SIEMENS
Ingenuity for life

Testing the Internet of Things 2.0

Opportunities and challenges of the Industrial Internet of Things

This white paper is a continuance of the white paper "Testing the Internet of Things," discussing the key software challenges presented in the development of IoT devices, and how best practices can be leveraged to mitigate many of the challenges faced throughout the product lifecycle.

A white paper issued by: Siemens PLM Software

www.siemens.com/polarion

Contents

Executive summary

As the buzz surrounding the "Internet of Things" (IoT) starts to subside we now are beginning to see the evolution as well as the fallout from everything connected. There are currently more than 12 billion devices connected to the internet, and that number is projected to double within four years. IoT has been most pervasive in consumer goods such as wearable tech and home automation; however, industrial applications are where the true benefits of interconnectivity have been seen. It has been estimated that manufacturing companies worldwide will spend $500 billion annually by 2020 on Industrial Internet of Things (IIoT) technologies and that the value generated by the IIoT will reach a staggering $15 trillion per year by 2030.

This white paper reexamines the emerging software opportunities and challenges associated with IIoT and focuses on how technology and software testing plays a critical role in developing an interconnected product.

"By 2018, mobile phones are expected to be surpassed by IoT devices, including connected cars, machines, utility meters, remote metering and consumer electronics. The number of IoT devices is expected to grow at a compound annual growth rate (CAGR) of over 20 percent between 2016 and 2022. By 2022, the number of connected devices is expected to reach 29 billion."

Ericsson Mobility Report: On the Pulse of the Networked Society, June 2016

Security threats are rising in the age of the Internet of Things

According to the 2016 Norton Cyber Security Insights Report released by the technology company Symantec, 689 million people across 21 countries were affected by cybercrimes last year.

Dealing with cybersecurity should be a top priority for software development. Software security hasn't been inherently designed within most IIoT devices. With the advent of new vulnerable devices now being put into service, 2017 will see hackers continue to exploit IIoT systems. In 2016, the largest distributed denial of service (DDoS) attack disrupted the internet using a weapon called the Mirai botnet which comprised of an array of internet-enabled devices and saw the rise of a new method for hackers to exploit and access personal and financial information. Expect even more large scale breaches as hackers look for newly connected devices, especially in the energy and transportation sectors where the largest disruption could occur.

Prevention is key

In 2016 there were some major announcements, such as the Industrial Internet Consortium releasing its security framework. However, building a highly secure device is not easy, especially in complex environments, and it is not enough to deal with problems as they become apparent. Prevention is key to experiencing flawless software and getting the most out of systems, applications and your development teams. Exposing unnoticeable weaknesses in an infrastructure by using dependable software risk analysis solutions ensures the proper identification of threats, vulnerabilities and security flaws.

Several great security-related software solutions are available that should be incorporated into your testing arsenal. Ultimately, companies need to implement and identify security vulnerability/threat use cases that can be incorporated into the product development lifecycle. Once companies create security requirements, they can create plausible test cases and continue to build a library of ever-expanding vulnerabilities and threats. Although not all-encompassing the following areas for security and privacy challenges should be included:

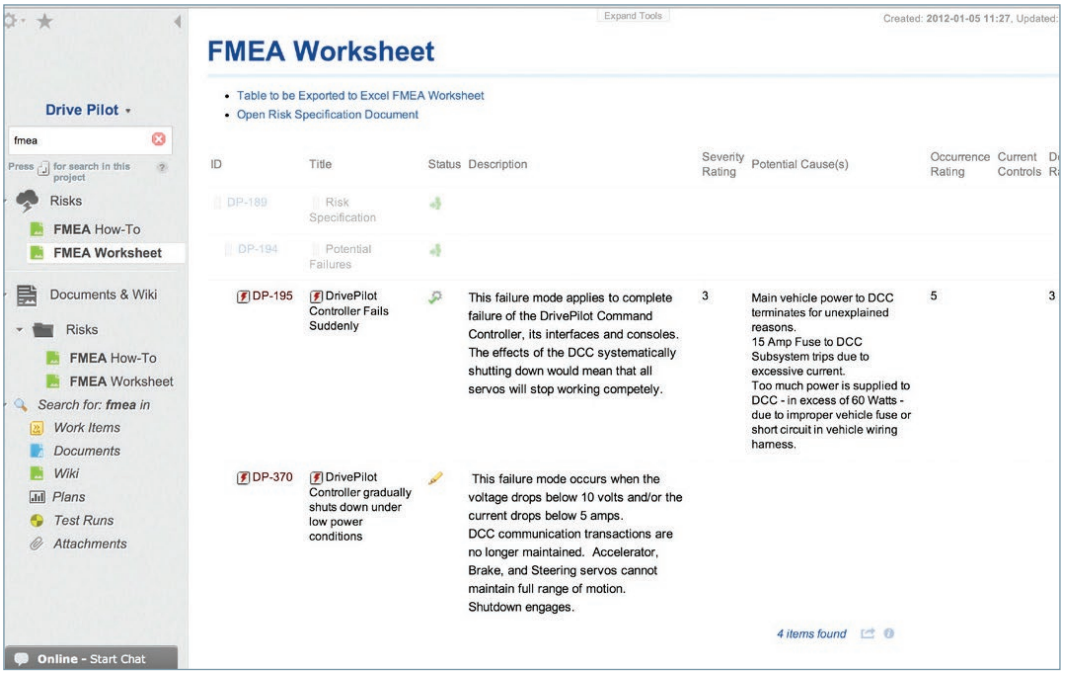
- Insufficient user authentication
- Poor or nonexistent data encryption
- Little or poor secure code practices
- Data privacy

For example, in the case of an IIoT automotive assembly line, several technology components are involved:

- Sensors in the vehicles
- Gateways
- Services
- Web interface
- Mobile interface

If we apply some form of threat assessment such as the STRIDE software approach that was developed by Microsoft to help answer the question "what can go wrong in this system we're working on?," we can identify the various attack scenarios and mitigation options for each of the components above.

Security constraints for IoT are so critical that analyst firm Gartner evaluates the worldwide spending for the IoT security market will reach $348 million for 2016, a rise of 23.7 percent from $281.5 million in 2015, and forecasts $547 million by 2018 (Forecast: IoT Security, Worldwide, 2016).



Regulations

With the merger of the Open Interconnect Consortium and the Allseen Alliance into the Open Connectivity Foundation, 2016 brought us a little closer to standards interoperability. There is still a long way to go for a cohesive standardization but regulations will follow. Prudent organizations are already starting to plan for this day by implementing flexible workflows. Risks increase when new regulations are introduced and IIoT manufacturers know only too well the risks of product delays and product recalls.

Governments globally are starting to focus on IIoT based devices. There is even commonality with emphasis being placed on loss of privacy and data protection. Any new solution should include various integrated solutions and will require standards. The IIoT industry may be the beneficiary, but it is not unrealistic to expect that there will be different regulations in different jurisdictions, just as with the cloud, data privacy and other technologies. This diversity will generate risk and additional complexity.

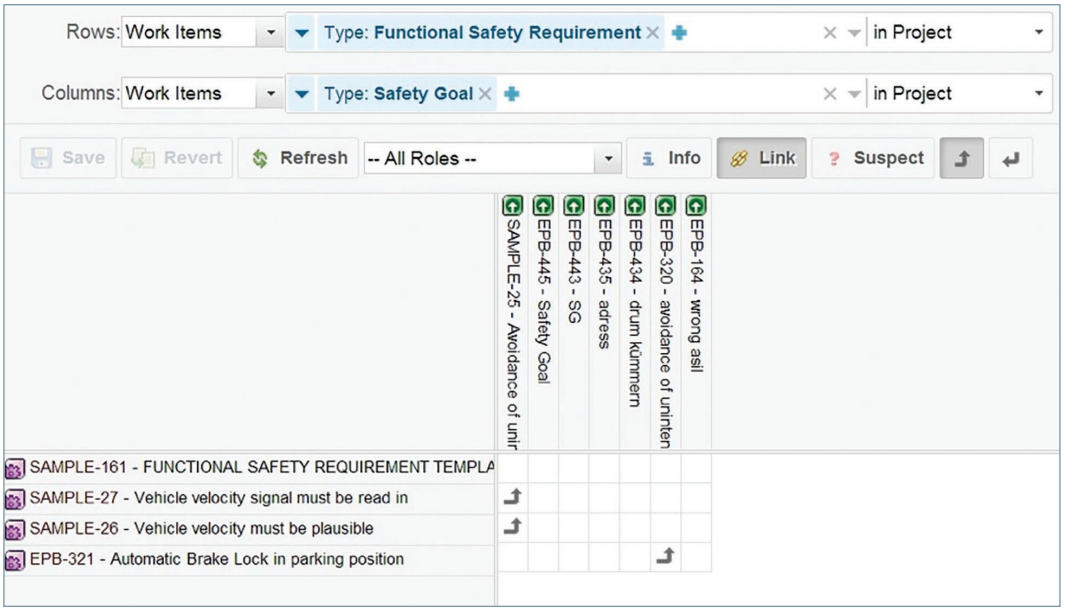
"If we want to secure our increasingly computerized and connected world, we need more government involvement in the security of the 'Internet of Things' and increased regulation of what are now critical and life-threatening technologies. It's no longer a question of if, it's a question of when."

Bruce Schneier, Security Technologist
"Your WiFi-connected Thermostat Can Take Down The Whole Internet. We Need New Regulations"
Washington Post, November 3, 2016

Incorporate regulations without missing a step

The design of Polarion QA™ software from Siemens PLM Software enables risk and compliance departments to execute their methodologies with confidence, with complete visibility and traceability from requirements to the detailed lines of code. With its unique framework capabilities and customizable workflow-based approach, Polarion QA provides a pragmatic and highly configurable software solution to support any organization's compliance process.

The impact of regulatory requirements on product design and development can be assessed only if there is clear visibility into how each requirement will affect the scope and complexity of development. The bottom line is that companies need to know the impact of each new regulation and how it affects product design and development.



Silos

"Perhaps the hardest challenge to overcome is that of breaking silos between different disciplines and departments," notes Gary Mitchell, an industry-leading writer on automation, control, software, manufacturing, marketing and leadership.

Bridging the gaps that divide us

Information Technology (IT) and Operational Technology (OT) departments should be reviewing current business practices and operational systems in an effort to bring together the IIoT components and back-end facilities to streamline standard operations and problem resolution. A unified communications infrastructure can supply the tools needed to move ahead of the competition.

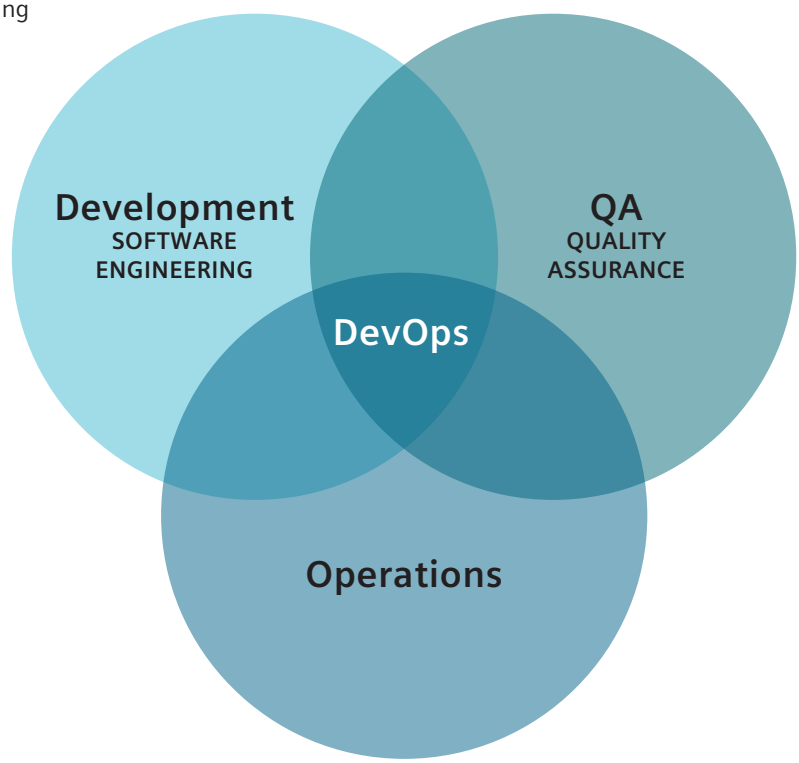
DevOps integrates IT with software development, and is dedicated to maximizing efficiencies during the entire service lifecycle, from design through to development to production to support using various techniques known as Agile operations.

How does this help in bridging the proverbial gap? It provides a methodology for creating a relationship between IT and development, and if done properly advocates an Agile relationship. A key goal of DevOps is to change and improve the cross-disciplinary relationships by advocating better communication and collaboration between the IT and development business units. Secondly, it provides a mix of tools that facilitate continuous testing and instant notification of testing results.

Developers and testers need to be able to rapidly create production-like environments to deploy, test and experiment with code and application changes. This capability is facilitated through Platform as a Service (PaaS) technology using tools such as Red Hat® OpenShift Container Platform (OCP).

Eliminating silos between groups can be seamless by leveraging the right combination of technology, using instant communication, social forums, push notifications and anything else that fosters passive collaboration. Collaboration isn't just about communication between geographically dispersed teams, it is knowing what is going on and who is doing what at any given time through the entire testing/development process.

Polarion QA enables teams to collaborate on shared assets easily and securely. You can control who can see what, who can change what, and when via granular permission controls and robust configurable workflow automation.



Quality is key

The design and delivery nature of IIoT promotes rapid product development. This fosters small nimble teams who collaborate online, using web-based tools that are not only intuitive but also cost-effective, resulting in rapid product development. This quick turnaround requires the ability to secure code without slowing down development, the integration of various testing tools and processes are essential. Like any competitive industry, the goal is to produce functioning solutions that can be released as quickly as possible. However the greater challenge faced is that IIoT (and IoT at large) introduces a variety of quality challenges. As mentioned, quality is at the top of the list and it feels like every day a major security breach or recall is making the headlines - from cars to garage doors to Barbie dolls.

Security testing, as mentioned, is an absolute priority within IIoT solutions and must be inherently adopted through the entire development process, starting with secure code practices, vulnerability and threat modeling, traditional and automated testing while using continuous testing practices.

Ensuring privacy of customer data has always been a major software issue. Organizations must emphasize a privacy-focused strategy for planning, testing and development. For example, regulated industries such as medical know that the stakes are very high, and should focus testing on access control, data encryption, structured data and even data sanitization. This is all the more reason to place priority on your software testing strategy.

DevOps encourages testing in all phases of development and deployment. The main goal of DevOps is to the release highest quality product as fast as possible. Quality is a culture built into the fabric of DevOps.

These three conditions further place QA in a critical role in the organizational structure because they emphasize direct responsibility on quality throughout the entire product development process.

The very nature of these workflow conditions can create software quality issues. The pressure to release functional product that includes hardware and embedded software puts excessive demands on quality assurance departments. Industrial and infrastructure use demands that software is released at hyper speed but the caveat is an expectation that critical products and systems must work as intended, and are continually updated without disruption.

IIoT use case and the importance of software testing

With automation and connectivity, manufacturing has become leaner and more flexible, and provides the added advantage to mass customize products. The manufacturing process is now driven using software that allows activities to be fully integrated into the development process in ways that simply didn't exist before. Connectivity creates complete visibility into all processes, ranging from logistics to quality control. Quality has never been more important, now that connectivity dominates many industries. We expect products to work according to spec without disruption or error.

The medical industry, for example, is adopting connectivity with mass customization. Healthcare is a leader in adopting IoT and is expecting tremendous benefits with wireless monitoring, wearable tech and general connectivity. We now have medical devices that are capable of transmitting vital patient data from anywhere to medical staff. These devices are capable of transmitting data such as heart rate, blood pressure, oxygen saturation, etc., all in real time. The highly regulated nature of the medical industry creates significant challenges for quality assurance departments when handling, processing and transmitting real-time patient data. There are multiple security and data privacy concerns as well as the obvious expectation that potentially life-threatening devices must work correctly and accurately. The good news is that the concerns can be addressed using the following testing practices:

- Leveraging big data from actual production in real time can significantly increase efficiency and quality by improving requirements and your testing process with real-world user behavior.
- Defects can be reported and analyzed in real time with a thorough impact analysis.
- Field results can be incorporated into production-level software processes and continuously tested.
- Performance and reliability can be measured and monitored with rigorous testing using automation.
- The ubiquity of wireless networks and the increase of mobile data means that a comprehensive security plan must be implemented.

The end result is that product recalls are far more likely to be avoided, as all the components and processes of the entire system get integrated, transparent, and automated.

Polarion QA solution

Traditional software testing/QA models are evolving along with IIoT. The QA team must now focus on usability testing, simulating the environment where the device is to be used. This must be done to ensure that information is exchanged in a secure manner and devices are performing in a manner that fulfills service-level agreements. Leveraging technology is key to achieving these goals. We discussed a solution that combines a multitude of integrated software products and procedures. Polarion QA provides a centralized platform for managing the required software applications, using customizable workflows that support most DevOps and risk mitigation models. All of your testing pieces continue to interact accordingly and are coordinated based on need. For example, if you need to run a series of automated tests for performance, the series is launched using a scheduled job and once the process is complete, actual automated test results are captured, managed and stored in Polarion QA.

Final thoughts

The key challenges of developing secure IIoT solutions might seem daunting. However, the problems associated with device capabilities, supply chain concerns, security, divisions between people, and safety all ultimately demonstrate the extent to which departments, entire enterprises, and manufacturers must work together to navigate this new trend in technology going forward. In every case, there is a course of action available; it's simply up to companies to determine how they would like to proceed and what tools they choose to leverage.

To learn more about how Polarion QA™ from Siemens PLM Software can assist you to further protect and maximize your software investment, visit the Polarion Blog, or better yet 'Test Drive' Polarion QA™ Live for free.

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

61947-A3 3/17 B