

# 阿里云物联网平台

刘煜  
西安中心



# 目录

平台架构

平台功能

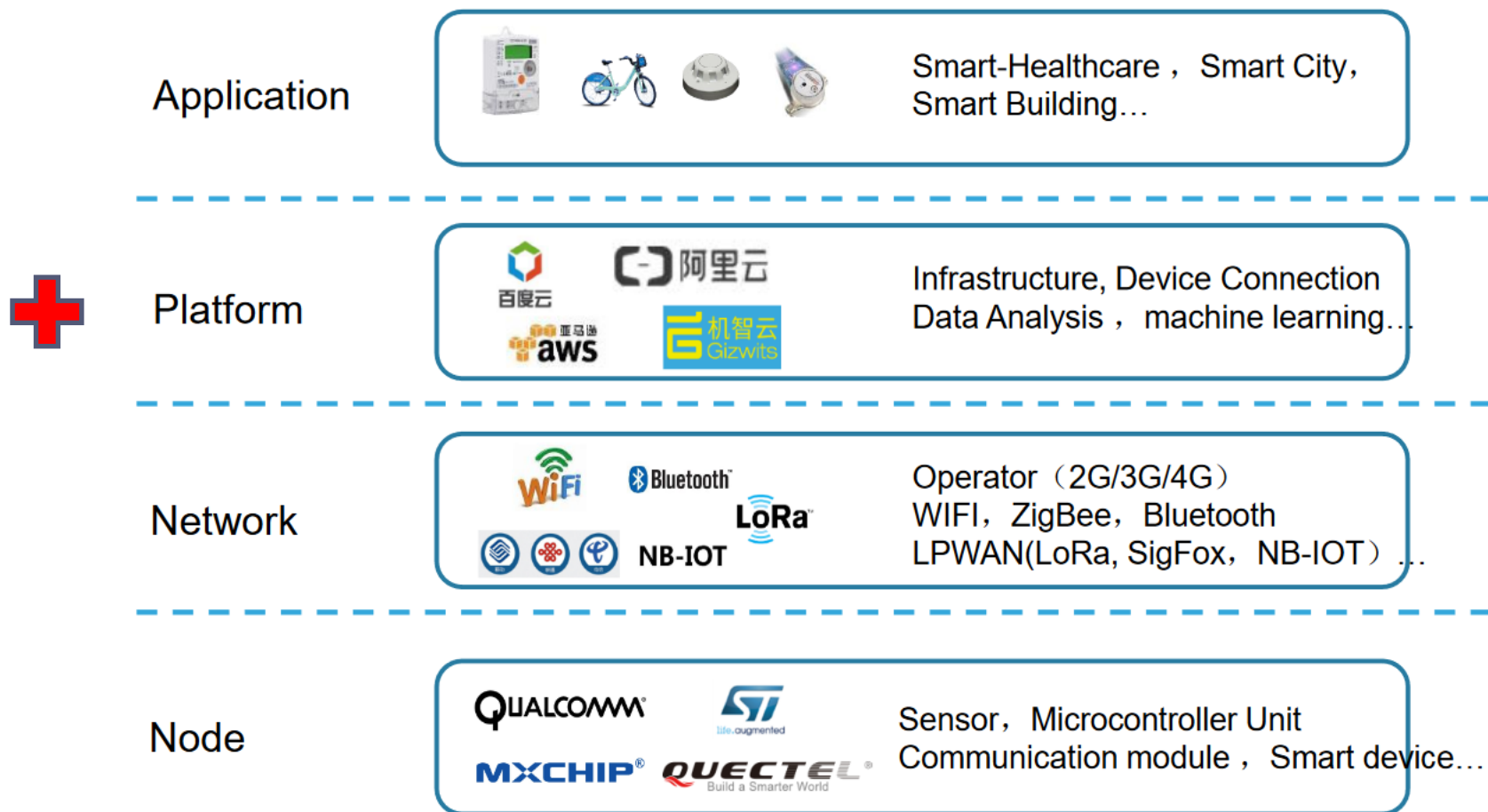
平台优势

设备接入

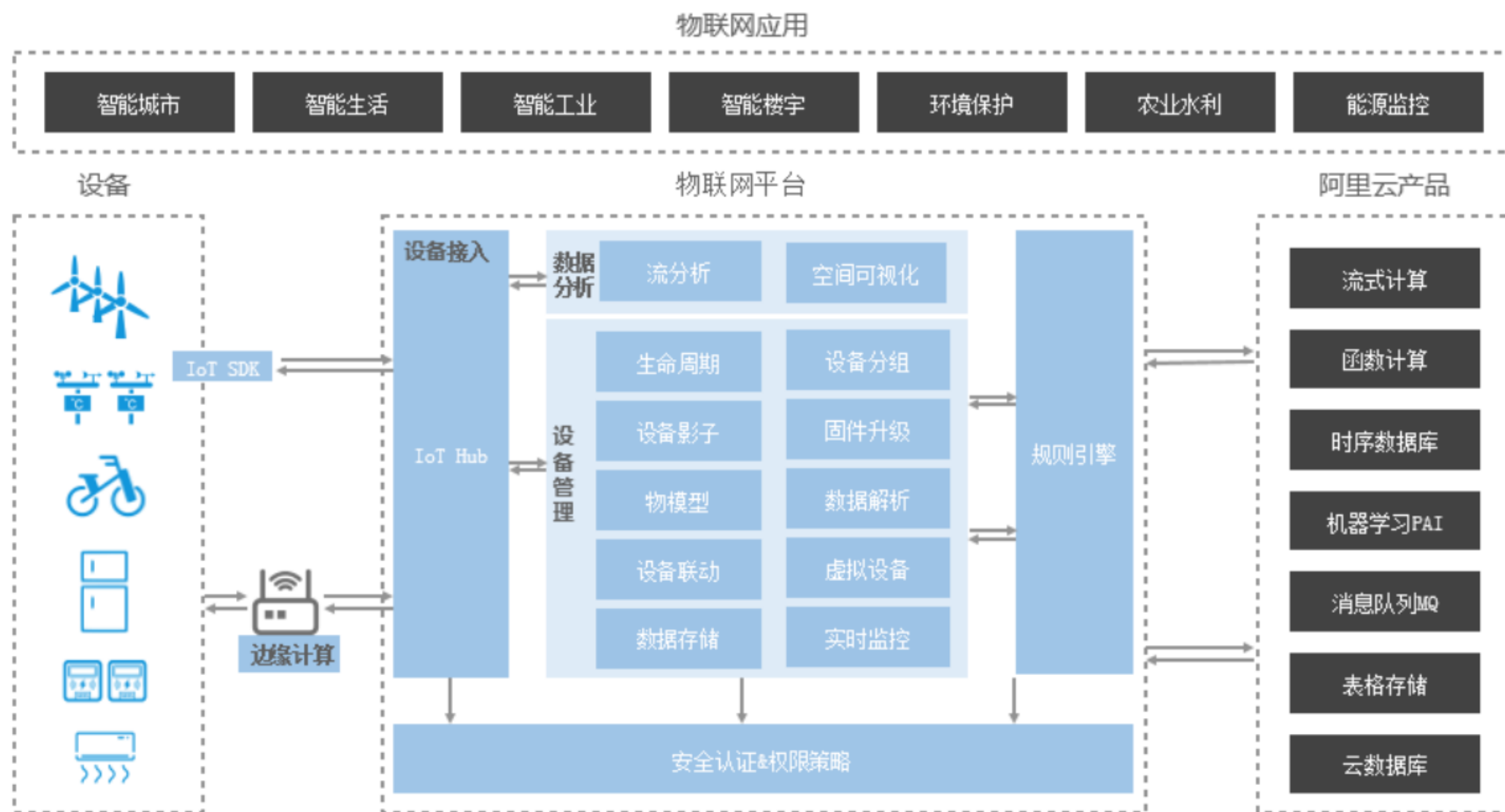
物模型

ALink协议

# 什么是物联网平台



# 平台架构



## 平台功能



## 设备接入



开源多种平台设备端代码，提供跨平台移植指导，赋能企业基于多种平台做设备接入。



提供MQTT、CoAP等多种协议的设备SDK，既满足长连接的实时性需求，也满足短连接的低功耗需求。



提供2/3/4G、NB-IoT、LoRa等不同网络设备接入方案，解决企业异构网络设备接入管理痛点。

## 设备通信



设备可以使用物联网平台，通过IoT Hub与云端进行双向通信。物联网平台提供了设备与云端的上下行通道，为设备上报与指令下发提供稳定可靠的支撑。

## 设备管理

提供完整的设备生命周期管理功能，支持设备注册、功能定义、脚本解析、在线调试、远程配置、固件升级、远程维护、实时监控、分组管理、设备删除。

提供设备物模型，简化应用开发。

提供设备上下线变更通知服务，方便实时获取设备状态。

提供数据存储能力，方便用户海量设备数据的存储及实时访问。

支持OTA升级，赋能设备远程升级。

提供设备影子缓存机制，将设备与应用解耦，解决不稳定无线网络下的通信不可靠痛点。



## 安全能力（认证）




提供一机一密的设备认证机制，降低设备被攻破的安全风险，适合有能力批量预分配ID密钥烧入到每个芯片的设备。安全级别高。



提供一型一密的设备预烧，认证时动态获取三元组，适合批量生产时无法将三元组烧入每个设备的情况。安全级别普通。

## 安全能力（通信）



支持TLS（MQTT\HTTP）、DTLS(CoAP)数据传输通道，保证数据的机密性和完整性，适用于硬件资源充足、对功耗不是很敏感的设备。安全级别高。



支持TCP(MQTT)、UDP(CoAP)上自定义数据对称加密通道，适用于资源受限、功耗敏感的设备。安全级别普通。



支持设备权限管理机制，保障设备与云端安全通信。



支持设备级别的通信资源（TOPIC等）隔离，防止设备越权等问题。

## 规则引擎解析转发数据

配置规则实现设备与设备之间的通信，快速实现M2M场景。

将数据转发到消息队列（MQ）中，保障应用消费设备上行数据的稳定可靠性。

将数据转发到表格存储（Table Store），提供设备数据采集 + 结构化存储的联合方案。

将数据转发到流计算（StreamCompute）中，提供设备数据采集 + 流式计算的联合方案。

将数据转发到TSDB，提供设备数据采集 + 时序数据存储的联合方案。

将数据转发到函数计算中，提供设备数据采集 + 事件计算的联合方案。

## 物联网平台的优势

	基于阿里云物联网平台开发	传统开发
设备接入	提供不同环境下设备端SDK，帮助设备快速接入云端。支持全球设备接入，支持异构网络设备接入，支持多协议设备接入。	不仅需要搭建基础设备，还需要自行寻找嵌入式开发人员与云端开发人员联合开发，工作量大，效率低。
性能	具备亿级设备的长连接能力，百万级并发的能力，并且架构支持水平性扩展。	需要自行实现扩展性架构，极难做到从设备粒度调度服务器、负载均衡等基础设施。
安全	提供多重防护保障设备云端安全。	需要额外开发和部署各种安全措施。
稳定	服务器可用性99.9%，单点故障，自动迁移。	需要自行发现宕机并完成迁移，迁移过程服务会中断。
简单易用	一站式设备管理、实时监控设备场景、无缝连接阿里云产品，物联网复杂应用的搭建灵活简便。	需要购买服务器搭建负载均衡分布式架构，需要花费大量人力物力开发“接入+计算+存储”一整套物联网系统。

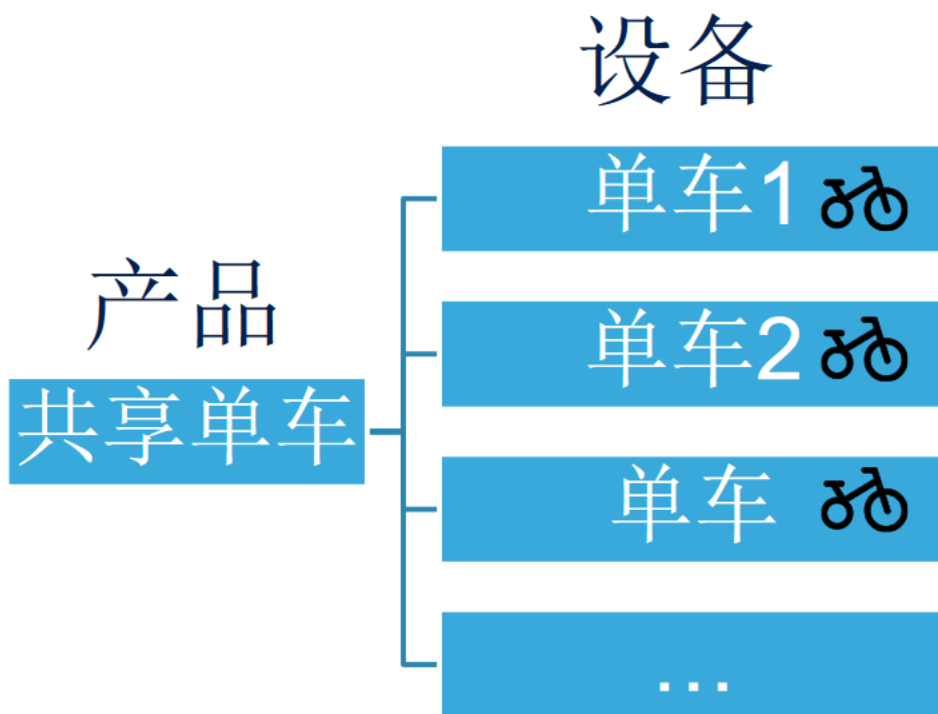
## 产品与设备

### 产品

- 设备的集合，通常指一组具有相同功能的设备。物联网平台为每个产品颁发全局唯一的**ProductKey**。每个产品下可以有成千上万的设备。

### 设备

- 归属于某个产品下的具体设备。物联网平台为设备颁发产品内唯一的证书**DeviceName**。设备可以直接连接物联网平台，也可以作为子设备通过网关连接物联网平台。



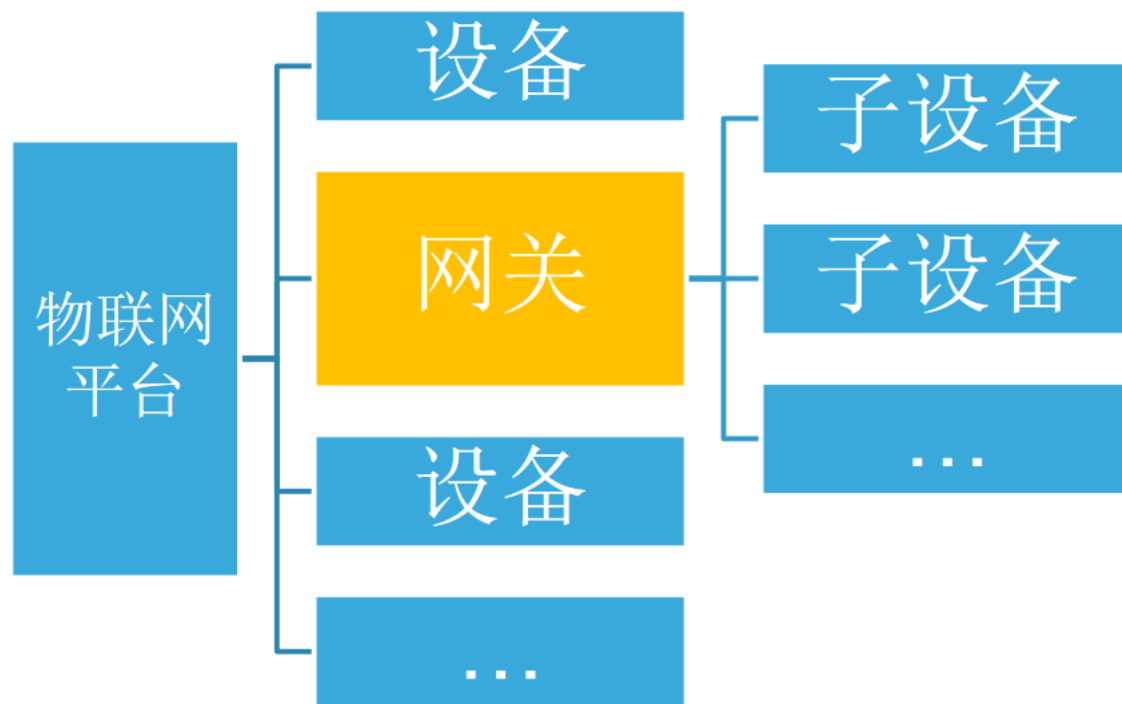
## 网关和子设备

### 网关

- 能够直接连接物联网平台的设备，且具有子设备管理功能，能够代理子设备连接云端。

### 子设备

- 本质上也是设备。子设备不能直接连接物联网平台，只能通过网关连接。



## 设备认证

ProductKey

- 物联网平台为产品颁发的全局唯一标识。

ProductSecret

- 物联网平台为产品颁发的密钥，和ProductKey成对出现。

DeviceName

- 在注册设备时，自定的或自动生成的设备名称，具备产品维度内的唯一性。

DeviceSecret

- 物联网平台为设备颁发的设备密钥，和DeviceName成对出现。

## 认证方案

对比项	一机一密	一型一密	子设备动态注册
设备端烧录信息	ProductKey、DeviceName、DeviceSecret	ProductKey、ProductSecret	ProductKey
云端是否需要开启动态注册	无需开启，默认支持。	需打开动态注册开关	需打开动态注册开关
是否需要预注册DeviceName	需要，确保产品下DeviceName唯一	需要，确保产品下DeviceName唯一	需要，确保产品下DeviceName唯一
产线烧录要求	逐一烧录设备证书，需确保设备证书的安全性	批量烧录相同的产品证书，需确保产品证书的安全存储	<ul style="list-style-type: none"><li>· 网关可以本地获取子设备ProductKey</li><li>· 将子设备ProductKey烧录在网关上</li></ul>
安全性	较高	一般	一般
是否有配额限制	有，单个产品50万上限	有，单个产品50万上限	有，单个网关最多可注册1500个子设备
其他外部依赖	无	无	依赖网关的安全性保障



## 设备生命周期



创建设备：真实的物理设备要连接到物联网平台，首先需要在平台上创建（或者叫注册）设备。



激活设备：设备创建后默认处于“未激活”状态，真实物理设备在云端认证成功，上线一次后即激活，激活后的设备状态为“在线”或“离线”。



删除设备：当设备处于报废、被攻击或者不可用时，可以删除设备。



禁用设备：设备发生异常，例如通信异常、连接异常时，有可能被攻击，但又不想将其彻底删除，这时可以对设备进行禁用，云端会断开与设备的通道，以防止风险进一步扩大。



启用设备：当设备处于禁用状态时，管理者确认设备恢复正常后，可以对设备启动，恢复设备与云端的连接。

## 物模型

物模型，简称TSL，即Thing Specification Language。是一个JSON格式的文件。它是物理空间中的实体，如传感器、车载装置、楼宇、工厂等在云端的数字化表示，从属性、服务和事件三个维度，分别描述了该实体是什么，能做什么，可以对外提供哪些信息。定义了这三个维度，即完成了产品功能的定义。



属性：设备运行的状态，支持GET和SET服务，应用可以发起对属性的读取和设置请求。



服务：设备可被外部调用的能力或方法，可设置输入参数和输出参数。相比于属性，服务可通过一条指令实现更复杂的业务逻辑，如执行某项特定的任务。



事件：设备运行时的事件，事件一般包含需要被外部感知和处理的通知信息，可包含多个输出参数。如，某项任务完成的信息，或者设备发生故障或告警时的温度等，事件可以被订阅和推送。

## 物联网应用示例

- 设备每分钟上报可燃气体浓度值
- 设备在可燃气体浓度超过阈值后报警，并通知应用服务器
- 设备收到警报解除信息后停止报警
- 可燃气体浓度值被平台转发到应用服务器，并存储到数据库，同时在web端显示近期浓度数据曲线
- 报警消息被平台转发到应用服务器，并在web端显示
- 用户通过web端页面解除报警
- 用户通过web端页面设置【阈值】参数



# ■ Alink协议

Alink协议是针对物联网开发领域设计的一种数据交换规范，数据格式是JSON，用于设备端和物联网平台的双向通信，更便捷地实现和规范了设备端和物联网平台之间的业务数据交互。如果产品定义了物模型，设备可以按照属性、事件、服务，协议分别上报数据。

属性：

上行

请求Topic: /sys/{productKey}/{deviceName}/thing/event/property/post

响应Topic: /sys/{productKey}/{deviceName}/thing/event/property/post\_reply

下行

请求Topic: /sys/{productKey}/{deviceName}/thing/service/property/set

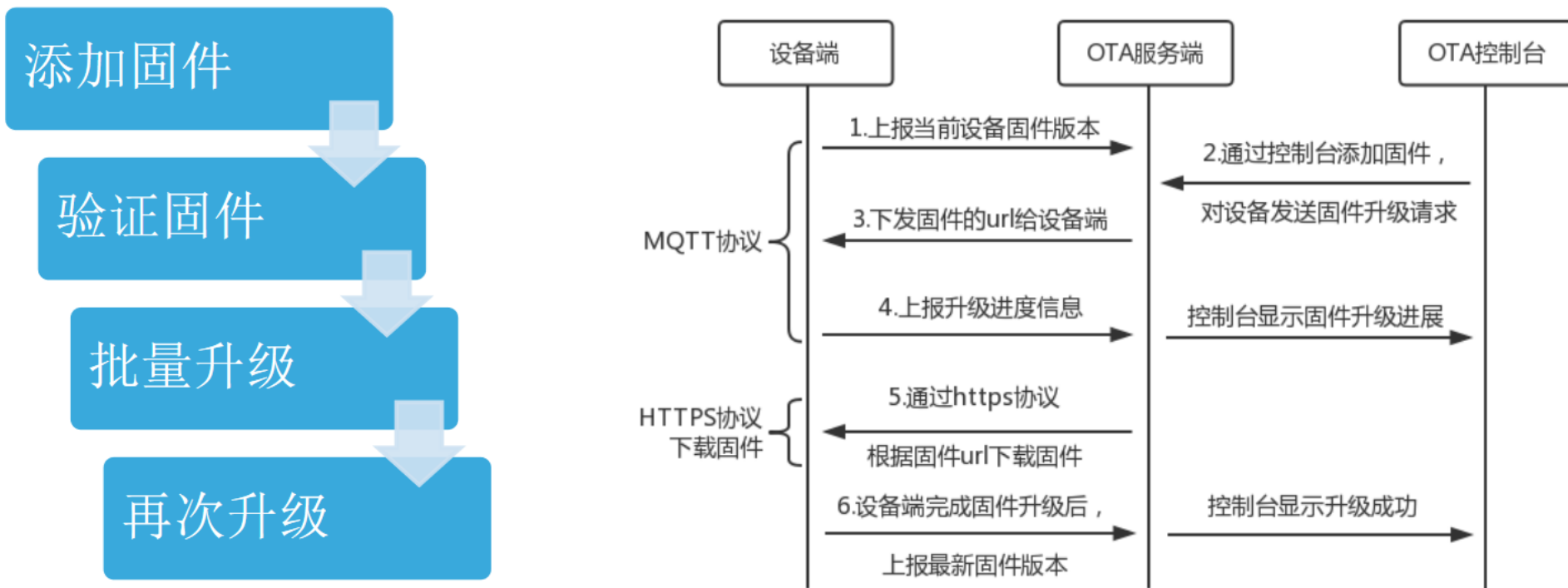
响应Topic: /sys/{productKey}/{deviceName}/thing/service/property/set\_reply

## 阿里云MQTT实现

支持的MQTT协议版本	兼容3.1和3.1.1版本
与标准MQTT的区别	不支持遗嘱消息
	不支持retained message
	不支持QoS2
	心跳间隔范围：30~1200秒，建议300秒以上
	在原生MQTT topic上支持RRPC同步模式，服务器可以对设备进行同步访问(得到设备回执)
安全等级	支持TLS v1, v1.1, v1.2版本
	支持非加密通道连接

## 固件升级

- 当设备固件发现重大bug或安全漏洞时，通过OTA服务升级固件，降低bug及安全风险。



## 应用层开发流程





海量视频 贴身学习



超多干货 实时更新

# THANKS

— 谢谢 —