The market for Internet of Things (IoT) applications is continuing to blossom as applications are developed to take advantage of the universally-expanding network of connected physical devices. Analyst firm Gartner says that 4.9 billion devices will be connected in 2015, and will rise to 25 billion in 2020.¹

The availability of personal devices such as smart phones and tablets with mobile connectivity contributes to this growth and a significant portion of connected devices are predicted to be dedicated for use in the consumer sector, but a rapidly growing percentage will be accounted for by industrial applications, mostly in automotive, manufacturing, utilities, and transportation verticals. Gartner’s prediction is that by 2020, utilities, manufacturing, and government (largely including “smart city” approaches for reducing energy consumption) will have the three highest numbers of connected devices highlights the rapid acceptance of the concept of the IoT within industrial contexts.
The industrial enterprise comprises a wide variety of sensors, machines, and instruments of varying vintage, each with its own demands for monitoring, control, and maintenance. Some of these machines are already hardwired to connect to the Internet, yet many older machines are prime candidates for being retrofitted to be able to join a mesh network. Evolving an ecosystem to increase automation for oversight and control embodies the concept of an Industrial Internet of Things, (IIoT), which is a type of environment architecture that connects a broad community of equipment, devices, sensors, and machines within a mesh-connected network.

While consumer-based IoT application growth may be attributable to the ubiquity of smart mobile devices, the potential for fast growth of the development of (IIoT) applications is enabled by the ease of wireless connectivity, often using the infrastructure that is already installed within most industrial environments. Yet more than three-quarters of industrial machines in the world are not connected via any type of network, and this represents a total addressable market (TAM) of $21 Trillion, with a compound annual growth rate (CAGR) of 21%. This is the most concrete and tangible opportunity in the IIoT space today, to create innovation and commercial traction by providing manufacturers with an easy, yet low-cost way to connect these effectively invisible assets.

According to the Berg Institute, the installed base of wireless devices in industrial applications reached 10.3 million connections at the end of 2014, with the number expected to expand at a 27.2 percent compound annual growth rate to 43.5 million devices by 2020. And analyst firm IDC suggests that the “IoT market in manufacturing operations will grow from $42.2 billion in 2013 to $98.8 billion in 2018, a five-year growth rate of 18.6%.”

These are powerful numbers but beyond that driver, it is important to recognize the critical synergy that can be achieved by connecting IIoT devices using wireless connectivity. Mobile network business models are engineered to accommodate people who pay for their access to the network. But because those business models are not generally organized for connecting non-paying things, mobile operators would need to adjust their economic approach should they desire to generally support connecting billions of devices. Yet as we will see, an industrial business's need for seamless IoT connectivity cannot depend on the mobile networks or rely on consumer funding, and must look for economical solutions and rely on the broad-based capacity for wireless interconnections.

---

2 Wi-NEXT analysis of Gartner reports and NAC Scores by Accenture 2015
CHARACTERISTICS OF SEAMLESS IIOT CONNECTIVITY

The value of IoT in the industrial environment lies primarily in optimizing for increased productivity, reduced costs, and more efficient use of machinery. Analytical models that continuously monitor power consumption, as well as ambient temperature, humidity, air quality, vibrations and other relevant variables can predict imminent undesirable events and notify technicians prior to the events occurring so that the issues can be proactively mitigated.

And to support the Industrial IoT, one must ensure that the sensors actuators, and all other devices can be internetworked using a connectivity fabric that exhibits predictable and reliable behaviors. The characteristics of that connectivity fabric include:

- **Availability**
  The network must be trusted to remain available on a predictable basis as well as support rapid recovery when there is an interruption in service. In addition, the enterprise must ensure that network connectivity is pragmatically accessible within the locations where the devices are situated.

- **Ubiquity**
  Devices must be connectable everywhere within the industrial environment.

- **Controllability**
  The network environment must offer the authority to control how devices join the network, what level of service is supported for connected devices, and how network performance is monitored and maintained.

- **Range**
  While some of the devices are within a relatively close proximity to each other, the network fabric must be able to easily cover a range that spans the industrial footprint.

- **High-Bandwidth**
  The amount of data pushed through the network will grow at least proportionally to the number of communicating devices attached to the network. Therefore, the network fabric must provide enough bandwidth to efficiently carry all the data to be transmitted.
• **Low-cost**
There should be a way to limit the costs associated with connectivity, ranging from the costs for adding a new device to the network, infrastructure provisioning and maintenance, as well as continued operations and management costs.

• **Low-power**
Reduced power consumption not only allows more sensors and devices to be incorporated into the network, it also includes devices that are powered using batteries.

• **Retrofittability**
In many industrial environments, there are many machines and devices in service that were not originally designed to be connected to the Internet. Therefore, the network fabric must be adaptable to these legacy devices and machines that are being retrofitted to connect to a communications mesh.

• **Integrability with new devices**
As more devices and sensors are engineered with the capability to be connected in a mesh network, the connectivity fabric must easily incorporate those newer devices.

• **Consistency and Predictability**
To support a dynamically growing (or shrinking) set of devices, the network must have consistent up-time and be predictable for ensuring efficient communication.
WHY WI-FI IS THE RIGHT CHOICE FOR INDUSTRIAL IOT

If one were to consider availability and ubiquity as the primary characteristics to support the conceptual IoT, then the mobile cellular networks seem to be a reasonable alternative. That being said, when you factor in the costs and instability associated with cellular machine to machine (M2M) connectivity, this alternative loses some of its appeal.

Clearly, wired connectivity is out of the question; when you consider the level of effort for designing and implementing the infrastructure, plant downtime for the lengthy implementation, hard-wiring the connections, and enforcing policies for introduction of new devices into the environment, the overhead will overwhelm the anticipated benefits of an elastic mesh configuration. And even in environments that are prewired for Ethernet cables and drops, there will still be challenges with retrofitting older machines with the standard RJ45 connectors as well as integrating new devices that lack an RJ45 port.

A different alternative is using a wireless protocol such as Bluetooth. While Bluetooth is good for wireless connectivity, its range is severely limited, and would not be able to support the needs of enterprise-wide meshes.
In fact, there is only one networking framework that meets the needs of evolving Industrial IoT configurations: Wi-Fi. Wi-Fi’s value proposition as the wireless networking protocol of choice for the IIoT is reflective of the high degree to which it exhibits the desired characteristics described above:

• Wi-Fi is often already deployed within an organization’s facilities, and commodity components are easily acquired and put into service to expand the capacity, boost the strength of the signal, or otherwise improve availability. In addition, for those environments that do not already have wireless networking, Wi-Fi is relatively easy to deploy and expand.

• The availability of commodity components simplifies the extension of an organization’s Wi-Fi environment, thereby allowing devices across the enterprise to be easily added to the mesh network.

• Cloud-based servers can be used to bridge Wi-Fi networks across different physical locations.

• Well-defined protocols are standardized for controlling how nodes are added to the network as well as monitoring and controlling its performance.

• The range of accessibility to a Wi-Fi network is 100-150, but can be easily extended using extenders and repeaters.

• Most industrial machines in the plant produce Gigabits of data per day. Wi-Fi is a broadband technology, up to 1 Gbps with 802.11AC, and can easily collect and transport huge amount of data from many different sources (including machines, camera, sensors, etc.).

• Wi-Fi is low-cost, and does not incur data usage fees like M2M over 3G/4G networks. In fact, Wi-Fi provides the capability to scale at low cost, in particular with the use of mesh technology.

• Wi-Fi is a Worldwide Standard that easily connects to installations across the globe and can easily scale no matter what country you are in.

• It is easy to retrofit heritage machines and components by integrating or rewiring to attach to sensor nodes with Wi-Fi connectivity.
• Wi-Fi can be easily used to collect and bridge wireless analog narrow band technologies such as ZigBee or low energy Bluetooth to the broadband IP level.

• An increasing number of sensors are designed with integrated wireless connectivity.

• Wireless communications protocols over Ethernet networks are mature and can be relied on.

• Mobile devices that can be used to monitor and control the IIoT environment can also connect to the ecosystem via wireless.

When considering these factors, one can see that Wi-Fi is the optimal solution for creating a mesh network to support an Industrial IoT. However every plant will be different, and have a different mix of legacy and new equipment. It is important to evaluate the current equipment and connectivity, in order to best judge the feasibility of each networking and management alternative within your organization and compare how they comply with the characteristics above.

Once you assess the costs, downtime of implementation, the ease of adding new machinery to the network, as well as the bandwidth and stability needed to run a smooth operation, it will be clear that wireless mesh should be at the center of your Smart Factory solution.
ABOUT THE AUTHOR

David Loshin, president of Knowledge Integrity, Inc, (www.knowledge-integrity.com), is a recognized thought leader and expert consultant in the areas of analytics, big data, data governance, data quality, master data management, and business intelligence.

David is a prolific author regarding information management best practices, with numerous article published at searchBusinessAnalytics.techtarget.com, and numerous books and papers on Big Data, Analytics, Business Intelligence, Data Warehousing, data governance, and data quality.

ABOUT THE SPONSOR

Wi-NEXT, Inc. is an Industrial IoT Company pioneer in Enterprise grade Wi-Fi based and distributed computing.
Wi-NEXT helps industrial companies reduce the complexity and cost of networking equipment, optimize data management processes and asset performance of the industrial plant.

Wi-NEXT sells its patented networking and edgeware distributed Fog Computing solutions globally. Wi-NEXT was named Gartner Cool Vendor in IoT for 2015, Click Here to download the report for free.

For additional information about Wi-NEXT and the WiseMesh® family of products, please visit www.wi-next.com or follow Wi-NEXT on Twitter @winextcom
CONTACTS:

US OFFICE
530 Lytton Avenue,
94301 Palo Alto,
California USA
Ph. +1 (650) 617-3491

ITALY OFFICE
Piazzale Biancamano 8,
20121 Milano - Italy
Ph. +39 02 62032044

www.wi-next.com
info@wi-next.com
@winextcom

NOTE
© 2015 Wi-NEXT. All rights reserved. This document may be reproduced in whole but not in part. The information contained in this document is subject to change without notice and is made available in good faith without liability on the part of Wi-NEXT. All trademarks acknowledged.