目 录

图目录

表目录

1

汽车数据安全发展形势

数据作为汽车产业数字化发展的重要基础设施，汽车数据汇聚带来价值聚变，可以推动供应链透明化管理、智能化技术迭代升级、促进低碳减排。但日益增长的数据安全风险不容忽视。2020 年至今，汽车行业安全攻击超过280万次。企业需要加强企业数据安全能力建设，智能汽车发展才能避免“沙滩上起高楼”的危局。未来，在汽车大数据产业发展的带动下，汽车安全防护有望处于安全技术产业的领跑位置。

（一）数据成为汽车产业数字化发展的重要基础设施

汽车在研发、生产、供应、销售、服务等全生命周期环节产生海量数据，仅在整车使用过程中，L2 级辅助驾驶功能的乘用车每年上传至云端的数据就超过20000PB(1EB=220GB)。 汇聚这些数据形成规模化数据池，成为智能汽车发展的核心底座，也将支撑汽车产业数字化转型。同时带动产业上下游数据流不断从长链到短链、从封闭转向开放、从线下到线上，在客户满意度、生产研发、生产成本等方面都有明显提质增效的表现，产生意想不到的效果（见图1）。

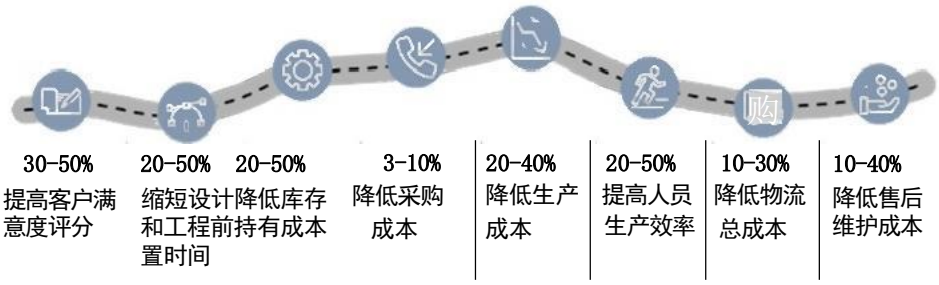

图 1 汽车数据链提升供应链管理效能

信息来源：麦肯锡，车百智库研究院整理

通过赋予每一个整车、零部件产品一个数字身份，关联全生命周期的数字化信息，如碳减排信息、整车使用信息等，形成全链“数据粮仓”，会带动“碎片化”数据由“垃圾资产”变成“集成式数据金矿”，产生价值裂变。 一方面，强化整车、软硬零部件可追溯性，提高供应链管理透明度，形成高效敏捷的供应链。另一方面，促进智能驾驶、智能座舱、大模型等技术迭代升级。此外，还能够服务于碳足迹认定、电池追溯等，创造更多新价值。

（二）汽车数据安全形势不容乐观

1、 汽车数据安全问题日益凸显

根据工信部车联网动态监测情况显示，2020年以来发现的针对整车企业、车

联网信息服务提供商等相关企业的恶意攻击达到280余万次。2023年初至今，就发生超过20起与车企相关大规模数据泄露事件，泄露数据涉及企业内部业务、车辆驾驶、用户隐私等众多数据。过去5年中，全球汽车行业因网络攻击造成的数据泄露损失超过5000亿美元。

2、汽车数据可能遭受的攻击面更广、攻击点更多

汽车智能化、网联化打开了原有车内域、车间域、交通域、车云域的边界，打破汽车控制系统原有封闭生态，汽车数据将面临来自“云-管-端”三方面的安全风险。

一是车端汽车数字身份漏洞会引起黑客攻击隐患。汽车网关、充电系统、智能钥匙、外部进程、3G/4G 网络等通信接口的不断增多，且存在错综复杂的传输介质、协议等，导致汽车面临的攻击范围更大且受攻击点数量更多，数据安全防护难度较大。据统计，2023 年美国汽车远程被盗比例同比增长142%。另外，还会导致汽车动力系统被控制，威胁用户人身安全。2023年5月，车联网安全挑战赛中，各支队伍都能在短时间内触发10次以上车体车灯、车窗和雨刷器、读取汽车里程数，部分队伍还能触发车速表部件动作，开启刹车灯、转向灯（见表1）。

二是云端潜在的安全隐患。智能网联汽车单天产生数据达TB 级，在车端存储资源制约下，云端成为汽车数据的最佳汇集点。但云平台潜在的不安全接口、未授权访问、系统漏洞等安全隐患可能造成敏感信息泄露，不法分子甚至可通过伪造、篡改指令及数据内容等方式非法控车，危及用户人身安全和公共交通安全。

三是数据交互、数据共享等传输过程也存在信息泄露风险。车内数据传输主要根据功能进行编码，按照报文 ID进行标定和接收过滤，通讯网络很容易受到嗅探、窃取、伪造以及篡改等攻击威胁。但通讯协议中引入安全隔离、数据加密等防护技术，会造成较大时延，加大智能网联汽车行驶的安全风险。如何能在数据安全传输的前提下降低通信时延，是亟待突破的技术难题。