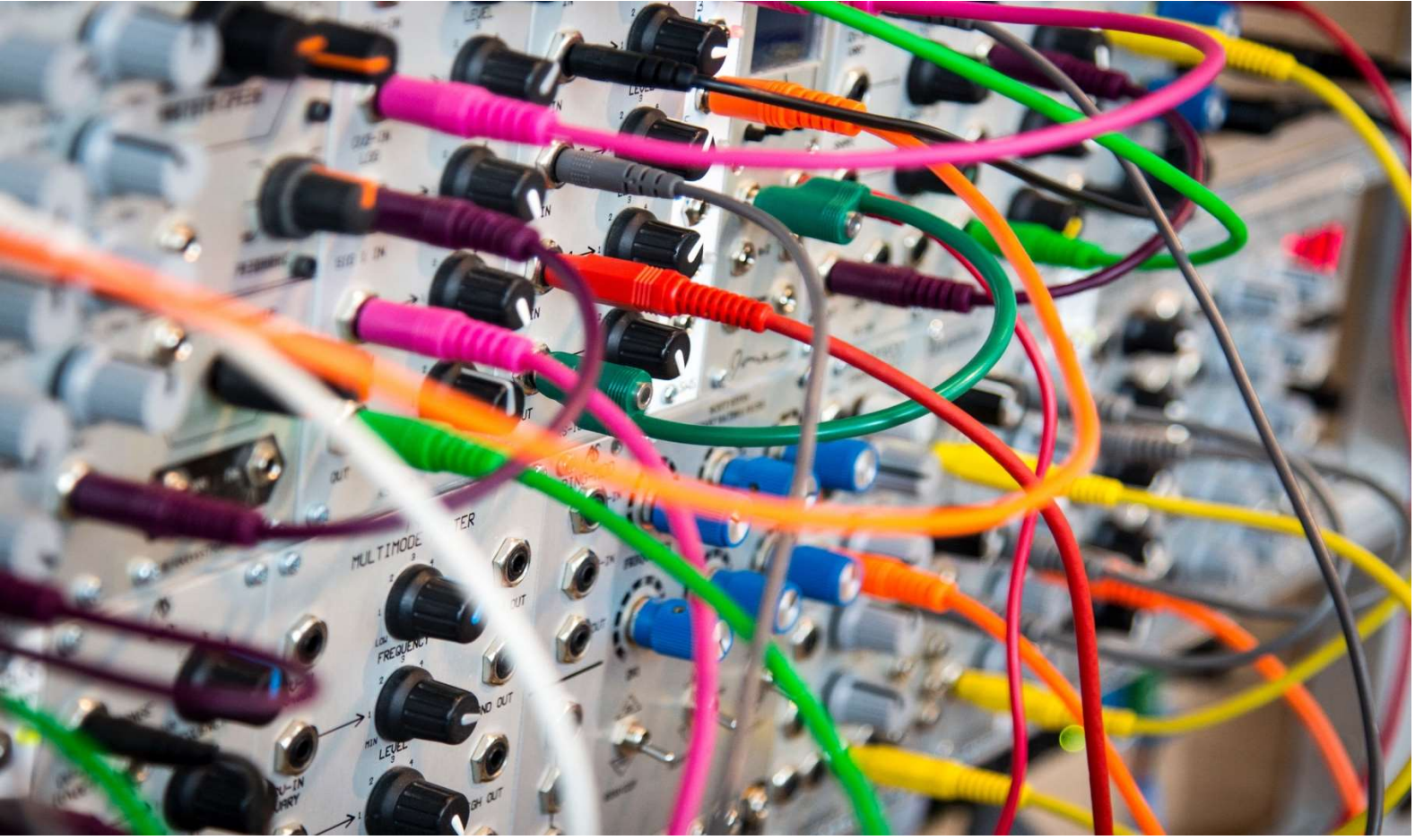


Digital twins for Industrial IoT with Altior

A technical white paper

Part 2: device twins networking and communications

InkwellData
Connected Innovation

Digital twin for industrial IoT with Altior

Part 2: device twins networking and communications

Introduction

This is the second of a short series of technical white papers, by Massimo Cesaro, about Inkwell Data Ltd.'s Altior digital twin and middleware software platform for Industrial IoT application and services.

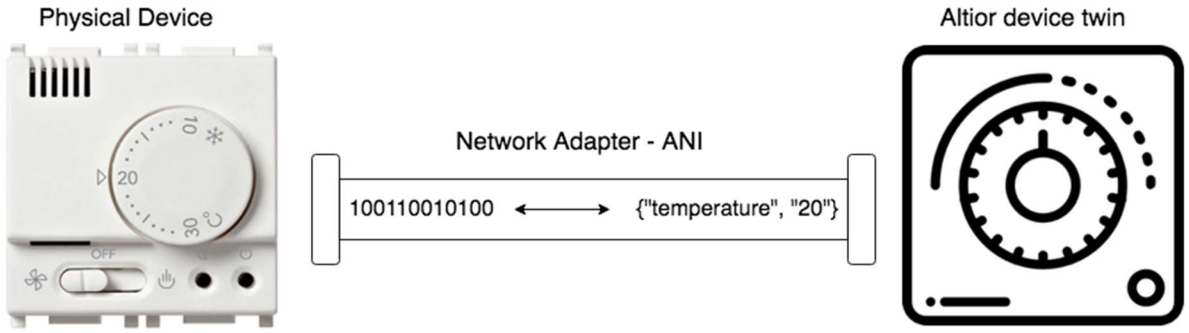
The purpose of this series is to introduce the reader to the Altior architecture and how it can be applied to many different cases, without requiring a specific knowledge of software development of telecommunication engineering disciplines.

For more information about the digital twin design concepts in Altior, please refer to part 1.

The digital twin communications model

Digital twins on Altior are logical entities connected to their physical counterpart (the actual devices) through a virtual pipeline, in a point-to-point secure link.

The virtual pipeline is independent from the underlying communication technology and acts as a smart component because it provides a conversion from the low-level physical protocol (usually made of binary frames) to the high-level data structure representation in the digital twin.



Abstracting the network communication is part of the middleware features of Altior.

In the Altior architecture, the term middleware refers to the software layer that resides between the physical layer components (hardware), firmware, or embedded software, which deal with low-level system calls and communication protocols, and the upper layer applications generally interacting via the network.

The network adapter is also known as the Abstract Network Interface (ANI) of Altior; the ANI is another "Altior Function", that is a high level Altior component like the device twins' runtime environment (RTE).

The scope of the ANI is to provide digital twin instances with a generalized network access and interactions; this allow Altior device twins to be independent of the actual network technology used.

To set up a communication channel with a physical object, the device twin instance subscribes to the ANI its physical counterpart. This is called a digital twin to network binding.

For example, a Wi-Fi thermostat is connected to Altior through a Wi-Fi network interface. The corresponding digital twin of the Wi-Fi thermostat is connected to a Wi-Fi ANI.

The association between the physical thermostat and its digital twin is maintained by one or more unique physical parameters, such as the Wi-Fi (IP) address of the physical thermostat, its serial number, GPS installation coordinates or any other feature included in the digital twin definition.

Altior then associates the physical object to a uniquely identified device twin instance.

The ANI then creates the virtual data pipeline between the physical thermostat and the digital twin, handling all the connection details whilst delivering only meaningful data to both sides of the pipeline.

Note that Altior keeps separate pipelines (communication channels) for every digital twin. This means that:

- if a network connection fails, it only affects the single digital twin instance it is linked to;
- communication channels run concurrently for minimal latency;
- the data traffic from different digital twins is isolated; and
- the security encryption/decryption keys are different for every instance.

Communication channels are transparently managed by Altior, and just like any other Altior Functions; these can be distributed and replicated for scalability and improved reliability.

The middleware approach to network abstractions allows the Altior users to focus on the design and implementation of their IoT services, rather than worry about network implementation details.

This is an important advantage of developing an IoT services on Altior: you are not designing and building a service based on the features and services offered by a specific technology, because as long as there is an Altior ANI for it, any network technology can be used to the same effect.

What is involved in a “standard”?

Choosing a network technology for an industrial, deployed at-scale, IoT application should be a matter of many considerations, not only of a strictly technical nature but first and foremost of a strategic one.

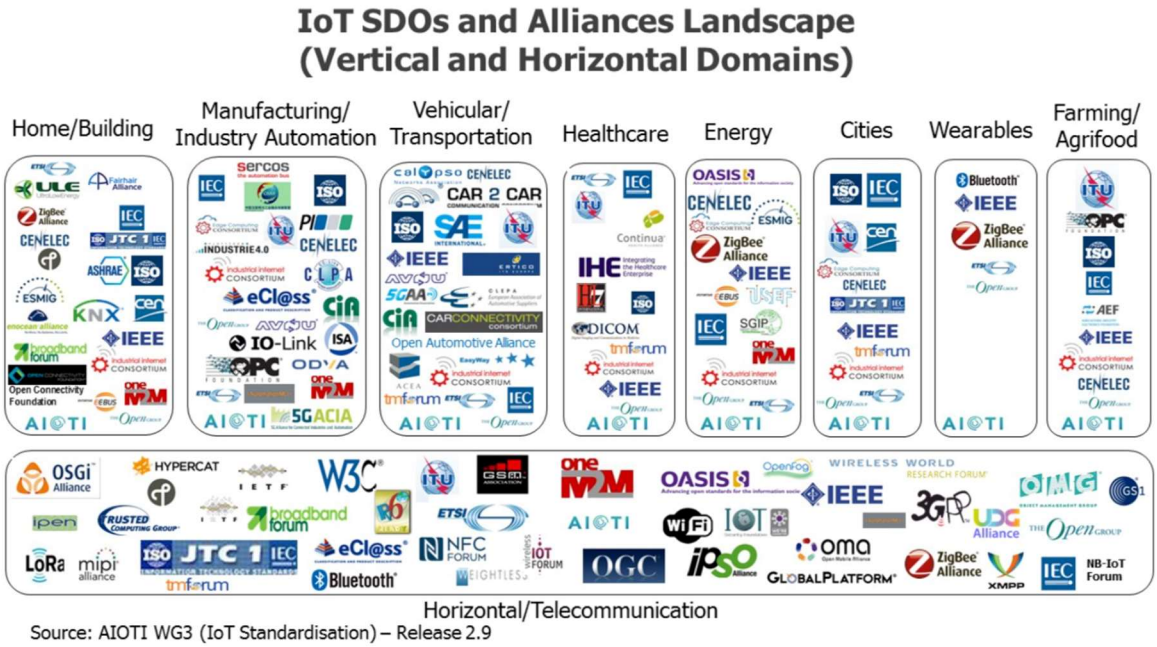
The supposedly safe choice is to select an “industry standard” network technology, in the hope that being a shared technology, maybe supported by an industrial consortium or alliance, it will make it “easy” to support a specific IoT service.

But even choosing a “standard” technology is a difficult task: the amount of existing industry standards is staggering, and most of the standards are pseudo-standards, heavily marketed, at the risk of spreading hype-driven solutions.

Making things worse, “technical standards” are typically not compatible with one another. This can be due to the foundations of the protocols or to more subtle differences, but the end-result is the same – one “standard” network cannot be converted to another “standard” without a major overhauling of the IoT service.

The number and variety of IoT industry standards is the subject of an interesting classification made by the “Alliance for Internet of Things Innovation”, the AIOT[1].

[1] https://aioti.eu/



Source: AIOTI WG3 (IoT Standardisation) – Release 2.9

For the Telecommunication domain alone, there are over twenty different, and sometimes conflicting, industry alliances/standards before the introduction of the widely-debated 5G networks, meaning that choosing the right one for a specific application is a convoluted process.

At Inkwell Data, we believe that before considering the specific technical features of wide-ranging network technologies, strategic questions about selecting an industrial IoT network infrastructure should focus on the underlying domain problem to be addressed, and the related business model, including:

- **Is the network technology supported by an ecosystem?**
  An existing or growing ecosystem means device availability. It is common to find industrial IoT solutions, such as smart metering or smart lighting, built on a stovepipe model where everything, from the physical sensor to the network devices and the head-end system are provided by a single vendor. While this might look attractive, because it lessens the problems of integration, a vendor lock-in is probably not acceptable for most applications at scale.

- **Is it a proprietary technology?**
  It is often not immediately apparent if a technology is proprietary or not. In the LPWAN[2] world, for example, there are supposedly open technologies with components (sensors and network devices) available from different manufacturers and suppliers (e.g. LoRa).
  Unfortunately, these components ultimately depend on proprietary/patented technologies controlled by a single company.
  On the other hand, there are really open LPWAN technologies where everything, from the circuit design schematics and the low-level firmware to the application layer are open sourced and publicly available and very well supported (e.g. wMBus or Weightless). We believe that truly open technologies are often not only possible, but highly recommended.

[2] Low Power Wide Area Network are an interesting technology to provide wireless connectivity to low-power and low-cost devices over large distances, usually in license exempt frequency bands.

- **Can the technology be deployed as a private network?**
  Public networks, such as mobile and cellular networks, can be a viable solution for many business cases. This is particularly true, when the cost or the time required to set up a private network infrastructure is not compatible with the end users' business requirements.
  The drawbacks of a public network are however not negligible: the security of the network, the service and data availability, the actual network coverage are all in the hands of the network operator.
  Then there is the longevity of the network to consider: most of the machine-to-machine applications developed in the last 10 years and depending on the public cellular network are already badly affected by the 2G networks sunsetting.
  While unpredictable network longevity might be acceptable for some services, for most long term IoT applications where the lifespan of the service is 10+ years, only deploying a private IoT network will provide full control of the data transport infrastructure and better budgeting and costs control over the long run.

- **Is the technology sustainable?**
  Calculating the ROI (return on investment) for an industrial IoT technology infrastructure is a complex task. The licensing fees or the data transport costs need to be transparent and coherent with the end user's business model.
  For massively deployed industrial IoT services such as electricity, water or gas smart metering, the connectivity cost and availability must be carefully considered for all the lifetime of the meter itself. This is commonly up to 10 years or more, and for this period of time the "truck rolls", servicing the deployed devices, can be a ROI killer.
  On a public cellular based network infrastructure, the truck roll to replace a SIM card required to switch the network operator can be a logistic barrier. Building a private LPWAN infrastructure requires a lot of initial effort in terms of time, money and skills required but ensures full network control for the lifetime of the IoT service. A major difference in terms of predictable ROI calculation.

In most real-world applications, the choice of the IoT infrastructure cannot be or should not be an exclusive, make-or-break decision.

For the majority of smart city applications, including smart metering and sub-metering applications, no single technology can or should try to cover the 100% of devices installed. The right "horse" should be chosen for the right "course."

In fact, the service requirements will largely dictate the type of network(s) to use.

For an asset tracking IoT application, the device itself is moving and can adapt to a spotty network coverage, for applications with fixed devices, such as smart meters or street lighting, the network coverage simply must function when needed.

The network architecture will also be a function of the device installation density: for example, in urban areas with a high device concentration a point-to-multipoint LPWAN will be a sound choice, whilst in a rural setting using a public cellular network could be more convenient.

A combination of different network technologies will often be required to operate successfully a complex industrial IoT service at scale.

At Inkwell Data we believe that selecting a specific network technology should not be an irreversible path, and that, moreover, rolling-out a successful IoT service requires a lot of flexibility to deal with the fast-changing network communications landscape.

Altior industrial IoT service design

Using different network technologies for the same class (type) of IoT service should not be an additional burden; from an application point of view, private LPWAN or public cellular connectivity should NOT require different management.

This is exactly what the Altior middleware feature delivers, by hiding the technology details for the high-level applications.

With Altior, Inkwell Data has developed a top-down method to industrial IoT service designs:

1. First, let the business requirements drive what kind of IoT service needs to be implemented, its peculiarity and features, regardless of the network technology characteristics.
   Defining the digital twin feature allow for an easier selection process of the physical devices and sensors to be used.

2. Second, design and prototype the IoT service with the Altior digital twins and application development tools, to evaluate the fulfillment of the original business requirements, keeping in mind that when the design will be validated, the application will be deployed at scale without further modifications.

3. Lastly, adapt the final application to the technologies available and those better fitting the business requirements. Build a pilot system to validate the complete application on a small but representative sample and evaluate the results thoroughly; use the feedback to fine tune the application and then proceed with the massive roll-out.

> Using the previous thermostat device example, to develop a temperature tracking application does not require the knowledge of what kind of network technology is used to get the temperature data out of the temperature sensor. On Altior, it is just a matter of reading the “temperature” property of the digital twin instance and use the data in the way required. The physical thermostat can be connected on Altior using a Wi-Fi network, or a cellular or LPWAN network. This selection will not, in itself, alter the application, which will remain the same, regardless of the communication link, and the different data transport technologies can be used concurrently on the same application.

The Altior approach to industrial IoT service design has several additional benefits:

- the prototyping phase can also include one or more network technologies to evaluate which is best suited for the IoT service at the moment of the roll-out, for example because sensors and devices are already available on the market;

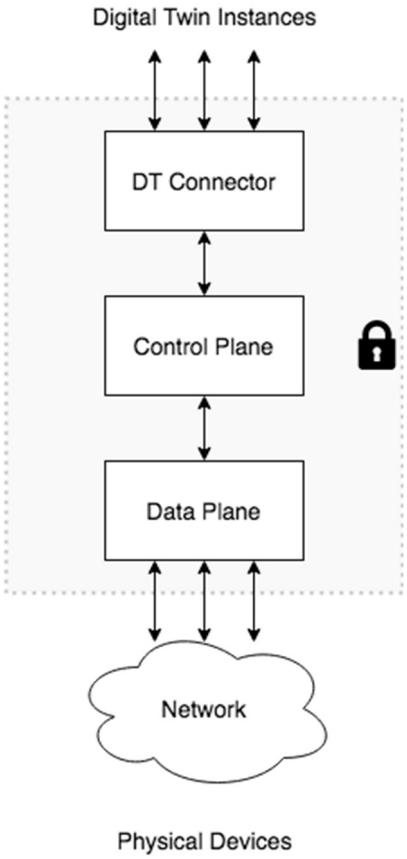
- it also makes rooms for future improvements without affecting the existing deployed solution, making the Altior approach to IoT service design effectively **future-proof.**

How it works

The Altior middleware implementation relies on the definition of Abstract Network Interfaces (ANI) to create the communication channels from digital twins and the outside world.

An Altior ANI can be seen as an extension of the Altior digital twin that models not just the network interface, but also the routing of data, to and from the physical devices, to their digital counterparts.

The ANI architecture is represented in the gray box area of the following diagram:



The Altior abstract network interface is effectively made of three major components:

- The ANI DT (Digital Twin) connector is a standard interface implemented by all the Altior digital twins; the DT connector applies a publish-subscribe pattern, such that any digital twin instance that needs a specific network connection can simply register itself to the ANI, providing the basic data routing information. A single digital twin instance can register to one or more ANI simultaneously, depending on the number of network interface types supported by the physical object.
  For example, if a device has two different network interfaces, such as for example Wi-Fi and LoRa, the digital twin instance will register itself on the two different ANIs: one for the Wi-Fi network and one for the LoRa network.

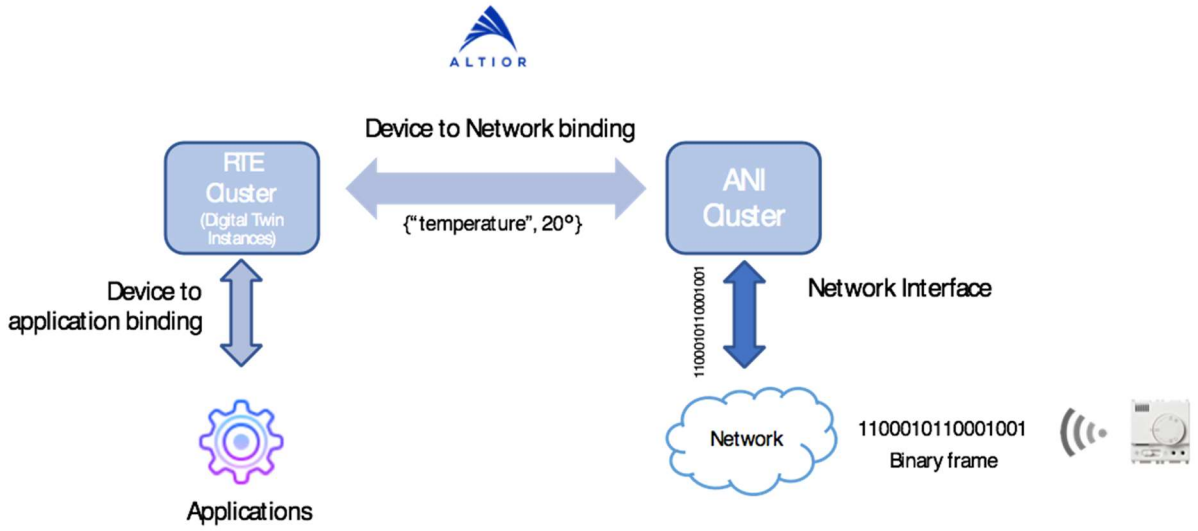
- The ANI's control plane contains all the logic to deal with the different network technologies; the control plane is responsible for setting up and maintaining the logical connections from the digital twins and the actual network.

This component manages the connection to the cellular network (for example by opening a specific service port) or with an LPWAN data concentrator or gateway (such as LoRa or wireless MBUS) and implements the low-level protocol to send and receive data from the network. The control plane creates the logical circuit from the data plane and the DT connector.

- The ANI data plane is the component that implements the actual interfacing of Altior with the chosen network technology, creating the virtual channel (data pipeline).
  The data plane role is to handle the data stream to and from the digital twin instance on the data transport network and that provides the basic integrity checks on the channel status.
  The data plane also maintains the separation of the virtual channels, so there is an instance of a virtual channel for every digital twin registered instance.

The ANI has also a few other functions, such as handling the chosen security model for a network adapter using Inkwell Data's "Aegis" security provider[3], or sending the logging data to the central logging facility.

But most notably, the ANI can be distributed and replicated in an Altior cluster to provide reliability (as the state of the network connections is replicated) and scalability with load balancing.



Physical objects (devices and sensors) implementing the open source Altior API for devices also have the capability to define a redundant network interface and service configuration which can be switched automatically in the case of a primary network failure.

By decoupling the data transport mechanism from the application logic with a middleware approach, Altior digital twins are effectively "network technology agnostic" since they do not rely on specific network features to carry out their job.

[3] The Aegis security framework will be described in part 4 of this series.

Conclusions

Altior network abstraction middleware is a proven way to future proof large scale IoT applications.

Combined with the device twin management system, Altior provides the IoT service designer with the freedom to focus on his/her business requirements rather than the technology details.

A user can start designing an industrial IoT service today with the currently available resources (devices and networks), focusing only on the required result, without being influenced or limited by the features of a specific technology, or worse, afraid of a vendor lock-in.

Altior allows the IoT applications to evolve to include new network technologies when available, without throwing away existing investments.

For more information and contact requests:

Inkwell Data Ltd.

Iveagh Court
Harcourt Road
Dublin 2 - Ireland
+44 (0)203 951 0831

[1]84, Shepherds Bush Road
W6 7NL London - UK
+44 (0)203 951 0831

Inkwell Data Italia

via degli Zabarella, 24
35121 Padova - Italy
+39 (0)49 689 8423

info@inkwelldata.com
https://inkwelldata.com

Cover photo by John Barkpile on unsplash.com