
**Office:** 010 597 0835 | **Facilitator:** 083 821 8801 | **E-mail:** anna@compliancelearningcenter.net
**Website:** www.compliancelearningcenter.net |
**Address:** 10A Lever Street Brackenhurst Alberton, South Africa
**Registration nr:** 2018/242685/07 | **Vat nr:** 4070281904

# Study Guide

**THE INTERNET OF THINGS AND INSURANCE: ONLINE CPD COURSE 2020 / 2021**



*February 2020*

## Course summary

The Internet of thing and insurance course is a short course providing an explanation of the internet of things and how it is impacting on insurance.

## Time allotted for course

The course consists of 2 topics with an assessment that needs to be completed. The time allotted for each aspect is as follows:

| Topic number | Title | Word count | Level | Time allotted |
|---|---|---|---|---|
| Topic 1 | The internet of things defined | 763 | Entry level | 5 minutes |
| Topic 2 | Why the internet of things matters in insurance | 1 852 | Entry level | 15 minutes |
| | Assessment | | | 15 minutes |

| | |
|---|---|
| **Total time** | **0.5 hours** |

## Assessment and certification

After completion of the workshop the learner must complete an electronic assessment on the learning management system.

- **Form of assessment:** Multiple Choice Questions
- **Number of questions**: 5 questions
- **Duration:** 15 minutes
- **Competency mark:** 60%

Upon obtaining a competency mark of 60% the learning will receive a certificate of completion. The learner will be afforded an opportunity to re-do the workshop should a competency mark not be attained.

## Course accreditation

**CPD Category:** Online programme

**COB Category:** Short-term Insurance: Commercial Lines

**Financial Planning Component:** Risk Management

**Advice Component:** Insurance

**Accreditation valid until:** 31 January 2021

**CPD Points allocated:** 0.5 points/hours on completion and pass of assessment

**FPI approval number:** FPI20030031

## Copyright notice



Anna Bouhail
10A Lever Street
Brackenhurst
Alberton
1449
South Africa

**Ordering information**
If you would like to order the publication, please contact author at address above.

## Table of contents

# Topic 1 THE INTERNET OF THINGS DEFINED

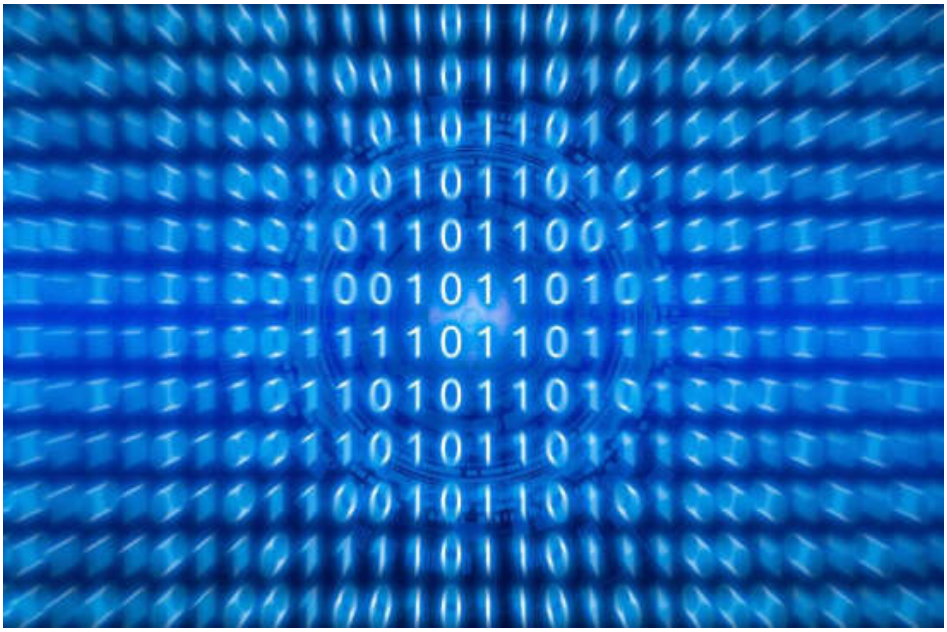
**LEARNING OUTCOMES**

After studying the topic, the learner should be able to-

- Define the internet of things.

## 1.1 Introduction to the internet of things

`The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UID) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.



A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and is able to transfer data over a network.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business.

## 1.2 The history of the Internet of Things

Kevin Ashton, co-founder of the Auto-ID Center at MIT, first mentioned the internet of things in a presentation he made to Procter & Gamble (P&G) in 1999. Wanting to bring radio frequency to the attention of P&G's senior management, Ashton called his presentation "Internet of Things" to incorporate the cool new trend of 1999: the internet. MIT professor Neil Gershenfeld's book, When Things Start to Think, also appearing in 1999, did not use the exact term but provided a clear vision of where IoT was headed.

IoT has evolved from the convergence of wireless technologies, microelectromechanical systems (MEMS), microservices and the internet. The convergence has helped tear down the silos between operational technology (OT) and information technology (IT), enabling unstructured machine-generated data to be analyzed for insights to drive improvements.

Although Ashton's was the first mention of the internet of things, the idea of connected devices has been around since the 1970s, under the monikers embedded internet and pervasive computing.

The first internet appliance, for example, was a Coke machine at Carnegie Mellon University in the early 1980s. Using the web, programmers could check the status of the machine and determine whether there would be a cold drink awaiting them, should they decide to make the trip to the machine.

IoT evolved from machine-to-machine (M2M) communication, i.e., machines connecting to each other via a network without human interaction. M2M refers to connecting a device to the cloud, managing it and collecting data.

Taking M2M to the next level, IoT is a sensor network of billions of smart devices that connect people, systems and other applications to collect and share data. As its foundation, M2M offers the connectivity that enables IoT.

The internet of things is also a natural extension of SCADA (supervisory control and data acquisition), a category of software application program for process control, the gathering of data in real time from remote locations to control equipment and conditions. SCADA systems include hardware and software components.

The hardware gathers and feeds data into a computer that has SCADA software installed, where it is then processed and presented it in a timely manner. The evolution of SCADA is such that late-generation SCADA systems developed into first-generation IoT systems.

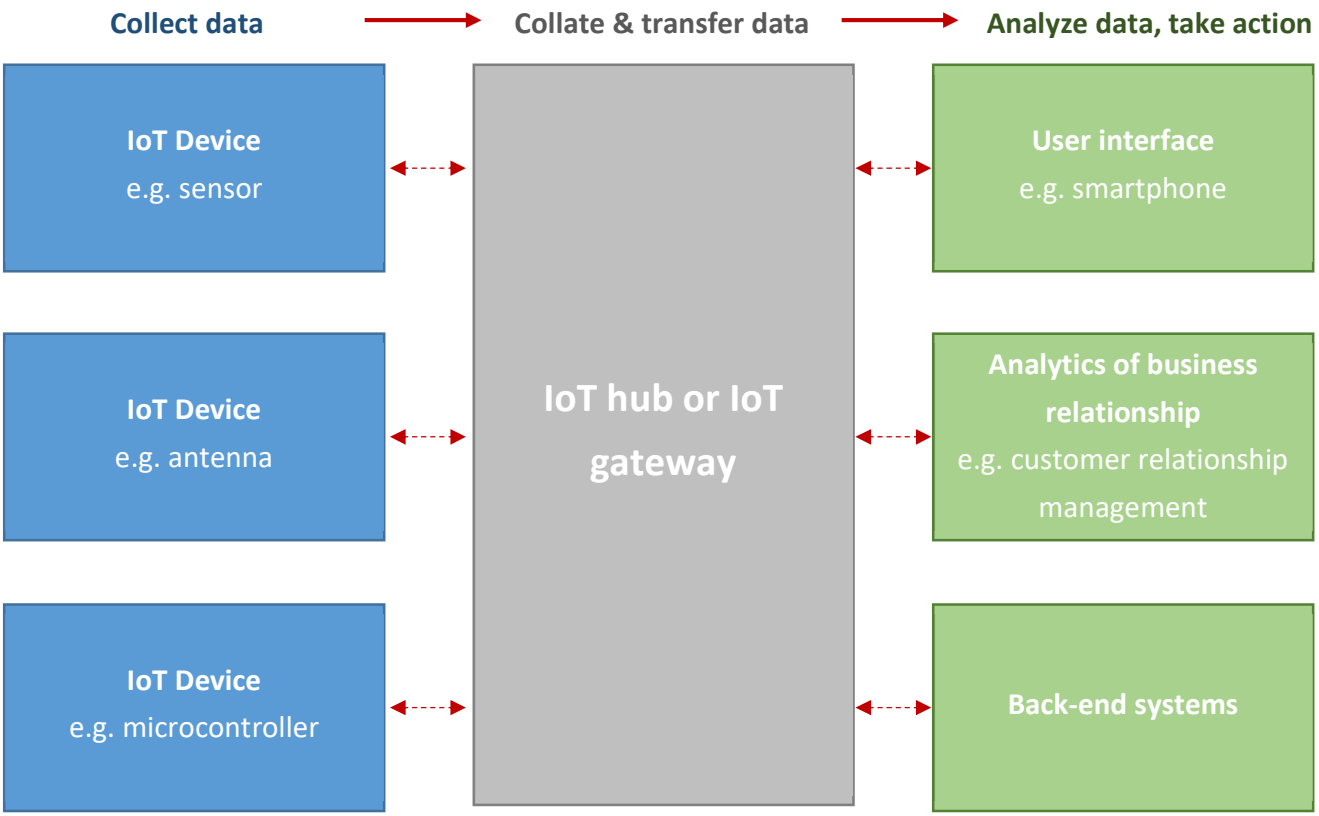
The concept of the IoT ecosystem, however, did not really come into its own until the middle of 2010 when, in part, the government of China said it would make IoT a strategic priority in its five-year plan.

## 1.3 How the internet of things works

An IoT ecosystem consists of web-enabled smart devices that use embedded processors, sensors and communication hardware to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for instance, to set them up, give them instructions or access the data.

The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed.

*Figure 1: Example of an Internet of Things System*



# Topic 2 WHY THE INTERNET OF THINGS MATTER IN INSURANCE

**LEARNING OUTCOMES**

After studying the topic, the learner should be able to-

- Describe how the Internet of Things has already and will likely impact insurance in the future.

## 2.1 Introduction

Until recently, the Internet of Things (IoT) was on the strategic agenda of only the largest and most progressive insurers. The IoT was largely viewed as a futuristic concept, and many insurers adopted a "wait and see" attitude. Such a posture is no longer viable.

Early adopters have established a clear and compelling value proposition by demonstrating how data from in-home and automotive sensors, wearable technology, drones, GPS, mobile and telematics devices, networked appliances and multiple other sources can help grow new business, improve risk assessment and proactively engage policyholders in loss prevention. The IoT offers truly disruptive and transformative potential to the insurance industry.

## 2.2 Data streams

For insurers, the most impactful data streams and sources from the IoT are likely to include the following:

- **Wearable or personal technology:** This is also sometimes called fit tech and often used in the context monitoring heart rate, steps walked and other health-related metrics. This technology is rapidly developing, with prototype patches already performing blood work and ECGs and automatically administering drug doses.
- **Sensors on objects:** This includes personal and commercial vehicles and shipping containers, that measure distances traveled, speeds and frequency and level of braking
- **Location-based sensors:** This is sensors in factories, warehouses or offices and in-home sensors, including smart thermostats, security technologies such as alarms and cameras and industrial control systems.

- **Other geographic information systems (GIS):** These systems provide geophysical, topographical, climatological and hydrological data, as well as information about utility grids and flight path. It may include drone and satellite imagery.

While this data is directly accessible by or streams to insurers via sensors or mobile devices, third-party organizations may also play a role in owning, aggregating, and distributing to insurers. All of these data types are potentially useful for the full range of products and lines of business, from commercial (which was an early adopter and has been an advanced user of such data for many years), to life, property and casualty and health insurance.

## 2.3 The impact

The IoT's impact within insurance is coming fully into focus. At the highest level, better use of IoT and sensor data means insurers have the opportunity to:

- Establish direct, unmediated customer relationships based on direct access to objective and unfiltered data.
- Gain more granular and precise understanding of who their customers are and how their needs change over time.
- Individualize offerings of products, features and access options.

For insurers that have relied on agents and brokers, the ability to directly access objective and unfiltered customer data represents enormous change.

Historically, much customer data was unavailable, and the information insurers could access was often subjective or inaccurate. Consider the common misrepresentation of data around certain behaviors (smoking, alcohol consumption, exercise regime, miles driven per week) on insurance applications.

The IoT greatly expands the universe of accessible data, opening up new possibilities in many functions.

Coupled with advanced analytics capabilities, new data streams and sources have set the foundation for entirely new business models. Usage-based insurance (UBI) — so-called pay-as-you-live or pay-as-you-drive business models — have quickly moved out of pilot phases and proved their viability and value around the world. In fact, there are an estimated 5 million active UBI policies in 35 different countries.

From this relatively low base, it is estimated that UBI policies will reach 15% market penetration by 2020 in Europe, Asia and the Americas.

## 2.4 Cross impact

The internet of things has a cross-enterprise and cross=industry impact on the financial sector. The subsection following consider these impacts.

**The view from underwriting**

The convergence of different data types leads directly to increased precision in assessing risk, pricing policies and estimating necessary reserves. T

here are clear advantages over current approaches, which rely on backward-looking claims data and historical risk studies. Through constant monitoring, underwriters can recommend real-time pricing and policy term modifications. The can also model the impact of new health and well-being services to manage mortality and morbidity risk over time.

**The view from the claims process**

The IoT is likely to drive further evolution in claims, as it orients more toward active loss prevention. For instance, in-home sensors can monitor for fire, wind and water damage. In-vehicle sensors can also be useful in providing warnings in case of dangerous driving patterns.

Within group health insurance, the discounts offered to employees who monitor their activity levels and heart rates could be considered a claims prevention program. Increasingly, within commercial lines, fitness monitors may feature in officer-and-director insurance.

There are also data-driven opportunities to enhance incident management and claims service, such as proactively offering towing or “loaner” vehicles in the event of an accident, rather than just covering these costs.

**The impact on commercial short-term insurance**

The IoT has already impacted the commercial short-term insurance industry in a big way and is continuing to advance.

In-vehicle sensors and tracking devices were first installed in trucking fleets decades ago and industrial control systems have long been standard within manufacturing environments.

Commercial insurers have also matured their modeling capabilities, especially relative to natural disasters.

These advancements paid off during the experience of Superstorm Sandy in 2012, where insurers carefully tracked the impact of the storm and proactively alerted policyholders of imminent risks.

Combining data — layering wearable technology data with GIS streams for example and contrasting real-time data against historical patterns — enables deeper understanding of risk, both in real time and across historical perspectives.

**The impact on long-term insurance**

Life insurers can now automate and streamline the traditionally intrusive and lengthy underwriting process, because sensor data provides the means to answer a lot of the questions from yesterday's paper-based application forms. This opens the door to a greater focus on millennials and younger customers, as well as on policies with lower face amounts.

Wearable technology allows for ongoing risk profiling, the promotion of healthier lifestyles and potentially pay-as-you-go models. There are even opportunities to automate retirement planning processes and offer simpler and more affordable products.

## 2.5 Challenges[1]

While most stakeholders might see attractive possibilities in the opportunity for behavior monitoring across the insurance ecosystem, inevitable hurdles stand in the way of wholesale adoption.

How insurers surmount each potential barrier is central to successful evolution. For instance, the industry's historically conservative approach to innovation may impede the speed and flexibility required for carriers to implement enhanced consumer strategies based on IoT technology.

Execution may require more nimble data management and data warehousing than currently in place, as engineers will need to design ways to quickly aggregate, analyze, and act upon disparate data streams. To achieve this speed, executives may need to spearhead adjustments to corporate culture grounded in more centralized location of data control.

Capabilities to discern which data are truly predictive versus just noise in the system are also critical. Therefore, along with standardized formats for IoT technology, insurers may see an increasing need for data scientists to mine, organize, and make sense of mountains of raw information.

Perhaps most importantly, insurers would need to overcome the privacy concerns that could hinder consumers' willingness to make available the data on which the IoT runs. Further, increased volume, velocity, and variety of data propagate a heightened need for appropriate security oversight and controls.

For insurers, efforts to capitalize on IoT technology may also require patience and long-term investments. Indeed, while bolstering market share, such efforts could put a short-term squeeze on revenues and profitability. To convince wary customers to opt in to monitoring programs, insurers may need to offer discounted pricing, at least at the start, on top of investments to finance infrastructure and staff supporting the new strategic initiative.

This has essentially been the entry strategy for auto carriers in the usage-based insurance market, with discounts provided to convince drivers to allow their performance behind the wheel to be monitored, whether by a device installed in their vehicles or an application on their mobile device.

Another challenge is that risk levels are reduced through smart automation, and therefore, the requirement for purchasing insurance may also decrease. This will have the effect of shrinking risk pools to levels where those seeking insurance find the pricing to be unaffordable.

For example, if embedding sensors in cars and homes to prevent hazardous incidents increasingly becomes the norm, and these sensors are perfected to the point where accidents are drastically reduced, this development may minimize or eliminate the need for personal auto and home liability coverage, given the lower frequency and severity of losses that result from such monitoring. Insurers need to stay ahead of this, perhaps even eventually shifting books of business from personal to product liability as claims evolve from human error to product failure.

## 2.6 In conclusion

As usage-based insurance (UBI) applications and pay-as-you-go business models have matured and entered the mainstream, it is become clear that the IoT is here to stay in insurance. Therefore, insurers must overcome the industry's traditional reluctance to change and commit to fully developed and risk informed strategies across all lines of business and within multiple operational areas. They must focus on capabilities that are not easily replicated and assume a bias toward action in putting sensor and IoT data to work.

Such strategies are necessary to use these new data streams to improve essential business practices and processes. More importantly, they are required to seize the fully transformative potential of the IoT and harvest the substantial value it represents for the insurance industry.

[1] Adapted from the Internet of Things in Insurance Deloitte University Press