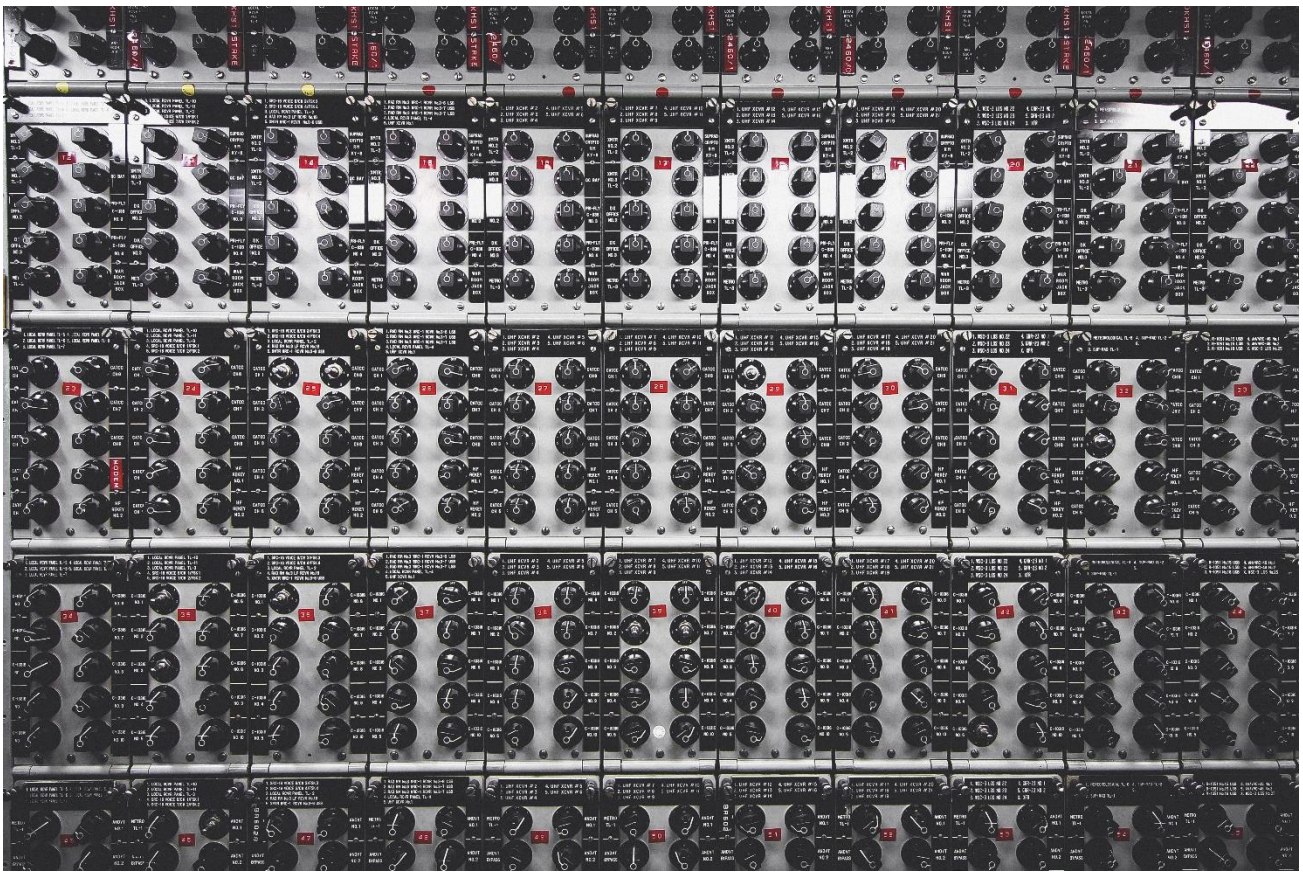
AuVerte

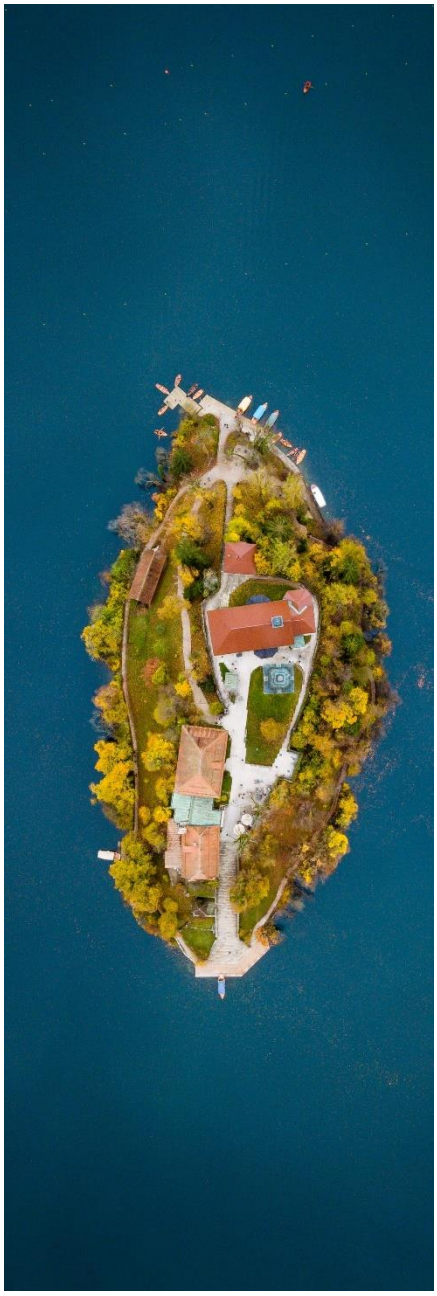
WHITE PAPER

IoT Systems Without Gateways

Version 1.0 ▲ 11 August 2020



AuVerte AG ▲ Rothusmatt 14, CH-6300 Zug, Switzerland ▲ www.AuVerte.com



Would you buy network equipment or computers that are unable to directly use internet protocols? Decades ago, all the proprietary network protocols gave way to IP (internet protocol). We would have a difficult time to even think of how a world would look like without this standardized connectivity. And yet, many IoT (Internet of Things) devices today are unable to directly connect and communicate with the internet. They carry "Internet" in their name but require gateways to provide the protocol conversions for connectivity to the IP world. Such systems form isolated islands where the gateway is the only means to and from the Internet. In this whitepaper, we review some of the reasons why so many IoT systems turn out to be IoG (Internet of Gateways) systems and how it impacts the ownership experience. We also present a possible way forward.

Today, why are so many IoT systems based on gateways and closed eco-systems? Let us first review this topic from the angle of the IoT vendor.

When we think of IoT we often envision a large quantity of smart gadgets that enrich our lives. As buyers, we desire these devices and prefer to purchase them at a reasonably low cost. With global manufacturing capacity and agile engineering processes, it is relatively easy for manufacturers to offer these devices at aggressively low pricing. However, this hardware-centric business model does not allow for enough profitability for IoT companies to also offer design, customization, integration, application, and maintenance services. Vendors have a justifiable need to search for solutions that will sustain their business in a meaningful manner, and that means profits need to be generated from more than just the hardware-only business. This is best achieved by forming eco-systems of devices that lock a customer into a specific technology and offering. Offering proprietary gateways is an effective way to achieve this lock. This allows for higher profit margins and has the potential for ongoing revenue creation. In the building automation industry, this very trend started in the early 1970s with the advent of the microprocessor and this strategy has survived into the age of IoT. This is demonstrated by the uncountable number of building automation protocols and 'standards'. It follows then that vendors will apply a large marketing budget to substantiate why their eco-systems and applications are the preferred ones. But are these objectives in the best interest of the IoT customer? Are the disadvantages possibly bigger than they first appear?

At first glance, the pure IoT versus IoG architecture does not matter. If we look at a black box model with a collection of IoT devices forming a system and that is somehow connected to the internet, we might very well not be able to discern a measurable difference. If an IoT device sends an event to a remote host, we cannot readily see a difference between and end-to-end packet and a protocol conversion at the gateway. Similarly, if we send a control command from the internet to an IoT thermostat, we cannot differentiate if the command gets translated by a gateway or if the command goes transparently to the end device. With a gateway in charge, we might get a quicker acknowledgement. However, only an actual acknowledgement from the

targeted end device will assure that the desired function has been executed fully. Because this black box observation does not yield much differentiation, we need to look inside the two topologies.

A number of challenges befalling the gateway-based IoT topology:

- Gateways treat the end-nodes as dumb sensor and actuators and do the heavy lifting of providing internet facing APIs and device context management. Any added device type that the gateway does not readily recognize forces a major upgrade to the gateway.
- Gateways are the nerve center of a certain number of IoT devices. The complexity to manage and operate an application is growing exponentially with the number of devices and services. This tends to make gateways rather complex devices. Any change to an application requires touching the setup, firmware, or hardware of the gateway.
- Firmware upgrade to the IoT devices are meaningless if the upgraded features are not supported by the gateway's API.
- It is difficult to manage the cyber security assessment for the secondary side non-IP protocols of a gateway. The old assumption that just the internet-facing side is prone to cyber security attack is no longer valid. We are better off to assume that all networks are multi-homed (e.g. any Bluetooth network could be bridged to the Internet by any connected mobile device).
- If a deployed gateway is obsoleted, or if the gateway vendor changes their commercial strategy or goes out of business, it is almost impossible to re-purpose the existing IoT devices onto a new gateway and vendor. This often forces the need for a forklift upgrade and creates unwanted costs and comes at an unnecessary environmental burden.
  The majority of the IoT investment is in the field devices (sensors, actuators), their wiring, and their maintenance. By assuring that they remain relevant, useful and properly maintained for as long as possible creates a sound investment horizon. Forklift upgrades demanded by obsolete gateways is costly for business.

AuVerte offers full end-to-end IP-connectivity for all its devices without the need of a gateway. This capability is not only available for all devices directly connected to the Ethernet but includes all other devices as well and even includes the battery powered 802.15.4 Rf mesh network sensors. Each device supports the CoAP over DTLS protocol that provides standard end-to-end IP connectivity with its well understood cyber security mechanisms. Any firmware upgrade to any device will directly result in enhanced network facing APIs. No consideration must be made for upgrading or maintaining gateways.

Utilizing DTLS allows for easier third-party integration of AuVerte's IoT devices where the cyber security aspects are covered through certificates. This allows control of the access policies, such as providing a time-limited connectivity to a device or the cancellation of issued certificates without having to re-key the entire IoT system.

AuVerte is not against gateways. Rather, our position is that gateways can serve a valid purpose in certain instances. However, gateways should not dictate network and application topology and a gateway cannot be made the mandatory single element that needs to be present in any and every IoT deployment. Gateways and end-to-end IP connectivity in fact can co-exist. For example, a DALI lighting gateway might be a sound choice to achieve a cost-effective light control application. We can describe such a device as a gateway that connects the internet with the DALI dimming nodes. The key in this instance is that such a gateway should not be overloaded with non-DALI functionality.

When an IoT buyer chooses an advanced pure IoT solution that is not centered around a gateway, it means less dependency on the technology vendor, a strategic advantage. When every device has true IP connectivity and an open API, a vendor's integration strategy, cloud and middleware offering can be replaced or augmented with additional technology providers under the control of the IoT system owner. This creates an improved and more competitive playing field for innovation and lowers the cost of IoT systems. If desired, IP-enabled devices with an open API can be decoupled from a vendor eco-system and these devices can become part of a yet to be defined future system. This puts the IoT owner in control of his digital journey.

Philipp Roosli, AuVerte CTO