Smart IIoT Devices

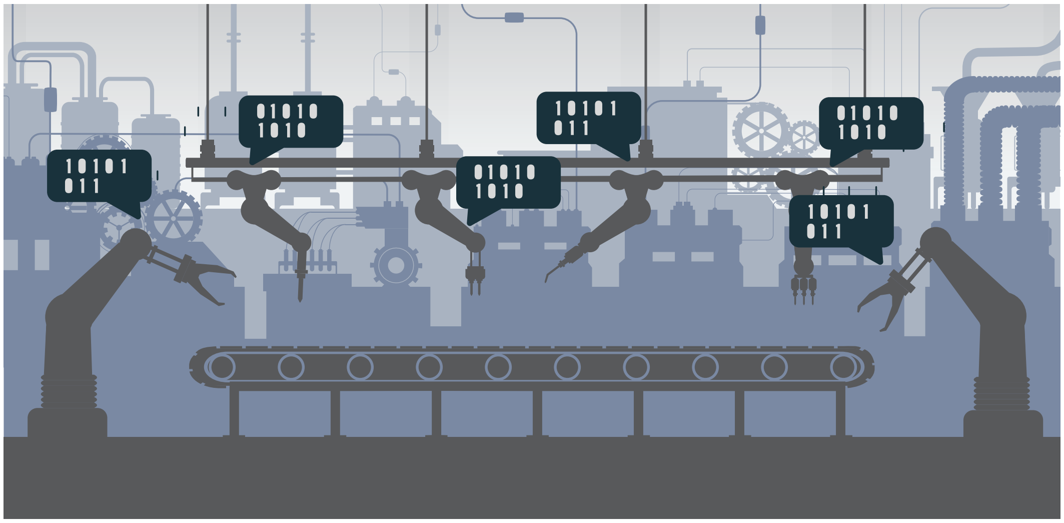
When planning a new manufacturing industrial internet of things (IIoT) deployment, the fundamental tenet of operation must be within the details of the smart (devices) design for the entire system. Without this basis, the full value of the implementation may be lost. Time and effort invested in the architecture step will pay dividends into the future for harvesting the vast amount of information needed to make informed decisions. The building blocks of the smart architecture can be identified as: sensing and data acquisition, communication, algorithms, cloud processing, analytics and security.

In order to properly architect a smart IIoT system for manufacturing, we must first start with the end in mind by answering two fundamental IIoT questions. First, what problem or response needs to be solved? Once we know that, the second question must be answered — What predictor information do we need in order to solve it? This will drive the design architecture from the top down. Once the problem and required data are understood, then the larger architecture can be designed down to the sensor. If the design is started in advance of answering these two fundamental questions, then the sensed data and subsequent processing may not satisfy the requirements. The problem and the required solution must be known.

SENSING

The value of sensing can often be overlooked and undervalued. Many IIoT architectural maps focus squarely on the cloud processing complexity with only superfluous circles at the exterior as the 'dumb sensors'. In this approach, the sensors provide little value other than to stream basic data back to a gateway and cloud, where the 'real computations' happen. This can be a possible solution if the expectation of the sensor is reduced to only low-quality data and not meaningful information. However, a cautionary tale may be appropriate here as garbage in equals garbage out. Consequently, dumb sensors may also provide 'dumb data'. The fidelity of the data cannot be improved later if it does not meet the requirements of the second fundamental question above.

When dumb sensors are not adequate, some intelligent processing at the sensor node or gateway may be required. A smart device will consider variations of a sensor's dynamic range, filters, trigger threshold points and conditional AND/OR events that relate multiple sensor data together. Static configurations may not be sufficient to process all the scenarios that are presented within the manufacturing environment. The sensor node settings may need to change based on dynamic external operational events (Taranovich S.). Any adaptation to the sensor information should be planned within the IIoT architecture design phase. The spatial placement of sensors, both in absolute terms throughout the operation and relative to other sensors must be ascertained in advance of deployment.



ALGORITHMS AND FILTERING

Although algorithms and data filtering could take place within the cloud, it often makes more sense to accomplish this activity earlier along the data ingestion pipeline within the gateway or sensor node if processing power is available (Grizhnevich A). For example, vibration sensing nodes located on machinery may change their filter response or decimation mode depending upon a change in activity on the machine. If the sampling rate of a temperature sensor is more frequent than needed, an averaging algorithm can be invoked to extend the dynamic range of the sensor at the expense of less frequent samples. These aspects of data requirements and sensor configurations should be well understood at the time of architecture design to embed any low-level algorithms at the sensor or gateway.

DATA COMMUNICATION

A smart device must include a communication plan for data to and from the sensor edge nodes, all the way to the cloud. Getting data from the edge sensor nodes and gateways into the cloud is paramount to the success of the smart IIoT system. While this communication could either be wireless or wired, the integrity of the data transmission must be maintained. While interpolation of missing data is possible, it is often not preferred. Therefore, a robust wireless link >99.99% is typically required in the presence of known RF interference. The architecture planning should account for any changes in the manufacturing environment that could inhibit this link integrity such as changes in significant metal structures, walls, and new equipment.

If an RF solution is simply not an option, a wired industrial ethernet connection may be a second choice. This will require the added hassle of additional cables. But it will remove any uncertainty of an RF communications link.

CLOUD

The cloud is the final aggregation point where data fusion across all sensor nodes can take place. Broadly encompassing all ingestion points, the data can be parsed and analyzed across a single machine, a unique operational section, a full factory or across an entire enterprise. Large enterprises may have their own internal cloud platform that provides a proprietary advantage. Others can leverage open cloud platforms that provide sophisticated dashboards, analytics packages, mobile applications and support structures. As seen in FIGURE 1.

Part of the smart device design needs to plan the rate and quantify the amount of data that is sent to the cloud. If events are time critical within the operation for control feedback, then the transmission latency must be minimized to the cloud. (Saviant) A timing measurement analysis that simulates the time required for sensed data to reach the cloud analytics dashboard may be needed to understand the overall system latency. Similarly, any data with synchronous timing ambiguity across disparate sensing devices must also be planned.

Smart Architecture for IIoT

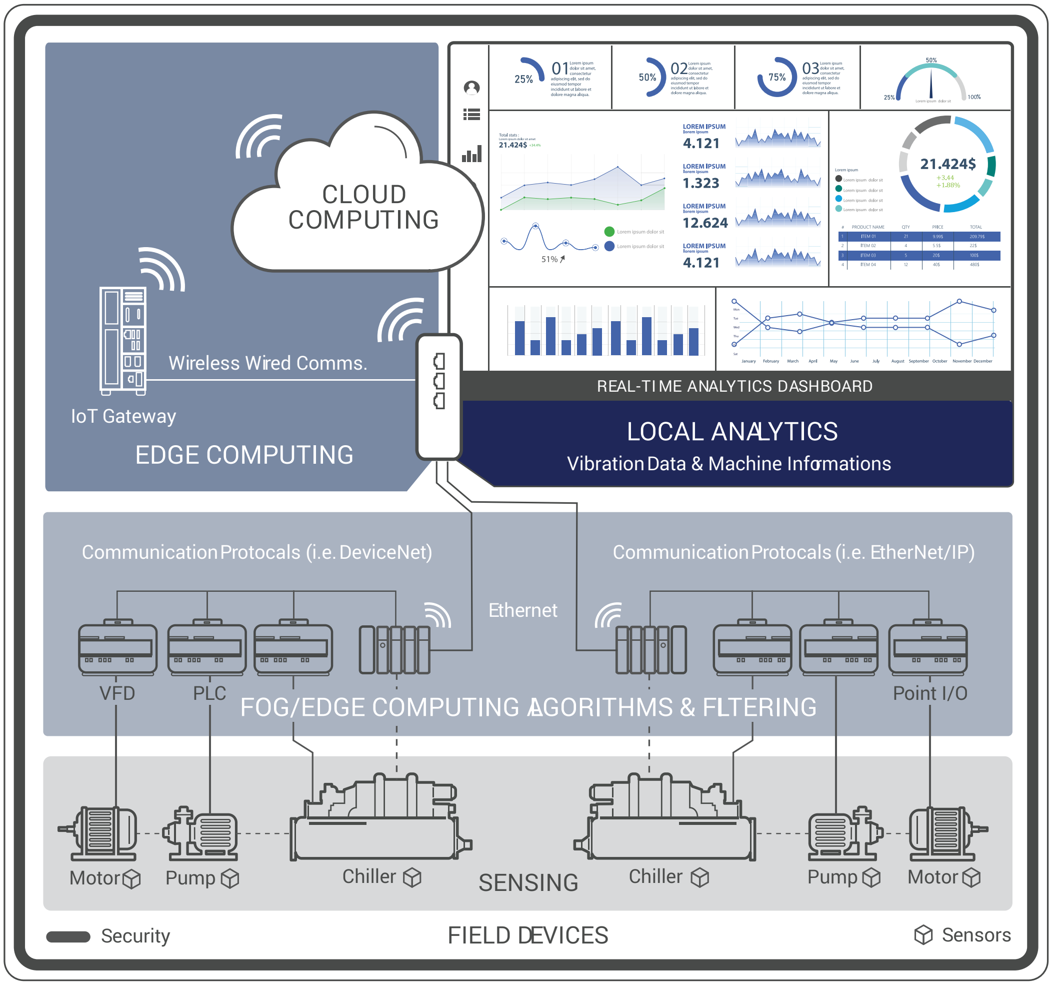
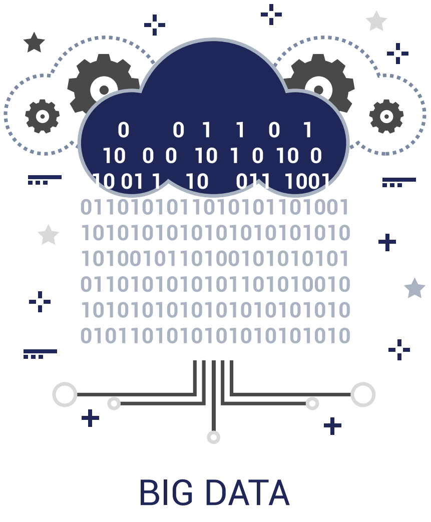


FIGURE 1

ANALYTICS

If the sensed behavior is known, such as a predictable mechanical failure or an inefficient operation, then a trained analytical model can be used against this known expectation of data. A more challenging analytics approach occurs when the expected behavior itself is unknown and the model must be formed from ongoing new data (Shi-Wan Lin). Artificial intelligence methods can ingest new data and re-train existing legacy models to adapt for new incoming information. This allows the data modelling to stay current as new changes obsolete prior observations or make them less relevant than more recent data.



Once the complete dataset can be obtained from the relevant sensor sources, a data model is employed to extract insights. The input to the model should be all the predictor information needed to answer our second fundamental design question from above. The output of the model should eventually be adequate to solve the problem identified in our first fundamental question.

SECURITY

The security of the overall manufacturing IIoT must be included as a process within all steps of the architecture design. In order to be effective, the security of the system cannot be an afterthought of the design as a wrapper or password. Every step in the communication chain, for both hardware and software, has the potential for unauthorized access (Beavers, Maclean 2018). Therefore, a critical assessment of the security needs and risks should be embedded in each phase of the smart architecture planning.

After the smart architecture design planning is complete, the answers to the two fundamental IIoT questions should have a pathway to be realized. All the hardware, software and information generated by the IIoT deployment should be focused on solving the manufacturing problem(s) identified. With the end-goal in mind as the leading reason for the IIoT effort, the smart device design phase should not be open-ended, but have a targeted reason for deployment with clear data evidence to make informed decisions going forward.