IDEATION
CBM for all

IoT is the Best Place to Run the Condition Based Maintenance Strategies From

IoT is a network of physical devices, enabling these devices to communicate and exchange data, following the principles of the internet. IoT is not based on deterministic or syntactic models, but it relies on event-driven architecture. This makes IoT a perfect architecture for the implementation of any kind of condition-based maintenance strategy.

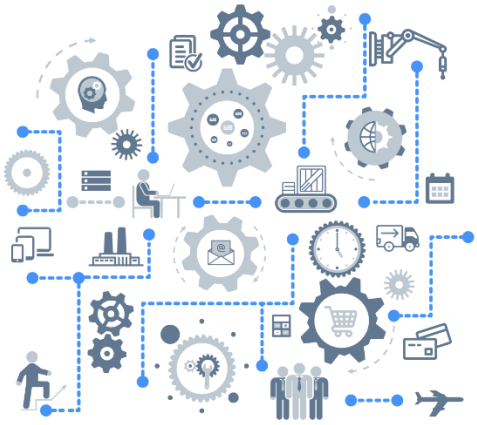

Fig 1. Depiction of the Internet of Things (IoT)

The foundation of IoT is based on the following facts:

- IoT field devices have the communications capabilities that are based on general IT standards of the day and do not require proprietary networks.
- IoT field devices have sensing, processing and storing capabilities, enabling them to analyse data and apply sophisticated logical algorithms. They do not have to communicate with controllers or control systems to get sophisticated algorithms and strategies applied.
- IoT is not a control system, but a communications and exchange network, therefore, there is no need to control anything, but just to route and communicate effectively actionable information.

If this is the case, why do some people still consider marshalling IoT devices through proprietary control networks and systems, rather than relying on general IT infrastructure?

The reasons are multiple, and the fundamental assumptions they make are just the legacy from the old-fashioned control systems networks. In general, they used to assume that:

- Field devices are "dumb" and they are designed to provide the maximum possible high-quality sensor data
- The "intelligence" is embedded in local controllers, or in the central control system (such as DCS or SCADA console)
- The system exists to control something, and we need sophisticated control strategies to meet this objective

However, these assumptions no longer hold and are inappropriate in the world of IoT.

Historically, as control systems advanced, their communications capabilities improved significantly, and they adopted and modified general IT networks principles. However, their purpose is to control and optimize processes, which means that they have to be highly secure. By "pushing" through a process network the IoT type of data, such as condition based maintenance information, we make these systems unnecessarily complex, we choke the system and deny access to people that need to have access to the IoT type of data, and lastly, we apply the wrong criteria to the data that had nothing to do with the control of processes.

In the world of IoT, the assumptions surrounding these new networks should be:

- Field devices are not dumb, but very powerful micro-processors with storage and communications capabilities. They do not need to (unless they are control devices) send masses of data, only actionable information.
- Intelligence no longer has to be distributed in controllers and central systems. The devices have enough power to do whatever is necessary.
- Unless you have a process control system, for maintenance and reliability purposes, there is no need to control anything. In accordance with the IoT principles of operation, we just need information to trigger actions.

This means that we neither want to use process control systems for information that are not related to process control and optimization, nor we want to build a new control system dedicated to maintenance and reliability. We should be quite content with the "confederate" approach of IoT architecture.

The nature of the Internet is confederate at its core. This is even more true for IoT, as a particular sub-version of the Internet applied to physical devices. This is the strength of IoT. The moment we try to control it or create control systems that supervise the traffic, we lose the versatility and the raison d'etre for IoT. This is where the control systems kind of thinking goes wrong.

To have an effective IoT, we just need smart field devices, enabled to communicate with other devices and/or applications on confederal networks. CBM Predictor is a prime example of this new generation of IoT devices. The only remaining piece of the puzzle we need to sort out is the communications part, where various routers and gateways come into the picture.

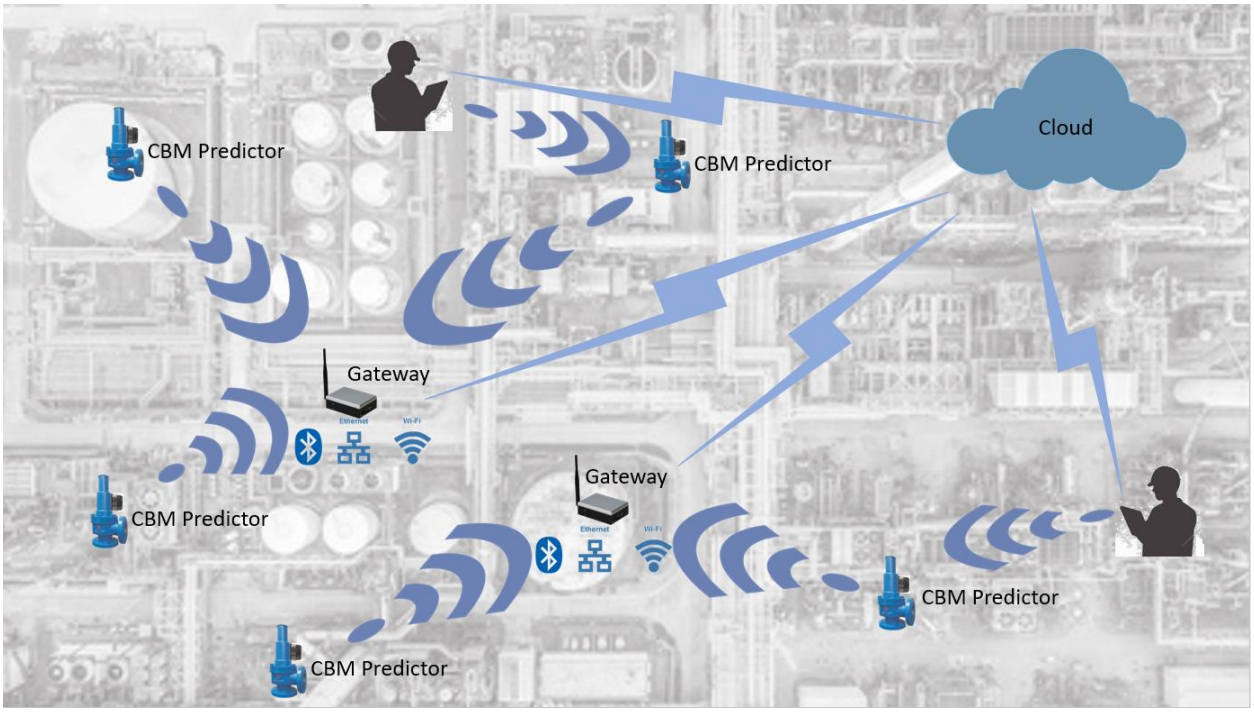

Fig 2. Architecture for deploying CBM Predictors in a IoT network

The solution advocated by Ideation AS by using CBM Predictor, is indigenous to IoT networks. There are no controllers and/or central control systems. All the necessary functionality is run inside every CBM Predictor and the only additional hardware are standard gateways. The gateways transpose the Bluetooth signal coming from CBM Predictors into a WiFi signal, which is then transmitted to a higher-level business and maintenance systems as either a WiFi signal or via the ethernet connections. If customers rely on operator driven maintenance walk-downs, then the gateways are not necessary as the operator hand-held tablet is used to communicate with the CBM Predictor.

CBM Predictor has been designed to be simple and easy to install. It requires no knowledge of the embedded algorithms, it communicates with the cloud via the Bluetooth / WIFI network, and it reports only actionable information when appropriate. It is designed to monitor Process Safety Valves (PSV) and notify customers of the popping action and potential leaks as a consequence of a failure to re-seat.

Ideation AS