）、应用防火墙、端口服务（SSH、telnet、ADB）等
通信	对外通信协议	外部通信协议： 以太网、CAN
	对内通信协议	内部通信协议：无
	数据流	CAN 数据交互
数据	系统配置文件	包括标定数据等与软硬件行为相关的设置数据

	敏感数据、个人信息和重要数据	包括与其他 TOE 之间通信的数据、密钥、证书、用户 ID、用户账号、用户口令、信号量、控制命令等等
	日志	包括系统日志、安全日志等记录系统及安全事件活动。

-在相关项定义期间，需描述相关项的操作环境 （参见 [RQ-09-02]）。操作环境为 TARA 的分析活动提供补充信息。表 H.13 展示了本附录中使用的操作环境的示例描述。

表 H.13 操作环境的示例描述

该相关项网关与其他车内控制器如车身控制器、娱乐影音控制器、动力域控制器等通过数据通信连接。
车内其他控制器如娱乐影音控制器具有安装第三方应用程序的功能： 假设： -第三方应用软件的安装都设计了身份认证校验机制。 车内其他控制器如娱乐影音控制器具有如下外部通信接口： -蓝牙网络 -蜂窝网络 假设： -娱乐影音域控制器配置了防火墙以阻止来自外部接口的无效数据通信。

H.3.2 资产识别

[RQ-09-03] 按照 15.3 节要求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.14 资产和危害场景列表的示例

资产	安全属性			危害场景
	C	I	A	
网关芯片 MPU-NXP XxxG	—	X	X	破坏网关 MPU 的安全性能，通过发送自制的软件升级包误导 MPU 对转向ECU 进行错误更新，导致车辆在行驶中以外转向。

H.3.3 影响评级

[RQ-09-03] 也按照 15.3 节要求进行影响评级来为危害场景的影响评分。影响评级的示例结果如表 H.4 所示。

表 H.15 危害场景影响评级的示例

危害场景	影响分类	影响级别
破坏网关 MPU 的安全性能，通过发送自制的软件升级包误导 MPU 对转向ECU 进行错误更新，导致车辆在行驶中以外转向。	S	严重

根据威胁分析的结果，对危害场景所造成的影响从安全、经济、操作、隐私和法律（SFOP）四个方面进行分析，并得出每个影响的指标值。

安全：S3 级。因为车辆行驶中意外转向，会威胁生命安全，并且伤害不确定是否会生存，是否会有致命伤害，所以对应的指标值为 1000。

经济：Medium。因为所造成的损害会导致重大的财物损失，但不会威胁到组织的生存，所以指标值为 100。

操作：High。因为未能满足安全或监管要求，所以指标值为 100。

隐私和法律：High。因为违反了法律，所以指标值为 100。

影响计算实可根据实际情况计算，本文中影响参数值等于各指标值相加。

IV=1000+100+100+100=1300.影响等级评估规律如表 H.4 所示：

表 H.16 影响等级评估规律

影响参数总值	影响等级	影响等级值
0-19	可忽略	1
20-99	中等	2
100-999	重大	3
>=1000	严重	4

根据上表的对应关系，可知影响等级为严重，影响等级值为4。

H 3.4 威胁场景识别

[RQ-09-03] 也按照 15.4 节要求进行威胁场景识别。威胁场景识别的示例结果如表 H.5 所示。

表 H.17 威胁场景的示例

危害场景	威胁场景
破坏网关 MPU 的安全性能，通过发送自制的软件升级包误导 MPU 对转向ECU 进行错误更新，导致车辆在行驶中以外转向。	攻击者使用伪造的软件升级数据，破坏 MPU 的安全性能，导致网关进行错误更新。
	通过发送自制的软件升级包误导网关对转向ECU 进行错误更新，导致车辆行驶中意外转向。

H 3.5 攻击路径分析

[RQ-09-03] 也要求按照 16.6 章进行攻击路径分析。表 H.6 展示了攻击路径分析的示例结果，图 H.3 展示了基于攻击树进行攻击路径分析的示例。

攻击路径的分析可以考虑假设。在本示例中，可以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.18 威胁场景的攻击路径示例

威胁场景	攻击路径
攻击者使用伪造的软件升级数据，破坏 MPU 的安全性能，导致网关进行错误更新。	i. 攻击者攻入汽车企业 APN 专网 ii. 攻击者收集车辆信息 iii. 攻击者穿透 T-BOX 安全机制 iv. 攻击者向车辆发送 FOTA 流程
通过发送自制的软件升级包误导网关对转向ECU 进行错误更新，导致车辆行驶中意外转向。	i. 攻击者攻入汽车企业 APN 专网 ii. 攻击者收集车辆信息 iii. 攻击者穿透 T-BOX 安全机制 iv. 攻击者向车辆发送 FOTA 流程

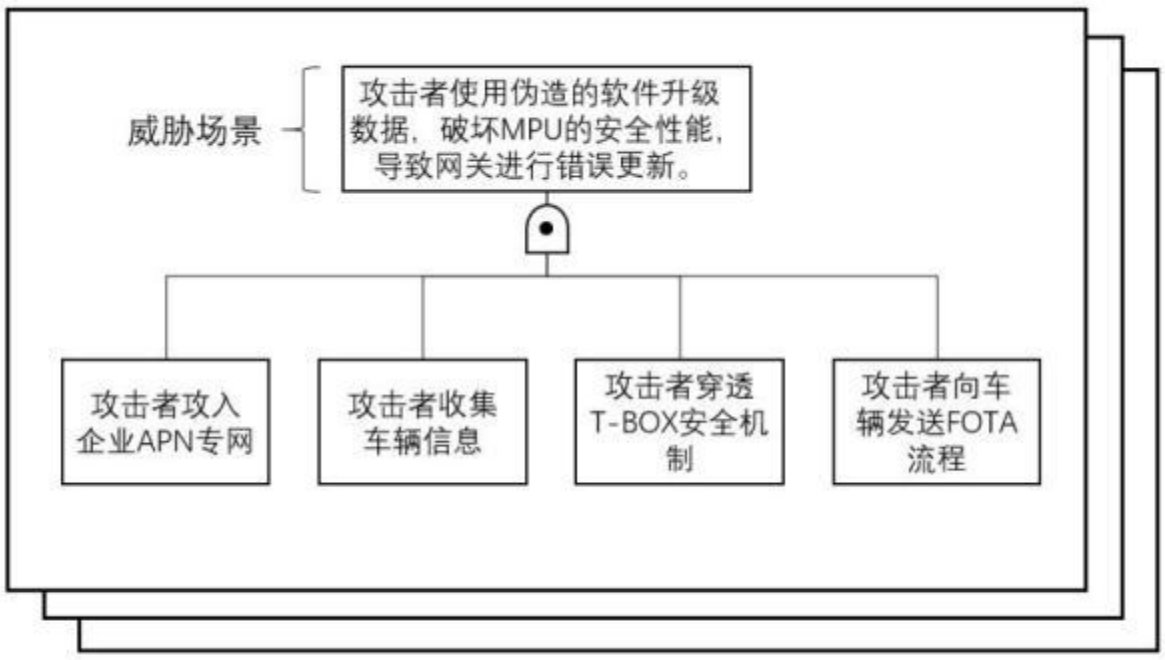

图 H.5 基于攻击树进行攻击路径分析的示例

H.3.6 攻击可行性评级

[RQ-09-03] 也要求按照 15.7 章进行攻击可行性评级。表 H.7 展示了根据 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。表 H.8 展示了根据 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。

表 H.19 基于攻击向量的方法进行攻击可行性评级的示例

攻击路径	攻击可行性评级
i. 攻击者攻入汽车企业 APN 专网 ii. 攻击者收集车辆信息 iii. 攻击者穿透 T-BOX 安全机制 iv. 攻击者向车辆发送 FOTA 流程	低

注 1 ：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 （参见 [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.20 基于攻击潜力的方法进行攻击可行性评级的示例

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
利用伪造的软件升级数据，破坏MPU的安全性能，导致 GW 进行错误更新，通过发送自制的软	i. 攻击者攻入汽车企业 APN 专网 ii. 攻击者收集车辆信息 iii. 攻击者穿透 T-BOX 安全机制 iv. 攻击者向车辆发送 FOTA 流程	4	6	7	0	7	24	低

件升级包误导 GW 对转向 ECU 进行错误更新，导致车辆行驶中意外转向。								
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 2：各组织可以依据各自的政策来制定每个评级的原则。例如，因为网关属于半开放接口，第一条攻击路径的机会窗口被赋值为 0 （无限，参见表 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.3.7 风险值确定

[RQ-09-03] 也要求按照 15.8 章对每个威胁场景的风险值进行确定。风险值可以使用组织定义的风险矩阵来确定，用于将影响和攻击可行性的评级组合，映射到风险值。表 H.8 展示了一个风险矩阵示例，表 H.10 展示了使用表 H.9 进行风险值确定的示例结果。

表 H.21风险矩阵示例

		攻击可行性评级			
		极低	低	中	高
影响评级	严重	2	3	4	5
	重大	1	2	3	4
	中等	1	2	2	3
	可忽略	1	1	1	1

表 H.22 风险值确定的示例

威胁场景	综合的攻击可行性评级	影响评级	风险值
利用伪造的软件升级数据，破坏 MPU 的安全性能，导致 GW 进行错误更新，通过发送自制的软件升级包误导 GW 对转向 ECU 进行错误更新，导致车辆行驶中意外转向。	低	严重	S:3

风险值也可以由组织定义的风险计算公式来确定。如以下公式和表 H.11 所示：

$$R = 1 + I \times F$$

表 H.23 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

攻击可行性评级	攻击可行性的数值 F
极低	0
低	1
中	1.5

严重	2	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.3.8 风险处置决策

[RQ-09-04] 要求根据 15.9 选择处置方案。表 H.12 展示了风险处置决策的示例结果。

表 H.23 风险处置决策的示例结果

威胁场景	风险值	风险处置方案
利用伪造的软件升级数据，破坏 MPU 的安全性能，导致 GW 进行错误更新，通过发送自制的软件升级包误导 GW 对转向 ECU 进行错误更新，导致车辆行驶中意外转向。	S：3	降低风险