escrypt
SECURITY. TRUST. SUCCESS.

in co-operation with
KPMG

白皮书

数字化智能化时代
汽车制造商和供应商面对全新的安全挑战

保障汽车网络安全迫在眉睫



卡尔·奔驰 (Carl Benz) 在1886年推出汽车时，他对安全的关注与当今的汽车制造商完全不同。 在网络安全变得重要之前，过去的一个世纪汽车安全主要围绕机械类的主被动安全展开。 而现在，对汽车的各种网络攻击使网络安全的话题逐渐引起了公众和立法者的注意。 联合国已经发布一项对整个行业有重大影响的法规：将来，只有在车辆制造商获得网络安全管理体系 (CSMS) 认证的情况下，才可以进行车辆型式认证。 这意味着网络安全需要成为每个汽车制造商的重要话题。



目录

汽车网络安全的发展 4

汽车网络安全新要求 5

- UNECE WP.29 TF-CS/OTA 5
- ISO/SAE 21434 5

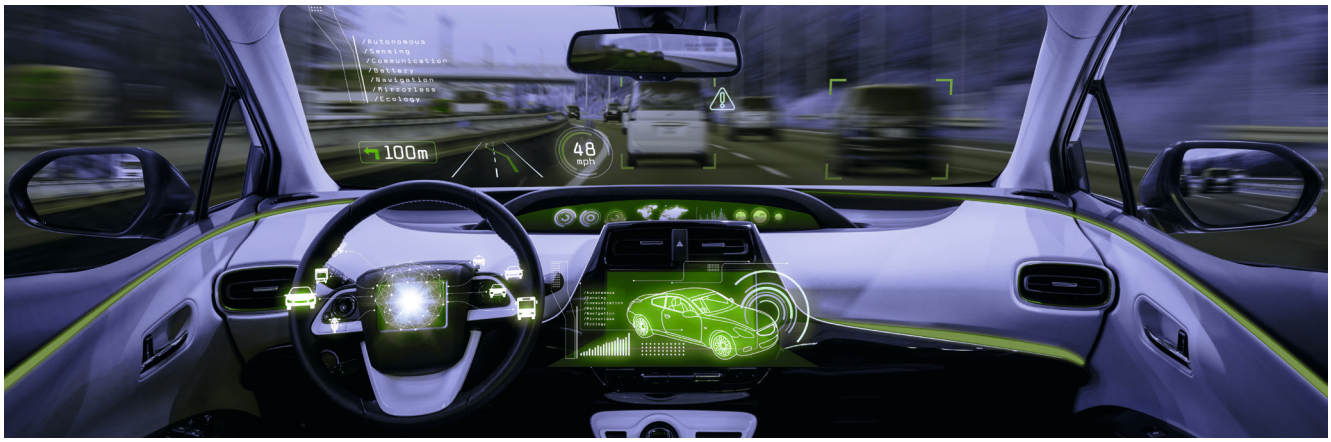
对汽车行业的影响 6

专家支持 7

- ESCRYPT 与毕马威在汽车网络安全话题深入合作 7
- 为企业提供经实践验证的解决方案 7
- 结合企业现有资源和优势快速转型 7

© ESCRYPT GmbH. All rights reserved.

汽车网络安全的发展



由Stephen Checkoway于2009年领导的一组科学家进行了最早的汽车黑客攻击。他们批露了如何将笔记本电脑连接到汽车的车载诊断端口以访问汽车的内部网络。 这使他们能够操纵汽车中的关键系统。例如，他们能够关闭发动机并阻止刹车。在此类攻击中，科学家利用车辆网络各种漏洞和ECU进行重放攻击，侵入汽车的嵌入式系统并篡改其功能。尽管黑客很难将笔记本电脑连接到受害者的车辆，他们仍然可以使用更小巧便捷的车辆远程控制设备，来恶作剧甚至危及驾驶者和路人的安全。

在2010年，一名20岁的年轻人远程控制了100多台车辆，使其不能发动。 “德克萨斯汽车中心”租赁公司在其租车系统中安装了硬件，可以通过联网的方式对其进行控制。 如果客户未付款，该系统允许出租公司停用点火开关。 这名黑客之前被公司裁员，离职后通过员工帐户访问该系统，并成功控制租赁车队的相应硬件组件导致车队瘫痪。

2015年，Charlie Miller、Chris Valasek成功远程控制了一辆Jeep。通过该车的娱乐系统，他们可以进入其多媒体系统，挡风玻璃刮水器和空调系统，并控制刹车和车辆速度。在测试中他们成功控制在高速上行驶的汽车停了下来。与在2009年的实验不同，这一次他们不需要电缆，通过网络就可以与汽车连接。为此，克莱斯勒付出了对140万辆汽车进行召回维修的代价。

近期，车辆网络攻击事件频发，其中多数利用了车辆中越来越多的数字化和网联功能。这一趋势已经揭露出保护机制不足的车辆对制造商、车辆拥有者和道路使用者造成的风险。 随着车载IT系统的数量和复杂性不断增加，对网络安全的需求正在迅速增长。将车辆视为封闭系统是不可行的也是违背基于风险管理的安全策略的。 汽车中提供新的数字化服务，汽车与制造商之间的通信（OTA），车车通信（V2V），汽车与基础设施之间的通信（V2I）， 以及与第三方供应商提供的智能手机和设备进行通信——所有这些发展都带来了更多的的攻击面，需要对其进行系统地分析和控制。 ■

 © ESCRYPT GmbH. All rights reserved.

汽车网络安全新要求

全球范围内，进一步规范和标准化汽车网络安全的活动在不断进行。 美国国会中的立法提案，欧盟的《网络安全法》，中国的ICV计划以及日本JASPAR的新指南。它们都展示了三个主要趋势：当关注网络安全话题时候，更多关注汽车行业的特殊性；关注对已量产车辆网络安全管理所面临的挑战和要求；法规的强制性越来越强，车型准入时将网络安全包括在内。这些趋势在UNECE WP.29 TF-CS/ OTA和ISO / SAE 21434中尤为明显，它们明确定义了用于车辆网络安全的管理体系。

UNECE WP.29 TF-CS/OTA

联合国车辆型式认证世界论坛（WP.29）通过了在新车型准入中结合考虑网络安全法规。TF-CS / OTA工作组的建议包含两个核心要求：对企业网络安全管理体系（CSMS）运行的认证； 以及在车型准入时CSMS在特定车辆类型上的应用。 欧盟计划从2022年起强制执行这些要求。

考虑到汽车行业传统的开发周期和开发模式，制造商和供应商需要立即着手落实这些网络安全要求，以确保下一个产品可以顺利通过车型准入。为此，他们必须遵循基于风险管理的方法，该方法可以针对车辆具体情况，持续分析、实现并维持适当的风险水平。这包括从网络安全角度管理来自供应商，服务提供商和其他第三方的供应关系及信息。

考虑到不断变化的威胁环境和汽车较长的生命周期，CSMS首先要关注的重点是SOP以后及后续车辆运行期间持续的风险管理。因此，必须在技术和组织层面两方面解决汽车安全问题。尽管制造商和供应商可以借鉴信息安全标准（例如ISO 27000系列）的经验，但是CSMS设计中的主要挑战在于考虑车辆本身的特殊性。 除了产品和供应链的高度复杂性之外，其他关键方面还包括与功能安全性的交互和融合，关注排放法规及防盗保护。

ISO/SAE 21434

除了TF-CS / OTA之外，汽车行业还在国际标准化组织（ISO）和SAE International的框架内开发针对车辆网络安全的ISO / SAE 21434标准。 与WP.29定义的CSMS相似，此标准重点关注合理的安全组织架构，及贯穿整个车辆的生命周期的安全流程和活动，以保护车辆免受网络攻击。鉴于联合国法规随附解读文件始终引用该标准来实施CSMS要求，因此ISO / SAE 21434需要被特别关注和重视。 它将拉通行业基本共识，创建通用术语，并对关键活动建立共同的理解，制造商和供应商可以在此基础上明确接口和职责分配，建立合理流程。 21434最终版本预计在2020年底发布。 ■

© ESCRYPT GmbH. All rights reserved.

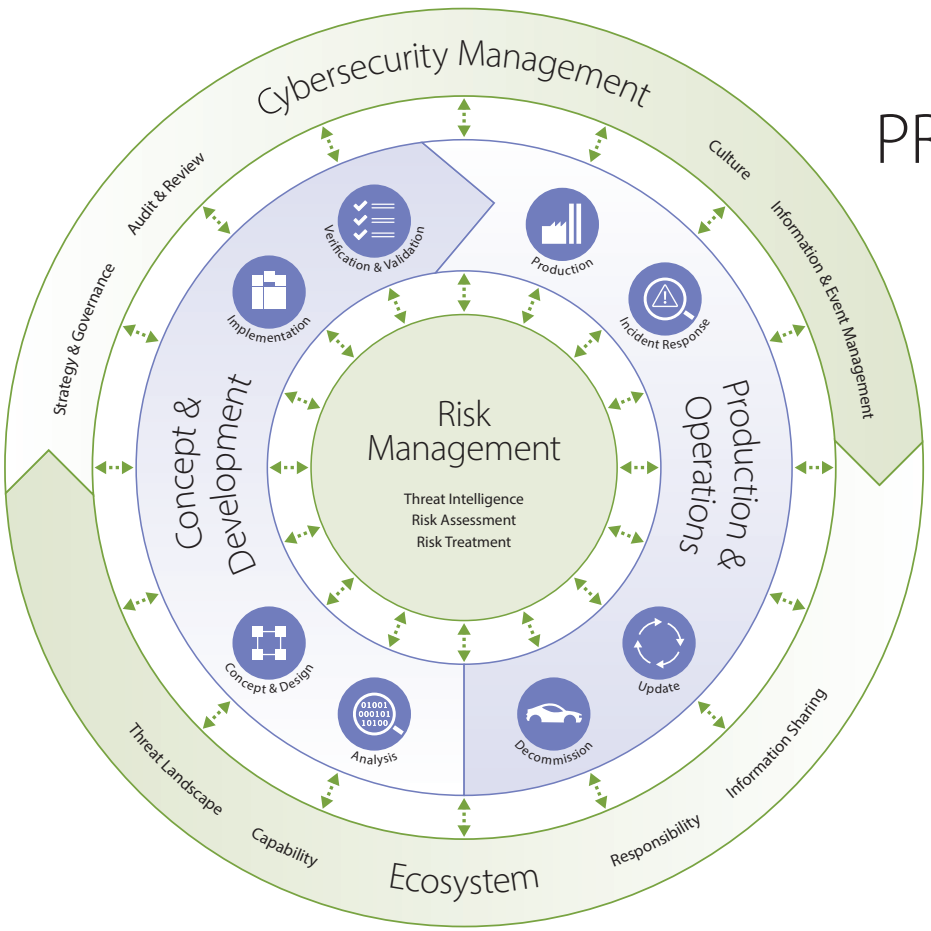
对汽车行业的影响

汽车行业对法规要求并不陌生。 但是，与汽车产品安全有关的法规并不多。 鉴于OEM对供应商信息安全的透明度要求日益提高，德国汽车工业协会（VDA）制定了信息安全评估（ISAs）目录，同时，借助TISAX模型，OEM可以检查供应商信息安全实践情况，例如如何处理敏感数据。

类比TISAX，ISO / SAE 21434定义了网络安全和产品安全的要求。 虽然近年来，汽车行业已经加强了对车辆的保护，但随着联合国法规生效，网络安全将成为强制要求。它将成为OEM和供应商提高竞争力的先决条件。 在各企业都在寻求数字化转型的背景下，这不仅是遵守法规要求的问题，更是真正落实公司战略和产品路线图的最有效方式。

OEM和供应商必须实施全面的组织和技术措施，使他们能够在整个价值链中持续定义、控制、管理和改善网络安全。 因此，对差距分析的需求在近期不断增长，这种差距分析可以衡量企业CSMS的实施状态并根据差距分析结果得出有针对性的改进方案。

产品安全组织框架



PROOF

 © ESCRYPT GmbH. All rights reserved.

专家支持

与许多其他行业一样，汽车行业面临该领域技术人才的短缺。既了解网络安全又了解汽车行业特殊要求的专家很少。同时，车辆不断提升的数字化智能化水平正迅速地提高网络风险水平，汽车行业积累的产品安全方面的知识通常无法跟上步伐。公司将发现很难用自己现有资源及时解决所有安全挑战。 同时，车型准入中尽可能有效地切实执行所有法规要求又是极为重要又迫切的需求。

ESCRYPT 与毕马威(KPMG) 在汽车网络安全话题深入合作

ESCRYPT和毕马威 (KPMG) 提供专业的咨询服务，以帮助OEM和供应商。ESCRYPT在汽车网络安全方面有丰富项目经验，支持从概念开发到批量生产及后续安全运营阶段持续满足安全要求。毕马威 (KPMG) 是信息安全评估审计及帮助企业建立信息安全管理体系 (ISMS) 的专家。双方合作利用了这些优势，并将它们组合为一种整体方法以更好为客户服务。 例如，所有在组织流程方面的设计优化，都会同步考虑如何更有效地体现和落实在开发和运营的安全方案上。

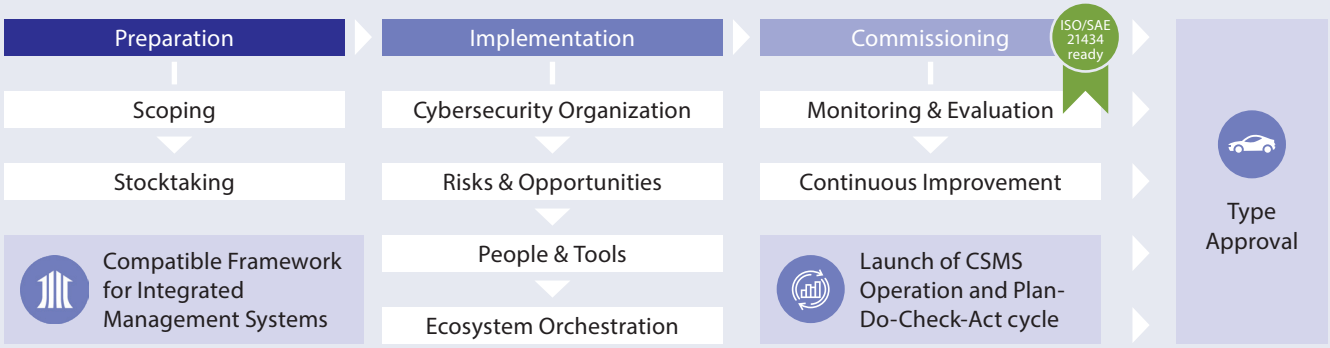
为企业提供经实践验证的解决方案

ESCRYPT和毕马威 (KPMG) 在所有细分领域为汽车行业提供支持，从豪华跑车制造商到全球排名前五的OEM以及自动驾驶主流供应商。服务方案基于合作双方十几年来的经过实践验证的可靠经验积累。 我们提出CSMS的实施框架包括三个主要步骤：a) 准备，b) 实施以及 c) 运行和持续改进。

结合企业现有资源和优势快速转型

综合考虑数字化带来的挑战的复杂性，以及网络安全将很快成为类型认证所带来的必要性，因此避免一切从零开始、重新建立至关重要。 取而代之的是，必须利用现有优势，并在其基础上搭载部分解决方案，最后集成到完全合规的网络安全管理体系中。现有的优势可能包括信息安全管理系统 (ISMS)，质量管理系统和用于实现功能安全的既定做法。 为实现这一目标，ESCRYPT和毕马威提供专业的审计和差距分析，以找出与相关标准的潜在差距并发现现有优势，使公司能够建立基准并确定措施的优先次序，通过最快和最好的路线，从而最大程度地提高投资回报率并使公司实现目标。 ■

Proven and structured methodology for a CSMS



© ESCRYPT GmbH. All rights reserved.

联系我们

卢星旺
Escrypt 中国区负责任人
Xingwang.LU@etas.com
Tel. 021 2218-6251

相靓宇
咨询顾问 汽车网络安全
Jingyu.XIANG@etas.com
Tel. 185 1808 5920

易特驰汽车技术（上海）有限公司
长宁区，福泉北路333号
上海，中国
Tel. 021-2218-5800

www.escrypt.com

张令琪
合伙人 网络安全
richard.zhang@kpmg.com
Tel. 021- 2212 3637

邬敏华
副总监 网络安全
fm.wu@kpmg.com
Tel. 136 1197 9505

毕马威企业咨询（中国）有限公司
恒隆广场2期
上海，中国
Tel. 021- 2212 2888

www.kpmg.com
www.kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.
© ESCRYPT GmbH. All rights reserved.

Status: 10/2020