SIEMENS
Ingenuity for life

Testing the Internet of Things

This white paper discusses the key software challenges presented by the Internet of Things (IoT) and IoT-based products, and how best practices leveraging test management software can mitigate many of the issues with interconnected devices.

A white paper issued by: Siemens PLM Software

www.siemens.com/polarion

Contents

Executive summary

The Internet of Things (IoT) is already disrupting traditional business models. The Gartner information technology research and advisory company estimates that there will be 50 billion connected devices by 2020, which is probably a conservative estimate. From automobiles to light bulbs to smoke detectors, and even the watch you wear, devices may already be embedded with connected software. The rapid adoption and popularity of interconnected devices is creating multiple new opportunities and challenges.

This explosion of product releases in the IoT landscape has surpassed many software best practices normally implemented for traditional software development and testing. The industry is scrambling to catch up, and has been somewhat reactive rather than proactive in meeting these challenges. Never before have we seen so many product recalls and fixes that are directly the result of software issues, ranging from massive automotive recalls to replacement of everyday household items. Smart companies are aggressively seeking methods to address the challenges that now permeate most industries due to IoT. The challenges are serious, but not impossible to solve. Some have already been addressed during the rise in popularity of web-based applications, including security threats and privacy issues. But many critical issues remain, and most of these are software-based. As we move deeper into the "Internet of Everything," we must overcome these challenges using accelerated quality processes combined with exceptional software management.

In this whitepaper, we will discuss the key software challenges when dealing with IoT-based products and how best practices leveraging test management software can mitigate many of the issues with interconnected devices.

"The Internet of Things presents a significant mix of opportunity and risk."

John Dixon
Crunch Network

Addressing the challenges – the Internet of threats

We frequently hear news about software quality issues, ranging from automotive recalls to consumer home devices such as fire alarms not working properly. Since the advent of the Internet, where software is the key driver with anything connected, software engineers still face traditional software challenges:

Security
Unsurprisingly, given the rapid deployment of new devices, security is a fundamental issue with anything connected to the Internet. The shift to interconnected products across vast networks exposes once secure products to a variety of Internet vulnerabilities, ranging from malware cyber threats to privacy concerns. For example, many companies with existing products that are shifting to IoT have experienced threats and risks, or have been compromised in ways not initially anticipated. Secondly, the heavily data-driven nature of IoT products requires modifications to business processes: how we collect, test, analyze and manage data. Data privacy, and the lack thereof, is a primary concern when dealing with data-driven IoT devices. This can become a company's nightmare when customers' private information is compromised and released to the outside world. Unfortunately, there is no magic formula that can mitigate every possible cybersecurity risk. Risk management and intrusion detection methodologies should be incorporated into the overall development process.

70 percent of the most commonly used Internet of Things devices had serious security vulnerabilities

Source: HP Security Research

~500 billion devices will be hooked to the Internet by 2025

Source: CISCO

15 seconds to hack into Google's Nest Thermostat

Source: WeLiveSecurity

140 million records

This year alone, more than 530 security breaches have compromised more than 140 million records kept by credit card and insurance companies, hospitals, government agencies and others.

Source: University of Washington

Risk management

Managing risk is a common best practice in regulated industries such as automotive, medical device, pharmaceuticals and aerospace, and will need to be incorporated quickly and correctly when developing anything for IoT. Products that incorporate various sensors that constantly transmit data via the Internet at regular intervals can pose serious risks for end users. Besides security threats, software errors that cause catastrophic or fatal product malfunctions are a constant risk that must be identified and mitigated with appropriate actions to avoid such disasters.

For example, smart meters have been compromised in ways similar to any web-based application. A recent statewide implementation had major interruptions when the smart devices overheated: a remote connectivity feature did not disconnect, causing small fires and subsequent removal of all the devices in the field. The endless variations of IoT applications and devices pose a wide variety of risk-based challenges.

Quality assurance agility

Software inherently has defects, but with the explosion of interconnected devices fueled by customer expectations, software quality is imperative. End users expect IoT-based products to work as advertised and do not want to worry about security threats or the potential for product malfunctions. Compounded with elevated customer expectations is the evolution of software development, using rapid development methodologies such as Agile, Scrum and continuous delivery, which ultimately means that quality assurance (QA) departments must adopt accelerated testing processes while maintaining and even improving software quality. QA agility is not an easy task by any stretch of the imagination. The practice of QA agility – an incremental approach using smaller iterations with rapid feedback loops for improving quality – requires new tools and methods such as collaborative test case management with unified application lifecycle management (ALM).

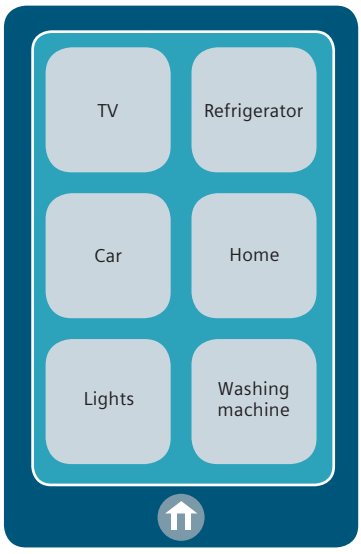
Knowledge and interoperability are also key QA challenges in the new world of IoT. Another consequence is the continual deluge of new and rapidly changing technologies, device protocols and other factors. Testing may be the glue that holds a product together, but it must be both a bonding adhesive for quality, and permeable for workflow interactions from various other software tool sets. Technology advances, combined with the lack of device standards and evolving tool sets, create a fluid testing recipe where many changes must be absorbed on a regular basis. Many of these can occur in real time and may require a lightning-fast response. The QA infrastructure should have the adaptability and flexibility to meet these ever-changing technology requirements.

An integrated test management approach

Meeting these challenges requires an end-to-end approach that encompasses a complete integration of the entire software development ecosystem: the ability to link and manage all processes throughout the entire development lifecycle, without compromising delivery schedules and quality, which is not an easy task. Complete integration also provides full visibility into all aspects of software projects, from creation of requirements, to test cases and management of defects. And finally, it provides an easy way to generate documentation for traceability, impact of changes and general information for various types of stakeholders, including the consumer.

Test management
Achieving and maintaining software quality while accelerating and improving the overall quality process requires some form of test management (TM) solution. A solution such as Polarion QA provides a central platform for managing all testing-related activities.

With IoT, software drives all product activities. However, software testing and quality are emerging as the primary focus in software development. Quality has never been more important in the production of products and their eventual outcomes. We now live in a world where common, everyday products are interconnected and controlled by software. You may get up in the morning and brush your teeth with a Bluetooth®-connected toothbrush that sends brushing data to your smartphone app; you drink coffee from a smart coffee maker, and then drive to work enjoying your infotainment system while your smart vehicle plans the route to avoid accidents and road construction; all of your health biometrics are analyzed by a wearable device that acts as a smartphone while you communicate with family and co-workers.



IoT: Internet of Things

Obviously, all of these common, everyday and now connected products must work correctly, reliably and, most importantly, safely. For all of these products, software testing must be done rigorously and efficiently to ensure that all expectations are not merely met, but exceeded. This cannot be achieved with one simple tool, or even a combination of disparate applications and testing processes.

Risk management
With IoT-related products, the concept of risk – already mandatory in regulated industries – must be incorporated into requirements elicitation. What risks are associated with the product? Is it at risk of malfunctioning and harming someone? Test management should support the mechanisms and processes for managing risk in your software project. Test management and its best practices perform the heavy lifting by testing risk-based requirements and recording the actual behavior. There must be a simple yet effective way to link and connect all testing artifacts to the original requirements and the actual outcomes of executing risk-based test cases, including all related files, source control, links, images and documents.

Test management software should facilitate the entire process of managing risks and hazards associated with your product. When requirements are created it should be easy to link the corresponding risk-based test cases and the actual outcome of testing activities. You should be able to easily leverage the data that you gather from your customer base and incorporate the data into your test plan.

Traceability and workflow

A forensic-level audit trail from inception of requirements to execution of test cases is the critical foundation for developing IoT-based products. However, the nature of interconnected solutions requires rapid response times as well as multiple configurations to test and support. End users expect products to work according to specifications and have little tolerance for error. Brand loyalty is negligible, and as we continue to see in the news, product recalls can be disastrous to a corporation.

The testing ecosystem must be able to quickly respond when issues occur. It is far more cost-effective to address quality issues earlier in a project than to suffer the fallout resulting from a public failure. Collaboration is vital throughout the entire project. The ability to anticipate and manage change minimizes risk and becomes a competitive advantage. A test management solution should be flexible enough to manage issues at any time during the entire lifecycle of a product. Although prevention is highly desirable, the key is having the mechanisms in place to react as quickly as possible and the ability to trace the original source of issues and fix them accordingly. Workflow with email notifications and process rules such as escalation using project templates ensure that your process is correctly followed while keeping track of everything that happens.

Single source

With a great test management solution, all testing-related activities are managed centrally from a single source, even if external testing tools are employed for some testing functions. Managing issues quickly and effectively can only be achieved if all these activities are managed in a unified environment where all stakeholders can easily access relevant information. Most organizations function with multiple projects, software applications and configurations. It becomes critical to have the ability to view, manage and assess results from a single source. Polarion QA delivers 24/7 access from any web browser to everything in the testing ecosystem. From a prevention perspective, you can manage risks and address defects in real time as you develop your IoT release. When issues occur in the field, feedback can be captured instantaneously and addressed accordingly.

If we use the example of the smart meter, Polarion QA could have managed all test case scenarios and test execution results from any source with direct linking to the original requirements for verification and validation from a pre-release perspective.

Once the smart meter is deployed in the field, and when software-related problems occur, issues can be automatically generated, prioritized and linked to the directly affected source files. A combination of quality prevention with an efficient reaction process, managed from a single QA source, could have mitigated some of the serious issues.

The future

We are now in a transition phase where software increasingly controls everyday devices and drives innovation. Some of the fallout from poor software quality has already impacted the consumer landscape with results ranging from simply annoying to devastating. The business community is only now beginning to recognize the need for an adaptable and comprehensive software quality strategy for the IoT industry.

Current practices for IoT software testing are not sustainable. Luckily, the impact to date has been mostly on perception and not always physically harmful. However, there have been impacts on company revenue, and there is a growing probability that harm may occur.

Users do not care why an app fails in the connected chain. As they become increasingly accustomed to connected devices and IoT, they will expect the new technology and apps to work flawlessly from the start.

Software quality must be managed effectively in real time without compromising value and delivery. This is only achievable through a truly integrated testing ecosystem that focuses on risks, with complete transparency of all testing-related activities. Companies that focus on quality will ultimately be the winners.

Siemens PLM Software

Headquarters
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

Americas
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

Europe
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

Asia-Pacific
Suites 4301-4302, 43/F
AIA Kowloon Tower,
Landmark East
100 How Ming Street
Kwun Tong, Kowloon
Hong Kong
+852 2230 3308

About Siemens PLM Software

Siemens PLM Software, a business unit of the Siemens Digital Factory Division, is a leading global provider of product lifecycle management (PLM) and manufacturing operations management (MOM) software, systems and services with over 15 million licensed seats and more than 140,000 customers worldwide. Headquartered in Plano, Texas, Siemens PLM Software works collaboratively with its customers to provide industry software solutions that help companies everywhere achieve a sustainable competitive advantage by making real the innovations that matter. For more information on Siemens PLM Software products and services, visit www.siemens.com/plm.

www.siemens.com/plm

55651-A4 7/16 F