i-nergy

Artificial Intelligence for Energy

AI4Europe discussions: Security collaboration

Timotej Gale / ComSensus

27 January 2023

Online

Outline

I-NERGY introduction

Security Framework (T3.6) overview and approach

Potential collaboration directions

I-NERGY vision/objectives

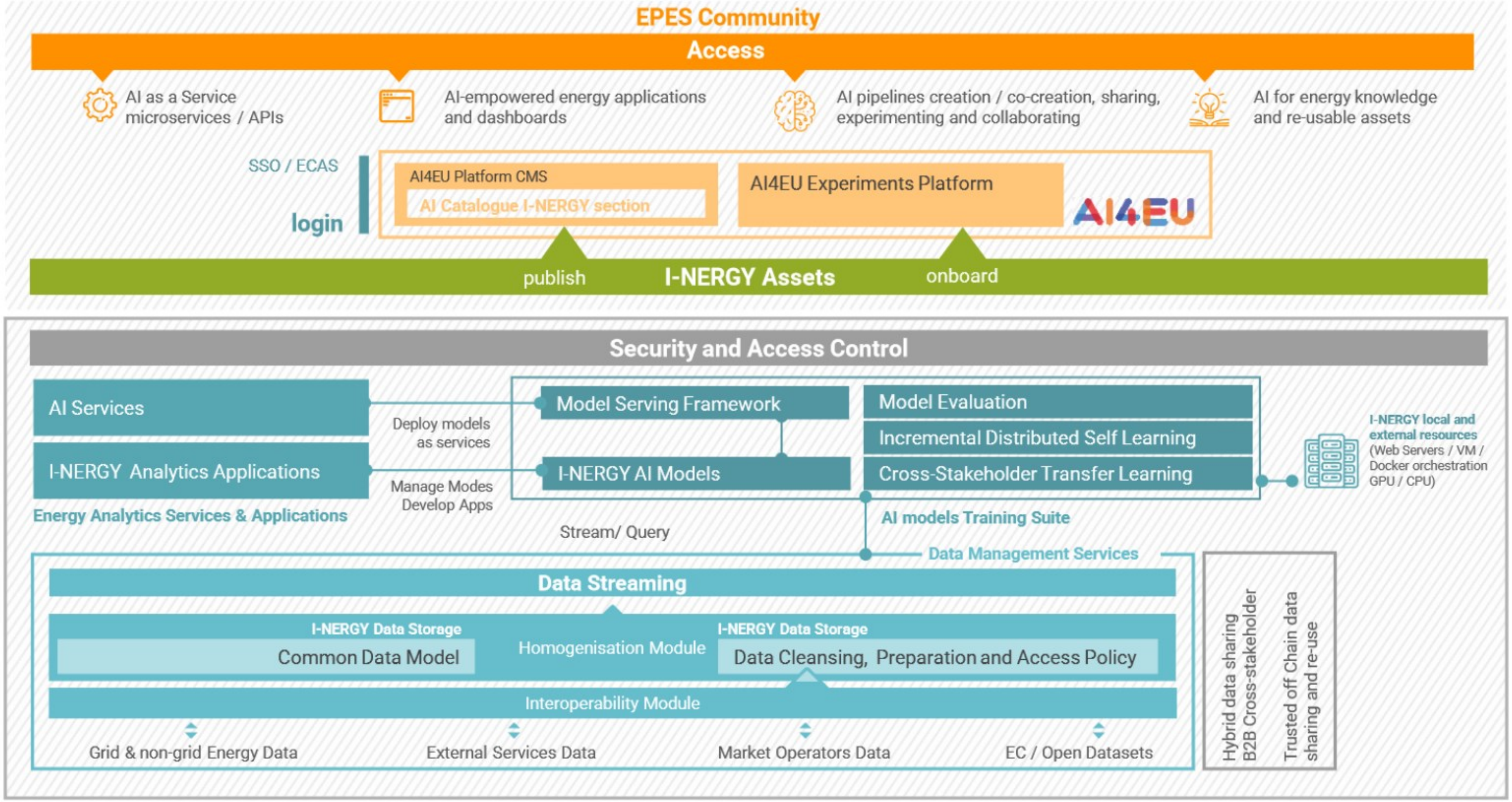
Deliver an energy-specific **open modular framework for supporting AI-on-Demand in the energy sector (AI4 Energy)**

Based on state-of-the-art AI and Data technologies

O1. Reinforce the service layer of the AI-on-demand-platform:

O2. Reach out to new user domains and boost~~ing~~ the use of the platform through use cases and small-scale experiments:

I-NERGY Conceptual Architecture



EPES Community

Access

AI as a Service microservices / APIs

AI-empowered energy applications and dashboards

AI pipelines creation / co-creation, sharing, experimenting and collaborating

AI for energy knowledge and re-usable assets

SSO / ECAS

login

AI4EU Platform CMS

AI Catalogue I-NERGY section

AI4EU Experiments Platform

AI4EU

publish

I-NERGY Assets

onboard

Security and Access Control

AI Services

I-NERGY Analytics Applications

Energy Analytics Services & Applications

Deploy models as services

Manage Modes Develop Apps

Model Serving Framework

I-NERGY AI Models

Model Evaluation

Incremental Distributed Self Learning

Cross-Stakeholder Transfer Learning

AI models Training Suite

I-NERGY local and external resources (Web Servers / VM / Docker orchestration GPU / CPU)

Stream/ Query

Data Management Services

Data Streaming

I-NERGY Data Storage

Common Data Model

Homogenisation Module

I-NERGY Data Storage

Data Cleansing, Preparation and Access Policy

Interoperability Module

Grid & non-grid Energy Data

External Services Data

Market Operators Data

EC / Open Datasets

Hybrid data sharing B2B Cross-stakeholder

Trusted off Chain data sharing and re-use

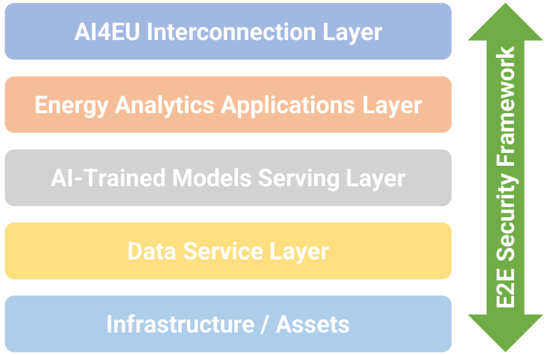
T3.6: Objectives and scope

Objectives

- Provide high-level **security**, fine-grained **access control**, **anonymization** and **encryption** across the architectural components
  - data exchange, data analytics, energy and building services
- Guarantee that the **platform** keeps the information safe, prevents any unauthorized actions and enhances the trustfulness among stakeholders, taking into account legal and security policies and mechanisms
  - authentication, authorization, auditing, policy-based management, and data encryption
- Every developed component will undergo a **validation process** against data protection requirements

Key concepts

- Privacy
- Anonymization
- Authentication, Authorization, Auditing
- Encryption
- Vulnerabilities/flaws detection and mitigation
- Involved entities: data, infrastructure/assets, services + AI/ML/BD, end-users


AI4EU Interconnection Layer
Energy Analytics Applications Layer
AI-Trained Models Serving Layer
Data Service Layer
Infrastructure / Assets
E2E Security Framework

Inputs

- WP2 architecture
- WP3 data services requirements
- WP4 AI services requirements
- Cloud infrastructure
- AI4EU interconnection

Outputs

- Platform deployment and services instantiation

T3.6: Overview

Security Framework is an I-NERGY vertical layer, spanning all I-NERGY components/assets, which provides high-level security, fine-grained access control, auditing, management and encryption of inter-service traffic, …

Approach, toolset

Keycloak

Authentication, auditing, fine-grained authorization policies

Istio

Service mesh microservices composition for application-level security and secure service integration

Wazuh

Vulnerability detection and mitigation, threat intelligence framework

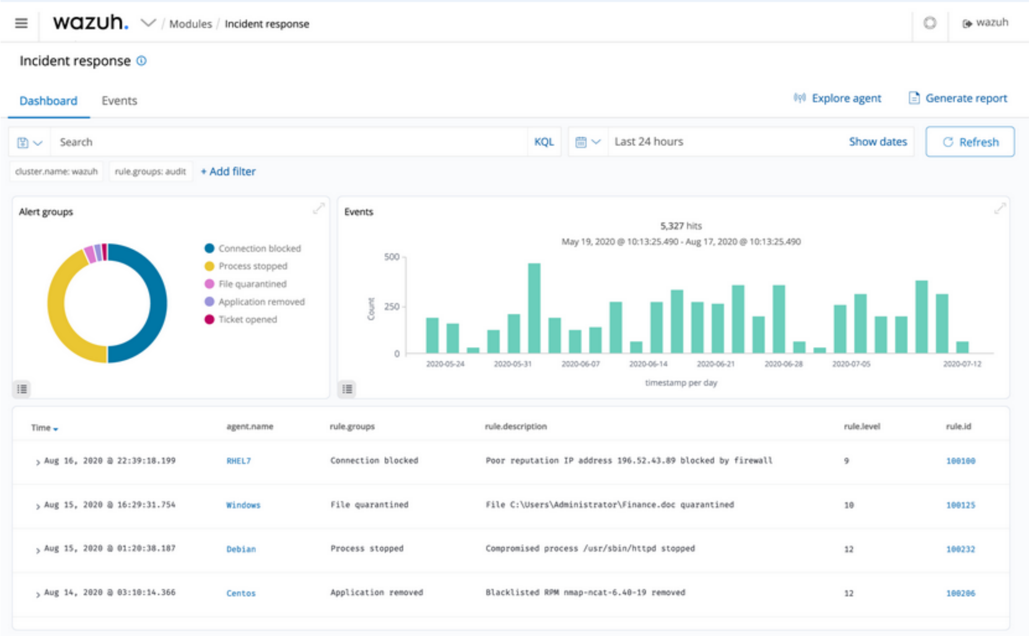
Wazuh – overview

An open-source platform enabling security data monitoring and analysis, focusing on endpoint/cloud security, threat intelligence and security operations

Central cloud platform <> distributed lightweight agents

Features:

- Configuration assessment
- File integrity monitoring
- Threat hunting
- Vulnerability detection
- Log data analysis
- Malware detection
- Audit and compliance
- Container security
- …



Time	agent.name	rule.groups	rule.description	rule.level	rule.id
Aug 16, 2020 @ 22:39:18.199	RHEL7	Connection blocked	Poor reputation IP address 196.52.43.89 blocked by firewall	9	100100
Aug 15, 2020 @ 16:29:31.754	Windows	File quarantined	File C:\Users\Administrator\Finance.doc quarantined	10	100125
Aug 15, 2020 @ 01:20:38.187	Debian	Process stopped	Compromised process /usr/sbin/httpd stopped	12	100232
Aug 14, 2020 @ 03:10:14.366	Centos	Application removed	Blacklisted RPM nmap-ncat-6.40-19 removed	12	100206

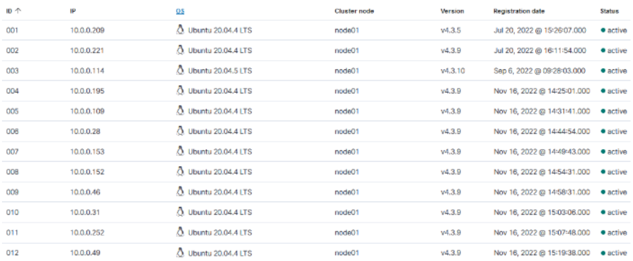
Wazuh in I-NERGY

Security and vulnerability monitoring on all I-NERGY cloud resources via Wazuh agents

Cloud environment compliance analysis

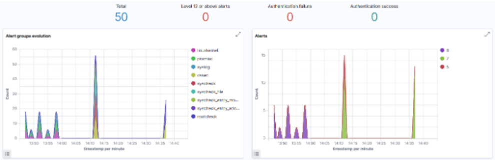
Cloud environment hardening (primarily OS-level)

Penetration testing using common attacks



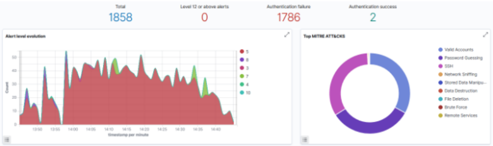
ID ↑	IP	OS	Cluster node	Version	Registration date	Status
001	10.0.0.209	Ubuntu 20.04.4 LTS	node01	v4.3.5	Jul 20, 2022 @ 15:26:07.000	● active
002	10.0.0.221	Ubuntu 20.04.4 LTS	node01	v4.3.9	Jul 20, 2022 @ 16:11:54.000	● active
003	10.0.0.114	Ubuntu 20.04.5 LTS	node01	v4.3.10	Sep 6, 2022 @ 09:28:03.000	● active
004	10.0.0.195	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 14:25:01.000	● active
005	10.0.0.109	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 14:31:41.000	● active
006	10.0.0.28	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 14:44:54.000	● active
007	10.0.0.153	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 14:49:43.000	● active
008	10.0.0.152	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 14:54:31.000	● active
009	10.0.0.46	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 14:58:31.000	● active
010	10.0.0.31	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 15:03:06.000	● active
011	10.0.0.252	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 15:07:48.000	● active
012	10.0.0.49	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 15:19:38.000	● active

Figure 2: Agent list view in Wazuh dashboard.



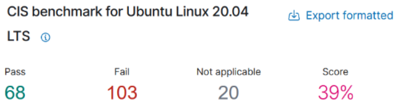
Total 50
Level 12 or above alerts 0
Authentication failure 0
Authentication success 0

Figure 3: Wazuh overview during normal functionality of the system.



Total 1858
Level 12 or above alerts 0
Authentication failure 1786
Authentication success 2

Figure 4: Wazuh overview during abnormal functionality of the system.



CIS benchmark for Ubuntu Linux 20.04 LTS

Pass	Fail	Not applicable	Score
68	103	20	39%

Figure 6: CIS benchmark result of the master node.

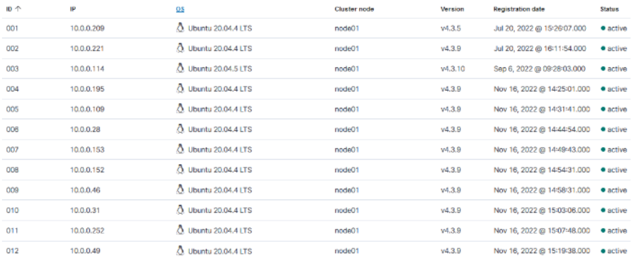
Wazuh and AIoD Platform

Are there use cases for Wazuh in the AIoD Platform?

Security scans for Docker containers that are referenced by the platform? E.g. AI4EU Experiments?

Security Scans for other types of artifacts?

Sustainability: who could operate the the server beyond I-Nergy project?



ID ↑	IP	OS	Cluster node	Version	Registration date	Status
001	10.0.0.209	Ubuntu 20.04.4 LTS	node01	v4.3.5	Jul 20, 2022 @ 15:26:07.000	● active
002	10.0.0.221	Ubuntu 20.04.4 LTS	node01	v4.3.9	Jul 20, 2022 @ 16:11:54.000	● active
003	10.0.0.114	Ubuntu 20.04.5 LTS	node01	v4.3.10	Sep 6, 2022 @ 09:28:03.000	● active
004	10.0.0.195	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 14:25:01.000	● active
005	10.0.0.109	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 14:31:41.000	● active
006	10.0.0.28	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 14:44:54.000	● active
007	10.0.0.153	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 14:49:43.000	● active
008	10.0.0.152	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 14:54:31.000	● active
009	10.0.0.46	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 14:58:31.000	● active
010	10.0.0.31	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 15:03:06.000	● active
011	10.0.0.252	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 15:07:48.000	● active
012	10.0.0.49	Ubuntu 20.04.4 LTS	node01	v4.3.9	Nov 16, 2022 @ 15:19:38.000	● active

Figure 2: Agent list view in Wazuh dashboard.

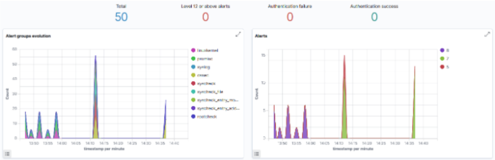


Figure 3: Wazuh overview during normal functionality of the system.

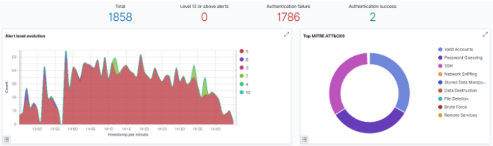
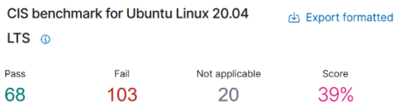


Figure 4: Wazuh overview during abnormal functionality of the system.



CIS benchmark for Ubuntu Linux 20.04 LTS

Export formatted

Pass	Fail	Not applicable	Score
68	103	20	39%

Figure 6: CIS benchmark result of the master node.

Potential collaboration directions regarding Wazuh

AIOD platform and related infrastructure:

- Security/vulnerability scanning
- Continuous security/vulnerability monitoring
- Penetration testing
- Compliance benchmarking, e.g., CIS (OS images etc.)
- Security hardening

Security/vulnerability scanning of new/existing uploaded/onboarded AIOD assets (or periodic)

…

Keycloak – overview

Keycloak AAM (https://www.keycloak.org/)

Open-source identity and access management platform

Features:

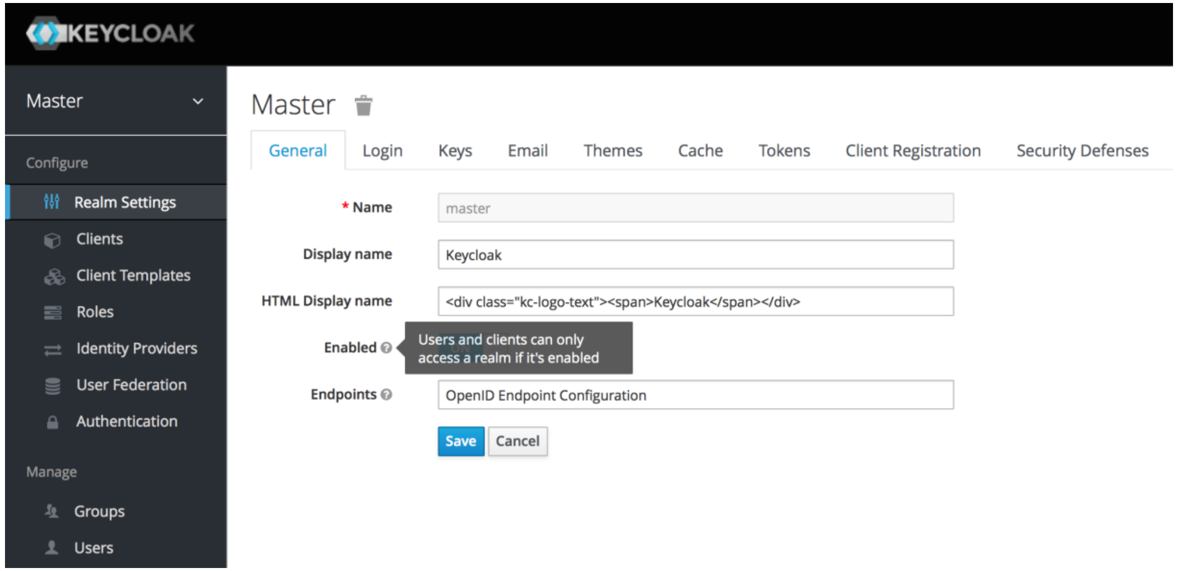
Admin Console, Account Management Console, Standard Protocols (support for OpenID Connect, OAuth 2.0, and SAML), Single-Sign On, Identity Brokering and Social Login, User Federation, Client Adapters

Keycloak authorization

Attribute-based access control (ABAC), Role-based access control (RBAC), User-based access control (UBAC), Context-based access control (CBAC), Rule-based access control, Time-based access control, Custom access control mechanisms (ACMs)

Keycloak auditing

Event logs



* Name: master

Display name: Keycloak

HTML Display name: <div class="kc-logo-text"><span>Keycloak</span></div>

Enabled: Users and clients can only access a realm if it's enabled

Endpoints: OpenID Endpoint Configuration

Keycloak in I-NERGY

Authentication and authorization

- Role-based access control (RBAC)
- Event logs and auditing

Each I-NERGY service or tool integrates a Keycloak client adapter (OpenID Connect protocol)

EU Login (ECAS) integration via Keycloak as identity provider

Open Questions regarding Keycloak and AIoD

Packaging Keycloak as a (preconfigured?) Docker AAM extension for some AIOD assets

Common SSO, EU Login for services/tools, or uploaded assets?

How could EU-Login and Keycloak be integrated?

- cascaded? => Contradicts EU-Login usage policy...
- Can EU-Login be used for authorization => take the role of Keycloak?
- Shall each subsystem be responsible for fine grained permissions?
- Who could operate Keycloak beyond I-Nergy project?
- What are the positions of the EC and AI4Europe on this?

…

i-nergy
Artificial Intelligence for Energy

Thank you!

Timotej Gale, ComSensus

@inergy_h2020 I-NERGY Project contact@i-nergy.eu | www.i-nergy.eu

I-NERGY project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 101016508