



从车机端和云端为车辆打造网络安全

随着汽车逐渐成为高密度的数据信息交换中心，它也成为网络安全黑客的攻击对象。为车辆提供更安全、更环保解决方案的盖瑞特，把网络安全管理作为进入智能网联汽车市场的支点，其端到端的网络安全解决方案为车辆保驾护航。

□ 盖瑞特

打造智能车辆网络安全的“护城河”

智能网联汽车的时代在加速到来。如果将4G、5G、蓝牙及近场通讯等技术计算在内，目前汽车的互联度可达到15%左右。到2025年，这一数字有望超过75%，甚至达到100%。随着汽车逐渐成为高密度的数据信息交换中心，它也成为网络安全黑客的攻击对象。消费者在享受自动驾驶、车载冲浪等种种便利时，不能忽视车辆的网络安全。

根据2019年的信息网络安全报告显示，黑客攻击路径来源多样，包括：数据服务器（21%）、无钥匙进入（19%）、OBD端口（10%）、移动应用程序（7%）及信息娱乐系统（7%），它们正成为黑客对汽车发起攻击的主要路径（图1）。除此之外，蜂窝网络、Wi-Fi、传感器、USB端口、蓝牙、

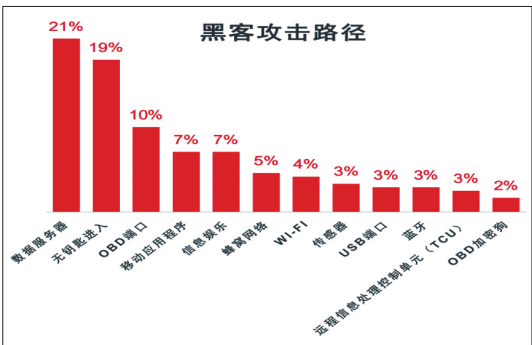


图1 黑客攻击的主要路径

远程信息处理控制单元以及OBD加密狗也是时常遭受黑客攻击的目标。除窃取驾乘者信息外，黑客还可通过上述端口存在的漏洞，进入车辆、操控车辆或劫持车辆，对驾乘者造成物损或形成安

全隐患。在某些案例中，黑客还将利用车辆上存在的软件漏洞对汽车制造商进行勒索。

为车辆提供更安全、更环保解决方案的盖瑞特，把网络安全管理作为进入智能网联汽车市场的支点，从车机端和云端为车辆打造网络安全的“护城河”。

盖瑞特端到端的网络安全解决方案主要由“盖瑞特网络入侵检测系统 IDPS”和“安全运营中心 SOC”两个模块组成，将“检测—隔离—报告—修复”整合成闭环（图 2）。

其中，IDPS 主要是通过监测车内网络信号保护车辆免受网络攻击，该系统可以防范整个车内网络中的异常信号。具体来看，盖瑞特的 IDPS 包含了 50 多种成熟算法，可以实现跨总线检测，覆盖超过 90% 的黑客攻击。不仅如此，IDPS 还适用于 CAN、CAN FD 及以太网等多种不同的车载网络，并且很容易和车端硬件集成。而 SOC 则主要是使用高级分析工具全天候监控威胁，以对各种事件进行汇总、分类和

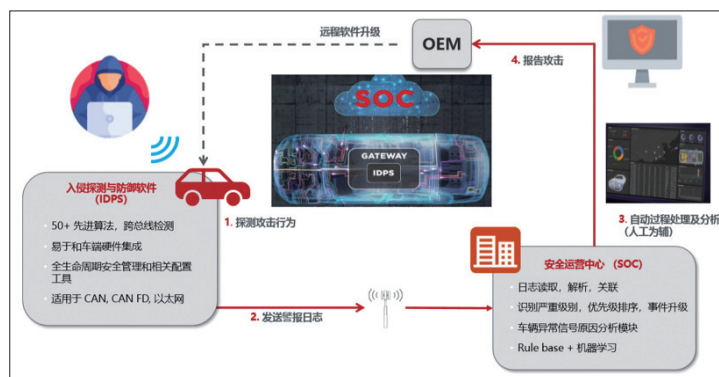


图 2 盖瑞特端到端的网络安全解决方案

关联。一旦发生黑客入侵，该解决方案在检测异常同时，还能向主机厂报告，排除车辆当前及后续的安全隐患，阻止黑客攻击的蔓延。

这套系统的特色在于，既发挥车端快速响应和杜绝风险的能力，将确定异常、会对车辆产生攻击的信号直接屏蔽掉，又能利用算力充足的云端对未能确定的信号结合系统和人工进行综合分析，按照时间、严重级别等进行优先级排序，由 SOC 向主机厂做出防御的策略建议。

盖瑞特网络安全解决方案的能力与逻辑，源自盖瑞特及前身

霍尼韦尔在航空航天和过程工业控制领域网络安全防范管理，以及跨行业迁移应用的经验。深耕汽车行业超过 65 年的盖瑞特与所有主流 OEM 长期、深入地合作，洞察汽车行业趋势，管控研发及把握批产流程，盖瑞特布局汽车智能网联软件，为今后长期加速发展奠定坚实的基础。

盖瑞特全球拥有包括上海在内的四大软件研发中心，其先进的网络安全方案已经应用于全球领先 OEM 的量产车型上，同时为国内主机厂开发的量产车型也将上市，从而为日益壮大的智能网联汽车保驾护航。AI

（上接第 26 页）

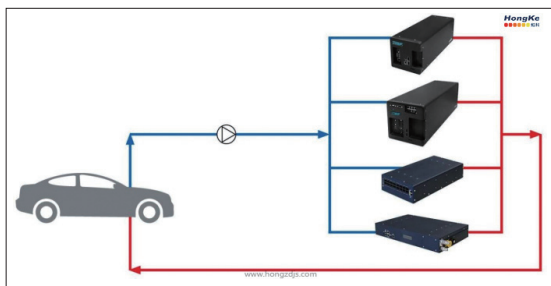


图 5 液体冷却电路

DynaCOR 可以利用商用车辆的液压系统，具体取决于设备数量和现有基础设施的容量。冷却一个外部温度为 40℃ 的设备

所需的流量仅为 2 L/m，工作压力为 2 bar（1 bar=10⁵ Pa）。

即使 DynaCOR 40-34 使用的功率可以高达 450 W，出口处冷却液的温度也仅会升高 1 ~ 3℃。因此，如果入口冷却液的温度为 40℃，则返回回路时温度将为 41 ~ 43℃，这对总负载产生的影响很小。

结论

启用 L5 级自动驾驶会带来

前所未有的挑战，一些传统嵌入式技术难以应对这些挑战。计算性能、存储容量和网络带宽要比大多数公司在其坚固耐用的设备中提供的性能高几个数量级。

我们充分利用了坚固耐用的计算和 HPC 方面的丰富经验，创建了完整的 HPEC 系统产品组合，可用于创建“轮子上的数据中心”，即坚固耐用且经过认证的设备，这些设备通常具有 Edge 功能，通常属于数据中心。AI