IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY | an informa business
Unlimited Validation Knowledge Awaits...
Published on *IVT Network* (http://www.ivtnetwork.com)

Connected Device System Validation & Quality - Best Practices

By **Carolyn Wright**

Aug 28, 2017 7:00 am EDT

Introduction

No matter where you are or what you are doing chances are that you are using, or are being exposed to technology in ways that were not even possible 20 years ago. Most people utilize smartphones or laptop computers in their daily life. This technology has been further expanded to include connected devices that have the ability to enhance a customer's experience and health as well as to offer employees increased flexibility and access to the data they need. Surprisingly, there are very few government regulations that guid the development, manufacture and management connected device systems. This paper reviews the results of a multi-industry survey that was conducted to identify the various verification and validation practices industries are utilizing in the absence of specific regulatory guidelines.

The ability to connect devices wirelessly has significantly expanded the ways in which we can connect to data sources or share data while staying mobile. As companies develop products that utilize this wireless connectivity it is important that they:

1.) Ensure their products will work seamlessly for the user;
2.) Ensure their software will be protected;
3.) Ensure that the data transmitted accurately and securely;
4.) Plan how they will utilize the data stream that is available to their company from the connected device further enhance the customer experience.

The direction from government agencies especially in the area of health care has usually taken the form of regulations, guidance documents and directives however in the case of connected devices very few documents have been issued. The medical device arena is the only industry that has received formal expectations from government bodies and these documents pertain primarily to medical mobile applications, software that is embedded in the medical devices and how medical data should be protected.(European Commision, 2014, 2017a, 2017b; FDA, 1999, 2002, 2015a, 2015b, 2016, 2017a, 2017b). In the absence of directives or regulations it is left to manufactures to determine the best practices to ensure the highest safety and quality of their product.
This new product type and the lack of specific regulations has also left the role of the quality department a little unclear. When you compare to the traditional QA role in nonconnected product markets, the connectivity of these systems adds the elements of software, networking, pushed firmware updates to units and data analysis which is very different from the current skill set of the traditional Quality Assurance staff member.

This paper will:

- Identify the activities that are currently being done in various industries to ensure high quality performance of the connected devices;
- Review the results from a survey created to learn the best practices from multiple industries involved with connected devices,
- Describe the new role of the quality department in this connected device market;
- Identify some of the voluntary international standards that support the connected device systems market.

What is a connected device?
In order to get started in this exploration process it is important to define a connected device system. For the sake of this discussion a connected device system is one that includes a piece of hardware that is placed in the appropriate location for its design, functions as intended, with the added benefit of being able to be controlled and monitored remotely by the user. To achieve this functionality this devise will transmit data to a server that is able to communicate wirelessly to the remote user.

Why are connected device systems so popular now?
The primary drivers of this new technology are: 1.) the deployment of sensors and smart devices (phones, laptops and other). Sensors are smaller, cheaper and they require less power and have more compute capacity than in the past. 2.) Data storage options are more available on servers and in the cloud. These two capabilities provide the ingredients necessary for businesses to drive tremendous change in the products they develop. This has encouraged companies in all industries to explore new opportunities to utilize the data these sensors can provide to better manage the performance of their products, as well as to track consumers' behavior and in order to enhance their experience. (Jason Mann, 2015)

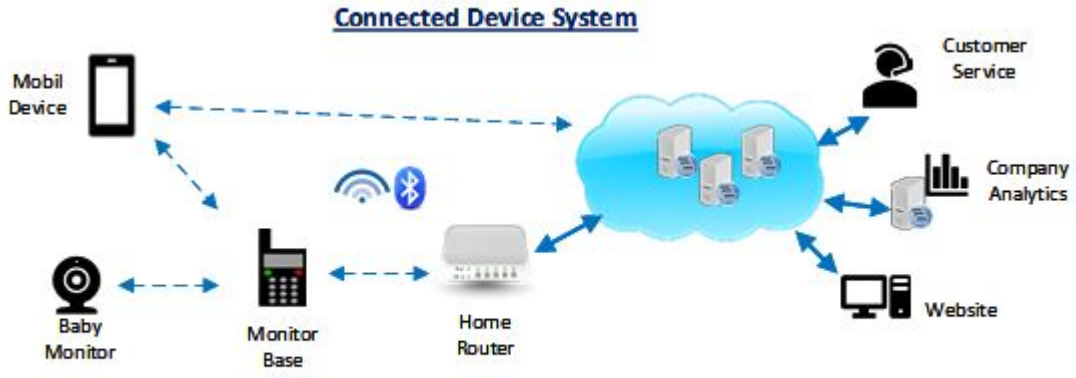
What industries are using connected device systems?
You can find connected devises in all industries and countries. Some examples include a car AutoStart app, mobile health apps, security system, baby monitors, remotely monitored equipment, household appliances and any other product that can transmit data and/or be controlled via smart phone or website account.

Concerns with connected devices
Of course, with this technology explosion consumer's expectations (requirements) are rising especially around data security as they share more and more of their personal information electronically. While companies are benefitting from the demand for new connected products they are also wrestling with new expectations. Specifically, they are looking for the best way to enable a smooth customer experience from the start-up of the product throughout its use life while protecting the device and the transmitted data from inadvertent or malicious corruption. This obligation is not unique to any one industry and must be addressed while the product is in the development process and the safeguards to the software, data streams and application can be built into the system. The verification and validation processes will ensure the customer requirements will be met throughout the life of the product.

Value of a Connected Device System Validation
Once the customer requirements are clearly identified, the product development teams, at all companies, will launch their development process. At some point before product launch there will need to be a validation that product meets the customer requirements. In the case of a connected device system the validation can be quite an undertaking because of all the potential

components in the system. For example, in the case of a baby monitor, the following components with their Infrared (IR) transmission methods might be included in the system validation to confirm that the entire system works as intended.

Figure 1. Connected Device System



?

Some examples of requirements for this baby monitor system might include:

1. Easy to set-up (monitor and app)
2. Clarity of sound and image
3. Modern look
4. Secure system
5. Data analytics for the company's marketing, sales and product development teams
6. Product performance information for customer support team
7. Company website updates for customer access

When you think about how each of these components contribute individually to each of the customer requirements it is easy to see how the system validation becomes quite extensive.

Overall Validation and Verification Process

One of the most important things to do in the early development of a product is to lay out the Master Validation Plan. This plan will include a clear description of the different types of validation and verification activities that are applicable to the product type and the manufacturing process being developed (Sherman, 2015). A second critical component of the master validation plan is the schedule of when these activities will be conducted. These tasks will be done at different stages through the development process in fact some of the product validation activities cannot be completed until much later in the process (Stevans, 2009). The third major component is the assignment of activity responsibilities to team members based on their role in the overall validation process.

The process of creating a Master Validation Plan is not formally required by any regulatory agency however it will be one of the first items an inspector will ask to see when auditing a facility.(Stevans, 2009) The plan will be a primary guide on how the verification and validation activities will be conducted. As connected devices become a stronger component of the development pipeline the intricacy of these verification and validation activities should be laid out in an approved plan to describe the responsible parties and activities that will be conducted.

Survey Conducted

The complexity of connected device system validation requires many different departments to contribute to the effort however, from an organization standpoint it is important for companies to decide which group will be responsible to lead the process. Fortunately, there are many industries that share this same necessity and a review of their various practices can allow us to distill their best practices for companies that are just getting started developing connected device systems.

In 2017, a connected device industry survey was conducted by Carolyn Wright that included 31 responses from global companies in the following industries.

- Consumable goods (7)
- Electronic & Household Appliances (3)
- Medical Device (16)
- Financial (1)
- Automotive (1)
- Water and Wastewater (1)
- Pharmaceutical (1)
- Supply Chain (1)

Quality and Information Technology professionals responded to an anonymous survey that was designed to collect information about how companies are managing their Connected Device product development and commercial lifecycle activities. For the purposes of this survey a Connected Device was defined as;

“A product that communicates and can be controlled by a mobile device or the Internet or both. For example, a smartwatch communicates with its counterpart app in a smartphone via Bluetooth, which in turn accesses services on the Internet via WiFi. Devices in the home are increasingly connected to users some examples include security cameras, baby monitors, thermostats and door locks.”

The survey asked inquired about:

A. How their industry handled connected device system validation and what types of verification and validation activities were included in their product development processes;

B. What the common failures were during system validation;
C. How was change control handled post validation;
D. How the customer experience was enhanced because of the data availability of the connected device.

The following sections of this report include some of the learnings from the survey results.

Overall Responsibility for System Validation

A connected system validation contains many different components and supporting systems making it difficult for any one group to take responsibility for the entire system validation. It is more common for each group to manage and facilitate their portion of the validation including the connectivity to the previous and post steps. Therefor a system validation manager needs to work across the organization to ensure the customer needs are met with the newly developed product.

The industry survey results indicate that the group most likely to manage the system validation from a high level was the Quality Assurance / Validation group. This is likely due to the fact that the quality assurance and validation groups are cross functional in nature and manage all ends of the supply chain as well as the complaint management. Variation of course occur company to company even within a single industry and this variation is likely related to the size and organization structure the company.

Table 1: Frequency of Connected Device System Validation Leadership

System Validation Leadership	
Quality Assurance & Validation	43%
Product Development	18%
Information Technology (IT)	14%
Digital / Software Development Team	14%
Project Management / Other	7%
Third party device management	4%

The key learning is that there is variation within each industry however the quality assurance and validation organization appears one of most probable groups to be managing the overall system validation.

Validation Process for Connected Device Systems

The goal of the validation process for a connected device system is to ensure that the complete collection of hardware, software, networking connections and supporting infrastructure produces the intended results as defined by the customer. It is also important to realize that with any product there is more than one customer involved with the requirements. Groups that should be considered customers for this type of product include:

- The end customer that purchases the product;
- The customer service and repair groups that support the product throughout its life;
- The marketing, sales and product development organizations that could benefit from use patterns and sales knowledge;
- The company shareholders that have expectations for the product revenue.

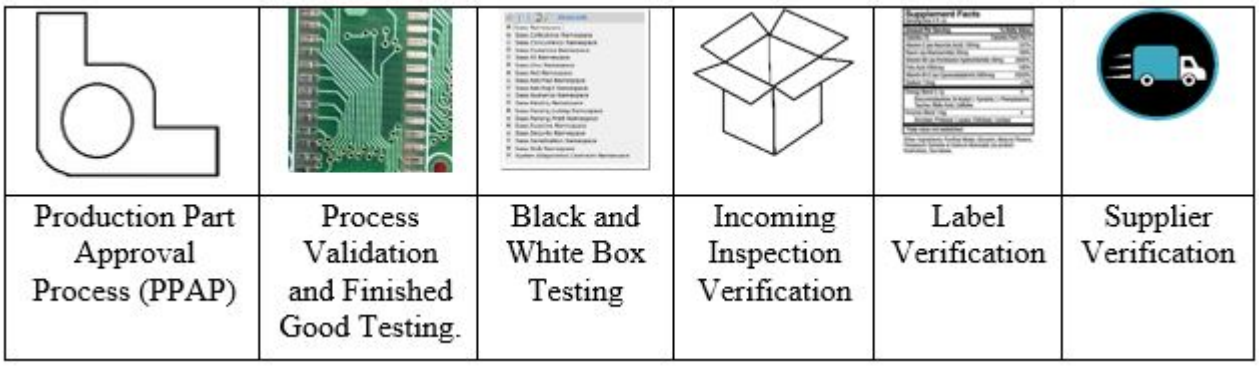
These customer expectations should all be included in the product requirements and then validated once development is complete.

Validation of all requirements cannot be done in a single step because of the complexity of a connected device system and therefor it is generally managed through a Master Validation plan. It is also very common to have a customer requirement that are satisfied by a combination of lower level, more technical requirements that work together as a subsystem. In this case a set of system requirements may be developed allowing each subsystem to be measured against its intended purpose.

Component

In a connected device system, the component level is typically handled earlier in the process validation process. Independent of whether the component is a circuit board, a plastic part or a piece of firmware (software on the unit) there should be some verification that the component meets its intended purpose relative to the customer requirements or the system requirements. These activities take different forms depending on the component type. A process validation may be conducted on a plastic part (PPAP) or a circuit board (validation) while a piece of software may require black or white box testing (verification). Other types of verification include incoming inspection of components, raw material or subassemblies as well as supplier verification that is designed to ensure that the supply chain will meet the needs of the customer through the life of the product.

Figure 2: Component Verification and Validation Activities



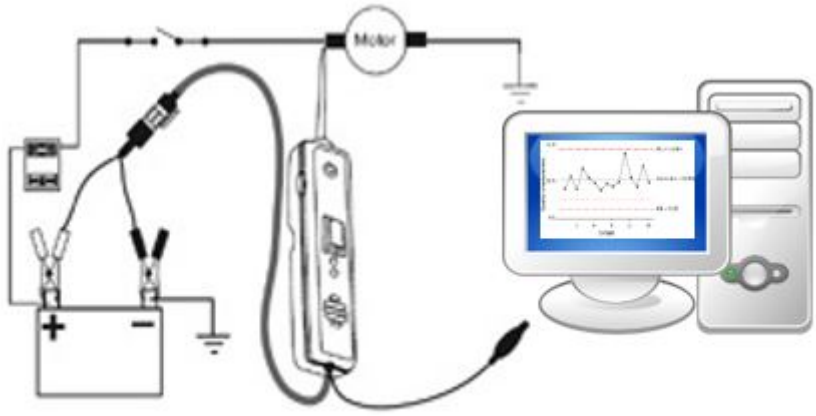
Production Part Approval Process (PPAP) Process Validation and Finished Good Testing. Black and White Box Testing Incoming Inspection Verification Label Verification Supplier Verification

The use of standards for quality measurement and data transmission should also be included in the verification so that a known reference can be attributed to the results. As stated before there are very few government standards for this product type however there are several industry standards that are helpful to ensure security of devices (Borrelli, 2001; Christoph Eckstein, 2014; National Institute of Standards and Technology, 2017), gateways (Mukherjee, 2016), networks(CISCO, 2006), applications (Quirolgico, Voas, Karygiannis, Michael, & Scarfone, 2015) and websites(Rescorla, 2008).

Subassembly

When two or more components are attached they are often tested to ensure that they were assembled properly and that together they meet the system requirements. This is frequently done in-line before being included in the final product assembly. This in-line testing is primarily a cost savings activity that identifies issues early and supports the manufacturing teams goal of a profitable manufacturing process (company shareholder requirement). A subassembly for example, might include a piece of software that goes onto a circuit board that is connected by wires to a small motor. In this case, in-line testing will to ensure a signal on the board triggers the software to activate the motor, thereby verifying the subassembly has been designed and manufactured to meet the intended system requirements. The verification and validation activities that would be required in this case would be a test equipment and test method validation.

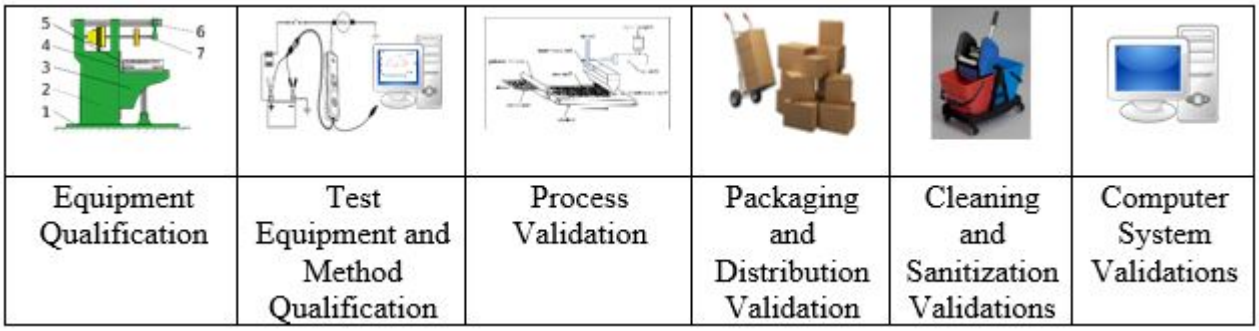
Figure 3: Inline test equipment and test method validation.



Final Product Assembly

The assembly of the product is often attained by joining several subassemblies and components together in a manufacturing process. The product will contain all appropriate software, hardware, system settings, and accessories needed to meet the customer requirements. The finished product unit will then be tested at the end of the manufacturing process using test equipment (that of course has been validated) to ensure that the product meets specifications.
Once assembled, the units will be placed in the appropriate display and shipping packaging and labeled according to specific requirements applicable to the product type and market of distribution (packaging and distribution validation). Associated GMP documentation will be assembled in a Device History Record (if applicable) and a product release processes will be utilized.
The validation of the Final Product Assembly process including the testing and packaging process is conducted over time to ensure that the process consistently produces product that meets specification (process validation). If the connected device Final Product Assembly includes computer systems or a chemical process then the appropriate Computer, Cleaning and/or Sanitation validations would also be conducted.

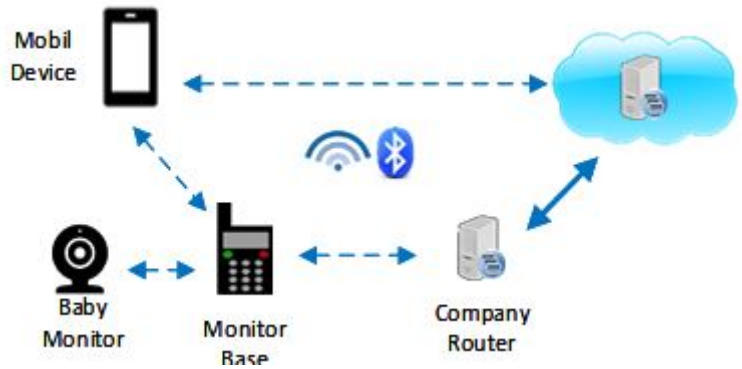
Figure 4: Subassembly and Final Product Assmebly Verification and Validation Activities



Mobile Application

Mobile applications have a development process as described in the component section that includes black and white box testing, however the application cannot be assured to meet the customer requirements unless it is proven to function with the unit. Typically, the validation process for a Mobile Application includes units that are proven to be controlled by the mobile application. In this case software developers will create various use cases and operating environments based on the customer requirements. The mobile application would then be tested and expected to meet predetermined outcomes as it controlled the unit, displays and shared the data. Once the verification was successfully completed then the application would be released to be uploaded to the deployment tool for distribution to the user.

Figure 4.1: Web Application Verification and Validation Activities



Customer Use

The rubber meets the road when the product, or in this case, the connected device system is used by the customer in their intended environment. Companies need to simulate the customer experience prior to product distribution to detect any issues early. The validation that customer requirements will be met with the final connected device system is often done through distinct types of testing depending on the current user practices. Referencing back to the customer groups that were identified in the initial validation process description you can see how they will need different methods of requirement validation.

- End customer Validation can be done with a panel of potential product users, that receive the product in the same manner they would receive from their distribution source. They should be monitored for their product experience without coaching to ensure that the instructions, software, and product functions as intended.
- Customer service and repair groups should be monitored to ensure that they are receiving intended information from

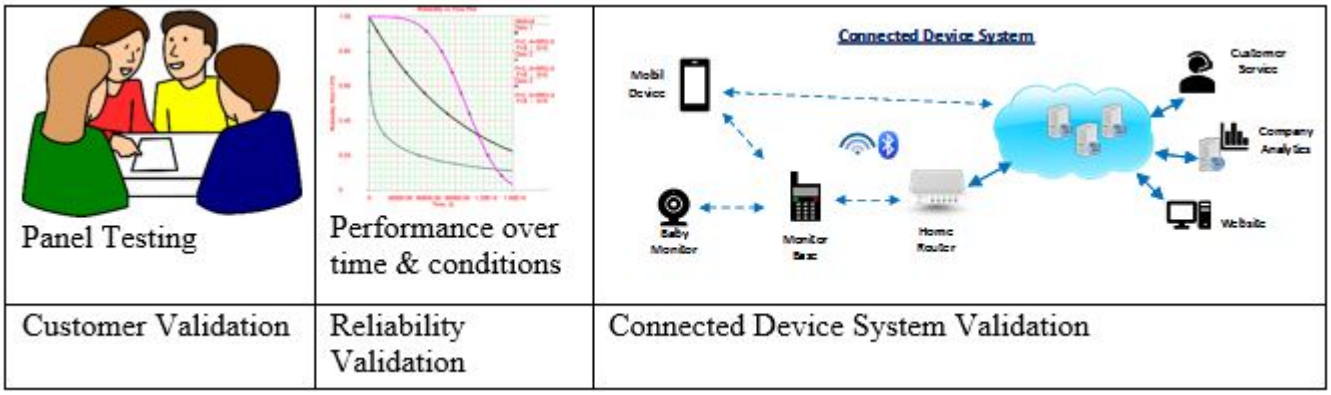
the device to support the service and repair calls.

- Marketing, sales and product development organizations should be interviewed to ensure that the flow of data they are receiving from the connected device system is meeting their intended use requirements.
- Company shareholders requirements can be evaluated from sales and revenue data obtained. There may also be other less tangible goals that can be evaluated associated with market share and product leadership. All of these requirements should be evaluated to see if the project has been successful.

Reliability Validation of the connected device system supports many of the customer requirements and is usually measured through accelerated processes in order to predict product performance. The testing protocol needs to be written to ensure that the entire system works properly over a range of environmental factors, use rates and over the life of the product. Reliability validation should be conducted to ensure that the customer requirements continue to be met over the extended use of the product.

System Validation is a process that includes as many variations as possible in connections and components that might be used by the end consumer to ensure that all groups continue to receive the results they expect. For example, variations in mobile devices, internet service, router connections and website browsers.

Figure 5: Customer Use Validation



Validation Types Performed Relative to Connected Systems

The results of the multi industry survey indicate that there is no specific set of validation types that are always used. As a matter of fact, it seems all validation types are used at one point or another depending on the components and function of the connected device. Quality and IT professionals were asked about the types validation they used for their connected device. The table below shows the percent each of the validation types are being utilized by industry.

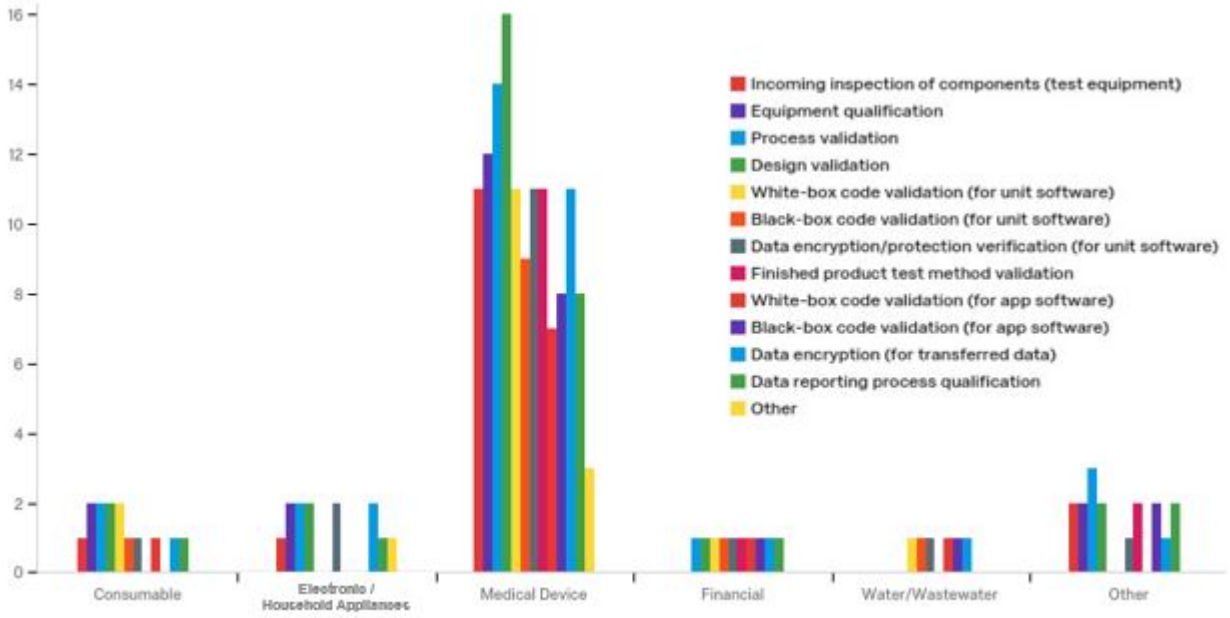
Table 2: Industry Survey Results on Validation and Verification Activities

Verification and Validation Activities Utilized	%
Design validation	77%
Process validation	73%
Equipment qualification	60%
Data encryption (for transferred data)	57%
Data encryption/protection verification (for unit software)	57%
Incoming inspection of components (test equipment)	50%
White-box code validation (for unit software)	50%
Finished product test method validation	47%
Data reporting process qualification	47%
Black-box code validation (for unit software)	40%
Black-box code validation (for app software)	40%
White-box code validation (for app software)	33%
Other	13%

?

Apart from the automotive industry that primarily relies on data integration verification, all other industries responding to this survey indicate that they use all of these validation verification types. The graph below shows the validation types are uniformly used across the industries. It should be noted that there is no industry relying solely on a single type of validation.

Figure 6: Verification and Validation Types by Industry



Common failures during system validation

The value of a system validation is the confirmation through objective evidence that the customer needs have been met. This is an important business activity, independent of regulations, because it just makes business sense to release products to the market that meet the customer needs. The goal of the system validation designer is to create a thorough set of tests that challenge the connected device system. What makes this work so difficult is that the designer needs to predict the combinations of components that will be used with the system when the customer has flexibility to choose many of the components of the system. Responses from the industry survey about the common failure modes seen during the system validation include those listed in the table below.

Table 3: Common Failures During System Validation

What are the most common failures during system validation for your connected devices?

What are the most common failures during system validation for your connected devices?
Incorrect user input (unintentional errors)
Data Reporting
Errors in calls to databases and services.
Network Configuration Issues
Network Disconnects.
Equipment Malfunctions
Software
Usability testing in association with cultural norms and multiple languages.
Coding Errors, Lack of testing against end to end infrastructure, Unidentified Updates/modification to iOS
Lack of formal and standardized approach within the organization
Data integration with other data sources.
Coding Errors
Packet Contention
Effects of heavy magnetic fields (near MRI, etc.)
Wall Shielding
Memory Management Issues
Lack of well-defined software or system requirements
The need to test multiple platforms and interconnections

?

Changes to Connected Device Systems

Most products are upgraded or evolve over time based on obsolescence, upgrades in software or upgrades in features, therefore a system validation may need to be repeated to ensure that as these changes occur the customer requirements continue to be met. The communication of changes and assessment of when revalidation is needed is often managed through a change control process.

Connected Device Change Control Processes

The function of a change control process is to ensure that all proposed changes are evaluated for their impact to the customer requirements prior to being implemented into production. If a component (software, platform, electronic or hardware) needs to be changed a team of subject matter experts should review change and the master validation plan for the system to evaluate the impact of the change to the previously executed validation activities.

The master validation plan contains several types of validations and it may not be necessary to repeat all of them. Instead, it may be possible to localize the revalidation efforts to those that tests the potentially impacted customer requirements. In most cases it will still be necessary to repeat at least in part the system validation to ensure that the connected device system still works as intended.

Backward compatibility will be an issue that is addressed in the change assessment to ensure that units that are currently in the market continue to function as intended and/or receive the intended update via the change process. Backward compatibility is often a separate set of tests that need to be conducted with units that are maintained at their historic deployment condition.

The industry survey that was conducted included questions about the type and formality of the change control process that companies utilize for their connected devices. It appears that in most industries a formal change control process is followed however there is flexibility in those business with lower levels of regulatory scrutiny.

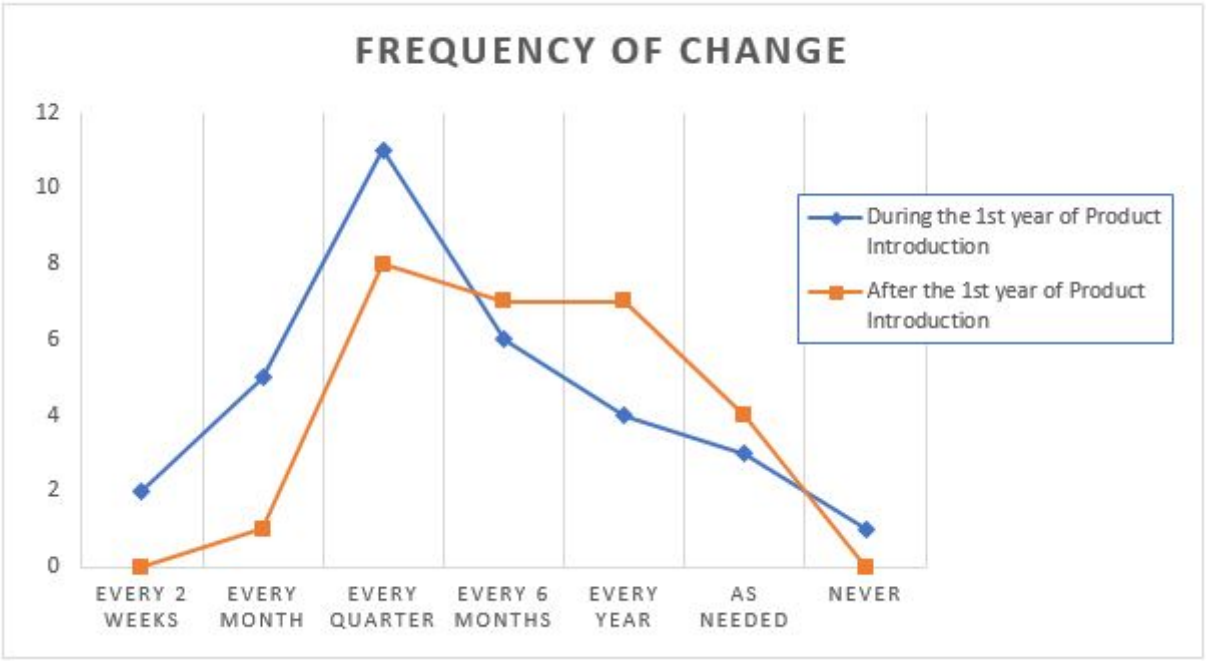
Table 4: Change Control Process Formality by Industry

Product Type	Informal	Formal
Medical Device		14
Consumable		4
Electronic / Household Appliance	1	1
Drug-Device Connected devices (e.g., web-based apps)		1
Pharmaceuticals - use of devices in R&D operations		1
Water/Wastewater		1
Automotive	1	
Financial		1

Frequency of change

Ensuring high quality software changes is a universal requirement that all industries. The question is how often should changes be expected in a connected device? And is there a pattern based on product age or product type? Well the industry assessment that was conducted indicates that the frequency of changes can be as often as every 2 weeks in the first year of the product's life and then depending on the product type may continue at that rate or decrease frequency to every quarter or every year. You might think that the regulated medical device area has a lower frequency than the other product categories or that over-the-air-updates of software increase the change rate but in reality the frequency of change depends on the need of the product.

Figure 7: Connected Device Change Frequency based on Product Launch Date



The key take-away is that changes in connected device systems is inevitable so a robust change control and deployment process is critical to ensure that the customer needs continue to be met through the life of the product.

Security of Connected Device Software

Once the connected device system validation is completed and deployment of the product to the market has occurred it is critical that the software and its data stream be secure from unintended access and change. This is where the connected device security plan is critical and should include a:

- Secure development software storage systems
- Software encryption that requires authentication
- Use of Secure Sockets Layer if using WIFI for over-the-air downloads(Administrator, 2005)

Enhancing the Customer Experience with Connected Device Systems

Referencing once again, to the customer groups, there will be requirements for the connected device system to transmit data to the:

- End customer that purchases the product;
- Customer service and repair groups that support the product throughout its life;
- Marketing, sales and product development organizations that could benefit from use patterns and consumable sales knowledge;

The data requirement that each group needs should be clarified in a measurable way so that the development team can configure the software and the system validation can be written.

The survey of various industries indicates that those companies with connected device systems are using the data in the following ways:

- Sending it to the customer for display on their mobile device
- Customer feedback and unit data provided to the development team allows for improvements in software to meet customer expectations.
- Tracking of unit and its performance.
- Customer Service can troubleshoot issues with the device to obtain both unit event information and data handling issues.
- Marketing and Sales can send and receive customer feedback surveys.
- Customer can review and analyze data as well as update the device with applicable information using their mobile device.
- Medical personal can monitor medical devices that have been implanted in people remotely. Reduces customer office visits and patient costs.
- Allows for increased process control optimization within manufacturing facilities.
- Increased communication and efficiencies for the sales force in companies.
- Support patient adherence (i.e., remind patients of need to take medication and/or of upcoming medical appointments);
- Provide training on how to use the device or prepare the medication;
- Record key vital health signs or symptoms that the patient can track over time and share with his/her healthcare professional; and,
- Educate the patient and/or healthcare professional regarding the drug product (e.g., risks, benefits, how to take it, interactions with other medications).

How is “Big Brother” perception handled with connected devices

The increased level of transmitted data by connected devices may cause concern for some customers that their privacy is being exploited. This concern can be escalated if they are receiving unsolicited contact from companies that have access to the performance of their connected device. The value of the proactive contact is high for the company and the medical community however privacy needs to be maintained for the consumer. The industry survey revealed that 68% of respondents do make proactive contact with their consumer based on their devices’ transmitted data. Industry was also queried about how the privacy issue was handled to reduce the “Big Brother” anxiety. Some of the ways this concerned is addressed include:

- Emphasizing the importance of understanding the system and network status information
- Discuss the advantages and security protocols
- For many patients, this concern is balanced against the time and energy to come into the physician's office. The benefits of time and energy savings generally far outweigh the "Big Brother" perception.

- Customers are informed that data is used for product monitoring, not people monitoring.
- Security awareness and training - security culture development
- Very clearly explained expectations. Transparency on device management.

Regulations and Standards for Connected Devices Systems

Regulations and standards are created by government agencies or standards bodies to 1.) provide assurance of quality and 2.) to document a minimum set of practices for manufacturing, testing and/or quality. Regulations are laws that government agencies require their manufacturers and distributors follow if they intend to sell products within their country. In contrast standards are created by volunteers at standards organizations that specialize in the field and understand the best and most economical way for things to be done. Standards are not laws however many government agencies require that certain standards be followed in addition to the regulations.

Connected devices are sold in nearly every country in the world however the development of regulations for connected devices is relatively rare in comparison to the pharmaceutical or medical device industries. In general, government agencies have placed more effort in the creation of regulations for the higher public risk product categories. This doesn't minimize the need for standards in the connected device industry therefor international standards groups have attempted to meet this need.

Table 5: Connected Device System Regulations and Standards

Standard/Regulation	Product Category
ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements	All
ISO/IEC 27013 Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	All
ISO/IEC 27003:2017 Information technology -- Security techniques -- Information security management system implementation guidance	All
NIST Special Publication 800-121 Revision 2 - Guide to Bluetooth Security	All
NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations	All
NIST Special Publication.800-163 Vetting the Security of Mobile Applications	All
AAMI TIR 57:2016 Principles for medical device security—Risk management	Medical Device
AAMI TIR 45: 2012 Guidance on the use of AGILE practices in the development of Medical Device Software	Medical Device
FDA Guidance Postmarket Management of Cybersecurity in Medical Devices	Medical Device
FDA Fact Sheet - FDA's role in Medical Device Cybersecurity	Medical Device
FDA Cybersecurity Website page	Medical Device
FDA Guidance Off-The-Shelf Software use in Medical Devices	Medical Device
FDA Guidance Mobile Medical Applications	Medical Apps
FDA Guidance Medical Device Data Systems, Medical Image Storage Devices and Medical Image Communication Devices	Medical Device
FDA Guidance General Principals of Software Validation: Final Guidance for Industry and FDA Staff	All
IEEE 802.3 Cyclic Redundancy Check	All
The Transport Layer Security (TLS) Protocol Version 1.2	All
European Commission Green Paper on mobile Health ("mHealth")	Medical Apps
EU Regulation 2017/746 In Vitro Diagnostic Medical Devices	Medical Device
EU Regulation 2017/745 Medical Devices	Medical Device

Conclusion

When you examine the rate of change in the connected device market it really is no surprise that the regulatory authorities are lagging in the area of regulation and guidance development for this product category. Embedded medical device software and patient record security are the only areas that the FDA and EU have established significant government expectations. Fortunately, there have not been serious health crisis, data security issues or outcries for public safety regulations in this area

so it seems acceptable that governments are allow industry to move forward developing their own standards for best practices. Organizations like AAMI, ISO, NIST IEEE have all stepped forward and created specific and industry guidance's that together have been able to piece together a controlled, secure and effective connected device market that makes business sense.

The industry survey that was conducted indicates that companies are in the practice of performing connected device system validation and in most cases the Quality Assurance or the Validation departments are leading this overall effort. The primary components of the system validation are driven not by the industry category, but by the product components and their backward compatability, this coincidently demonstrates a risk based approach to the validation process, which the FDA would recommend. As the connected device market evolves there are sure to be more product optimizations, not necessarily to satisfy a regulatory requirement, but more importantly, to satisfy the customer and shareholder expectations.

If there comes a time that governments feel the need to increase their regulatory oversight for connected devices then it would behoove them to look at these international standards first. It is likely that they will be able to spring board from these best practices to create regulations that ensure the markets are consistently developing products that meet high performance and safety standards.

References:

Administrator, S. c. (2005, 6/7/2005). What is SSL - Secure Sockets Layer. Retrieved from http://info.ssl.com/article.aspx?id=10241

Borrelli, C. (2001). IEEE 802.3 Cyclic Redundancy Check. *XILINX.* Retrieved from https://www.xilinx.com/support/documentation/application_notes/xapp209.pdf

Christoph Eckstein. (2014). Validating Security Configurations and Detecting Backdoors in New Network Devices. *SANS Institute Reading Room*. Retrieved from https://www.sans.org/reading-room/whitepapers/networkdevs/validating-sec...

CISCO. (2006). *Configuration Management: Best Practices White Paper*. Retrieved from http://www.cisco.com/c/en/us/support/docs/availability/high-availability...

European Commision. (2014). *GREEN PAPER on Mobile Health ("mHealth").*

European Commision. (2017a). *2017/745 Medical Device*. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2017:117:TOC.

European Commision. (2017b). *2017/746 for invitro diagnostic Medical Devices*. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2017:117:TOC.

FDA, U. (1999). *FDA Guidance Off-The-Shelf Software Use*.

FDA, U. (2002). *General Principals of Software Validation Final Guidance for Industry and FDA Staff.* Retrieved from https://www.fda.gov/medicaldevices/deviceregulationandguidance/guidanced....

FDA, U. (2015a). *FDA guidance Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices.* Retrieved from https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance....

FDA, U. (2015b). *FDA Guidance Mobile Medical Applications*. Retrieved from https://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf.

FDA, U. (2016). *FDA Guidance Post Market Management of Cybersecurity in Medical Devices*. Retrieved from https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance....

FDA, U. (2017a). FDA Cybersecurity Website page. Retrieved from https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

FDA, U. (2017b). *FDA Fact Sheet - FDA's role in Medical Device Cybersecurity.* Retrieved from https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf.

Jason Mann, D., Industry Product Management, SAS. (2015). *The Internet of Things: Opportunities and Applications across Industries.* Retrieved from International Institute for Analytics.: iianalytics.com

Mukherjee, A. G. J. P. a. A. (2016). *Design and build secure IoT solutions, Part 1_ Securing IoT devices and gateways*. *IBM developerWorks.* Retrieved from https://www.ibm.com/developerworks/library/iot-trs-secure-iot-solutions1...

National Institute of Standards and Technology, U. D. o. C. (2017). Guide to BluetoothSecurity (Vol. NIST Special Publication 800-121 Revision 2).

Quirolgico, S., Voas, J., Karygiannis, T., Michael, C., & Scarfone, K. (2015). NIST.SP.800-163 Vetting the Security of Mobile Applications. *National Institute of Standards and Technology*. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-163

Rescorla, T. D. a. E. (2008). The Transport Layer Security (TSL) Protocol Version 1-2 *Standards Track.*

Sherman, M. (2015). *The Medical Device Validation Handbook*. Rockville, MD: Regulatory Affairs Professionals Society.

Stevans, A. P., Justin. (2009). Validation Master Plans-Reader Q&A. *Journal of Validation Technology, 15*(Summer), 4.
