KU LEUVEN

DEPARTMENT OF COMPUTER SCIENCE

Shared Internet-of-Things Infrastructure Platform (SIoTIP)

Part 1A

Requirements Analysis

Breyne–Serruys–Vandeputte

Academic Year 2018–2019

H09B5B: Software Architectuur
H07Z9B: Software Architecture

Emile Breyne (r0629298)
Hendrik Serruys (r0754196)
Harold Vandeputte (r0632371)

1. Utility tree of ASRs

	Quality Attribute	Attribute Refinement	Summary Rationale ***Business Value*** Rationale ***Architectural Impact***
1	Availability	Sensor / actuator / mote failure	The system can compare sensor readings to values of nearby, similar sensors to detect incorrect responses. The Infrastructure Owner and the SIoTIP system administrators are notified in $<$ 60s after a failing sensor has been detected. (H,H)
			H: *Correctly working hardware is essential for all stakeholders involved. Failing hardware therefore needs to be detected as soon as possible as it can cause damage to the entire system.*
			H: *Comparison of sensor readings is complicated and will affect different parts of the system. Which sensors can be compared? When is data considered faulty? Must readings be synchronised in time? ...*
2			When a device failure is detected, applications using this device can automatically switch to a nearby and equivalent device when possible. Applications are therefore 99% available. (H,M)
			H: *Application availability is highly important to satisfy the paying customers (Application providers and Customer Organisations)*
			M: *Application instances need to be made aware of sensor failure. It will however be the responsibility of the application providers to make their application compatible with different kinds of sensors, if possible.*
3		Gateway failure	Online Service must detect gateway failure and notify SIoTIP system administrators and Infrastructure Owner in $<$ 60s.(H,L)
			H: *Availability of the entire system is highly important to all stakeholders.*
			L: *Detecting Gateway failure is rather straightforward. The Online Service can simply ping the Gateways when no data has been received in a long time.*
4		Online Service failure	SIoTIP Online Service must be available 99.999% of the time. (H,M)
			H: *The Online Service contains the servers whom are essential to data processing, data storing, communication across the system,... When the Online Service is down, it won't be long before other parts will start to fail as well.*
			M: *Although the availability of the Online Service is mainly in hands of the Server providers, the system itself can be prepared for Online Service failure (e.g.: gateway caching, replication,...)*
5			In case of Online Service failure, the sensor data should be cached at the Gateway and send at the first possible occasion. (M,L)
			M: *Data loss should be reduced to a minimum. However, losing data during Online Service failure is not the end of the world.*
			L: *Gateway caching won't have a profound architectural impact. It should be transparent for all devices who are exchanging data with the gateway.*
6		Application instance failure	The system detects if an application instance fails and notifies the SIoTIP system administrators and the application providers within 60s. (H,L)

	Quality Attribute	Attribute Refinement	Summary Rationale ***Business Value*** Rationale ***Architectural Impact***
			H: *Faulty applications can damage the system. All parties involved require correctly working applications.*
			L: *An application instance crash can easily be detected with a ping.*
7	Interoperability	APIs for application providers	SIoTIP must provide services or APIs to accommodate distributed applications. This means APIs in the gateways and in the online service. Interface functions involved in passing sensor must successfully process 99.99% of information. (H,H)
			H: *An important business goal of SIoTIP is to allow third party Application Providers to create Applications which run on the SIoTIP platform. This of course requires the necessary APIs.*
			H: *This has a mayor architectural impact. The architecture needs to provide classes for the APIs. It must be guaranteed that these APIs meet all Safety and Security concerns.*
8		Environments for application providers	For application providers, a development, testing and debugging environment is provided. This provides easy access to all APIs provided by SIoTIP. 95% of exchanged information between the application and the sandbox environment must be successful. (H,H)
			H: *The sandbox environment for testing applications is essential to allow third party Application Providers.*
			H: *The sandbox environment is a fundamental part of the architecture which will require coordination between different parts of the System.*
9		MicroPnP devices - Gateway Interoperability	Sensor/Actuator data is passed between mote and local gateway by use of GET or PUT requests. The message contains sensor/actuator type which indicates how the information must be interpreted, and a timestamp. This information is 99% successfully processed. (H,M).
			H: *Sensor data must be as accurate as possible so the applications can work optimally.*
			M: *First of all, this requires accurate transmission as some sensors might not be able to resend corrupted data packages. Secondly, any data conversations must be as accurate as possible.*
10			Sensors can request to send new information to the gateway either periodically or caused by a state change. The requests are accepted if the mesh network is not overloaded, and rejected otherwise. In case of consistent rejection, SIoTIP System Administrators and the Infrastructure Owner are notified. (M,M)
			M: *Overloaded mesh networks can cause data loss, which is not good for business.*
			M: *The System must monitor the mesh network throughput and must be capable of notifying the necessary stakeholders.*
11		Gateway - Online Service Interoperability	The Online Service opens a permanent connection with a gateway over a wired or WiFi network. This connection is periodically used by the Gateway to synchronize data. 99% of information exchanged should be successfully processed as gateways have only limited storage capacity. (H,M)
			H: *Quasi-perfect interaction between Online Service and Gateways is critical in deploying a robust platform.*
			M: *The connection will mostly depend on telecom and server providers. Synchronized data transfers must be monitored and failure will require notificitions.*

	Quality Attribute	Attribute Refinement	Summary Rationale ***Business Value*** Rationale ***Architectural Impact***
12			The Online Service communicates sensor configuration updates or actuator activation to a given Gateway over their permanent connection as soon as the command is given or as soon as the gateway becomes reachable. (H,M)
			H: *Fast response times are sometimes critical for applications and must be assured when possible.*
			M: *This requires critical code sections in the SIoTIP software on both the Online Service as well as the Gateways.*
13	Modifiability	Modifying software configuration	Customer Organization (un)subscribes to a new application at runtime without any further effort. (H,H)
			H: *(un)subscribing to applications is central to the financial aspect of the SIoTIP corporation.*
			H: *A new subscription to a certain application causes the system to move software around (gateways must be prepared to handle application), hardware requirements must be checked etc. Proper handling of changing customer subscriptions is essential to the working system.*
14			Customer Organizations / End-users can configure the method of delivered notifications and alarms without any financial cost or further human effort. (M, M)
			M: *Configuring alarms and notifications is somewhat important. However, business can thrive without many modification options regarding notifications.*
			M: *The correct working of alarms and notifications and their modifications will require some work but will not fundamentally change the architecture.*
15			Infrastructure Owner (re)allocates installed sensors and actuators to Customer Organizations without any further cost, effort or time delay. (H, H)
			H: *Modifiability of who's using which sensors, as well as sharing sensors between Customer Organisations, is an important business goal of the firm.*
			H: *There are important architectural aspects to sharing sensors and actuators. The system must assure the correct working of these devices when they are potentially used for different goals by different organisations.*
16			Infrastructure Owner modifies his topology without any further effort or time delay. (H, H)
			H: *Enabling an Infrastructure Owner to modify his topology is essential to support both upcoming technologies and changing demands.*
			H: *Topologies play an essential role for the system. A modification of a topology will trigger other modifications (which applications are supportable? Similar sensors for data comparison? Gateway support?)*
17		Modifying SIoTIP software components	The SIoTIP system can be made compatible to a new IoT technology stack in less than 30 calendar days. (M, H)
			M: *This QA has a medium business value as MicroPnP is the only stack which is technically required to have an operational system.*

	Quality Attribute	Attribute Refinement	Summary Rationale ***Business Value*** Rationale ***Architectural Impact***
			H: *The architectural impact however will be profound. Adding a new stack might be impossible if the system is not designed with this abstraction in mind. If the system is well-designed towards this purpose, a period of 30 days should suffice to adapt and test the interfacing.*
18		Modifying hardware components	New installed sensors/actuators/motes are automatically tested by the system, in less than 60 seconds, before being activated. There is no additional human effort required if tests are successful. (M, M)
			M: *Success of business will be negatively impacted if modifying hardware components cannot be done fast and easy.*
			M: *New hardware must be tested thoroughly and the system must have good knowledge and judgement of the different existing devices.*
19		Modifying applications	New features are added to a running application without requiring intervention from the Application Providers. The system tests the modifications automatically within 60s. Testing the modifications can take up to five calendar days if administrator intervention is required. (H,H)
			H: *Being able to update applications smoothly is essential for good business.*
			H: *Applications contain foreign code and can damage the system if they behave improperly. Updating application instances must also happen transparently to the application provider. This will require good coordination within the system between different components.*
20	Monitorability	Automated monitoring	The System should monitor the execution of application instances. This yields information regarding the performance of applications (CPU usage, memory usage). (M,M)
			M: *Making sure that applications behave appropriately will ensure a stable platform.*
			M: *Correct behaviour must be measurably defined. As applications run both on gateways as on the Online Service, multiple system components must be monitored and results must be synchronized.*
21	Performance	Gateway storage latency	Data from the hardware components should be permanently stored on the gateways within 5 seconds in normal operating mode. (M,H)
			M: *If they are not stored quickly, data may get lost fairly easily, which is something we would very much like to avoid.*
			H: *Gateways have to reserve a big enough amount of disk time to write all incoming data within the time limit.*
22		Online service storage latency	Historical data from the gateways should be backed up on/synchronized with the online service every 5 minutes on average. (M,M)
			M: *Some applications will exploit all the historical data retrieved by the sensors. As gateways may crash, connectivity will go down, etc,.. the data should be backed up on the server every now and then to prevent data loss.*
			M: *Gateways and online service have to work together to synchronize at appropriate times, online service should have enough disk throughput to write all received data.*
23		Latency	Data from sensors should be processed at the gateway with an average latency of 0.5 seconds. (M,H)

Quality Attribute	Attribute Refinement	Summary Rationale ***Business Value*** Rationale ***Architectural Impact***
		H: *Gateways are the first logical units processing the received data. If they fail to maintain a decent latency, this may induce extra waiting time in the entire system.*
		H: *Mesh network and gateway resources must be managed in such a way that no saturation occurs (max 26 packets per second), and packets are processed in time.*
24		Sensor data should be sent to and processed by the online service (and the applications run on it) with an average latency of 10 seconds.
		H: *For convenience of the application users (most applications will require fairly quick response) the applications running on the server should have access to relatively up to date data.*
		H: *This requires efficient resource managing and queuing algorithms in the whole infrastructure.*
25		Important messages (e.g. alarms, notifications) should be sent, processed, and available for the application user almost immediately: within 3 seconds.(M,M)
		M: *Some applications may require important messages to arrive almost instantly, when a fire breaks out for example.*
		M: *This requires to implement queuing algorithms that send and process important data more quickly, both at gateway level as on the server.*
26	Throughput	Gateways should be able to process up to 26 packets per second. (H,L)
		H: *A mesh network can transport up to 26 packets per second. An infrastructure owner expects that the gateway is able to process at least these packets.*
		L: *It shouldn't be that hard to provide gateways with sufficient processing power (26 packet/second isn't really that much, even for a little embedded system.*
27		The online service and the applications running on it should be able to process all the incoming data. When the load on the server exceeds 90% of CPU time/disk time/bandwidth, the system administrator must be notified within 5 minutes.
		M: *Normally, the total load on the server will not vary that quickly, and the server providers should be able to adapt to demand. If this is not the case, system administrators should be able to take actions.*
		L: *Just a system resource monitoring thread should suffice.*
28	Monitoring application resource usage	The online service should monitor the resources used by each application (disk access, CPU) and notify the system administrator (within 60 seconds) as well as the application provider in case of problems. (e.g. using more than it's share of CPU time). (M,L)
		M: *System administrators must ensure that one program doesn't claim all the system resources for himself, hereby blocking the execution of other applications/the online service itself.*
		L: *A simple recourse monitoring thread should suffice.*
29 Scalability	Additional hardware	adding new sensors/actuators/gates can be done at any time without having any notable effect on the performance and availability of the online service(H,L)
		H: *SIoTIP's online server should be able to handle an almost unlimited amount of sensors/actuators, so that an increasing demand can always be met*

Quality Attribute	Attribute Refinement	Summary Rationale ***Business Value*** Rationale ***Architectural Impact***
		L: *The performance of the online service can be increased by adding additional processing power, supporting parallel processing, and increasing bandwidth, which shouldn't affect the rest of the system. Furthermore, these requirements should be negotiated in the service level agreement with the server providers.*
30		Each mesh network can handle up to 26 packets per second before it's bandwidth is saturated. Infrastructure owners may sometimes want to add extra hardware, which will increase the load on the mesh network. When saturation occurs, the gateway should detect it and reconfigure the sensors to lower their polling frequency, or take other measures.(M,L)
		M: *A saturated mesh network can lead to additional latency or data loss in the worst case. Data loss is highly undesirable.*
		L: *This can be easily done by implementing some flow control thread in the gateway.*
31		Gateways are limited in terms of processing power, bandwidth, storage, etc. Connecting extra sensors/actuators to a gateway should never result in the inability of the gateway to handle all tasks/losing data. If the load exceeds 90% of CPU time, the gate sends a notification to the online server and decreases the polling rate of the sensors.(M,M)
		M: *Adding extra hardware can't affect the ability to store and process all data. Infrastructure owners should be notified when there are too much sensors and actuators on a mesh network, and a temporary measure should be taken (e.g. decreasing polling rate).*
		M: *Some thread should run on the gateway to monitor CPU usage. Gateway should be able to send a warning and have a temporary solution ready.*
32		To accommodate an increasing need for gateway resources in a mesh network, it should be possible to allocate additional gateways to networks in order to meet the requirements of more sensors and actuators.(M,M)
		H: *Overloading the gateway resources could result in additional latency or data loss, which is highly undesirable.*
		M: *The system must be implemented in such a way that the users (end-users, applications, system administrators) see no difference between motes being attached to the same or different gateways.*
33	additional application users	The Online Service should be able to service an arbitrary amount of end users, while maintaining equal performance (an average latency of 2 seconds for user requests).(H,L)
		H: *Application providers want to be able to service as most end-users as possible, with no limit to the amount of users.*
		L: *This is almost entirely in hands of the server providers, who need to allocate extra resources to adapt for the increasing load on the server.*
34	additional applications	The main goal of SIoTIP is to support 50 different applications in the first year. It should be possible to expand this further. Doubling the number of applications should be possible without increasing average latency of user requests by more than 10%. (M,L)
		M: *Being able to increase the number of possible application is necessary if we want to expand SIoTIP globally and attract more users.*

	Quality Attribute	Attribute Refinement	Summary Rationale ***Business Value*** Rationale ***Architectural Impact***
			L: *Applications are developed by third party companies. They all use the same interface, so this shouldn't affect the system a lot.*
35	Security	Authentication	Every user in the system should be validly authenticated. An unauthenticated user should be detected and removed within 60 seconds. (H,H)
			H: *SIoTIP needs to be trustworthy, as some applications can be very sensitive (e.g. access control in a building. Unauthenticated users could do much harm to the system if undetected.*
			H: *Implementing this security mechanism that each and every user will have to identify himself on login. Additionally, a system-wide detection and removal algorithm has to be written.*
36		access control	Each sensor/actuator is accessible to a limited group of users (e.g. building access control). 99.999% of device access calls should be made by authorized users only.Unauthorized accesses should be detected and blocked. (H,H)
			H: *Customer organizations expect that only authorized users have access to their confidential data/ can access protected devices. SIoTIP has to maintain a trustworthy status.*
			H: *Every function call has to be checked to see if the user has the proper rights, on all software levels (application, online service, gateway).*
37		Confidentiality	The online service should be able to parry 99% of attacks aiming to read private historical data stored on the server.(M,H)
			M: *Some sensors could provide sensible data. The customer organizations expect this data to be safe from intruders.*
			H: *The system should provide an effective means of repelling malicious users from reading confidential data. This greatly affects the implementation of all the storage mechanisms.*
38		Gateway isolation	Gateways are distributed over the entire network and are much more accessible. They can be compromised fairly easily as they reside offsite. A compromised gateway should not have access to any other data outside of itself.(H,M)
			H: *As explained above, gateways are easily accessible. If one compromised gateway could compromise another, this could lead to a chain reaction and a total blackout of the system, which is unacceptable.*
			M: *The system should not only provide a way of protecting the online service and gateways from malicious users, but also to protect from other gateways.*
39		Integrity	Data stored in gateways should not be altered by malicious users. 90% of corrupted data should be detected by the system.(M,M)
			M: *SIoTIP has to maintain a trustworthy reputation, and application users expect to receive valid data.*
			M: *Gateways have only limited resources, so adding a defense layer to protect from malicious data changes won't be easy.*
40			Data stored in the online server should not be altered by malicious users. 99% of corrupted data should be detected by the system.(H,M)
			H: *SIoTIP has to maintain a trustworthy reputation, and application users expect to receive valid data. The central online system is expected to be more robust to attacks than the distributed gateways.*

	Quality Attribute	Attribute Refinement	Summary Rationale ***Business Value*** Rationale ***Architectural Impact***
			M: *There should be a layer protecting the data and checking for inconsistencies.*
41	Testability	Application testing	When a new application is uploaded, the application is automatically tested in a sandbox environment. The results are captured and should produce a 95% statement coverage in 60s. If all tests are successful, the application is made available for Customer Organisations. (H,H)
			H: *Automatic tests are critical for Application Providers and will greatly impact business value.*
			H: *The sandbox environment is a fundamental part of the architecture which will require coordination between different parts of the System.*
42		Hardware testing	A new piece of hardware is tested before it is made available (Testing ability to communicate, response time, data packet integrity...). The time to perform tests should be < 60s. The results are captured, logged and both a System Administrator and the Infrastructure Owner are notified if tests fail. (M,L)
			M: *For Infrastructure Owners, installing new devices should be 'plug-and-play'.*
			L: *Different tests may need to be implemented varying per device.*
43		Unit testing	When the SIoTIP gateway software / Online Service software is completed and must be integrated, a test suite is executed and the results are captured. 98% of path coverage should be tested within 1 hour. (H,H)
			H: *The SIoTIP software must be strongly tested as it envelops the System.*
			H: *To extensively test the System software, many unit tests will need to be derived.*
44			Customer Organization, Infrastructure Owner, System Administrator and Application Provider dashboard has to be tested extensively for both functionality as well as safety and security of possible actions. Every dashboard is tested when its code is completed or updated and time to test should be < 5 minutes (H,M)
			H: *Dashboards are the main interaction between SIoTIP and its stake holders. They must be clean and user friendly. Furthermore, tests must make sure that no damage can be done to the system through a dashboard.*
			M: *Dashboards are limited in its functionality. Setting up these tests will not profoundly impact the architecture.*
45	Usability	User Initiative: Learning	End-user learns the main components of the dashboard and how to navigate through them in 3 minutes.(M,L)
			M: *As the dashboard is the main tool for interaction between the company and customers, it's ease of use will greatly affect customer satisfaction.*
			L: *If dashboards are designed with modifiability of design in mind, then usability can easily be upgraded based on user experience later on. Updating the dashboards does not have much impact on other aspects of the architecture.*
46			End-user learns how to configure notifications and alarms in 1 minute. (M,L)

Quality Attribute	Attribute Refinement	Summary Rationale ***Business Value*** Rationale ***Architectural Impact***
		M: *Correct and ease of use of notifications and alarms can greatly affect user experience with the system as a whole.*
		L: *This is merely a small part of the architecture.*
47		Application providers learn how to interface their application with the SIoTIP system in 30 minutes. (M,M)
		M: *Attracting good application providers is essential to business. The learning curve to integrate their applications to our systems should therefore be minimal.*
		M: *How foreign applications communicate with SIoTIP software is important as it's a potential source of malicious attacks against the system. The interface must therefore be designed with both security and usability in mind.*
48		Application providers learn the necessary steps to upload, test and debug an application to the SIoTIP system within 30 minutes. (H,M)
		H: *Ease of use with respect to uploading, testing and debugging applications can make or break the SIoTIP product value.*
		M: *Developing an user-friendly, isolated testing and debugging environment has strong architectural significance.*
49		Application providers learn how to manage and update their active applications within 10 minutes. (M,M)
		M: *Updating an application should be as transparent as possible to the providers.*
		M: *Architecturally, this ASR goes hand in hand with modifiability of applications.*
50	User Initiative: Configuring the system	Customer Organization (un)subscribes to an application. The system executes the user request in a transparent manner and the system responds within 3 seconds, verifying that the request was made. (H, H)
		H: *(Un)subscribing from applications in a transparent user-friendly way is essential to good business.*
		H: *To enable transparency, the system must be aware of the requirements of applications and the topology under which the Customer Organization operates. The action of subscribing can trigger modifications throughout the system (w.r.t. hardware, resources...). User-friendly subscribing will thus impact different aspects of the architecture.*
51		Customer Organization gets an overview of the invoices of their application subscriptions without any delay. (M, L)
		M: *This is important w.r.t. providing insight in used services. Everyone wants to know what their paying for.*
		L: *This is a simple database query.*
52		Infrastructure Owner orders new hardware with a maximum system delay at checkout of 5 seconds. (M, H)
		M: *Ease of purchase is of course essential to any business.*
		H: *If not outsourced, setting up a user-friendly online store will have significant architectural impact.*
53		Infrastructure Owner allocates sensors and actuators to Customer Organizations without any delay. (M, M)

Quality Attribute	Attribute Refinement	Summary Rationale ***Business Value*** Rationale ***Architectural Impact***
		M: *Usability of the system for Infrastructure Owners will reflect further upon the End-user. To satisfy the End-user, it's therefore important to make the system as easy to use as possible for Infrastructure Owners.*
		M: *This will mostly involve good design of access rights.*
54		Infrastructure Owner alters topology of their infrastructure without any delay. (M, M)
		M: *Ease of use of the system is an important business goal in general.*
		M: *The system relies on these topologies to make other decisions.*
55		System administrator interacts with End-user while accessing End-users' configuration settings (e.g.: topology of Infrastructure Owner) without any delay. (H, M)
		H: *Important w.r.t. providing good customer support.*
		M: *This mainly involves access rights.*
56		System administrator shuts an application down within 10 seconds. (H, M)
		H: *Many stakeholders rely on working applications. Faulty applications must be found and contained as soon as possible.*
		M: *Malfunctioning applications can damage the system. Quick action must be possible and potential damage must be isolated.*
57	System Initiative	When a purchase of hardware fails at checkout, the Infrastructure Owner and system admins are notified within 2 seconds. The system remembers the hardware present in the shopping bag before checkout. (H, M)
		H: *Money is involved.*
		M: *The system must use transactions and stateful sessions.*
58		The system notifies the infrastructure owner of a failed sensor / actuator in 60 seconds. (H, M)
		H: *Business depends highly on a working environment. If sensors fail, applications potentially fail to work and End-users can be hindered in their working activities. It's therefore essential that the system takes initiative to detect and notify failing hardware.*
		M: *A proper working notifications system will have significant architectural impact.*
59		The system notifies System Admins and Application Providers of misbehaving applications in 3 seconds. (H, M)
		H: *Misbehaving applications can potentially damage the system. The necessary stakeholders must therefore be notified so actions can be made.*
		M: *A proper working notifications system will have significant architectural impact.*
60		The system notifies System Admins of failing system components in 3 seconds. (H, M)
		H: *If a gateway fails, this can heavily impact a lot of people. SIoTIP HW / SW failure must be solved as soon as possible.*
		M: *A proper working notifications system will have significant architectural impact. Furthermore, correct behaviour of all important components of the system must be defined and checked in a timely manner.*

	Quality Attribute	Attribute Refinement	Summary Rationale ***Business Value*** Rationale ***Architectural Impact***
61			When a new application or update is uploaded, the system reports the status of the automatic tests and points out potential issues to the Application Provider. (M, M)
			M: *Providing automatic feedback to the application provider will greatly affect usability of the system.*
			M: *Automatic testing and a notifications system both require significant design decisions.*

2. Quality Attribute Scenarios

2.1 Availability: Detecting incorrect sensor readings

The system can compare sensor readings to values of nearby, similar sensors to detect incorrect responses.

- **Source:** internal: hardware
- **Stimulus:** fault: the system compares a malfunctioning sensor output to values of nearby, similar sensors and detects incorrect responses.
- **Artifact:** sensor
- **Environment:** normal operation
- **Response:**
  - Detection:
    - The fault is logged.
  - Preventing the fault from becoming a failure:
    - The sensor readings are no longer propagated to applications.
    - If possible, the applications are given nearby, similar sensor data instead. The system can locate such sensors based on the topology of the Infrastructure Owner.
    - If the problem persists for longer than 30s, the Infrastructure Owner and SIoTIP System Administrators are notified.
  - Recover:
    - Sensor is temporarily made unavailable while repair is being effected.
- **Response measure:**
  - The Infrastructure Owner and the SIoTIP system administrators are notified in <60s after a failing sensor has been detected.

2.2 Modifiability: Updating a running application

New features are added to a running application without requiring intervention from the Application Providers. The system tests the modifications automatically.

- **Source:** Application developer
- **Stimulus:** Update to an active application
- **Artifact:** The application code
- **Environment:** The application is updated at runtime
- **Response:**
  - Test modification:
    - The system tests the updated application automatically in a safe and isolated sandbox environment. The system must assure the updated application does not behave inappropriately, cannot cause system crashes, memory leaks, ...
    - If automatic tests fail, a SIoTIP system administrator is notified. The admin must run additional tests before deciding to accept or reject the updated application. Furthermore, the System provides the Application Providers with feedback of the failed tests.
  - Deploy modification:

    * Deploy if automatic tests succeed or system admin approves the deployment.
    * The System updates the status of the application to notify the Application Provider.
    * The application is made available to the subscribed Customer Organisations.
    * Updates of a specific application instance depends on the choice of a Customer Organisation to either automatically update the existing application or not.

- **Response measure:**
  - The system tests the updated application in <60s.
  - If the automatic tests fail, a period of five calendar days is required to allow for system admin intervention.

2.3 Usability: Customer Organisation subscribes to a new application.

- **Source:** End-user of a Customer Organisation responsible for application subscriptions
- **Stimulus:** End-user tries to use the system efficiently to subscribe to a new application
- **Artifact:** Customer Organisation Dashboard
- **Environment:** At runtime
- **Response:**
  - The respective dashboard provides a section / tab / window dedicated to viewing and configuring application subscriptions. Through this portal window, another window is reached, which is dedicated to finding and subscribing to new applications.
  - In this window, the system anticipates the user's needs by providing multiple ways to find new applications. This can either be done through selecting required features of the application, or through consulting an overview of all available applications.
  - The system anticipates what information the user requires about a specific application (Application features? Ready for activation? Estimated delay (e.g. due to missing hardware) before activation? Cost of using the application? etc.).
  - The system provides a one-click subscribe button.
  - The system asks for confirmation (is the user sure he wishes to subscribe?).
- **Response measure:**
  - Accomplished tasks:
    * End-user located dashboard application subscription window.
    * End-user browsed available applications.
    * End-user subscribed to an application.
  - Task time: 5 minutes.
  - User satisfaction: 80%

2.4 Security: Access Control

- **Source:** external human user who has been authenticated
- **Stimulus:**
  - An End-user tries to read data from a sensor using a web browser.
  - An End-user tries to access an actuator using a mobile device.
- **Artifact:** sensor/actuator

- **Environment:** normal operation, system is online, device is connected to online service network
- **Response:**
  - Only a subset of the users may access each device. The system checks if the user has the right permissions to access the device.
  - Authorized access
    * If this is the case, the system shall fulfill the request normally.
  - unauthorized access
    * If the user does not possess the required rights, the unauthorized access should be detected immediately.
    * The request cannot be fulfilled. No data is given away and no device state is changed.
    * The user will be notified of the access error.
    * The attempt should be logged and stored permanently for later analysis purposes.
- **Response measure:**
  - At least 99.999% of all successful device accesses are made by authenticated and authorized users.