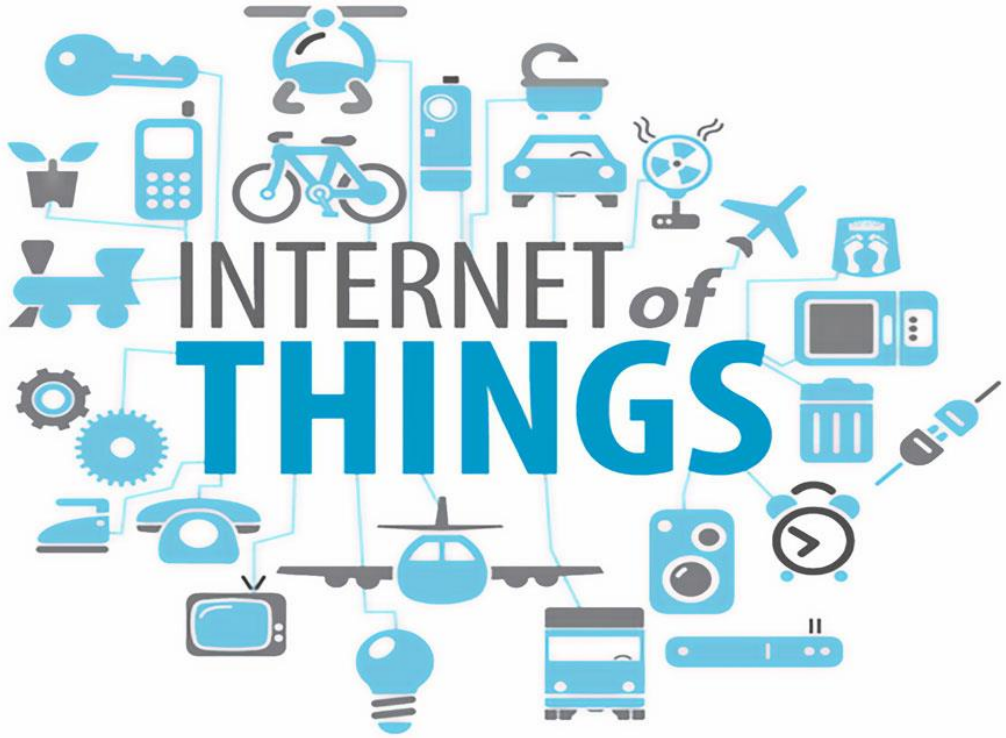
Verification And Validation of IoT Systems

Prepared By: Hamdan Hejazi. Supervisor: Prof. Istvan Majzik

Outline :

- Internet of Things (IoT) and why Testing IoT systems is a complex exercise?.
- Case Study 1 & 2.
- Challenges in Testing IoT systems.
- Testing Requirements in IoT systems.
- Objectives of V&V at IoT system layers.
- A Framework for V&V of IoT systems.
- Case study 3.
- What we need more for effective V&V ?.
- Conclusion.



Internet of Things (IoT)

IoT systems become an indispensable part of our daily lives so, it is vital to test these systems rigorously and stringently to ensure that they are secure and efficient.

So, Testing IoT systems is a complex exercise, with several Verification and Validation (V&V) activities required to ensure end-to-end system functionality.

Why Testing IoT systems is a complex exercise ?

- As IoT systems become increasingly integrated into our day-to-day lives→ it becomes essential to test them to ensure that they are secure, efficient, perform their intended tasks.
- To comply with government regulations and industry standards..
- Heterogeneous Components : IoT systems combine hardwar devices and sensors, network components, and softwar applications. .
- real-time features of IoT systems, in which large volumes of dat are constantly exchanged, add to the testing complexities.

What we need ?

At the same time, enterprises are recognizing the pitfalls of not integrating V&V for IoT systems – including the impact on end-user experience, business operations, and brand value – and devoting considerable time and resources to the testing processes.

Case study 1

Failure to test IoT products led to product recalls, hurting a children's smartwatch manufacturer's brand image.

What happened ?

EU recalled a children's smartwatch because hackers could access data captured by the device and locate the whereabouts of the children wearing it.

Why?

The manufacturer failed to comply with the EU's Radio Equipment Directive, which lays down standards for privacy and data theft.

Case study 2

A ransomware attack forced a natural gas facility to shut down its operations for two days.

What happened ?

US-based natural gas facility operator had to shut down operations after a ransomware attack prevented its personnel from receiving crucial operational data from the firm’s connected equipment. This resulted in an operational shutdown of the entire pipeline asset for about two days. causing significant business losses.

Case study 2

Why?

The malfunction’s direct impact was limited to one facility, facilities in other geographies also had to halt operations because of pipeline transmission dependencies.

The enterprise cited gaps in security knowledge and the wide range of possible permutations and scenarios that need to be tested as reasons for failing to adequately incorporate cybersecurity into their systems

What we need ?

The increased complexities of IoT testing and the impact of IoT systems' inefficient validation on enterprises warrant a framework-led approach for V&V.

Such An approach can help enterprises define the wide range of scenarios that need to be tested and build a holistic testing approach to streamline the functioning of these systems.

Challenges in Testing IoT systems:

IoT system layers

IoT technology stack	Description
 Business applications layer	End-user facing layer – which includes web and mobile applications, UI/UX, and dashboards – which displays insights and reports to customers
 Platform and data layer	Enablement platforms that facilitate data import and storage and integration with standard protocols; the data processing layer, and analytics and visualization applications for insights and reporting are also a part of this layer
 Connectivity and gateways	The layer that enables data transmission from edge devices and sensors to platforms, and includes basic device connectivity features, data selection, and data protocol standardization
 Devices	Edge devices (data capturing sensors, actuators, and connected devices such as smart lights, smart speakers, and connected automobiles); the layer may also include features for computing and analytics to be performed at the edge

Challenges in Testing IoT systems

System complexity : increasing number of devices, sensors, and platforms, the possible permutations that need to be tested go up significantly

External dependencies: external factors such as availability of sensors, devices, and human interfaces to provide gesture and voice inputs.

Standardization: as simulating test environments needed to support different protocols requires heavy investment in infrastructure

Scale: Scalability tests are important as system performance is impacted by variations in scale, affecting latency and reliability.

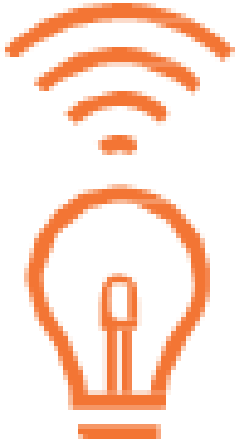
Regulatory conformance: Enterprises need to ensure compliance with the regulations.

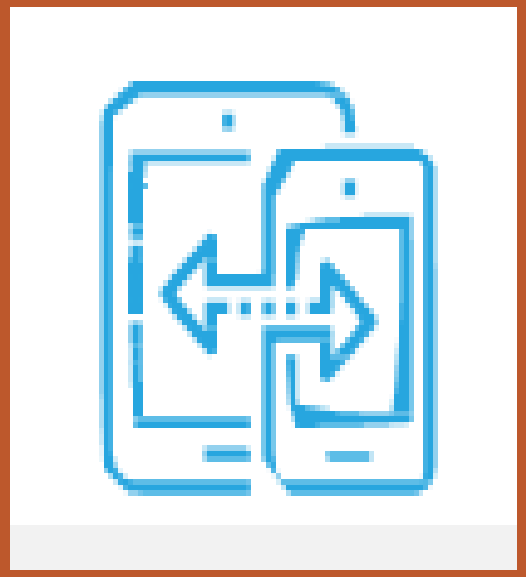
Testing Requirements in IoT systems According to Cyber- Physical Production Systems (CPPS)

CPPS Requirement	Testing	Challenges
Scalability	1. Increase number of network nodes. 2. Increase available data. 3. Increase service availability.	Latency; Cost of acquiring new devices and upgrade resource power; Constrained data processing methods.
Reliability	1. Long term execution. 2. Anomaly injection to generate failures. 3. Extreme environment conditions. 4. Overall counting of received/sent packages.	Relationship between anomaly and generated failures; Code verification methods.
Security & Privacy	1. Cyber attack injection. 2. Stealing sensitive data. 3. Security resources are up and running.	Unavailability to inject zero-day attacks; Simulate known attacks; Lack of expertise regarding cyber security methods.
Timing & Determinism	1. Guarantee cycle time. 2. Compare equipment process with varying parameters.	Identify which component introduces delay; Evaluate the influence of environmental conditions over the process.
Safety	1. Simulation of safety process parameters (both in controlled and relevant environment). 2. Counting number of accidents in the shop-floor.	Knowing if accident is caused by human or machine error; Reliable parameter simulation; Availability of relevant environment to test.
Recovery	1. Evaluate continuous operation of the system when some of its parts are shut-down. 2. Maintain previous state after rebooting (both individual node or global system). 3. Analyze time of reboot.	Identify the damage level where the system is unable to recover; Identify what is the previous state of the system; Identify the acceptable time of rebooting.
Interoperability	1. Send messages with non matching semantics or not defined in ontologies (both between different nodes or modules in the same node). 2. Integration with 3rd party platforms (legacy entities).	Communication API does not exists; Non compatibility between existing APIs.
Reconfigurability	1. Analyze time of reconfiguration. 2. Verify system reconfiguration when is defined a new system topology. 3. Verify system reconfiguring when a new node is added.	Being able to verify reconfiguration in such complex systems; Identify acceptable time of reconfiguration.

Objectives of V&V at Device Layer:

- Ensure device functionality, data capture, data transmission, etc.
- Validate device conformity to regulations.
- Validate device compatibility with various networks and data protocols.
- Secure the device against third-party attacks.





Objectives of V&V at Connectivity/gateway Layer:

- Validate that the gateway can take data from multiple devices and convert it into standard protocols.
- Ensure that the network/ gateway is transmitting data with low latency to the cloud.
- Validate device compatibility with various networks and data protocols.
- Validate gateway functionality with variations in scale.

Objectives of V&V at Platform Layer:

- Validate the data processing and analytics functions to ensure that business objectives are met.
- Certify that the platform is able to interact with the UI layer, and onboard data from multiple networks.
- Ensure the system's performance is unaffected by variations in scale.
- Secure data storage against third-party access.

Objectives of V&V at Business application Layer:

- Validate that relevant data can be accessed by users, and ensure that these insights are consistent across channels – web, mobile app, dashboards, etc.

- Secure access to the UI layer to prevent unauthorized access.

Objectives of V&V for the whole IoT System:

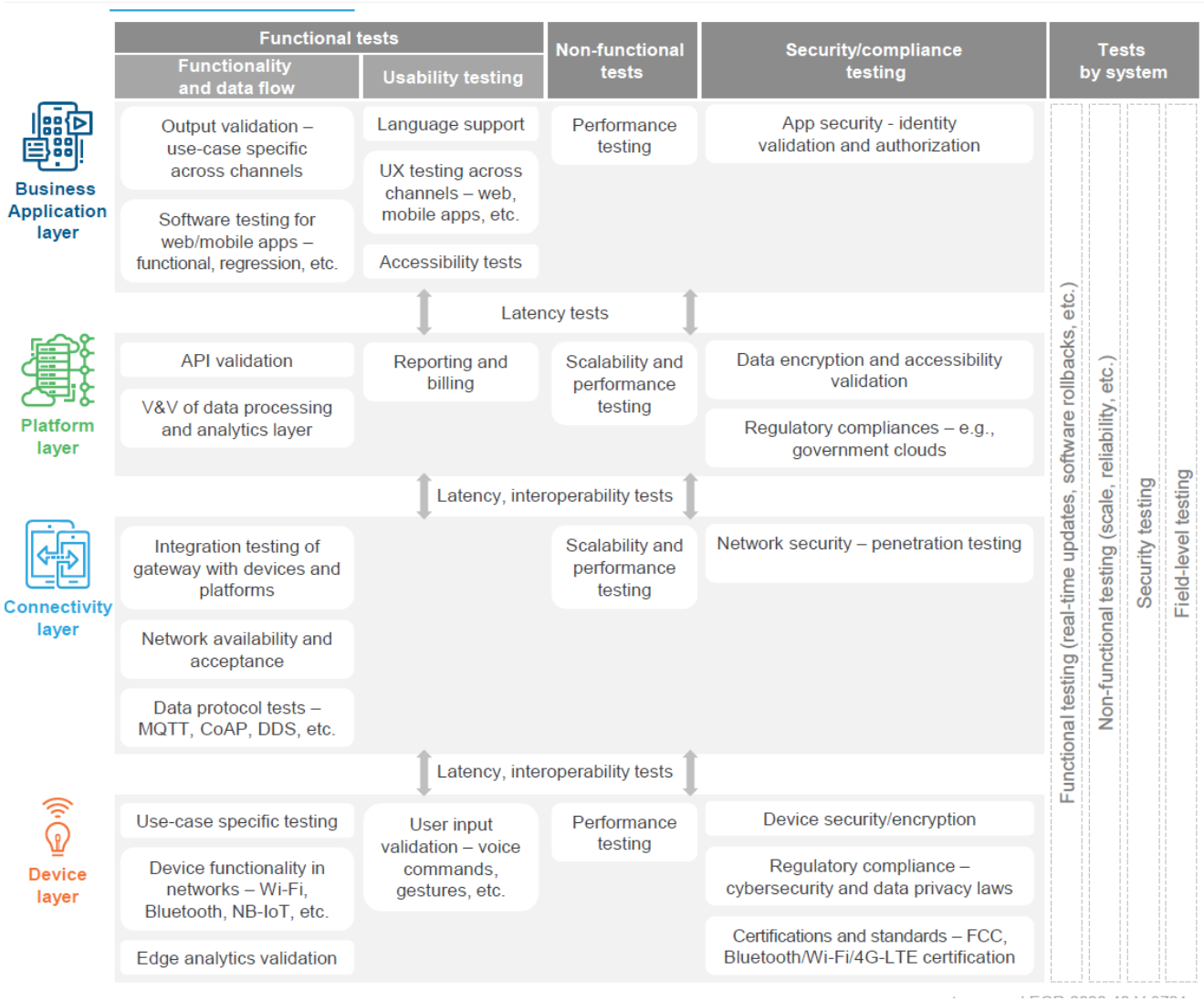
Validate overall system functionality per design and Ensure data privacy and security of the overall system

Ensure that individual layers and the overall system meet latency requirements

Validate the system against real-life conditions when it needs to interact with external devices and systems

A Framework for V&V of IoT systems

Given the multiple challenges associated with IoT systems' V&V and the fact that testing at each of the layers and at the system level is complex and has different objectives, there is a need for a framework-led approach that defines V&V requirements from end to end.



A Framework for V&V of IoT systems

Case study 3

End-to-end validation of a smart home system helped an enterprise achieve significant savings in time-to-market and budgeted costs

What happened ?

A leading smart home solutions enterprise wanted to validate its end-to-end smart home automation solutions to enable customers to remotely control their devices from a mobile application

Case study 3

How ?

The enterprise partnered with a provider, which laid out a comprehensive V&V plan to carry out functional testing across all the four layers

The Result:

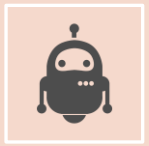
This approach, which covered multiple layers at the same time, reduced the enterprise’s time-to-market by 40% and the budgeted cost by 30%.

What we need more for effective V&V ?

While a whole host of different tools can be used to carry out V&V activities described in the framework.

Such Tools must leverage technologies such as Automation, Simulation, and Analytics to improve the effectiveness and efficiency of V&V, and ensure comprehensive test coverage. Let us take a closer look at each of these.

Automation, Simulation, and Analytics Tools Are a must for effective V&V:



Automation: Iterative V&V activities that need to be executed each time an upgrade is rolled out in addition to Test execution of scripts that check for functionality and interoperability.

Simulation: Simulating device/sensors to test the platform and application layer in addition to Simulating high load conditions to carry out performance and scalability tests of the entire system.

Analytics: To improve visibility into scenarios and test cases in addition to help expand software testing tools' productivity and monitor the V&V team's productivity to reduce test cycles.

Conclusions

In conclusion, various complexities around validating IoT systems make it necessary for enterprises to adopt a more structured approach for the V&V of IoT systems, as well as leverage technologies such as automation , simulation and analytics for more effective V&V.

For example : AI and ML can be used to automate the entire process, from test case generation to execution and analysis, thereby expediting the V&V process and generating actionable insights from the test data collected.


Thank You!