SDN in the large - SoftFIRE and beyond

Orchestration of Federated Testbeds/Field Trials on SDN-NFV-5G Workshop – San Francisco May 3-4, 2016

Roberto Minerva, Telecom Italia Lab

Susanne Kuehrer, EIT Digital

SoftFIRE in a NutShell

- European funded Project, GA 687860
- Duration: 24 months
- Budget: € 4.384.510, nearly half of budget allocated to third parties for experimentation on the SoftFIRE Platform
- Consortium partners:

  EIT Digital (Coordinator), Deutsche Telekom, Ericsson, Fraunhofer FOKUS, Reply, Technical University Berlin, Telecom Italia, University of Surrey
- The Consortium is pursuing the integration of experimental facilities, testbeds and laboratories into FIRE+.
- Strong EIT Digital involvement and Leadership

Objectives

- Three key elements are considered: **interoperability**, **programmability**, and **security**. These properties have to be studied in terms of **efficiency**, **functional responsiveness, end to end latency** and generally **end to end QoS**.
- The three properties are essential to drive advanced solutions towards industrial adoption.
- The **main objective of this project is to demonstrate and assess the level of maturity of adopted solutions and to show how they can support the full potential of these properties in a real world infrastructure by creating, nurturing and supporting an ecosystem of third parties able to make use of the SoftFIRE testbed and to functionally extend it**.

Interoperability

- **Interworking** is the wanted property that should guarantee that islands with new or different technological capabilities are interoperable in spite of different underlying technologies. **Federation and interworking** between different nodes of a multifaceted environment are to be provided, checked and assessed. In addition new technologies and solutions should also be interoperable with legacy ones in order to ensure the smoother path possible from initial infrastructure to the newer one. Attention will also be paid to the emergent application of SDN and Virtualization to terminals and edge devices as well as the evolution of these technologies as a fundamental part of the evolution towards 5G for minimisation of latency.

Programmability

- **Programmability** is the pursued capability offered by the combination of SDN plus NFV, i.e., the possibility to directly govern network resources and to create virtual infrastructures on them in order to support the communication, storage and processing needs of networked applications. Programmability has to be challenged, assessed and evaluated against composite systems that comprise islands with different technologies, different management rules and different network capabilities. A proposition of the project is to consolidate the middleware infrastructure and empower European companies to become prominent providers or users of these solutions. This aims at counterbalancing the current advantage of other parts of the world in these technologies development and usage.

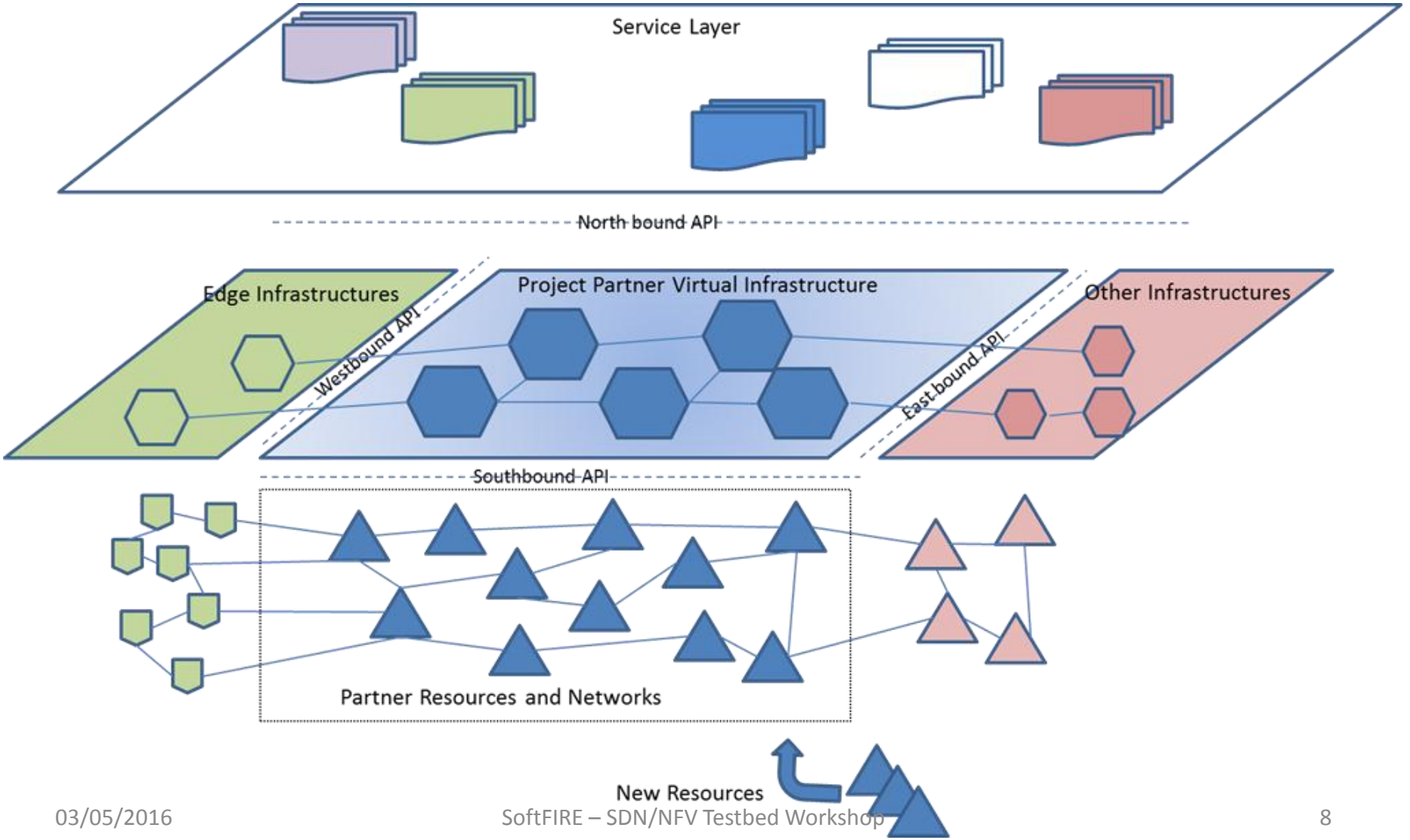
Security

- **Security** is the crucial property of these new programmable systems, in fact the opening up of programmable interfaces should occur in a safe and secure manner. Programmability is an essential feature, but if the security of interfaces, underlying mechanisms and systems is not guaranteed, then it becomes a risk rather than an opportunity. These technologies will not be adopted if they do not prove secure since their initial adoption and deployment phase. Security is a fundamental requirement that determine the acceptability of this envisage technology.

The Federated Testbed

- The infrastructure relies on existing experimental testbeds already set up by partners and it includes necessary extensions, integrations, adaptations and reconfigurations that serve the experiments. The federated testbed is open to new additions and extensions as technologies and standardization evolve towards a definition and support of SDN/NFV and towards 5G.
- A good mix ranging from Experimental test beds to preproduction implementations (Usurrey, Fokus –TUB, Telecom Italia, Ericsson),

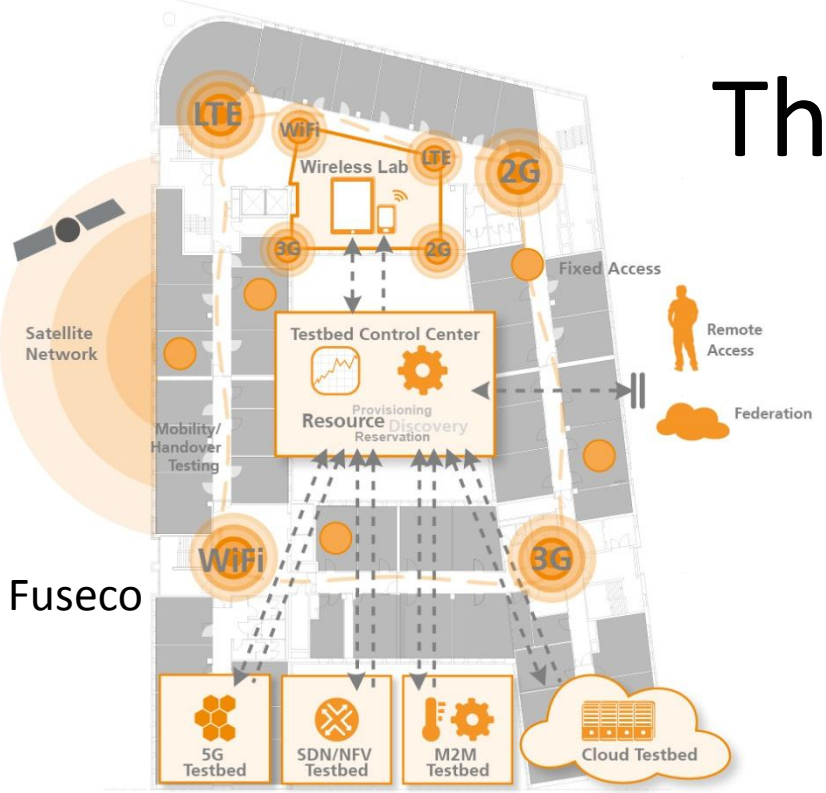
Logical View of the SoftFIRE Testbed



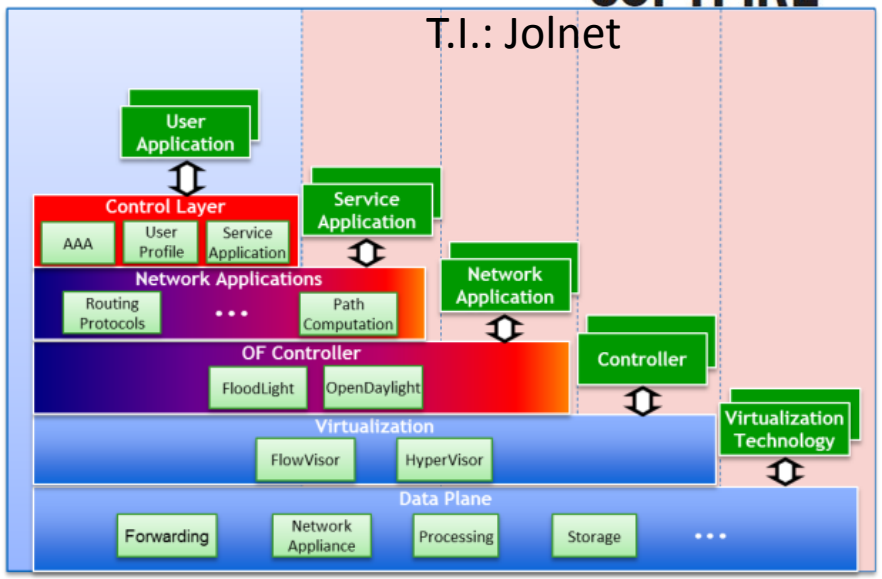
The Test Beds

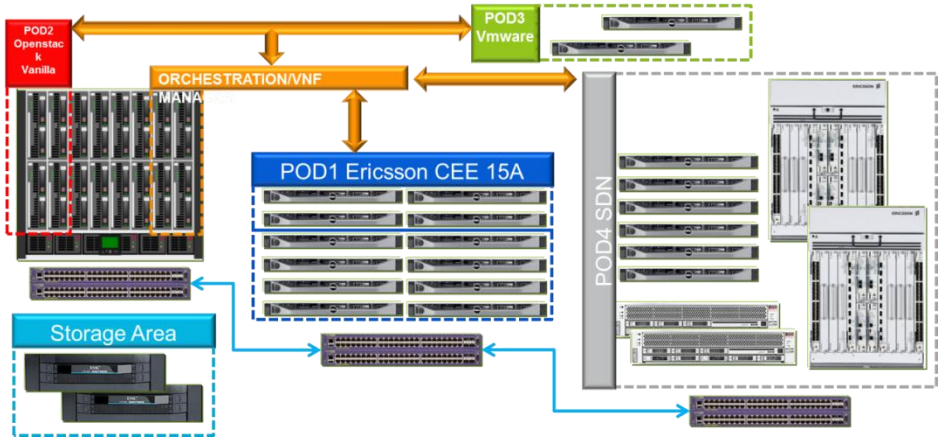
SOFTFIRE

Fuseco

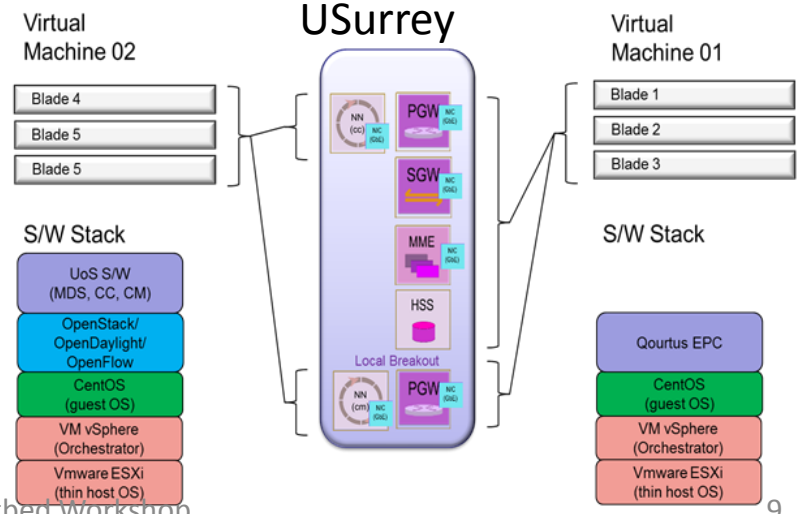


T.I.: Jolnet

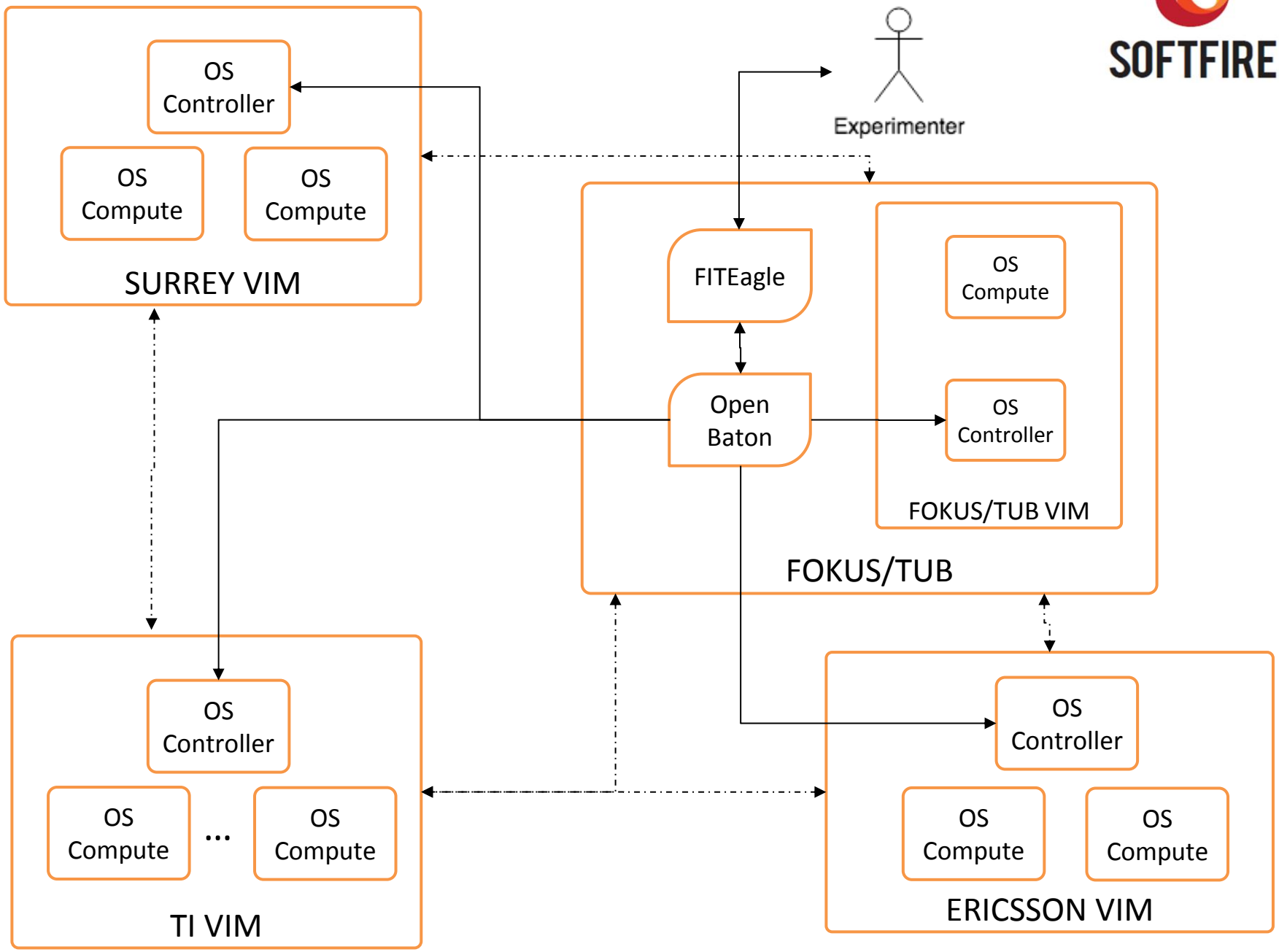




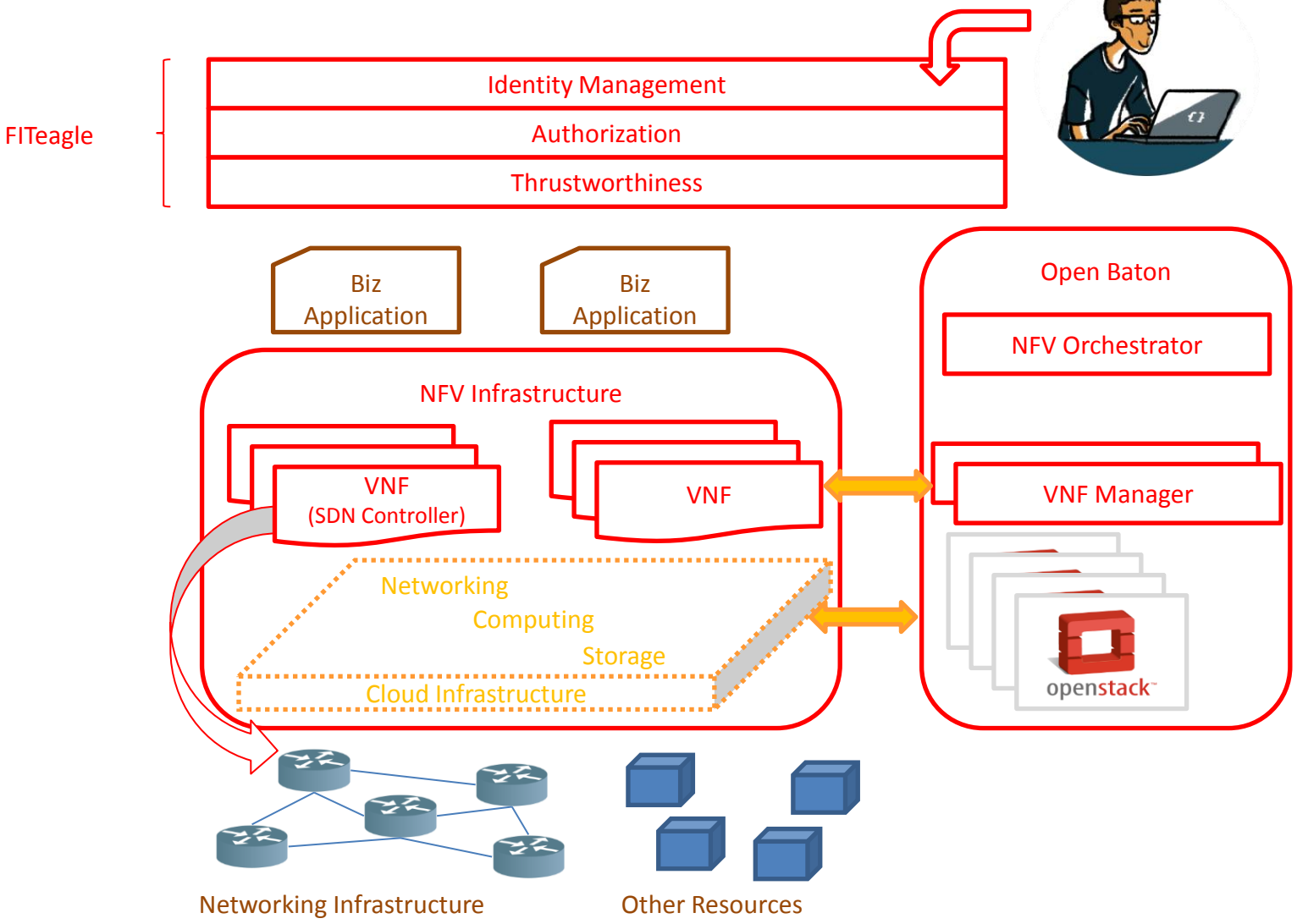
USurrey



Infrastructure architecture



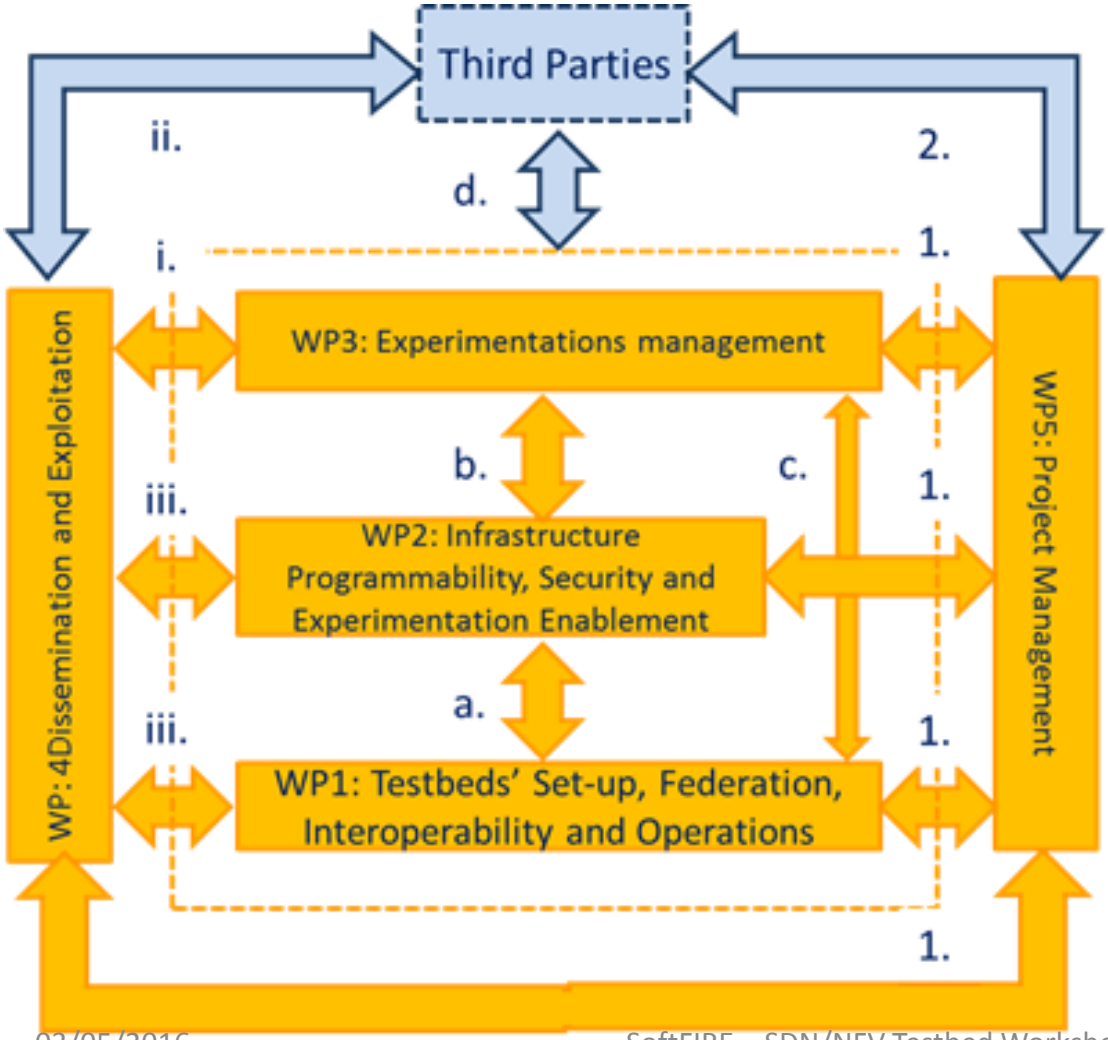
The Agreed Logical View



Approach and Methodology

- The SoftFIRE approach is very straightforward and effective.
  - The project's partners will provide a viable testbed for experimentation. It will support interoperability and it will provide programmable interfaces and basic security functions.
  - On top of this platform Third parties will be called to develop services and application by means of several waves of Open Calls. Third parties will also be engaged and challenged in order to develop specific extensions or functionalities useful for the testbed. Those particularly appealing could be integrated in the platform on a permanent basis.
- All these activities will be measured against a set of KPIs defined at the very beginning of the project in order to evaluate the three main properties of the testbed: interoperability, programmability and security. The project partners and the Third parties will be requested to evaluate the Testbed against the KPIs.
- In addition, Third parties will be provided with rules, guidelines and minimal tools in order to make effective use of the testbed. This will constitute a first bulk of operations for managing the access of testbed services and functionalities.

The Project Structure



Legenda

Testbed related relationships

a. Usage and integration of testbed functionalities in order to build and consolidate the testbed federation
b. Integration and usage of service and security functions in order to offer a secure programmability framework
c. Integration and usage of testbed functions in order to provide and assess interoperability
d. Usage and exploitation of testbed interfaces and functions for the construction of services and evaluation/challenge of testbed functionalities

Ecosystem related relationships

i. Suggestions and improvement from an a platform provider perspective
ii. Suggestion and recommendationfro Third parties
iii. Specifc technical suggestions

Assessment and Evaluation

1. Project management
2. Ecosystem Management and Fund allocation

A few Milestones

- Milestones at M06
  - M2.1:NFV/SDN/MEC experimentation service ready for 1st open call wave
- Milestones at M12
  - M2.2: NFV/SDN/MEC experimentation service ready for 2nd open call wave
  - M2.3: Tool for monitoring illegal accesses and control and extract sensitive information regarding performance and threat monitor across the entire network
- Milestones at M18
  - M2.4: NFV/SDN/MEC experimentation service ready for 3rd open call wave
  - M2.5: Tool for programmatic control of security polices
- Milestones at M24
  - M2.6:Tool for Use the flexible path management to isolate the intrusions
- Milestones at M09
  - M3.1 Start of First Wave: PlugTest.
- Milestones at M12
  - M3.2Start of Second Wave: Hackathon on SoftFIRE testbed
- Milestones at M15
  - M3.3 Start of Third Wave: Hackathon on SoftFIRE Testbed
- Milestones at M19
  - M3.4 Start of Challenge to SDN/NFV community on SoftFIRE testbed

Nurturing an Ecosystem

- The project will interconnect the different available testbeds, and will extend available functionalities and APIs
- Three waves of Open Calls for experimentation at M05, M11 and M16.
- A first Plug Test at M06 to test initial interoperability
- Other 2 Hackatons at M12 and M18 to nurture and assess an available ecosystem
- A final challenge at M23 to assess the maturity level of the federated testbed

OPEN CALLS

Expected Impacts

- The creation of a federated Platform that can foster the studies towards 5G
- The definition of KPIs and the initial proposition of best practices
- The strong integration of Security with platform development.
- The creation and support for a rich SDN/NFV ecosystem
- The possibility to interact and create further linkages with similar initiatives in USA, ASIA and elsewhere
- Strong interaction with FIRE+ community
- Influence to standards (ETSI, others …)

An Important Byproduct

- All these testbeds will be operated in different ways (from no operation to pre-industrial operation)
- Providing a federation will push for common guidelines and rules
- They could be the basis for defining initial best practice for an effective Operation of these new platforms.
- SoftFIRE is engaged also in this objective

Some Initial Findings - General

- NFV is usually looked at as a major goal
  - Network functions virtualization is used for many existing capabilities
  - Orchestration still a major issue with proprietary and experimental solutions
- SDN is lagging a bit behind in terms of real implementations
- Lack of integration between the two technologies
- General lack of already well virtualized solutions
- These platform are focusing more on the «proof of concept» and less on Management
- Security is usually not a concerns and it is disregarded

Some initial Findings

- Interoperability
  - Same version of OpenStack make life easier, other platforms or different version require a lot of tuning
  - Need for competences on OpenStack (it is time consuming to move to newer versions)
  - Interworking at the physical and transport level is «easy» unless of stringent SECURITY requirements
    - Many companies require stringent processes for opening up interfaces and systems to third parties. There is NOT a simple or standard policy for doing so
  - Interoperability at the level of software is difficult to achieve
    - User identity, segmentation and slicing, security concerns

Interoperability - End to End QoS

- Very different platforms with significantly different goals
  - Form NFV to 5G demostation
- Differentiation between KPIs
  - Platform related → should be supported by each test bed
  - Service/application related → strongly service specific should be implemented within the service
- Platform related KPIs: so far more than 60 different KPIs under consideration
  - They cover almost all the aspects of the Service Life Cycle (from setting up to running and closing the exeprimentation)
  - Use of Zabbix for collecting info, need time to understand and define general KPIs
  - There is a need for a framework for user defined and controlled KPIs

Programmability

- Lack of standard process for programming the platform
  - Handbooks and manual are missing in a large part of them (with few eccption)
  - Programmers have to have a strong relationship with platform providers
  - Lack of a large set of virtualized and programmable functionalities
  - Need to understand how to represent in the platfor (description languages, interfaces, …) new functionalities
- SDN and NFV are not integrated yet
  - SDN controllers are not usually provided
  - Programmers have to define their own resources

Security

- A general lack of attention to security (very detrimental for NFV/SDN)
- Prototypes very keen to hacking
- Virtualization alone doesn’t guarantee security
- Needs to define process and an information model for accessing and collecting security related information