WHITEPAPER

Testing the Internet of Things – Intelligence is Required

sqs.com

Authors: Colin Bull (Manufacturing Vertical Consultant)

SQS Group Limited UK

Sven Euteneuer (Global Head of Technical Quality)
Kai-Uwe Gawlik (Head of Service Management)

SQS Software Quality Systems AG Germany

Published: September 2016

Transforming the World Through Quality

COLIN BULL

Manufacturing Vertical Consultant
colin.bull@sqs.com

Colin is a product and manufacturing specialist. He has over 26 years of design, engineering and manufacturing experience, with over 16 years in the development and successful deployment of Product Lifecycle and Manufacturing Execution applications, within Automotive, Aerospace and Defence and consumer appliances. He joined SQS three years ago to lead the UK consultancy in the manufacturing vertical. He has a passion for quality delivery of PLM enterprise applications, MES and integration into ERP and CRM systems. Colin is part of the global consultancy team leading the iIoT and Smart Factory services and innovations.

SVEN EUTENEUER

Global Head of Technical Quality
sven.euteneuer@sqs.com

Sven Euteneuer graduated from the University of Bonn, majoring in Computer Science, and has been active in IT projects in various roles, with a focus on quality assurance, for over 18 years. After joining SQS as a Senior Consultant in 2007 he has delivered projects in the domain of technical quality for a wide range of customers. He is currently responsible for the portfolio of technical services.

KAI-UWE GAWLIK

Head of Service Management
kai-uwe.gawlik@sqs.com

Dr Kai-Uwe Gawlik is Head of SQS Group Service Management. He has 20 years' experience in project, quality and test management for small and large software development projects in SQS strategic industries. Company and technology change targeting corporate stakeholders, and development and improvement operations have been an ongoing focus of his consultancy work.

Contents

Management summary

Nowadays, many companies define their digital strategies to allow businesses to benefit from opportunities based on new technologies. These technologies consist of globally-interacting and partially autonomous systems (Internet of Things – IoT) continually gathering a huge amount of information (big data) for real-time control, user feedback and decision-making. The complexity and behaviour of such technology ecosystems reveals new types of risks and needs answers from quality management. In addition to an overview of quality challenges we will discuss how SQS test methodology (TRIP/TRIO), accompanied by Artificial Intelligence, provides a sustainable basis and an additional self-optimising mechanism for quality assurance. We take the IoT in manufacturing as our example for this overview; the principles are the same in other industries.

Keywords

IOT
ARTIFICIAL INTELLIGENCE
PROCESS BASED TESTING
INPUT OUTPUT BASED TESTING
TEST REPOSITORIES
CYBER PHYSICAL SYSTEMS

Introduction

The widespread adoption of IP-isation [1] of products known as the Internet of Things (IoT) is becoming embedded in our everyday lives. However, the quality risk of the IoT is physical. Unlike traditional software applications, IoT by its very nature is cyber-physical. This means that the interconnected pieces of software will interact with the physical world and this adds a different dimension to software quality. In this scenario, failure is not an option, or if failure could occur then a safe or controlled way of failing needs to be ensured. For many years, cars have had embedded software to run critical systems; the Mercedes C class runs 100 million lines of code [2] just to get it off the drive.

Safety-critical applications and software have traditionally been secure through their inherent lack of connectivity with the outside world, with information being provided by a distributed set of sensors on the product itself. However, the increase in the number of data points from other devices not in control of the device itself makes the quality of the software that performs safety-critical operations subject to outside influence.

Take, for example – although not safety-critical – Lexus software being damaged by a data load from an outside weather data provider, forcing the recall of thousands of units to have their software reinstalled to remove the inherent bug [3].

The IoT – a massive game changer disrupting the manufacturing industry

So, if IP-isation and the IoT add so many requirements that need to be considered, particularly with regard to their impact on safety, why has it already proven so successful in areas ranging from smart homes to cars, and from agriculture to manufacturing industries!

Let's have a look at manufacturing to understand the substantial positive impact of the IoT or, as some have termed it, the industrialised IoT (iIoT) and related developments on this industry.

Digital twin. Every product that is produced starts out as a digital model, and will have a physical representation or twin, for example, a car. The whole process of developing a new car starts with – physical sketches, drawings and clay models, but these are soon digitised to enable the digital development to continue: computer aided design and validation to ensure the car can meet requirements, manufacturing process definition via digital factory to ensure the car can be built, even servicing of the product in the field with VR and augmentation to ensure the car can be maintained. Each physical part of the product and organisation will be digitised, and vast amounts of digital data will be processed throughout the organisation and beyond.

Smart products and factories. With the digital twin and the seamless two-way data flow, coupled with the IoT, augmented operators, smart parts and products, big data and analytics, cloud and mobile capabilities, manufacturers are able to form a digital thread throughout the organisation and their supply chain. This data flow and analytics are enabling products and factories to become smarter and capable of making informed decisions autonomously, whilst at the same time allowing management to make informed decisions about the state of their organisation's performance and gain a real competitive advantage and even a novel edge in alternative revenue streams.

Convergence of information technology (IT) and operational technology (OT). Manufacturing organisations operate two main stakeholder communities that deploy software and technology. On the one side is IT, which typically manages and supports the business systems, infrastructure and architecture. On the other side are the operations technology teams, who support the factory operations systems, infrastructure and architecture. They both have similar objectives in keeping the business running, but with very different skill sets and requirements to achieve these objectives. However, this will have to change with the iIoT and the digital twin throughout the organisation. The IT and OT domains will have to converge to ensure that the value that can be gained from data and insights is actually achieved. The solution is to take a balanced approach to integrating information technology and operational technology to ensure that the objectives and capabilities of the data centre and the plant floor are met. An architecture similar to the one shown below illustrates the complex nature of such a structure in the future.

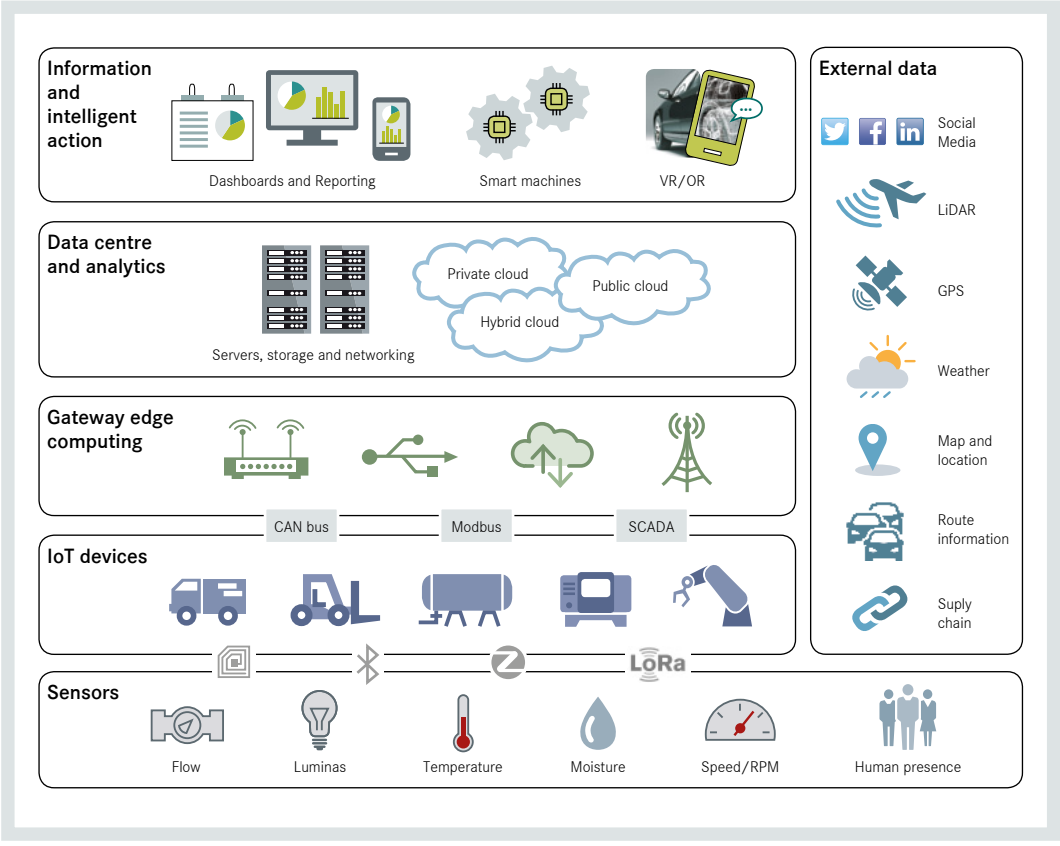

Figure 1: The IoT and its layers in a manufacturing environment

As can be seen from Figure 1, the iIoT architecture has many layers and starts with a sensor on a device. Each device may have many sensors to provide data to the gateway layer. Based on real time requirements, the gateway will process that data and pass information back to the device to perform an action, or the data will be communicated back to the data centre alongside many external data points for further processing and for insights and intelligent actions by the enterprise.

Data leads to intelligent actions – moving from analysis of what happened to predicting what will happen.

The IoT delivers a considerable amount of potential value to manufacturing – the ability to improve speed, cost and quality over a tactical layer, i.e. during day-to-day operations, such as decreasing the mean time required to transport raw materials to machines. At the same time, it offers the same potential over a strategic layer, i.e. being able to use the transparency gained through the collection and integration of data to take better and more accurate decisions.

Disruption requires a review of the way we produce and maintain software

Within manufacturing today, a number of disparate systems, silos of information sources and automation of business processes exist. These mainly consist of Product Lifecycle Management (PLM), Enterprise Resource Management (ERP) and Manufacturing Operations Management (MOM). This complexity is further increased when individual plants and supply chains also have their own information silos. All this data requires resource-intensive manual analysis and contextualisation to provide valuable and intelligent information to the various stakeholders within the business. To achieve even greater operational cost savings, these data silos require integration to form a constant digital thread across the enterprise before the enterprise can start to recognise the true value of the iIoT.

The iIoT changes the way that the product and the manufacturer interact and this means that the software must be able to achieve different requirements across the entire ecosystem and across all users. This leads to complexity in the stakeholder's view of the quality of the software providing data and driving processes across the organisation. There are four main areas where quality needs to be considered, and these are Machine to Human, Machine to Machine, Business to Business and Business to Customer.

1. **Machine to Human –** The end user has the ultimate perception of the quality of the product. Mechanically, the product could be of optimum quality and never require maintenance, except at the scheduled service interval; or as per the IoT and the predictive nature of maintenance, when the product tells you it's time to maintain. However, in the event of failure of the software that allows you to interact with the device, or allows other devices to connect, the product and the manufacturer would be perceived to be of poor quality. The user interfaces need to be managed focusing on the end user interacting with the device; the operator only requires the UI that is pertinent to their role, such as passenger, driver, machine operator, assembly operator, whereas a maintenance worker will require a UI that allows diagnostics capabilities, the same device with different roles.

1. **Machine to Machine –** By its very nature, the IoT world will encounter devices that will talk to other devices to provide data about the state of the:
   - Factory – Machines will be cognisant of the operational effectiveness of the whole cell, line or factory and supply chain, and able to make use of algorithms to enable autonomous decisions regarding what to route and where to, or even change processes to enable the production of, say, additional manufactured parts in real time. Machines will also be aware of their own health and process quality and able to make adjustments to achieve greater quality parts and stay on line to reduce downtime.
   - Roads and Infrastructure – The modern car today interacts remotely with the on-board information providing real time data on the car's immediate surroundings. This is evident today with Advanced Driver Assistance Systems (ADAS). However, in the connected car future, there will be external information systems providing the vehicle with data for autonomous decision-making, such as the approach speed to a junction to coordinate with a green light, other vehicles warning of poor road-holding due to ice or water on the road, corroborated by temperature and water sensors on the road surface and at local weather stations, reducing the vehicle's speed and adjusting the ride dynamics to suit the road conditions.
2. **Business to Business –** The value of the IoT lies in the fact that systems and devices will not be working in isolation from other systems. However, this involves a supply chain of software and data providers inputting directly to influence the devices' performance in the physical world. As with hardware, this added complexity means that the software quality must be inherent in the entire supply chain to meet the quality targets of the product owners.
3. **Business to Customer –** The IoT is an opportunity for product owners to continue their engagement with the customer long after the purchase of the product, delivering services and ultimately a continuous revenue stream. It will provide intelligence on how the customer perceives the product and how it is actually used, thus providing valuable feedback for ongoing development. This will drive improvements to features regularly used, and highlight new use cases and features. The IOT is also a seen as a game changer in the way the customer purchases products all together: rather than buying products, the customer buys a service. We can see the emergence of this today with car sharing instead of car ownership, for example the Uber, Lyft and VW mobility schemes.

Market analysis

With wearables and home automation making their mark in the consumer markets, it is estimated that the number of connected devices will grow to 21 billion by 2020, from approximately 6 billion in 2016 [4]. The value to business is worth trillions of dollars so there is a significant amount at stake. According to research by CISCO the overall value is $14.4 tn. However, fifty percent of that 14.4 tn will be realised by four main industries, who stand to gain the most out of the opportunity. Manufacturing with 27%, the retail trade with 11%, information services and finance with 9% combined [5]. Obviously manufacturing has the most at stake with an estimated $1.95 tn of value. The value is derived from smart factories and intelligent machine tools and assembly plant, and the opportunity is so great that this paper will concentrate on the industrial Internet of things – the iIoT – and its related use cases.

The focus of manufacturing is changing from a mechanical bias to one of software-driven hardware. This is evident today with one of the largest booths occupied by Microsoft at the Hannover Messe 2016. The Hannover Messe is the world's largest trade fair for manufacturing technology, and it is dominated by a software company, not an industrial giant like Siemens or General Electric.

The iIoT requires intelligence in quality assurance, and AI provides it

As we have seen, industrial processes of the future rely on autonomous, connected and intelligent machines, tools and devices. While central control will still be present, it will not wield as much influence or as tight a reign over the mechanical production stakeholders as it does today.

iIoT and Industry 4.0 – requirements for QA and testing

Ultimately, the requirements for implementing quality assurance and testing for such devices, machines and – in the end – integrated production or manufacturing systems in sectors ranging from agriculture to the automotive production floor, will differ from the very static and human-centric approach in place today. The focus will be much more heavily based on QA and testing and will be:

- Driven by data and configuration, not just code
- Integrated tightly with the machines and devices themselves
- Able to leverage whatever environments are available for the purposes of testing
- Proactive so that defect modes can be anticipated, much as the machines of today are programmed to recognise modes of wear and proactive maintenance
- Aware of the cyber-physical nature of the IoT

Let's take a typical manufacturing environment as an example, where production machines, warehouses and independent material transporters interact with each other to ensure smooth day-to-day operations. Their individual decisions are based on access to a wealth of sensor data, not just from themselves and not just current data, but the plethora of information available through big data including a pool of present and historic information.

An independent material transporter may have just delivered raw material to one machine and be free to transport another payload. Previously, a central logistics unit would have computed the optimal routing payload and routing. With the IOT, the transporter itself will be able to make that call based on the available information on material requirements from the machines, as well as on priorities, available material and the distances it will need to travel. At the same time, every transport order delivered will be added to its own set of data, improving its predictions of times needed, distances travelled, etc.

Obviously, such a highly complex, interactive and data-driven system is incompatible with a traditional approach towards testing. How would a classic test project ever be able to emulate the complex interactions of the production environment or be able to identify the crucial combinations of values in the big data base that trigger machine or device behaviour?

Managing complex IoT ecosystems in testing

This type of interaction involving partially autonomous systems requires different approaches, particularly for system integration testing.

Additionally, the physical behaviour (e.g. sensors) of some IoT components creates a wide variety of inputs influencing the system. Consequently, the number of possible test cases is extremely high, so high in fact that for manual test design and execution, stringent management of the combinatorial explosion is required and only few combinations actually make it into testing. Risk assessment is required in order to make this selection, and needs to be accompanied by the right methodology for test case specification, ideally based on SQS experience documented in our test repositories. In order to assure both functional and non-functional quality, the SQS approach provides two variants of test design methodology:

1. **TRIP: Test Repositories in Process Based Testing** – Repository-driven

   The requested functional and non-functional interaction of integrated IoT components based on a certain trigger can be documented using process documentation during the requirement specification phase. If projects are based on process models, the relevant quality assurance gives the following results:

a. Simulation: The requirements are validated by executing walkthroughs via processes. Besides correctness and completeness, information about actual need and suitability is derived. This is used to support final decision-making regarding the scope of implementation, risk mitigation and thus costs and time-to-market.

b. Test Case Generation: Complex scenarios documented by process descriptions can be enriched by test-relevant steps and information including the data to be simulated if IoT components are not available. From here, so-called test model test cases can be automatically generated by operating different data objects along possible paths through the test model. Test models and not test cases are the artefacts to be maintained and these form part of the SQS repositories. Testing is driven by these repositories.

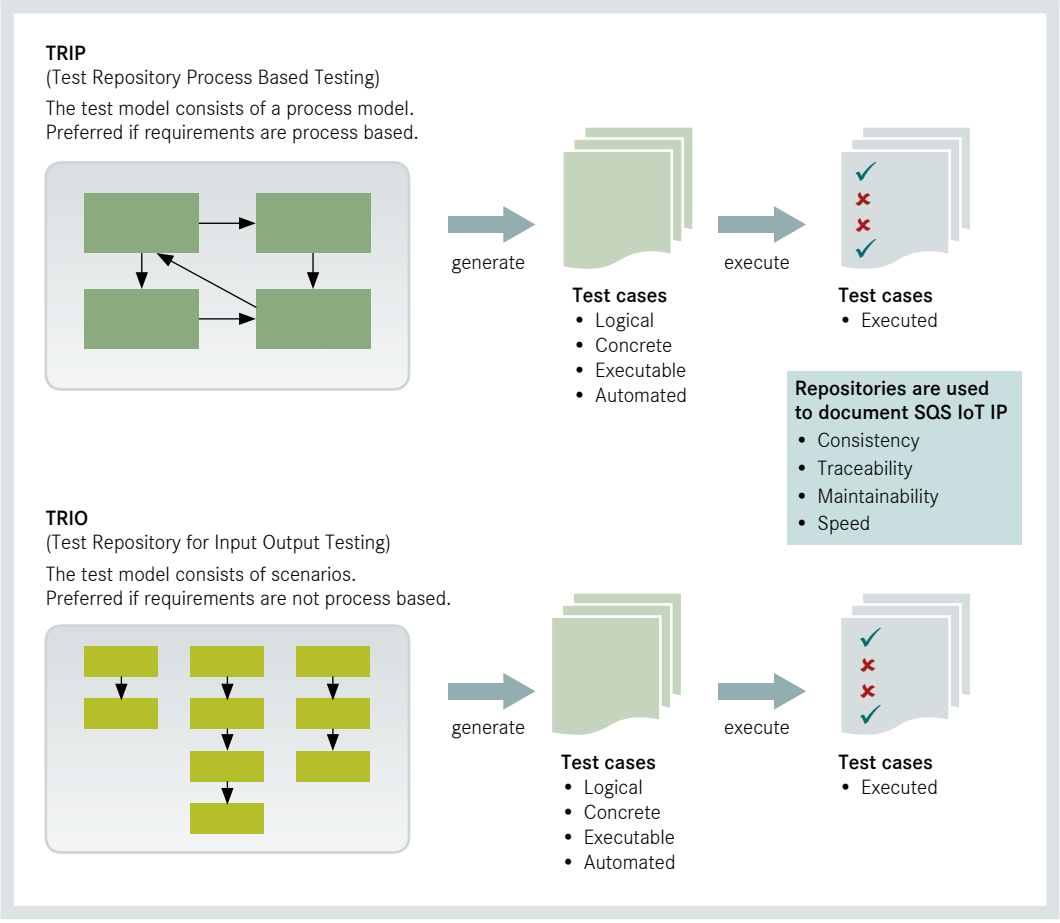

Figure 2: The semi-formal TRIP and TRIO notations

2. **TRIO: Test Repositories for Input-Output Based Testing** – Repository-supported

   Another approach is executed if the test basis cannot easily be described in a process-oriented way (for instance in the case of autonomous, networked devices). In this case we still follow a scenario-oriented route, with the scenarios consisting of a sequence of key activities derived from a test basis and SME interviews. Depending on the test object (business process or system process), the activities are more abstract or related to application interfaces like GUIs, or other services respectively. For each activity, the principal input output behaviour is defined by conditions documenting which typical inputs or outputs (verifiers) are relevant. In this case a repository consists of typical scenarios and their input and output conditions. Test cases are specified by selecting the conditions needed throughout the scenarios. Based on this selection, executable test cases are again generated.

The principles of both SQS notations (TRIP and TRIO) are shown in Figure 2. Both approaches are based not on test cases but on an intermediate maintainable and reusable asset layer (test repositories based on processes or conditions). For use cases such as testing of the IoT, particularly in a manufacturing environment, TRIP and TRIO offer a highly compatible way of describing requirements and test conditions and, thus, deriving test cases. Scenarios are the focus and test cases are their refinement based on the detailed, expected behaviour of IoT systems.

Initially, repositories can be created in a semi-formal and manual way by having a test analyst evaluate and select all relevant paths and combinations of test conditions to derive test cases that satisfy defined coverage and risk objectives as exit criteria. Finally, the quality of test cases is defined by a set of complete and executable test cases. Formal criteria can easily be defined but the complexity inherent in the IoT (scenarios) and the volume of non-discrete states (data) leave room for uncertainty with respect to coverage and risk.

Artificial Intelligence for further optimisation

Artificial Intelligence (AI) is now an extension to manage the complexity of IoT systems via a self-optimising mechanism based on information from test repositories, but also additional relevant data such as performance and quality KPIs. AI can be leveraged from this database.

There are many ways in which intelligent behaviour can be used to automate or improve test tasks in the age of the IoT. For instance, intelligent execution of test cases on machines and devices in a live environment can help to ensure the desired behaviour in complex situations with many factors and players involved. Of course, machines and devices do not act based on these test cases so this can be considered halfway between a simulation and a fully-fledged execution in the live environment.

However, as part of this whitepaper we would like to highlight two aspects which we consider to have a significant impact on the efficiency and effectiveness of IoT testing.

When looking at interesting targets for automation during testing, test preparation offers an obvious and particularly attractive target. Not only are test preparation activities highly labour-intensive, they are particularly so in an IoT environment due to the complexity of interlinked semi-autonomous decision-making. To date, test preparation is among only a few activities in the fundamental test process

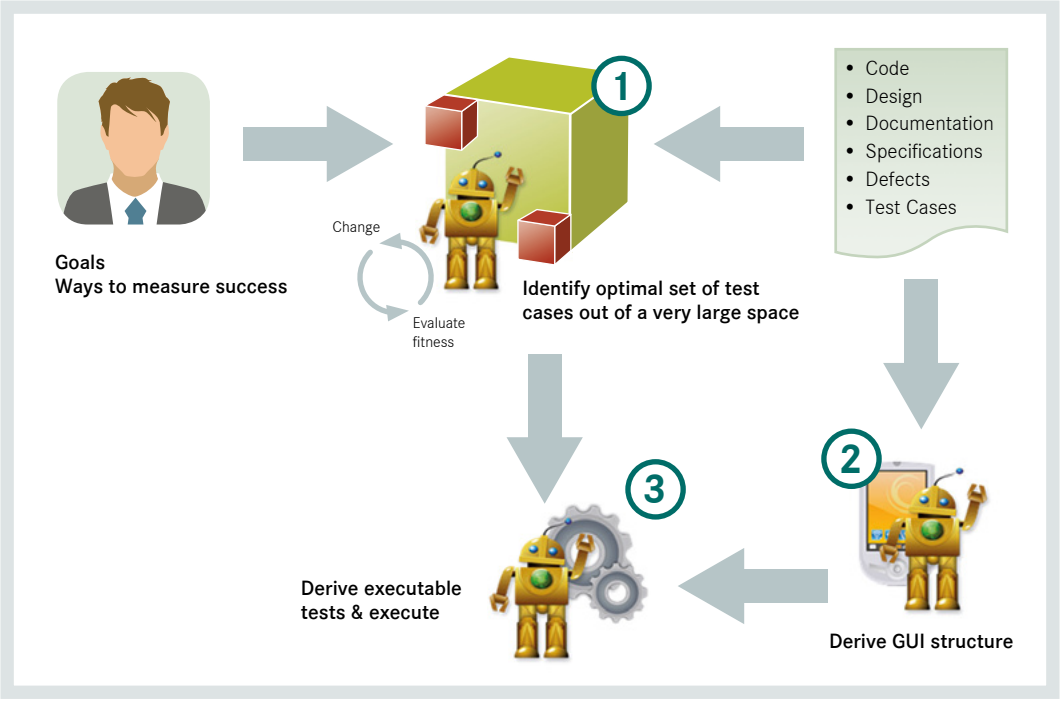

Figure 3: Typical approach found in search-based testing

that are still almost entirely manually performed or tool-aided (cf. previous section “Managing complex IOT ecosystems in testing”).

Test execution, conversely, is generally well-supported by test automation approaches, ranging from GUI-driven automation to automation of environment provisioning, data loading, results comparison or automation on an API or service layer. Any activities concerned with the logistics of execution, i.e. the arranging and chaining of test cases into test suites, is again largely left to humans, leading to often sub-optimal executions due to sub-optimal chaining. Solutions centred on search-based approaches have emerged over the last decade that open this field up to analysis and optimisation by algorithms.

Figure 3 showcases a typical approach to using search-based methods in testing. In this example, the algorithm needs criteria to establish whether it is improving or not in terms of input, just as it considers the specification of the application under test as input. Using the semi-formal models discussed in the previous section, this information can be provided to the algorithm.

Using these inputs, the algorithm discovers the area of possible sequences through the AUT, – as well as all of the inputs into it –, which are needed to derive logical and concrete test cases. If the user interface of the AUT is accessible to the algorithm, it may even relate inputs to GUI widgets and generate test cases which can be executed automatically.

The road to intelligent iIoT testing

Obviously, moving from a mainstream testing approach to one that implements AI as part of its core methodology is a major disruption that few organisations are willing to take in a single step. However, pathways exist that can help businesses to take smaller steps, one at a time. We will examine such a pathway below.

To understand how to progress with the AI-based approach to testing, it is essential to dissect it into its key components:

- Low level AI (data analytics, KPIs, models) provides the base and foundation for AI by collating the relevant data sources and enabling them for later analysis / reasoning.
- High Level AI uses the previously-defined databases as a basis for search-based or analytical algorithms that automate further testing and delivery tasks. At the moment, this does not extend to even higher-level approaches such as neural networks.

With this insight, the steps towards intelligent testing become clear. As a first step, the low level data needs to be collated and used. At the same time, key data needs to be made available in a format that is accessible to machines and algorithms rather than just to humans.

Admittedly, initially this sounds like a lot of overhead with little value in itself except as a precondition for applying AI algorithms and automation. However, when examining the approach in more detail, it becomes clear that this is not the case. Everything that is done in this step can already add value to the QA and test effort as soon as it is in place.

How can this be? Let's look at requirements and test cases as an example. Typically, these will be found in some sort of written document. While there are many approaches towards using models to support or even drive the testing of complex systems, none of these have attained any relevance except for in safety-critical niche markets such as the aerospace and automotive industries [6].

As long as this is the case, many AI-based approaches will either fail, require substantially higher effort or will cause the quality of the result to drop. Fortunately, requirements, test conditions and test cases can be expressed using the semi-formal TRIP and TRIO models as a means to curb the complexity in manually testing IoT systems. As a consequence, there is an iterative and efficient path from traditional testing to AI-supported testing in the IoT domain:

1. Provide the foundation by making artefacts such as requirements accessible to machine analysis by describing them in semi-formal models. This avoids the steep learning curves associated with full-on model-driven approaches but gives enough benefits to apply AI later on.

   In addition to making key test basis artefacts accessible to the algorithms, a testing and quality KPI system needs to be set up if this does not already exist. This KPI system is needed in order for the AI to track its progress in optimising the test suites.

2. Implement AI approaches such as search-based test case generation or test suite optimisation on top of this data. As yet there are no standard COTS solutions available, which means that any AI implementation is necessarily a bespoke development.

   Implementers need to make sure that they have enough confidence in the added value provided by AI when compared to the lifecycle cost of maintaining the resulting implementation.

Conclusion and outlook

The use and application of AI and search-based intelligent methods in the testing domain have picked up speed in 2015, and a number of players, small and large alike, have publicly announced the availability of solutions based on the application of such techniques.

Research analysts have taken up the topic and have reported that even systems integrators are applying AI, having announced the availability of intelligent solutions covering root cause analysis and test case optimisation with a view to extending their use to cover the full software lifecycle.

This example demonstrates the immense capabilities that testing organisations see in AI-based approaches. These will give testing what the waves of industrialisation and digitalisation have brought to the manufacturing industries: an ever increasing amount of tasks that can be executed efficiently and repeatably by a robot rather than requiring manual labour. Just like the assembly line worker, the software tester of the future will work on very specific parts of the overall testing programme, while mundane test design and execution tasks will be handled by software.

References

[1] Colin Bull. Trusting The IoT. http://www.softwaretestingnews.co.uk/trusting-the-iot/, May 2016

[2] Martin Wieczorek, Dik Vos, Heinz Bons. Systems and Software Quality - The next step for industrialisation, Springer 2014

[3] Faulty update breaks Lexus cars' maps and radio systems, http://www.bbc.co.uk/news/technology-36478641, 08 June 2016

[4] Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent from 2015 http://www.gartner.com/newsroom/id/3165317, 2015

[5] Joseph Bradley, Joel Barbier, Doug Handler. Embracing the internet of everything, 2013

[6] Roßner, Brandes, Götz, Winter. Basiswissen Modellbasierter Test, Heidelberg, 2016

SQS Software Quality Systems AG
Phone: +49 2203 9154-0
Fax: +49 2203 9154-55
info@sqs.com | www.sqs.com