如何在智能汽车浪潮中赢得先机?

Richard Viereckl博士是思略特Strategy&法兰克福办事处的合伙人，同时也是公认的汽车工业领域专家，他为一些国际领先的汽车企业提供制造、销售，以及研发方面的建议。

Alex Koster是思略特Strategy&瑞士办事处的执行合伙人，他为来自电信、互联网、高科技，以及汽车行业的客户提供数字化方向的咨询业务。

Richard Viereckl
Alex Koster

智能网联汽车技术和服务的供应商们会根据自己独有的优势制订竞争策略，瞄准那些能让自己发挥最大优势的细分市场。思略特预测，智能网联汽车行业将会涌现四种互补的商业模式。

未来的四种商业模式

数据和受众整合者：有些公司将自己定位为收发数据的参与者。他们会收集智能网联汽车的数据，并将其发送给对司机驾驶行为，以及对车辆性能感兴趣的第三方公司，例如保险公司。

经营规模是这种方式成功的关键，保险公司需要大量的数据，广告商需要吸引百万眼球。而科技公司往往具备成为整合商所需要的条件，即遍布全球的经营规模、技术能力和开放的系统。而汽车制造商往往没有足够的车辆，更不用说联网车辆，根本无法与亚马逊、谷歌和苹果等公司进行大规模竞争。当然，整车生产商也可以通过建立合作关系，并利用他们和极小众的受众，如高端车车主之间的联系来成为整合商。

整车生产商还有一项非常关键的优势：拥有汽车的原始数据。整合商需要掌握获取智能网联汽车数据的控制权，例如车辆的位置和传感器的信息，以及类似搜索引擎和社交媒体等的数据采集点。

数字化服务提供商：很多供应商会通过智能网联汽车技术提供数字化服务，包括娱乐服务、移动性管理和健康监控等。数字化服务将成为一个高度分散的市场，因为其中的参与者来自不同的行业领域。但只有那些提供符合移动用户需求和最佳用户体验的参与者才会成为最终赢家。高品质的产品和服务平台将会成为差异化竞争的最关键因素。整车制造商也应该努力开发专门的娱乐和资讯娱乐系统，确保自身贴近数字化服务市场，同时更好地进行客户分析。

数字化衍生产品提供商：许多汽车制造商可以利用自身掌握的汽车产业专业知识和对客户的洞察力，提高自身车辆的性能和效用。他们可以向大型车队运营商提供包括车队管理、预防性维护和自动驾驶等一系列数字化服务。这种参与方式需要参与方拥有独家的车辆传感器数据、与客户的计费关系、可靠的导航数据和自动驾驶车辆的人工智能引擎。

数字化推动者：有些参与者则会试图开拓小众市场，成为智能网联汽车基础配件中高价值数字化部件的供应商。这些专业的参与者很有可能针对单一的产品进行开发，如能告知自动驾驶车辆路况是否良好的道路监测传感器。其目标就是成为某种特定部件的主要供应商，并向全球的汽车整车生产商提供该部件。当然，此类参与者也会在不同层面参与市场活动，即他们既要成为其他智能网联汽车产品和服务供应商的竞争者，也要成为他们的供应商。对于此类竞争者来说，通过专利和标准掌握技术是他们成功的关键。

以上提到的四种价值主张都要求汽车制造商把自己定位为服务提供商。这也要求他们需要开发新的运营模式、发展新的能力，并且开创新的文化思维模式。建立在高效生产和硬件销售基础上的市场进入模式已经无法满足消费者的需求，尤其是那些已不单纯满足物理特性（如功率和操控），而更看重数字化服务价值的消费者。

行业结构也将随之发生变化。目前，一级供应商根据汽车制造商的要求来设计、供应部件。随后，汽车制造商再通过装配和运输将车辆送至经销商手中。最后，车辆通过经销商进入销售市场。然而，这是一个建立在具体产品和零售思维模式基础上的被控制的、封闭的生态系统。新的汽车产业将会是一个更开放、更多层次、更注重数字服务而非具体产品的全新生态系统。在这样一个新的生态环境中，我们将看到新车和二手车的销售将会降低，而汽车租赁和汽车共享服务则会迅猛发展。跨品牌的服务平台和合作也会日益增多。新进入者将会在自动驾驶车辆进入市场的过程中发挥关键作用（**见下图**）。

最后，需要处理的关键问题是自动驾驶车辆所面临的法律责任事宜。即使所有的安全性问题都得到了妥善的解决，但还是发生了事故，那么该由谁来承担法律责任?汽车生产商？道路基础设施提供商？软件供应商？传输信息的电信公司？乘客？导航供应商？又或者是以上所提到的参与者都需承担部分责任?面对网络安全挑战的威胁，正如我们在下一个部分将阐述的，这个悬而未决的问题将变得尤为突出。

新的增长点，新的挑战

智能网联汽车是一个新的收益增长点，但同时也会带来前所未有的危险。据Wired杂志报道，曾有黑客让一辆联网的吉普车在高速公路上自动刹停。智能网联汽车安全研究员已经能够劫持特斯拉的车载系统，切断车辆电源，让其动力系统失效，并且能操控车辆的门窗。还有一组安全研究员成功进入宝马汽车的“Connected Drive”系统，并远程解锁了一辆宝马。安全隐患已成为汽车生产商所面临的最大威胁之一，因为这危及司机安全，也会影响生产商的声誉和财务状况。

黑客可以通过潜入汽车网络的方式，在不支付任何费用的情况下享受数字化服务，或是让消费者为他们未订购的服务埋单。芯片调谐器可以通过CAN总接口增加引擎功率，并且操控引擎。犯罪分子还可以通过禁用汽车的防盗系统，并设置汽车行驶方式远程偷盗车辆。客户的移动设备和他们车辆之间的同步又增加了个人信息泄露的危险，因为黑客可以通过入侵车辆蓝牙或无线接口的方式，远程窃取用户的个人信息。

黑客通过攻击后端或是第三方系统来操控车辆传感器、发动机和车辆的其他功能。他们可以将车门锁上、禁用制动器或使发动机加速运转至全速。然而，最令人不安的是这种不安全性很有可能被恐怖分子利用，他们可以侵入自动驾驶系统并引发严重事故。

这些安全隐患严重影响了客户对智能网联汽车的信任，而这种信任对汽车生产商来说又是至关重要的。当消费者知道使用智能网联汽车可能会泄露个人信息，甚至有可能危及人生安全时，他们自然会对智能网联汽车产生抵触心理。因此，如果想要实现数字汽车技术的巨大潜能，汽车生产商就必须说服消费者，并且使他们相信这种完全依赖于开放电子网络的技术是安全可靠的。

得安全性架构者得市场

要构筑有效的网络安全策略，首先要了解数字化和互联网如何改变汽车工业以及供应链的IT基础架构。汽车制造商长久以来都把IT看作是多个独立系统的集合：后台系统处理和管理数据、支持操作和处理交易等；生产IT系统则运营工厂，并负责供应商和分销商的相关事宜；车载系统控制车辆运行，并且将车辆连接至互联网、移动电话网络和其他数字服务提供商。

行业高管考虑信息安全时，常常把车载系统看作是漏洞。然而，互联网将汽车IT的三个领域连成了一个整体，这也就意味着黑客只要入侵其中一个领域，例如CAN总接口，他们便可以绕过认证、防火墙以及其他安全措施，对车辆的其他领域造成损害。如果技术更熟练，并且更有耐心的话，黑客还可以侵入与银行或信用卡相关的应用程序；跟踪车辆的位置，并且利用这些数据进行盗窃、间谍活动、勒索或控制车辆等行为。

黑客往往不需要切切实实地入侵车载系统便可以实现他们的目标。宝马公司的黑客事件说明，外人可以通过控制汽车生产商的后端系统，在完全不触及车辆的情况下使车辆自主运行离开。

由此可见，网络安全问题不仅仅是IT人员需要处理的技术挑战。汽车制造商不能将IT视作是一个独立的功能。一个有效的安全策略必须是一个单独的且多向量连接的系统，从蓝牙系统到无线网络，再到其他各种终端接口。汽车制造商必须将这些系统都汇集到综合性的安全伞下，并让整个供应商生态系统从高管到工厂，再到研发部门都参与到整个利益链中去。

面对网络安全的威胁，汽车制造商应在产品研发早期阶段就解决信息安全问题。一级供应商需要在运营过程中嵌入安全措施，甚至是向消费者收取各种数字化服务费的第三方参与者，也需要采取相应措施以控制保密的个人信息不被入侵。在内部，汽车制造商需要风险管理系统来识别和量化威胁，以及相关的政策和程序用来保护数据，使系统免受入侵。同样重要的是严格的检测和报告制度，以确保安全措施的有效性，并且检测和提示系统中的薄弱点。咨询机构和宣传机制也应该到位，只有这样才能帮助相应的决策者了解安全问题所在。

公司员工必须接受培训，学习最行之有效的保护信息的方式，以及软件安全开发生命周期。生产、物流和其他部门等作为采购、业务开发和规划等配套服务中的一个环节，也将发挥重要作用。

总之，所有这些措施构成了一个完整的“信息安全管理体系”。这一体系将有助于安全策略的开发、责任分配、资源分配、行动协调、性能检测、威胁回应，以及安全措施的不断提高和完善。

汽车产业结构的现状和展望