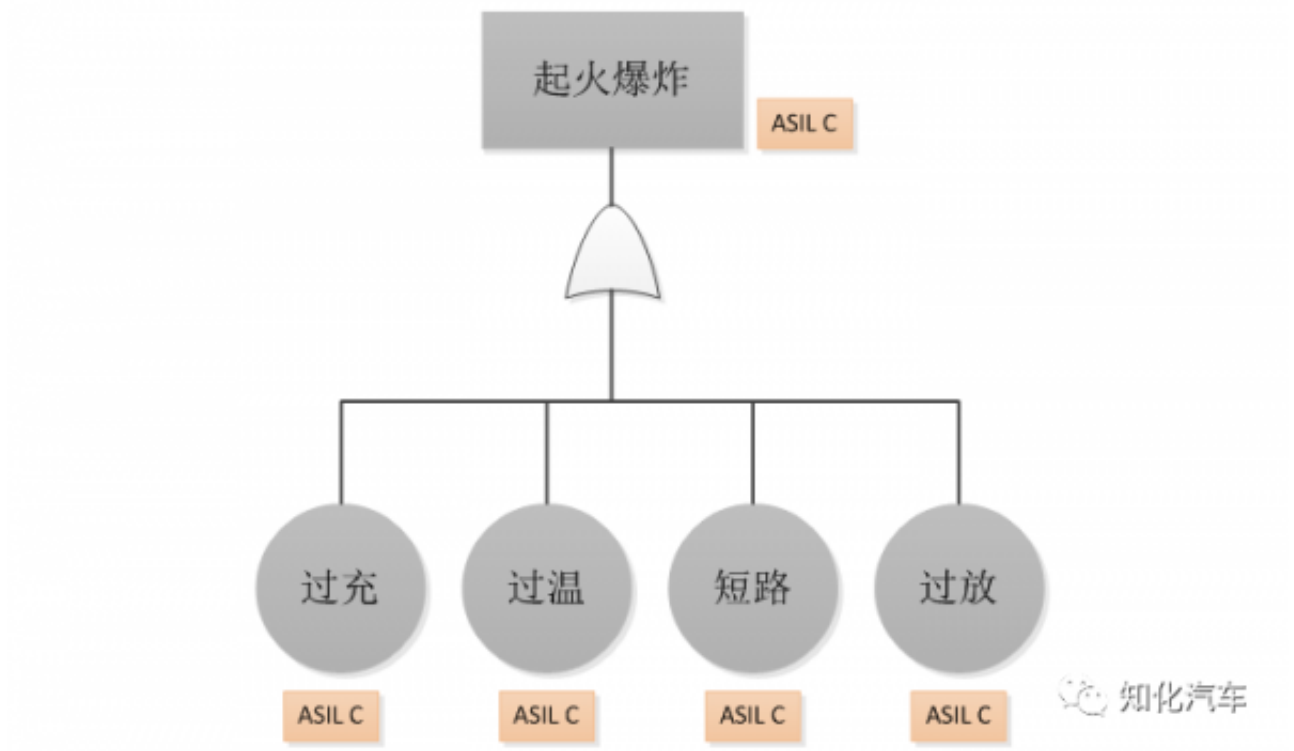
从Tesla/蔚来限充电量看电芯过充的功能安全设计

尽管Tesla/蔚来汽车近期的起火事件尚没有正式发布调查结果，但双方事后都对充电策略进行了调整，其中蔚来汽车则临时将充电量限制到90%，而香港停车场Model S事前电量充至97%，也有过充的风险。

对于电动汽车来讲，起火爆炸是最为严重的事件，从事故的严重度（Severity）、暴露率（Exposure）和可控性（Controllability）综合来看，都应该是一个ASIL C等级或以上的功能安全目标。在这一点上绝大多数的主机厂的意见是一致。

电芯的过充会直接导致起火爆炸的事件发生，根据ASIL等级的继承性，这应该也是一个ASIL C或以上的安全目标。

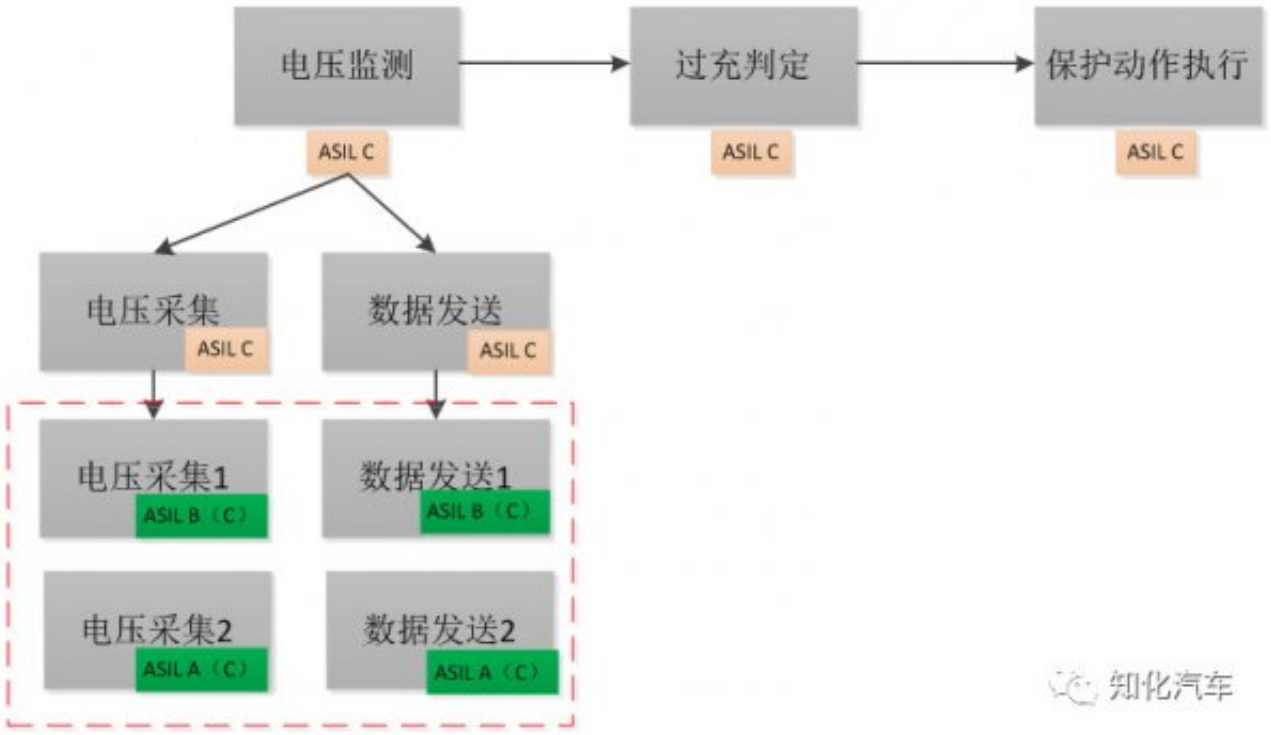


由此，可以得出一个功能安全目标，即在过充的情况下电池包不能发生起火，这需要一个ASIL C等级的设计。通常，电池包会有一系列的功能来防止过充后热失控的发生，这些相关的功能要满足ASIL C的要求，从功能的角度来看，主要可以分为3大部分：第1是电压的监测；第2是过充的判定，即电压是否超过了限定值；第3过充确认后执行保护措施，如断开高压。功能框图如下：

大部分的整车或PACK企业会把些功能的实现在电池包内完成，其中，监测主要由传感器实现，过充判定主要由BMS完成，保护动作执行主要由继电器实现。每一个功能都继承了过充ASIL C的属性，以下分别来看下每个功能的分析：

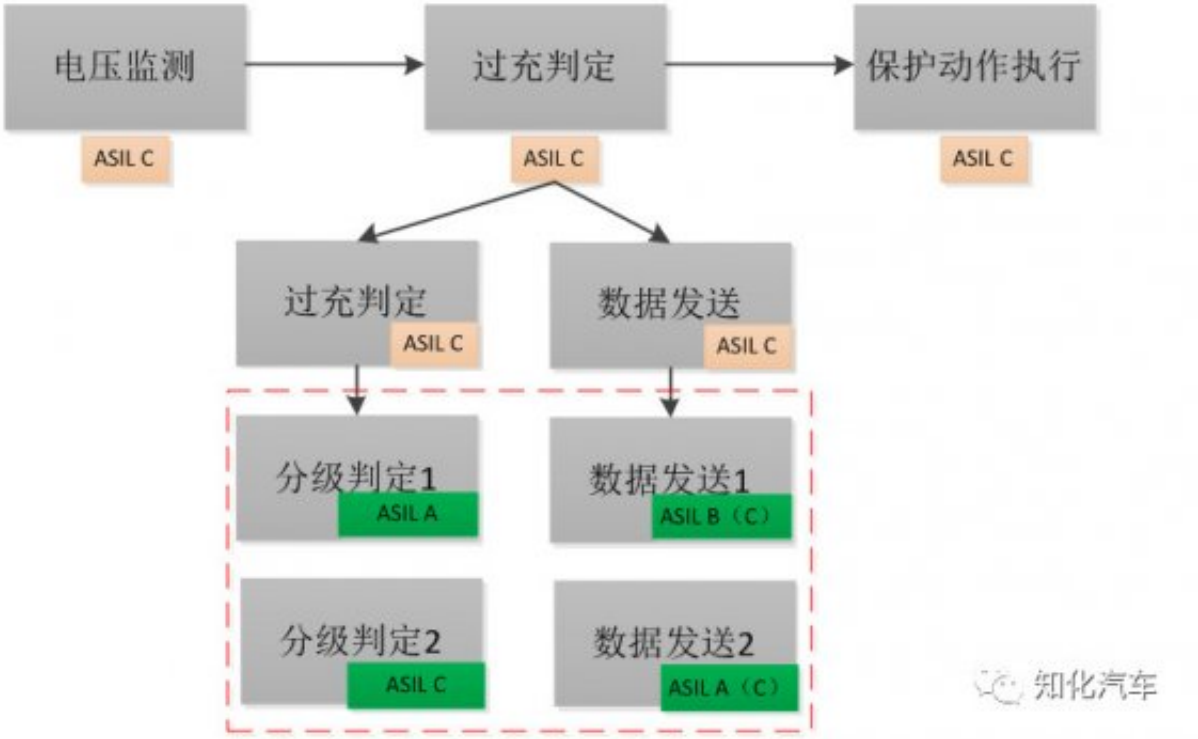
电压监测：首先，由电压传感器对电压进行监测，这里包括电压采集的精度、采集的频率；其次，将监测到的电压数据发送给BMS。这里需要电芯企业提供过压的阀值。为满足ASIL C的要求，传感器的失效率需要供应商提供，并且

要能满足要求，如失效率过高，就需要选用失效率低的产品，或是冗余一个传感器；电压数据传输路径CAN能否满足失效率要求，否则也需要增加一个冗余方案。如果采用了冗余的设计，就涉及到ASIL的分解，比如说一个定为ASIL B，另一个定为ASIL A。



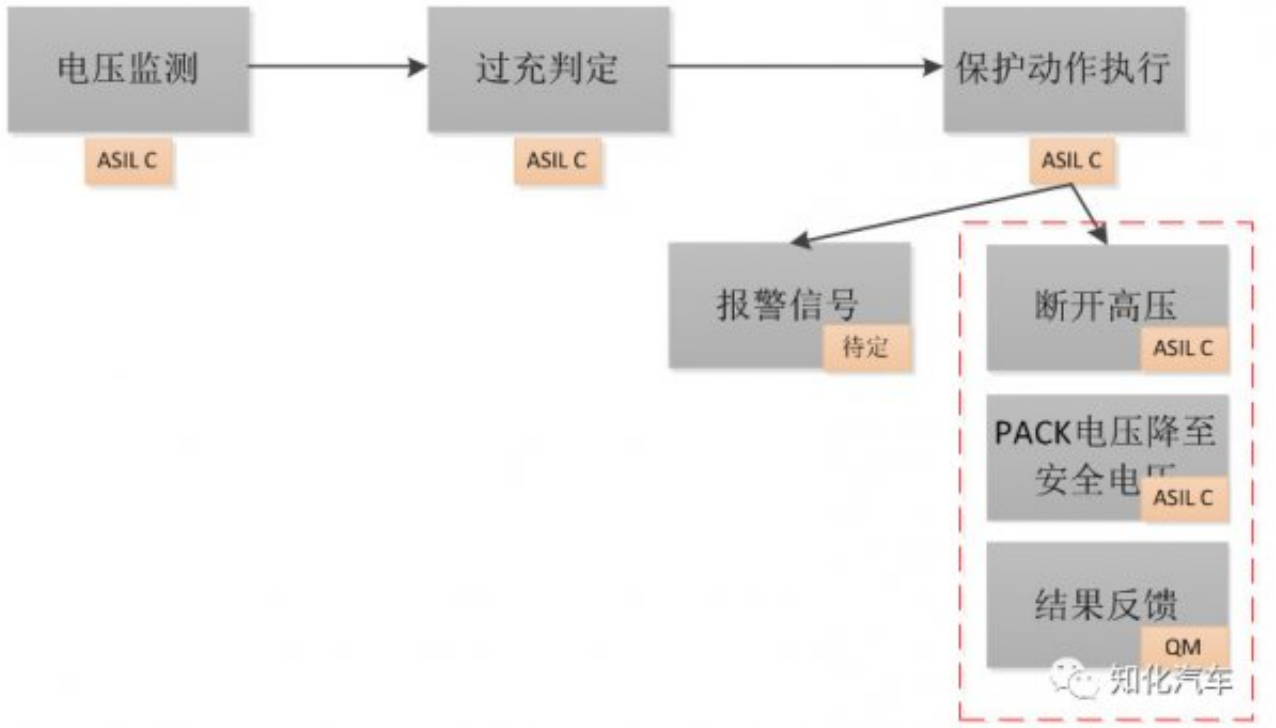
过充判定：

BMS收到采集来的电压数据，会根据电芯的过压的判定条件对是否过压进行判定。这里可能会涉及到不同的策略，不同的企业可能也有不同的做法，常见的是将电压分等级，当电压超过电压阀值1时（比如超过4.2V多少时间），BMS发送该等级的过压指令，当电压超过电压阀值2时（比如超过5V多少时间），BMS发送该等级的过压指令，根据等级的严重程度可以都继承ASIL C的属性，也可以允许个别等级低于ASIL C。如果BMS一直没有收到电压数据，也会做出相应的安全指令。



保护动作执行：

根据BMS对过电压等级的判定，以及发送的指令，继电器或其他部件进行热行。通常，较低过电压会发送报警信息给到整车，并通过声音或可视信号告知车主，较高过电压的会执行关断高压的指令。同样地，如果没有接收到BMS发来信号即BMS与执行功能之间的通讯失效，继电器也应该关断高压。



整个过充功能安全设计的思路如下：

以上任何一个功能环节出现问题都将无法防护过充造成进一步的危害。回到蔚来的这次事故，假定是由于过充导致的起火，则可能的情况：

（1）
发生过充，但是没有监测到，在采集环节出现了问题，没有采集到，或是采集的精度发生变化，采集不准确；

（2）准确采集到了电压但在过充判定时，计算出现了问题，SOC本身往往就具有比较大的误差；

（3） BMS发出过充指令，继电器发生故障，如粘连，无法断开高压。

在长时间发生过充的情况下，电芯正负极，隔膜等温度持续升高，最终导致单个电芯开始冒烟，起火，进而引起相邻电芯发生热失控。

原文地址：http://www.china-nengyuan.com/tech/139696.html