OTA 更新需要灵活的汽车架构支持

一辆汽车静静地在车库里过夜，一动不动，等待着它的驾驶员回来，带它展开下一次旅行。但是，这辆车并不是简单地在等待，而是在扩展其功能，提高安全性和智能水平，并学习如何执行与当天新下线的汽车一样的新功能。

软件在线更新技术 (OTA) 的应用让这一切成为可能。OTA 被集成到汽车架构中后， 整车制造商便可以在汽车出厂后，仍能不断对汽车的安全、信息娱乐等功能进行更新，不仅体验优雅，且可扩展、低风险，并且经济高效。

基于集中式计算并针对 OTA 进行优化的架构设计有助于确保顺利、安全地进行软件和固件更新，无论应用程序、OEM 策略和消费者偏好要求的频率如何。OTA 不仅对制造软件定义的汽车至关重要，而且还为打造创新型新服务、功能交付的新方法和新的商业模式奠定了基础，带来了前所未有的灵活性和可扩展性。

为软件定义的汽车提供支持

大部分 OEM 都在推出软件定义的汽车，以期在后期能够通过蜂窝或 Wi-Fi 网络提供软件及固件的 OTA更新，从而继续交付更多功能。而承载这些功能的系统变得愈发复杂，其安全性变得更为重要，因此这些更新的执行必须安全、可靠。

虽然 OTA 越来越普遍，但它并不是一种随随便便即可具备的功能；相反，汽车架构在设计之初就应考虑如何集成 OTA 的问题。针对 OTA 的架构优化的关键是将车辆内的计算能力集中起来，这样更新只需下载到集中的位置即可，而不必分布到整个车辆的系统中。

所幸的是，汽车电子架构已经在朝着集中化的方向迈进了。例如，安波福的卫星式传感系统将雷达、摄像头等传感器的计算集中在一个强大的域控制器中。这种方法使传感器体积更小、重量更轻，提高了封装和设计的灵活性，同时也使整车制造商能够更好地管理车体架构散热问题。同时，安波福卫星式传感系统在域控制器上实现了先进的功能，如应用传感器融合将各种传感器的输入统一到一个整体性的环境模型中。

一些软件或固件内容仍保留在雷达或摄像头上，但这些代码很少需要上市后再进行更改。而软件功能及组件的计算（如负责识别车辆周围的物体并跟踪它们的运动的追踪软件）则由中央计算器负责。

这种方法需要用于验证软件变化的工程资源很少，因而可以降低成本。

在任何软件进行更新或“刷新”之前，每个更新的组件都必须经过一套严格的全新测试条件验证，以确保正常运行。例如，如果跟踪器位于智能传感器中，那么每一个传感器在部署更新之前，都必须重新验证。然而，如果跟踪器等受更新影响的软件组件位于域控制器中，则只有域控制器需要重新验证。这不仅简化了流程，而且需要的资源和时间也更少。

每一次 OTA 更新都会产生一定的成本，除了重新验证之外，还包括将软件上传到云端、云端管理、加密、下载和空传用量的成本。尽可能地简化这些更新有助于降低成本。

如果更新不能完全集中进行，那么指定一个主控器来控制车辆中其它各个组件的更新，以确保它们都能正确刷新并相互兼容，也是可取的做法。在安波福的智能汽车架构 (Smart Vehicle Architecture™) 中，车辆中央控制器 (Central Vehicle Controller) 即是这样一个主控器。这种方法可确保避免系统出现不匹配的情况，例如，一个组件需要另一个组件提供某种格式的数据，但由于更新不完整或损坏而没有收到这类数据。

除了无线升级，软件的集中化还有更多其它优势。随着软件应用程序在一个通用平台上实现容器化，对这些应用程序执行互操作性测试及网络安全应用将变得更加容易。

由于上述原因以及更多原因，集中化在行业中势头不断增强。

速度更快，安全性更高

为了实现更安全、更可靠的 OTA 更新，域控制器中的每一个处理器（必要时还有传感器中的处理器）必须有足够的内存容量来容纳新旧软件映像。只有当新的软件映像经过完全下载、解密和验证后，系统才会进行切换，且所有受影响的处理器都会同时进行切换。这确保了每个组件仍然可以随时重启。

在 OTA 应用方面，行业正在采取三种做法：每种方法的 OTA 速度都在持续稳定地提升。越来越多的制造商也转而应用更快速的方法，以提高安全性及灵活性。

1. **通过外部存储更新：**在这种情况下，新的软件映像会被缓冲在一个外部网关中，该网关通过蜂窝调制解调器与云端进行通信。这种方法经济高效，因为它不需要增加域控制器或传感器的内存。它还能够使当前的所有组件做好准备，支持 OTA。然而，如果发生故障，便无法恢复到以前的映像。一个高级驾驶辅助系统 (ADAS) 域控制器的一般更新可能需要2分钟的时间。
2. **通过本地存储更新：**在这种情况下，新的软件映像会被下载到电子控制单元内的本地存储中。更新时，新映像会从本地存储复制到活动闪存中。举例来说，使用这种技术来更新一个雷达传感器大约需要14秒。
3. **通过双倍闪存更新：**在这种情况下，处理器拥有足够的内存，能以 A/B 配置的方式同时容纳新旧软件映像。一旦下载完成并经过验证，几乎可即时切换到新映像，且切换对系统的可用性没有影响。如果发生故障，也可即时恢复到以前的映像。

所有这些OTA发生的时机都由 OEM 决定。一种方法是在车辆行驶过程中下载软件映像，然后在车辆下次启动时安装新映像。另一种方法是在点火装置关闭时下载和安装更新，也许是夜间。后一种方法要求系统在这段时间保持通电，所以必须考虑到电源管理的问题。

更新频率如何？

应用程序通过 OTA 更新的频率也由 OEM 决定，并可能取决于应用程序的类型。

例如，一个旨在满足合规要求的成熟功能可能不需要经常通过 OTA 进行更新或根本不需要更新。但是，为舒适性而设计的软件配置可能需要定期更新，而那些更高级的功能可能需要持续的、即时的更新，以确保消费者能在自己的座驾中享受到最新功能。当然，这也意味着一旦出现情况，工程师马上就需要推出错误修复程序。

频繁更新非常契合持续集成/持续部署 (CI/CD)，后者是一种始于 IT 行业的开发和运营的方法，正在迅速被汽车行业采用。通过 CI/CD，开发人员可使用自动化工具更频繁地进行软件更新，并在准备好后立即将这些变更应用于市场，而 OTA 技术也正在不断发展以便为此提供支持。

“针对 OTA 的架构优化的关键是将车辆内的计算能力集中起来，这样更新只需下载到集中的位置即可，而不必分布到整个车辆的系统中。”

未来：实现部分更新

今天，大多数 OTA 更新都需要对整个映像进行重新编程。但系统正在迅速发展，以期支持对软件的一小部分进行更新，而无需完全更换映像，就像我们习惯使用的智能手机一样，可更新单个应用程序。事实上，随着安卓等操作系统逐渐被应用于汽车平台，通过对应用程序进行OTA更新已经在汽车行业中出现了。

随着汽车中软件数量的不断增加，OTA 更新的需求也在增加。虽然今天大多数汽车的自动驾驶水平还在 0 到 2 之间，但 3 级及以上自动驾驶的汽车将会配置更多软件，如果每次都要更新全部映像，可能会令消费者望而却步。

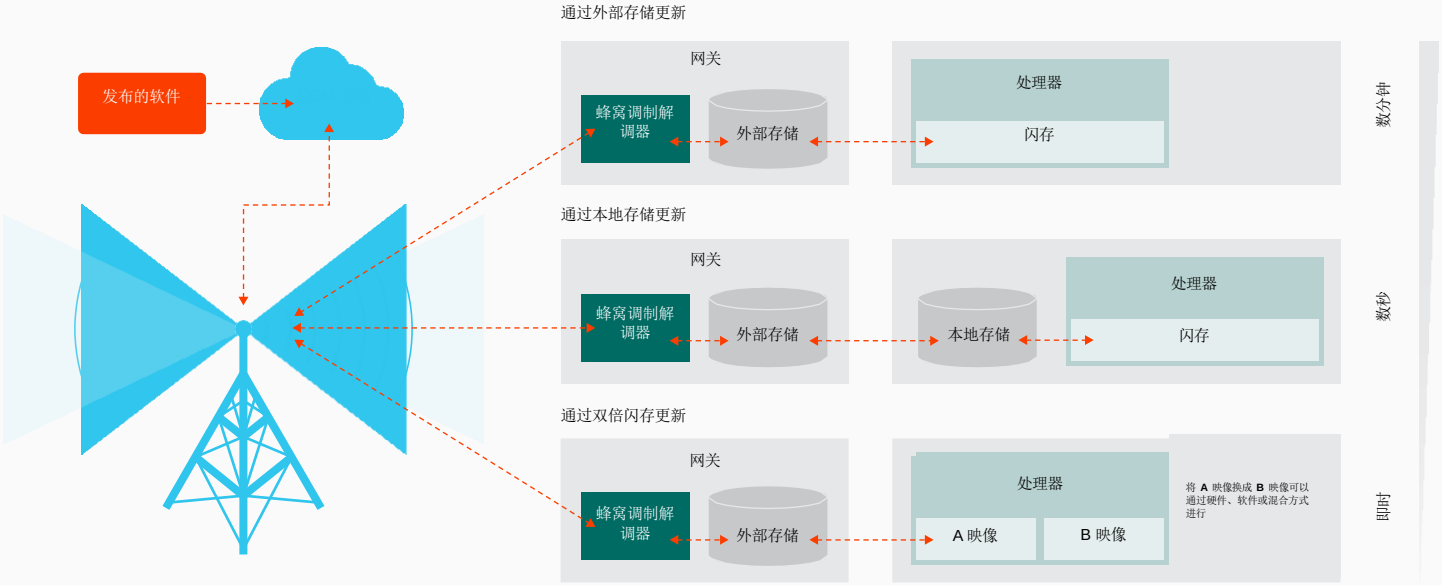
同时，由软件定义的功能不断增加，意味着代码行将会更多，组成软件的来源也将会更多。理想情况下，OEM 会希望能够通过单一信源对车辆上的部分软件进行更新（如跟踪器或自适应巡航控制功能），而其它部分保持不变。因此，需要专门开发软件来实现部分更新，它们被植入相应的位置，然后重新启动系统。这就是软件的架构设计非常重要的原因，它必须实现容器化，将各部分分开，并支持增量更新。

对于所有 OTA 更新来说，安全是整个过程中每一步的头等大事。在部署更新之前，工程师必须对代码进行全面分析，不仅要确保代码与车辆中的其它软件配合良好，还要检查它是否存在威胁，是否存在漏洞。ISO/ SAE 21434 汽车网络安全标准中规定了一些最佳做法，但从根本上，系统本身的设计必须包含“假定伤害”的心态 — 即假设任何新软件都有可能造成伤害，无论是故意的（如果有网络攻击）还是无意的 — 并采取主动和被动措施来控制这种伤害。

“软件定义的汽车能否取得成功取决于 OTA 能否让车辆像其它产品一样，可以持续改善功能，满足消费者的期待。”

重新刷新的情况

随着软件被发布到云端，车辆将更新下载到一个集中的外部存储器，然后通过外部储存器应用多种方式将这些更新传播到各个处理器中。



新型商业模式

车辆功能的持续改进将大有可为，而由 OTA 应用而带来的新的商业模式也前景广阔。

一种可能的模式是通过订阅服务提供功能，通过定期结算的方式收取功能费用。或者，一位司机可能想激活一个高速公路辅助驾驶功能，可用时间只需满足一次周末度假的需求即可。OTA 将支持仅在订阅的时间内下载或启用这些功能。

若车辆有足够的内存和计算能力，同时配有一系列的雷达、摄像头等传感器，那么要获取任何新功能，只需要通过OTA 获取相应软件。

OTA是新一代电子电气架构中一个关键要素。安波福已经设计出了智能汽车架构 (Smart Vehicle Architecture™) 以及相应的新一代 ADAS 平台，其优化的设计使之可以尽可能高效、安全地接收 OTA 更新。

软件定义的汽车能否取得成功取决于 OTA 能否让汽车像其它产品一样，可以持续改善功能，满足消费者的期待。OTA 应用是培养软件提供商生态系统、挖掘他们的创新、并在车辆的使用寿命期间不断推出创新的一个关键因素。

作者简介

Nabeel Bitar
高级安全启动中心车辆系统架构师

Nabeel Bitar 在主动安全事业部负责全球 OEM 项目中主动安全领域的新商业机会相关的技术探讨和设计。Nabeel 已在安波福工作超过 25 年，负责软件及系统工程方面的工作。自 2003年以来，他一直从事开发 ADAS 和自动驾驶系统的工作。在此之前，Nabeel 在 Delphi Saginaw Steering（现在的耐世特公司）从事防抱死制动、牵引力控制软件、电动助力转向系统等方面的设计工作。

更多详情请访问 APTIV.COM/智能网联与安全