The Internet of Things: QA Unleashed

To seize the IoT high ground, QA organizations need to view software testing beyond devices and sensors, and think holistically about added technical complexity that comes with the huge volumes, velocity and variety of data generated across a smart and connected ecosystem.

Executive Summary

The wide gamut of IP-aware and -addressable technology known as the Internet of Things (IoT) is embedded deeply into our professional and personal lives. "The Internet of Things installed base will grow to 26 billion units by 2020," says Gartner.[1] "IoT product and service suppliers will generate incremental revenue exceeding $300 billion, mostly in services, in 2020. It will result in $1.9 trillion in global economic value-add through sales into diverse end markets."

The sensors at the heart of IoT are embedded in a wide range of applications, from tweeting turbines (GE's Brilliant Machine metaphor) and toothbrushes, through smart thermostats (think Nest) and personal health monitoring devices (think Fitbit). These sensors are transforming how we work and live. The combination of sensors and applications are making the new smarter cities, homes, railways, healthcare services and much more. Further, data analytics from the evolving connected world holds immense promise for continuously improving the system.

Though the influence of IoT is already evident across different verticals, emerging markets will witness rapid growth as product designers dream up ways to exploit real-time machine-to-machine connectivity and intelligence. This white paper captures the aspects of IoT that are relevant to QA organizations. Further, it elaborates the paradigm shift required in QA in order to embrace the technology changes applicable to products and services offered in IoT's wide spectrum.

Core Components

Though multiple definitions exist for IoT, we define it as a network of physical objects that contain sensors or embedded technologies to interact with the internal or external environment and to take intelligent decisions. Core components of IoT include three different components: things, communication and computing (see Figure 2, next page).

- **Things:** Things are the real-world objects or devices that include the sensors and embedded software required to communicate with the external environment.

The Many Manifestations of IoT

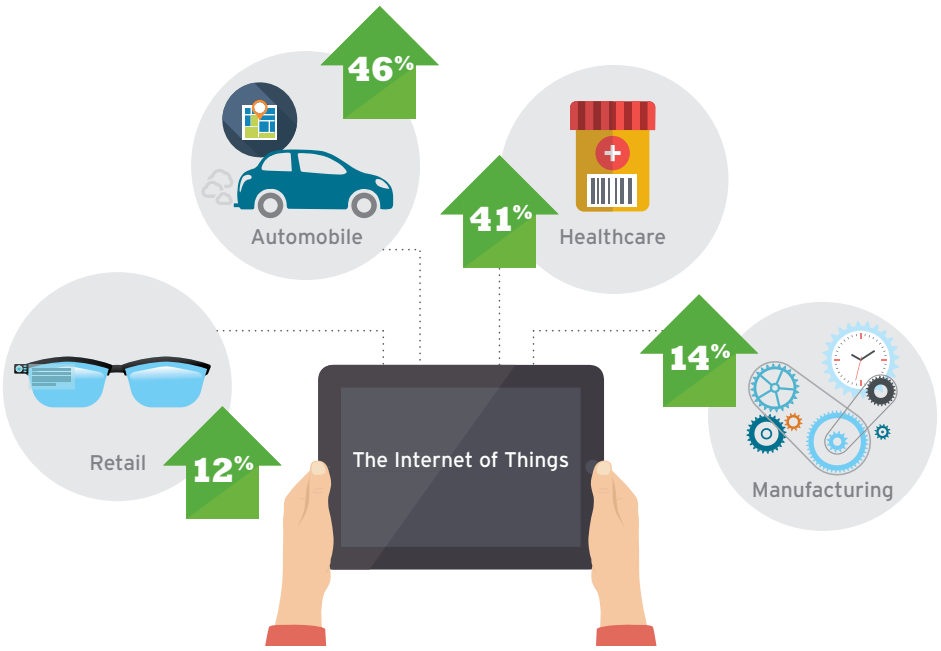

Figure 1

- **Communication:** Communication is the core networking component that helps the *thing* communicate with another *thing* or the external environment. Typically, communication protocol is based on the type of network such as the WAN, LAN or PAN. The network is 4G in the case of WAN; WiFi or Wifi Direct in the case of LAN; and BLE, Zigbee, ANT+, sub 1GHz in the case of PAN. Sometimes it is possible that the communication is wired as well.
- **Computing:** Computing is often done on a mobile device, desktop or server, based on the amount of data that needs to be processed and analyzed. Computing occurs at two levels: one, to make intelligent decisions within the system, and the other to form the vital link for business to perform big data analysis for understanding IoT user behavior.

IoT's Key Components

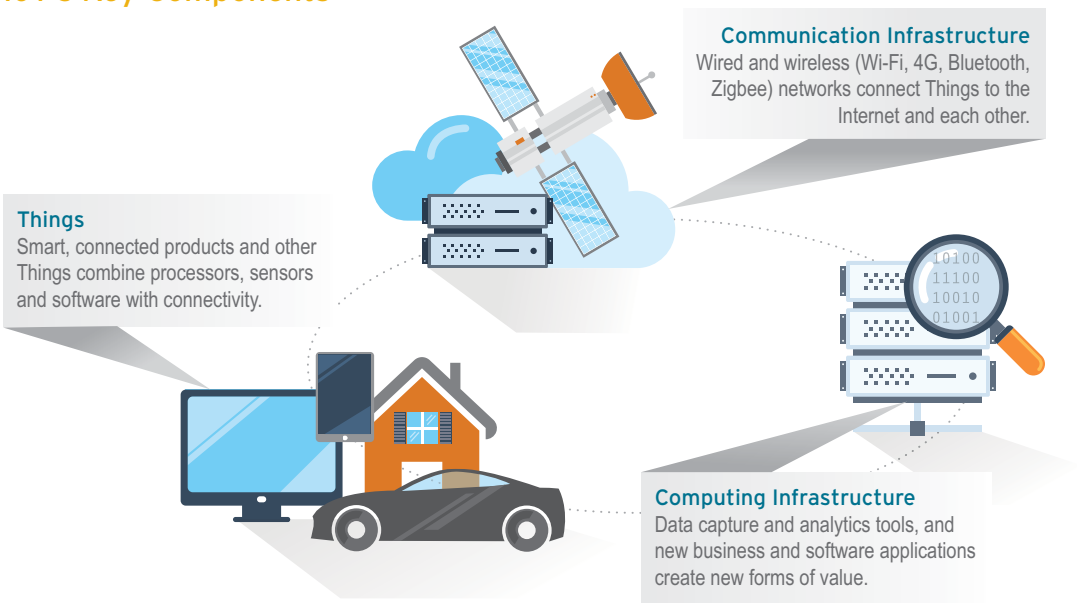

Figure 2

Defining QA's Role

There is a plethora of applications under development to expand the existing hyperintelligent, connected world. However, organizations need to perform testing on these applications before they reach prime time. The role of QA is therefore critical, because it involves testing hardware and software and transmitting massive amounts of real-time intelligence. Top challenges and solutions that QA managers can enlist include:

- **The hardware/software convergence of QA:** Devices, sensors and applications form the ecosystem. However, there is a phase shift from sheer testing of applications in a defined environment to testing the experience in a dynamic environment. With several million sensors and different types of devices providing the experience in conjunction with intelligent software, mere functionality validation is not enough in an environment as complex as IoT.
- **A working system is not sufficient:** To certify an IoT system or service, it is not enough to merely ensure a working set of device software. For instance, a shipment tracking system with sensors and devices that communicate with multiple software back-ends will need intelligent algorithms to ensure accurate product delivery. This requires a very robust QA validation process. The use cases could be extremely complex in real time; the variety of real-time scenarios can become a challenge for QA.
- **Large number of sensor interactions:** The creation of an environment to test a real-time IoT implementation is a challenge. It entails not only configuring an environment to validate the correctness, but also to assess scalability and reliability. The system is built on numerous analytics engines, and demands a significant experience in simulation to build out a test environment. While the hardware and the protocols are typically well tested by device makers, understanding application intelligence and the device's real-time complexity is an extremely new art and science for many application developers and QA experts.

In a nutshell, the software testing challenges go beyond devices and sensors to include the added complexity that comes with big data (i.e., huge volume, velocity and variety), which makes validation of real-time IoT certification a major headache.

Addressing IoT's QA Complexity

A comprehensive QA strategy is required to cover the depth and breadth of IoT testing. The strategy must include the types of testing, test lab setup, testing tools and simulators that should be deployed. Considering the difficulties in generating big data from the *thing* in a testing environment, it is crucial to evaluate data simulation and virtualization techniques. Stubs can be considered as options during early stages while data recorders can serve as alternatives at later stages. Beyond test planning and data simulation, metrics-driven exhaustive test execution is performed to achieve a stable system.

QA organizations can split IoT test areas into two layers, as described below. While the QA needs to be performed across both layers, it is always easier to identify techniques and the types of testing that can be adapted to each layer to enhance the QA strategy.

- **The device interaction layer:** This layer is where the software and the hardware components of a real-time IoT environment interact.

  One typical example is a Bluetooth device transmitting real-time data to a mobile device app. Oftentimes, there is a lot of interaction testing occurring on the functional side of QA. However, other types of testing could also be required. The following are the broad types of other required elements, in addition to typical software testing:

  - **Conformance with standards:** These are mostly device performance attributes that are specific to devices and sensors. These attributes must be validated against the standards of the device and its communications protocol. Hardware vendors perform most of these tests, but there could be certain domain- or use-case-specific requirements such as the use of such devices in an environment that was not tested.
  - **Interoperability:** The ability of different devices to support the required functionality among themselves, other external devices and implementations.
  - **Security:** With billions of sensors in the making, it's crucial to tackle data privacy and the security concerns across the IoT ecosystem. The following are the different types of security testing requirements:
    - Identity and authentication.

- Data protection.
- Data encryption.
- Storage data security in local and remote clouds.

- **The user interaction layer:** This layer is the touch point between the *thing* and the user. The success of the overall system depends on the user receiving a seamless experience. Key testing areas in this layer include:
  - **Network capability and device level tests:** The specific aspects of network communication such as connectivity are validated by simulating different network modes in addition to device-level validation such as energy consumption tests, etc.
  - **Usability and user experience:** Usability and user experience are important in terms of the real-time usability; it involves human/machine interaction and also the real-time experience that the IoT system provides in a specific interaction. For example, contactless payments compared with a physical card-based payment.
  - **The IoT services and back-end IoT environment:** While integration testing of the interfaces is key, there is a complex data layer that comes into play. For example, a typical IoT system packs a complex analytical engine to ensure an exceptional user experience.

Creating a QA environment to enable validation of such an interface means addressing the growing data volume, velocity and variety challenges of the IoT ecosystem. The front-end validation environment can be done by assembling data recorders and simulators. The service and data layer validations will involve complex simulation services such as the generation of millions of sensor hits, machine learning algorithms and the ability to generate time-boxed traffic.

There are a few methods to create such an ecosystem; for example, leveraging sandboxes of development services or creating mock environments using virtualization tools. However, numerous implementation synergies are required to establish a working set of environments for a thorough services and back-end validation platform.

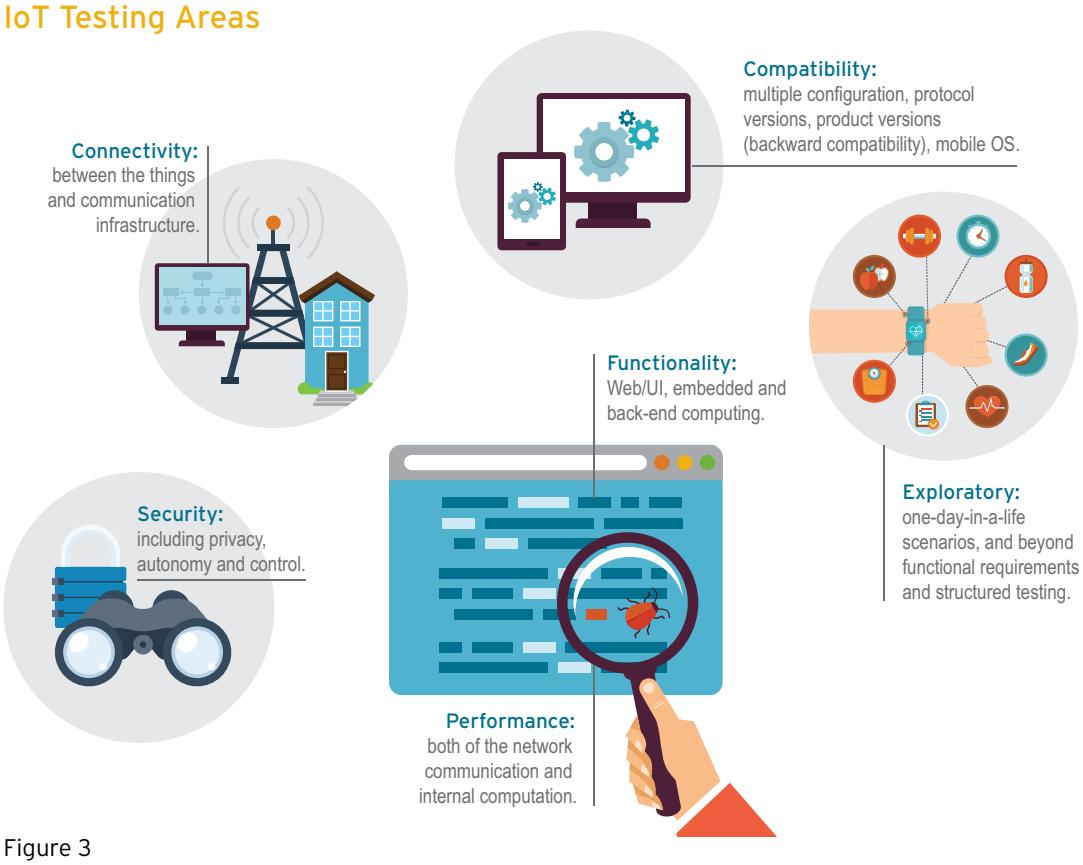

Figure 3

IoT Testing Types

A simple IoT ecosystem borrows several software testing approaches from regular QA parlance to validate IoT applications. It is important to focus on all three core components of the IoT system to treat functional and connectivity testing as critical elements of overall IoT ecosystem testing.

The following types of testing must also be performed across the IoT ecosystem:

- **Performance testing** that covers the rapidity of the communication network model, as well as the internal computation capabilities of the embedded software system.
- **Security testing** that covers privacy, autonomy and spying.
- **Compatibility testing** with the possible combination of device version, protocol version, mobile devices and mobile OS version.
- **Exploratory testing** to test from the user's perspective and beyond predefined test procedures.

Solutions and Framework Opportunities

The IoT ecosystem puts forth a myriad of QA challenges. Importantly, the QA organization should view these challenges as opportunities to build frameworks and solutions. The following are a few such opportunities:

- **Protocol simulators:** One of the interesting aspects of IoT QA is the ability to work with multiple protocols. Protocol simulators can come in handy when there is a huge variety of device end-points and interfaces to validate.
- **Data recorders:** Data recorders from different types of devices can be helpful in smart validation across device sets. The recorded data can be played across different device end-points automatically, which in turn can be a great enabler in compatibility testing of apps across different device sets and communication layers.
- **Virtualization:** This is an important aspect of IoT validation. Due to highly complex IoT interfaces, there is little opportunity for real-time validation of application behavior. Therefore, it will still be beneficial to bring in an ample amount of virtualization into the services on which IoT applications are built. Virtualization of an IoT ecosystem yields the benefits of faster turnaround and reduced costs due to minimal dependency on the production environment for testing. It also leads to earlier identification of defects, thereby establishing a new dimension within the validation process.

Looking Forward

The investments made in IT infrastructure and marketing can take businesses only so far, particularly if they do not have a holistic approach to testing the IoT ecosystem. As IoT expands beyond the periphery into the mainstream of consumer and enterprise markets, QA teams must gear up to help their organizations take advantage of the tremendous opportunities created by the ongoing business digitization.

It's time for QA organizations to empower their companies with reliable IoT products and services that make good on the promise of smart, connected devices that elevate everything from personal wellness/hygiene and driving, through manufacturing, logistics management and air travel. With ever-greater blending of IoT into business and IT, it is necessary for the QA teams to upskill beyond traditional functional testing and gear up for integrated testing of embedded software, IT solutions and big data — and to understand their influence on one another.

To prepare for the Iot onslaught, QA organizations should focus on the following:

- **Orient people to gain an amalgamation of skills,** combining QA, quality engineering and hardware validation to meet the demands of IoT QA.
- **Build collaborative QA teams with a view toward performing integrated tests** spanning hardware, software and big data layers, thereby augmenting the niche and broader aspects of IoT testing.
- **Look for tool-build opportunities:** As the distinctions between hardware and software blur, there is a plethora of opportunities to build solutions to enhance QA across the internal systems ecosystem.
- **Build labs that serve the entire digital portfolio,** to experiment and simulate real-time experiences that inform smarter ways of testing.
- **Build a culture of "test as a user" vs. a mind-set in which the organization merely tests against requirements;** this will ensure the "experience" component of the IoT stream is well-established for a comprehensive quality product or service.

Footnote

[1] http://www.gartner.com/newsroom/id/2636073.

About the Authors

Subbiah Muthiah is an Associate Director within Cognizant's Quality Engineering & Assurance (QE&A) Center of Excellence (CoE). He is responsible for techno-business development and building quality assurance for trending themes such as digital services, connected devices, wearables and telematics. Subbiah has more than 14 years of relevant industry experience with in-depth knowledge across the mobile stack – from the application layer to RF. He holds a bachelor's degree in engineering and works out of Chennai in Tamil Nadu, India. Subbiah can be reached at Subbiah.Muthiah@cognizant.com.

Ramakrishnan Venkatasubramanian (Ram) is a Director within Cognizant's QE&A Technology Center of Excellence. He has over 15 years of experience in the information technology industry. Ram's experience spans software development, product engineering, test automation, mobility, cloud, the Internet of Things and technology consulting. He leads the Digital Stream of Technology CoE including R&D, mobility, virtualization and Internet of Things streams within the Cognizant QE&A practice. Ram can be reached at Ramakrishnan.Venkatasubramanian@cognizant.com.

About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process outsourcing services, dedicated to helping the world's leading companies build stronger businesses. Headquartered in Teaneck, New Jersey (U.S.), Cognizant combines a passion for client satisfaction, technology innovation, deep industry and business process expertise, and a global, collaborative workforce that embodies the future of work. With over 75 development and delivery centers worldwide and approximately 211,500 employees as of December 31, 2014, Cognizant is a member of the NASDAQ-100, the S&P 500, the Forbes Global 2000, and the Fortune 500 and is ranked among the top performing and fastest growing companies in the world. Visit us online at www.cognizant.com or follow us on Twitter: Cognizant.

World Headquarters
500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277
Email: inquiry@cognizant.com

European Headquarters
1 Kingdom Street
Paddington Central
London W2 6BD
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102
Email: infouk@cognizant.com

India Operations Headquarters
#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com

TL Codex 1233