THREE WAYS TO MAKE THE INTERNET OF THINGS REAL

By Alejandro Nieto and Dagoberto Mata

The Internet of Things (IoT) is transforming a wide range of industries and bringing increasingly intelligent, connected devices to market. Examples include smart thermostats that ensure energy efficiency and home security, software-controlled automobiles that can be remotely serviced and upgraded and sensors that monitor oil-drilling equipment to prevent breakdowns.

But for many businesses, the reality of the IoT remains elusive. While the promise of the technology can't be denied, and while many firms are making the IoT a top priority, defining and implementing a strategy that moves the needle and yields quantifiable benefits presents a challenge.

Based on field observations, Softtek advises companies seeking to achieve actual results from the IoT to consider three key elements in their action plans:

• Bridge the language barrier between IT and Business Operations
• Start small (while thinking big)
• Make connectivity king

One: Bridge the IT/OT Language Barrier

In too many cases today, IT and operational teams don't speak the same language. Chief Technology Officers (CTOs) often lack insight into the realities of the shop floor, focusing instead on theoretical models. The eyes of shopfloor and operational managers, meanwhile, glaze over at talk of "digital transformation." The result is that IT and Operations function in isolated, discrete towers – enterprise planning systems, for example, typically can't share data in real time with Operations teams, resulting in delays in critical reporting and information sharing.

This isolation, of course, is anathema to the IoT, which by definition requires the integration of IT and operational expertise. Communication enables understanding of key business issues, which in turn makes it possible to generate new ideas and to identify and prioritize potential IoT opportunties. And without insight into a specific business problem that needs solving, the myriad options presented by IoT technologies can be paralyzing.

More specifically, IT/OT collaboration on the shop floor makes it possible to identify the process levers that enable data collection and that power the virtuous cycle of analysis, automation and continuous improvement that underlies IoT innovation.

Two: Start Small, Think Big

The pervasiveness and all-encompassing nature of the IoT can lead organizations to aim for grand strategies that yield dramatic results. Aggressive plans can also be seen as necessary to satisfy the lofty expectations of business stakeholders.

The problem is, an overly ambitious, long-term approach can be an obstacle to identifying specific actions or priorities or to measuring results. This, in turn, complicates the task of developing the quantifiable business case needed to justify the massive investment that a major program requires. The result is typically paralysis by analysis and lack of concrete benefits.

A more effective strategy for IoT is to employ a Minimal Viable Product (MVP) methodology characterized by early release, adjustments based on testing and user feedback and quick capture of ROI – followed by a repetition of the process. For example, a MVP approach can be applied to develop a sensor that monitors heat and vibration of industrial parts on a factory floor; the data collected by the sensor can be analyzed to assess wear and tear on the equipment and enable predictive maintenance. The ROI benefit can be calculated in terms of preventing a breakdown that requires an assembly line stoppage. Subsequent roll-outs can enhance data collection and analysis features and automate additional parts of the process.

The MVP Development Cycle

Understand the Business

Identify the opportunities and pick the best ones

Based on the opportunities, generate MVP's

Choose the most valuable MVPs and improve over them

Release, capture quick ROI and repeat

RunLean Approach
Gloal Implementation Approach
IoT Talent at Scale

Technology Leadership
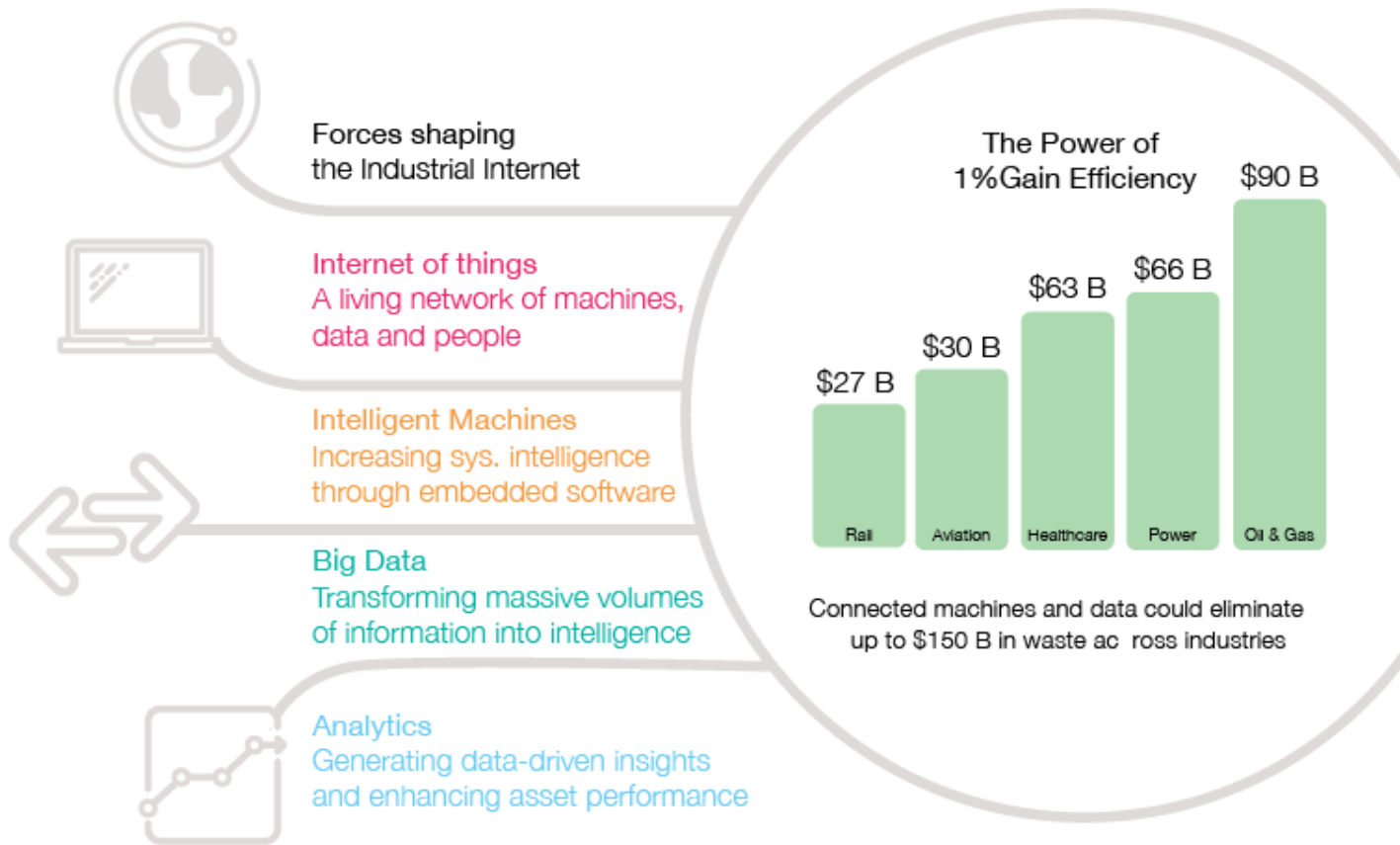IT & OT Security
Industry Expertise

The MVP approach offers a number of advantages. Continual feedback institutionalizes communication between IT and Operations, drives a focus on business outcomes and facilitates the development of a common language (see point #1 above). In addition, MVP makes the task of data analysis more manageable – rather than seeking a needle of insight from a haystack of numbers, the model provides a window of perspective to expand upon. And, the timeline for a MVP project – which can range from 1 to 3 months – will appeal to executive sponsors.

Put simply, the MVP approach breaks the elephant of IoT into bite-sized, digestible and affordable chunks.

In terms of ROI, a "start small" approach that yields even minimal gains can reap significant benefits over time. According to General Electric's "power of 1%" calculation, a 1% efficiency improvement in how healthcare providers locate and use medical equipment can save $63B over 15 years. For power generators, a 1% improvement in equipment monitoring and predicting network problems can yield $66B over that period. Oil and gas producers, meanwhile, can save $90B through a 1% reduction in fuel and operating costs and similar improvement in equipment productivity and availability.

The Industrial Internet

Forces shaping the Industrial Internet

Internet of things
A living network of machines, data and people

Intelligent Machines
Increasing sys. intelligence through embedded software

Big Data
Transforming massive volumes of information into intelligence

Analytics
Generating data-driven insights and enhancing asset performance

The Power of 1%Gain Efficiency

$27 B — Rail
$30 B — Aviation
$63 B — Healthcare
$66 B — Power
$90 B — Oil & Gas

Connected machines and data could eliminate up to $150 B in waste ac ross industries

GE Renewable Energy May 2015
Source: Industrial Internet Pusing the Boundaries of Minds & Machines, GE, Nov 2012

© 2015 GE Proprietary Information

Three: Make Connectivity King

The IoT is characterized by the integration of multiple intelligent devices and assets into a "system of systems" powered by real-time communication and data sharing across flexible platforms. This connection of individual assets into a broader network produces a powerful combination of "local" and "global" capabilities that can be applied to specific issues as well as to high-level, long-term requirements. In a smart city environment, for example, an intelligent sensor that monitors traffic on a street corner not only alerts police in case of an accident, it continually collects and feeds data on traffic flow into an analytical engine that receives similar data from across the city and automatically adjusts the timing of traffic lights to reduce congestion.

To achieve the required level of integration between multiple devices, an IoT platform must accommodate a wide range of standards and protocols. The challenge lies in selecting an approach that optimizes connectivity between different devices with a minimal amount of customization. And while all major IoT platforms purport to be "open system" solutions, the reality is that some are more open than others.

Elements of IoT Connectivity

Bluetooth
RFID
802.5.4
ZigBee
Infrared
Communication

Biometry
Video
Identification

RFID
GPS
Localization and Tracking

Internet of Things

Sensors
Biometry
Video

Devices
RFID tag
Embedded Mobile
Mobile Phone
Constrained device with radio

Security
Video
Video
Video
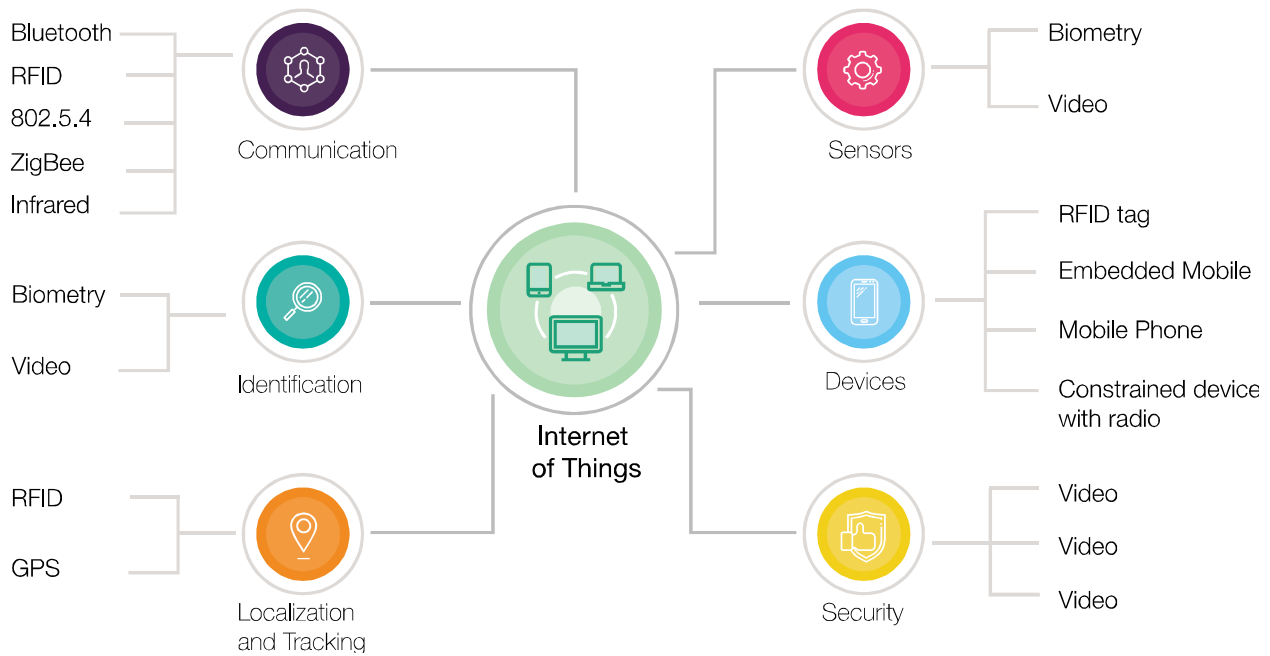
Source: IoT Worm, "Internet of Things Connectivity Challenges"

While connectivity is obviously central to an IoT strategy, assessing the specific level of connectivity is imperative. In the broader context of "buy vs. build" considerations, moreover, building connectivity should be avoided. A mature solution enables integration and data sharing between devices, leverages existing investments, connects pre-configured assets without extensive third-party intervention and captures data from those assets in real time.

A sub-optimal solution, meanwhile, requires connectivity to be built from scratch, which in addition to limiting functionality essentially amounts to reinventing the wheel. Devices that merely access databases and then require complex interfaces to transform collected data into insights and business outcomes are another red flag.

Connectivity is also essential to an effective IoT cybersecurity strategy – "if it's connected, it needs to be protected." Extensive customization and re-configuration of assets increase the number and complexity of the touch points between the "building blocks" of the IoT, thereby introducing new potential vulnerabilities. Simplifying these multiple touch points, meanwhile, can significantly mitigate a wide range of risks.

Summary

The IoT is transforming a wide range of industries and redefining how goods and services are designed, developed and delivered. In the process, enterprises seeking to reap the potential benefits of an integrated system of connected intelligent devices face myriad emerging opportunities and challenges.

While the range of options regarding IoT solutions and strategie can be confounding, staying on the sidelines is not an option. The good news is that enterprises can take specific steps to develop reasoned yet aggressive initiatives that move the needle, yield results and build momentum, without committing to major investments and unproven long-term courses of action.