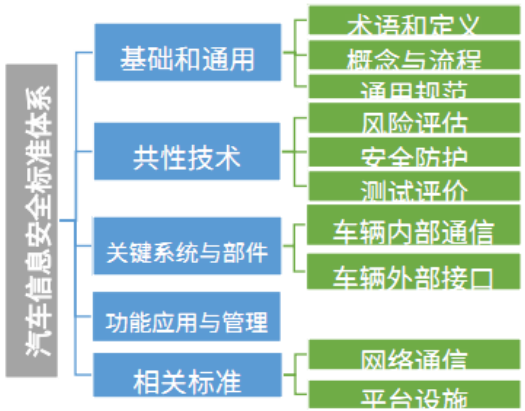
汽车信息安全风险评估标准化需求研究报告解读
Interpretation of Standardization Requirements Research Report on Automotive Cyber Security Risk Assessment

报告人：郭盈

2021.7.8

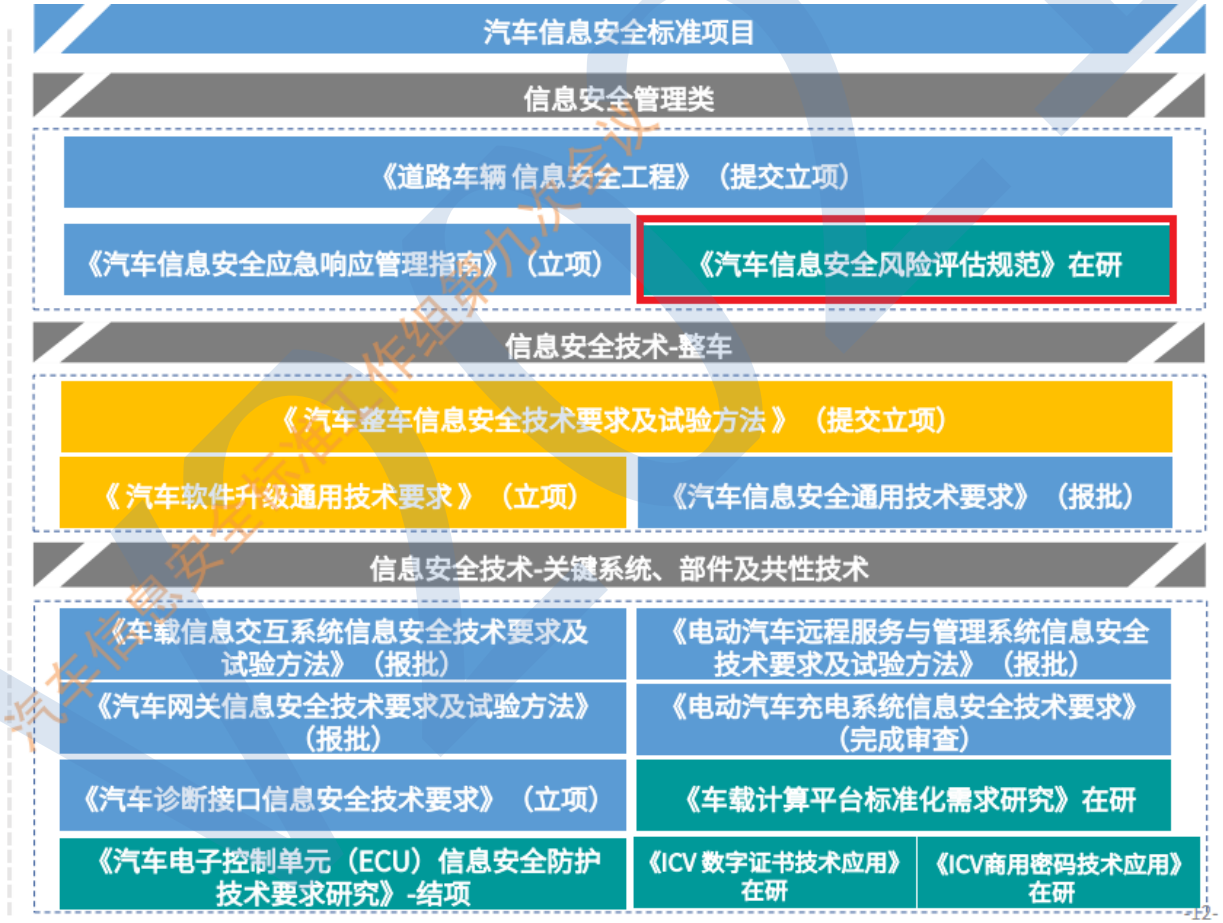
信息安全工作组依据体系规划截止目前已分4批次开展了15项标准制定及研究项目，涵盖整车、系统部件技术与过程管理类标准。



GB 强制性国家标准

GB/T 推荐性国家标准

预研 标准化需求研究



汽标信息安全标准体系
System of SAC/TC114/SC34 Information Security WG

汽车信息安全风险评估研究报告

起草单位：

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）

中国汽车技术研究中心有限公司

国汽（北京）智能网联汽车研究院有限公司

东风汽车集团有限公司技术中心

东风商用车有限公司

中国第一汽车股份有限公司

大众汽车（中国）投资有限公司

北京航空航天大学

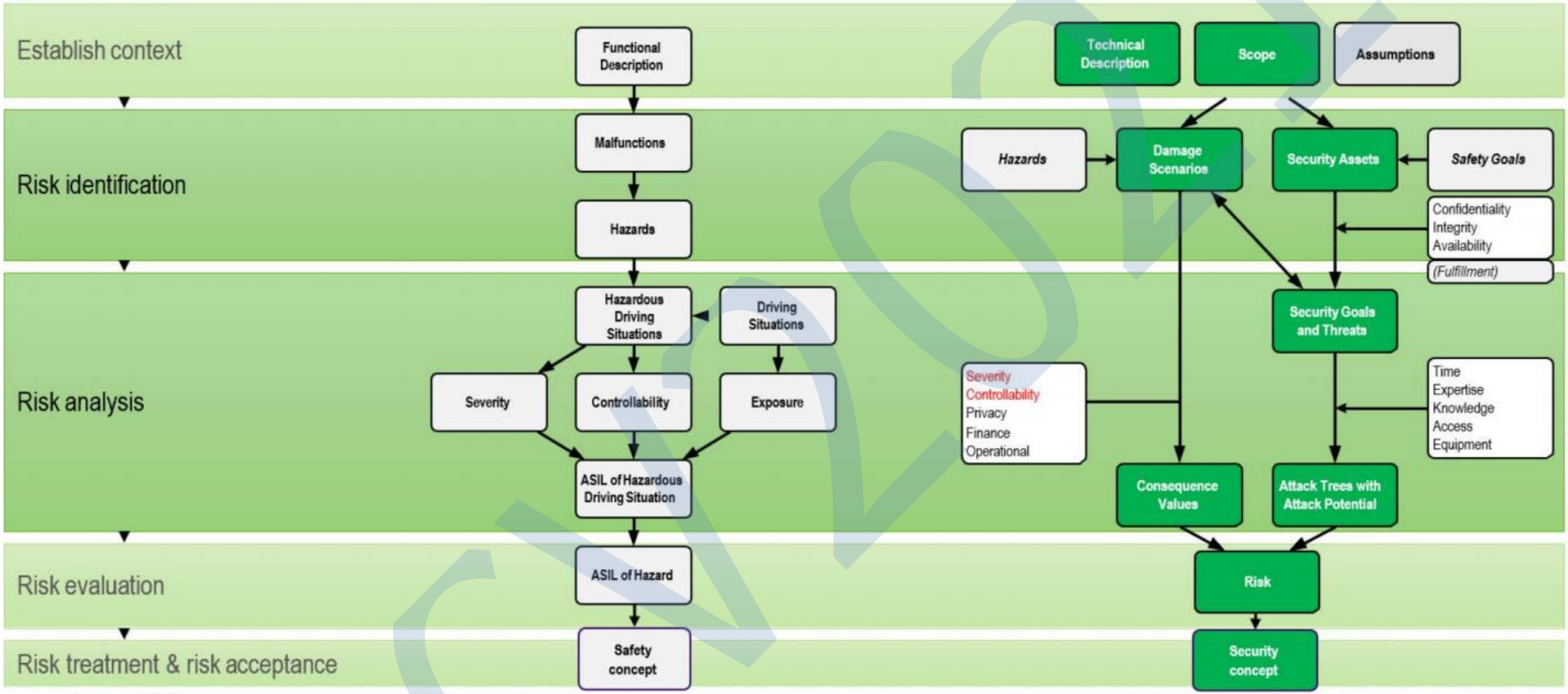
博世汽车部件（苏州）有限公司

广东为辰信息科技有限公司

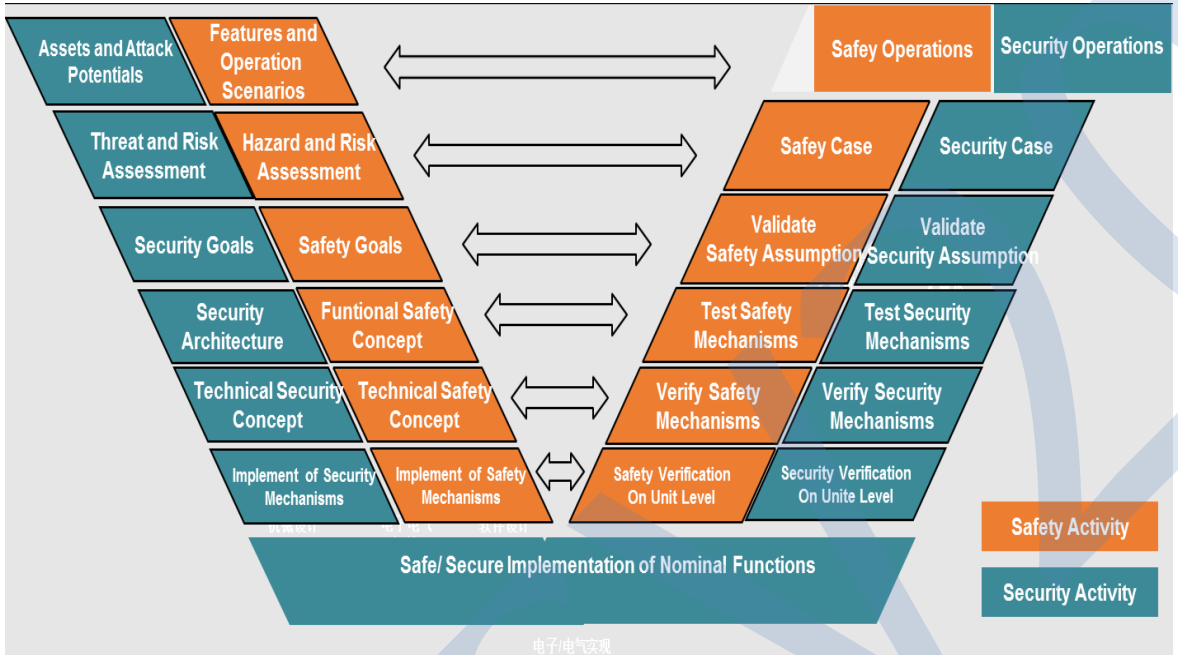
中国信息通信研究院

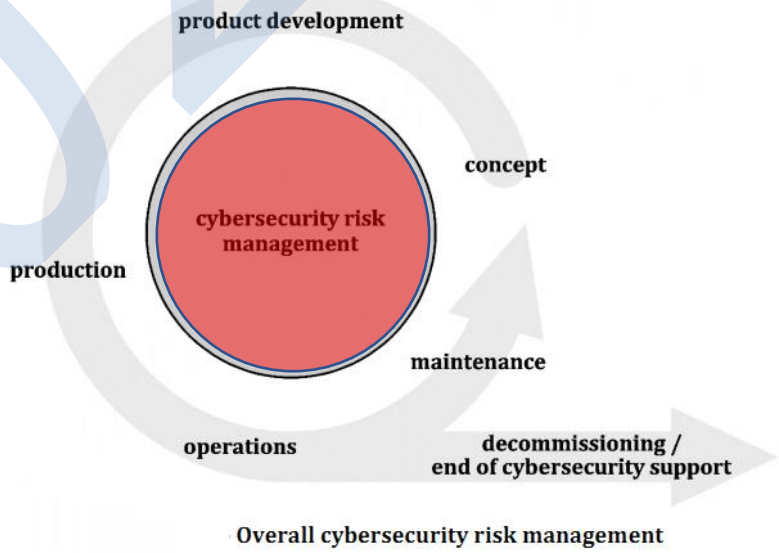
沃尔沃汽车技术（上海）有限公司

汽车信息安全风险评估标准化需求研究报告框架
Standardization Requirements Research Report on Automotive Cyber Security Risk Assessment

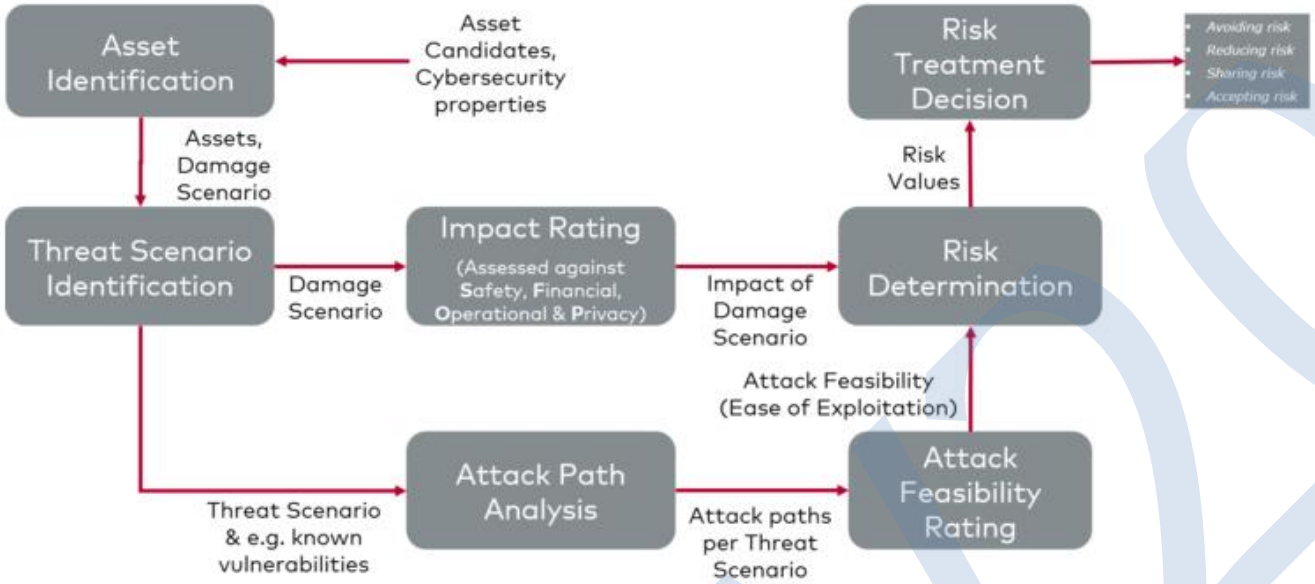


ISO 26262 Vs. ISO/SAE21434
HARA/TARA危害分析与风险评估/威胁分析与风险评估





安全风险评估扮演的角色/Role of CyberSecurity Risk Assessment



资产识别 Asset Identification
威胁场景识别 Threat Scenario Identification
影响评级 Impact Rating
攻击路径分析 Attack Patch Analysis
攻击可行性分析 Attack Feasibility Rating
风险值计算 Risk Value Determination
风险处置策略 Risk Treatment Decision

15. Threat analysis and risk assessment methods

15.3 Asset identification	15.4 Threat scenario identification	15.5 Impact rating	15.6 Attack path analysis	15.7 Attack feasibility rating	15.8 Risk value determination	15.9 Risk treatment decision

汽车信息安全风险评估流程
Process of ICV CyberSecurity Risk Assessment
Risk assessment in cybersecurity is used to determine what negative actions could occur and their associated likelihood, resulting in an overall risk value
网络安全风险评估用于确定可能发生的负面行为及其相关可能性，从而得出总体风险值

资产识别

具有价值或贡献价值的对象（通常，资产有一个或多个**网络安全属性**，这些属性的破坏可能会导致一个或多个危害场景）

网络安全属性 = 保密性、完整性、可用性

即：

识别网络安全属性被侵犯的对象

Asset Identification

Object that has value, or contributes to value. (An asset **has one or more cybersecurity properties** whose compromise can lead to one or more damage scenarios

Cybersecurity property = C、I、A

Identify object whose cybersecurity properties could be violated (damage scenario)

Eg 举例

功能类别	子类别	详细资产
网络	车内网络	总线、车载以太网等
	车外网络	WIFI、C-V2X、蓝牙、GPS、GNSS 等
网络设备	边界设备	TBOX、OBU 等
	车内设备	总线网关、以太网网关等
车载系统	娱乐系统	车机、导航系统等
	动力总成控制	发动机管理系统（EMS）、自动变速器控制系统（ATCS）、整车控制器（VCU）、混合动力控制单元（HCU）和驱动电机控制器（MCU）等
	底盘控制	气囊控制单元、转向控制单元、ADAS 系统单元、 刹车控制单元及传感器
	车身控制系统	仪表组、中央门锁控制系统（CLCS）、车灯控制单元、车窗控制单元安全带、安全气囊系统（SRS）
	自动驾驶系统	ADAS、无人驾驶系统

威胁场景识别

识别损害情况发生潜在原因

威胁场景识别是系统的识别和分析可能危及资产网络安全属性的威胁场景的过程。识别出的威胁场景应与相应的资产和损害场景相关联，一个损害场景可对应多个威胁场景。可利用头脑风暴、误用案例提取等方法列举威胁

Threat Scenario Identification

Identify way(s) in which a damage scenario could occur

Threat scenario identification is the process of system identification and analysis of threat scenarios that may endanger the network security attributes of assets. The identified threat scenario should be associated with the corresponding asset and damage scenario, and one damage scenario can affect multiple threat scenarios. Use methods such as brainstorming and misuse case extraction to enumerate threats

Eg STRID举例

Threat	Example Asset	Security attribute
Spoofing	Sensor	Authenticity
Tampering	Software, messages	Integrity
Repudiation	Wireless communication	Non-repudiation
Information Disclosure	Cryptographic keys, log data	Confidentiality
Denial of Service	In-vehicle communication, CPU	Availability
Elevation of Privilege	Features (enabling/disabling)	Authorization

脆弱性分析

识别可能被用于攻击的缺陷和弱点，自身的问题

如：需要实现特定的威胁场景

弱点的举例：

1）缺少需求或规范

2）架构和设计缺陷，包括不正确的安全协议设计

3）软件或硬件的设计缺陷

4）操作过程或程序自身的缺陷

5）使用过时或废弃的函数

脆弱性与弱点的关系？

脆弱性：可以作为攻击路径的一部分加以利用的弱点

Vulnerability Analysis

Identify potential flaws and weaknesses in the product that could be used in an attack

i.e. needed to realize a particular threat scenario

Systematic identification and evaluation of Vulnerability.

Weakness:

eg，1)missing requirement or specification

2)architectural or design flaw, including incorrect design of a security protocol

3)implementation weakness, including hardware and software defect, incorrect implementation of a security protocol

4)flaw in the operational process or procedure, including misuse and inadequate user training

5)use of an outdated or deprecated function, including cryptographic algorithms

Weakness Vs. Vulnerability

影响分析

如果损害发生，分析其损害程度

关注利益相关者在安全、操作、财产和隐私方面的影响

严重、高、中、低（级别）

Impact Analysis

Determine the level of impact if the damage scenario were to be realized.

Impact to the stakeholders in regarding to SOFP

Safety, Operational, Financial, Privacy

Impact rating=> severe, major, moderate, negligible

(a) Safe operation of vehicle affected;

(b) Vehicle functions stop working;

(c) Software modified, performance altered;

(d) Software altered but no operational effects;

(e) Data integrity breach;

(f) Data confidentiality breach;

(g) Loss of data availability;

(h) Other, including criminality.

序号	等级	描述
1	低	• 安全：人身安全不受影响（AIS 0） • 财务：可忽略不计的财务损失 • 操作：可忽略的操作损害，导致车辆功能或性能的不明显降级 • 隐私：可以忽略不计的影响 • 法律：法律法规以及合同的违背是可修复的
2	中	• 安全：人身安全受到轻度影响（AIS 1——表层受伤、肌肉疼痛等） • 财务：中等财务损失，与车辆子系统价值相当 • 操作：操作损害导致车辆功能或性能的部分降低 • 隐私：违反 PII 隐私保护规定，为影响对象带来不便 • 法律：法律法规以及合同的违背将导致受到惩罚
3	高	• 安全：人身安全受到较大影响（AIS 2-4——人员受伤但不威胁生命） • 财务：严重财务损失，与整车价值相当 • 操作：操作损害导致车辆功能或性能严重下降 • 隐私：违反 PII 隐私保护规定，为影响对象带来严重但可克服的影响 • 法律：法律法规以及合同的违背将导致严厉的法律后果（如刑事诉讼）以及惩罚
4	极高	• 安全：人身安全受到致命危害（AIS 5-6——生命威胁或死亡） • 财务：财务损失超出了整车价值，可能导致个人破产 • 操作：操作损害导致车辆不工作，直至车辆不可操作 • 隐私：违反 PII 隐私保护规定，为影响对象带来无法克服的影响 • 法律：法律法规以及合同的违背将导致无法预计的法律后果

攻击路径分析

确定实现威胁场景所需的步骤

攻击路径，一套深思熟虑的步骤来实现威胁场景

方法：

1）自顶向下，通过分析可以实现威胁场景的不同方式来推断攻击路径。如攻击树，攻击图（概念、开发阶段）

2）自底向上，从已识别的网络安全漏洞构建攻击路径（实现完成阶段）

Attack Path Analysis

Identify the steps required to realize a threat scenario

Attack path, set of deliberate actions to realize a threat scenario

Approaches

1） Top-Down approaches

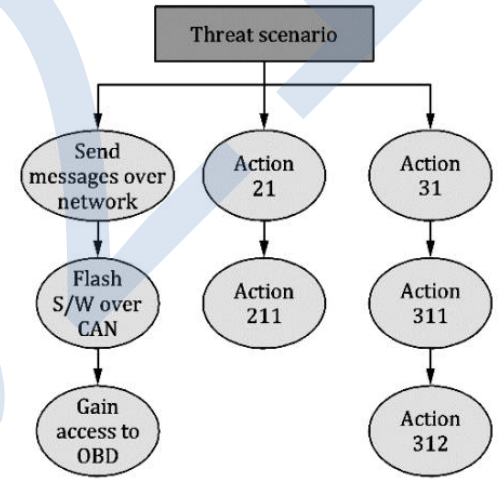
deduce attack paths by analyzing the different ways in which a threat scenario could be realized. E.g. Attack trees, attack graph

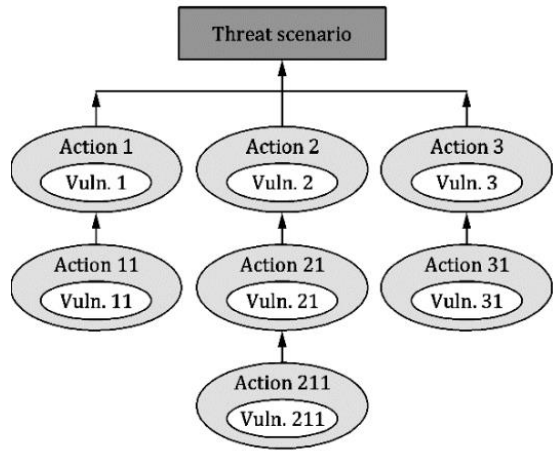
（**concept and development phases** ）

2） Bottom-Up approaches

build attack paths from the cybersecurity vulnerability identified

（**Implementation of the item or component is available**）





Methods for determining attack paths

攻击可行性分析

评估执行特定攻击路径步骤的可行性

方法：

1）基于攻击潜力分析

2）基于CVSS评分分析

3）基于攻击向量分析

Elapsed time		Specialist expertise		Knowledge of the item or component		Window of opportunity		Equipment	
Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value
≤ 1 day	0	Layman	0	Public	0	Unlimited	0	Standard	0
≤ 1 week	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
≤ 1 month	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
≤ 6 months	17	Multiple experts	8	Strictly confidential	11	Difficult/ none	10	Multiple bespoke	9
> 6 months	19								

攻击向量（V）	网络/邻居/本地/物理	0.85/0.62/0.55/0.2
攻击复杂度（C）	低/高	0.77/0.44
权限要求（P）	无/低/高	0.85/0.62/0.27
用户交互（U）	不需要/需要	0.85/0.62
攻击可利用率（E）=8.22×V×C×P×U E 在 0.12～1.05 之间，攻击可被利用性为很低，给 1 分； E 在 1.06～1.99 之间，攻击可被利用性为低，给 2 分； E 在 2.00～2.95 之间，攻击可被利用性为中，给 3 分； E 在 2.96～3.89 之间，攻击可被利用性为高，给 4 分。		

攻击向量（V）	网络/邻居/本地/物理	高/中/低/很低
注： 对应等级评估分值：4、3、2、1		

Attack Feasibility Analysis

Estimate the feasibility to carry out the steps of a particular attack path

Approaches

1） The attack potential-based approach

elapsed time, expertise, equipment, Knowledge, windows of opportunity

2） The CVSS-based approach

attack vector, attack complexity, privileges required, user interaction

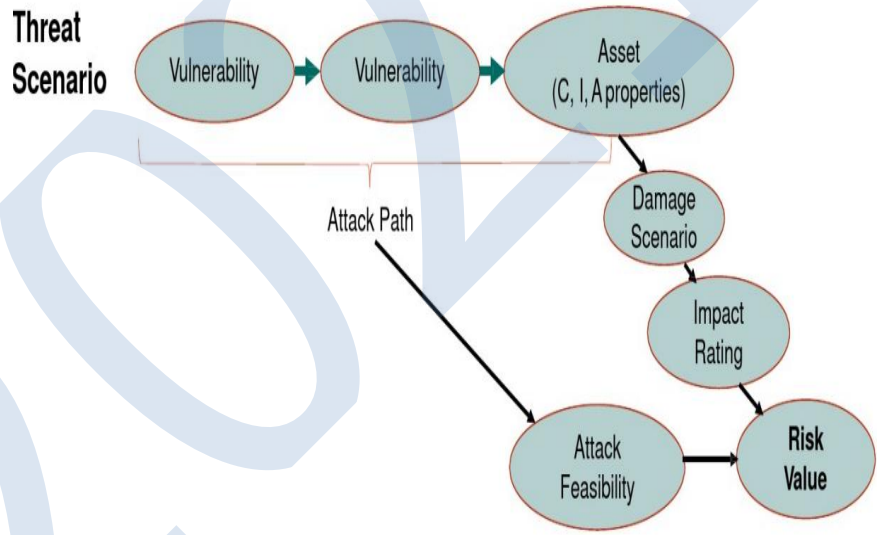
3） The attack vector-based approach

风险值计算

由相关破坏场景的影响和相关攻击路径的攻击可行性来确定。

Risk Value Determination

Determined from the impact of the associated damage scenarios and the attack feasibility of the associated attack paths



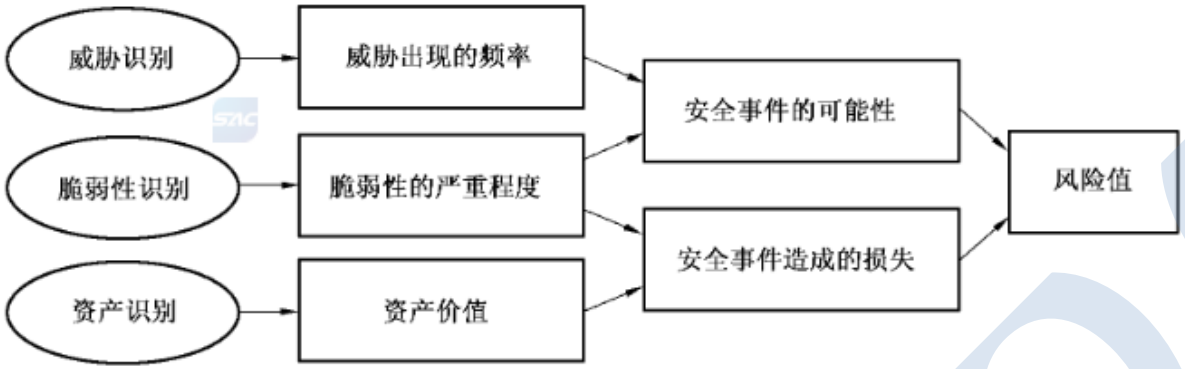
风险处置决策

1）消除风险
2）减低风险
3）分担风险
4）保留风险

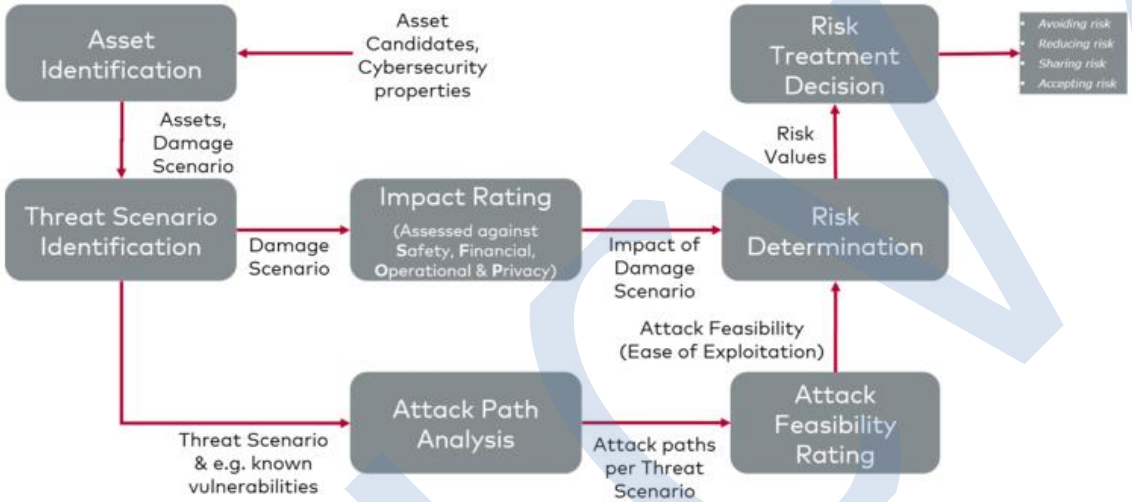
Risk Treatment Decision

1）avoiding the risk
2）reducing the risk
3）sharing the risk
4）retaining the risk

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	2	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1



- ✓ 每个模块的分析顺序可以自行决策
- ✓ 风险处置策略基于组织容忍度进行不同处置
- ✓ 风险评估是一种方法论，每个模块的分析维度可灵活扩展



- ✓ Each module can be proceeded in any order
- ✓ Risk Treatment Decision is then assessed by the business and based on the associated risk tolerance of the organization
- ✓ Risk assessment is a methodology in which the analytical attributes of each module can be flexibly extended

CSTC中国评测

谢谢聆听！

CCID 赛迪汽车