ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 97-2022

车辆信息安全概念设计阶段技术要求

Technical requirements for the conceptual design stage of vehicle cybersecurity

2022-11-02 发布　　2022-11-03 实施

吉林省汽车电子协会　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。

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。

本文件由中国第一汽车集团有限公司智能网联开发院、一汽解放汽车有限公司商用车开发院联合提出。

本文件由吉林省汽车电子协会归口。

本文件由吉林省汽车电子协会组织实施。

本文件主要起草单位：一汽解放汽车有限公司商用车开发院、中国第一汽车集团有限公司智能网联开发院。

本文件主要起草人：谷倩、高德志、张丽波、梁亚丽、郑岩、冯祺、王春锦、张彪、李军龙、李木子、刘毅、李木犀、陈后立。

本文件参与起草单位：吉林大学汽车仿真与控制国家重点实验室、中国第一汽车集团有限公司检测试验院、沙龙机甲科技有限公司、岚图汽车科技有限公司、一汽奔腾轿车有限公司、东风汽车集团有限公司技术中心、摩登汽车有限公司。

本文件参与起草人：李杰、郑建明、王思涵、龚军、雷凯、周海鹰、孙伟、李原。

本文件审查人：杨彦鼎（东风汽车集团有限公司技术中心）、夏国强（中国汽车工程研究院股份有限公司）、马文峰（一汽奔腾轿车有限公司）、马喜来（一汽解放汽车有限公司）、占锐（东风汽车集团有限公司技术中心）、孔晓霜（中国第一汽车集团有限公司创新技术研究院）。

本文件为首次发布。

引　言

车辆研发是一个复杂的系统工程，从研发到投入市场需要较长的周期。概念设计作为车辆研发全生命周期中不可缺少的一部分，主要承担着前期情况调研、项目准备、风险及可行性评估等工作内容。随着汽车产品信息化程度的不断增加，由此产生的潜在漏洞层出不穷，前期对汽车产品中可能存在并引发信息安全事件的风险进行识别，开展车辆信息安全概念设计变得尤为重要。

因此，有必要编制一个基础性标准对车辆信息安全概念设计阶段进行标准化要求，提供一套可行的指导车辆信息安全概念设计，使得车辆风险可控的方法。

本技术要求主要在相关项定义、威胁分析与风险评估、信息安全目标定义、信息安全概念定义等安全技术要点进行要求和规范，以形成通用性的技术要求。

车辆信息安全概念设计阶段技术要求

1 范围

本文件规定了车辆信息安全概念设计阶段的总体目标、安全技术流程等有关内容，同时对安全技术流程提出了安全技术要求。

本文件适用于车辆研发过程中的信息安全概念设计阶段，旨在导出涉及的车辆级功能信息安全概念，以实现对应的信息安全目标。

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。

ISO/SAE 21434 道路车辆 网络安全工程（Road vehicles — Cybersecurity engineering）

ISO 26262-3 道路车辆 功能安全 第3部分:概念阶段（Road vehicles — Functional safety — Part 3: Concept phase）

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

具有价值或对价值有贡献的对象。

3.3

攻击路径 attack path

实现威胁场景的蓄意行动集合。

3.4

攻击可行性 attack feasibility

攻击路径的属性，描述成功执行相应的一组行动的难易程度。

3.5

信息安全声明 cybersecurity claim
关于风险的声明，可包括分担或保留风险的理由。

3.6

信息安全控制措施 cybersecurity control
缓解风险的信息安全控制措施。

3.7

信息安全目标 cybersecurity goal
与一个或多个威胁场景相关的概念级的信息安全要求。

3.8

信息安全概念 cybersecurity concept
相关项的信息安全要求和对操作环境的要求，以及有关信息安全控制措施的相关信息。

3.9

信息安全属性 cybersecurity property
值得保护的属性，包括保密性、完整性、可用性。

3.10

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

3.11

影响 impact
对损害场景下的损害或身体伤害程度的估计。

3.12

相关项 item
实现车辆级功能的组件或组件集。

3.13

操作环境 operational environment
在车辆功能、生产、服务维修中运行使用中的相互作用。

3.14

威胁场景 threat scenario
一个或多个资产的信息安全属性受到损害的潜在原因，以实现相应的损害场景。

3.15

验证 verification

通过提供客观证据，确认特定要求已得到满足。

4 缩略语

下列缩略语适用于本文件：

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

E/E——电子电气(Electrical and Electronic)；

EVITA——电子安全车辆入侵保护应用程序（E-safety Vehicle Intrusion Protected Applications)；

FIRST——国际网络安全应急论坛组织(Forum of Incident Response and Security Teams)；

PASTA——攻击模拟和威胁分析过程（Process for Attack Simulation and Threat Analysis)；

STRIDE——身份假冒、篡改、抵赖、信息泄露、拒绝服务、特权提升（Spoofing，Tampering，Repudiation，Information Disclosure，Denial of Service，Elevation of Privilege)；

TARA——威胁分析与风险评估（Threat Analysis and Risk Assessment)；

TVRA——威胁、脆弱性和风险评估(Threat, Vulnerability and Risk Assessment)。

5 车辆信息安全概念设计阶段技术要求

5.1 总体目标

概念设计阶段是车辆研发流程中具体化产品要求及设计目标的重要阶段。在车辆概念设计阶段中，应给出详细的能够实现既定需求的设计目标，对车辆信息安全而言，车辆信息安全概念设计阶段中主要确认需要保护的安全对象、安全对象面临的威胁及风险、对安全对象的保护目标及要求，以满足车辆产品的信息安全需求。

5.2 安全技术流程

以下为车辆信息安全概念设计阶段的安全技术流程，如图1所示：

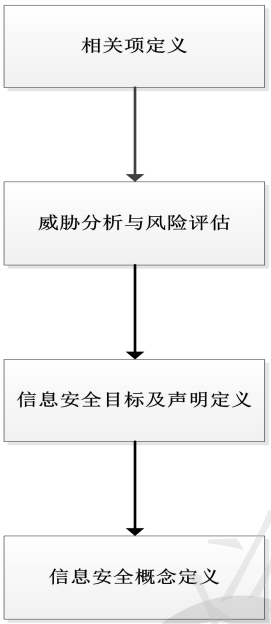

图1　车辆信息安全概念设计阶段安全技术流程

a) 识别当前相关项系统模型的现有信息，包括操作环境、车辆E/E架构设计、已有开发文档及现有安全措施等；
b) 结合相关的信息安全信息，同时基于必要的前提或假设，对识别到的相关项的关键资产进行威胁分析与风险评估；

注1：信息安全信息如公开的信息安全事件、权威平台的漏洞、相关标准法规的约束等。

注2：必要的前提或假设如攻击者无法破坏标准化且当前推荐的加密算法。

c) 对确定的信息安全风险的处理决策，应指定信息安全目标或信息安全声明，并对过程及结果进行验证；
d) 提出信息安全要求，分配给相关项，将其描述形成信息安全概念设计方案，并对过程及结果进行验证。

5.3　安全技术要求

5.3.1　相关项定义

相关项定义要求如下：

a) 应确定相关项的边界、功能、初始架构设计；
b) 应确定信息安全相关项的操作环境信息；
c) 应确定相关项的现有安全措施。

5.3.2　威胁分析与风险评估

5.3.2.1　概述

本节描述了用于确定相关组织及个人受威胁场景影响程度的方法总览，如图2所示。这些方法及其工作产物统称为威胁分析和风险评估。

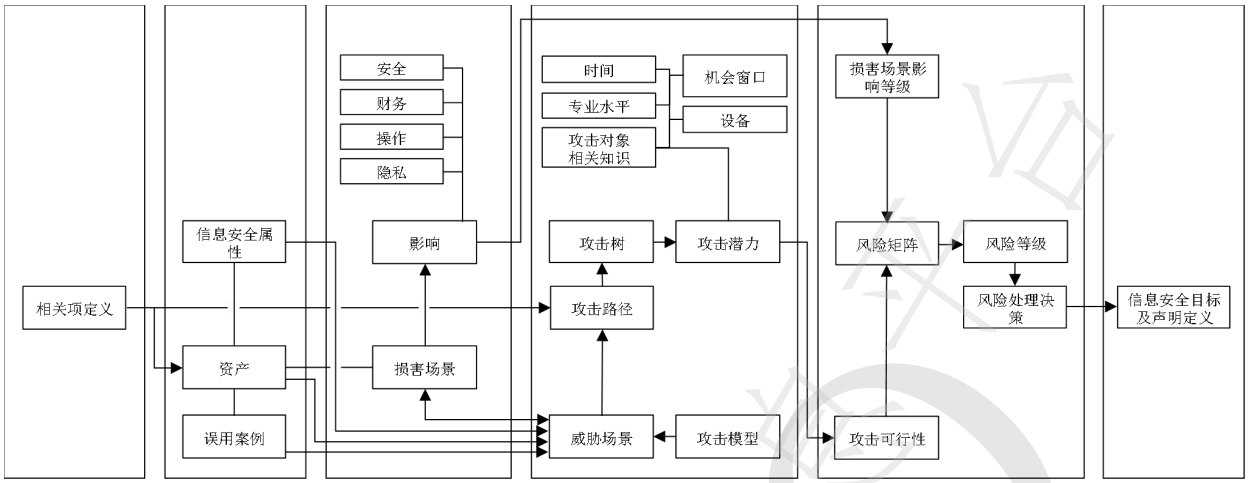

图2　TARA分析方法实例

5.3.2.2　目标

本方法的目标是：

a)　识别资产、其信息安全属性及其损害场景；
b)　识别威胁场景；
c)　确定损害场景的影响等级；
d)　识别实现威胁场景的攻击路径；
e)　确定攻击路径被利用的难易程度；
f)　确定威胁场景的风险值；
g)　为威胁场景选择适当的风险处理方案。

5.3.2.3　资产识别

资产识别要求如下：

a)　应确定损害场景。对损害场景的描述可包括：
　　1)　相关项的功能与不良后果之间的关系；
　　2)　对相关组织及个人损害的描述；
　　3)　相关资产。
b)　应识别具有信息安全属性的资产，其危害会导致损害场景。资产的识别可以基于：
　　1)　分析相关项定义；
　　2)　进行影响评级；
　　3)　从威胁场景中推导出资产；
　　4)　使用预定义的目录。

5.3.2.4　威胁场景识别

威胁场景识别要求如下：

a)　应识别威胁场景，对威胁场景的描述可包括：
　　1)　目标资产；
　　2)　资产的信息安全属性受损情况；
　　3)　信息安全属性受损的原因。

注：一个损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损害场景。

b) 威胁场景识别方法可以使用小组讨论或一些系统方法，如基于EVITA、TVRA、PASTA、STRIDE等框架的威胁建模方法。

5.3.2.5 影响评级

影响评级要求如下：

a) 损害场景应针对道路使用者在安全、财务、操作和隐私的影响类别中的潜在不利后果进行评估；

b) 损害场景的影响等级应针对每个影响类别确定为以下之一：

1) 严重的；

2) 重大的；

3) 中等的；

4) 可忽略的。

c) 安全相关影响等级应参考ISO 26262-3；

d) 如果已经得出了损害场景一个影响类别的等级，并且可以论证其他影响类别的等级不会对最终结果造成影响，那么可以省略对其他影响类别的进一步分析；

注：如损害场景的安全类别影响被评为“严重”，那么可以不进一步分析该损害情景的财务影响。

e) 影响等级最终应以影响类别中最严重的级别作为评定结果。

5.3.2.6 攻击路径分析

攻击路径分析要求如下：

a) 应对威胁场景进行分析以识别攻击路径。攻击路径分析可以基于：

1) 自上而下的方法，通过分析可以实现威胁场景的不同方式来推断攻击路径，例如攻击树、攻击图；

2) 自下而上的方法，从识别的漏洞构建攻击路径。

b) 攻击路径应与相应的威胁场景相关联。在产品开发的早期阶段，攻击路径通常不完整或不精确，应随着可用信息的增多及时更新攻击路径。

5.3.2.7 攻击可行性评级

攻击可行性评级要求如下：

a) 对于每个攻击路径，攻击可行性等级应按照表1中的描述确定；

表1 攻击可行性等级及描述

攻击可行性等级	描述
高	攻击路径可以利用较少的付出来完成。
中等	攻击路径可以利用中等的付出来完成。
低	攻击路径可以利用较高的付出来完成。
非常低	攻击路径可以利用非常高的付出来完成。

b) 攻击可行性等级应基于以下方法之一定义：

1) 基于攻击潜力的方法，攻击可行性等级应根据经过的时间、攻击者专业水平、掌握攻击对象的知识、机会窗口、设备来确定；

2) 基于CVSS的方法，攻击可行性等级应根据基本指标组的可利用性指标确定，包括攻击向量、攻击复杂性、所需特权、用户交互；

3） 基于攻击向量的方法，攻击可行性等级应基于攻击路径中主要攻击向量的评估来确定。

5.3.2.8 风险值确定

风险值确定要求如下：

a） 对于每个威胁场景，风险值应根据相关损害场景的影响等级和相关攻击路径的攻击可行性等级来确定；

注1：如果威胁场景对应于多个损害场景或相关损害场景对多个影响类别产生影响，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个攻击路径，则相关的攻击可行性等级可以适当合并。

b） 威胁场景的风险值应介于（包括）1和5之间，其中1表示最小风险。确定风险值的方法：

1） 风险矩阵，见表2；

2） 风险公式，通过构造经验函数，将损害场景的影响等级与相应攻击路径的攻击可行性等级进行运算得到风险值。

表2 风险矩阵实例

风险值		攻击可行性等级			
		非常低	低	中等	高
影响等级	严重的	2	3	4	5
	重大的	1	2	3	4
	中等的	1	2	2	3
	可忽略的	1	1	1	1

5.3.2.9 风险处理决策

对于每种威胁场景，考虑到其风险值，应确定以下一种或多种风险处理方案：

a） 规避风险；

b） 降低风险；

c） 分担风险；

d） 保留风险。

5.3.3 信息安全目标及声明定义

信息安全目标及声明定义如下：

a） 如果威胁场景的风险处理决策是降低风险，应指定一个或多个相应的信息安全目标；

b） 如果威胁场景的风险处理决策是分担风险或因风险评估中使用了一个或多个假设而保留风险，应指定一个或多个相应的信息安全声明；

c） 应对成果物进行验证确认：

1） 对定义的相关项，风险评估结果的正确性和完整性；

2） 对风险评估结果，风险处理决策的完整性、正确性和一致性；

3） 对风险处理决策，信息安全目标和信息安全声明的完整性、正确性和一致性；

4） 所有的信息安全目标和信息安全声明的一致性。

5.3.4 信息安全概念定义

信息安全概念定义如下：

a) 应描述实现信息安全目标的技术或运营层面的安全控制措施及其相互作用，充分考虑相关项功能之间的依赖性及信息安全声明；

注：描述可包括实现信息安全目标的条件，如预防入侵、检测和监控入侵；专门用于处理威胁场景的具体功能，如使用安全通信信道。

b) 应为信息安全目标确定相关项的信息安全要求及对操作环境的要求；

c) 信息安全要求应分配给相关项，如果适用，则分配给其一个或多个组件；

d) 应对成果物进行验证确认：

1) 对信息安全目标，成果物的完整性、正确性、一致性；

2) 对信息安全声明，成果物的一致性。

附 录 A
（资料性）
信息安全验证报告模板

信息安全验证报告参考表A.1。

表A.1 信息安全验证报告参考

验证项	验证属性	验证结果
一、资产识别		
有关相关项/组件的现有信息是否被考虑？ 例如：架构设计	完整性	是/否
是否列举了具有信息安全属性的资产？如果是，请选择方法： a) 分析相关项定义； b) 进行影响评级； c) 从威胁场景中推导出资产； d) 使用预定义的目录； e) 其他方法请注明。	正确性	是/否
…	…	…
二、威胁场景识别		
是否已确定威胁场景？	正确性	是/否
每个威胁场景是否与至少一个损害场景相关联？	一致性	是/否
…	…	…
三、影响评级		
是否针对四个核心影响类别（即安全、财务、操作和隐私）评估了已确定的损害场景？ 如果否，请指定考虑的影响类别。	正确性	是/否
…	…	…
四、攻击路径分析		
是否分析了威胁场景？	正确性	是/否
是否确定了来自公共资源的已知漏洞？	正确性	是/否
…	…	…
五、攻击可行性评级		
是否确定了攻击可行性评级方法？如果是，请说明。	正确性	是/否

表A.1　信息安全验证报告参考（续）

验证项	验证属性	验证结果
…	…	…
六、风险值确定		
是否确定了风险值确定方法？ 如果是，请说明。	正确性	是/否
是否为每个威胁场景计算了风险值？	完整性	是/否
…	…	…
七、风险处理决策		
考虑到影响类别、攻击路径和风险确定的结果，是否确定了风险处理方案？	正确性、完整性	是/否
是否所有风险处理决策都属于以下广泛的风险处理选项： a)　规避风险； b)　降低风险； c)　分担风险； d)　保留风险。	正确性	是/否
…	…	…
八、信息安全目标/声明		
分配的信息安全目标是否源自批准的 TARA？	一致性	是/否
如果适用，是否为运营和维护以及退役定义了分配的信息安全目标？	完整性	是/否
…	…	…
最终评审结果		
通过/未通过/重新验证		

附 录 B
（资料性）
攻击可行性评级参考

本附录提供了关于如何应用以下方法进行攻击可行性评级的参考：

a) 基于攻击潜力的方法，参见表B.1；
b) 基于CVSS的方法，参见FIRST组织相关标准；
c) 基于攻击向量的方法，参见表B.2。

表B.1 攻击潜力方法参考

类别	等级	描述
经过的时间	<=1天	-
	<=1周	-
	<=1个月	-
	<=6个月	-
	>6个月	-
攻击者专业水平	外行	不了解情况，没有特别的专长的人。
	精通的人	知识渊博，熟悉产品或系统的安全行为的人。
	专家	熟悉产品或系统的底层算法、协议、硬件、结构、安全行为、所采用的安全原理和概念，定义新的攻击的技术和工具、密码学、经典攻击方法等的人。
	多领域专家	攻击的不同步骤需要不同的专业领域的专家。
掌握攻击对象的知识	公开信息	相关项或组件的公开信息。
	受限的信息	相关项或组件的限制开放的信息，如开发者组织可根据保密协议共享的信息。
	机密的信息	相关项或组件的机密的信息，如开发者组织内授权团队成员可访问的信息。
	严格保密的信息	相关项或组件的限制绝密的信息，如只有少数人可访问，并严格控制访问权限的信息。

表B.1　攻击潜力方法参考（续）

类别	等级	描述
机会窗口	没有限制的	通过公共或不受信任的网络实现高可用性，没有任何时间限制（即资产始终可访问）。没有物理存在或时间限制的远程访问以及无限的物理访问相关项或组件。
	容易的	高可用性和有限的访问时间。没有物理存在即可远程访问相关项或组件。
	中等的	相关项或组件的可用性低。有限的物理和/或逻辑访问。物理访问车辆内部或外部，无需使用任何特殊工具。
	困难的	相关项或组件的可用性非常低。没有可执行攻击的对相关项或组件的访问方式。
设备	标准的	现有的设备，并且很容易得到。
	专业的	攻击者不容易获得设备，但无需过度努力即可获得。如购买适量的设备。
	定制的	设备是专门生产的并且不轻易向公众提供，或者设备非常专业以至于其分发受到控制，甚至可能受到限制。 或者，设备非常昂贵。
	多种定制的	攻击的不同步骤需要不同类型的定制设备。

表B.2　攻击向量方法参考

类别	等级	描述
高	远程	潜在的攻击路径与网络堆栈绑定，没有任何限制。
中等	近程	潜在的攻击路径与网络栈绑定；但是连接在物理上或逻辑上受到限制。
低	本地	潜在的攻击路径不受网络堆栈和威胁代理的约束，需要直接访问相关项以实现攻击路径。
非常低	物理	威胁代理需要物理访问才能实现攻击路径。