ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

D7.3

First Period Dissemination, Standardization and Outreach Report

This deliverable presents the first results of the ANASTACIA Task 7.1 which aims to identify the metrics in order to raise awareness thanks to the presentations, workshops and conferences.

Distribution level	PU
Contractual date	30.06.2018 [M18]
Delivery date	02.07.2018 [M19]
WP / Task	WP7 / T7.1
WP Leader	THALES
Authors	S.A.NAAS, A. Laghrissi, T. Taleb (AALTO), R.Marín Pérez (ODINS), D.Belabed (THALES), E.Cambiaso, (CNR), S.Bianchi (SOFT), M.Sethi, N.Beijar (ERICSSON)
EC Project Officer	Carmen Ifrim carmen.ifrim@ec.europa.eu
Project Coordinator	SoftecoSismatSpA Stefano Bianchi Via De Marini 1, 16149 Genova – Italy +39 0106026368 stefano.bianchi@softeco.it
Project website	www.anastacia-h2020.eu

ANASTACIA has received funding from the European Union's Horizon 2020 research and innovation programmeunder Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

Table of contents

Index of figures

PUBLIC SUMMARY

This document outlines the standardization, dissemination and exploitation achievements and activities within the ANASTACIA project. It also identifies the main metrics to raise awareness through presentations, workshops, conferences, and other events.

1 INTRODUCTION

1.1 AIMS OF THE DOCUMENT

This document represents the first results of ANASTACIA's WP7.Itpresents the main dissemination activities and events held to raise awareness on the project achievements within the community of researchers and industrials. These events consist of workshops, presentations and conferences.

WP7 is responsible for the dissemination and outreach activities while receiving contributions from other work packages [1].

This document is structured as follows. Section 2 presents the dissemination activities of the project partners. Section 3 presents the different standardization activities conducted in ANASTACIA. Outreach and Conclusions are drawn in Sections 4 and 5, respectively.

1.2 APPLICABLE AND REFERENCE DOCUMENTS

This document refers to the following documents:

- ANASTACIA project deliverable D7.1 - Initial Dissemination, Standardization, and Outreach Strategy Plan

1.3 REVISION HISTORY

Version	Date	Author	Description
0.1	24.6.2018	Si-Ahmed NAAS	First draft of D7.3
0.2	28.6.2018	Si-Ahmed NAAS	Content for Chapter 4-6
1.0	01.7.2018	Tarik Taleb	Editorial corrections, Final

1.4 Acronyms and Definitions

Acronym	Meaning
CGA	Cryptographically Generated Address
EAP	Extensible Authentication Protocol
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IoT	Internet-of-Things
LWIG	Light Weight Implementation Guidance
T2TRG	Thing-to-Thing Research Group
SDO	Standards Development Organization
GIoTS	Global Internet of Things Summit
IRSG	Internet Research Steering Group
EVE	Evolution & Ecosystems
ISG	Industry Specification Group
LI	Lawful interception
SBA	Service Based Architecture
ONAP	Open Network Automation Platform
ADMF	administrative function
SDNs	Software Defined Networks
NFVs	Virtual Network Functions
AAF	Application Authorization Framework
SEC	Security Subcommittee
STIX	Structured Threat Information Expression
SDOs	STIX Domain Objects
SROs	STIX Relationship Objects
SOL	solution

2 DISSEMINATION

In this section, we present the different publications and dissemination activities conducted by the project partners.

- **Publications:**
  - Y. Khettab, M. Bagaa, D. Dutra, T. Taleb, and N. Toumi, “Virtual Security as a Service for 5G Verticals,” in Proc. IEEE WCNC 2018, Barcelona, Spain, Apr. 2018.
  - A.M. Zarca, J.B. Bernabe, I. Farris, T. Taleb, A. Skarmeta, and Y. Khettab, “Enhancing IoT Security through Network Softwarization and Virtual Security Appliances,” in ACM Int’l J. of Network Management
  - H. Sedjelmaci, S.M. Senouci, and T. Taleb, “An Accurate Security Game for Low-Resource IoT Devices,” in IEEE Trans. Vehicular Technology, Vol. 66, No. 10, Oct. 2017, pp. 9381 – 9393.
  - S. Lal, A. Kalliola, I. Oliver, K. Ahola, and T. Taleb, “Securing VNF Communication in NFVI,” in Proc. IEEE CSCN’17, Helsinki, Finland, Sep. 2017.
  - I. Farris, J.B. Bernabe, N. Toumi, D. Garcia, T.Taleb, A.F. Skarmet, and B. Sahlin, “Towards Provisioning of SDN/NFV-based Security Enablers for Integrated Protection of IoT Systems” in Proc. IEEE CSCN’17, Helsinki, Finland, Sep. 2017.
  - M. Bouet and V. Conan, “Geo-partitioning of MEC Resources,” in Proceedings of the Workshop on Mobile Edge Communications, New York, NY, USA, 2017, pp. 43–48.
  - M. Bouet and V. Conan, "Mobile Edge Computing Resources Optimization: A Geo-Clustering Approach," in IEEE Transactions on Network and Service Management, vol. 15, no. 2, pp. 787-796, June 2018.
  - I. Vaccari, E. Cambiaso and M. Aiello, "Remotely Exploiting AT Command Attacks on ZigBee Networks", Security and Communication Networks, vol. 2017, pp. 1-9, 2017.
    Link to the publication:
    https://doi.org/10.1155/2017/1723658
  - E. Cambiaso, G. Papaleo and M. Aiello, "Slowcomm: Design, development and performance evaluation of a new slow DoS attack", Journal of Information Security and Applications, vol. 35, pp. 23-31, 2017.
    Link to the publication:
    https://doi.org/10.1016/j.jisa.2017.05.005
  - Alejandro Molina, Dan Garcia, Jorge Bernal, Jordi Ortiz, Rafael Marin-Perez, Antonio Skarmeta. "Managing AAA in NFV/SDN-enabled IoT scenarios", the Global Internet of Things Summit (GIoTS), 2018.

❖ **Dissemination:**

- IoTitaly is one of the pioneer events on the contributions around IoT in Italy. Held in Genoa on February 9, 2018. It was the perfect opportunity to present the ANASTACIA framework and activities.

- The first Cyberwatching.eu (Figure 1) Concertation Meeting took place in Brussels on April 26, 2018; with over 75 participants, 50 Projects represented and 48 Service Offers.UMU, as the technical coordinator, presented the ANASTACIA project. This event was an excellent opportunity to exchange ideas and information over what other projects are working on, and identify collaboration opportunities.

Figure1. The first the Cyberwatching.eu Concertation Meeting in Brussels 26th April 2018

- The International Event on IoT Solutions World Congress 2017 took place in Barcelona on October 3-5, 2017 with more than 14000 visitors from over 120 countries (Figure 2). During two days of this event, the ANASTACIA project was presented in an exhibition panel. Visitors were very interested in security and privacy solutions in order to obtain seals or certifications for private clients and IoT deployments. Link to the event:
  www.iotsworldcongress.com

- The ANASTACIA project was also promoted using regional and national associations and companies of innovative technologies such as CENTIC, CEEIM, and Planetic (Spanish technological platform for the diffusion of electronic and information and communications technologies). Links to the events:
  centic.es/odinsproyecto-anastacia-iot/

  https://www.ceeim.es/odins-participa-proyecto-europeo-anastacia-iot/

http://www.planetic.es/sites/default/planeticfiles/content-files/articles/Proyecto-ANASTACIA.pdf

Figure 2. The International Event on IoT Solutions World Congress 2017- Barcelona

❖ **Social Media outreach:**

- Creation of a Website and Social Media Accounts (e.g., Linkedin and Twitter) with more than 1000 followers in order to promote the ANASTACIA project among our networks of Clients, Suppliers, Partners of IoT products:
  - http://www.odins.es/en/project/anastacia-seguridad-confianza-en-arquitecturas-it/
  - https://twitter.com/odinsolutions
  - https://www.linkedin.com/in/odinsolutions

3 STANDARDIZATION

During the first period, the members of the consortium have been actively involved in Standards Development Organization (SDOs), affecting the direction of standardization with inputs and standards contributions. In addition to direct contribution, ANASTACIA monitors the development in the SDOs and aligns its work accordingly.

3.1 UPDATE ON STANDARDIZATION ACTIVITIES

In this section, we provide an overview of the main standardization activities related to the ANASTACIA project during the first period. This overview complements the description provided in Deliverable D7.1 with the latest development.

3.1.1 STANDARDIZATION ACTIVITIES IN IETF

Ericsson is involved in several IETF activities of which some are related to IoT security. Within ANASTACIA, Ericsson has produced an IETF contribution documenting the implementation experiences of public-key cryptography on small devices. The draft was approved by the IESG (Internet Engineering Steering Group) in March 2018 and published as RFC 8387. It is available online in https://tools.ietf.org/html/rfc8387. The RFC shows that it is often incorrectly assumed that resource-constrained IoT devices cannot perform cryptographic operations needed for strong security. This document presents our experiences of implementing RSA and Elliptic Curve Cryptography on small micro-controllers and introduces them to the Light Weight Implementation Guidance (LWIG) working group of the IETF. The RFC is one of the main standardization contributions planned to be produced in ANASTACIA. Based on our continuous contributions and voluntary work, Mohit Sethi from Ericsson was appointed as the co-chair of the LWIG working group.

We have submitted a draft updating EAP-TLS given that we have a new version of TLS namely, version 1.3 (https://tools.ietf.org/html/draft-mattsson-eap-tls13-02). This document will update RFC 5216. We have been instrumental in starting the EAP method update working group at the IETF. The working group charter was approved by the IESG in February 2018. We also have a draft contribution for secure bootstrapping of IoT devices. This contribution would extend the Extensible Authentication Protocol (EAP) framework and define a method for out-of-band (OOB) authentication and key derivation (https://tools.ietf.org/html/draft-aura-eap-noob-02). This EAP method is intended for bootstrapping all kinds of Internet-of-Things (IoT) devices that have a minimal user interface and no pre-configured authentication credentials. We have been updating the open-source implementation of the EAP-NOOB protocol: https://github.com/tuomaura/eap-noob together with Aalto University. Additionally, we are working on developing a formal model of the protocol to verify its correctness. Lastly, we are currently planning an internal implementation of EAP-TLS with TLS 1.3 before making final changes to the draft.

The overview document on IoT security that is part of the Thing-to-Thing Research group (T2TRG) (https://tools.ietf.org/html/draft-irtf-t2trg-iot-seccons-14) has now been reviewed and voted on by the leadership of the IRSG (Internet Research Steering Group). Note that the document has already undergone 3 revisions since the last report. We are now in the process of addressing the

feedback comments received during the IRSG vote. Thereafter, the document would be sent to the IESG for final checks before it is submitted to the RFC editor for publication. This document discusses the various stages in the lifecycle of an IoT device. It then documents the security threats to an IoT device and the challenges that one might face in order to protect against these threats. Lastly, it discusses the next steps needed to facilitate the deployment of secure IoT systems.

Our contribution on secure neighbour discovery for resource-constrained devices was updated in February 2018 based on feedback received (https://tools.ietf.org/html/draft-ietf-6lo-ap-nd-06). We have since received many security related questions from the IETF community as well as the security area directors (Eric Rescorla and Benjamin Kaduk). We have been answering the questions received which are now in the process of updating the draft before the next IETF. This contribution defines an extension to existing neighbour discovery mechanism specified in RFC 6775 to provide additional security. Nodes supporting this extension would rely on cryptographic addresses instead of EUI-64 addresses that are specified in RFC 6775. We had earlier reported that the working group is currently discussing the appropriate size of the identifiers. The working group has now concluded that it would use 256-bit identifiers for addressing. While this would increase the cost of routing marginally, the resource-constrained nodes would not have to solve cryptographic puzzles for registering cryptographic addresses (which was the case for Cryptographically Generated Address (CGAs) defined in RFC 3972).

3.1.2 STANDARDIZATION ACTIVITIES IN ETSI ISG NFV SEC

ETSI Industry Specification Group (ISG) for NFV is now at the release 3 specification stage. At release 3, the main focus is to develop normative specification for protocols and data models. In order to reflect that, plenty of work is currently ongoing at ETSI ISG NFV such as developing TOSCA based NFV descriptor spec (SOL001), YANG based NFV descriptor spec (SOL006), various RESTful protocol specifications (SOL002/ SOL003/ SOL005), etc.

From the ANASTACIA project perspective, the most interesting working group is the ETSI NFV SEC working group. Having said that, other working groups are getting involved in defining some security aspects, while defining the protocols. Therefore, now it is not only the SEC WG that is working on security, but other working groups such as solution (SOL) WG is also involved in defining some security requirements.

The SEC WG is moving steadily as there are now a lot of active work items. In the following, there is a summary of the active work items in the SEC WG as of March 8th, 2018:

- DGS/NFV-SEC005 (GR): Certificate management report
- DGS/NFV-SEC015 (GS): MANO Security spec
- DGR/NFV-SEC016 (GR): Location, locstamp and timestamp
- DGR/NFV-SEC017 (GR): Security Policy Guidelines Report
- DGR/NFV-SEC018 (GR): Remote Attestation Architecture report
- DGS/NFV-SEC019 (GS): System Architecture Spec for NFV Security enhancement
- DGS/NFV-SEC020 (GS): Identity Management & Security spec
- DGS/NFV-SEC021 (GS): VNF Package Security Spec
- DGS/NFV-SEC022 (GS): API Access Token Spec

At the moment, all of the work items are at a very early stage of their development. Only exception is the SEC005 work item, which have been much closer to publication yet due to some objections the future of this work item is currently unknown. Besides these active work items, SEC

WG is providing feedback on several other WG specifications. The most notable work items that the SEC WG has reviewed are from the Solution (SOL) WG and the Evolution & Ecosystems (EVE) WG on various topics such as VNF package security, network slicing, authentication and authorization for restful API, etc. Furthermore, the SEC WG has convinced other WGs to do a security analysis of their own specifications. Meaning that all the specifications developed by other WGs have to write a section on security analysis. This is a very high-level analysis to outline the assets, most common known threats and some mitigation. SEC WG is currently reviewing and providing feedback to this security analysis work.

Lawful interception (LI) is a very important topic for the SEC WG. The initial study report (GR) on LI (SEC011) has been completed recently by the SEC WG and it is currently undergoing approval by remote consensus phase. The SEC WG has already taken initiative to start the next phase of LI i.e. to start normative specification of LI. During the last face to face meeting during NFV#21, the SEC WG has decided to start two new normative work items for LI. One work item will specify a more generic architecture that supports LI functionality not only in NFV scenario, but also in other cases e.g. 5G Service Based Architecture (SBA), Open Network Automation Platform (ONAP), Zero touch network and Service Management Industry Specification Group (ETSI ZSM ISG), etc. Within this work item, the plan is to specify the interface between a LI administrative function (ADMF) and the LI controller.

The second work item for LI related interface specification aims to specify the interfaces between the NFV MANO block and the Security controller that is defined in SEC013. The goal is to define the interface for security management purpose and these will be reused by the LI controller. This will reduce the duplication work and the number of interfaces required in the MANO block. Note that both of these work item are currently under discussion phase and these are yet to be submitted to the ETSI ISG NFV plenary for approval to become active work items.

In ETSI NFV, Ericsson will continue the work on virtualization security, and take applicable input from ANASTACIA into consideration.

3.1.3 STANDARDIZATION ACTIVITIES IN ONAP

The Open Network Automation Platform (ONAP) aims to provide a platform for policy driven, real-time orchestration of both virtualized and physical network functions. ONAP is an open source software platform that delivers capabilities for the design, creation, orchestration, monitoring, and life cycle management of Virtual Network Functions (VNFs), carrier-scale Software Defined Networks (SDNs) that contain them and higher-level services that combine the above. Since NFV orchestration is central in the ANASTACIA project, we follow the work of ONAP.

In essence, ONAP is the platform above the infrastructure layer that automates the network. Automation is the key for ONAP and it allows the end users to orchestrate products and services through the infrastructure and allows deployments of VNFs and scaling of the network in a fully automated manner.

This open source project is governed under the auspices of the Linux foundation. This initiative was started during 2017 when AT&T and China Mobile joined forces and submitted their internal projects ECOMP and Open-O respectively as seed codes for ONAP. Since then, it has been growing very fast and most of the major operators and vendors have already joined forces to develop ONAP into a de facto standard for NFV.

Figure 3 depicts the high-level architecture for ONAP from Amsterdam release (first release). As shown in the figure, ONAP is composed of many different software subsystems and all of which belong to two major architectural components. These two architectural components are a design-time environment and an execution-time environment. The design time environment provides functionalities to design, define and program the platform and the execution-time environment executes the logic programmed in the design phase. Additionally, the execution time environment provides additional functionalities such as security framework, health and performance measurement, analytics, etc. that are vital for managing a large automated system.

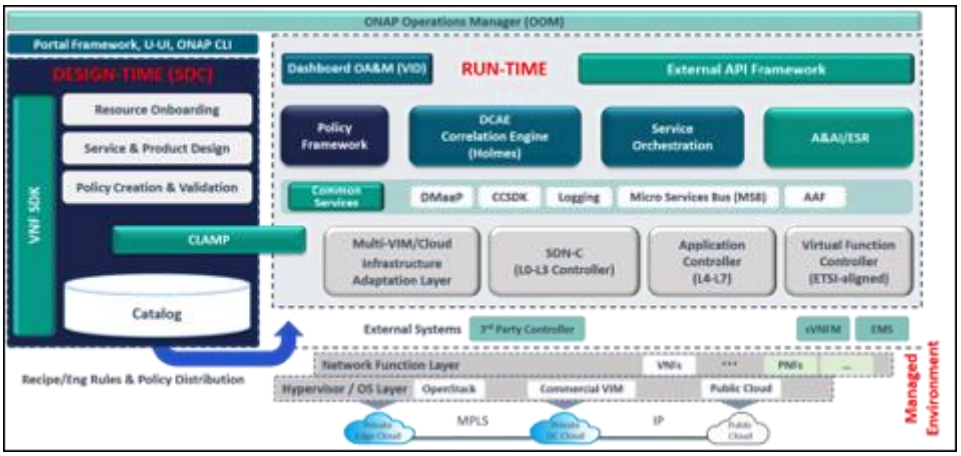


Figure 3: ONAP high-level architecture Amsterdam release [1]

ONAP has adopted a 6 months release cycle. Recently, in March 2018, ONAP has released the 2nd version of ONAP architecture which is called the Beijing release. In this release, the ONAP architecture has evolved and it is shown in Figure 4. The main changes towards the new architecture are to incorporate the new accepted projects and also to go for a more mature version focusing on micro service based architecture.

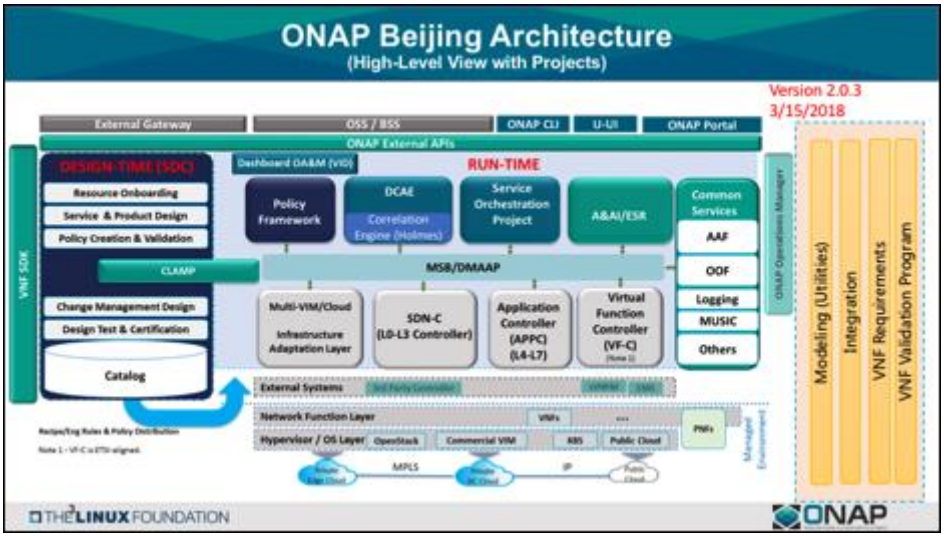


Figure 4: ONAP high-level architecture Beijing release [2]

From ANASTACIA project perspective, the most interesting project to look into ONAP is the Security Framework. It is an umbrella project for many of the security subsystems. AT&T is the main contributor to this part of the codebase using their OpenECOMP API-based Security Framework. One such set of APIs is the Application Authorization Framework (AAF), which in turn

calls external security platforms. Another interesting group within ONAP to influence and guide security is the Security Subcommittee (SEC). This is a technical steering committee for security in ONAP with the role of defining, promoting and proposing proactive security activities, providing best practices, security guidelines, etc.

3.1.4 STANDARDIZATION ACTIVITIES IN 3GPP

We plan to make 3GPP contributions based on the components of the ANASTACIA architecture and results from the rest of the work done during the project. The work for 3GPP includes contributions to develop the 5G system, including specific enhancements taking into account IoT specific requirements.

3GPP is currently focusing on standardization of 5G, where phase II is starting. Internet of Things and machine-to-machine communications are part of the main focus areas. Ericsson is active in 3GPP standardization and follows up on topics related to ANASTACIA.

3.1.5 STANDARDIZATION ACTIVITIES IN IEEE

UMU and MAND are vice-chairing the IEEE Communication Society Internet of Things Technical Committee, facilitating the development of standards, white papers, and other initiatives. In that sense, IEEE will serve as for a where we can use the IEEE IoT Initiativehttp://iot.ieee.org/ channels like the newsletter and the WF-IoT conference for communication and dissemination activities.

3.1.6 STANDARDIZATION ACTIVITIES IN OASIS

OASIS works on several topics relevant to ANASTACIA. In particular, ANASTACIA utilizes Structured Threat Information Expression (STIX) for incidence reports (CHECK). STIX is a language and serialization format used to exchange cyber threat intelligence, e.g. between organizations. Many aspects of suspicion, compromise and attribution can be represented with objects and descriptive relationships. Information can be visually represented or stored as JSON for easy automated processing. OASIS provides STIX as open source.

Currently, STIX defines the following STIX Domain Objects (SDOs): Attack Pattern, Campaign, Course of Action, Identity, Indicator, Intrusion Set, Malware, Observed Data, Report, Threat Actor, Tool, and Vulnerability. In addition, two STIX Relationship Objects (SROs) are defined: Relationship (linking two SDOs) and Sighting (indicating belief that an element of cyber trust intelligence was seen).

ANASTACIA follows the development of STIX with the optic of using it in the architecture. Based on the experience of using STIX, there may appear need for requesting new formats or changes to the current STIX definition. In that case, ANASTACIA will consider contributions to OASIS.

3.1.7 STANDARDIZATION ACTIVITIES IN ISO

We still consider the possibility of sharing relevant results of ANASTACIA related to the dynamic and privacy seal with ISO, especially with the technical committee ISO/IEC JTC.

4 OUTREACH

- ICT 2018 is a key European ICT research & innovation event organised by the European Commission, and will take place in Vienna on December 4-6, 2018. This research and innovation event will focus on the European Union's priorities in the digital transformation of society and industry. It will present an opportunity for the stakeholders involved in this transformation to share their experience and vision of Europe in the digital age. Project partners will attend the Exhibition event, where Connect Europe will include a 5 000m² exhibition area showcasing the best accomplishments and pioneering results of EU funded research and innovation actions. This will be a great opportunity to promote the ANASTACIA project and its outputs.

- Application for registration to the "cyberwatching.eu", which is the European observatory of research and innovation in the field of cybersecurity and privacyhttps://www.cyberwatching.eu/. The candidature has been accepted and the Anastacia project is available in the service catalogue of the "cyberwatching" since August 2017, on "https://www.cyberwatching.eu/services/catalogue-of-services/anastacia".Figure 5 presents the registration of ANASTACIA to the "cyberwatching.eu"

Figure 5. Registration of ANASTACIA to the "cyberwatching.eu"

5 ONLINE PRESENCE

In this section we present different statistics of web access and social media of ANASTACIA's project accounts.

5.1 WEBSITE

The ANASTACIA project's website is available at: http://www.anastacia-h2020.eu

As a single-page site with different sections: CONCEPT, FRAMEWORK, HIGHLIGHTS, TIMELINE, RESULTS, FIGURES, TEAM, IAB, CONSORTIUM, CONTACTS. In particular, the sections TIMELINE and RESULTS have been periodically updated to provide proper evidence of activities (meetings, events etc.) and deliveries (public deliverables, publications etc.). This is depicted in Figure 6 and Figure 7.

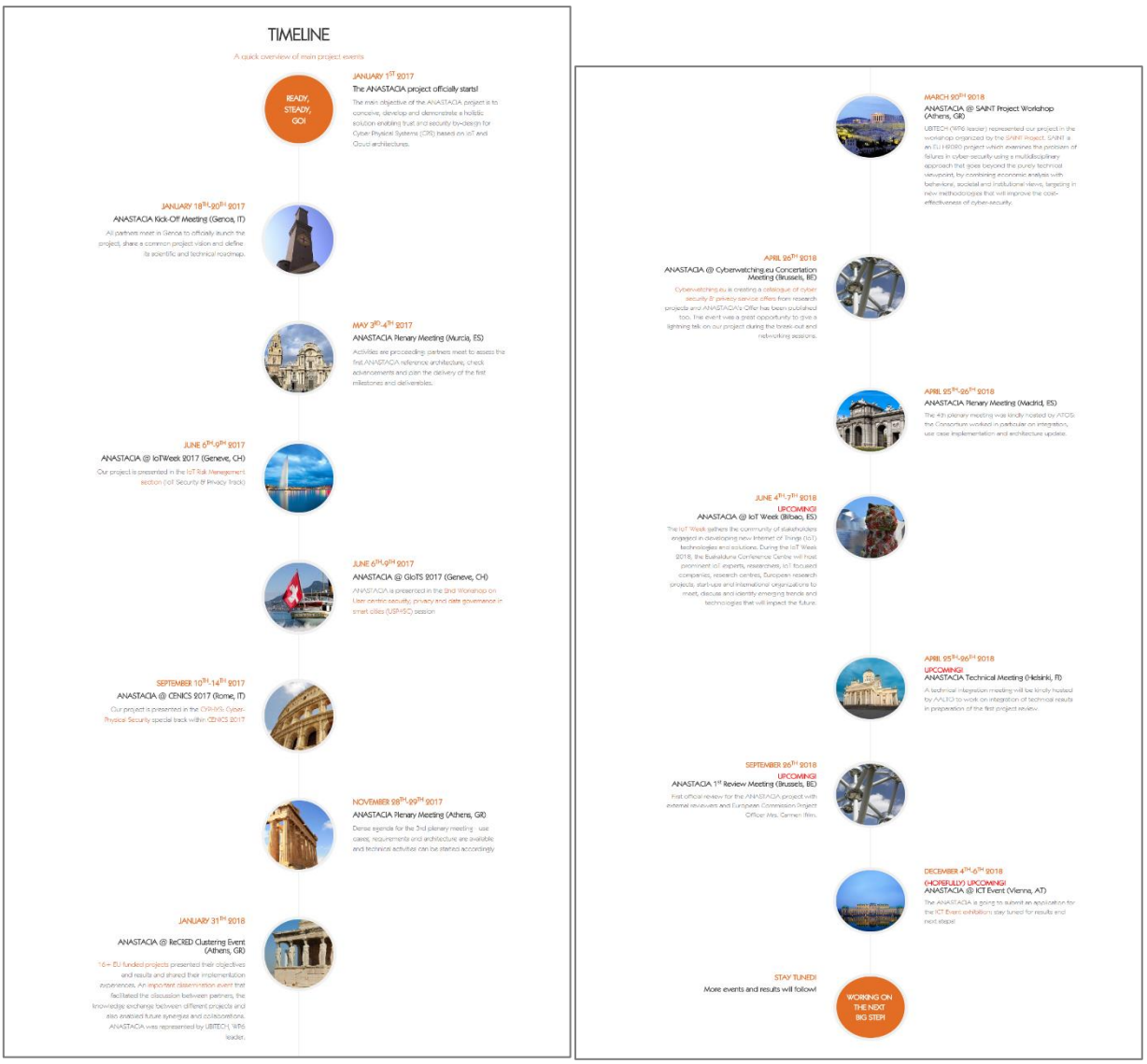
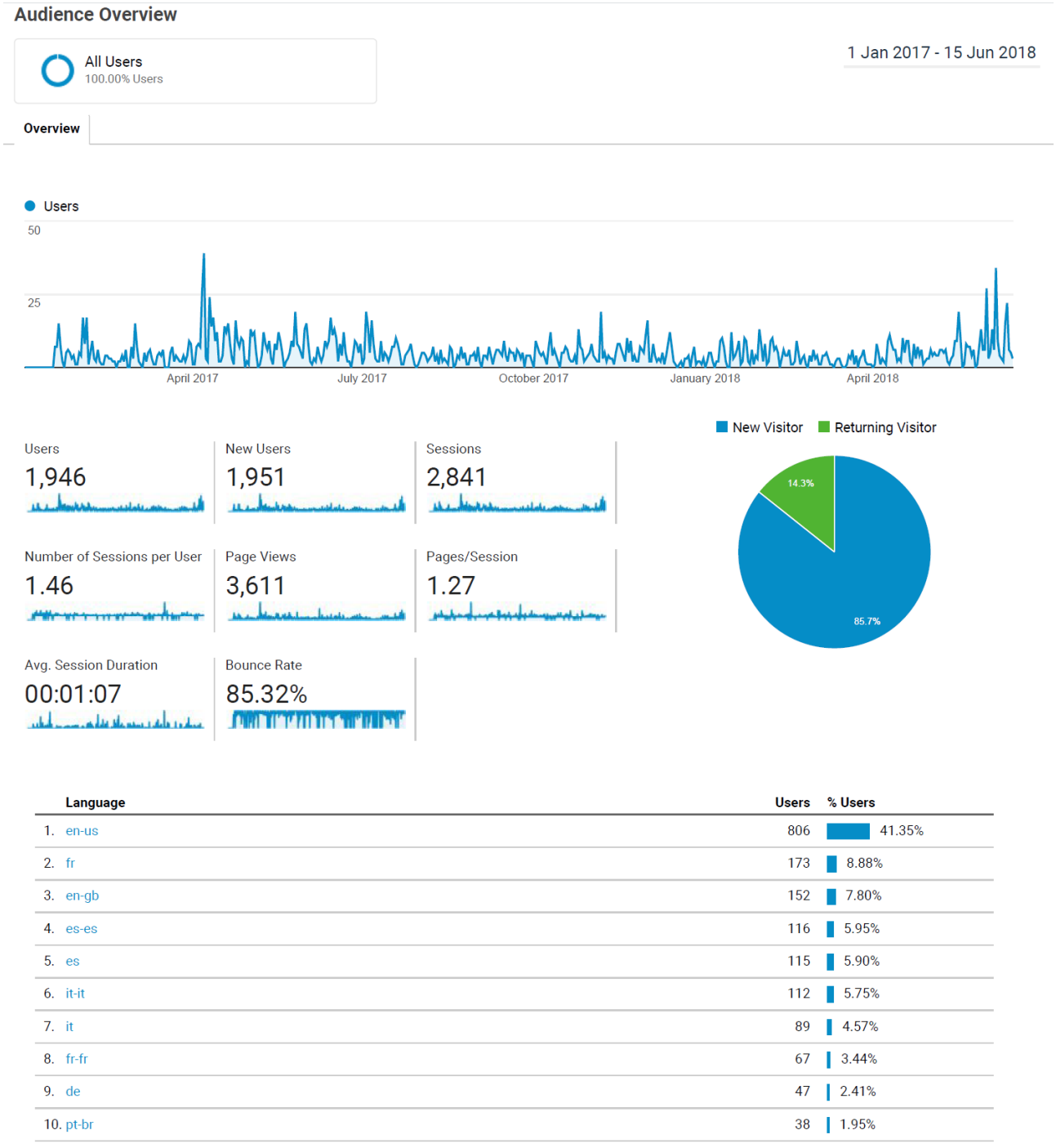


Figure 6. TIMELINE section of the ANASTACIA project's website.

Figure 7. RESULTS section of the ANASTACIA project's website.

The website is monitored by Google Analytics tools (https://analytics.google.com). The data on the audience activity (website visitors) registered since the beginning of the project (January 2017) is summarized in Figure 7.



Language	Users	% Users
1. en-us	806	41.35%
2. fr	173	8.88%
3. en-gb	152	7.80%
4. es-es	116	5.95%
5. es	115	5.90%
6. it-it	112	5.75%
7. it	89	4.57%
8. fr-fr	67	3.44%
9. de	47	2.41%
10. pt-br	38	1.95%

Figure 8. Audience Overview for the ANASTACIA project's website (Source: Google Analytics).

Information on acquisition modalities (i.e. ways to vehiculate user traffic on the project website)are summarized in Figure 9.

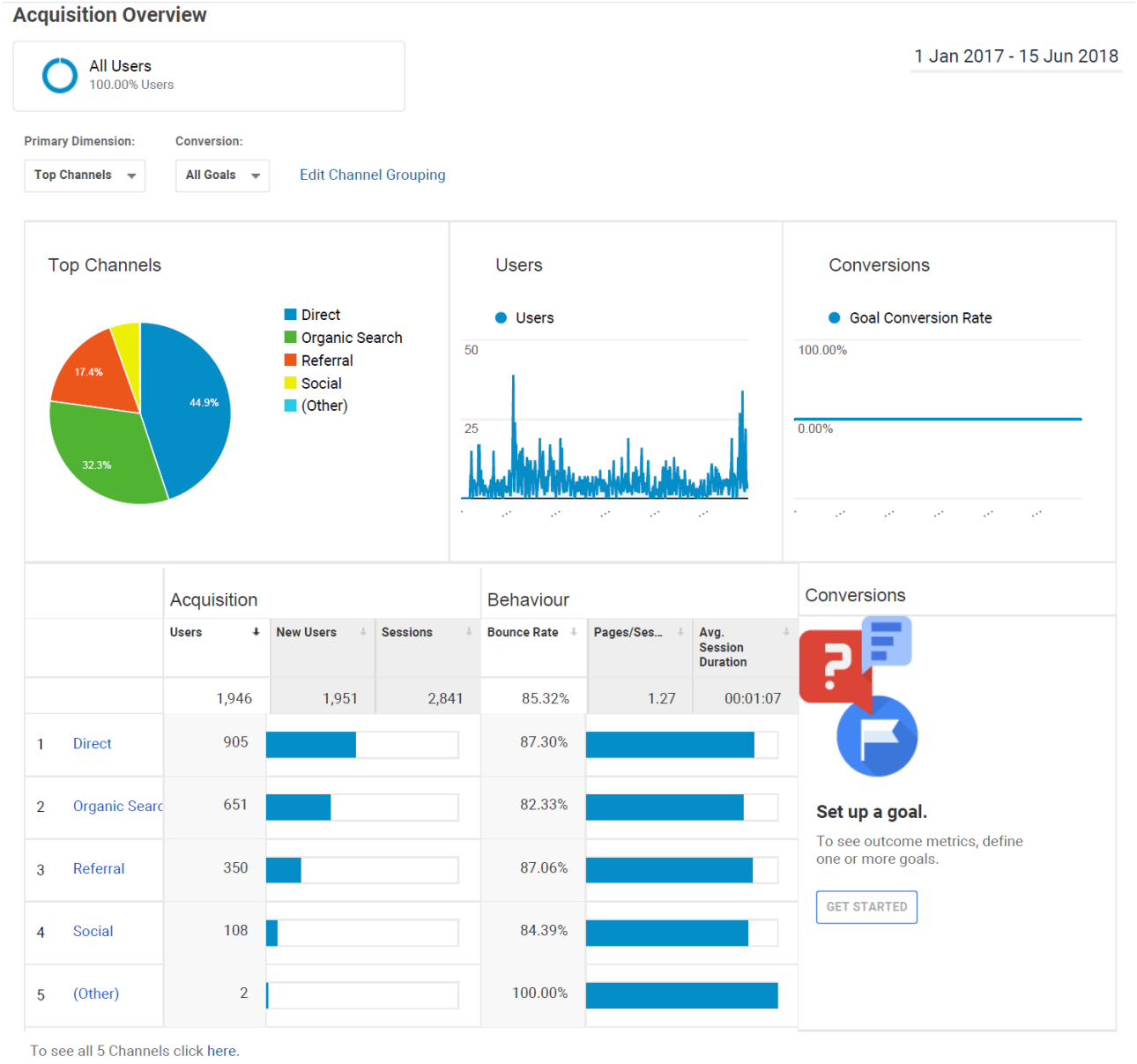


Figure 9. Acquisition Overview for the ANASTACIA project's website (Source: Google Analytics).

The geographical distribution of the website visitors is summarized in Figure 10 and Figure 11.

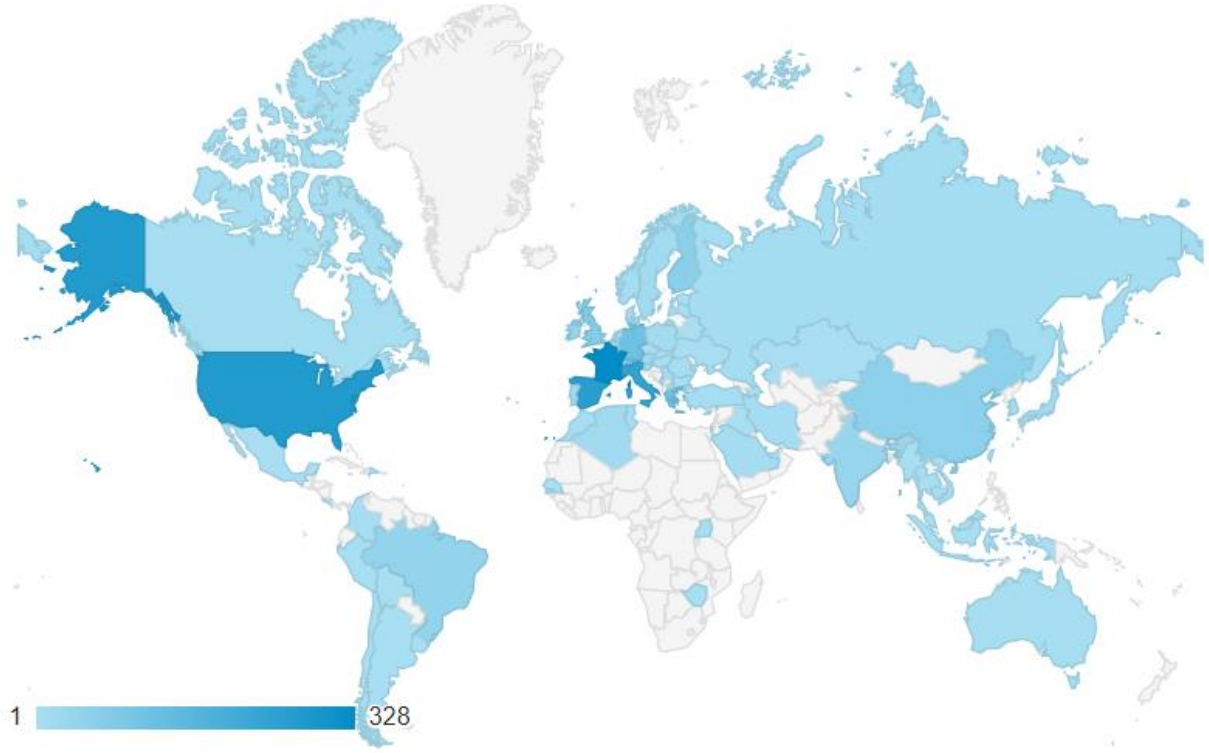


Figure 10. Visitors' geographical distribution – world map view (Source: Google Analytics).

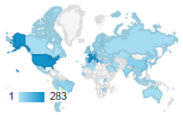
Location

All Users
100.00% Users

1 Jan 2017 - 15 Jun 2018

Map Overlay

Summary



Country	Acquisition			Behaviour			Conversions		
	Users	New Users	Sessions	Bounce Rate	Pages/Session	Avg. Session Duration	Goal Conversion Rate	Goal Completions	Goal Value
	1,946 % of Total: 100.00% (1,946)	1,952 % of Total: 100.05% (1,951)	2,841 % of Total: 100.00% (2,841)	85.32% Avg for View: 85.32% (0.00%)	1.27 Avg for View: 1.27 (0.00%)	00:01:07 Avg for View: 00:01:07 (0.00%)	0.00% Avg for View: 0.00% (0.00%)	0 % of Total: 0.00% (0)	US$0.00 % of Total: 0.00% (US$0.00)
1. France	**283** (14.24%)	280 (14.34%)	356 (12.53%)	85.96%	1.23	00:00:45	0.00%	0 (0.00%)	US$0.00 (0.00%)
2. United States	**264** (13.28%)	265 (13.58%)	321 (11.30%)	92.21%	1.14	00:00:27	0.00%	0 (0.00%)	US$0.00 (0.00%)
3. Spain	**255** (12.83%)	247 (12.65%)	395 (13.90%)	86.08%	1.22	00:00:53	0.00%	0 (0.00%)	US$0.00 (0.00%)
4. Italy	**235** (11.82%)	233 (11.94%)	421 (14.82%)	80.76%	1.42	00:01:59	0.00%	0 (0.00%)	US$0.00 (0.00%)
5. Germany	**117** (5.89%)	112 (5.74%)	146 (5.14%)	86.30%	1.35	00:01:11	0.00%	0 (0.00%)	US$0.00 (0.00%)
6. Greece	**111** (5.58%)	108 (5.53%)	196 (6.90%)	85.71%	1.23	00:01:07	0.00%	0 (0.00%)	US$0.00 (0.00%)
7. Switzerland	**86** (4.33%)	82 (4.20%)	138 (4.86%)	81.88%	1.26	00:01:29	0.00%	0 (0.00%)	US$0.00 (0.00%)
8. United Kingdom	**71** (3.57%)	68 (3.48%)	86 (3.03%)	84.88%	1.27	00:01:08	0.00%	0 (0.00%)	US$0.00 (0.00%)
9. Finland	**63** (3.17%)	63 (3.23%)	112 (3.94%)	82.14%	1.28	00:01:06	0.00%	0 (0.00%)	US$0.00 (0.00%)
10. China	**55** (2.77%)	55 (2.82%)	55 (1.94%)	96.36%	1.29	00:00:21	0.00%	0 (0.00%)	US$0.00 (0.00%)
11. Brazil	**43** (2.16%)	44 (2.25%)	58 (2.04%)	93.10%	1.09	00:00:39	0.00%	0 (0.00%)	US$0.00 (0.00%)
12. Ireland	**37** (1.86%)	36 (1.84%)	54 (1.90%)	79.63%	1.37	00:01:40	0.00%	0 (0.00%)	US$0.00 (0.00%)
13. India	**36** (1.81%)	35 (1.79%)	45 (1.58%)	88.89%	1.13	00:00:37	0.00%	0 (0.00%)	US$0.00 (0.00%)
14. Belgium	**31** (1.56%)	27 (1.38%)	35 (1.23%)	94.29%	1.06	00:00:08	0.00%	0 (0.00%)	US$0.00 (0.00%)
15. Austria	**26** (1.31%)	25 (1.28%)	37 (1.30%)	75.68%	1.46	00:00:52	0.00%	0 (0.00%)	US$0.00 (0.00%)
16. Netherlands	**20** (1.01%)	20 (1.02%)	28 (0.99%)	82.14%	1.25	00:02:13	0.00%	0 (0.00%)	US$0.00 (0.00%)
17. Slovenia	**15** (0.75%)	15 (0.77%)	34 (1.20%)	64.71%	1.76	00:01:44	0.00%	0 (0.00%)	US$0.00 (0.00%)
18. Algeria	**14** (0.70%)	13 (0.67%)	19 (0.67%)	84.21%	1.37	00:01:12	0.00%	0 (0.00%)	US$0.00 (0.00%)
19. Portugal	**14** (0.70%)	14 (0.72%)	17 (0.60%)	88.24%	1.29	00:00:19	0.00%	0 (0.00%)	US$0.00 (0.00%)
20. Sweden	**14** (0.70%)	14 (0.72%)	25 (0.88%)	76.00%	1.68	00:01:47	0.00%	0 (0.00%)	US$0.00 (0.00%)

Figure 11. Visitors' geographical distribution – table view, up to position 20 (Source: Google Analytics).

5.2 TWITTER

The Twitter account of the ANASTACIA project is available at:

https://twitter.com/ANASTACIA_H2020

Figure 12. ANASTACIA project's Twitter account - home page.

The Twitter account has been the most exploited social /online communication channel, with an intensive and constant activity focused on highlighting the main project results and dissemination events.

In the first year of activities, the project published over 100 tweets and reached more than 150 followers.

Monthly Twitter activity is illustrated in the following 4 screenshots extracted from Twitter analytics tools.

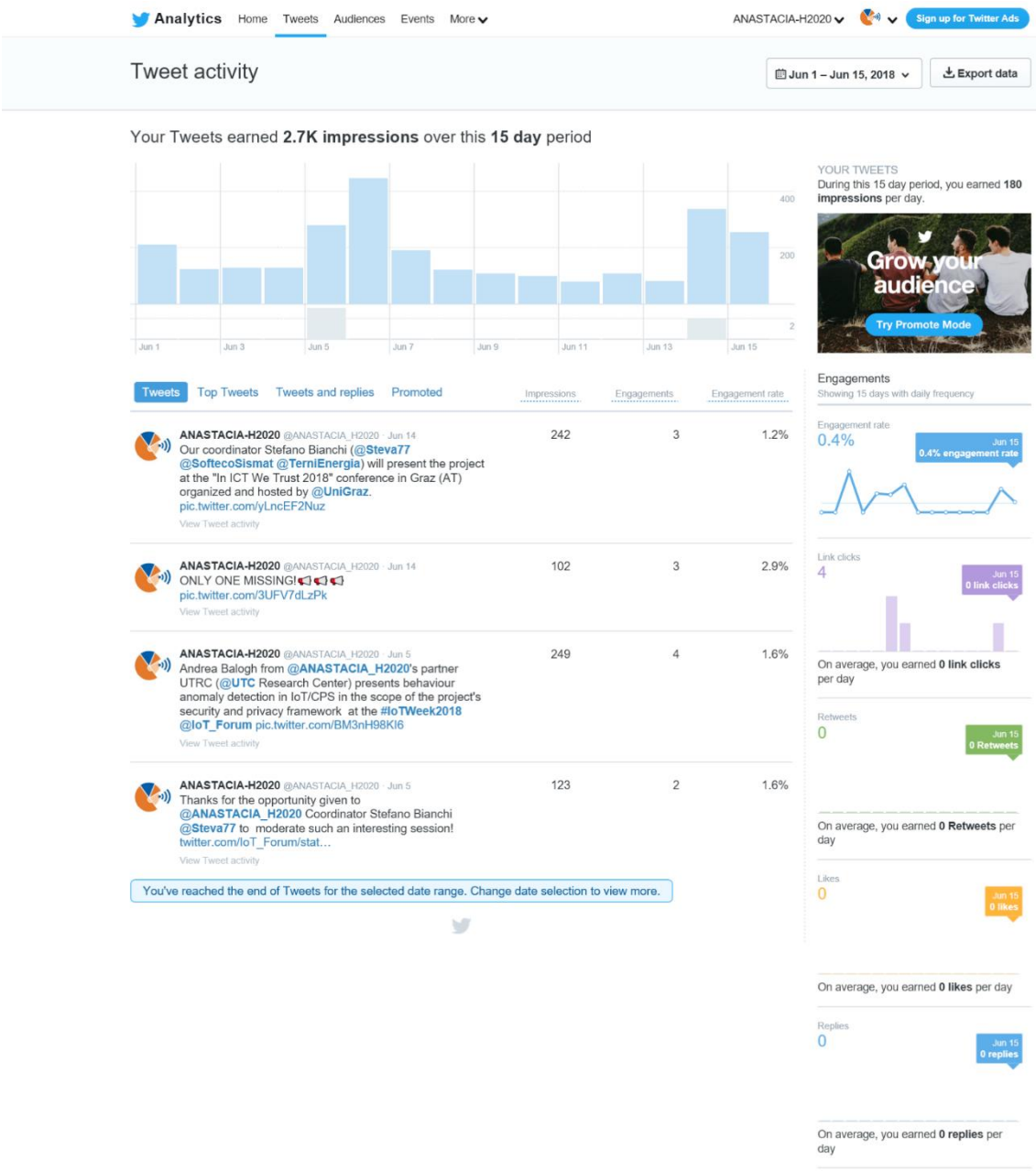


Figure 13. ANASTACIA project's Twitter account Activities over 15 days–(Source: Twitter Analytics).

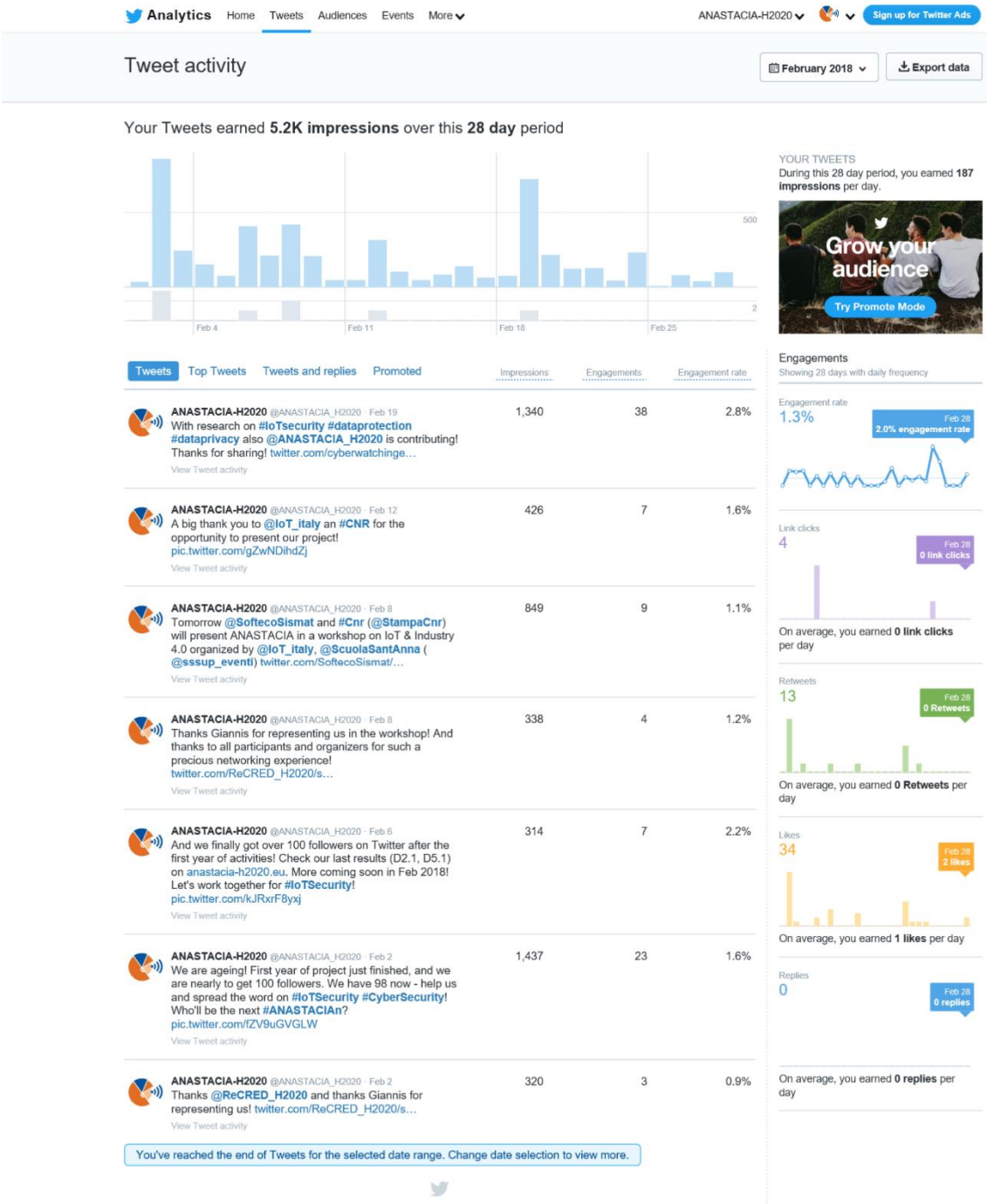


Figure 14. ANASTACIA project's Twitter account Activities over 28 days – (Source: Twitter Analytics).

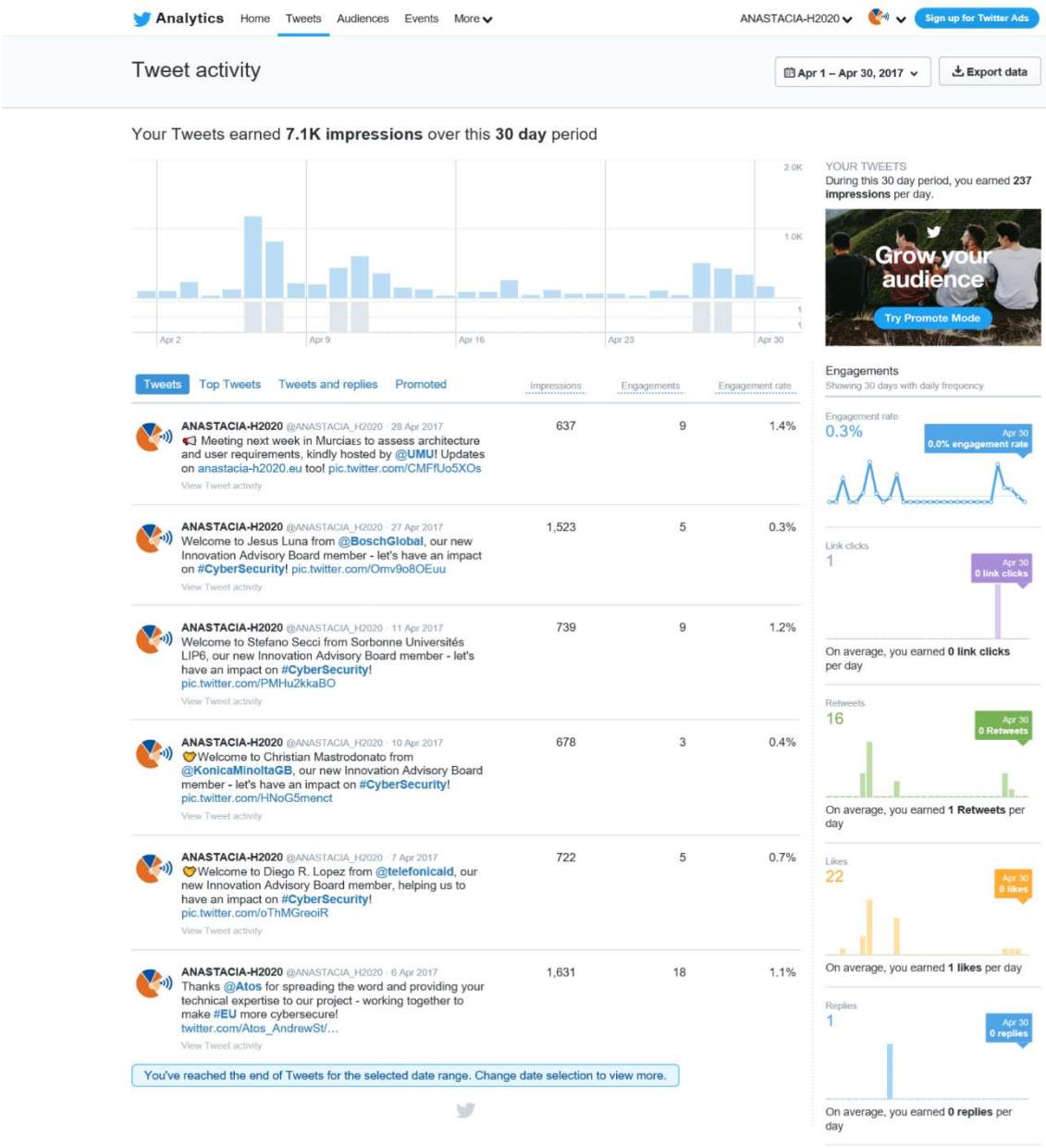


Figure 15. ANASTACIA project's Twitter account Activities over 30 days – (Source: Twitter Analytics).

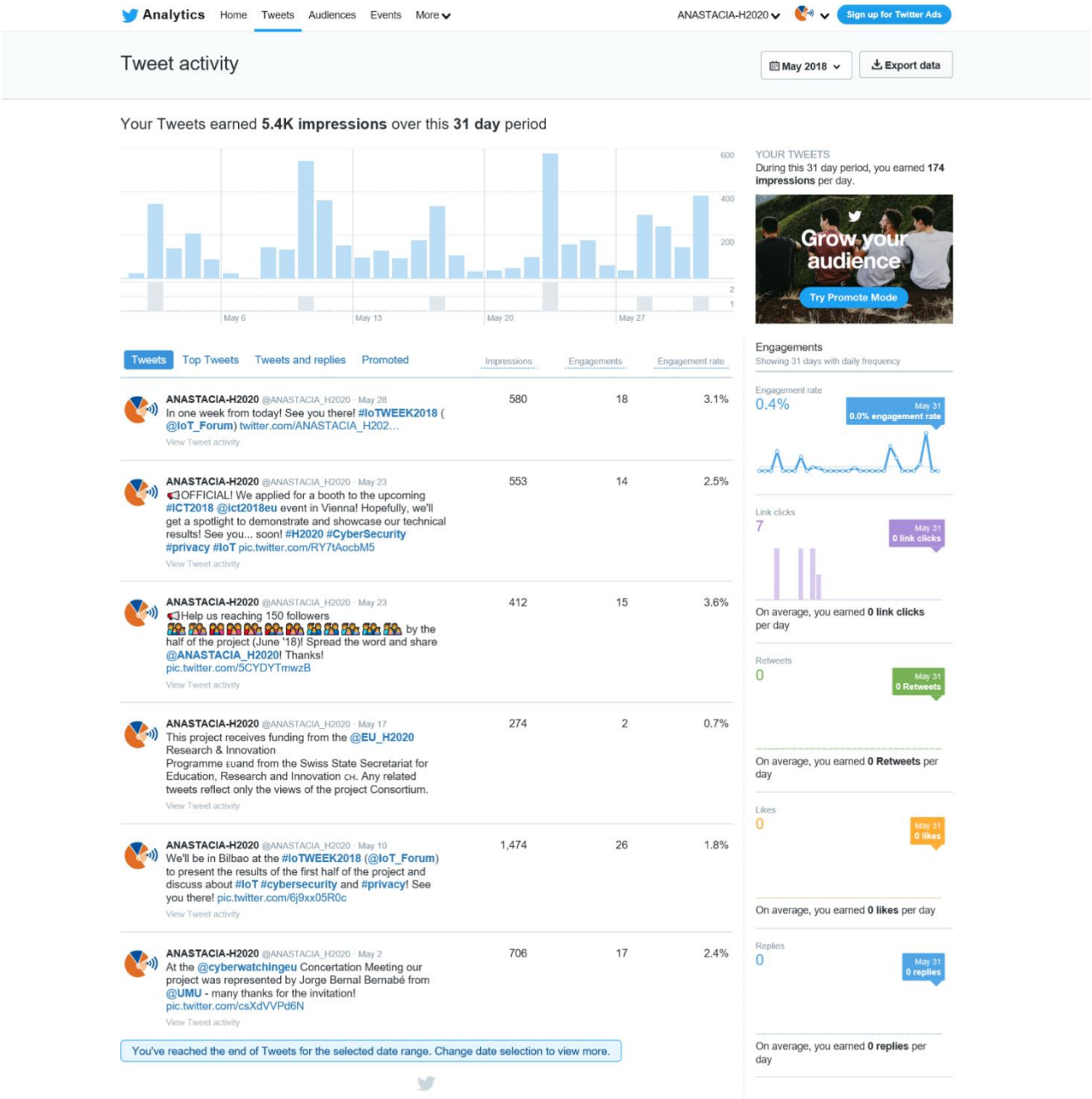


Figure 16. ANASTACIA project's Twitter account Activities over 31 days – (Source: Twitter Analytics).

5.3 YOUTUBE

The project's YouTube account/channel is available at:

http://youtube.anastacia-h2020.eu

which redirects to:

https://www.youtube.com/channel/UCfb6Ll7eKUyE7_Ztc_utEFQ

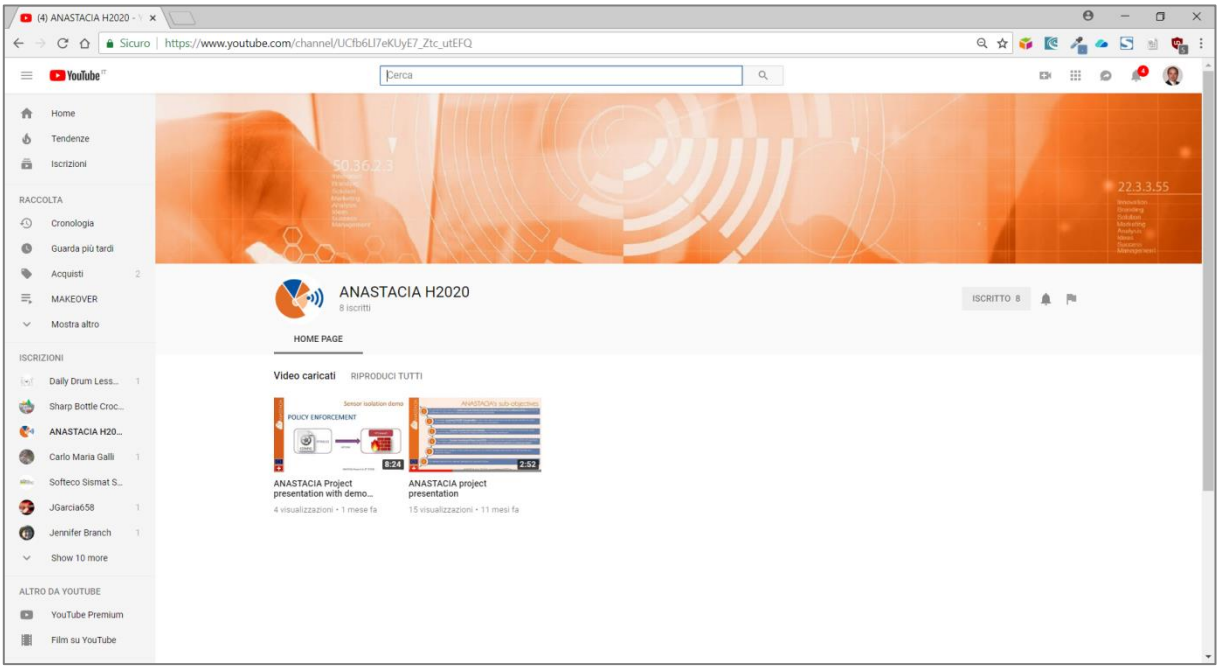


Figure 17. Project's YouTube account/channel.

So far, the YouTube channel has been exploited in a limited way, since the technical results to be demonstrated/illustrated will be available starting from the beginning of project Y2.Two short videos are available on the channel so far:

- **ANASTACIA project presentation (2:52)**
  A quick introduction to the ANASTACIA project.
  https://www.youtube.com/watch?v=cQOz9SfyAc8
- **ANASTACIA Project presentation with demo session (8:23)**
  An extended video of ANASTACIA first technical results, illustrating the ANASTACIA framework cycle in a first testbed deployment with use of a firewall and IoT-Honeynet.
  https://www.youtube.com/watch?v=wHTt4zmzZWI

5.4 LINKEDIN

The presence of the project on the professional social network LinkedIn is based on a Group (moderated by the project coordinator), available at:

http://linkedin.anastacia-h2020.eu

Actually, redirecting to:

https://www.linkedin.com/groups/8588635

The Group currently includes 35 members, yet the activity (posts and discussions) has been limited in Y1, as the Consortium preferred to concentrate efforts on more direct, interactive channels such as Twitter to raise attention on the project activities.

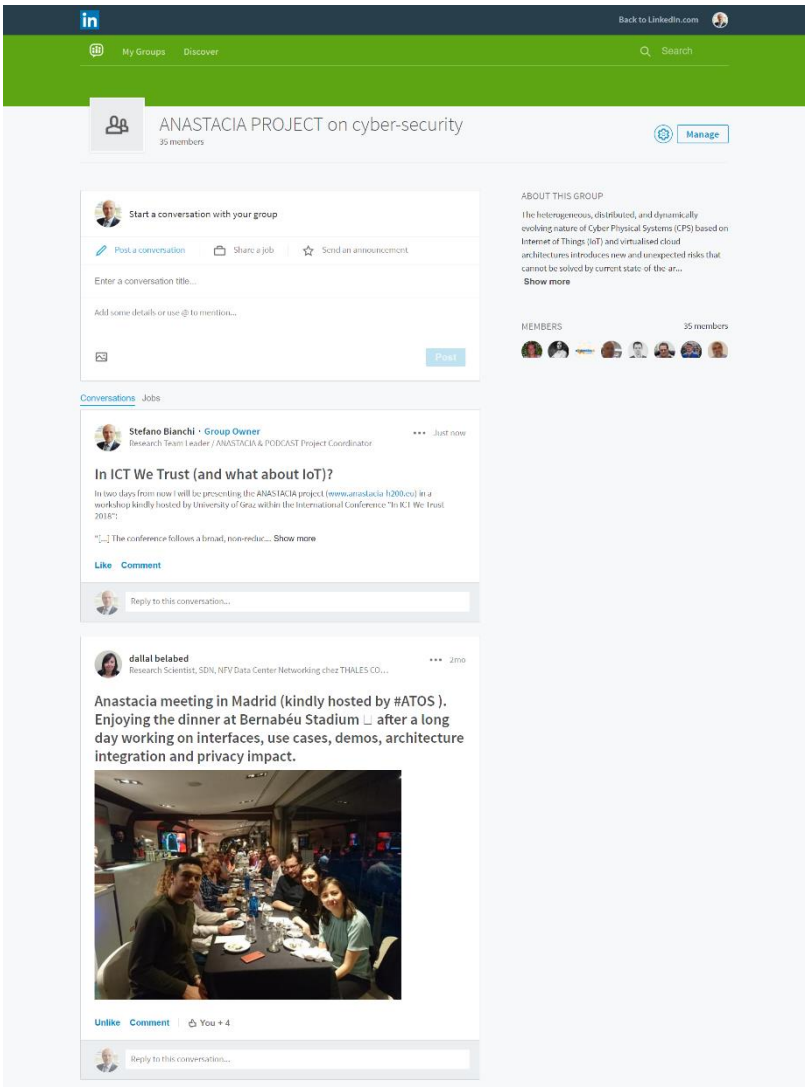


Figure 18. ANASTACIA project's Group on the professional social network LinkedIn.

6 PROMOTIONAL ACTIVITIES (IOTWEEK2018 @ BILBAO)

The main objective of the IoTWeek2018 @ Bilbao is to present ANASTACIA holistic framework and to promote ANASTACIA with IoT ecosystem (business and academia). Another objective is also to collect feedback and suggestions and to explore possibilities for cooperation with other projects.It was an opportunity to meet colleagues and discuss project's achievements. The IoT week is presented in the following figures:

Figure 19. Official Photo of the IoT Week 2018

Figure 20. The IoTWeek2018 @ Bilbao

Figure 21. The IoTWeek2018 @ Bilbao, (Promotional Material)

Figure 22. ANASTACIA BOOTH (1)

Figure 23. ANASTACIA BOOTH (2)

In the following we present the sessions and workshops of ANASTACIA.

- Figure 24 presents Artificial Intelligence and IoT sessions with Stefano Bianchi, SoftecoSismat, Project coordinator Andrea Balogh, United Technologies Research Center Mythili Menon, and Mandat International:

Figure 24. Artificial Intelligence and IoT sessions

- Figure 25 represents GIoTs workshops with Antonio Skarmeta (University of Murcia, Scientific coordinator) and Alejandro Molina Zarca (University of Murcia).

Figure 25. GIoTs Workshops

- We concluded during **IoTWeek2018 @ Bilbao** that ANASTACIA has a higher visibility among our target audiences. While the representatives of the important international organizations, IoT companies and research organizations talked with us and the European Commission Officials visited our Booth.

7 CONCLUSIONS

This document presents the first results of ANASTACIA and identifies the different metrics in order to raise awareness with presentations, workshops and conferences. It provides disseminations and standardization activities for ANASTACIA project. This aims to improve the effectiveness of communication activities during the project timespan in an iterative way.

8 REFERENCES

[1] ANASTACIAD7.1: http://www.anastacia-h2020.eu/deliverables/ANASTACIA-WP7-T7.1-AALTO-D7.1-InitialDisseminationStandardizationAndOutreachStrategyPlan-v13.pdf