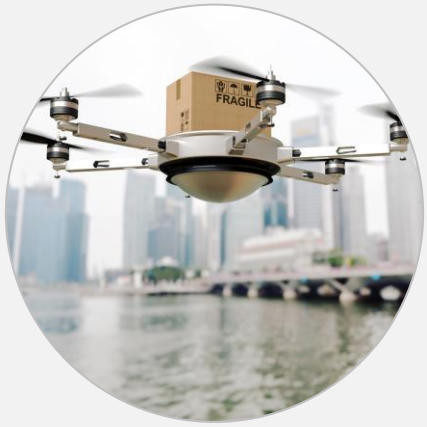
Out of the Fog:

Use Case Scenarios

Industry	Supply Chain
Application	High-Scale Drone Package Delivery



" 'Your order will be delivered in 23 minutes.' Drone fleets for package delivery sound like science fiction, but the drones are almost at our doorstep—literally. You can bet that there are business plans for drone mail or product delivery on boardroom tables of some of the biggest companies in the world. But it's fog computing that will make this futuristic transportation idea a safe and profitable commercial reality."

Charles Byers, IoT Systems Architect
Cisco Corporate Strategic Innovation Group

Executive Summary

Challenges

- Volume and expense of traditional package delivery
- Safety, bandwidth, and operational challenges associated with large-scale commercial drone operations
- Regulatory complexities, especially for autonomous or non line-of-sight operations

Solution

- Fog computing controllers on the ground communicate with fog nodes on drones to coordinate the complex, split-second coordination of landings, takeoffs, loading, unloading and maintenance
- Fog computing nodes located on the drone to support autonomous awareness, analysis and sub-millisecond response to changing conditions in the air
- Fog computing nodes on the drone provide a full complement of security measures, from downloading and installing patches to perimeter defense

Technology

- Eight pillar fog computing architectural approach for commercial drone deployments

Supply Chain Management in the Era of IoT

Every day, workers pick up and deliver billions of packages and pieces of mail. The logistics and infrastructure investments associated with these deliveries are staggering. The cost of the resulting congestion in roadways, sea lanes and airspace, as well as the impact on the environment, is incalculable. On top of this, transportation companies have to deal with rising costs in labor, maintenance, facilities and insurance — all of which affect the price of goods.

Internet of Things (IoT) technology is streamlining aspects of fleet management with innovations in areas like proactive vehicle maintenance, in-transit visibility and traffic management for route optimization. The biggest impact, however, will be up—literally. Coming soon to the skies near you will be drone fleets delivering mail and packages—even data.

The concept of using drones—also known as flying robots and unmanned aerial vehicles (UAVs)—is gaining a lot of attention. Drone fleets can reduce costs, congestion and environmental impact to a degree that no one would have imagined possible.

Drone delivery can also create new markets that simply aren't practical with traditional vehicle fleets. For example, using drones can:

- Extend the reach of delivery to inaccessible places
- Greatly reduce customer wait time between order and delivery
- Enable last mile delivery of large digital files, from video to big data

Drones are also emerging in other commercial applications, such as monitoring traffic conditions, reporting public safety incidents, locating missing persons, conducting inspections on infrastructure, etc. This use case concentrates on the use of drones in supply chain delivery.

Challenges to Drone-filled Skies

For high-scale drone delivery to become a reality, the following problems must be solved:

Collisions (Safety)

Shared airspace is the only way to arrive at high-scale drone delivery services. When there are only a few thousand drones in the air, there may not be much concern about collisions. When there are millions, however, there will be a very real threat of drones crashing into each other (as well as birds, airplanes and tall structures). Unmanned vehicles will need a way to recognize imminent collisions and make course alterations in sub-milliseconds.

Bandwidth Bottlenecks and Expense

Constant communication and tracking is required whenever a drone is being prepared for a delivery or is in transit. This translates to a constant stream of data for every drone flight. Access to the cloud may require expensive satellite links in remote areas, making some commercial applications cost-prohibitive.

Drone Hub Management

As drone delivery takes off, it will become impractical for every vendor to have an independent fleet that operates independently of every other fleet on the planet. In order to scale drone use, the industry will need to develop drone hubs that can coordinate the flights of many companies, much like airports do. Managing these hubs with advanced technologies is critical in order to coordinate drone activities with traffic and operations on the ground and in the air.

Regulatory Complexities

Drones will need to operate in a complex regulatory environment. The U.S. Federal Aviation Administration (and their counterparts worldwide) have regulated the operation of drones. Some of these regulations limit drone flights to within line-of-sight of the operator and prohibit operation in many flight areas and conditions. Future rulemaking will weigh in on opening up operations beyond vision line-of-sight when enabled and secured through advanced technologies.

Solution with Fog Computing

Split-second coordination on the ground

Imagine the busiest airport on the busiest travel day of the year. Long lines of airplanes are queued up for takeoff and planes are coming in on the runways, taxiing to gates.

Now imagine a commercial drone hub operating on the same model—and the same or greater volume of air traffic on a daily basis.

Instead of gates, there are multi-drone docking pads. Parcels are loaded and unloaded by highly automated equipment. The drones are checked and maintained before and after every flight. All drones must have flight plans, so takeoff and landing can be scheduled to prevent collisions.

Consider the split-second timing required to coordinate the loading, takeoff, landing and maintenance of this volume of drones.

A drone could be traveling at 100 miles per hour on final approach—or 147 feet per second. During descent, a real-time loop cycle of hundreds of updates per second would be required between the drone and the "control tower" on the ground.

Consider that the best cloud round trip latency is around 80 milliseconds. During that time, the drone flies about 12 feet between cloud messages. Delays introduced by routing all of that information through the cloud can make it impossible to achieve near-time response.

This is where fog computing solves the many problems of how to provide the communications, storage and computation with the speed necessary to safely control high-volume drone traffic. Fog computing provides for a more efficient way to upload continuous software updates, massive amounts of data and other computational and communication requirements.

Fog controllers on the ground provide the proximity required to shorten the communications loop between the drone and the "control tower." Latency can be reduced to such a degree that a drone will only travel two inches before the next update is delivered. If that same communications were to go through the cloud, the drone will have traveled 12 feet.

A subset of this on-the-ground information can also be routed to the cloud for analytics. Complete logs of the communication can be sent to the cloud for long-term archiving.

Split-second safety in the air

When picturing commercial drone services, you may conjure up an image of drone-filled skies. But this is not likely to be the case. The amount of drones in the air at any time will be regulated for safety, just like passenger and cargo transport is regulated today.

But there is a different dimension to drone safety in the air. Drones are unmanned. So there is no pilot, co-pilot and navigator on board reviewing and adjusting for prevailing weather conditions or other aircraft in the area.

Because drones are unmanned, they require sufficient on-board intelligence to act with autonomy when needed. First, this requires fog nodes on the drone that can provide awareness of anything within close proximity to the drone—including weather conditions, other drones, birds or buildings.

Fog computing also covers autonomous response: the ability to take the appropriate automated corrective action sequence.

The time involved from sensing a problem to analyzing it to responding to it is mere sub-milliseconds. Trying to make this loop through the cloud would take far too long. By the time the drone reports the problem, the time to act will have passed.

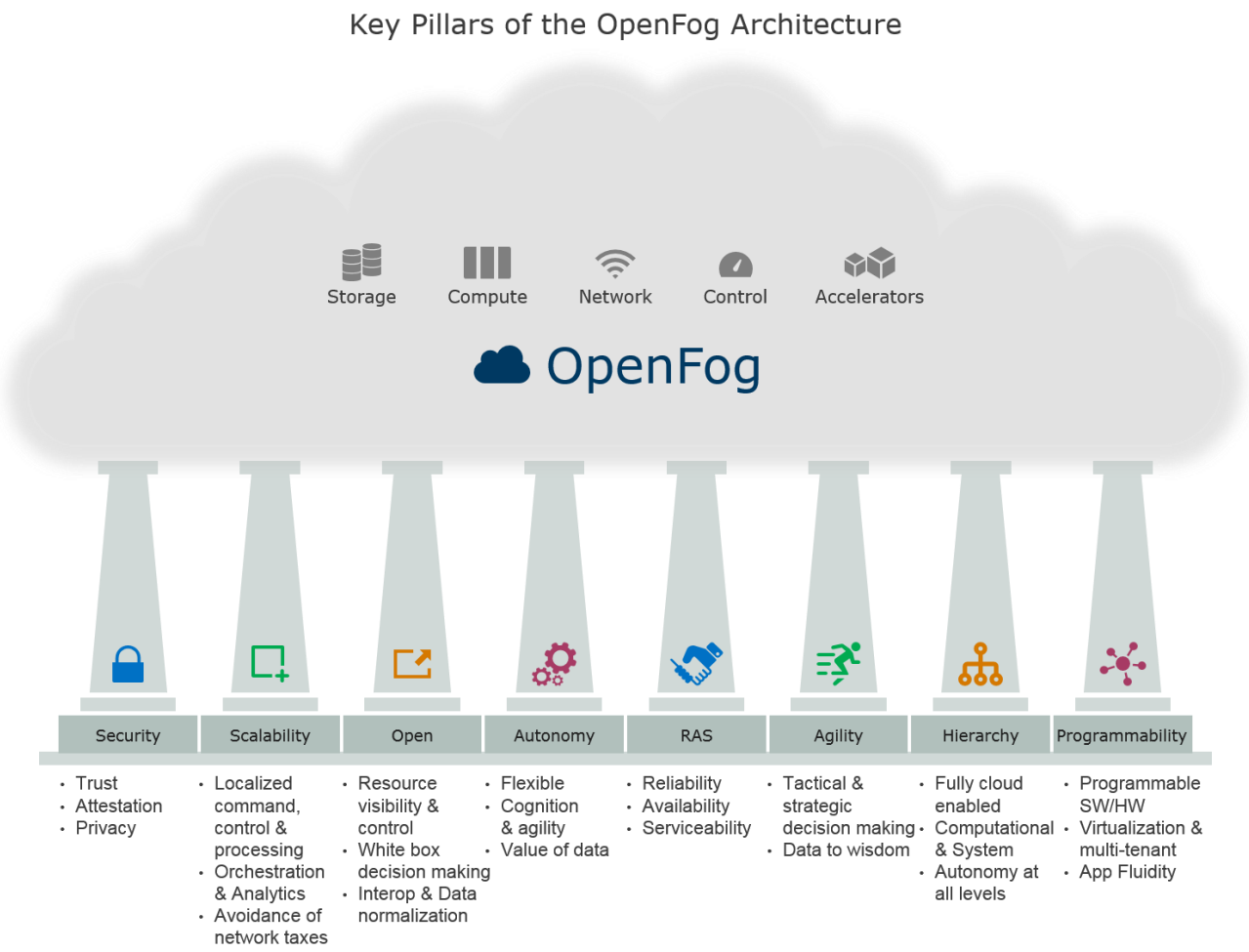
Autonomy in the air also means that the drone can run through self-check procedures to ensure that all systems are operating properly. And, in the event it detects a problem, the fog computing node on the drone can take the appropriate action to correct, or compensate for, the problem—or even return to the hub for maintenance.

Security on the ground and in the air

Security is an important concern with drones. Imagine hackers targeting and rerouting drones carrying medical supplies, drugs, and even data. Adding security features such as encryption and anti-cloning chips on multiple sensors, will increase the cost of the drone. Downloading security credentials, patches and updates from the cloud to the drone can consume valuable bandwidth. Both of these approaches may result in making security compromises.

Instead, a fog node on the drone can handle security, without adding complexity, size or cost to any other drone parts. The fog node can take care of security updates even in mid-flight. And it can provide perimeter defenses against hackers.

An Architectural View of Commercial Drone Deployments



[The 8 pillars of an open fog computing architecture. Source: OpenFog Consortium]

The OpenFog Consortium has identified eight pillars of fog computing architecture. In high-scale drone deployments, each pillar plays a critical role:

- **Hierarchy** – A single flat layer of ground support computers for high-scale drone networks doesn't match the computational problem. Fog networks need to support a hierarchy, with local, neighborhood, and regional levels to efficiently divide the computational tasks.
- **Open** – Having open standards will be critical to scale, as many different stakeholders will want to provide hardware and software for drone ground support systems.

- **Programmability** – Ground support networks add much of their value through software. The fog nodes providing the support must be highly programmable to allow for continuous software innovation.
- **Security** – Drone systems can be quite dangerous if hacked, and there are additional privacy concerns. Fog computing adds extra layers of security to make these systems safer.
- **Scalability** – Drone networks must have scalable performance and capacity. From a performance perspective, it must be possible to build systems with millisecond level latency. As drone services grow, the fog infrastructure must scale its capacity as well.
- **Reliability/Availability/Serviceability (RAS)** – Drone support systems are often mission critical, with stringent availability requirements. This means the hardware and software must be highly reliable, and the support systems that configure and maintain them must be very efficient.
- **Autonomy** – Drones and their ground support networks will be called upon to make their own operational decisions, especially when other Internet resources are unavailable due to overload or failures
- **Agility** – Fog elements supporting high-scale drone operations must adapt in the face of rapidly-changing requirements and applications

What is Fog Computing?

Fog computing is a system-level horizontal architecture that distributes resources and services of computing, storage, control and networking anywhere along the continuum from Cloud to Things.

- **Horizontal architecture:** Supports multiple industry verticals and application domains, delivering intelligence and services to users and business.
- **Cloud-to-Thing continuum of services:** Enables services and applications to be distributed closer to things, and anywhere along the continuum between Cloud and Things.
- **System-level:** Extends from the Things, over the network edges, through the Cloud, and across multiple protocol layers – not just radio systems, not just a specific protocol layer—not just at one part of an end-to-end system, but a system spanning between the Things and the Cloud.

The OpenFog Consortium

High-scale drone delivery services is just one of many industry use cases whose commercial viability will depend on fog computing to achieve the rapid response, bandwidth and communication necessary in advanced digital applications.

The OpenFog Consortium is helping to enable game-changing innovation enabled by fog computing through an open architectural framework. ARM, Cisco, Dell, Intel, Microsoft and Princeton University founded OpenFog in November 2015. Today, the consortium has members throughout North America, Europe and Asia. Learn more at www.OpenFogConsortium.org