智能网联汽车信息安全测评方法论

信息安全评测方法发展现状

国内外政策法规要求

国内外在围绕智能网联汽车信息安全出台的法律政策方面，总体上呈现出了一种以汽车联网、自动驾驶等复杂应用场景为目标抓手，促进汽车产业链上各环节加强对信息安全保障投入的发展态势，各国均在积极推进汽车信息安全相关法规、标准等制定工作，旨在为行业或企业提供可实施的规范。目前，国际上智能网联汽车信息安全法规、标准大多都停留在最佳实践、指南、关键原则上。

美国《现代汽车信息安全最佳实践》

智能网联汽车信息安全法规政策方面，欧、美、日等世界汽车强国都在积极推动相关政策和标准规范制定工作。美国在谷歌、苹果、微软等互联网巨头以及福特、通用、特斯拉等汽车制造商的大力支持下，政府和行业对汽车信息安全关注较早。2016 年 10月份，美国 NHTSA 发布了《现代汽车信息安全最佳实践》（Cybersecurity Best Practices for Modern Vehicles），针对快速发展的智能网联汽车信息安全及隐私保护等问题推出了最佳实践框架结构。

在产品的网络安全防护方面，NHTSA 建议汽车企业在开发或集成车辆的安全关键系统时，需要优先考虑车辆网络安全并从组织管理上给予保障。明确指出要对智能网联汽车实施广泛的网络安全测试，防止汽车接入未授权的网络，保护关键安全系统和个人数据。

欧洲《智能汽车网络安全与适应力》

2017 年欧洲网络信息安全局（ENISA）发布了《智能汽车网络安全与适应力》的研究报告（简称“ENISA 指南”），目标受众是汽车制造商、供应商和服务商。报告对智能汽车安全架构、当前面临的威胁（攻击面和场景模式）进行了深入研究，并从政策和标准、组织方法、技术三个层面给出了智能网联汽车网络安全的最佳实践建议。为了增强智能网联汽车产业链各方（汽车制造商、供应商和服务商）之间的信任，保证智能网联汽车的安全及健康发展，“ENISA 指南”提出如下建议：

1. 提升智能网联汽车的网络安全：产业链各方必须建立全面的产品安全开发流程，包括现场的设计、开发、测试和安全维护，有效提高产品的安全性；
2. 增强产业链各方间的信息共享：加强产业链间的信息共享，可使产业链各方建立相互信任机制，有利于标准制定和采用、采用公认的方案、建立安全方面的团队、发现安全问题并调解等；
3. 明确产业链参与者之间的责任划分：明确产业链各方的责任，相关责任问题应按照国家相关法律进行处理；

4. 形成统一的技术标准与实践方案；
5. 确定一套独立的第三方安全评估机制；
6. 开发安全分析工具：开发智能网联汽车专用的安全分析工具，以提高安全测试能力，一些已建立的软件工具可以用于智能汽车安全分析，如资产识别、威胁建模等，同时开发一些用于智能网联汽车安全实施、安全测试、安全监控等方面的工具。

英国《智能网联汽车网络安全关键原则》

生产制造供应链上所有参与者，从设计师、工程师到零售商和高级管理人员，都需一份指导这一全球性产业发展的统一指南。因此，英国交通部和国家基础设施保护中心联合制定了贯穿汽车行业、智能网联汽车、智能交通系统（ITS）及其产业链的关键指导原则。2017 年 8 月，英国政府对外发布了《智能网联汽车网络安全关键原则》（The Key Principles of Cyber Security for Connected and Automated Vehicles），该指南细分出 8 大原则，29 个细则。《智能网联汽车网络安全关键原则》将网络安全责任拓展到汽车产业链上的各参与主体，包括第三方承包商，要求在汽车全生命周期内考虑网络安全问题，并在遭受网络攻击时要保证车辆安全运行的基本功能，也就是满足功能安全（Safety）或韧性（Resilience）的要求。简而言之，汽车网络安全问题是汽车全生命周期的问题，其安全防护工作更是一个不断迭代完善的工作，需要产业链协同完成：

1. 管理层推动：推进安全计划、安全方案设计等；
2. 安全风险管理与评估：风险评估与管理、风险识别、分类、优先排序、威胁处理等；
3. 产品售后服务与应急响应机制；
4. 整体安全性：安全分级管理、安全保证、安全可追溯可验证；
5. 系统设计：纵深防御与分段技术、边界防护、远程终端防护；
6. 软件安全管理：安全编码、配置管理、审计测试、代码共享；
7. 数据安全：存储安全、传输安全、个人数据管理、敏感数据；
8. 韧性设计：功能可用性保证、失效保护、功能恢复与响应。

中国《国家车联网产业标准体系建设指南》

为了加强顶层设计，推动车联网产业技术研发和标准制定，推动整个产业的健康可持续发展，2018 年由工信部、国家标准委共同开始制定《国家车联网产业标准体系建设指南（智能网联汽车）》。计划到 2025 年，系统形成能够支撑高级别自动驾驶的智能网联汽车标准体系。

该指南综合不同的功能要求、产品和技术类型、各子系统间的信息流，将智能网联汽车标准体系框架定义为“基础”、“通用规范”、“产品与技术应用”、“相关标准”四个部分。在该标准体系中，信息安全标准在遵从信息安全通用要求的基础上，以保障车辆安全、稳定、可靠运行为核心，主要针对车辆及车载系统通信、数据、软硬件安全，从整车、系统、关键节点以及车辆与外界接口等方面提出风险评估、安全防护与测试评价要求，防范对车辆的攻击、侵入、干扰、破坏和非法使用以及意外事故。

从国内外智能网联汽车信息安全的实践内容来看，信息安全应贯穿全生命周期，信息安全评测工作是智能网联汽车持续健康发展的重要支撑。国际上发布的汽车信息安全最佳实践、关键原则等均表明需要从开发流程和产品功能两个方面保障智能网联汽车的信息安全，同时其信息安全评测也应该涵盖开发流程和产品功能两个方面的安全性。上述介绍的大多数实践也都提到了风险评估、测试等相关内容，这些都是智能网联汽车信息安全评测工作涉及的重要活动。

智能网联汽车信息安全标准法规

在汽车信息安全工作持续推进的过程中，国际上积极开展相关标准法规的制定工作，在首个针对汽车网络安全而制定的指导性文件 SAE J3061 正式发布后，国际上一直致力于 ISO/SAE 21434、UN/WP29 CS 等多个标准法规的编制。

SAE J3061

2016 年 1 月，美国汽车工程师学会（SAE）率先推出了全球首部汽车信息安全指南SAE J3061《信息物理汽车系统网络安全指南（Cybersecurity Guidebook for Cyber-Physical Vehicle Systems）》，为汽车产业提供了参考和建议，协助整车厂通过实施结构清晰的项目，以保证汽车在全生命周期中都可获得有效的保护。SAE J3061 提供了车辆网络安全的流程框架和指导，旨在帮助企业识别和评估网络安全威胁，将网络安全设计理念渗透到信息物理汽车系统整个生命周期开发过程中。其主要内容包括：定义了完整的生命周期流程框架，企业可以裁剪、利用这个框架，使网络安全设计贯穿车辆的全生命周期，包括概念、开发、生产、运营、维护、报废各个阶段；提供了车辆网络安全相关的工具和方法论，内容涉及汽车信息安全完整性等级、测试方法和工具等，以保证汽车在全生命周期中都可获得有效的信息安全保护。

由于第一版 SAE J3061 的内容并入了 ISO/SAE 21434，美国汽车工程师学会汽车电气系统安全委员会（SAE Vehicle Electrical System Security Committee）开始制定一套比ISO/SAE 21434 更深入或更具技术性的指导文件，旨在为汽车系统的网络安全工程提供额外的指导或支持。SAE J3061 分为三部分，第一部分定义汽车网络安全等级（ACSIL）以及威胁分析和风险评估（TARA）方法用于将威胁分类，对于可能导致功能安全受影响的威胁，还将包括 ACSIL 如何与汽车功能安全等级（ASIL）建立相关联系。第二部分和第三部分着重于安全测试，第二部分重点介绍了供应商对未知硬件和定期更新软件的安全测试方法，第三部分对安全相关工具的制造商及其能力做了概述。

ISO/SAE 21434

ISO/SAE 21434《道路车辆 信息安全（Road vehicles—Cybersecurity engineering）》是基于 SAE J3061 制定的、覆盖车辆整个生命周期的工程管理标准，不涉及具体技术实现细节，目前仍在制定中，计划 2020 年末完成。该标准基于 SAE J3061，参考 V 字模型开发流程，主要从安全风险管理、产品开发、生产、运营/维护、跨产品或者组织层面的保障流程（例如：审核）等四个方面来保障汽车信息安全工程工作的开展。目标是使得依据该标准设计、生产、测试的产品能具备一定的信息安全防护能力，标准内容主要包括：

(1) 信息安全相关的术语和定义；
(2) 信息安全管理：包括企业组织层面和具体项目层面；
(3) TARA（威胁分析和风险评估）；
(4) 信息安全概念阶段开发；
(5) 架构层面和系统层面的威胁消减措施和安全设计；
(6) 软硬件层面的信息安全开发，包括信息安全的设计、集成、验证和确认；
(7) 信息安全系统性的测试及其确认方法；
(8) 信息安全开发过程中的支持流程，包括需求管理、变更管理和配置管理等；
(9) 信息安全事件在生产、运营、维护和报废阶段的识别、防止、探测、响应和恢复等。

本标准介绍的风险评估方法模块包括资产识别、威胁场景识别、影响评估、脆弱性分析、攻击路径分析、攻击可行性评估和风险评估。风险评估方法通常从识别资产和通过损害场景分析相关资产的威胁开始，确定道路使用者的相关影响。随着设计过程的开展，可能会出现脆弱性，并且可以确定潜在的攻击路径来确定相关的攻击可行性，这些是风险计算的输入。风险评估结果用于选择适当的应对方案来处置该风险，推导车辆的信息安全需求。

UN/WP29 CS

联合国世界车辆法规协调论坛（UN/WP29）负责制定有关网络安全（CS）和在线升级（OTA）的法规草案。其中，关于网络安全的建议包含与（a）批准和认证汽车制造商网络安全管理体系的要求和（b）车辆型式认证中网络安全认可相关的法规，将提供有关流程和程序以及最佳实践（威胁和缓解）的指导。网络安全管理体系（Cyber Security Management System，CSMS）是指一种系统的基于风险的方法，用于定义组织流程、责任和治理，以处理对车辆的网络威胁并保护车辆免受网络攻击。在进行车辆型式认证评估之前，车辆制造商应向审批机构或技术服务部门证明其网络安全管理系统具有与被批准的车辆类型相关的有效 CSMS 合规证书。

2018 年 10 月，德国汽车工业联合会质量管理中心（Verband der Automobilindustrie，Qualitats Management Center，VDA-QMC）在车辆型式认证法规和 ISO/SAE 21434 标准的推动下成立了汽车网络安全管理系统工作组，负责制定网络安全审计和评估流程的标准，目的是使 CSMS 可审核和可认证，以满足联合国法规的要求以及其他标准。ISO/SAE 21434 是车辆型式认证的基础，应在国际标准化环境中满足网络安全审计和认证的要求，将 ISO/SAE 21434 实施到公司的规则和流程中，符合联合国对 CSMS 的要求。

信息技术安全测评通用标准

目前，我国已经制定和引进了几十个重要的信息安全标准，其中随着 GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》的发布，形成了新的网络安全等级保护基本要求标准。而在信息安全管理方面，ISO 27000 系列已经成为国际上应用最广泛的信息安全管理标准。

在整个信息安全评估准则的发展历程中，国际上有三个非常重要的里程碑式的标准：TCSEC、ITSEC 和 CC 标准。其中，CC 信息技术安全评估准则（Common Criteria for Information Technology Security Evaluation），简称CC标准，是IT产品安全认证的国际标准（ISO / IEC 15408）。它综合了已有的信息安全准则和标准，如美国的TCSEC、欧洲的ITSEC、加拿大的CTCPEC等，形成一个更全面的框架，旨在确保IT产品安全的规范、实施和评估过程以严格、标准和可复制的方式在与其目标使用环境相对应的水平上进行，是第一个信息技术安全评估国际标准。在信息安全标准的制订方面，我国主要采用与国际标准参照引用的方式，将 ISO/IEC 15408:1999 系列标准转化为国家推荐性标准 GB/T 18336-2001《信息技术 安全技术 信息技术安全评估准则》，之后 GB/T 18336-2015 又参照 ISO/IEC 15408-2009进行了更新。最新的ISO/IEC 15408:2022系列，国内尚未进行对比更新。

国际上，把CC 作为评估IT技术安全行的通用尺度和方法。许多政府、企业、组织也把“是否拥有CC认证”作为采购软件或硬件产品的重要评估项甚至必要条件。CC及其配套的信息技术安全评估通用方法（CEM）构成了信息技术安全评估准则互认协议（CCRA）的技术基础。尽管每个国家都有自己的认证流程，但CCRA承认针对协作保护概况（cPP）的评估。这意味着所有成员国都将承认这些认证。

CC 适用于所有IT 产品，不管是硬件、软件、固件，都能在一个框架下评估，还可用于知道产品和系统开发。用户可使用保护配置文件（PP），指定安全功能要求（SFR）和安全功能保证要求（SAR）。企业可以实施和声明其产品的安全属性，并寻求实验室来评估其产品是否符合这些生命，从而获得CC认证。

ISO/IEC 15408主要包括三个部分内容：

- IT安全评估准则 Part1 介绍和通用模型。即 ISO/IEC 15408-1:2022, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model。
- IT安全评估准则 Part2 安全功能组件。即 ISO/IEC 15408-2:2022, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components
- IT安全评估准则 Part3 安全确认组件。即 ISO/IEC 15408-3:2022, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components

为了补充完善，后来又增加了2个部分：

- IT安全评估准则 Part4 评估方法和活动的规范框架。即 ISO/IEC 15408-4, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities
- IT安全评估准则 Part5 安全需求的预定义包。即 ISO/IEC 15408-5, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements

为了指导评估人员开展CC系列信息技术安全测评工作，ISO/IEC还发布了最小活动方法论。即 ISO 18045-2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation 是一个IT安全评估的方法论。该标准定义了测评工作者为了执行 ISO/IEC 15408 系列评估（使用ISO/IEC 15408 系列中提及的评估依据和评估证据）所需进行的最小活动。

国内标准参考ISO/IEC 15408:2009 制定了 GB/T 18336-2015 系列标准：

- GB/T 18336.1-2015 《信息技术 安全技术 信息技术安全评估准则 第1部分：简介和一般模型》
- GB/T 18336.2-2015 《信息技术 安全技术 信息技术安全评估准则 第2部分：安全功能组件》
- GB/T 18336.3-2015 《信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件》

GB/T 18336 作为评估信息技术产品及系统安全特性的基础准则，已被部分国内开发者应用于其所开发的相关产品及系统中。

基于CC的信息安全测评，包括三大部分：

（1）基本思路和一般模型。
一般模型定义了评估目标、安全目标、保护轮廓等概念和用法，规定了 ST 和 PP 的格式和要点。

（2）为满足安全功能要求（SFR），可供ST或PP选用的安全功能组件。
这些安全功能组件共分为11个大类，大类下面又分为不同的族、组件、组成要素。11个类型包括：

- 安全审计
- 通信
- 密码支持
- 用户数据保护
- 标识与鉴别
- 安全管理
- 隐秘
- TSF保护
- 资源利用
- TOE访问
- 可信路径/信道

CC评估不强迫使用所有功能组件。

（3）可供ST或PP选用的安全保障要求。
安全保障要求（SAR）涵盖：

- ST的评估准则
- TOE的开发

- 生命周期支持
- 指导性文件
- 测试
- 脆弱性评定

在开展SAR测评时，CC标准给出了7个评估保障级（EAL），每个评估保障级都将上面6个方面的要求细节进行了搭配和固化。

面向智能网联汽车的信息安全测评标准

2019 年 3 月 25 日，国家标准委下达第一批推荐性国家标准计划。汽标委智能网联汽车分标委提交的 4 项有关汽车信息安全的推荐性国家标准项目（汽车信息安全通用技术要求、电动汽车远程服务与管理系统信息安全技术要求、车载信息交互系统信息安全技术要求、汽车网关信息安全技术要求）获批立项，其中汽车信息安全通用技术要求中将以最高的防护目标定义共性的原则性技术要求。未来，这些技术要求可以用于汽车领域保护轮廓（类似于 CC 标准中 PP）的构建。

目前，国内汽车信息安全标准的制定工作正在有序推进，除上述基础通用及行业急需标准的制定外，汽车软件升级、汽车信息安全风险评估等应用类标准的制定也在有序开展，此外，汽标委还在系统开展汽车整车及零部件信息安全测试评价体系研究，启动车载硬件环境及操作系统相关标准体系规划及预研。本着“急用先行”的策略，中国智能网联汽车产业创新联盟、中国汽车工程学会等也在积极推进相关团体标准的制定，其中《智能网联汽车车载端信息安全技术要求》针对已经大规模使用的车载端信息安全定制了一套全面系统的技术要求供车厂和供应商借鉴，在提升车载端信息安全水平的同时，填补了我国智能网联汽车领域信息安全标准的空白。

从上述国内外智能网联汽车信息安全标准化工作来看，ISO/SAE 21434 将规范企业组织层面在信息安全管理和风险管理方面的要求，车辆上电子电气系统、系统间的接口交互、系统间的通信在安全生命周期内的信息安全技术要求、威胁分析与风险评估方法、安全策略、信息安全系统性的测试评价方法、信息安全流程开发管控要求。在已发布或即将发布的智能网联汽车信息安全标准中，ISO/SAE 21434 是一个重量级的标准，和 ISO 26262 在功能安全领域一样，是目前汽车信息安全最佳参考标准，可用于产品开发流程的评测，也将支持 WP29 后续的 CSMS 认证工作。因此，中国版 ISO/SAE 21434 ——GB 《整车信息安全技术要求及测试方法》，这一国家强制标准也在研制过程中。

术语与缩略语

- 评估对象（TOE）： 如软件、固件和/或硬件的集合，可能附带着指南（信息资料）。
- 资产（assets）： 评估对象（TOE）所有者赋予了价值的实体。
- 安全要求（security requirement）： 用标准化的语言陈述的要求，旨在达到TOE的安全目的。
- 安全目标（security target；ST）： 针对一个特定的已标识的TOE，且与现实相关的安全需求陈述。

- 保护轮廓（protection profile；PP）：针对一类TOE的、与实现无关的安全需求陈述。
- 评估（evaluation）：依据定义的准则对PP、ST或TOE进行的评价。
- TOE安全功能（TSF）：正确执行SFR所依赖的TOE的所有硬件、软件和固件的组合功能。

缩略语

TOE：评估对象
SAR：安全保障要求
SFR：安全功能要求
ST：安全目标
PP：保护轮廓
TSF：TOE安全功能

基本概念

TOE

评估对象（TOE）被定义为一组可能包含指南（信息、数据、配置）的软件、固件和/或硬件的集合。常见的TOE例子包括：

- 软件应用
- 操作系统
- 智能卡集成电路
- 密码协处理器（例如HSM）
- 包括所有终端、服务器、网络设备和软件的局域网
- 数据库应用
- 其他

智能网联汽车中的网络产品/组件、数据产品/组件均可认为是安全测评的评估对象。例如：CAN通信系统、车载以太网、T-Box、IVI、车机交互软件、ECUs中的芯片及固件等等。

TOE的表现形式

TOE的表现形式有多种，除了有实体外形的硬件（如域控制器）、网络（如CAN网络线路和网关），还包括各种软件或数据形态，例如：

- 配置管理系统中的文件列表
- 编译后的代码文件
- 准备交付客户的光盘、手册、升级包

- 已经安装和运行的软件版本
- 其他

TOE的不同配置

一般来说，车载信息产品同一般IT产品都可以使用多种方法配置：以不同的方法安装、使用不同的启用或禁用选项，由于在测评期间，它将确定TOE是否满足特定的要求。由于TOE的所有配置必须满足要求，所以这种配置上的灵活性可能会导致很多问题。为了便于开展测评，通常在TOE的指南部分对TOE可能的各种配置进行严格限制，换句话说，TOE的指南不同于车用IT产品的通用指南。

操作系统就是比较常见的例子。车机中安装的Andorid系统，可以多种方法进行配置，例如用户类型、允许/禁止WiFi默认连接、访问口令的设置等等。

如果同一款车用IT产品要成为一个TOE，并且依据一组合理的要求评估，则配置应该受到更加严格的控制，因为许多选项（如允许所有类型的外部链接或系统管理员不需要被鉴别）将导致TOE不能满足要求。

出于这些原因，车用IT产品或智能网联汽车整体的产品指南（允许多种配置）和TOE指南（仅允许一种配置或者在安全相关方面没有不同的配置）通常有所不同。

注意，如果TOE指南仍然允许多种配置，这些配置统称为TOE，其中的每种配置必须满足TOE的指定要求。

信息安全测评的目标读者

有三类群体对TOE安全测评感兴趣，分别是：

- 消费者：评估是为了满足消费着的需求，这是评估过程的基本目的和理由。消费者可以使用评估结果来帮助决定一个TOE是否满足他们的安全需求，这些安全需求通常是风险分析和策略指导的结果。消费者也可以使用评估结果来比较不同的TOE。安全测评/评估为消费者，尤其是消费者群体和行业团体，提供一个独立于实现的结构，即保护轮廓（PP），在其中以一种明确的方式表达他们的安全要求。
- 开发者：安全评估为开发者准备并协助他们对TOE的测试，以及标识TOE满足的安全要求。这些安全要求包含在一个与实现相关的ST中。ST可以基于一个或多个PP，来说明ST符合消费者在这些PP中制定的安全要求。安全评估还可以用于确定责任和行为，以便于提供TOE满足安全要求的必要证据。它也定义了证据的内容和形式。
- 评估者：安全评估包含了用于评判TOE与其安全要求是否相符的原则和结果。

信息安全测评的背景

为了使信息安全测评具有更好的可比性，测评/评估应在权威的评估体制框架内执行，该体制框架负责制定标准、监控评估质量、管理评估机构和评估者必须符合的规章制度。例如：CNAS、CMA体制。

不同的信息安全测评/评估机构的测评框架必须一支，以达到相互认可评估结果的目标。

使评估结果具有更好的可比性的第二种方法是使用通用方法达到这些效果。通用方法的使用主要是确保评估结果的可重复性和客观性，但仅靠评估方法本身是不充分的。许多评估准则需要使用专业的判断和背景知识，而这些较难达到一致。为了增强评估结论的一致性，最终的评估结果可能提交给认证过程来处理。

认证过程是对测评/评估结果的独立审查，并产生最终的证书或正式批文，该证书通常是公开的。

信息安全评测方法基本框架

一般模型

本文所讨论的面向智能网联汽车的信息安全测评方法，将依据CC信息安全测评标准（ISO/IEC 15408:2022）展开，即开展信息安全评估有两个重要的环节：

第一步，对确定的安全目标的评估。安全目标可以遵从某个PP，也可以没有PP而是针对特定产品而编写。提出ST 和 PP的基本准则是根据某个或某类产品需要保护的信息资源的价值、以及此（类）产品使用环境收到敌意攻击的威胁程度，来选取合适的安全功能组件和安全保障级别。如果此（类）产品实现了所要求的安全功能组件，并且这些功能的设计和实现是达到了所要求的安全保障级别的，那么从理论（即CC的理想）上讲此（类）产品有能力抵御来自所处的使用环境的威胁，因而能够有效保护所拥有的信息资产。安全目标的制定应符合CC标准的第一部分一般威胁模型的方法。

第二步，CC评估的是对安全目标中所定义的TOE的评估。这一步的评估要点在于通过对产品的设计文档、代码实现、生产流程、使用安装、功能测试、脆弱性分析等等多个角度和方面来衡量判定此产品是否真正地实现了在其ST中所宣称的安全功能，是否真正地达到了所宣称的安全保障级。这里要强调指出的是，ST中指定的安全保障级中包含的安全保障要求将贯彻覆盖到所选用的全部的安全功能组件。

对于EAL1到EAL4的CC评估，CCRA 还发布了通用标准评估方法论（Common Criteria Evaluation Methodology，简称CEM），并被接纳为国际标准ISO/IEC 18405。

概括来讲，CC评估是基于CC第一部分提出安全威胁模型，该模型根据产品面临的安全问题（假定、威胁和组织安全策略），确定安全目标，并根据CC第二部分的安全功能要求选择产品的安全功能，基于CC第三部分的安全保障要求开展CC评估。

下面介绍其一般模型中的要素和评估要点。

资产与对策

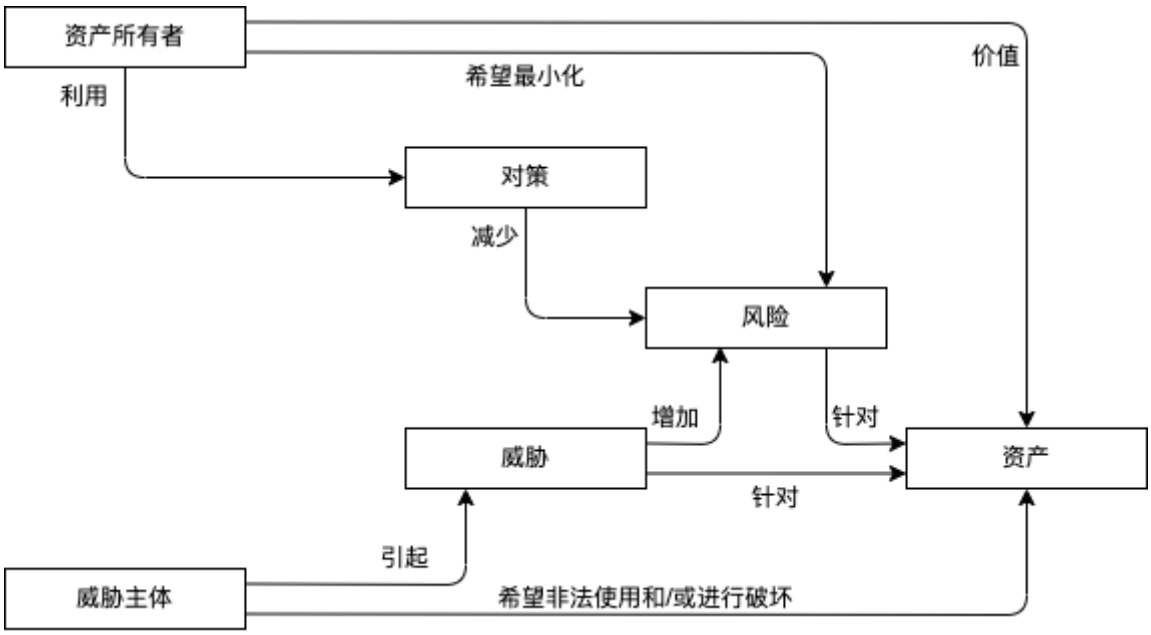
安全与资产保护有关，资产是赋予了价值的实体，智能网联汽车相关资产的例子有：

- 车内用户隐私数据
- 自动驾驶域控制器
- 路径规划算法
- 带有HSM功能的SoC芯片
- CAN车载通信系统
- WiFi 网络
- 蓝牙钥匙
- OTA升级包
- 车机Andorid 系统的镜像文件和配置
- TSP 访问能力
- 远程控制的可用性

为了避免过于主观的估计使任何事物成为资产，通常我们将资产放置的环境成为运行环境，例如：

- 车辆机仓
- 4G移动通信环境

许多资产均以信息的形式由车用IT产品存储、处理和传送，以满足信息所有者的要求。信息所有者为乐信息的可用性，会严格控制信息的传播和修改，并且资产受到保护措施的保护以抵御威胁。下图说明了这些概念和关系。

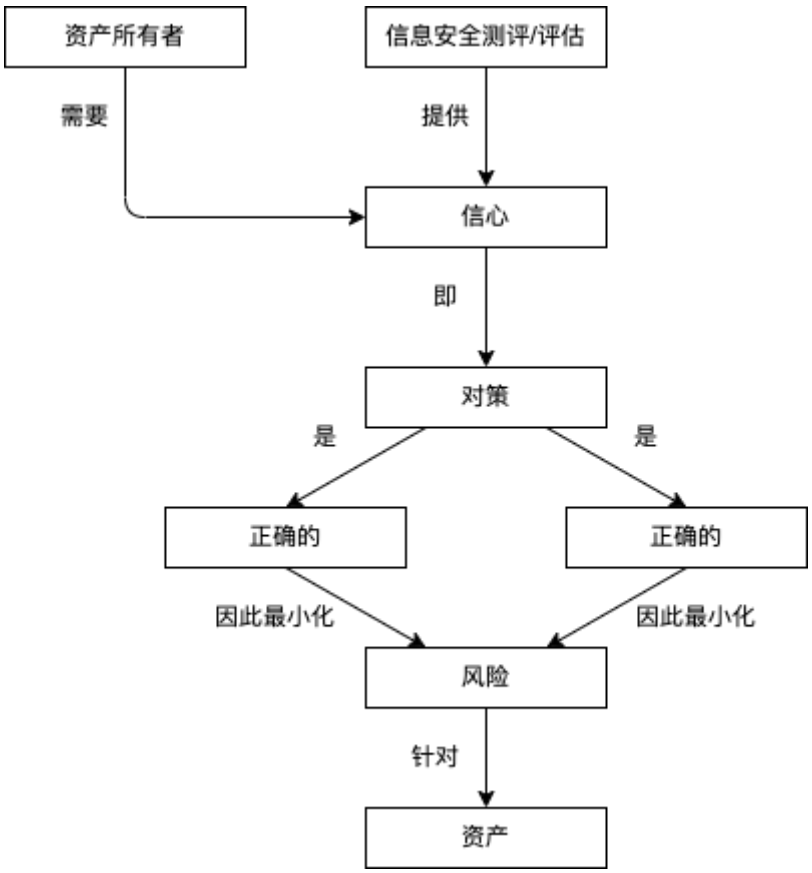


保护资产是对资产赋予价值的所有者的责任。实际或假想的威胁主体，也可能对资产赋予价值，并试图以危害资产所有者利益的方式滥用资产。威胁主体的例子包括：黑客、恶意用户、非恶意用户的不当操作、计算机进程和事故。

资产所有者可能要对资产负责，因此，应有足够的理由支持资产所有者做出决定，以接受由资产暴露给威胁所带来的风险。为了支持这项决定，应该能够证明下面两方面：

- 对策是充分的：如果对策做了声称要做的事，就能够对抗威胁；
- 对策是正确的：对策做了声称要做的事。

许多资产所有者事缺少必要的知识、专业技术和资源来判断对策的充分性和正确性，他们不希望仅依赖于开发者，因此所有者/消费者会引入评估，以增加对所有或部分对策的充分性和正确性的信心。下图描述了信息安全测评/评估的概念及关系。



对策的充分性

在安全测评/评估中，对策的充分性是通过一个称为安全目标的概念来分析的。安全目标从描述资产和对这些资产的威胁开始，然后安全目标描述对策（以安全目的形式），并证实这些对策对于对抗这些威胁是充分的，如果对策做了声称要做的事情，那么对策就足以对抗威胁。

安全目标将对策划分为两组：
（1）TOE的安全目的：描述了需要在评估中确定其正确的对策；
（2）运行环境的安全目的：描述了不需要在评估中确定其正确性的对策。

这样划分的理由是：

- 信息安全测评仅适合评估信息、网络、数据等IT相关对策的正确性，因此非IT类对策（机械装置、功能安全、企业治理）总是放在运行环境中考虑。
- 对策的正确性评估耗费时间和金钱，因此苹果所有对策的正确性不一定可行。
- 某些对策的正确性可能已经在其他评估中评估过了，因此再次评估无成本效益。

安全目标证实了安全功能要求（SFRs）满足TOE安全目的，TOE安全目的和运行环境安全目的足以对抗威胁，因此SFR和运行环境安全目的足以对抗威胁。这样看来，正确的TOE与正确的运行环境结合起来对抗威胁。

TOE的正确性

TOE的设计和实现可能不正确，可能因此包含着导致脆弱性的错误，攻击者通过利用这些脆弱性，可能破坏和/或滥用资产。这些脆弱性可能由开发时的意外错误、糟糕设计、故意添加的恶意代码和糟糕的测试等引发。为了确定TOE的正确性，可以执行的活动包括：

- 测试TOE
- 检查TOE的各种设计表示
- 检查TOE开发环境的物理安全

安全目标以安全保障要求（SAR）的形式提供了这些活动的结构化描述，以确定正确性。这些安全保障要求用标准化语言来表示，以保证正确性和可比性。

开展信息安全测评的基本方法在于针对给定的测评对象，首先确定其安全目标，然后根据相关标准或行业一致性方法对测试目标进行安全功能和安全保障的测评。如果满足了SAR，那么就可保障TOE的正确性，因此TOE几乎不可能包含可以被攻击者利用的漏洞。在TOE正确性方面的保障程度，由SAR本身确定，“弱”的SAR所能提供保障少，而许多“强”的SAR可提供更安全的保障。

运行环境的安全性

运行环境的设计和实现也可能不正确，因此可能包含导致脆弱性的错误，攻击者通过利用这些脆弱性，仍然可以破坏和/或滥用资产。通常，安全测评无法保障运行环境的正确性，换句话说，运行环境的安全性通常不做评估。就评估过程而言，运行环境被假设为可以100%实现运行环境安全目的。

这并不排除TOE的消费者使用其他方法确定运行环境的正确性，例如：

- 对于一个操作系统，运行环境安全目的生命“运行环境将确保来自不可信网络的尸体只能通过ftp访问TOE”，消费者可以选择一个经过评估的防火墙，配置它为仅允许通过FTP对TOE进行访问。
- 如果运行环境安全目的生命“运行环境将确保所有管理人员没有恶意行为”，消费者可以调整其与管理人员的合同，使其包括对恶意行为的惩罚性制裁，但这不是信息安全测评的一部分。

信息安全测评/评估

基于CC标准，我们认可两种形式的评估：一是下面描述的ST/TOE评估（多数情况）；二是ISO/IEC 15408-3中定义的PP评估。

ST/TOE 评估分为两步进行：
（1）ST评估：确定TOE和运行环境的充分性；
（2）TOE评估：确定TOE的正确性，就像前面所说的，TOE评估不评估运行环境的正确性。

ST评估，应用安全目标评估准则对安全目标进行评估。

TOE评估更为复杂，TOE评估的主要输入是：评估证据，包括TOE和ST，通常也包括来自开发环境的输入，如设计文档或开发者测试结果。TOE评估由适用于SAR（来自安全目标）的评估证据组成。准则应用的SAR的方法，是由所使用的评估方法确定的。应用SAR的结果如何被文档化，需要生成的报告及细节由适用的评估方法及执行评估的评估体制确定。

TOE评估过程产生的结果为下列两种情况之一：

- 并未满足所有SAR，因此评估结果未达到ST中所述的TOE满足SFR的特定保障级别；
- 满足所有SAR，因此评估结果达到了ST中所述的TOE满足SFR的特定保障级别。

TOE评估可以在TOE开发完成之后进行，或者与TOE开发并行。

安全需求的制定

为了允许消费者群体或公共监管部门表达他们的安全需求并编写ST，有两个特殊的概念需要被掌握：保护轮廓（PP）和包（Package）。

包

包是一个安全要求的命名集合。一个包可以是：

- 只包含安全功能要求（SFR）的功能包；
- 只包含安全保障要求（SAR）的保障包

不允许同时包含SFR和SAR的混合包。

包可以由任何团体定义，意在可重用。为此，他应该包含有用且易于组合的要求。包可以用于构造更大的包，PP和ST。目前没有评估包的准则，因此，任意SFR或SAR的集合都可以成为一个包。保障包的例子是评估保障级EAL。

保护轮廓

虽然ST通常用于描述一个特定的TOE（如某车型特定型号版本的T-Box），PP却意在描述一类TOE（例如一般意义的T-Box）。因此，相同的PP可以作为模版用于构造许多不同评估的ST。

一般来说，ST为一个TOE描述要求，由TOE的开发者编写，而PP为一类TOE描述通用要求，典型的编写者为：

- 为一个给定的TOE类型寻求一致要求的用户；
- TOE的开发者，或者系统为该类型TOE建立最小基线的类似TOE开发群体；
- 为采购过程而详细说明其要求的组织，例如政府或大型公司。

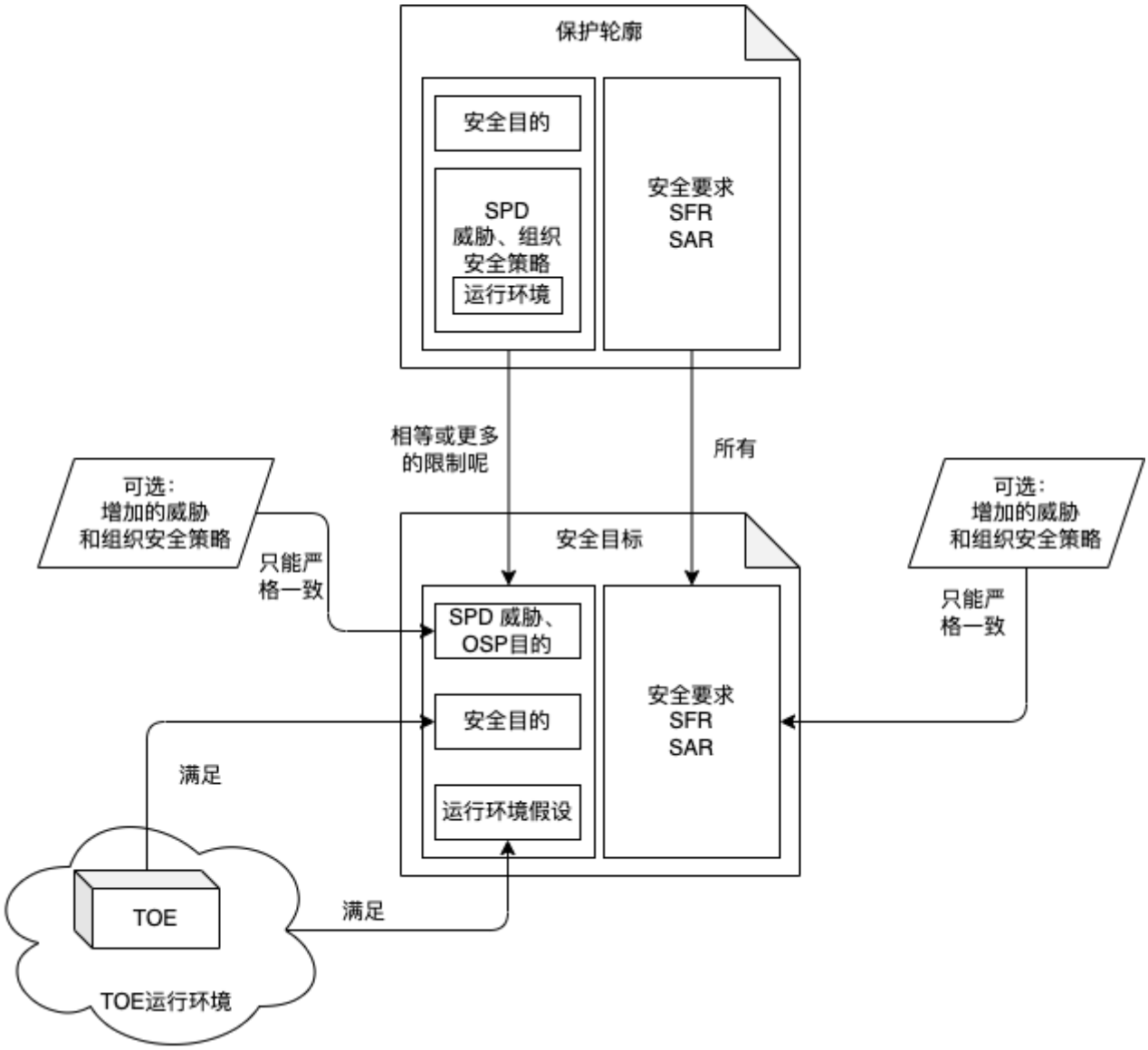
PP确定了允许ST符合（保持一致）PP的方式，即PP生命规定了ST符合的方式是：
（1）如果PP声明需要满足严格的符合性，ST就应严格地与PP符合；
（2）如果PP声明需要满足可论证的符合性，ST就应以严格的或可论证的方式与PP符合；

换言之，如果PP明确允许可论证的符合性，那么仅允许ST以至少可论证的方式与PP符合。

如果ST声明与多个PP符合，它将以PP规定的方式（上述两种）与每个PP符合。注意，ST与PP符合是否存在不一致或可能被质疑。因为基于CC的信息安全测评不认可“部分符合”。因此PP作者的责任是确保PP不会过于繁琐，而妨碍PP/ST作者声明与这样的PP符合。

由于一下认识，ST等同于PP，活着ST比PP约束更多：
（1）所有满足该ST的TOE也满足该PP；
（2）所有满足该PP要求的运行环境也满足该ST的要求。

通常，ST比PP对TOE施加相同或更多的家限制，并对TOE的运行环境施加相同或更少的限制。



使用保护轮廓和包

如果ST声明与一个或多个包和/或保护轮廓相符合，ST的评估将证实ST实际上与他们声明符合的包或PP符合。

这允许出现以下过程：

（1）一个寻求获取特定类型IT安全产品的组织，根据其安全需求开发一个PP，使其通过评估并发布；

（2）开发者采用这个PP，编写ST以声明与其相符合，并使用其通过ST评估；

（3）然后开发者构造TOE（或者使用一个一存在TOE），并使TOE对照该ST进行评估。

结果是开发者能够证明他的TOE与组织的安全需求相符合；组织因此能够购买该TOE。

使用多个保护轮廓

基于CC标准的信息安全测评，运行一个PP与其他PP符合，允许给予以前的PP构造PP链。

例如：可以使用域控制器集成电路的PP和嵌入式OS的PP，构造一个域控制器PP（涵盖了硬件安全和操作系统安全），在域控制器PP中声明与另外两个PP符合，然后可以基于域控制器PP和应用软件PP，编写IVI系统的PP。最后，开发者可以基于这个PP构造一个面向IVI设备的ST。

安全要求及其裁剪

通常，基于CC的安全确认需要利用安全功能和安全保障实现安全要求。可以严格按照 ISO/IEC 15408-2 和 ISO/IEC 15408-3 中的定义使用，也可以使用允许的操作进行裁剪。当使用这些裁剪操作时，PP/ST 的作者应当注意其他要求对此要求的依赖关系应得到满足。允许的操作包括：

（1）反复：允许一个安全功能组件/安全保障组件在不同操作时被使用一次以上；

（2）赋值：允许指定参数；

（3）选择：允许从一个列表中选定一项或多项；

（4）细化：允许增加细节。

复制和选择操作只允许用于组件中明确指定的位置，反复和细化允许用于所有组件。

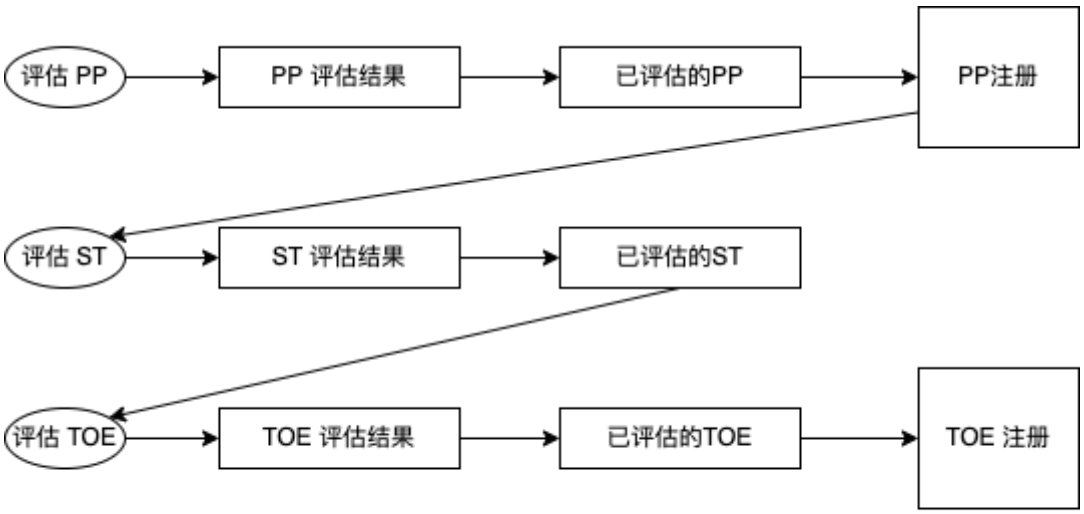
评估结果

根据CC标准执行的PP和ST/TOE评估过程，将产生下列结果：

（1）PP评估产生的一评估的PP目录。

（2）TOE评估框架中使用的ST评估的中间结果。

（3）ST/TOE评估产生的已评估的TOE目录。在许多情况下，这些目录指的是TOE所在的IT产品，而不是特定的TOE。因此目录中的IT产品不应解释为整个IT产品已经被评估过，ST/TOE评估的实际范围由ST定义，需要参考相关目录示例的参考手册。



评估结果示意图

ST 可以基于包、以评估的活未被评估的PP，但是没有强制要求，因为 ST 不必基于任何包或PP。评估应能产生能引为证据的客观的和可重现的结果，即使没有绝对客观的尺度来衡量安全评估结果时也应如

此。存在一套评估准则是使评估产生有意义的结果的必要前提条件，这也为不同评估机构之间互认评估结果提供了技术基础。

一个评估结果代表了对TOE安全特性进行专门考察时的结果。这个结果并不自动保证适用于任何特定应用环境。允许一个TOE在特定应用环境下使用的决策，应给予对多个安全因素的考虑，包括评估结果。

PP 评估结果

基于CC的安全测评框架包含了要求评估者参考的评估准则，以便声明 PP 是完备的、一致的和技术合理的，因此适用于在开发ST中。评估结果也应包括“符合性声明”。

ST/TOE 评估结果

基于CC的安全测评框架包含了要求评估者参考的评估准则，以便确定ST中是否存在TOE满足SFR的充分保障。因此，TOE评估将为ST给出通过/失败的结果。如果ST和TOE的评估结果均为通过，其基础产品就是合格的，包含在注册库中。评估结果也应该包括“符合性声明”。

可能有这种情况，评估结果要在随后的认证过程中使用，这个认证过程与评估过程不相同，本文不做讨论。

符合性声明

符合性声明表示要求集合的来源由通过评估的PP或ST来满足，该符合性声明包含了一个基于CC的符合性声明：
（1）PP或ST声明符合的ISO/IEC 15408 的版本的描述。
（2）与ISO/IEC 15408-2（安全功能要求）的符合性描述：
（2.1）ISO/IEC 15408-2 符合：如果PP或ST中所有SFR仅仅基于 ISO/IEC 15408-2 的功能组件，那么该PP或ST与ISO/IEC 15408-2是符合的，或
（2.2）ISO/IEC 15408-2 扩展：如果PP或ST中有一个SFR不是基于 ISO/IEC 15408-2 的功能组件，那么该PP或ST与ISO/IEC 15408-2是扩展的。
（3）与ISO/IEC 15408-3 （安全保障要求）的符合性描述：
（3.1）符合：如果PP或ST中所有SAR仅仅基于 ISO/IEC 15408-3 的保障组件，那么该PP或ST与ISO/IEC 15408-3是符合的，或
（3.2）ISO/IEC 15408-3 扩展：如果PP或ST中有一个SAR不是基于 ISO/IEC 15408-3 的功能组件，那么该PP或ST与ISO/IEC 15408-3是扩展的。

另外，符合性声明也可以包括与包有关的陈述，可以包括如下情况：
（1）包选定符合：一个PP或ST与一个预定义的包符合（如 EAL），如果：
（1.1）PP 或 ST 中的SFR与包中的SFR相同，或
（1.2）PP 或 ST 中的SAR与包中的SAR相同。
（2）包选定增强：一个PP或ST是一个预定义的包的增强，如果：

（2.1）PP或ST中的SFR包含了所有包中的SFR，但至少增加了一个SFR或者有一个SFR级别高于包中的一个SFR；
（2.2）PP或ST中的SAR包含了所有包中的SAR，但至少增加了一个SAR或者有一个SAR级别高于包中的一个SAR。

注意，当一个给定ST的TOE被成功评估了，ST的任何符合性声明TOE也应遵循，因此TOE也可以是如ISO/IEC 15408-2 符合的。

最后，符合性声明也可以包括两个域保护轮廓相关的陈述：
（1）PP符合，一个PP或者TOE满足特定PP，该PP作为符合性结果列出。
（2）符合性陈述（仅对PP）：该陈述描述了PP或ST必须与相关的PP符合的方式；严格的活可论证的。

使用ST/TOE评估结果

一旦ST和TOE经过评估，资产所有者可以获得TOE及其运行环境对抗威胁的保障（在ST中定义的），评估结果可以由资产所有者用于决定是否接受资产暴露给威胁的风险。

然而，资产所有者应该仔细检查是否存在下列情况：
（1）ST中的安全问题定义是否匹配资产所有者的安全问题。
（2）资产所有者的运行环境与ST描述的运行环境安全目的是否相符。
如果上面两种情况不相符，那么TOE可能不适用于资产所有者的目的。

另外，一旦一个已经评估的TOE处于运行中，TOE中以前的未知错误或脆弱性仍然可能出现，这时开发者可以修正TOE（修复漏洞），或者修改ST从评估范围中排除该脆弱性。无论哪种情况，旧的评估结果可能不再有效。

如果需要重新获得信心，需要重新评估。