



Grant Agreement No.: 871808  
Research and Innovation action  
Call Topic: ICT-20-2019-2020: 5G Long Term Evolution



# INSPIRE-5Gplus

**INtelligent Security and Pervaslve tRust for 5G and Beyond**

## **D6.4: Final Report on Dissemination, Communication and Standardisation Activities**

Version: v1.0

Deliverable type	R (Document, report)
Dissemination level	PU (Public)
Due date	31/10/2022
Submission date	08/11/2022
Lead editor	Ramón Sánchez Iborra (UMU)
Authors	Pol Alemany , Charalampos Kalalas , Raul, Muñoz , Ricard Vilalta(CTTC), Anastasios Kafchitsas, Sabina Sandia, Orestis Mavropoulos (CLS), Vincent Lefebvre (TAGES), Chafika Benzaid, Amir Javadpour, Tarik Taleb (OULU), Noelia Pérez, Antonio Skarmeta (UMU), Uwe Herzog, Pooja Mohnani (EURES), Diego Lopez, Antonio Pastor (TID), Maria Christopoulou (NCSRD), Gürkan Gür (ZHAW), Edgardo Montes de Oca (MI), Dhouha Ayed, Geoffroy Chollon (TSG), Pawani Porambage (UOULU), Mika Ylianttila (UOULU)
Reviewers	Santorinaios Dimitris (NCSRD), Pawani Porambage (UOULU)
Work package, Task	WP6, T6.1 & T6.2
Keywords	Dissemination, communication, standardisation

---

### *Abstract*

This deliverable presents the final report for the outreach activities (Dissemination, Communication, and Standardisation) in INSPIRE-5Gplus. This document is the third related report after deliverable D6.1, which covers the activities' initial planning, and D6.2, which covers all activities accomplished up to month M18, i.e., 30/04/21. Therefore, this document details the activities carried out during the second half of the project, presents the overall results attained at the end of the project, and compares them with the established KPIs.

---



### Document revision history

Version	Date	Description of change	List of contributor(s)
v0.1	28/07/2022	First draft version	UMU
v0.2	27/09/2022	First complete version	UMU, Eurescom, TID, MI, ZHAW, OPL, UOULU, NCSRD
v0.3	14/10/2022	First review	NCSRD, UOULU
v0.4	25/10/22	Second complete version	UMU, Eurescom
v0.5	28/10/22	First final draft version	All
v0.6	31/10/22	Final editing	UMU
v0.9	31/10/22	Final editing, version for GA approval	Eurescom
v1.0	08/11/22	Submission of GA approved version	Eurescom

### List of contributing partners, per section

Section number	Short name of partner organisations contributing
Section 1	UMU
Section 2	UMU, MI, TID, UOULU, CTTC, EURES, ZHAW, TSG, NCSRD, CLS, TAGES
Section 3	TID, UMU
Section 4	ALL
Section 5	UMU

### Disclaimer

This report contains material which is the copyright of certain INSPIRE-5Gplus Consortium Parties and may not be reproduced or copied without permission.

All INSPIRE-5Gplus Consortium Parties have agreed to publication of this report, the content of which is licensed under a Creative Commons Attribution-Non-Commercial-NoDerivs 3.0 Unported License<sup>1</sup>.

Neither the INSPIRE-5Gplus Consortium Parties nor the European Commission warrant that the information contained in the Deliverable is capable of use, or that use of the information is free from risk and accept no liability for loss or damage suffered by any person using the information.



CC BY-NC-ND 3.0 License – 2019-2022 INSPIRE-5Gplus Consortium Parties

### Acknowledgment

The research conducted by INSPIRE-5Gplus receives funding from the European Commission H2020 programme under Grant Agreement No 871808. The European Commission has no responsibility for the content of this document.

<sup>1</sup> [http://creativecommons.org/licenses/by-nc-nd/3.0/deed.en\\_US](http://creativecommons.org/licenses/by-nc-nd/3.0/deed.en_US)



## Executive Summary

Deliverable D6.4 presents a detailed description of the project's outreach activities done from M18 to M36. These activities are categorized in Dissemination, Communication (covered in Section 2) and Standardisation (covered in Section 3). Thus, the activities described in Section 2 aim to increase the impact and visibility of the INSPIRE-5Gplus project in different specific and generalist target groups. In turn, the actions reported in Section 3 focus on Industry Standards awareness and adoption. Finally, the document presents the list of KPIs defined in document D6.1 and the status of their accomplishment by the end of the project (Section 4).

The main activities in communication are: 7 publications in journals, such as Institute of Electrical and Electronics Engineers (IEEE), Association for Computing Machinery (ACM), and Institution of Engineering and Technology (IET); 31 participations in different congresses and conferences, including 2 keynote speech and 3 invited talks in prominent international events. 4 international workshops and 1 Industrial Forum organised under the umbrella of relevant conferences; 1 Project white paper and a collaboration in an additional one published by Alliance for the Internet of Things Innovation (AIOTI); 3 press releases devoted to the advances achieved in the project; 2 international mentions of project's developments; 2 tutorials/webinars as well as 1 doctoral course; several related Thesis (BSc, MSc, PhD); and 24 news items via the website.

Related to standardisation results, several contributions into documents have been made focusing on different Standard Development Organisations (SDO). Active participation was carried out in six groups in ETSI, three in IETF and two in IEEE. Finally, additional contributions have been made in two relevant Open-source initiatives relevant to standardization, namely OSM and 5Greplay, and a demonstration with functional software in ETSI-ZSM.



## Table of Contents

<b>Executive Summary .....</b>	<b>3</b>
<b>Table of Contents .....</b>	<b>4</b>
<b>List of Figures .....</b>	<b>5</b>
<b>List of Tables .....</b>	<b>6</b>
<b>Abbreviations.....</b>	<b>7</b>
<b>1 Introduction .....</b>	<b>9</b>
<b>2 Communication and dissemination activities.....</b>	<b>10</b>
2.1 Communication and dissemination results (M18-M36).....	10
2.1.1 Publications .....	10
2.1.2 Other dissemination activities.....	12
2.1.3 Workshop Organisation.....	16
2.1.4 White papers .....	17
2.1.5 Awards/Mentions.....	17
2.1.6 Brochure .....	18
2.1.7 Website.....	18
2.1.8 Social Media .....	22
2.1.9 Project tracker .....	27
<b>3 Standardisation activities .....</b>	<b>28</b>
3.1 Standards-related strategy summary .....	28
3.2 Standards-related results .....	28
3.2.1 ETSI .....	29
3.2.2 IETF/IRTF.....	30
3.2.3 IEEE .....	31
3.2.4 Open-source initiatives.....	32
<b>4 Communications and Dissemination KPIs .....</b>	<b>34</b>
<b>5 Conclusions .....</b>	<b>38</b>
<b>Appendix A INSPIRE-5Gplus' organised workshops .....</b>	<b>39</b>
<b>Appendix B INSPIRE-5Gplus project flyer .....</b>	<b>50</b>
<b>Appendix C ETSI ZSM PoC #6 - Demo Poster.....</b>	<b>51</b>



## List of Figures

Figure 1: INSPIRE-5Gplus Website .....	18
Figure 2: INSPIRE-5Gplus Website visitor analytics .....	19
Figure 3: INSPIRE-5Gplus Website visitor - geographical information.....	19
Figure 4: INSPIRE-5Gplus news item in the website .....	21
Figure 5: INSPIRE-5Gplus security newsletter database and subscription .....	22
Figure 6: Twitter account .....	23
Figure 7: INSPIRE-5Gplus Twitter insight .....	23
Figure 8: INSPIRE-5Gplus Twitter insight .....	24
Figure 9: INSPIRE-5Gplus Twitter engagement & tweets .....	24
Figure 10: LinkedIn profile Project INSPIRE-5G plus .....	25
Figure 11: LinkedIn Analytics.....	25
Figure 12: Post engagements.....	26
Figure 13: YouTube page of INSPIRE-5Gplus.....	27
Figure 14: Project tracker.....	27
Figure 15: ETSI ZSM PoC # 6 Security SLA assurance in 5G network slices .....	32
Figure 16: News with the use of OSM in INSPIRE-5Gplus PoC.....	33



**List of Tables**

Table 1: Other dissemination activities..... 16

Table 2: INSPIRE-5Gplus’ organised events ..... 17

Table 3: Standardization activities in M18-M36 period..... 29

Table 4: KPIs and achieved results for communication activities ..... 35

Table 5: KPIs and achieved results for dissemination activities..... 37



## Abbreviations

<b>3GPP</b>	3rd Generation Partnership Project
<b>5G PPP</b>	The 5G Infrastructure Public Private Partnership
<b>ACM</b>	Association for Computing Machinery
<b>AIOTI</b>	Alliance for the Internet of Things Innovation
<b>CDX</b>	Cyber Defence Exercises
<b>CERT/CSIRT</b>	Computer Emergency Response Team / Computer Security Incident Response Team
<b>COSE</b>	CBOR Object Signing and Encryption
<b>DGKA</b>	Dynamic Group Key Agreement
<b>DL</b>	Deep Learning
<b>DLT</b>	Distributed Ledger Technologies
<b>EAP</b>	Extensible Authentication Protocol
<b>EDHOC</b>	Ephemeral Diffie-Hellman Over COSE
<b>EMU</b>	EAP Method Update
<b>ENI</b>	Experiential Networked Intelligence
<b>ETI</b>	Encrypted Traffic Integration
<b>ETSI</b>	European Telecommunications Standards Institute
<b>GDPR</b>	General Data Protection Regulation
<b>GSMA</b>	Global System for Mobile Communications Alliance
<b>I2NSF</b>	Interface to Network Security Function
<b>ICT</b>	Information Communications Technology
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IET</b>	Institution of Engineering and Technology
<b>IETF</b>	Internet Engineering Task Force
<b>IRTF</b>	Internet Research Task Force
<b>ISO</b>	International Organization for Standardisation
<b>ITU</b>	International Telecommunication Union
<b>KPI</b>	Key Performance Indicator
<b>LPWAN</b>	Low Power Wide Area Network
<b>MEC</b>	Multi-access Edge Computing
<b>MIMO</b>	Multiple-Input and Multiple-Output
<b>MTC</b>	Machine-Type Communication
<b>NFV</b>	Network Function Virtualisation
<b>NFVI</b>	NFV Infrastructure
<b>NIS</b>	Network and Information Systems



<b>P2MP</b>	Point to Multi-Point
<b>QKD</b>	Quantum Key Distribution
<b>RFC</b>	Request For Comments
<b>RTO</b>	Research Technology Organization
<b>SAI</b>	Securing Artificial Intelligence
<b>SDN</b>	Software-defined networking
<b>SDO</b>	Standard Development Organisations
<b>SFC</b>	Service Function Chaining
<b>SLA</b>	Service Level Agreement
<b>SSLA</b>	Security Service Level Agreement
<b>SME</b>	Small Medium Enterprise
<b>SRIA</b>	Strategic Research and Innovation Agenda
<b>TA</b>	Target Audiences
<b>TEE</b>	Trust Execution Environment
<b>UAV</b>	Unmanned Aerial Vehicle
<b>V2X</b>	Vehicle-to-everything
<b>VNF</b>	Virtualised Network Function
<b>VSF</b>	Virtual Security Function
<b>ZSM</b>	Zero-touch network and Service Management





## 1 Introduction

Deliverable 6.4 – “Final Report on Dissemination, Communication and Standardisation Activities” details the conducted activities during the second half of the project to maximize the impact and visibility of the results of INSPIRE-5Gplus:

- **Dissemination.** This activity focuses on two main targets, namely, Industrial and Scientific ecosystems. The main objective is to increase the awareness among specialized communities, stakeholders, or regions aiming at boosting an interchange of knowledge that can enrich the developments and advances of the project. Regarding Academic dissemination, dedicated efforts have been made in publications in top-ranked journals and international conferences over multiple disciplines around networks, 5G and security, as well as several workshop-organisation activities aiming to bring together experts and specialist in the topics treated by the project. Besides, technical webinars have been provided and certain project’s advances have been included in undergraduate education programmes by the Academic partners in the consortium. Industrial dissemination has not been left behind, and several invited talks, keynotes and presentations have been made in the telecommunications and security areas in different Industrial forums and events.
- **Communication.** This specific action focuses on all the activities conducted to increase the general visibility and impact of the project. Specific material includes flyers, white papers, newsletter, etc. The participation in events with big audiences, e.g., Mobile World Congress, also fall in this category. Several tools have been activated and improved over the M18-M36 period. This is the case of the web portal and various social media channels (Twitter, YouTube, and LinkedIn) in which the activity has been notably fuelled to increase the number of followers and reached audience.
- **Standardisation.** These activities have a specific focus on the most relevant bodies in the Telecom area (ETSI, ITU), communication (IEEE) and Internet protocols (IETF). Also, a special collaboration with European Public Private Partnerships (PPP) has been pursued. This is the case for 5GPPP and ECSO.



## 2 Communication and dissemination activities

### 2.1 Communication and dissemination results (M18-M36)

#### 2.1.1 Publications

Publishing project outcomes in prestigious journals, magazines or conferences is a fundamental vehicle to disseminate the technical advances achieved in the project. In the following, we present the works published or already accepted for their publication during the second half of the project.

##### **M18-M36:**

- W. Niewolski et al., "Security Context Migration in MEC: Challenges and Use Cases," in Electronics (MDPI), 2022, doi: 10.3390/electronics00010005.

Contribution related to INSPIRE-5Gplus: This article presents the state of research on the migration of the Security Context between service instances in Edge/MEC servers, specify steps of the migration procedure, and identify new security challenges inspired by use cases of 5G vertical industries. For this purpose, the analysis of the Security Context structure and basic concept of the Security Service Level Agreement was done and presented. The results presented in this paper are linked to the work conducted in WP4.

- Y. Dang, C. Benzaïd, B. Yang, T. Taleb and Y. Shen, "Deep Ensemble Learning based GPS Spoofing Detection for Cellular-Connected UAVs," in IEEE Internet of Things Journal, 2022, doi: 10.1109/JIOT.2022.3195320.

Contribution related to INSPIRE-5Gplus: This paper proposes a novel deep ensemble learning-based, mobile network-assisted Unmanned Aerial Vehicle (UAV) monitoring and tracking system for cellular-connected UAV spoofing detection. The proposed method uses path losses between base stations and UAVs communication to indicate the UAV trajectory deviation caused by GPS spoofing. The paper is related to work conducted in WP3 on Anti-GPS spoofing enabler.

- P. Alemany, *et al.*, "Management and enforcement of secured E2E network slices across transport domains," Optical Fiber Technology, 73, 2022, doi:10.1016/j.yofte.2022.103001. Open-access link.

Contribution related to INSPIRE-5Gplus: This article introduces the relationship between Security Service Level Agreement (SSLAs) and E2E Network Slices. It introduces the architecture designed to deploy, monitor and enforce the right security requirements defined in an SSLA and associated to an E2E Network Slice. Using an attack use case, the presented infrastructure and its components are evaluated. The work of this journal is closely related to the experimental Demo1 implemented within the WP5 context of INSPIRE5G-Plus.

- C. Benzaid, T. Taleb and J. Song, "AI-based Autonomic & Scalable Security Management Architecture for Secure Network Slicing in B5G," in IEEE Network, 2022, doi: 10.1109/MNET.104.2100495. Open-access link.

Contribution related to INSPIRE-5Gplus: The paper introduces a novel autonomic and cognitive security management framework that extends the domain-level vision adopted in INSPIRE-5Gplus HLA to empower fine-grained zero-touch security management through different levels (i.e., network functions, sub-slice, and slice) and different administrative and technological domains. It is related to work conducted in WP2 (INSPIRE-5Gplus HLA) and WP3 (DDoS Mitigator enabler).



- R. Sanchez-Iborra and A. Skarmeta, "Who is wearing me? TinyDL-based user recognition in constrained personal devices," IET Computers & Digital Techniques, vol. 16, no. 1, pp. 1–9, 2022, doi: 10.1049/cdt2.12035.

Contribution related to INSPIRE-5Gplus: This paper explores the use of embedded Machine Learning models in IoT devices with the aim of increasing their security. The use of Deep Learning techniques for anomaly detection and other security tasks is widely used in big platform such as the one developed in INSPIRE-5Gplus. However, the adaptation of these mechanisms to be run in constrained units is not an easy task, which is investigated in this work. This work is linked to the work conducted in WP3.

- P. Alemany et al., "A KPI-Enabled NFV MANO Architecture for Network Slicing with QoS," in IEEE Communications Magazine, vol. 59, no. 7, pp. 44-50, 2021, doi: 10.1109/MCOM.001.2001077. [Open-access link.](#)

Contribution related to INSPIRE-5Gplus: This article focuses on the association of SLAs and Network Slices. The article shows the complete process to design all the descriptors elements (i.e., SLA, Network Slices, Network Services and VNFs) and their deployment and monitoring actions to finally have the service correctly deployed with the performance being constantly checked. The work done in this article served as the starting point for the work CTTC did, first in their proposed experimental test cases presented in D5.1 and later, to help on the design, development and implementation in the WP5 tasks for the final Demo1.

- T. MawananeHewa, I. Kovacevic, P. Porambage, N. Weerasinghe, M. Liyanage, E. Harjula, M. Ylianttila, "Blockchain-based Network Slice Broker to Facilitate Factory-as-a-Service," IEEE Transactions on Industrial Informatics, 2022. [Open-access link.](#)

Contribution related to INSPIRE-5Gplus: This paper introduces a secure blockchain-based network slice broker. The proposed secure network slice broker provides secure, cognitive, and distributed network services for resource allocation and SSLA formation with coordination of slice managers and SSLA managers. This article presents the detailed design of SFSBroker security enabler which is an outcome of WP3 and used in Demo 1 in WP5.

- N. Nguyen Huu, Z. Salazar, F. Zaidi, W. Mallouli, A. Cavalli and E. Montes De Oca, "A Network Traffic Mutation based Ontology, and its application to 5G networks," IEEE Access, 2022 (under review).

Contribution related to INSPIRE-5Gplus: This article presents a substantial extension of the ICSoft 2022 conference paper on mutation models and techniques used by the 5greplay tool for INSPIRE-5Gplus and for testing the resiliency of 5G components to attacks and abnormal traffic.



### 2.1.2 Other dissemination activities

Activity event material type	Event name / material name	Papers / presentation title	Start Date	End Date	Venue	Responsible partner
Conference contribution	IEEE Global Communications Conference 2022 (Globecom '22)	Misbehavior Detection in Vehicular Networks: An Ensemble Learning Approach	2022-12-04	2022-12-08	Rio de Janeiro, Brazil	CTTC
Conference contribution	IEEE Global Communications Conference 2022 (Globecom '22)	A Cost-Effective MTD Approach for DDoS Attacks in Software-Defined Networks	2022-12-04	2022-12-08	Rio de Janeiro, Brazil	UOULU
Conference contribution	18th International Conference on Network and Service Management - CSNM 2022	Graph Based Liability Analysis for the Microservice Architecture	2022-10-31	2022-11-04	Thessaloniki, Greece	ZHAW
Industrial event	Orange «Salon de la Recherche et de l'Innovation» 2022	Deep Attestation, LASM, MANIFEST, Orchestration under Constraints, and SYSTEMIC Demos	2022-10-18	2022-10-20	Paris, France	ORANGE
Conference contribution	2022 IEEE 5th Future Networks World Forum (FNWF'22) - S6. Symposium on Security for 5G and Future Networks	ETSI ZSM Driven Security Management in Future Networks	2022-10-12	2022-10-14	Montreal, QC, Canada	EURES
Conference contribution	17th International Conference on Availability, Reliability and Security (ARES 2022)	The Owner, the Provider and the Subcontractors: How to Handle Accountability and Liability Management for 5G End to End Service	2022-08-23	2022-08-26	Vienna, Austria	OPL
Conference contribution	9th International Conference on Future Internet of Things and Cloud (FiCloud 2022)	Security Constraints for Placement of Latency Sensitive 5G MEC Applications	2022-08-21	2022-08-23	Rome	OPL
Conference contribution	ICSOF 2022 : 17th International Conference on Software Technologies	A Formal Approach for Complex Attacks Generation based on Mutation of 5G Network Traffic	2022-07-11	2022-07-13	Lisbon, Portugal	MI
Conference contribution	2nd Workshop on Accountability, Liability and Trust for 5G and Beyond 2022	Level of Trust and Privacy Management in 6G Intent-based Networks for Vertical	2022-07-08	2022-07-08	Paris	TID



	(WALT5G+ 2022)	Scenarios				
Conference contribution	2nd Workshop on Accountability, Liability and Trust for 5G and Beyond 2022 (WALT5G+ 2022)	The Impact of Manufacturer Usage Description (MUD) on IoT Security	2022-07-08	2022-07-08	Paris, France	ZHAW
Conference contribution	2nd Workshop on Accountability, Liability and Trust for 5G and Beyond 2022 (WALT5G+ 2022)	eSIM adoption : Essential challenges on Responsibilities Repartition	2022-07-08	2022-07-08	Paris, France	Orange
Conference contribution	2nd Workshop on Accountability, Liability and Trust for 5G and Beyond 2022	Modeling the accountability and liability aspects of a 5G multi-domain on-demand security services: an unexpected journey	2022-07-08	2022-07-08	Paris, France	Orange
Conference contribution	4th International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-Defined and Virtualized Infrastructures (SecSoft 2022)	Model-Driven Network Monitoring Using NetFlow Applied to Threat Detection	2022-07-01	2022-07-01	Milan, Italy	TID
Conference contribution	IEEE International Conference on Network Softwarization 2022 (IEEE NetSoft '22)	Multi-domain Denial-of-Service Attacks in Internet-of-Vehicles: Vulnerability Insights and Detection Performance	2022-06-27	2022-07-01	Milan, Italy	CTTC
Conference contribution	IEEE International Conference on Network Softwarization 2022 (IEEE NetSoft '22)	TRAILS: Extending TOSCA NFV profiles for liability management in the Cloud-to-IoT continuum	2022-06-27	2022-07-01	Milan, Italy	Orange
Brochures	Beyond 5G: enabling technologies and challenges	Use Case proposal: "E2E Service Trust and Liability Management for Verticals"	2022-06-22	2022-06-22		OPL, Orange
Tutorial	The 2022 IEEE 95th Vehicular Technology Conference: VTC2022-	AI/ML-based Solutions for Automating Security in Future 6G	2022-06-19	2022-06-19	Helsinki, Finland	UOULU, ZHAW, NCSRD



	Spring	Networks				
Doctoral Course	Advanced Network Security in 5G and Beyond	Advanced Network Security in 5G and Beyond - Doctoral course	2022-06-01	2022-06-03	University of Oulu, Finland	UOULU, ZHAW, NCSR
Conference contribution	International Wireless Communications and Mobile Computing Conference (IWCMC 2022)	Transfer Learning based GPS Spoofing Detection for Cellular-Connected UAVs	2022-05-30	2022-06-03	Dubrovnik, Croatia	UOULU
Conference contribution	IEEE International Conference on Communications 2022 (IEEE ICC '22)	Reinforcement Learning Based Misbehaviour Detection in Vehicular Networks	2022-05-16	2022-05-20	Seoul, South Korea (Hybrid)	CTTC
Keynote	Layer123 Reunion: Intelligent Network Automation Congress	Trustworthy networks in the days of zero-trust	2022-04-27	2022-04-27	Madrid, Spain	TID
White paper	White Paper on Evolution of 5G Cyber Threats and Security Solutions	Evolution of 5G Cyber Threats and Security Solutions	2022-04-13	2022-12-31		INSPIRE-5Gplus consortium
Thesis	BA Thesis: Dynamic Trust Monitoring of Containerized Services in Network Functions Virtualization Infrastructure	Dynamic Trust Monitoring of Containerized Services in Network Functions Virtualization Infrastructure	2022-02-14	2022-06-10	Zurich, Switzerland	ZHAW
Conference contribution	2021 International Conference on Networking and Network Applications (NaNA 2021)	Deep Learning for GPS Spoofing Detection in Cellular-Enabled UAV Systems	2021-10-29	2021-11-30	Lijiang City, China	AALTO
Conference contribution	2021 IEEE 4th 5G World Forum (5GWF)	Enhancing trust and liability assisted mechanisms for ZSM 5G architectures	2021-10-13	2021-10-13	Montreal, QC, Canada	University of Murcia
Industrial event	INSPIRE5g-plus presentation to HEXA-X project	A ZSM based architecture solution for B5G security services	2021-10-05	2021-10-05		TID
Invited talk	3rd International Conference on Machine Learning and Intelligent Systems (MLIS 2021)	TinyML: A ground-breaking shift for the Internet of Things	2021-11-08	2021-11-11	Virtual event	UMU
Conference	ARES 2021: The 16th International	5Greplay: a 5G	2021-08-	2021-08-	Virtual event	MI



contribution	Conference on Availability, Reliability and Security	Network Traffic Fuzzer	-0-17	19		
Keynote	5th International Symposium on Mobile Internet Security (MobiSec 2021)	AI technologies and advanced security for connected devices in next generation networks	2021-10-07	2021-10-09	Jeju Island, Korea	UMU
Conference contribution - Proceeding	2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)	How DoS Attacks Can Be Mounted on Network Slice Broker and Can They Be Mitigated Using Blockchain?	2021-09-13	2021-09-16	Virtual event	UOULU
Industrial event	Innovationstreiber 5G at Technopark Winterthur	5G Security: Risks, Mitigation and Challenges	2021-11-9	2021-11-9	Virtual event	ZHAW
Conference contribution -	IEEE International Mediterranean Conference on Communications and Networking 2021	Reinforcement Learning-based Misbehaviour Detection in V2X Scenarios	2021-09-07	2021-09-10	Athens, Greece / Hybrid On-line Conference	CTTC
Invited talk	IEEE 7th World Forum on Internet of Things	AI technologies and advanced Connected devices in next generation networks	2021-07-23	2021-07-23	New Orleans, Louisiana, USA / Hybrid On-line Conference	University of Murcia (UMU)
Webinar	Webinar on Cyber-Physical systems security and resilience	Dynamic Security Deployment Based on SDN/NFV Scenarios Like Smart Building and Network Infrastructure	2021-07-14	2021-07-14	On-line event	University of Murcia
Conference contribution	IEEE 7th International Conference on Network Softwarization (NetSoft)	How DoS attacks can be mounted on Network Slice Broker and can they be mitigated using blockchain?	2021-06-28	2021-07-02	Virtual event	UOULU
Conference contribution	EuCNC and 6G Summit 2021	AI-Enabled Slice Protection Exploiting Moving Target Defense in 6G Networks	2021-06-08	2021-06-11	Porto, Portugal	NCSRD ZHAW MI
Conference contribution	EuCNC & 6G Summit 2021	6G Security Challenges and Potential Solutions	2021-06-08	2021-06-11	Porto, Portugal	UOULU ZHAW



Conference contribution	EuCNC & 6G Summit 2021	AI and 6G Security: Opportunities and Challenges	2021-06-08	2021-06-11	Porto, Portugal	UOULU
Conference contribution	EuCNC & 6G Summit 2021	SFSBroker: Secure and Federated Network Slice Broker for 5G and Beyond	2021-06-08	2021-06-11	Porto, Portugal	UOULU
Invited talk	EUCNC21 SN Workshop Telco Cloud Native: Time to Operationalise	Advancing security of softwarized networks	2021-06-01	2021-06-01	Porto, Portugal	CTTC
Conference contribution	Optical Networking and Communication Conference (OFC'21)	End-to-End Network Slice Stitching using Blockchain-based Peer-to-Peer Network Slice Managers and Transport SDN Controllers	2021-06-06	2021-06-10	Moscone Center, San Francisco, California, USA	CTTC

Table 1: Other dissemination activities

### 2.1.3 Workshop Organisation

One of the main dissemination and communication activity conducted by the consortium has been the active participation in workshops organisation. During the period covered by this report, 4 international workshops have been organised with the aim of serving as constructive discussion spaces with other projects, scientists, and different interested stakeholders and audience. In below Table 2 we list the organised events and provide additional information about them.

Event Title	Co-located with	Start date	End date	Venue
Workshop on Automated and Intelligent Security	EuCNC and 6G Summit 2021	2021-06-08	2021-06-08	Virtual event
4th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft)	IEEE International Conference on Network Softwarization (NetSoft'22)	2021-07-01	2021-07-01	Milan, Italy
2nd Workshop on Accountability, Liability and Trust for 5G and Beyond, WALT5G+ 2022	1st International Conference on 6G Networking (6GNet 2022)	2022-07-06	2022-07-08	Paris, France
Symposium on Security for 5G and Future Networks	IEEE Future Networks World Forum 2022	2022-10-12	2022-10-12	Montreal, Canada





Industrial Forum From 5G to 6G Smart Security Solutions	IEEE Future Networks World Forum 2022	2022-10-12	2022-10-12	Montreal, Canada
---	---------------------------------------	------------	------------	------------------

Table 2: INSPIRE-5Gplus' organised events

The programs of these events as well as pictures of the organised sessions are included in Appendix A.

### **FUTURE EVENTS**

Besides the events reported above, other activities will be organised after the end of the project to continue increasing the visibility of INSPIRE-5Gplus:

- Joint INSPIRE-5G and AI@EDGE projects workshop – “Platforms and Mathematical Optimization for Secure and Resilient Future Networks<sup>2</sup>, co-located with IEEE International Conference on Cloud Networking<sup>3</sup>, Paris, November 2022.
- INSPIRE-5Gplus' WP4 demonstration at the EuropeanCyberWeek<sup>4</sup>, Rennes, November, 2022.

#### **2.1.4 White papers**

After the first project's white paper, released during the first half of the project and in which the characteristics of the INSPIRE-5Gplus architecture were presented, a second white paper was released during the second half of the project. In this case, the INSPIRE-5Gplus security enabling technologies are presented, alongside the main challenges concerning each of these technologies and how they can be applied to improve cybersecurity in 5G networks. The reference of this white paper is as follows:

- R. Asensio, C. Benzaid, P. Alemany, D. Ayed, M. Christopoulou, C. Dangerville, G. Gür, V. Hoa La, V. Lefebvre, E. Montes de Oca, R. Muñoz, H. Nguyen, M. Nguyen, J. Ortiz, A. Pastor, P. Porambage, G. Santinelli, W. Soussi, T. Taleb, R. Vilalta, A. Zarca. White Paper: “Evolution of 5G Cyber Threats and Security Solutions,” INSPIRE-5Gplus, 2022. DOI:10.5281/zenodo.6457557.

Besides, INSPIRE-5Gplus has also contributed to different 5G-6G white papers/brochures in order to provide its vision regarding the upcoming security landscape in these ecosystems at the time of presenting its developments and use cases:

- AIOTI WG Standardisation, "IoT and Edge Computing impact on Beyond 5G: enabling technologies and challenges", Release 1.0, 2021. <https://aioti.eu/wp-content/uploads/2021/10/AIOTI-Beyond-5G-R1-Report-Published.pdf>

#### **2.1.5 Awards/Mentions**

The European Commission through its European Commission's Innovation Radar team has identified three innovative ideas developed and presented under the scope of the INSPIRE5G-plus project:

- The “Blockchain-based Management of Certified Network Slices” idea aims to study the possibility to evolve the Management of Network Slices by implementing a system in which only certified Network Slice elements would be accepted in a distributed-based system based on Blockchain. More information about the innovation may be found in:

<sup>2</sup> <https://aiedge-inspire5g.roc.cnam.fr/>

<sup>3</sup> <https://cloudnet2022.ieee-cloudnet.org/>

<sup>4</sup> <https://www.european-cyber-week.eu/>



<https://www.innoradar.eu/innovation/41970>

- “Vehicle authentication enhanced with misbehavior detection” innovation aims to: i) enhance the authentication efficiency in highly dense vehicular scenarios with the use of probabilistic data signatures which keep the end-to-end latency and false positive rate at controllable levels; ii) identify (detect and localize) vehicular misbehavior in real-time through the exploitation of spatiotemporal data (e.g., vehicle’s position, speed, acceleration, heading angle) cross-correlations and extraction of the underlying vehicle dynamics in a mobility model-agnostic manner. More information about this innovation may be found in: <https://www.innoradar.eu/innovation/41962>
- “Moving Target Defense and Anomaly Detection” innovation aims to integrate MTD concept into 5G and Beyond networks for proactive and smart security schemes. More information about the innovation may be found in: <https://www.innoradar.eu/innovation/41967>

### 2.1.6 Brochure

The project Flyer is available for download on the project website (<https://www.inspire-5gplus.eu/project-flyer/>). This communication item is used by partners to introduce the project briefly to other interested parties (online and off-line). They are used on several social media posts to raise awareness about the project. The INSPIRE-5Gplus flyer has been produced, to give an overview of the most important achievements of the project. It includes a diagram of INSPIRE-5Gplus high-level architecture, the defined test-case, as well as other general information about the project. The flyer can be found in Appendix B.

### 2.1.7 Website

The INSPIRE-5Gplus website (<https://www.inspire-5gplus.eu>) was launched at the start of the project and the principal mean for disseminating and communicating the activities of the project. During the execution of the project, it has been continuously updated with new content and sections, considering various SEO best practices and requirements for enhancing the organic positioning on search engines, such as the monitoring and analysis of keywords, increasing the number of internal and external links, and fulfilling accessibility requirements to offer valuable content to visitors regardless of the type of device they use to visit the website.



Figure 1: INSPIRE-5Gplus Website

Besides the last news and remarkable achievements of the project, it provides access to public deliverables, scientific publications, event dates as well as insights about the project activities and outcomes. All the new content uploaded to the website is highly promoted through the project and



partners' social media accounts to maximise the reach, inform followers and interested parties, and this drives the traffic to the website where visitors can get more information about a specific topic.

### Website visitors

We use *Google Analytics* to monitor and measure relevant metrics that indicate the traffic of the website to understand if the content provided is well received by visitors. Figure 2 presents data on the number of users, session, page views, and average session duration for the reported period.

Website visitors – 1 May 2021 – 13 October 2022



Figure 2: INSPIRE-5Gplus Website visitor analytics

Country	Acquisition		
	Users	New Users	Sessions
	2,849 % of Total: 100.00% (2,849)	2,834 % of Total: 100.04% (2,833)	4,091 % of Total: 100.00% (4,091)
1. United States	340 (11.80%)	339 (11.96%)	356 (8.70%)
2. France	305 (10.58%)	298 (10.52%)	537 (13.13%)
3. Spain	254 (8.81%)	249 (8.79%)	458 (11.20%)
4. Germany	213 (7.39%)	208 (7.34%)	443 (10.83%)
5. India	165 (5.73%)	164 (5.79%)	210 (5.13%)
6. Finland	133 (4.61%)	127 (4.48%)	225 (5.50%)
7. China	130 (4.51%)	127 (4.48%)	147 (3.59%)
8. Greece	108 (3.75%)	104 (3.67%)	183 (4.47%)
9. Netherlands	91 (3.16%)	90 (3.18%)	117 (2.86%)
10. Canada	85 (2.95%)	84 (2.96%)	99 (2.42%)

Figure 3: INSPIRE-5Gplus Website visitor - geographical information




Figure 3 presents a user analysis by country for the period from 1st May 2021 to 13th Oct 2022. There are visitors from EU countries and from non-EU countries such as the United States. Most of the visits come from countries where a project partner has its headquarters, but there are visits from users based in other EU countries, which means that the content and work done by the project partners is reaching other territories, driving innovation and research activities in the fields addressed by the Inspire project.

#### **News items**

The conducted activities are captured in the news section of the website as shown in Figure 4. Various activities are reported such as participation in events, the submission of papers, awards and recognitions, etc. thus promoting the digital visibility of the project.






### JOINT INSPIRE-5GPLUS AND AI@EDGE WORKSHOP AT 11TH IEEE INTERNATIONAL CONFERENCE ON CLOUD NETWORKING (IEEE CLOUDNET 2022)

October 28, 2022

11th IEEE International Conference on Cloud Networking (IEEE CloudNet 2022) is being held in Paris, France from 7–10 November 2022. H2020 INSPIRE-5Gplus project (ICT-20) co-organizes, with AI@EDGE (ICT-52) project, a [...]

[Read More](#)




### INSPIRE-5GPLUS ENABLERS HIGHLIGHT THE NEW CAPACITIES OF SECURITY COMMITMENTS

October 26, 2022

The Orange « Salon de la Recherche et de l'Innovation » was held the 18 to 20 of October in Chatillon (92 – France). During this event the INSPIRE-5Gplus project [...]

[Read More](#)




### Cerrando brechas en las REDES 5G y 6G

October 25, 2022

Press release covering the activities conducted in the project INSPIRE-5Gplus has been published in the October issue of the "Nova Ciencia" Spanish national-wide journal. This release focuses on Development [...]


[Read More](#)



### INSPIRE-5GPLUS MENTIONED IN CIGREF

September 20, 2022


Cigref – Futuribles International working group presents a report on: The outlook for 5G in 2030 in France and Europe. This report gives an overview on



### INSPIRE-5GPLUS AT THE FUTURE NETWORK WORLD FORUM

October 17, 2022

INSPIRE-5Gplus supports at Future Network World Forum. This forum aims to bring experts from industry, academia, and research to exchange



### INSPIRE-5GPLUS CONTRIBUTES IN INTERNATIONAL CONFERENCE ON FUTURE INTERNET OF THINGS AND CLOUD

Figure 4: INSPIRE-5Gplus news item in the website

## Newsletter

The project has released several newsletter releases per year. During the first year (2020) Newsletter #1 and #2-3 were designed, elaborated, and released. During the second year of the project the same approach was followed and performed. This year, Newsletter #8 and #9 have been released and the





release of #10 is still ongoing so that at the end of M36 the Newsletter #10 will be shared with the newsletter subscribers (by email) and made available on the project website for all visitors.

All available newsletters are available on the [Newsletter section](#) on the INSPIRE-5Gplus project website.

A call to action on the [homepage](#) and a dedicated site are available for new visitors so they can easily subscribe to the newsletter as well as manage their subscription, as shown in Figure 5.

#### 5G+ Security News

5G+ Security News is the free e-mail newsletter of 5G-PPP project INSPIRE-5Gplus. The newsletter is published quarterly and provides concise information about the activities and results of INSPIRE-5Gplus.



- 5G+ Security News – Issue 1 / May 2020 (PDF for download)
- 5G+ Security News – Issue 2-3 / August-November 2020 (PDF for download)
- 5G+ Security News – Issue 4-5 / March-June 2021 (PDF for download)
- 5G+ Security News – Issue 6-7 / July-December 2021 (PDF for download)
- 5G+ Security News – Issue 8 / March 2022 (PDF for download)
- 5G+ Security News – Issue 9 / July 2022 (PDF for download)

#### Free registration

In order to subscribe to '5G+ Security News', please enter your e-mail address in the form below and click 'Subscribe'. You will receive an e-mail containing a confirmation link, which you need to click for completing your registration.

Email \*

[Subscribe!](#)

[Data protection and unsubscribing](#)

Figure 5: INSPIRE-5Gplus security newsletter database and subscription

## 2.1.8 Social Media

The focus of the project's Social Media activities has been on Twitter and LinkedIn and have been used to promote and give visibility to advancements and relevant information.

Main posts are shared between these two platforms (LinkedIn and Twitter), to multiply the reach of each specific update of the project, but each platform has a very different return. Twitter and LinkedIn are the main focuses of the project, while Youtube helps in providing high-quality, and informative videos online and thus has been dedicated to videos produced by the INSPIRE-5Gplus consortium.

**Twitter:** The Twitter account (@INSPIRE-5Gplus) is specifically aimed at interacting and establishing a relationship with other related projects, which are part of the H2020 ecosystem.

Content was posted regularly to provide followers with relevant information about topics related to the project. Also, information posted by other accounts are re-tweeted and liked to generate interaction with key accounts while also amplifying the scope of the content offered by INSPIRE-5Gplus. In the last 3 months, a total of 7 tweets have been done at the by INSPIRE-5Gplus account. The number of posts is related to the number of activities and events where the project is participating. It shows that social media results can therefore be directly related to the performance of the project visibility as a whole.



Figure 6: Twitter account

Figure 7 and Figure 8 show Tweet impressions over the months of June, July and August 2022. We can view the performance of the tweets that led to engagements.

Your Tweets earned **1.0K impressions** over this **91 day** period

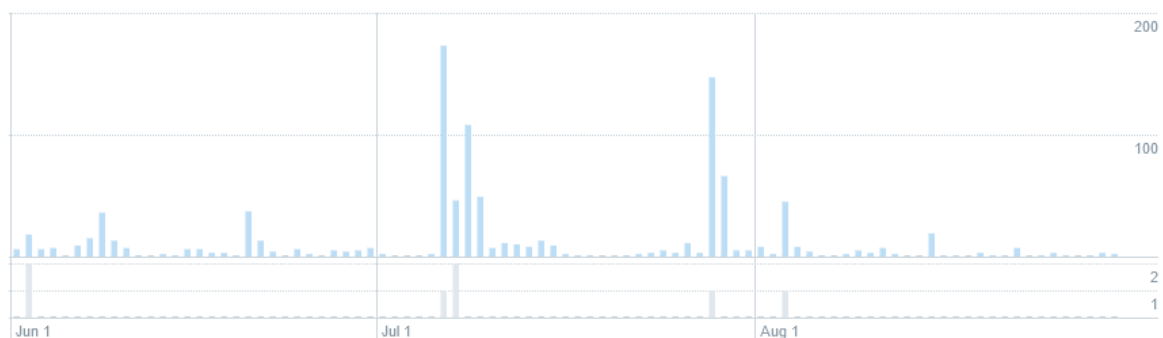


Figure 7: INSPIRE-5Gplus Twitter insight

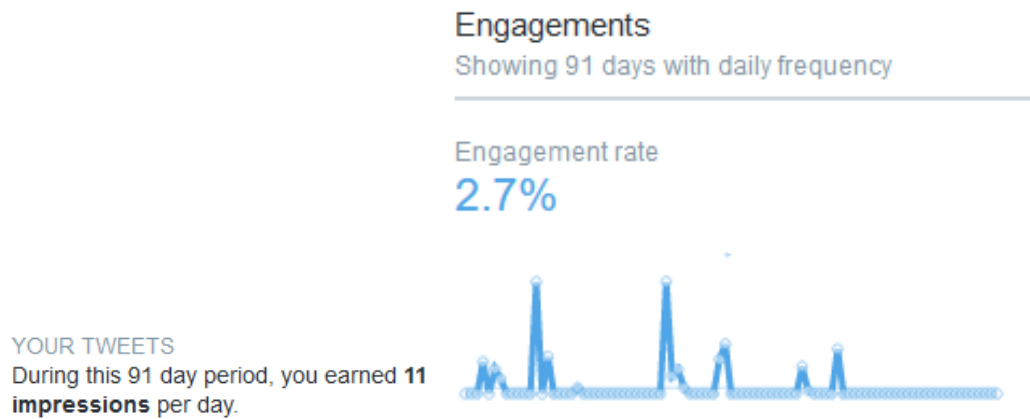


Figure 8: INSPIRE-5Gplus Twitter insight

Our Twitter strategy has been paying off as we are established at a current rate of 11 organic impressions per day, with 5 tweets in the last 3 months that have reached a minimum of 66 organic impressions to a maximum of 252 organic impressions.

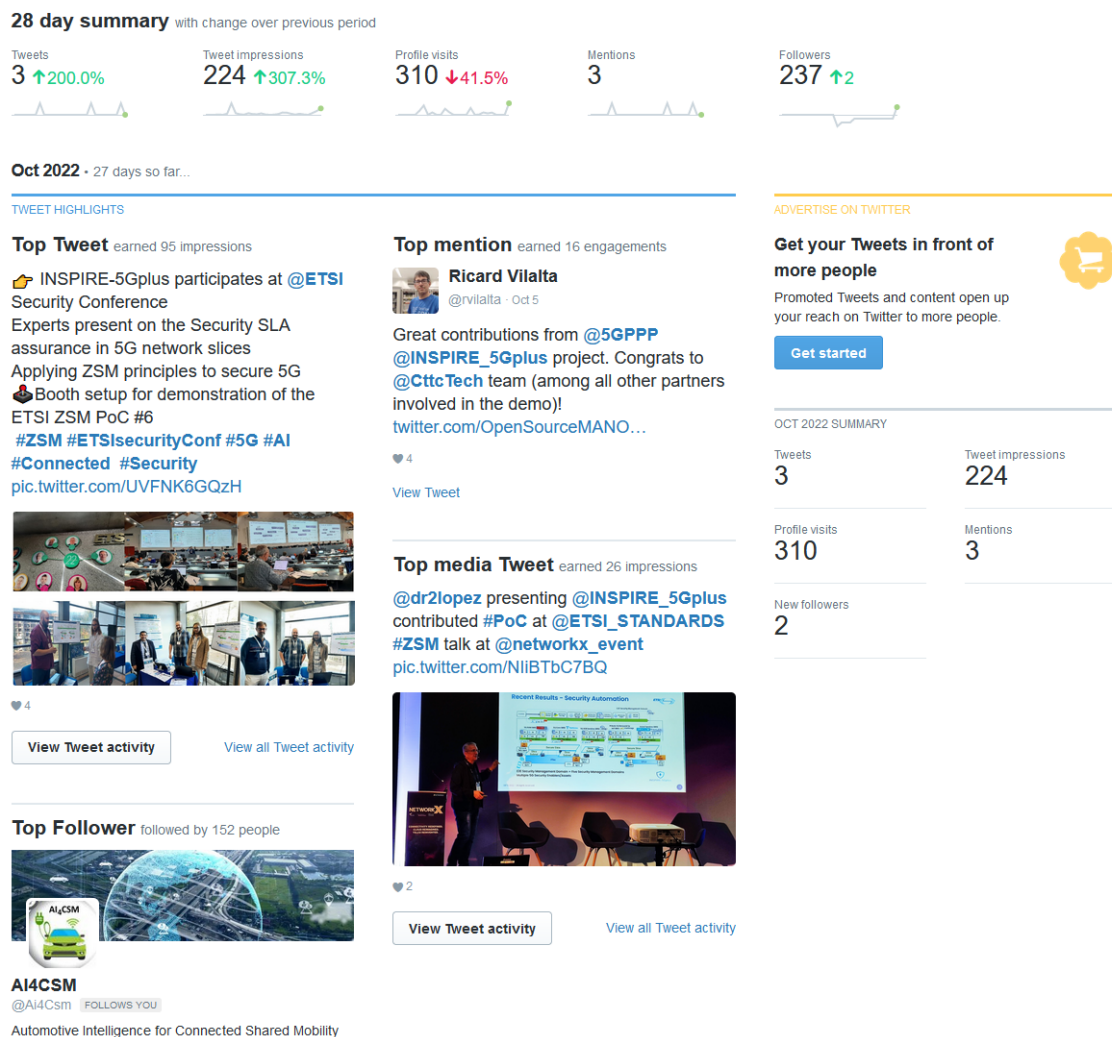


Figure 9: INSPIRE-5Gplus Twitter engagement &amp; tweets





**LinkedIn** -INSPIRE-5Gplus company page on LinkedIn (INSPIRE-5Gplus, Horizon 2020 Project at INSPIRE-5Gplus Project Consortium) (Figure 10) is an essential part of the communication and dissemination strategy.



Figure 10: LinkedIn profile Project INSPIRE-5G plus

This social network targets more professional and technical audiences and connects the project with specialized profiles that could be potentially interested in the project results. In this case, what matters are the rates and metrics indicating reactions from followers, which indicate if the content is well received by followers.

For this purpose, the analytics is the main focus. Figure 11 shows the number of profile views, impressions, and our search appearance. The reactions demonstrate that the project partners are providing quality content on LinkedIn that followers and visitors are interacting with.

## Analytics

Private to you

**22 profile views**  
Discover who's viewed your profile.

**511 post impressions**  
Check out who's engaging with your posts.

**8 search appearances**  
See how often you appear in search results.

Figure 11: LinkedIn Analytics

Figure 12 gives an overview of engagement on the recent posts of the project. Overall, the performance on this social network has been very good in accordance with the status of the project.

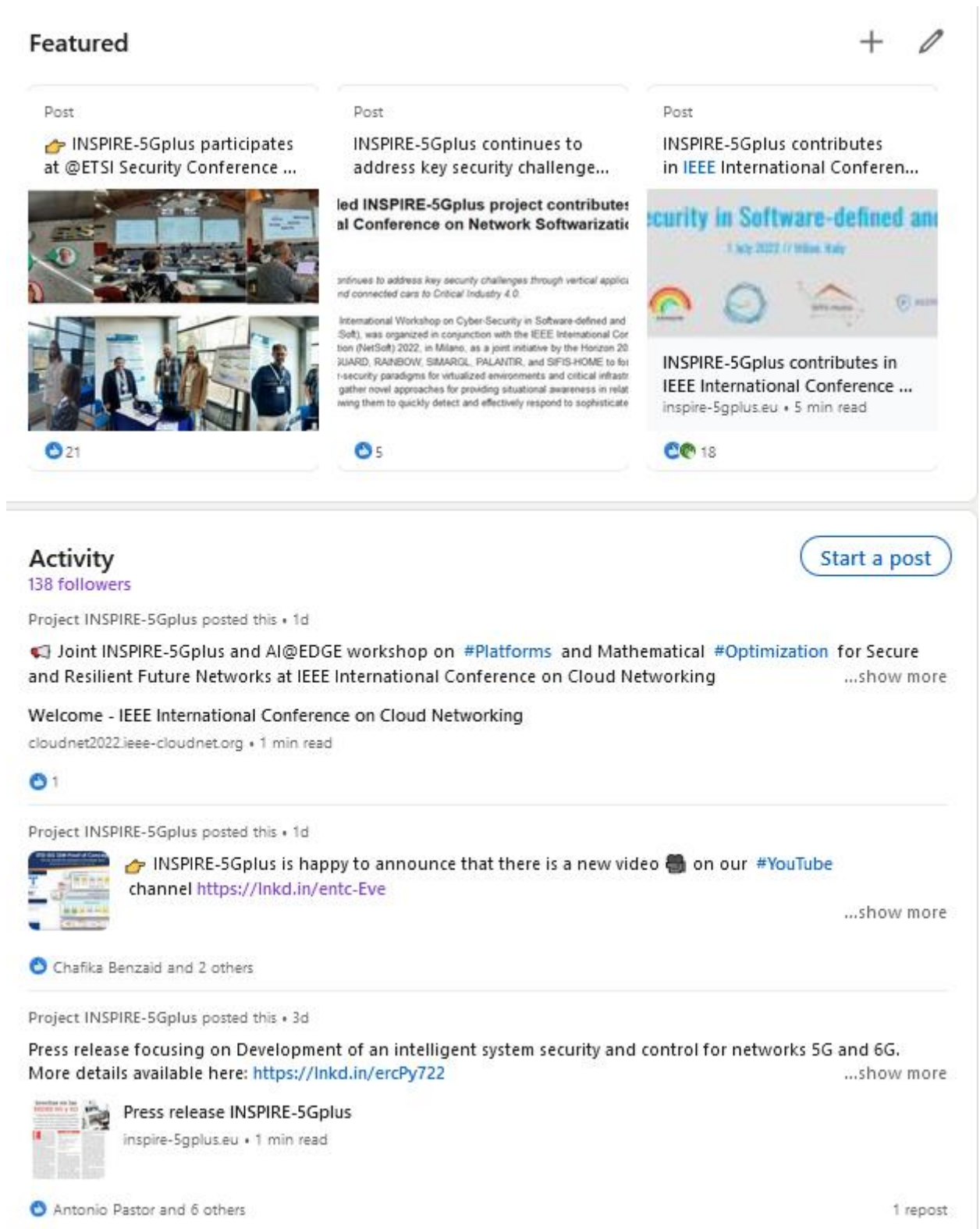


Figure 12: Post engagements

## YouTube

A YouTube channel of INSPIRE-5Gplus is dedicated to the project was primarily dedicated to upload different types of videos presenting and explaining the project. Project partners used this platform to present the progress of the technical development and its results in a visual way. Figure 13 is the glimpse of YouTube page. Currently, the channel has 17 subscribers and 5 videos.

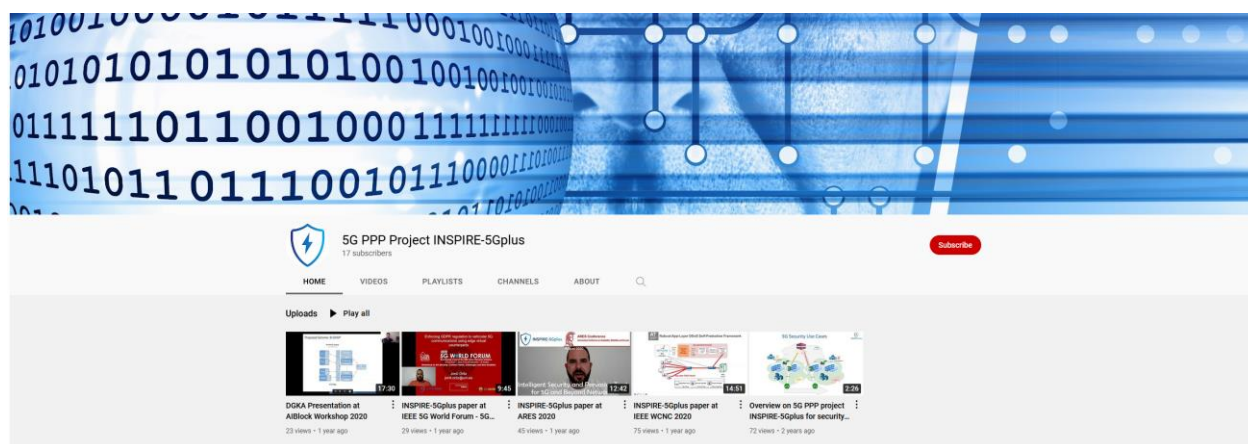


Figure 13: YouTube page of INSPIRE-5Gplus

### 2.1.9 Project tracker

EuresTools Tracker is a cloud-based tool for tracking and controlling dissemination activities and results that the Project has used during its lifetime. It provides an easy overview on activities and results, and facilitates the process of agreeing on dissemination documents. Through an easy-to-use export function, Tracker enables Horizon 2020 project partners to prepare up-to-date information on status of dissemination activities. It helps in keeping an overview of related activities in the project and therefore KPIs. Lists of dissemination activities and documents are fully customisable using this tool.

In addition, the tool also provided an automated integration of dissemination results on the project website. A screenshot of the tracker's main page is shown in Figure 14.

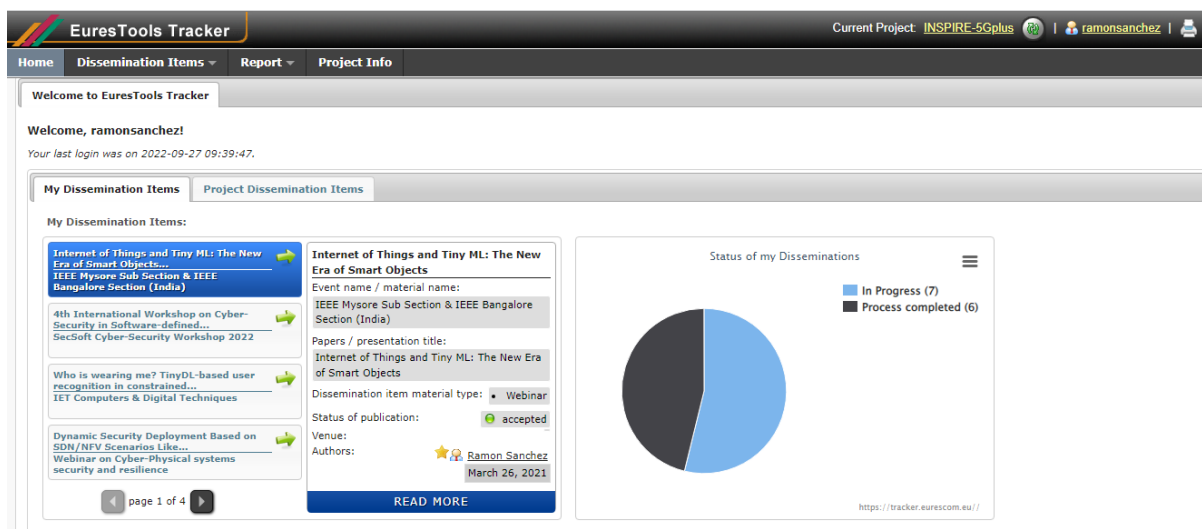


Figure 14: Project tracker



## 3 Standardisation activities

### 3.1 Standards-related strategy summary

The activities carried out within the standardization task (T6.2) in this period are based on the principles defined in D6.1. They can be defined as:

- Maintain the standardization strategy, including the most relevant target organizations, bodies, and professional societies where INSPIRE-5Gplus could contribute with project's key innovations.
- Constantly evaluate the applicable standardization bodies to identify new opportunities, reconsider and pivot efforts towards those most suitable to increase the impact of INSPIRE-5Gplus results.
- Update and promote the tracking tool, to assess progress, coordinate activity, raise awareness of new standardization opportunities, and increase commitment and participation among consortium partners.
- Combine the impact of standardization with the participation of partners in open-source software communities. Besides, create a parallel "fast track" in the standardization processes through "de facto" adoption through these open-source projects with high impact, some of them promoted by the standardization organizations themselves.

### 3.2 Standards-related results

This section completes the activities done after the ones reported in D6.2. Specifically depicts the final results of the standardization activities in INSPIRE-5Gplus during the second period of the project (M18-M36). Below Table 3 summarizes the actions and following subsections details them.

Standardization Body	Group	Activity type	Contributions <sup>5</sup>	Description
ETSI	ENI	whitepaper	2	ENI White paper (Details in Section 3.2.1)
ETSI	MEC	whitepaper	1	ETSI MEC White paper (Details in Section 3.2.1)
ETSI	MEC	document	1	Definition of a work-item MEC-0041 (Details in Section 3.2.1)
ETSI	NFV	whitepaper	1	Leading NFV Research Agenda and collaborating in ETSI's Research Strategy (Details in Section 3.2.1)
ETSI	NFV	document	1	Definition of a work-item (NFV-- IFA047) (Details in Section 3.2.1)
ETSI	ZSM	document	2	Contribution for Trust Management ZSM-014 (Details in report D6.3 and Section 3.2.1)

<sup>5</sup> Iterations in material over different sessions and meetings



ETSI	ZSM	update	2	ETSI ZSM PoC INSPIRE (Details in Section 3.2.3.1)
IETF	NMRG	update	6	IETF meetings in NMRG group (Details in Report D6.3 and Section 3.2.2)
IETF	NMRG	document	8	Draft for Network Digital Twin (Details in Report D6.3 and Section 3.2.2)
IETF	I2NSF	document	2	RFC 9061 and re-chartering (Details in Report D6.3 and Section 3.2.2)
IETF	SFC	update	1	SFC re-chartering support for application of PoT (Details in Section 3.2.2)
IEEE	WG P1920.1 and WG P1920.2	document	1	Contribution to security aspects of Draft IEEE 1920.1 Standard for Aerial Communications and Networking - under voting at IEEE.  Contribution to White Paper “Security for V2V Communications for Unmanned Aircraft Systems” of IEEE P1920.2 WG Standard for Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems
Open-Source project	5greplay	code	1	New open-source project. (Details in Section 3.2.3.3)
Open-Source project	OSM	update	1	Add INSPIRE-5Gplus to OSM research group (Details in Section 3.2.3.2)

Table 3: Standardization activities in M18-M36 period

### 3.2.1 ETSI

ETSI is recognised as a European Standards Organisation dealing with telecommunication, broadcasting and other electronic communication networks and services. ETSI does not involve national delegates—its members are international stakeholders from industry, organisations and government.

#### NFV

As part of the Network Function Virtualisation (NFV)<sup>6</sup> and the Industry Specification Group (ISG), INSPIRE-5Gplus partners supported the creation of a new working-item in the IFA (Interfaces and Architecture) working group, the NFV-IFA047. It focuses on standardizing the Management Data Analytics (MDA) function so it can be exploited by advanced AI/ML solutions.

Furthermore, ETSI NFV considered the added value provided by research activities, including a Proof of Concept (PoC) and open-source communities, for standardization. INSPIRE-5Gplus through a partner in a relevant position (TID) lead the development of a research agenda in this group, coordinating and proposing key security aspects to research derived from experience in INSPIRE-5Gplus. The result was

<sup>6</sup> <https://www.etsi.org/technologies/nfv>



reflected in the public document NFV(21)000072r1<sup>7</sup>, which ultimately drove the creation of the ETSI RISE initiative (Research Innovation Standard Ecosystem)<sup>8</sup>, focused on fostering collaboration between standards and research.

### ENI

The Experiential Networked Intelligence (ENI)<sup>9</sup> ISG focuses on the specification of cognitive network management system, including concepts such as autonomy and closed-loop in the network. Final use case H definition related to security analysis of encrypted traffic and later instantiated in Demo1 with crypto-mining attack has been contributed into “ETSI Whitepaper n°44: ENI Vision: Improved Network Experience using Experiential Networked Intelligence”<sup>10</sup>. The ENI system proposed in this use case covers the functionality of the Security Analytics Engine and Decision Engine from INSPIRE-5Gplus High Level Architecture (HLA).

### ZSM

The Zero Touch Network and Service Management (ZSM)<sup>11</sup> ISG has been taken as framework reference to define the HLA for INSPIRE-5Gplus. The consortium has increased its presence in this group, following 2 approaches. Firstly, by transferring the INSPIRE-5Gplus results to the standardization through a specific contribution into ZSM014 document, to include Trust Management service. This contribution was submitted and accepted in the ZSM#20 face-to-face meeting (10-13<sup>th</sup> October 2022) in Dublin, as ZSM(22)000343r3. Secondly, by proposing the INSPIRE-5Gplus for a Proof-of-concept (PoC) in ETSI ZSM to gain visibility of the project results in a standardization group. The proposal ([https://zsmwiki.etsi.org/images/e/e1/ZSM\\_POC\\_6.pdf](https://zsmwiki.etsi.org/images/e/e1/ZSM_POC_6.pdf)) was presented in ZSM#19 F2F meeting (16-19<sup>th</sup> May 2022) in Sophia Antipolis, as ZSM(22)000343, and accepted one month later. Details about the PoC are available at Section 3.2.4.13.2.4. This standardization activity involves commitments beyond the INSPIRE-5Gplus project lifetime.

### MEC

The Multi-access Edge Computing (MEC)<sup>12</sup> ISG focuses its activity on standardize the integration of applications, cloud, and IT systems solutions as multi-access edges platforms within 5G networks. The consortium supported with the knowledge acquired in the threat analysis and use case proposals to the security analysis done and published by the ETSI group related to security: “ETSI Whitepaper n°46: MEC Security; Status of standards support and future evolutions”<sup>13</sup>. Additionally, it contributed to the creation and definition of a new Work-item in progress: “MEC-0041.Multi-access Edge Computing (MEC); Study on MEC Security”.

## **3.2.2 IETF/IRTF**

The Internet Engineering Task Force (IETF) is the body acting as producer and maintainer of the core Internet specifications, from IP to HTTP, and explicitly referenced by many other bodies in their standardisation activities. IETF activity is organized in WG formed around a charter describing their objectives and plans.

---

<sup>7</sup> [https://docbox.etsi.org/ISG/NFV/Open/Other/NFV\\_Research\\_Agenda-202104.pdf](https://docbox.etsi.org/ISG/NFV/Open/Other/NFV_Research_Agenda-202104.pdf)

<sup>8</sup> <https://www.etsi.org/e-brochure/Research-Brochure/mobile/index.html>

<sup>9</sup> <https://www.etsi.org/committee/eni>

<sup>10</sup> [https://www.etsi.org/images/files/ETSIWhitePapers/etsi-wp44\\_ENI\\_Vision.pdf](https://www.etsi.org/images/files/ETSIWhitePapers/etsi-wp44_ENI_Vision.pdf)

<sup>11</sup> <https://www.etsi.org/committee/zsm>

<sup>12</sup> <https://www.etsi.org/committee/mec>

<sup>13</sup> <https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP-46-2nd-Ed-MEC-security.pdf>





### NMRG

The Network Management Research Group (NMRG) focuses on the research in new technologies around network management that is not mature enough to be addressed yet in other IETF WG.

During this period, support and improvement of the concept of Network Digital Twin (DTN) through the draft has continued aiming at consolidating the concepts of data generation, collection and security analytics AI models creation. The contribution has been done through several iterative draft versions until the adoption as a WG draft of the document “Digital Twin Network: Concepts and Reference Architecture”<sup>14</sup>. The activity has included discussions with participants using mailing list and at the FIP/IEEE International Symposium on Integrated Network Management (17<sup>th</sup> May 2021), and the IETF111 (27<sup>th</sup> July 2021), IETF112 (5<sup>th</sup> November 2021), IETF113 (24<sup>th</sup> March 2022), and IETF114 (27<sup>th</sup> July 2022) meetings.

### SFC

This Working Group focuses its activity on the architecture, protocols and metadata to provide Service Function Chaining (SFC)<sup>15</sup> capabilities in the network. One relevant result of the WG is the creation of the Network Service Header (NSH). The focus of the activity in INSPIRE-5Gplus has been to support the re-chartering of the WG to expand the possibilities and bring results from some enablers such as OPoT and other related management protocols.

### I2NSF

The standardisation of several interfaces for security network functions is the objective of the WG Interface to Network Security Function (I2NSF). In this period, it has been able to consolidate the draft related to the YANG Data Model for IPsec Flow Protection into the publication of the RFC 9061 (<https://datatracker.ietf.org/doc/rfc9061/>), thanks to the support of the proof-of-concept executed in the project with I2NSF IPsec enabler as part of Demo1. Additionally, the consortium has supported the re-chartering of the WG in order to consolidate the attestation mechanisms developed by some enablers.

## **3.2.3 IEEE**

In the first half of the project, we have contributed to the security aspects of *IEEE 1902.1 Draft Standard for Aerial Communications and Networking Standards*. IEEE 1902.1 Working Group (WG) carries out standardisation work related to an important vertical for 5G; wireless networking and communications of UAVs/drones including the security of those systems. The underlying WG premise was to render the baseline, establish connections with other SDOs/institutions like ASTM, NASA, and FAA, and have follow-up WGs to elaborate further, if possible. The work group is chaired by Prof. Kamesh Namuduri from University of North Texas. and Dr. Gürkan Gür from ZHAW who attended monthly group meetings (virtual) and was responsible for the security section (e.g., security analysis, threats, security controls) for the draft standard. Currently, the draft standard is going through the IEEE voting procedures to be approved and published. The contributions to this standard are related to WP2 work in INSPIRE-5Gplus.

Moreover, a new follow-up standardisation WG named IEEE 1920.2 WG on Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems<sup>16</sup> has also recently been established. It aims to define the protocol for exchanging information between the vehicles. The information exchange will facilitate beyond line of sight (BLOS) and beyond radio line of sight (BRLOS) communications. The information exchanged between the aircraft may be for the purpose of command, control, and navigation or for

---

<sup>14</sup> <https://datatracker.ietf.org/doc/draft-irtf-nmrg-network-digital-twin-arch/>

<sup>15</sup> <https://datatracker.ietf.org/wg/sfc/about/>

<sup>16</sup> <https://standards.ieee.org/ieee/1920.2/7517/>



any application specific purpose. ZHAW is a member of the Security subgroup in this standardization workgroup. It is also working to identify how to contribute to this standard from the security perspective. Currently, ZHAW has contributed to the IEEE 1920.2 White Paper “Security for V2V Communications for Unmanned Aircraft Systems”, This white paper is about to be finalized and expected to be published in the first quarter of 2023.

### 3.2.4 Open-source initiatives

Open-source communities, in general, are more agile than standardization bodies in meeting interoperability needs and testing the feasibility of standards and their incorporation. This has led to a growing interest in open source in recent times. This is why a beneficial symbiosis between standards and open source is being promoted. This virtuous circle is often realised through proof-of-concept or open-source projects sponsored by standardisation bodies. INSPIRE-5Gplus has not been unaware of this trend and some of the activities done in this area are highlighted below.

#### 3.2.4.1 ETSI ZSM PoC

One of the relevant activities from ETSI ZSM is promoting the proof-of-concept (PoC) to evaluate and improve its standards. INSPIRE-5Gplus based PoC was proposed and accepted by the ETSI ZSM in May2022<sup>17</sup>. The PoC called: “PoC 6 Security SLA assurance in 5G network slices” is based on Demonstration 1, described in D5.3.

The PoC has been publicly showed by representatives of TID and UMU in a booth that was part of the ETSI Security conference 2022, on 3-5th October in ETSI Headquarters in Sophia Antipolis, France<sup>18</sup> (Figure 15). Appendix C presents the PoC poster.

A video showing the participation on this event can reached at: <https://www.youtube.com/watch?v=b9H4PYUeYEQ>



Figure 15: ETSI ZSM PoC # 6 Security SLA assurance in 5G network slices

#### 3.2.4.2 ETSI OSM

Open Source MANO (OSM) is an open source solution adopted by ETSI as an OSG (Open Source Group). The idea is to help through these open software communities the quick acceptance of standards using the development capacity of this kind of projects as a “fast path” to adoption.

<sup>17</sup> [https://zsmwiki.etsi.org/index.php?title=PoC\\_6\\_Security\\_SLA\\_assurance\\_in\\_5G\\_network\\_slices](https://zsmwiki.etsi.org/index.php?title=PoC_6_Security_SLA_assurance_in_5G_network_slices).

<sup>18</sup> <https://www.etsi.org/events/upcoming-events/2068-etsi-security-conference#pane-6/>





INSPIRE-5Gplus has been working with OSM as one of the relevant assets used for the service management Domains. The work is recognised and added as a new project part of the OSM Ecosystem<sup>19</sup>, to provide visibility of the project (Figure 16).

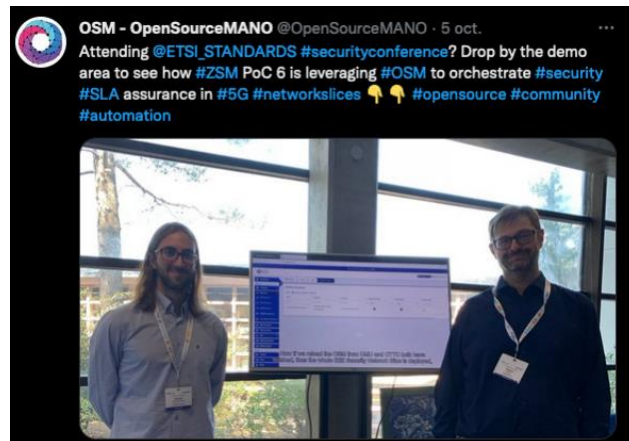


Figure 16: News with the use of OSM in INSPIRE-5Gplus PoC

### 3.2.4.3 5Greplay

INSPIRE-5Gplus has started an open-source project covering MI's monitoring solution (MMT) and from this has derived a tool called 5greplay. This tool is an open-source 5G fuzzer that allows forwarding 5G network packets from one network interface card to another with or without modifications. Thus, it can be used to test and certify the resiliency of 5G components to given attack types and anomalous packets.

5greplay can be configured by user defined rules. The rules allow specifying which packets should be filtered or not, which should be modified or not (e.g., an attribute, the payload), which should be duplicated or shuffled, and indicating what type of modification (e.g., a given value or random value) and more. Thus, 5Greplay allows performing stress testing, generating and executing cyberattacks, performing pentesting and fuzz testing<sup>20</sup>

<sup>19</sup> <https://osm.etsi.org/wikipub/index.php/Research#INSPIRE-5Gplus>

<sup>20</sup> Zujany Salazar, Huu Nghia Nguyen, Wissam Mallouli, Ana R. Cavalli, Edgardo Montes de Oca: 5Greplay: a 5G Network Traffic Fuzzer - Application to Attack Injection. ARES 2021: 106:1-106:8 (<https://5greplay.org/docs/publications/ares2021-slide.pdf>)



## 4 Communications and Dissemination KPIs

The following Table 4 and Table 5 present a comparison between the identified communication and dissemination KPIs and the achievements at the end of INSPIRE-5Gplus.

Communications means	Success indicator	Target # of outputs	Outputs achievement	Target audience	Reached audience
Liaison with relevant standardization bodies	# of active contributions to standards	5	20	Cybersecurity community	Cybersecurity community and standardization organisations
Liaison with ECSO, participation in WGs and events	# attended events	> 6	7 (WG1, WG6 and liaison for 5G security)	> 50 participants per event	50 participants in total (>15 per event)
Liaison activities, common events with other H2020 projects & knowledge exchange	# of relevant projects # of joint workshops	10 3	Collaborations: 12 Joint workshops: 5	> 100 researchers on projects	150 researchers on projects
Workshops/showcases	# of events / attendees	5	6	250 participants in total	300 participants in total
Policy-level events in Brussels	# of events	2	3 (ENISA, ECSO, 5G-PPP)	> 60 cybersecurity policy makers	75 cybersecurity policy makers
Project website	SEO Metrics  Average duration of visits	1  2 min	1  2 min 14s	> 5000 unique visitors	4179



Social Media	# of users  Number of accumulative posts	4 social media channel  500	4 social media channels (Twitter/Linkedin/YouTube/SlideShare)	>750 followers	393 (Twitter: 237, LinkedIn: 139; YouTube: 17; SlideShare: 0)
Project news	# of posts	>100	60	3000 visits	207
Press releases	# of elements	10	10	>1000 readers	>2000 readers
Project branding	# of factsheets, brochures, banners	> 8	2 leaflets 2 roll-ups 1 poster for ETSI PoC 1 poster for EUCnC'21 1 ETSI poster for MWC'19 1 poster for UMU national-event dissemination	Reached audience >200	>250
White papers	# of publications	4	4	500 recipients	523 recipients
Newsletters	# of publications	15	10	> 500 subscribers	200 subscribers
Promotional videos	# of views	5	6	> 500 views	267views
Project meetings / roundtables	# of events	10	11 (Plenary meetings + technical meetings)	> 40 internal and invited stakeholders	50 internal and invited stakeholders
Deliverables (public)	QA standards	> 20	22 (Deliverables (18) + white papers (4))	500 recipients	125 recipients

Table 4: KPIs and achieved results for communication activities



Measure	KPI & Success Index	Achievement (M01-M36)
Publications in conferences	No. of peer-reviewed publications at conferences and workshops $\geq 7$ per year on average	M01-M18: 14 M19-M36: 31
Publications in journals	No. of peer-reviewed publications in journals $\geq 3$ per year on average	M01-M18: 13 M19-M36: 7
Participation to industrial events/exhibitions	No. of industrial events $\geq 2$ per year on average	M01-M18: 24 M19-M36: 7  Forum International de la Cybersécurité 2021 & 2022 (MI)  HEXA-X (TID)  EUCnC (all)  Network X (TID)  Industrial forum 2022 (UMU/THALES)  EuropeanCyberWeek 2022 (OPL)  Orange «Salon de la Recherche et de l'Innovation» 2022 (ORANGE, OPL, TAGES)
Innovation workshop	No. of organized innovation workshops = At least 1 by the end of the project	M01-M18: 2 M19-M36: 5
Seminars	No. of organized seminars = At least 2 by the end of the project	M01-M18: 3 webinars M19-M36 2 webinars
Academic dissemination	Average number of participants per lecture = At least ~50-70 participants per lecture	M01-M18: Lectures based on the INSPIRE-5Gplus' High Level Architecture (50 students) M19-M36: Lectures based on the INSPIRE-5Gplus assets (50 students) 1 on-going doctoral course Lectures based on the INSPIRE-5Gplus' assets (17 students) 2 Bachelor Thesis 3 Master Thesis (2 finished, 1 ongoing) 2 PhD Thesis (1 finished, 1 ongoing) 3 internships
Participation and contribution to the 5G PPP programme	No. of participated/contributed 5G PPP WG's $\geq 6$	M01-M18: 2 participations in whitepapers M19-M36 >6. Architecture, Security, Test, Measurement and



		KPIs Validation, Trials, SME, Software Networks, 5GCAM
Interactions with worldwide fora and institutes	No. of iterations $\geq 1$ per year	M01-M19: ENISA 5G Specification 5G Threat landscape M19-M36: CyberSec4Europe: new challenges roadmap (UMU) 5GMobix: use case requirements (UMU) HEXA-X: INSPIRE-5Gplus advances presentation (TID) 5G Certification scheme (THALES) ENISA WG Enterprise Security (MI)

*Table 5: KPIs and achieved results for dissemination activities*

As can be seen, all the established goals for the Dissemination, Communication and Standardisation-related KPIs have been reached. We had some deviations regarding the activity of the website and the social media channels, but we consider that given the notable figures attained in the rest of dissemination and communication channels, the reached audience has been satisfactory in order to attract great attention from the different target audiences defined at the beginning of the project.



## 5 Conclusions

The impact of COVID-19 pandemic forced the consortium to adapt its strategy regarding Dissemination and Standardisation activities at the beginning of the project. Some of the programmed events were cancelled during the initial period of the pandemic (e.g., Mobile World Congress MWC'20), but a virtual model gradually took hold. For this reason, the consortium started to give greater weight to online events, talks, virtual conferences and virtual standardisation meetings, in order to achieve the planned dissemination and standardisation objectives.

Although this issue has negatively affected to all the related activities, the final outcomes achieved at the end of the project are satisfactory, the project has reached an important number of diverse audiences and, in most of cases, achieving the expected results.



## Appendix A INSPIRE-5Gplus' organised workshops

### **Workshop on Automated and Intelligent Security, co-located with EuCNC and 6G Summit 2021**

#### **Program**

##### Opening Session

- Pascal Bisson and Antonio Skarmeta

##### Session 1: Security and Trust Architecture for Beyond 5G Networks

- Defining the Security Management Closed-Loop for INSPIRE-5Gplus, Jordi Ortiz (University of Murcia, Spain); Chafika Benzaid (Aalto University, Finland); Maria Christopoulou (NCSR Demokritos, Greece); Pol Alemany (Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), Spain); Geoffroy Chollon (Thales, France); Wissem Soussi (Zurich University of Applied Sciences (ZHAW) & University of Zürich (UZH), Switzerland)
- Overview of the Security and Trust Mechanisms in the 5GZORRO Project, José M. Jorquera Valero and Pedro Miguel Sánchez Sánchez (University of Murcia, Spain); Alexios Lekidis (Intracom Telecom, Greece); James Taylor (Bartr Group, United Kingdom (Great Britain)); Javier Fernandez Hidalgo and Adriana Fernández-Fernández (Fundació i2CAT, Internet i Innovació Digital a Catalunya, Spain); Paulo Chainho and Bruno Santos (Altice Labs, Portugal); Jean-Marie Mifsud and Antoine Sciberras (Malta Communications Authority, Malta); Muhammad Shuaib Siddiqui (Fundació i2CAT, Internet i Innovació Digital a Catalunya, Spain); Manuel Gil Pérez, Alberto Huertas Celdrán and Gregorio Martinez Perez (University of Murcia, Spain)
- Metrics-Based Outlier Detection for 5G Security, Athanasios Priovolos, Dimitris Lioprasitis and Georgios Gardikis (Space Hellas S.A., Greece); Socrates Costicoglou (Space Hellas SA, Greece)

##### Session 2: Automated and Intelligent (smart) Security network management

- Towards a ZSM Security Orchestration for Multi-Tenant 5G Networks, Rodrigo Asensio-Garriga, Alejandro Molina Zarca, Jordi Ortiz, Jorge Bernal Bernabe and Antonio Fernando Skarmeta Gomez (University of Murcia, Spain) 5G-enabled AGVs for NPN Production Lines in Manufacturing (Manuel Fuentes, Fivecomm, 5G-INDUCE)
- 5G-INDUCE – A NetApp Orchestration Platform Enabling On-Demand Deployment of Security Services, Dimitrios Klonidis (UBITECH, Greece); Franco R. Davoli (University of Genoa & National Inter-University Consortium for Telecommunications (CNIT), Italy); Nicholas Sgouros (Eight Bells Ltd, Greece); George Amponis (K3Y, Bulgaria); Georgios Katsikas (Ubitech, Greece); Thanos Xirofotos (UBITECH, Greece); Roberto Bruschi (CNIT, Italy); Chiara Lombardo (University of Genoa & CNIT- Research Unit of the University of Genoa, Italy); Ioannis Giannoulakis (Eight Bells Ltd, Cyprus); Emmanouil Kafetzakis (Eight Bells Ltd., Cyprus); Panagiotis Gouvas (Ubitech, Greece)
- 5Growth: Hardening Interdomain Vertical Services with Moving Target Defense (MTD) Vitor A Cunha (Instituto de Telecomunicações, Portugal); Daniel Corujo (Instituto de Telecomunicações Aveiro & Universidade de Aveiro, Portugal); João Paulo Barraca and Rui L Aguiar (University of Aveiro & Instituto de Telecomunicações, Portugal)
- 5GMobix: Security Challenges on 5G CCAM Scenarios Luis Bernal-Escobedo (University of Murcia, Spain); Jose Santa (Technical University of Cartagena, Spain); Ramon Sanchez-Iborra and Antonio Fernando Skarmeta Gomez (University of Murcia, Spain)

##### Keynote

- Ashutosh Dutta. IEEE Communications Society Distinguished Lecturer and Co-Chair for IEEE Future Initiative.



### Session 3: Security Beyond 5G Networks and Services

- Hexa-X: Trustworthy Networking Beyond 5G, Diego Lopez (Telefonica I+D, Spain); Carlos J. Bernardos (Universidad Carlos III de Madrid, Spain); Bin Han (Technische Universität Kaiserslautern, Germany); Cédric Morin (IMT Atlantique & TéléDiffusion de France, France); Antonio de la Oliva (Universidad Carlos III de Madrid, Spain); Antonio Pastor (Telefonica I+D & Universidad Politécnica de Madrid, Spain); Cao-Thanh Phan (BCOM, France); Pawani Porambage (University of Oulu, Finland); Peter Schneider (Nokia Bell Labs, Germany); Hans D. Schotten (University of Kaiserslautern, Germany); Elif Ustundag Soykan (Ericsson Research, Turkey); Emrah Tomur (Ericsson Research & Middle East Technical University, Turkey)
- Cloud-Scale SDN Network Security in TeraFlow, Alberto Mozo (UPM, Spain); Antonio Pastor (Telefonica I+D & Universidad Politécnica de Madrid, Spain); Carlos Natalino and Marija Furdek (Chalmers University of Technology, Sweden); Rahul Bobba (NEC, Germany); Raul Muñoz, Ramon Casellas and Ricardo Martinez (Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), Spain); Juan Pedro Fernández-Palacios (Telefónica I+D, Spain); Ricard Vilalta (Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), Spain); Stanislav Vakaruk (Universidad Politécnica de Madrid, Spain)

### Session 4: Security Enablers for Beyond 5G Networks and Services

- SPIDER: ML Applied to 5G Network Cyber Range, Stanislav Vakaruk (Universidad Politécnica de Madrid, Spain); Alberto Mozo (UPM, Spain); Antonio Pastor (Telefonica I+D & Universidad Politécnica de Madrid, Spain)
- 5GASP: Security and Trust in NetApp Deployment and Operation , Jorge Gallego-Madrid (Odin Solutions); Ana Hermosilla (Odin Solutions, Murcia, Spain); Antonio F. Skarmeta (Odin Solutions S. L, Spain)
- Towards 5G Embedded Trust: Integrating Attestation Extensions in Vertical Industries, Thanassis Giannetsos and Dimitrios Papamartzivanos (Ubitech Ltd., Greece); Sofia Anna Menesidou (Ubitech Ltd, Greece); Sophia Karagiorgou (Ubitech, Greece)
- PALANTIR: Practical Autonomous Cyberhealth for Resilient Micro/Small/Medium-Sized Enterprises, Dimitris Papadopoulos (Infili Technologies, Greece); Antonios Litke (Infili Information Intelligence Ltd, Greece); Manuel Gil Pérez (University of Murcia, Spain); Maxime Compastie (i2CAT Foundation, Spain); Roberto Bifulco (NEC Laboratories Europe, Germany); George Xylouris (Orion Innovations PC, Greece); Michail Alexandros Kourtis (NCSR Demokritos, Greece); Vangelis Logothetis (Incites Consulting, Luxembourg); George Athanasiou (DBC Europe, Belgium)

In the following, some pictures taken during the event celebration.





Figure AA-1: Presentation of the Workshop on Automated and Intelligent Security

### Key Points for 5G Adoption and Usage



Figure AA-2: Keynote speech at the Workshop on Automated and Intelligent Security

### **4th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft), co-located with IEEE International Conference on Network Softwarization (NetSoft'22)**

#### **Program**

Welcome Session

Session Chair: Fulvio Valenza, Politecnico di Torino, Italy

Cyber Security EU funded projects

Session Chair: Alessio Sacco, Politecnico di Torino, Italy

- GUARD – Guarantee Reliability and trust for Digital service chains. Matteo Repetto, CNR-IMATI, Italy
- SIMARGL – Secure Intelligent Methods for Advanced Recognition of Malware and



Stegomalware. Joerg Keller, FernUniversität in Hagen, Germany

- SDN-microSENSE. Panagiotis Sarigiannidis University of Western Macedonia, Greece
- PALANTIR - Practical Autonomous Cyberhealth for resilient SMEs & Microenterprises. Ignazio Pedone Politecnico di Torino, Italy
- SIFIS-Home. Tom Tuunainen Centria University of Applied Sciences, Finland
- INSPIRE-5Gplus. Vincent Lefebvre Research Dpt and Tages, France
- ELECTRON - rEsilient and seLf-healed EleCTRical pOwer Nanogrid. Panagiotis Sarigiannidis University of Western Macedonia, Greece

#### Technical Session 1 – Attack Detection and Threat Identification

Session Chair: Joerg Keller, FernUniversität in Hagen, Germany

- Multi-domain Denial-of-Service Attacks in Internet-of-Vehicles: Vulnerability Insights and Detection Performance, Roshan Sedar, Charalampos Kalalas Centre Tecnològic de Telecomunicacions de Catalunya, Spain, Jesus Alonso-Zarate, Francisco Vázquez-Gallego i2CAT, Spain
- An application of Netspot to Detect Anomalies in IoT, Tom Tuunainen, Olli Isohanni, Mitha Jose Centria University of Applied Sciences, Finland, Model-Driven Network Monitoring Using NetFlow Applied to Threat Detection, Daniel González-Sánchez, Ignacio Domínguez Martínez-Casanueva, Luis Bellido, David Fernández Universidad Politécnica de Madrid, Spain, Antonio Pastor, Cristina Pinar Muñoz Zamorro, Alejandro Antonio Moreno Sancho, Diego Lopez Telefonica I+D, Spain

#### Technical Session 2 – Security Platforms and Architectures

Session Chair: Vincent Lefebvre, Research Dpt & Tages, France

- Evaluation of the data handling pipeline of the ASTRID framework, Matteo Repetto CNR - IMATI, Italy, Guerino Lamanna Infocom, Italy.
- Dynamic Risk Assessment and Certification in the Power Grid: A Collaborative Approach, Athanasios Liatifis, Panagiotis Radoglou Grammatikis, Panagiotis Sarigiannidis, University of Western Macedonia, Greece, Pedro Ruzafa Alcazar, University of Murcia, Spain, Dimitrios Papamartzivanos, Sofia Anna Menesidou, Ubitech Ltd., Greece, Thomas Krousarlis (Inlecom Innovation, Greece, Alberto Martin Molinuevo, Inaki AnguloTECNALIA, Spain, Antonios SarigiannidisSidroco, UK, Thomas Lagkas International Hellenic University, Greece, Vasileios Argyriou University of Surrey, UK
- Authentication and Authorization in Cyber-Security Frameworks: a Novel Approach for Securing Digital Service Chain, Giovanni Grieco, Domenico Striccoli, Giuseppe Piro, Alfredo Grieco Politecnico di Bari - CNIT, Italy, Raffele Bolla, Università di Genova - CNIT, Italy

#### Technical Session 3 – Security Models and Trust Schemes

Session Chair: Charalampos Kalalas, Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Spain

- A model of capabilities of Network Security Functions, Cataldo Basile, Daniele Canavese,



Leonardo Regano, Ignazio Pedone, Antonio Lioy Politecnico di Torino, Italy

- Always-Sustainable Software Security, Vincent Lefebvre Research Dpt and Tages, France, Gianni SantinelliTAGES, Italy
- Security Automation using Traffic Flow Modeling, Simone Bussa, Riccardo Sisto, Fulvio Valenza Politecnico di Torino, Italy

Keynote speech

Session Chair: Riccardo Sisto, Politecnico di Torino, Italy

- DDoS Mitigation and Network Softwarization, Carol Fung, Concordia University

Closing

Session Chair: Fulvio Valenza, Politecnico di Torino, Italy

In the following, the Workshop Call for Papers and pictures taken during the event celebration.



#### Call for Papers

The 4th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft) is a joint initiative from the H2020 EU Projects GUARD, RAINBOW, SIMARGL, PALANTIR, INSPIRE-5Gplus, SIFIS-HOME, ELECTRON and SDN-microSENSE to create a dialogue about emerging cyber-security paradigms for virtualized environments and critical infrastructures.

#### Scope

Evolving business models are progressively reshaping ICT services and infrastructures, with a growing "softwarization" trend, the massive introduction of virtualization paradigms, and the tight integration with the physical environment. Unfortunately, the evolution of cyber-security paradigms has not followed with the same pace, leading to a substantial gap in solutions capable of protecting the new forms of distributed and heterogeneous systems against an evolving landscape of cyber-threats.

Traditional security tools that organizations have long relied on to protect their networks (i.e., antivirus, intrusion prevention systems, firewalls) are no longer capable of providing sufficient security guarantees against the rapid escalation of advanced persistent threats and multi-vector attacks. The growing complexity of cyber-attacks are urgently demanding more correlation in space and time of (apparently) independent events and logs, and a higher degree of coordination among different security mechanisms.

#### Topics of interest

This Workshop aims to gather together novel approaches for providing organizations the appropriate situational awareness in relation to cyber security threats allowing them to quickly detect and effectively respond to sophisticated cyber-attacks.

Topics of interest include but are not limited to:

- Cyber-security platforms and architectures for digital services;
- Security, trust and privacy for industrial systems and the IoT (including smart grids);
- Monitoring and advanced data collection and analytics;
- Virtual and software-based cyber-security functions;
- Orchestration and Automatic Configuration of security functions;
- Novel algorithms and models for attack detection and threat identification;
- Authentication, Authorization and Access control;
- Intelligent attack mitigation and remediation;

- Machine learning, big data, network analytics;
- Secure runtime environments, including trustworthy systems and user devices;
- Formal methods and policies for security and trust;
- Trusted computing;
- Information flow control;
- Risk analysis and management, Audit and Accountability;
- Honey pots, forensics and legal investigation tools;
- Threat intelligence and information sharing.

Multi-disciplinary and collaborative research projects are encouraged to submit joint papers describing their integrated architectures and cyber-security platforms, with special emphasis on how they address the challenging cyber-security requirements of softwarized environments and critical infrastructures.

#### Paper submissions

Interested authors are invited to submit papers according to the following guidelines:

- papers must be up to 6 pages long, including tables, figures and references;
- the style to be used is IEEE 2-column US-letter style using IEEE Conference template, and papers must be submitted in pdf format.

Accepted and presented workshop papers will be published in the conference proceedings and will be submitted to IEEE Xplore.

For more details about submission form and procedure, please check the NetSoft conference website at

<https://netsoft2022.ieee-netsoft.org/authors/>

Only PDF files will be accepted for the review process and all manuscripts must be electronically submitted through EDAS: <https://edas.info/newPaper.php?cc=29270&track=109966>

**Important:** Please check NetSoft 2022 publication and no-show policy in the conference website at <https://netsoft2022.ieee-netsoft.org/authors/publication-and-no-show-policy/>.

#### Important dates

Workshop paper submission deadline:	March 21, 2022 (Extended, Firm)
Workshop paper acceptance:	April 21, 2022
Camera-ready papers:	May 5, 2022
Workshop date:	July 1, 2022

#### Workshop Co-Chairs

Fulvio Valenza, Politecnico di Torino, Italy  
Antonio Skarmeta, University of Murcia, Spain  
Matteo Repetto, IMATI-CNR, Italy

#### TPC Co-Chairs

Michal Choras, FernUniversität in Hagen, Germany  
Antonio Lioy, Politecnico di Torino, Italy  
Andrea Saracino, IIT-CNR, Italy

Figure AA-3: Call for Papers of the 4th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft)

## **2nd Workshop on Accountability, Liability and Trust for 5G and Beyond (WALT5G+ 2022), co-located with 1st International Conference on 6G Networking (6GNet 2022)**

### **Program**

Keynote Speech 1:

- Cybersecurity: A collective responsibility and power - Claire Loiseaux, Internet of Trust



### Session 1

- Framework for Trustworthy AI/ML in B5G/6G, Sokratis Barmounakis (WINGS ICT Solutions, Greece), Panagiotis Demestichas (University of Piraeus, Greece)
- Trust Enhanced Security for Routing in SDN, Nurefsan Sertbas Bulbul (Universität Hamburg, Germany), Orhan Ermis (Luxembourg Institute of Science and Technology, Luxembourg & LIST, Luxembourg), Serif Bahtiyar (Istanbul Technical University, Turkey), Mehmet Ufuk Caglayan (Yasar University, Turkey), Fatih Alagoz (Bogazici University, Turkey)

### Session 2

- Level of Trust and Privacy Management in 6G Intent-based Networks for Vertical Scenarios, Jesús A. Alonso-López (Universidad Complutense of Madrid, Spain), Luis Alberto Martínez Hernández (Universidad Complutense of Madrid, Spain), Sandra Pérez Arteaga (Universidad Complutense of Madrid, Spain), Ana Lucila Sandoval Orozco (Universidad Complutense of Madrid, Spain), Luis Javier García Villalba (Universidad Complutense of Madrid, Spain), Antonio Pastor (Telefonica I+D & Universidad Politécnica de Madrid, Spain), Diego Lopez (Telefonica I+D, Spain)
- Modeling the Accountability and Liability Aspects of a 5G Multi-Domain On-Demand Security Services: An Unexpected Journey, Chrystel Gaber (Orange Labs, France), Anser Yacine (Conservatoire National Des Arts Et Métiers (CNAM) Paris & Orange Labs, France)
- Defining the Threat Manufacturer Usage Description Model for Sharing Mitigation Actions, Sara Nieves Matheu García (University of Murcia, Spain), Antonio Fernando Skarmeta Gomez (University of Murcia, Spain)

### Keynote Speech 2

- Towards a Resilient and Trusted 5G & Beyond: Current Challenges and Future Directions - Roberto Cascella, ECSO

### Session 3

- The Impact of Manufacturer Usage Description (MUD) on IoT Security, Zeno Heeb (Zurich University of Applied Sciences, Switzerland), Onur Kalinagac (Zurich University of Applied Sciences, Switzerland), Wissem Soussi (Zurich University of Applied Sciences (ZHAW) & University of Zürich (UZH), Switzerland), Gürkan Gür (Zurich University of Applied Sciences (ZHAW), Switzerland)
- eSIM Adoption: Essential Challenges on Responsibilities Repartition, Chrystel Gaber (Orange Labs, France), Pierrick Kaluza (Orange, France)

### Panel: Liability and Trust in Future Networks for 2030

- Jean-Philippe Wary (moderator), Orange Labs
- Gürkan Gür (speaker), ZHAW
- Chrystel Gaber (speaker), Orange Labs
- Claire Loiseaux (speaker), Internet of Trust
- Roberto Cascella (speaker), ECSO

In the following, the Workshop Call for Papers and pictures taken during the event celebration.



WALT5G+ 2022 Workshop	Patrons	Call for Papers	Posters & Demos
<p><b>Important dates</b></p> <ul style="list-style-type: none"> <li>• Paper Submission Due February 28, 2022 (Firm deadline)</li> <li>• Notification of Acceptance April 22, 2022 (Extended)</li> <li>• Camera-Ready Papers due May 8, 2022 (Extended)</li> <li>• Conference Date July 6 - 8, 2022</li> </ul> <p><b>Technical Sponsors</b></p>    <p><b>Sponsors</b></p>  	<p><b>2nd Workshop on Accountability, Liability and Trust for 5G and Beyond</b></p> <p><b>WALT5G+ 2022</b></p> <p>The 2nd Workshop on Accountability, Liability, and Trust for 5G and Beyond (WALT5G+) will provide an interdisciplinary forum to exchange innovative research ideas, and recent results, and share experiences among researchers and practitioners regarding trust, liability, accountability, and security in communication networks.</p> <p>We solicit papers on all aspects of trust, security assurance, liability, and accountability in future networks related topics such as novel 6G applications, smart networks and services, IoT, mobile devices, edge-cloud continuum, and novel mobile communication techniques. Particular topics of interest include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• <b>Complex system management</b> <ul style="list-style-type: none"> <li>• Trust and liability in 5G infrastructure and its evolution for Beyond 5G systems</li> <li>• Trust and honesty in multi-agent systems</li> <li>• Security and trust metrics</li> <li>• Hardware-based trustworthiness enablers and techniques</li> <li>• Responsibility and accountability in multi-agent systems</li> <li>• Trust and liability for emerging network enablers such as AI/ML and autonomous management in Beyond 5G</li> <li>• Pervasive trust and liability in edge-cloud continuum</li> <li>• Low-complexity trust and liability management for large-scale Beyond 5G systems</li> </ul> </li> <li>• <b>Legal</b> <ul style="list-style-type: none"> <li>• Legal obligations for critical services operation</li> <li>• Legal obligations for providers and customers of network infrastructures and services</li> <li>• Trust and liability in contracts</li> <li>• Ethical issues in trust and liability</li> <li>• Legal implications of cloudification and telco clouds in Beyond 5G networks</li> </ul> </li> <li>• <b>Insurance</b> <ul style="list-style-type: none"> <li>• Risk management and insurance policies for software, network infrastructures and services</li> <li>• Risk management and insurance policies for critical services operation</li> <li>• Risk management and cyber security</li> </ul> </li> </ul> <p>Paper submissions must present original research or analysis. Only original papers that have not been published or submitted for publication elsewhere can be submitted. Each submission must follow the Author Guidelines established for the 6GNet conference.</p> <ul style="list-style-type: none"> <li>• Full Paper – up to 6 pages (11-point font) including tables, figures, and references.</li> <li>• Short Paper – 3 or 4 pages (11-point font) including tables, figures, and references.</li> </ul> <p><b>Submission link:</b> <a href="https://edas.info/N29653">https://edas.info/N29653</a></p> <p><b>Important Dates</b></p> <ul style="list-style-type: none"> <li>• Workshop paper submission: <del>May 25, 2022</del> <b>June 1, 2022 (Firm Deadline)</b></li> <li>• Notification of acceptance: <del>June 8, 2022</del> <b>June 14, 2022</b></li> <li>• Final papers due: <del>June 15, 2022</del> <b>June 20, 2022</b></li> </ul>		

Figure AA-4: Call for Paper of the 2nd Workshop on Accountability, Liability and Trust for 5G and Beyond (WALT5G+ 2022)




## Defining the Threat Manufacturer Usage Description Model for Sharing Mitigation Actions

Sara Nieves Matheu García  
University of Murcia



Figure AA-5: Presentation during the 2nd Workshop on Accountability, Liability and Trust for 5G and Beyond (WALT5G+ 2022)





Figure AA-6: Panel discussion during the 2nd Workshop on Accountability, Liability and Trust for 5G and Beyond (WALT5G+ 2022)

### **Symposium on Security for 5G and Future Networks, co-located with IEEE Future Networks World Forum 2022**

#### **Program**

##### Keynote

- Antonio Skarmeta Gómez, Universidad de Murcia-Spain – “Challenges in Security Management for 6G Networks”

##### Session 1

- Decoupling Statistical Trends from Data Volume on LDP-Based Spatio-Temporal Data Collection, Taisho Sasada (Nara Institute of Science and Technology & Graduate School of Science and Technology, Japan); Yuzo Taenaka and Youki Kadobayashi (Nara Institute of Science and Technology, Japan)
- ETSI ZSM Driven Security Management in Future Networks, Geoffroy Chollon and Dhouha Aayed (Thales, France); Rodrigo Asensio-Garriga, Alejandro Molina Zarca and Antonio Fernando Skarmeta Gomez (University of Murcia, Spain); Maria Christopoulou (NCSR Demokritos, Greece); Wissem Soussi (Zurich University of Applied Sciences (ZHAW) & University of Zürich (UZH), Switzerland); Gürkan Gür (Zurich University of Applied Sciences (ZHAW), Switzerland); Uwe Herzog (Eurescom, Germany)
- Deployment of 5G Network Applications over Multidomain and Dynamic Platforms, Ana Hermosilla (Odin Solutions SL, Spain); Jorge Gallego-Madrid (University of Murcia & Odin Solutions, Spain); Pedro Martinez-Julia and Ved P. Kafle (National Institute of Information and Communications Technology, Japan); Kostis Trantzas and Christos Tranoris (University of Patras, Greece); Rafael Direito and Diogo Gomes (Universidade de Aveiro & Instituto de Telecomunicações, Portugal); Jordi Ortiz (University Defense Center, (CUD), Spanish Air Force Academy, MDE-UPCT, Spain & University of Murcia, Spain); Spyros Denazis (University of Patras, Greece); Antonio F. Skarmeta (Odin Solutions S. L, Spain)

##### Session 2

- A Learning-Based Zero-Trust Architecture for 6G and Future Networks, Michael A. Enright (Quantum Dimension, Inc., USA); Eman Hammad (University of Toronto, Canada); Ashutosh



Dutta (Johns Hopkins University Applied Physics Labs (JHU/APL), USA)

- Federated machine learning through edge ready architectures with privacy preservation as a service, Konstantinos A Koutsopoulos (Qualtek Sprl., Greece); Anastasios Gavras (Eurescom GmbH, Germany); Stefan Covaci and Benjamin Ertl (Agentscape AG, Germany); Spyridon Tompros (Qualtek SPRL, Belgium); Antoine Simon (University of Rennes 1, France); Gouenou Coatricieux (IMT Atlantique, France); Katarzyna Kapusta (Thales SIX, France)
- SliceSecure: Impact and Detection of DoS/DDoS Attacks on 5G Network Slices, Md Sajid Khan, Behnam Farzaneh and Nashid Shahriar (University of Regina, Canada); Niloy Saha and Raouf Boutaba (University of Waterloo, Canada) // Remote
- Impact of Man-in-the-Middle Attacks to the O-RAN Inter-Controllers Interface, Walter Tiberti, Eleonora Di Fina, Andrea Marotta and Dajana Cassioli (University of L'Aquila, Italy)

In the following, the Symposium Call for Papers and pictures taken during the event celebration.



**Call for Papers**  
**SYMPOSIUM ON SECURITY FOR 5G AND FUTURE NETWORKS**

**SYMPOSIUM CO-CHAIRS**

Antonio Skarmeta, Universidad de Murcia, Spain, [skarmeta@um.es](mailto:skarmeta@um.es)  
Pascal Bisson, Thales, France, [pascal.bisson@thalesgroup.com](mailto:pascal.bisson@thalesgroup.com)  
Ved P. Kuffe, National Institute of Information & Communications Technology, Japan, [kuffe@nict.go.jp](mailto:kuffe@nict.go.jp)  
Chamseddine Talhi, École de technologie supérieure, Canada, [Chamseddine.Talhi@etsmtl.ca](mailto:Chamseddine.Talhi@etsmtl.ca)

**SCOPE AND MOTIVATION**

The 5G long term vision is to "turn the network into an energy-efficient distributed computer system that enables agile and dynamic creation, move and suppression of processes and services in response to changing customer demands and information flows, and that supports interaction with humans through new communication modes, such as gestures, facial expressions, sound, and haptics. To make this vision a reality, a shift towards a full automation of network and service management and operation is a necessity. However, a major challenge facing full automation is the protection of the network and system assets (i.e., services, data and network infrastructure) against potential cybersecurity risks introduced by the unprecedented evolving 5G threat landscape. Indeed, the risk of full automation is the ability to replicate a small isolated error or attack broadly and rapidly, putting the entire critical ecosystem (multi-party/tenant/technologies) into peril.

Although 5G and beyond-5G offer a multitude of benefits to the emerging applications, they are susceptible to the malicious or inadvertent introductions of vulnerabilities, such as malicious software or hardware, counterfeit components, and poor designs. Even worse, these new technologies are facing a series of inherent security and privacy threats, which intensify the vulnerabilities of the 5G networks. In addition, vastly increased numbers of devices and an elevated use of virtualization result in more 5G security threats and a broader, multifaceted attack surface. To realize strong and healthy communication networks, exploring the approaches to address the security and privacy threats are vital for both industry and academia. To address the aforementioned challenges in beyond 5G or 6G telecommunication infrastructure and services, the inherent support of full automation operations in

network and service management is a necessity. One of the most critical areas of application for zero touch automation is the protection of the network and system assets against potential cybersecurity risks introduced by the unprecedented evolution of the 5G threat landscape.

Our aim is to promote the development of 5G security by design.

**TOPICS OF INTEREST**

We invite submissions on a wide range of research topics, spanning both theoretical and systems research, including results from industry and academic/industrial collaborations, related but not restricted to the following topics:

- 5G and Beyond architecture with security and privacy considerations
- Security for new service delivery models
- AI and Machine Learning for 5G and Beyond security
- Verticals and business (non-technical) 5G and Beyond security requirements and solutions
- Big data analytics tools and techniques in 5G and Beyond Security
- Advances in lightweight cryptography and IoT security
- Wireless virtualization and slicing security
- Authentication, authorization, and accounting (AAA) for 5G and Beyond security
- Diameter security in 5G and Beyond
- Tera-Hertz communication and security for 5G and Beyond
- Millimeter wave and security for 5G and Beyond
- Quantum Safe Cryptography for 5G and Beyond
- Secure Integration of IoT and Cloud Computing
- Secure Device-to-Device communications in 5G and Beyond
- Secure integration of IoT and other networks
- Intrusion Detection/Prevention Techniques and System Integrity
- Secure data storage, communications and computing
- Energy efficient security in IoT
- Heterogeneous system modeling
- for 5G and Beyond security
- Secure sensing and computing techniques in 5G and Beyond
- Big data analytics for 5G and Beyond security
- Secure, privacy-aware and trustworthy IoT communications
- Trust models and trust handling/propagation for 5G and Beyond security
- Physical layer security for 5G and Beyond
- 5G and Beyond security standardization
- Privacy-preserving Machine Learning or Deep Learning in 5G and Beyond
- Adversarial Machine Learning or Deep Learning in 5G and Beyond
- Trustworthiness and Fairness in Artificial Intelligence for 5G and Beyond
- Security and Privacy for Blockchain Technology in 5G and Beyond
- Security and Privacy for Data-centric Networks in 5G and Beyond
- Security and Privacy for Fog Computing in 5G and Beyond
- Security and Privacy for Software-Defined Networks
- Security and Privacy for Network Function Virtualization
- Security and Privacy for Drone Communications in 5G and Beyond

**IMPORTANT DATES**

Paper Submission: **15 May 2022**  
Notification: 30 July 2022  
Camera Ready and Registration: 30 August 2022

**HOW TO SUBMIT A PAPER**

All papers for technical symposia should be submitted via [EDAS](https://fnwf.ieee.org/). Full instructions on how to submit papers are provided on the IEEE FNWF 2022: <https://fnwf.ieee.org/>



Figure AA-7: Call for Papers of the Symposium on Security for 5G and Future Networks





Figure AA-8: Keynote speech at the Symposium on Security for 5G and Future Networks

### **Industrial Forum From 5G to 6G Smart Security Solutions, co-located with IEEE Future Networks World Forum 2022**

#### **Program**

Moderator: Antonio Skarmeta, University of Murcia, Spain

#### **Invited Speakers**

- Xavier Costa-Pérez, ICREA Research Professor, Scientific Director at the i2cat Research Center and Head of 5G/6G Networks R&D at NEC Laboratories Europe, “5G Security Review and Future 6G Challenges”
- Carol Fung, Associate Professor at Concordia University Canada and Gina Cody Research Chair in Cybersecurity and the Internet of Things, “Cybersecurity Challenges in 5G Networks”
- Eman Hammad, Texas A&M, “Cybersecurity and Emerging Technologies: Leveling the Field”

#### **Round Table**

- Xavier Costa-Pérez, ICREA Research Professor, Scientific Director at the i2cat Research Center and Head of 5G/6G Networks R&D at NEC Laboratories Europe
- Carol Fung, Associate Professor at Concordia University Canada and Gina Cody Research Chair in Cybersecurity and the Internet of Things
- Eman Hammad, Texas A&M



- Ved Kafle (NICT Japan)
- Chamseddine Talhi (École de technologie supérieure, Canada)

In the following, some pictures taken during the event celebration.



Figure AA-9: Presentation of the Industrial Forum From 5G to 6G Smart Security Solutions



Figure AA-10: Audience of the Industrial Forum From 5G to 6G Smart Security Solutions



## Appendix B INSPIRE-5Gplus project flyer

### Key Targets

INSPIRE-5Gplus makes a revolutionary shift in the 5G and Beyond security vision by progressing 5G security and by devising a smart, trustworthy and liability-aware 5G end-to-end security platform for future connected systems.

INSPIRE-5Gplus will allow the advancement of the security vision for 5G and beyond through the adoption of a set of emerging trends and technologies:

- Zero-touch security management
- Software-defined security and trust models
- Smart end-to-end security orchestration through Artificial Intelligence
- Liable and trusted security management

INSPIRE-5Gplus will ensure that the provided security level is in conformance with security requirements by legislation, standards, and verticals. Trust and liability will be fostered through integration of novel mechanisms supporting confidence between parties and compliance with regulation:

- Trust and Reputation Manager: assigns trust and reputation values to monitored entities
- Service Trust Manager: implements smart-contracts calculating trust and reliability of a cloud infrastructure or its services
- End-to-End Trust Management: provides cross-domain versions of trust functions



Project coordinator: Uwe Herzog (Eurescom, Germany)  
Technical Coordinator: Dhouha Ayed (Thales, France)

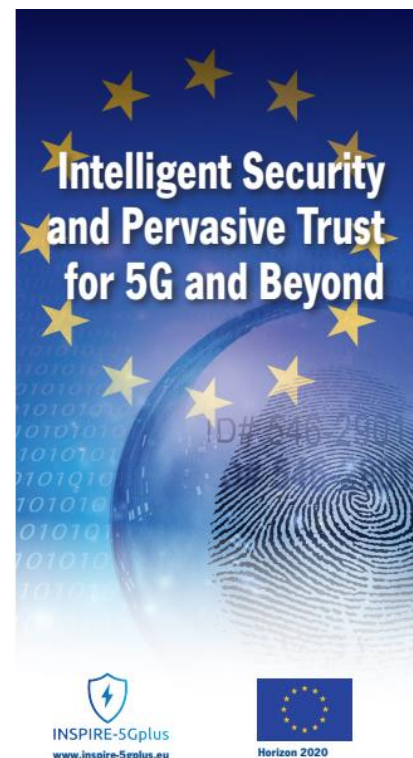
www.inspire-5gplus.eu

Twitter: @Inspire-5Gplus

www.linkedin.com/in/project-inspire-5gplus-0871961a4/



INSPIRE-5Gplus has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement no. 871808.



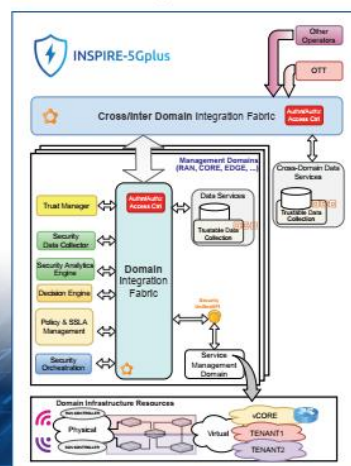
### Test Cases

Test Case (TC)	High-Level Architecture Category						
	Size Management	SSLA Manager	Security Orchestrator	Security Analytics	Security Function	Security Enforcement	Security Measurement
TC1: Secured Anticipated Cooperative Collision Avoidance	*	*	*				
TC2: Definition and Assessment of Security and Service Level Agreements and Automated Remediation		*	*				*
TC3: Attack Detection over Encrypted Traffic			*				*
TC4: E2E Encryption TEE secured SECaaS	*	*	*	*	*	*	*
TC5: End-to-End Slice Protection based on Moving Target Defense and Anomaly Detection			*				*
TC6: GDPR-Aware Counterparts for Cross-Border Movement	*	*	*	*	*	*	*
TC7: Intelligent and Secure Management of Shared Resources to Prevent (D)DoS	*	*	*	*	*	*	*
TC8: Security Posture Assessment and Threat Visualization of 5G Networks							*
TC9: Secure and Privacy Enabled Local 5G Infrastructure	*						

### High-Level Architecture

The INSPIRE-5Gplus architecture is designed to support fully automated end-to-end network and service security management in multi-domain 5G environments. The architecture empowers protection, trustworthiness, and liability in managing virtualized network infrastructures across multi-domains: radio, edge, and core segments.

Each Security Management Domain (SMD) is responsible for intelligent security automation of resources and services within its scope. INSPIRE-5Gplus' end-to-end SMD manages security of services that span multiple domains such as end-to-end slicing. Each SMDs comprises a set of functional modules, e.g. security intelligence engine, security orchestrator, and trust manager, that operate in an intelligent closed-loop way to enable software defined security orchestration.



### Main Results

- A comprehensive report on the current security landscape of 5G networks and the foreseen evolution trends of this landscape, either regarding security threats or security requirements.
- Intelligent and autonomic end-to-end cybersecurity architecture that can detect and mitigate both existing and new threats targeting 5G networks.
- Evolved and new security assets taking advantage of artificial intelligence and state-of-the-art techniques with a focus on trust and liability across 5G infrastructure and services.
- An integration and experimentation framework, with the objective of validating the project's developments in nine specific 5G security test cases.

#### INSPIRE-5Gplus at a Glance

Horizon 2020 Work Programme Topic:  
ICT-20-2019-2020: 5G Long Term Evolution

Start Date:  
1 November 2019 End Date: 31 October 2022

Consortium:  
14 partners from 8 countries

Figure AB-1: INSPIRE-5Gplus flyer





## Appendix C ETSI ZSM PoC #6 - Demo Poster

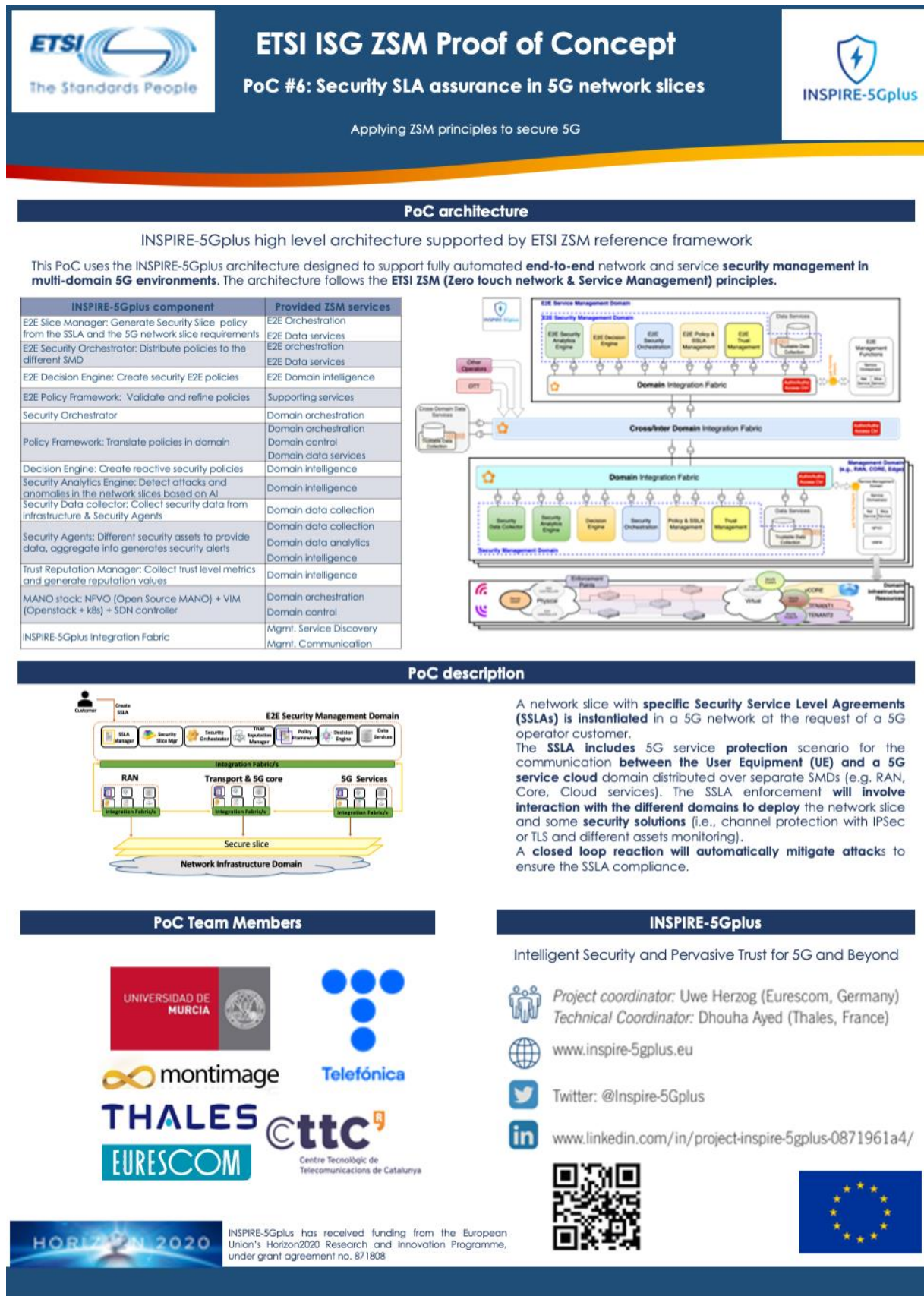


Figure AC-1: ETSI TSG ZSM INSPIRE-5Gplus' PoC poster