# OVERVIEW

This white paper describes Flexeye's view of the Internet of Things (IoT), how you as a stakeholder will benefit from the Iot and why identity, visibility and intelligence are key.

## Part 1: The Amazing Potential Of The IoT

In "The Amazing Potential Of The IoT" we discuss the projected $1.9 trillion of global economic value the IoT will add to industry, we propose key factors for successful participation and examine the impact this will have on our ability to communicate and to share information.

## Part 2: How You Establish Control

In "How You Establish Control" we look at the issue of trust in the IoT and how to establish control of the real world and digital entities that are important to you.

## Part 3: Controlling Entities With Flexeye

In "Controlling Entities With Flexeye" we briefly describe Flexeye's product EyeHub, and how it enables stakeholders maximise their quality, performance, compliance and security in a world of connected entities.

Whether you are a large or a small stakeholder, whatever your interest or geography, Flexeye can help you unlock the enormous potential of the Internet of Things.




# PART 1: THE AMAZING POTENTIAL OF THE IoT

We discuss the projected value the IoT will add to industry, propose key factors for successful participation and examine the impact this will have on how we communicate.

The concept of the **Internet of Things (IoT)** has been discussed since at least 1991, originally conceived as providing all objects in the world with a machine-readable identifier that could be used for tagging. Today the term is used to denote a world where real entities are identifiable and connected to digital networks in a variety of ways – enabling them to be treated as first-class digital objects and to participate in a new range of systems and services.

The Oxford English Dictionary added a definition for "Internet of Things" in September 2013:

**"A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data."**

So the big change is to connect all the things that have not been put online before. That means everything from toys to towns, houses to skyscrapers, shoes to shoe factories, cars to cows and packing crates to pack animals. The way you put an everyday object on the IoT is by first creating a **digital entity** to represent the real entity, which provides three important capabilities:

**Identity** – a way to define itself and capture its real world context in the digital world.

**Visibility** – a way to be digitally discovered and accessed by stakeholders, incl. other entities.

**Intelligence** – a way to become smart via digital processing, including the power to make decisions and take actions.

Next you need to connect the real entity to its digital entity counterpart using a mixture of devices:

**Sensors** – to provide analog-to-digital translation of data from the real world.

**Actuators**– to provide digital-to-analog translation of instructions to the real world.

**Gateways**– to connect the sensors and actuators to digital networks.

These devices provide the foundation and scaffolding for building the IoT and are entities in their own right.

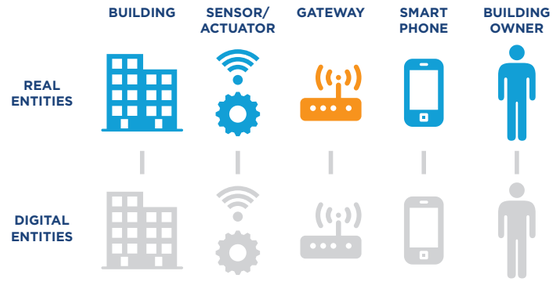


**Figure 1:** Real entities and their digital entity counterparts

## Example:

Jane works for ACME Properties, which owns 100 Central Place – a large office building in downtown Alpha City. To connect the building to the IoT, Jane first creates a digital entity for the building, then one for herself as a building owner. Next she connects the physical building via a mix of sensors & actuators to the digital network, e.g. via the legacy building management system or by installing new equipment.

Finally Jane creates digital entities for the other people who have a stake in 100 Central Place – e.g. her management team, tenants, merchants, building security and maintenance, contractors, etc.

## Humans vs. Machines

In his article "The Internet of Things and Humans", Tim O'Reilly describes "halfway houses" where IoT "applications in waiting" use humans to play roles that will eventually be played by machines. But a human with a smart-phone is **extremely capable** in the role of sensor/actuator, adding two more useful entities to the IoT and giving us a way to realise the IoT **right now**.

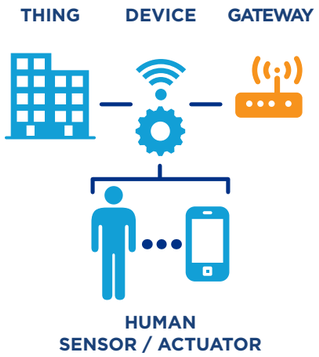


**Figure 2:** Human as sensor/actuator

Even more importantly, the combination of human + smart-phone is a practical solution to two of the thorniest problems with autonomous devices: how to provide reliable power and connectivity. People keep their phone batteries charged and their connection plans topped up, with **several billion** device-carrying people ready to play the sensor/actuator role, either in perpetuity or at least until we get our machine act together.




## Connect, Communicate & Share

Digital entities are concrete software objects hosted by a software service, which we refer to as a **Hub.**

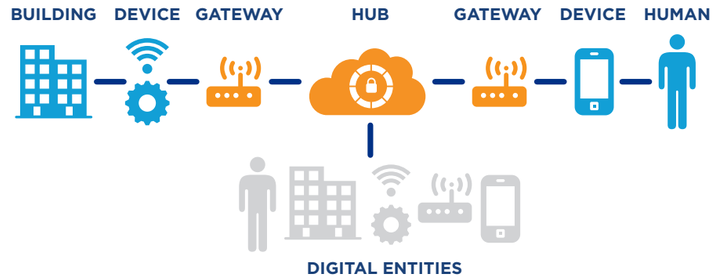


**Figure 3:** Hub as digital entity hosting service

The Hub provides storage, processing and connectivity for digital entities, running locally or remotely – in the cloud. This enables digital entities to define and execute behavioral **rules** for e.g. performance, quality, compliance and security, and to store **data** for e.g. attributes, relationships, events and logs.

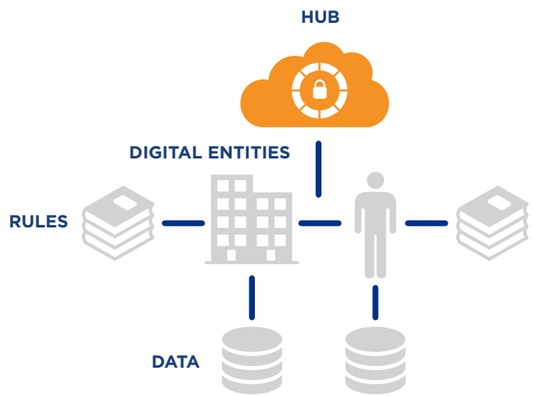


**Figure 4:** Digital entity rules and data

There will not be one **uber-Hub** - instead there will be lots and lots of Hubs of various sizes and flavours, connected together using two common patterns:

**Stacks** – where one Hub looks like an edge device to another Hub.

**Chains** – where one Hub looks like a peer service to another Hub.

## Smart Things Are Valuable Things

A connected digital entity enables stakeholders in the real entity to realise new value in the form of **efficiencies**, because a smart entity can perform tasks faster & cheaper than before, and **opportunities**, because a smart entity can interact with the world in new ways.

Tim O'Reilly's article "The Internet Of Things And Humans" also says that the IoT will make designers answer the question:

**"How does a smart thing make it possible to change the entire experience and workflow of a job we do in the real world?"**

### Example (continued):

Marco runs Reliable Repairs, a facility management company in Alpha City. He has a maintenance team operating a fleet of tool-equipped vans, which are all on the IoT. Louis, an HVAC expert for Reliable Repairs, is driving Maintenance Van #5 to 100 Central Place to carry out scheduled AC work for ACME Properties.

The digital entities for Van #5 and 100 Central Place are in communication – exchanging useful data, performing required security and compliance checks, and providing real-time guidance on routing and destination procedures. The digital entity for the Van relays information to Marco, prepping him for arrival on site. The digital entity for the Building does the same for the on-site staff at 100 Central Place.

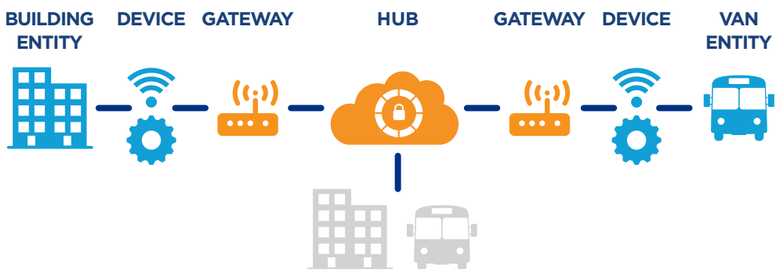


**Figure 5:** Smart building-vehicle communication

From the point of view of Marco and the ACME Properties staff, both the Vehicle and the Building have become **smart**, reducing the overhead of tracking, scheduling and delivering building maintenance and ensuring that Marco can get his job done efficiently, accurately and in compliance with the regulations and policies of both companies. Their digital entities also create an audit trail, compute any required statistics and update all the registered stakeholders on the initiation, progress and completion of the work by Marco at 100 Central Place.




## The Future Value Of The IoT

As digital entities accumulate more and more data about their interactions with the real world, they **become a new source for rich analytical information**. This drives up the variety and amount of intelligence we can inject into them and the amount of value we can derive from them, creating a virtuous cycle.

The explosion of connected entities between now and 2020 will create huge financial opportunities. Gartner estimates that the resulting global economic value add to industry as a result of increasing sales and decreasing inputs and costs will be **$1.9 trillion,** split across a variety of industry sectors: manufacturing (15%), healthcare (15%), insurance (11%), banking & securities (11%), retail & wholesale (8%), computing services (8%), government (8%), transportation (6%), utilities (5%), real estate (4%) and other (4%).

By 2020 Gartner estimate over $300 billion incremental revenue for IoT suppliers with c.$250 billion derived from services. This includes key service elements such as configuration & customization of IoT solutions, integration and data analytics.

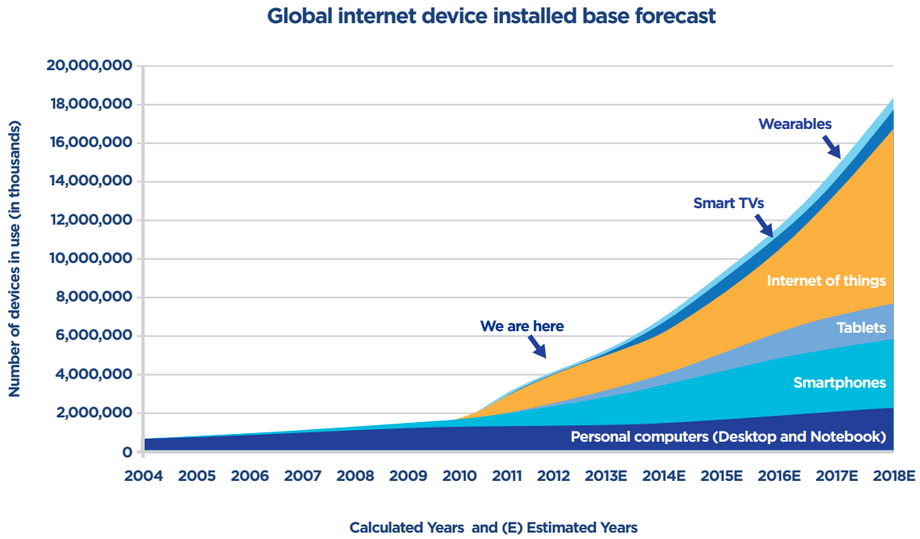


**Figure 6:** Projected growth of connected entities (Source: BII)

By 2020 the IoT will include an estimated 26 billion installed units. Others estimate that anywhere from 30 billion to 50 billion devices will be connected by then. Some analysts say even these estimates may be conservative.

## Smart Components

By connecting our real entities to the IoT we perform a kind of alchemy – where an entity that was previously dumb becomes smart by retrofitting it with IoT technology and providing it with digital processing capabilities. As these digital entities create ever-richer models of the real world, they can adopt a variety of roles based on their ability to monitor, measure, enforce and communicate.

For example, we can take advantage of the processing power and capacity of Hubs to not only represent Marco's vehicle or Jane's building, but also all of their sub-components as digital entities.

These **smart components** will be policy-driven – monitoring their usage, scheduling preventive maintenance and providing access to supporting information, e.g. for use by a third-party mechanic to perform diagnostic checks or carry out repairs.

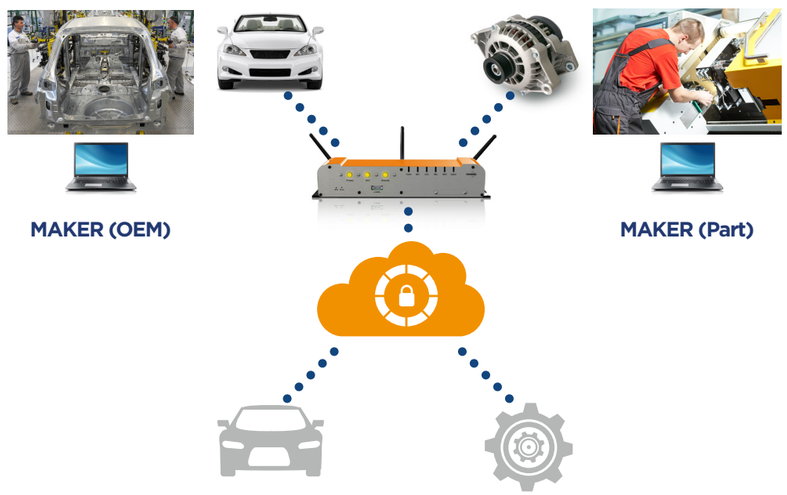


**Figure 7:** Smart vehicle components

At the same time the vehicle and component manufacturers can get access to rich information spanning across multiple vehicles in the field, which can be used to provide higher quality service and products to existing and future customers.

## Multiple Stakeholders

In the example above, the IoT enables new forms of communication between **all the stakeholders** in the vehicle – a list which includes not only the vehicle owner, drivers and passengers, but also the OEM, part manufacturers, dealers, service technicians and mechanics. Each of these stakeholders can **independently** maintain their own digital entity to represent the real vehicle.

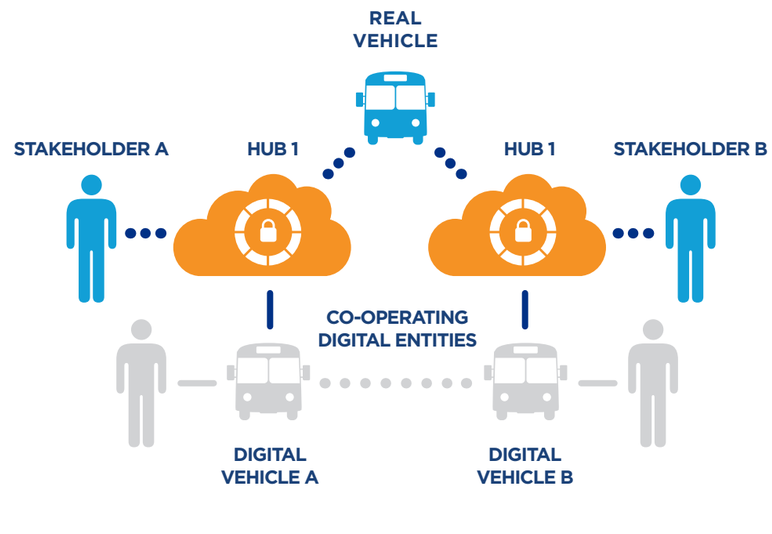


**Figure 8:** Real entity with multiple stakeholders

For example, take the case where Stakeholder A is the vehicle's owner and Stakeholder B the vehicle's OEM. The owner's digital entity will know about things like current vehicle location, fuel level, tire wear, insurance, tax and road-test, governed by rules that capture the owner's agenda, whereas the OEM's digital entity will know about the vehicle design, manufacturing history, dealership interactions and warranty, governed by rules that capture the OEM's agenda.

The IoT enables each stakeholder to pursue their own agenda, but also to come together via their **common interest** in and **common representation** of the vehicle, to find new ways to perform everyday tasks such as preventive maintenance, part replacement, fault diagnosis, personnel training and awareness.

# PART 2: HOW YOU ESTABLISH CONTROL

We look at the issue of trust in the IoT and how to establish control of the real world and digital entities that are important to you.

## Confidence In The IoT

While the tangible benefits predicted for the IoT are huge, there are several hurdles that need to be overcome before we can unlock its full potential. The most important of these is the **trust problem**, which stems from two sources:

1. The IoT has all the same security problems we have with information on the current Internet, except on a vastly **increased scale.**
2. The IoT introduces another security problem: a direct two-way connection from the digital world into the real world, which could be used to **abuse real entities.**

A participant in the IoT will have a stake in two sets of entities: their own entities and the entities of others. That means all stakeholders in the IoT simultaneously play two roles: the role of producer – creating & connecting their entities and updating them – and the role of consumer – connecting to and interacting with other entities.

To overcome the trust problem, a stakeholder must be able to confidently answer "Yes" to the following questions:

**Will my entities be represented and connected correctly and reliably?**

**Will the rules I set for my entities be respected, i.e. correctly enforced or executed?**

**Will the data for my entities be captured and stored completely & correctly?**

**Will my entities and their data be available when needed?**

**Will I be allowed to get access to other entities I want to use?**

**Will I be able to verify provenance of other entities and their data?**

**Will other entities be available when I need them?**

The owner of a real entity on the IoT must be able to control the visibility of their digital entity so it can be seen by other stakeholders and other digital entities securely - the visibility of the entity data and the visibility of the behavior the entity provides for accessing and controlling the real entity. We refer to this principle as **my-data-my-rules.**

The IoT is not just about data but about **communication** between entities, by and on behalf of their stakeholders. The interesting and most valuable part of the IoT is at the **intersection** of the agendas of these stakeholders. That is where communication, negotiation, opinion, transaction, observation and action come together and get resolved – to the mutual benefit of the interested parties.

## Solving The Trust Problem

The solution to the trust problem of the IoT has the following elements:

**Provisioning Things** – a way to connect new entities easily and securely or else building the IoT will take too long, be too expensive and be vulnerable.



**Capture Policies** – a way to easily capture and manage the rules that govern our entities or else maintaining the IoT will be too expensive, and we will not have control.

**Enforcing Policies** – a way to enforce our policies, esp. entitlements, compliance rules, quality measures and performance requirements or else the IoT will not be usable for our most important entities.

## Points Of Control

As with information and services on the Web, access to entities and their data must not be open to just anybody. We want each of our digital entities to implement a micro-perimeter that enforces the policies and rules that govern each type of entity.

With the support of Hubs a digital entity can **make control decisions** for all input and output to and from both the digital and the real entity, at each of the key control points on the IoT connection diagram.

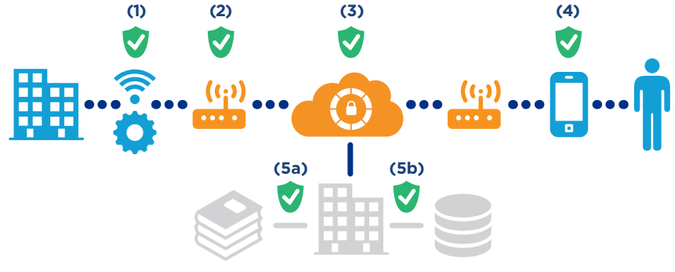


**Figure 9:** IoT entity access control points

The various control points in an IoT interaction where the entity perimeter can be checked include:

**(1) Sensor/Actuator Device** – physical security, certified installation & anti-tamper.

**(2) Gateway Device** – access to front-end & back-end connections.

**(3) Hub Service** – restricted inbound connection & service-scope permissions.

**(4) Client Application Device** – physical security & certified ownership.

**(5) Digital Entity** – read/write access to:

- **(5a) Rules** – behavioral policies, constraints & operations.
- **(5b) Data** – attributes, events, logs & analytics.

## Closed vs. Open vs. Hybrid Stacks

When we decide how to deploy a trusted IoT solution, there are three general approaches:

**Closed Stack** – single vendor solution, as a vertically integrated silo.

**Open Stack** – roll-your-own solution, using a mixture of components and protocols.

**Hybrid Stack** – consortium fronted by OEM, mixing best-of-breed components.

We favour the Hybrid approach, because the OEM can provide a single contract for management and support and guarantees the trustworthiness of the final solution, while using multiple suppliers to get the widest choice of hardware and software components.

# PART 3: CONTROLLING ENTITIES WITH FLEXEYE

We briefly describe Flexeye's product EyeHub, and how it enables stakeholders to maximise their quality, performance, compliance and security in a world of connected entities.

**".. [Flexeye] provides an entire IoT architecture that offers a fully provisioned two way data stream that is secured, and fully authenticated to the application or use case that resides in the cloud."**

Bettina Tratz-Ryan, Gartner VP, Cool Vendors in the Internet of Things 2014

The EyeHub product is a software platform for rapidly delivering trusted IoT solutions then evolving them to meet your changing IoT needs.

There are many benefits to using EyeHub for building and deploying IoT solutions:

**Represent Your Entities** – provides rich IoT digital entities out of the box, which can be extended to fit your custom requirements;

**Analyse Your Data** – provides rich, customisable analytics, future & historical timelines, with multiple publishing options, incl. catalogs (Hyper/CAT) and interactive screens for mobile and browser;

**Enforce Your Policies** – captures your policies, in the form of prescriptions bound to your digital entities; policies define rules to be executed by a decision service.

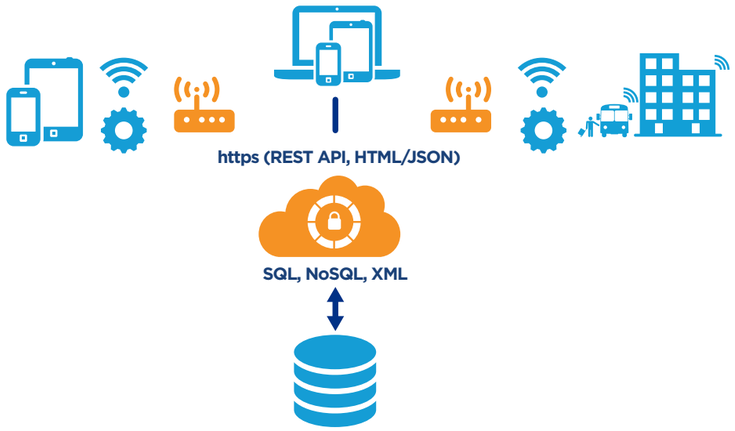


**Figure 10:** EyeHub - secure, configurable IoT Hub




## Represent Your Entities

EyeHub provides a rich set of IoT digital entities out of the box, which can be updated to fit your custom requirements. The digital entities are defined in meta-data and are runtime configurable so they can be extended and expanded to meet your changing needs.

EyeHub creates digital entities for your key real-world operating entities, their supporting entities and their key relationships, including:

**Identity** – in the digital world and the real world.

**Type** – of an entity, it's class or category.

**Ownership** – by a person or organisation.

**Representation** – by a connected sensor/actuator device.

**Delegation** – of rights to another entity.

**Equivalence** – to another entity with a different owner.

**Containment** – by another entity.

**Location** – position in physical space.

**Temporality** – position in the timeline.

## Analyse Your Data

EyeHub provides rich, customisable analytics, including computation across both future & historical timelines, which enables predictive and prescriptive analytical models to be implemented. The service provides multiple publishing options, incl. export to catalogs (e.g. Hyper/CAT), machine access via RESTful JSON API and human access via interactive screens for mobile and browser, or PDF output for offline reporting.

As with the IoT entity model, the analytics and the user experience are defined in meta-data and are runtime configurable, so they can be easily extended to fit your needs.

## Enforce Your Policies

EyeHub defines your behavioral policies, captured in the form of prescriptions, which are bound to your digital entities. The policies define machine-executable rules which can be used to e.g. control access, verify compliance, check quality and monitor performance.

EyeHub implements a policy-driven operating lifecycle for all IoT entities, using the external interface of the Hub to implement preventive and checking controls in the real world.

The stages of the operating lifecycle are:

**Procure / Discover** – Reuse, buy, lease, create or dispose of needed entity.

**Assess** – Identify and assess current opportunities & risks for the entity.

**Treat** – Identify and implement appropriate controls.

**Enforce / Audit** – Prevent or check for non-compliance with respect to required controls.

**Analyse** – Examine compliance & audit output.

**Advise** – Make recommendations for fixes, changes or improvements to the entity.

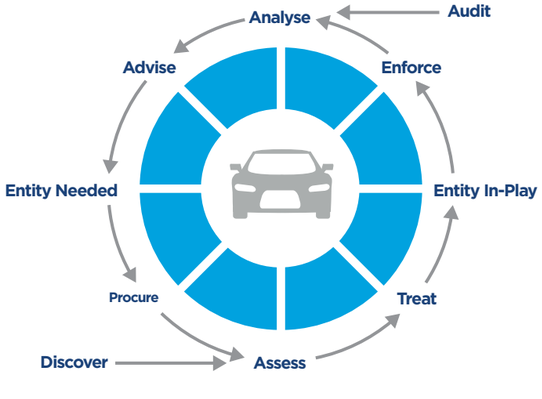


**Figure 11:** EyeHub IoT operating entity lifecycle

One key preventive control is **authorising access** to the digital entity itself, it's associated data & behavior and to the sensor/actuators connected to the real entity:

- Controls flow of data from sensors to the digital entity.
- Controls commands sent to actuators from the digital entity.

## Operating Modes

The EyeHub product supports three different operating modes:

**Enterprise Application** – full end-to-end IoT solution, including analytical processing and user experience for mobile and browser (embeds **Secure Hub** functionality).

**Secure Hub** – hosted IoT web service w/RESTful JSON web API to support custom clients (embeds Decision Service functionality).

**Decision Service** – policy decision component for automated IoT intelligence.




## About Flexeye

Flexeye partners with industry leaders to build smart & secure IoT applications that: optimize performance, quality & compliance; and reduce risks.

Flexeye has headquarters in the UK and offices in the USA and India. It has been recognised by Gartner as a Cool Vendor 2014 for the Internet Of Things and Cool Vendor Asia Pacific. It has been identified by Gartner as 'One to Watch' in their report: Market Trends: Digital Business Opportunities in Smart Cities Need IoT Foundations (July 2104). It has achieved techUK's Business Professional Certificate.

Flexeye is the leader of the Hyper/CAT consortium, a group of companies driving secure & interoperable Internet of Things for Industry building on a specification for interoperability funded by the UK's Technology Strategy Board and agreed by 50 leading IoT companies.

Whether you are a large or a small stakeholder, whatever your interest or geography, whichever industry you operate within, Flexeye's EyeHub product enables you to connect and manage your most important IoT entities with confidence.

## Your Feedback

We welcome your comments on the opinions and ideas expressed in this white paper. Please send us an email with the subject "LordsOfTheThings" to **ad@flexeye.com**