Connecting with the Industrial Internet of Things (IIoT)

The Network is the System

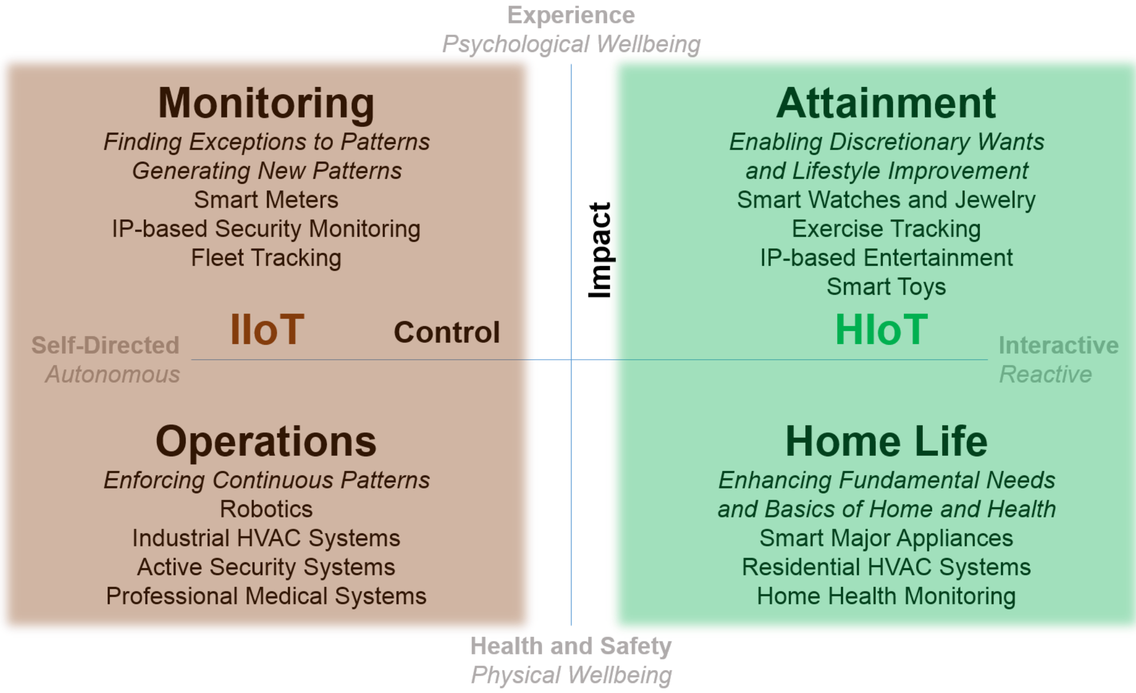
This paper continues the Internet of Things (IoT) market segmentation Moor Insights & Strategy started in the previous research note, *Behaviorally Segmenting the Internet of Things (IoT)*. Here we compare the **Industrial IoT (IIoT)** and the **Human IoT (HIoT)** at and near their end-points. Our comparison highlights near-term IIoT brownfield opportunities.

Executive Summary

The primary difference between IIoT and HIoT over the next few years is that the IIoT will incorporate over a century of existing, brownfield infrastructure (deployed mechanical and digital systems ready to be connected) while HIoT is an emerging set of greenfield services and technologies that must build infrastructure as it grows.

Designing for IIoT requires deep understanding of solution spaces and an ability to connect systems manufactured many decades apart. IIoT favors solutions vendors such as DIGI, Echelon, and Freescale, who have solid roots in the industrial control world. HIoT favors fast moving prototyping driven by leaps of faith in user experience (UX) and device design, exemplified by the Maker community in particular. The concept of “good enough” does not apply in the industrial world.

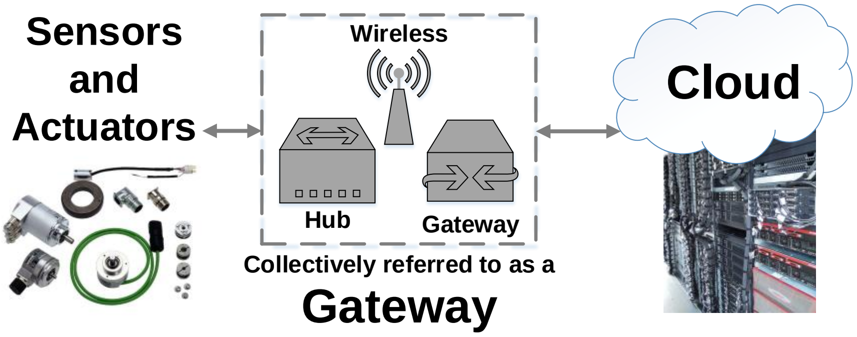
Figure 1: IoT Segments by IIoT and HIoT



What's the Difference?

As mentioned in our previous IoT paper, IIoT end-points must be more robust than HIoT end-points. Sensors embedded in end-points are not much help if the data they generate can't be collected and transmitted for analysis. We call these collection points "gateways."

Figure 2: Gateway Function in IoT



There are many vectors along which we can measure end-point "robustness." Table 1 summarizes these vectors:

Table 1: Near-term end-point differences between IIoT and HIoT

Attribute	Industrial IoT (IIoT)	Human IoT (HIoT)
Market Opportunity	Brownfield	Greenfield
Product Lifecycle	Until dead or obsolete	Whims of style and/or budget
Solution Integration	Heterogeneous APIs	Vertically integrated
Security	Access	Identity & privacy
Human Interaction	Autonomous	Reactive
Availability	0.9999 to 0.99999 (4–5 '9's)	0.99 to 0.999 (2–3 '9's)
Access to Internet	Intermittent to independent	Persistent to interrupted
Response to Failure	Resilient, fail-in-place	Retry, replace
Network Topology	Federations of peer-to-peer	Constellations of peripherals
Physical Connectivity	Legacy & purpose-built	Evolving broadband & wireless
Example Gateways	Commercial monitoring *Echelon SmartServer*	Consumer home automation *Revolv Hub*

Market Opportunity: "Brownfield" is a term borrowed from commercial real estate; it is used to denote a potential site for building development that had been previously developed for industrial or commercial use. IIoT uses brownfield to describe the opportunity to connect more than a century of in-service mechanical and electrical systems to the Internet and therefore to new cloud-based services and analytics back-ends. The equipment doesn't need to be repurchased, it just needs new, connected sensors. HIoT devices come prepackaged with sensors, their sensors are difficult to impossible to replace or upgrade without replacing the whole device, and therefore an entire system represents new market development. Even in the case of wearables, like the Nike Fuel fitness sensor, the sensor-based end-points must be completely replaced for a consumer to upgrade their features.

Product Lifecycle: IIoT products have long product cycles, and the products often must operate under extreme conditions, such as next to boilers, in automotive and jet engines, immersed in corrosive liquids, located in deserts, rain forests, volcanos, high altitude, and other hostile geographic environments – a few examples among many. Because of the expense and difficulty of qualifying new sensors and then replacing those in the field, IIoT deployments, current and future, typically have a useful operational cycle of five or more years, and sometimes decades. Often, they can't easily be physically serviced, either mechanically or because they are geographically remote. HIoT systems are replaced far more often, even for systems that have comparatively long cycles such as major appliances. Many HIoT systems will be based on functional platforms that are designed for specific and short lifecycles, rather than practically unlimited lifecycles based on regular servicing.

Solution Integration: Systems of systems installed and upgraded over decades of use, such as old HVAC boilers must be interoperable over at least one of many levels: physical (board and enclosure dimensions, ventilation restrictions, etc.), electrical (signal levels, standard analog and digital buses like the Actuator Sensor Interface and LonWorks), application binary interfaces (ABI) (such as ARM's "EABI" embedded ABI), application programming interfaces (API) (such as Oracle Java ME embedded APIs), and network protocol interfaces, (like Ethernet, TCP/IP, etc.). Systems of systems are multi-vendor by definition. Consumer-oriented systems like Revolv often rely on standard communications and networking layers, but the rest of the hardware and software stack is implemented as a vertically integrated, single-vendor solution in order to drive new and differentiated end-to-end feature sets faster than industry standardization might allow.

Security: Industrial systems like HVAC and power controls must be secure to prevent unauthorized access and abuse of physical infrastructure. Abuse of even as simple a feature as temperature control can have far-reaching real world impact. Driving up the temperature of an office building not only wastes energy and costs money, but it might be used to empty an office building as a prelude to an act of social engineering, theft, or worse. Critical infrastructure like transportation and power generation facilities have a much wider impact when their performance is impaired. HIoT systems like fitness trackers and home automation systems assume a single user or a small group of known users and are far more concerned with protecting their user's privacy and identity, if security is valued in the solution at all.

Human Interaction: IIoT systems are rules-based. Therefore IIoT data flow is asymmetric and predominantly upstream, from sensor to gateway to cloud service, with only minor control feedback flowing back downstream. Data flow is independent of network topologies and aggregation points, too. Humans can change IIoT rules, for instance, changing a thermostat setting does not reprogram the thermostat or change its functionality, but in the absence of human input to change the rules, industrial systems are designed to keep operating, using the thermostat example, the system maintains temperature at the most recent setting or changes it dynamically via a template or predictive algorithms. HIoT systems like Sonos, Korus and Fitbit are designed to react to humans whenever humans want to interact with them, and typically remain dormant or quiescent until then. When the human stops interacting they return to a quiescent state.

Availability: We measure availability by counting "nines" and looking at the remaining unavailable time at each level of availability:

Table 2: Availability vs. Unavailability

# of Nines	Availability	Yearly Unavailability	IoT Category
2	0.99	3.7 Days	HIoT
3	0.999	8.8 Hours	HIoT
4	0.9999	52.6 Minutes	IIoT
5	0.99999	5.3 Minutes	IIoT

NOTE: Five nines is equivalent to 0.864 seconds of downtime per day.

Four to five nines is usually referred to as "high availability" (HA). Generally the way to get better than five nines is to design-in redundant subsystems. If a system is built so that its redundant components can be replaced while the system is operating, then it may qualify as "fault tolerant" (FT), meaning that it is guaranteed to be always available (certainty = 1.0). In general, industrial systems, including IIoT, strive for at least HA. Consumers are far more tolerant of unavailability. Many of us own cars with less than two nines of availability, and redundancy provided by friends and family, by car rental services, or by multiple vehicle ownership. We expect that HIoT devices and their services will most likely range from two to three nines availability. Consumers regularly bridge small gaps in availability by simply retrying whatever it is they are attempting – HIoT systems will adopt the same strategy.

Access to Internet: IIoT systems cannot assume continuous Internet access to the cloud. Network interfaces fail, the network itself may fail occasionally, external interference may temporarily overwhelm a communications channel with noise and effectively sever the connection, etc. Therefore IIoT systems have to be autonomous and well-behaved during network service interruptions due to things like Internet Distributed Denial of Service (DDOS) and other attacks, backhoes severing landlines, cellular network outages, interrupted satellite communications, etc. In other words, infrastructure must act like infrastructure; it must function with minimal to no direct human interaction even when isolated from the network for extended periods of time. In contrast, consumers have an expectation that when a major systems like power, water, telephony, and Internet stops functioning, they will wait out the service interruption.

Response to Failures: Industrial systems must be resilient to failure because failure of components and subsystems is expected. These systems are designed to fail gracefully and in deterministic ways – some to save lives and health, like power generation and medical instrumentation, others to save money, resources, and time, like airline scheduling systems, so that they may be restarted quickly when repaired. State and data must not be lost. If critical systems fail, then the system shuts down to specific known operational states. Consumer and personal systems like Nike FuelBand can fail dramatically and in ways their designers did not anticipate. Many are designed not to be repaired, they must be traded-in or replaced. Others are designed to be difficult to repair, so that owners must take their device to an authorized service center.

Network Topology: IIoT end-point devices are often designed to federate into wider communities, in order to leverage resources and accomplish larger-scale goals. HIoT devices, while they may facilitate connecting individuals, are local to those individuals. An HIoT services back-end like Twitter, Foursquare, or Facebook connects people via their devices, and Big Data analytics embedded in services provide context for people to form wider communities and accomplish larger scale goals.

Physical Connectivity: Gateways should be agnostic to local physical network. IIoT uses whatever physical network fits the best: twisted pair, power line, Ethernet, wireless, cellular, satellite, etc. Multi-drop hardware topologies combined with “publish and subscribe” service APIs allow IIoT networks to scale efficiently. HIoT connectivity is already predominantly wireless at a personal level, becoming more so, and requires people to “pair” devices and services.

Note regarding end-point stickiness and the monitoring segment: From the perspective of the person or organization buying monitoring services, end-points are directly tied to the service. Consumer home security systems are a case in point: consumer choice for system upgrades for control and sensors is limited to equipment their service provider has already qualified and purchased on a consumer’s behalf, and when a consumer switches services, their entire system including gateway, control, and sensors is typically replaced by their new service provider. The service vendor’s costs to upgrade monitoring end-points are passed on to the customer, and installing new end-points is embedded in the switching costs for services. However, at a lower level, failed end-points are expensive for a service provider to maintain and replace, just like the operations segment. IIoT end-points, including their sensors and actuators, are configured for specific tasks and their local connectivity cannot be upgraded or replaced without adequate consideration.

Why End-Point Connectivity Matters

HIoT systems use the latest wireless technologies to connect end-points to their gateways, as it’s a matter of competitive differentiation for them. Companies coming from the HIoT world often prognosticate that every end-point will run a full IP stack and that every end-point will eventually have a high-bandwidth WLAN or WWAN radio and connect directly into a cloud service. Especially in the consumer HIoT world, if people want a new feature badly enough, their switching costs perception becomes biased and they may upgrade impulsively. The IIoT market behaves very differently.

In the Moor Insights & Strategy blog Big Data is Extra Sensory Correlation, we note that sensory systems include these mandatory functions:

- ***Signal*** *– physical or logical evidence generated by real world events*
- ***Collection*** *– sensors designed to measure specific signals*
- ***Transduction*** *– transmission and storage of sensor generated data*

And in our research note *How to Intelligently Build an Internet of Things (IoT)*, we included "Internet connected" in the definition of Intelligent Systems:

> *"It seems like a given, but it is not. Many sensors, in particular, will not be directly connected to the Internet. Direct Internet connectivity will be determined by use cases for cost, power consumption, security, and a host of other issues (including private innovation running ahead of public standards). Many sensor manufacturers will design their products to form their own private networks. The likelihood that every sensor or even every client device will aspire to full Internet citizenship is vanishingly small. This enables the "systems" part of IS".*

IIoT gateways aggregate, cache, and transmit "store-and-forward" data from many sensors. IIoT gateways are built into infrastructure deployments and owned as part of the infrastructure they are built into, or they are deployed by services as part of a contract. There is a much stronger coupling between end-points and a gateway's connectivity options, bandwidth, and its ability to store-and-forward data. Sensors, actuators, and gateways are optimized for specific domains and tasks within those domains.

HIoT gateways are either owned by people or they are rented to people by services. For the majority of consumer gateways, there is only a loose coupling between the gateway and other consumer owned devices. This is because 1) the communications link between HIoT gateways and devices has been highly standardized, and 2) HIoT gateways are assumed to have persistent Internet connections (they are always on, so they do not store data, they only forward it). HIoT gateways are standard and transparent, and so they are almost completely fungible. Their primary value is in supporting ever-evolving HIoT communications and networking standards. They are replaced whenever a consumer buys a compelling new HIoT end-point or the aggregate weight of many new end-points persuade a consumer to upgrade.

IIoT deployments are typically a mix of wired and wireless local connectivity and include "multi-drop" connectivity. Many sensors and devices cannot "phone home" directly over the Internet. Some predate the Internet, others are in awkward or remote physical locations, and many simply cannot afford the cost structure of full Internet Protocol (IP) software stack and the processing capability to run it.

Because of the huge brownfield installed base of infrastructure that will be connected to the IIoT, there is little opportunity or customer tolerance for single vendor end-to-end lock-ins. Gateways are the closest devices (in connectivity sense) to endpoints and sensors that can be upgraded and enhanced as needed, as long as they can maintain contact with those sensors and end-points.

State of IIoT End-Point Connectivity

The challenge for IIoT connectivity is that industrial systems have such long product lifetimes and product lifecycles that many physical media types and logical protocols never seem to die. Table 2 lists many of the connectivity standards in place across a broad swath of IIoT. It is an incomplete list, which demonstrates the complexity in connecting with a range of equipment deployed over many decades.

Table 3: Selected Industrial Network and Communications Standards

Wired	Wireless

• UART
• Serial
  o RS-232
  o RS-422
  o RS-485
  o I^2C
  o 1-Wire
  o SPI
  o Low Voltage Differential Signaling (LVDS)
• Hayes-compatible modem
• DSL modems
• Controller Area Network (CAN)
  o SAE J1939
• LonWorks
  o ISO/IEC 14908-1:2012
  o ANSI/ASHRAE 135-1995
• Ethernet
  o 1000BASE-T
  o 10BASE-T/100BASE-TX
• Power Line
  o CENELEC 50065-1 A-Band
  o CENELEC 50065 C-Band / IEC 14908-3
  o IEEE P1901.2 Draft
• Universal Serial Bus (USB)
  o 1.x, 2.x, 3.x
• Fiber Optics
  o IEC 61107
  o Others
	• Radio Frequency (RF) 6-8 MHz
	  o TV Channel Whitespace
	• RF 13.56MHz
	  o NFC
	• RF 868/900 MHz
	  o Automatic Meter Reading (AMR), Advanced Metering Infrastructure (AMI)
	• RF 2.4/5.0 GHz
	  o 802.15.4 (basis for ZigBee)
	  o ZigBee
	  o Bluetooth
	  o Wi-Fi 802.11 (various)
	• Cellular
	  o 4G
	  o 3G GPRS (GSM)
	  o 3G CDMA (EV-DO)
	  o 2G (GSM)
	• Satellite
	  o Inmarsat / SkyWave
	  o Iridium
	  o Etc.

NOTE: This is a select list of the relevant IoT standards. There are hundreds.

There is important work yet to be done at the gateway services layer. One of the key areas for differentiation is to provide high quality of service protocol conversions between end-point connections (point-to-point, peer-to-peer mesh, local area network (LAN), etc.) and server-side local and wide area networks (LAN and WAN).

Silicon vendors who serve broad IoT markets spanning IIoT and HIoT tend to focus on Ethernet, WiFi, and cellular networks because of their ubiquity and interoperability. Qualcomm is a good example here, with niche vendors like NXP specializing in newer standards like NFC.

In brownfield core IIoT applications, non-Ethernet wired infrastructure plays a much larger role. Silicon vendors who specialize in serving a wide array of industrial wired connections, such as Echelon and Freescale, will be increasingly important here.

At a higher level, board-level module and off-the-shelf systems vendors, like DIGI (partnered with Intel), are trying to cover broad portions of IIoT with designs based on processor designs from AMD, Echelon, Freescale, Intel, Qualcomm, and others.

Conclusion

The Industrial Internet of Things (IIoT) favors component and solutions vendors from the industrial control world who have extensive experience with a variety of legacy industrial connectivity solutions. These vendors specialize in understanding specific industrial usage models, and then they create domain expertise to translate those usage models into sensors, actuators, control logic, data aggregation, local network connectivity, and services layers. They have built experience in working with legacy industrial equipment built over the last century and developed trust from decades of working with customers.

Important Information About This Paper

Author

Paul Teich, Senior Analyst at Moor Insights & Strategy.

Editor

Scott McCutcheon, Acting Director, Research, at Moor Insights & Strategy.
Patrick Moorhead, President & Principal Analyst at Moor Insights & Strategy.

Inquiries

Please contact us here if you would like to discuss this report and Moor Insights & Strategy will promptly respond.

Citations

This note or paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

Licensing

This document, including any supporting materials, is owned by Moor Insights & Strategy. This publication may not be reproduced, distributed, or shared in any form without Moor Insights & Strategy's prior written permission.

Disclosures

Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this documented.

DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.