

# InSecTT: Intelligent Secure Trustable Things



## Final Report on Communication, Exploitation and Dissemination of Results

<b>Document Type</b>	Deliverable
<b>Document Number</b>	D6.7
<b>Primary Author(s)</b>	Peter Priller   AVL
<b>Document Version / Status</b>	1.0   Final
<b>Distribution Level</b>	CO (confidential – consortium only)

---

<b>Project Acronym</b>	InSecTT
<b>Project Title</b>	Intelligent Secure Trustable Things
<b>Project Website</b>	<a href="https://www.insectt.eu/">https://www.insectt.eu/</a>
<b>Project Coordinator</b>	Michael Karner   VIF   <a href="mailto:michael.karner@v2c2.at">michael.karner@v2c2.at</a>
<b>JU Grant Agreement Number</b>	876038
<b>Date of latest version of Annex I against which the assessment will be made</b>	2023-05-24



## CONTRIBUTORS

Name	Organization	Name	Organization
Peter Priller	AVL		

## FORMAL REVIEWERS

Name	Organization	Date
Łukasz Szczygielski	GUT	2023-09-08
Michael Karner	ViF	2023-09-28

## DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
0.5	2023-08-03	Peter Priller/AVL	Initial version
0.7	2023-08-04	Peter Priller/AVL	Exploitation added
1.0	2023-08-04	Peter Priller/AVL	finalized

# TABLE OF CONTENTS

<b>1</b>	<b>EXECUTIVE SUMMARY</b>	<b>6</b>
<b>2</b>	<b>OBJECTIVES</b>	<b>7</b>
2.1	Project-wide Objectives	7
2.2	WP6 specific Objectives	8
2.3	Stakeholders, Target Groups	8
<b>3</b>	<b>DESCRIPTION OF WORK</b>	<b>9</b>
3.1	Report of InSecTT communication activities in Y3	9
3.1.1	InSecTT Web Site	9
3.1.2	Search machine ranking of InSecTT	13
3.1.3	Project-Internal Communication: InSecTT SharePoint	14
3.1.4	InSecTT Social Media activities	15
3.1.5	InSecTT Newsletter	18
3.1.6	InSecTT Podcast	19
3.2	Report of InSecTT dissemination activities in Y3	22
3.2.1	Public deliverable, summarizing WP2 and WP3 technology results	22
3.2.2	Publications in InSecTT	23
3.2.3	Other Dissemination Activities (Conferences, Events, Press Release)	29
3.2.4	Participation and Booth at the EF ECS 2022	38
3.2.5	Development of InSecTT Open Innovation Framework	39
3.3	Report of InSecTT Exploitation Activities in Y3	41
3.3.1	InSecTT Exploitation Board	41
3.3.2	Project Liaisons	44
3.3.3	Report on Patents	44
3.3.4	Report of Exploitable Foreground	45
3.4	Evaluation of performance indicators and suggested improvements	49
3.4.1	Suggestions for Improvements in Y3	51
3.5	The InSecTT Book: Intelligent Secure Trustable Things	51
<b>4</b>	<b>CONCLUSIONS</b>	<b>55</b>
<b>5</b>	<b>REFERENCES</b>	<b>56</b>
<b>A.</b>	<b>ABBREVIATIONS AND DEFINITIONS</b>	<b>57</b>

## LIST OF FIGURES

Figure 1 Screen Shot of the InSecTT website (2023-08-03) .....	9
Figure 2 Audience Overview for the InSecTT web presence.....	10
Figure 3 Most visited pages on InSecTT's web presence in Y3 .....	10
Figure 4 Origin of Website users of the InSecTT web presence .....	11
Figure 5 User Flow on the InSecTT web presence.....	12
Figure 6 Website user's devices accessing the InSecTT web presence .....	12
Figure 7 Screen Shot of the InSecTT SharePoint site [2023-08-03].....	14
Figure 8 Project SharePoint usage analytics .....	15
Figure 9 Instagram Statistics Y3 .....	17
Figure 10 Twitter Followers Y3 .....	17
Figure 11 Twitter Impressions Y3 .....	18
Figure 12 Q1-2023 Issue of the InSecTT Newsletter.....	19
Figure 13 InSecTT Podcasts (retrieved 2023-08-03).....	21
Figure 14 Podcast download statistics August 2022 – August 2023 .....	21
Figure 15 WP2 sub-building blocks BB2.1 – BB2.5.....	22
Figure 16 WP3 sub-building blocks BB3.1 – BB235.....	23
Figure 17 InSecTT booth at the EF ECS 2022, 24.-25. November .....	39
Figure 18: Closed Innovation vs. Open Innovation .....	40
Figure 19: A graphical description of the Open Innovation Contest developed during InSecTT project for maximizing exploitation results .....	40
Figure 20: Fotos from two OIC events (InSecTT F2F and Interizon ICT) .....	41
Figure 21 Logo of project EREATOSTHENES .....	44
Figure 22 Logo of project DAIS.....	44
Figure 23 Logo of project AI-NET-ANIARA.....	44

## LIST OF TABLES

Table 1 Objectives from PCEDR (D6.1) .....	8
Table 2 Search engine ranking (per 2023-08-03) .....	14
Table 3 Social Network Channels used by InSecTT (per 2023-08-03).....	16
Table 4 Publications in InSecTT during Y3 as of 2023-08-03.....	29
Table 5 Dissemination Activities in Y3 per 2023-08-03 .....	38
Table 6 EB members during Y3.....	43
Table 7 Patents reported as of 2023-08-04 .....	45
Table 8 Exploitable Foreground reported by 2023-08-04 .....	49
Table 9 KPI Overview and Y3 Evaluation .....	50
Table 10 Summary of suggested improvement actions in InSecTT for Y3.....	51
Table 11 Main structure (chapter, subchapters) of the InSecTT Book .....	54

# 1 EXECUTIVE SUMMARY

This deliverable is the last document in a row, reporting activities and impact from Communication, Exploitation and Dissemination of Results (PCEDR) of project InSecTT. While the first one (D6.1, [1]) outlined the plan, the following ones reported yearly progress, discussed results so far and suggest corrective actions where needed.

This document reports on **results achieved in Y3**, building upon (and not just aggregating) the previous Y1 and Y2 reports. It provides an overview of InSecTT's communication, dissemination, and exploitation activities during Y3 (M25-M39), and analyses impact along different types and channels (e.g. social networks, publications, events etc.). If applicable, performance indicators (numbers, impact...) are measured and compared against the plan described in D6.1. By these means progress is validated and verified.

In order to further foster exploitation, and to support especially SME's in the consortium, the **Exploitation Board** (EB) has been active since the beginning of the project. The EB helps and advises partners in exploitation.

Partners in InSecTT have been working hard not only in research and development, but also in communicating and disseminating and exploiting the results. InSecTT was very successful regarding scientific dissemination with **70 publications** in Y3 (in addition to the 50 reported in Y2 and another 38 reported in Y1), as shown in Table 4, including technical papers, journal articles and master thesis, which also led to many presentations.

In addition, two public deliverables provide a summary of the technologies developed:

- D2.4, Publishable Summary of WP2 Results, 100 pages
- D3.4, Publishable Summary of WP3 Results, 100 pages

Regarding its public appearance, an appealing website attracts continuous views per month, and multiple social network channels have been continuously reporting news.

All these activities have resulted in top search-engine ranking, see 3.1.2.

The impact of these Internet presences is continuously monitored and maintained through the project.

Consortium members have reported in total 4 patent applications from the project, which indicates strong and dedicated exploitation efforts. This is supported by identification of **25 exploitable** items within the project results.

Finally, the consortium is proud to report on its upcoming book "Intelligent Secure Trustable Things", see section 3.5

Keywords: PECDR, dissemination, exploitation, social network channels

## 2 OBJECTIVES

An important aspect of research is to communicate its existence, its progress and especially its results to the intended target groups. Naturally, this faces challenges like (i) efficient soliciting and collecting information in a large and heterogeneous team of a cross-European project, (ii) finding suitable channels for communication, and (iii) processing and transforming information to draw the interest of target groups, while honoring the interests and potential confidentially aspects of project partners. InSecTT is set up so that most dissemination and exploitation is done directly by the partners. Task T6.1 (Dissemination and Exploitation) supports such activities, by creating opportunities, networking, counselling partners etc.

As an example, the project managed InSecTT-themed workshops at conferences, like the one at the IEEE WF-IoT 2021 conference and another at the MIKON-2022 conference in Gdansk.

Supporting exploitation of project results is supported in multiple ways, with a dedicated group (the exploitation board, EB) providing networking and advisory and organizing exploitation events, see 3.3.

In addition, project-wide communication is done by WP1 (Project Management) together with WP6. A highlight of the activities in WP6 and throughout the project Y3 is certainly the InSecTT book, see 3.5.

In addition, two public deliverables provide a summary of the technologies developed:

- D2.4, Publishable Summary of WP2 Results, 100 pages
- D3.4, Publishable Summary of WP3 Results, 100 pages

See section 3.2.1

### 2.1 Project-wide Objectives

Of the main objectives defined in the project proposal [3], the most important objectives of the InSecTT dissemination and communication activities are:

- Building project awareness
- Informing and educating the community on the topical area of AI, safety and security, privacy and trust in IoT
- Contributing to and delivering valuable educational and training content
- Engaging the community to get input / feedback
- Promoting and sharing of outputs and results to the community
- Helping partners to provide open access to publications
- Maximizing the impact of research
- Transferring of knowledge and results to entities that can make the best use of project results

## 2.2 WP6 specific Objectives

In the original PCEDR D6.1 [1], the following objectives were defined

Objective	Text	Final Status
1	Design and setup of the public project website	fully operational, continuously updated
2	Setup and maintain a project repository for all partners (SharePoint), see also chapter 3.1.3	Implemented, fully operational
3	Help partners to develop and maintain exploitation plans	T6.1 and EB sessions at InSecTT consortium meetings; EB external events
4	Publish project results in conference papers, journals, and articles	Done by many partners, see high numbers of publications

**Table 1 Objectives from PCEDR (D6.1)**

## 2.3 Stakeholders, Target Groups

As defined in [3], InSecTT results and deliverables are to be disseminated on both European and national level to the following audiences:

- Specific “external audiences” such as relevant target groups / institutions / organizations, other projects, as well as individuals
- InSecTT project Partners – academic / R&D / Industry organizations
- Other related EU / national projects / project participants
- Industry & Business Associations
- Academic communities and other interest groups, in particular in the InSecTT domains: railway, smart infrastructure, maritime, manufacturing, health, building, urban public transport, automotive, aeronautics
- Domain-specific forums and exchange groups
- Applied researchers in industry
- Researchers / Experts from the field of policy, science, and industry
- Students (PhD or Master thesis)
- Public authorities involved (incl. National Funding Authorities, KDT, EPOSS, INSIDE, ....)
- European Union / European Commission
- Standardization organizations (industry, national, international)
- Regional, national, and international media



### 3 DESCRIPTION OF WORK

#### 3.1 Report of InSecTT communication activities in Y3

##### 3.1.1 InSecTT Web Site

The official InSecTT project website <https://www.insectt.eu/> is maintained by project coordinator VIF.

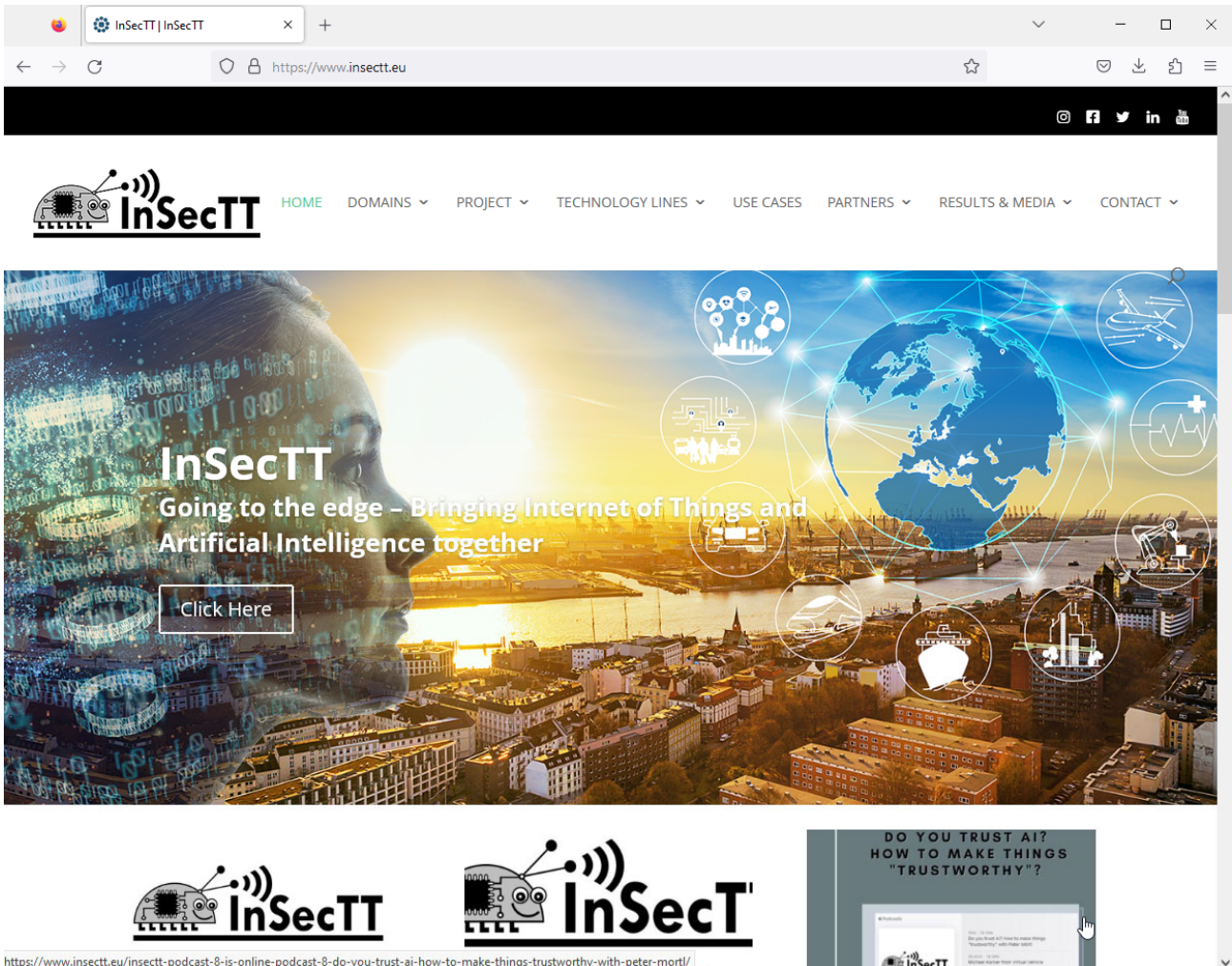


Figure 1 Screen Shot of the InSecTT website (2023-08-03)

Performance indicators of <https://www.insectt.eu/> as reported by Google Analytics tools show a continuous stream of visitors, with a total of about 5500 page views between 1.7.2022 and 1.7.2023 see Figure 2.

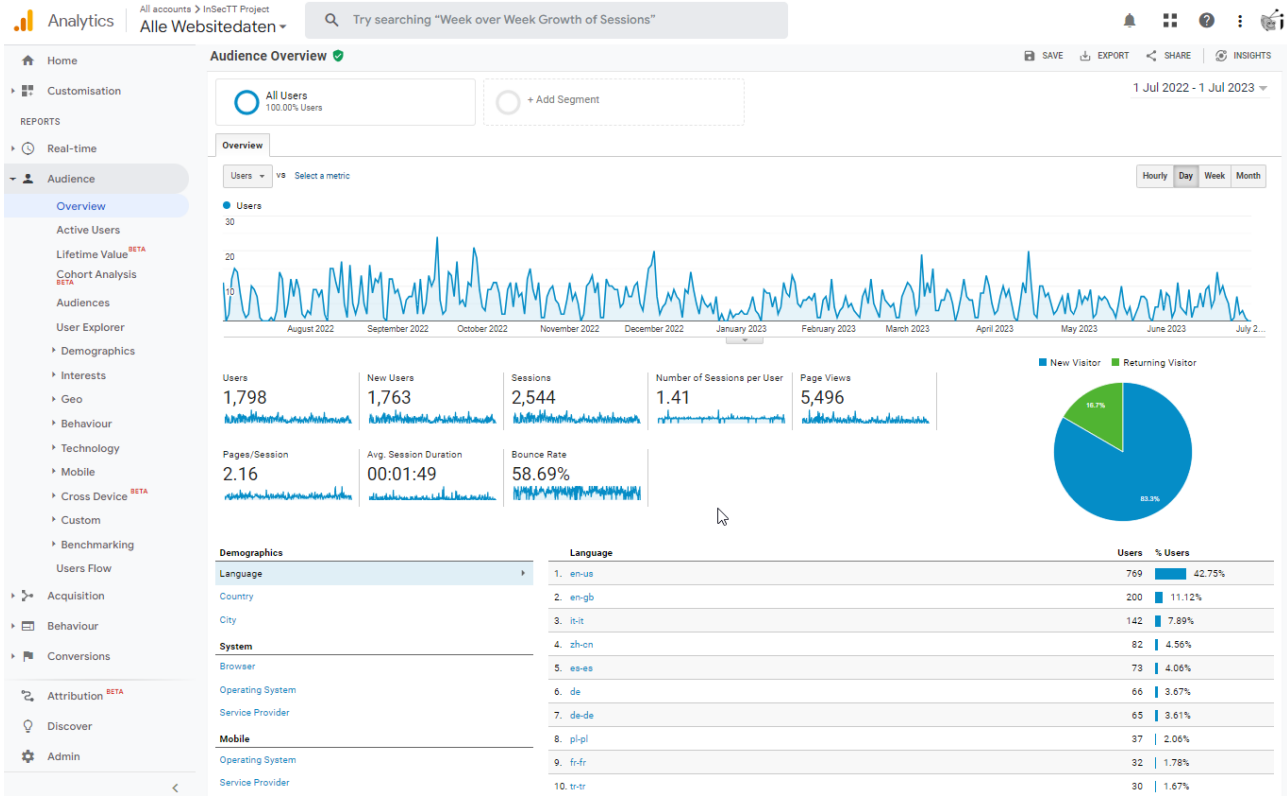
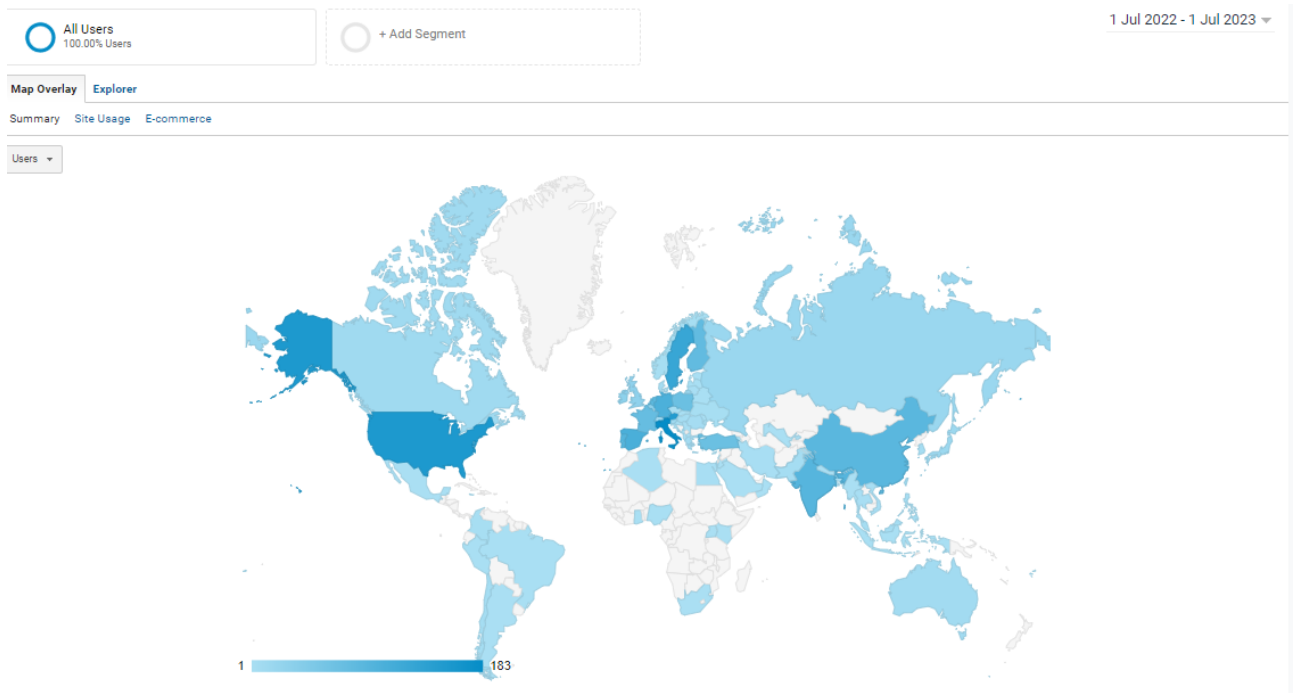


Figure 2 Audience Overview for the InSecTT web presence

Page	Page Views	% of Total (5,496)
1. /	2,506	45.60%
2. /project-overview/general-overview-concept-2/	357	6.50%
3. /partners/	348	6.33%
4. /project-overview/	334	6.08%
5. /use-cases/	238	4.33%
6. /publications/	135	2.46%
7. /related-projects/	114	2.07%
8. /project-overview/key-elements/	100	1.82%
9. /contact/	99	1.80%
10. /deliverables/	78	1.42%

Figure 3 Most visited pages on InSecTT's web presence in Y3



Country ?	Acquisition			Behaviour		
	Users ? ↓	New Users ?	Sessions ?	Bounce Rate ?	Pages/Session ?	Avg. Session Duration ?
	<b>1,798</b> % of Total: 100.00% (1,798)	<b>1,763</b> % of Total: 100.00% (1,763)	<b>2,544</b> % of Total: 100.00% (2,544)	<b>58.69%</b> Avg for View: 58.69% (0.00%)	<b>2.16</b> Avg for View: 2.16 (0.00%)	<b>00:01:49</b> Avg for View: 00:01:49 (0.00%)
1.  Italy	183 (9.97%)	177 (10.04%)	230 (9.04%)	52.17%	2.15	00:01:36
2.  United States	156 (8.50%)	153 (8.68%)	160 (6.29%)	85.00%	1.48	00:00:42
3.  Austria	151 (8.23%)	141 (8.00%)	268 (10.53%)	52.24%	2.49	00:03:24
4.  Sweden	127 (6.92%)	121 (6.86%)	247 (9.71%)	54.66%	2.38	00:02:12
5.  Spain	107 (5.83%)	102 (5.79%)	151 (5.94%)	42.38%	2.79	00:02:51
6.  Germany	105 (5.72%)	102 (5.79%)	142 (5.58%)	54.93%	2.42	00:03:03
7.  Portugal	95 (5.18%)	89 (5.05%)	143 (5.62%)	53.85%	2.21	00:01:49
8.  India	94 (5.12%)	94 (5.33%)	99 (3.89%)	69.70%	1.71	00:01:22
9.  China	89 (4.85%)	88 (4.99%)	92 (3.62%)	97.83%	1.07	00:00:09
10.  Netherlands	88 (4.80%)	84 (4.76%)	113 (4.44%)	52.21%	2.56	00:00:59

Figure 4 Origin of Website users of the InSecTT web presence

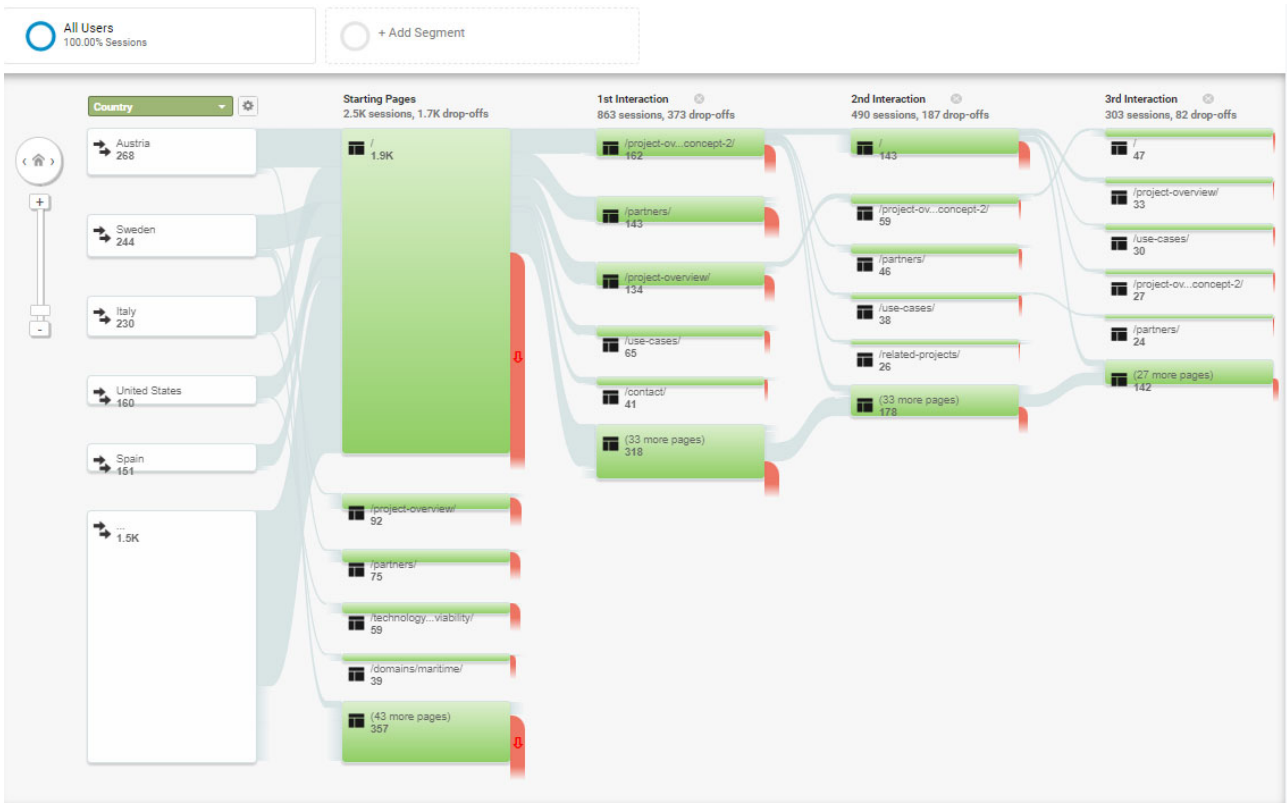


Figure 5 User Flow on the InSecTT web presence

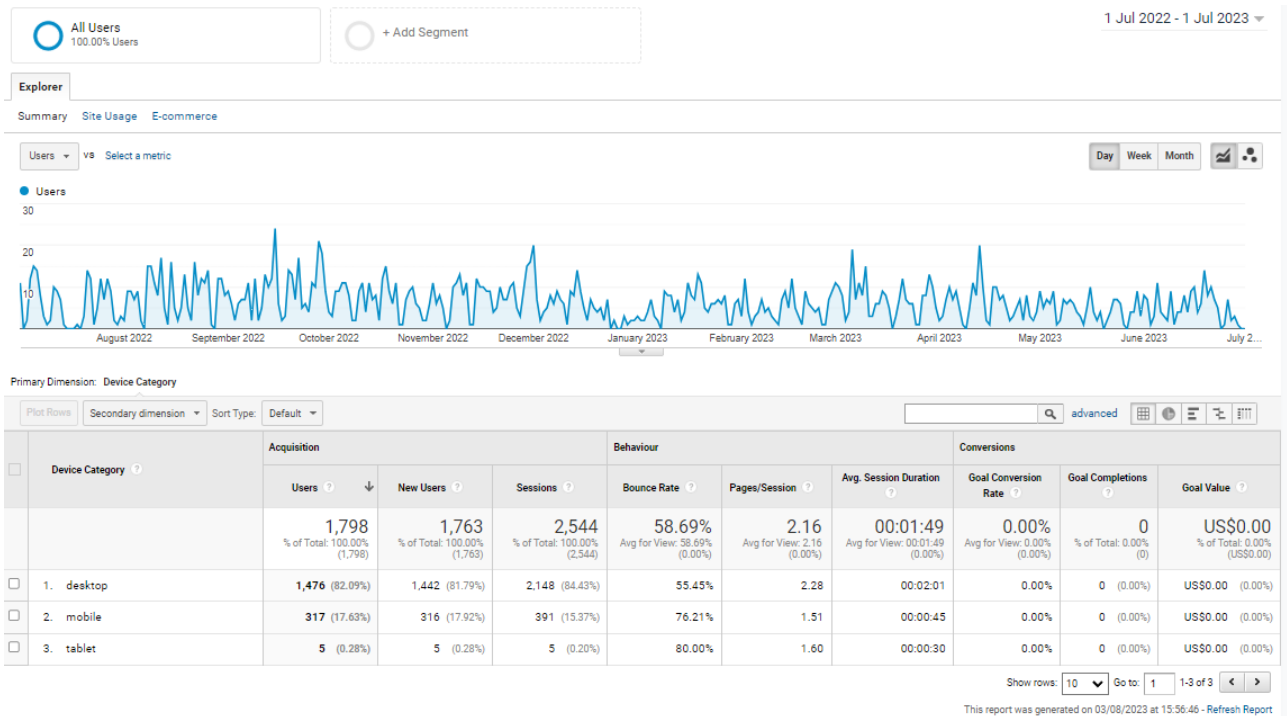


Figure 6 Website user's devices accessing the InSecTT web presence

### 3.1.2 Search machine ranking of InSecTT

Using the following three search engines in a private session (non-personalized) in Firefox on 2023-08-03 resulted in rankings reported in Table 2 for typical search strings relating to InSecTT (as defined in the original PCEDR):

1. [www.google.at](http://www.google.at)
2. <https://www.qwant.com/>
3. <http://www.baidu.com>

As can be seen, the phrases defined got **ranked high (often even as #1)** in most cases.

Visibility in the **Chinese speaking community (using Baidu)** has grosso modo improved since Y1 and Y2 (especially for finding the project name InSecTT itself).

Note: the string “trustworthiness framework” from [1] was too ambiguous, and therefore had to be extended to “intelligent secure trustworthiness framework”

String	First relevant Ranking Google: www.google.com	First relevant Ranking Qwant:	First relevant Ranking Baidu
InSecTT	KPI# 1.1a Target: 1 <sup>st</sup> <b>Actual: 1</b> <a href="https://www.insectt.eu/">https://www.insectt.eu/</a>	KPI# 1.1b Target: 1 <sup>st</sup> <b>Actual: 1</b> <a href="https://www.insectt.eu/">https://www.insectt.eu/</a>	KPI# 1.1c Target: 1 <sup>st</sup> <b>Actual: 8</b> <a href="https://www.insectt.eu/">https://www.insectt.eu/</a>
Intelligent Secure Trustable Things	KPI# 1.2a Target: 1 <sup>st</sup> <b>Actual: 1</b> <a href="https://www.insectt.eu/">https://www.insectt.eu/</a>	KPI# 1.2b Target: 1 <sup>st</sup> <b>Actual: 1</b> <a href="https://insectt.mind-net.org/">https://insectt.mind-net.org/</a>	KPI# 1.2c Target: 1 <sup>st</sup> <b>Actual: 3</b> <a href="https://www.insectt.eu/">https://www.insectt.eu/</a>
intelligent secure trustworthiness framework	KPI# 1.3a Target: 10 <sup>th</sup> <b>Actual 11</b> <a href="https://www.insectt.eu/wp-content/uploads/2022/11/Trustworthiness-Whitepaper-InSecTT-Format-v02-1-1.pdf">https://www.insectt.eu/wp-content/uploads/2022/11/Trustworthiness-Whitepaper-InSecTT-Format-v02-1-1.pdf</a>	KPI# 1.3b Target: 10 <sup>th</sup> <b>Actual: not within first 20</b>	KPI# 1.3c Target: 10 <sup>th</sup> <b>Actual: not within first 20</b>

String	First relevant Ranking Google: <a href="http://www.google.com">www.google.com</a>	First relevant Ranking Qwant:	First relevant Ranking Baidu
intelligent secure trustworthy systems	KPI# 1.4a Target: 10 <sup>th</sup> <b>Actual 1</b> <a href="https://www.insectt.eu">https://www.insectt.eu</a>	KPI# 1.4b Target: 10 <sup>th</sup> <b>Actual: 1</b> <a href="https://www.insectt.eu">https://www.insectt.eu</a>	KPI# 1.4c Target: 10 <sup>th</sup> <b>Actual: 10</b> <a href="https://www.insectt.eu/">https://www.insectt.eu/</a>

Table 2 Search engine ranking (per 2023-08-03)

### 3.1.3 Project-Internal Communication: InSecTT SharePoint

The collaboration platform used in InSecTT is hosted by VIF on SharePoint: <https://v2c2.sharepoint.com/sites/InSecTT/>

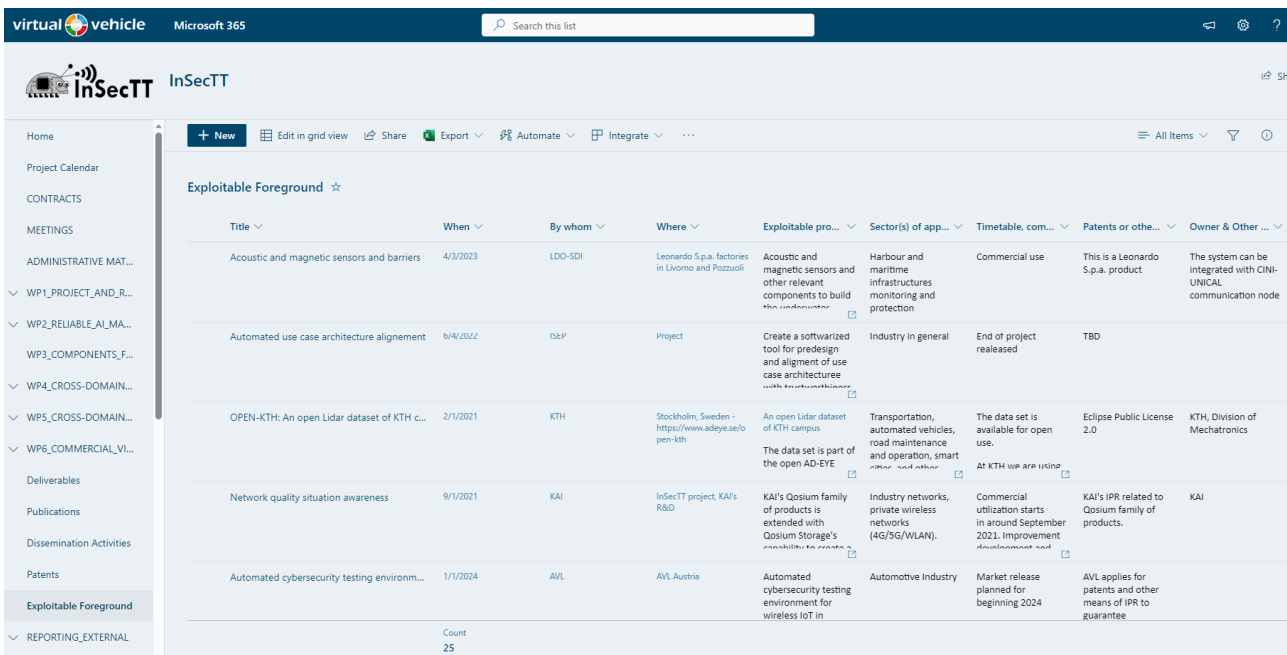


Figure 7 Screen Shot of the InSecTT SharePoint site [2023-08-03]

The SharePoint site is used as internal repository and for hosting project-internal information (e.g., activities, meeting schedules, deliverables etc.).

The site usage statistics for the last 90 days (invoked on 2023-08-03) indicates 372 unique users (project members) and 14800 site visits, which results in an average of 164 visits per day, see Figure 8.

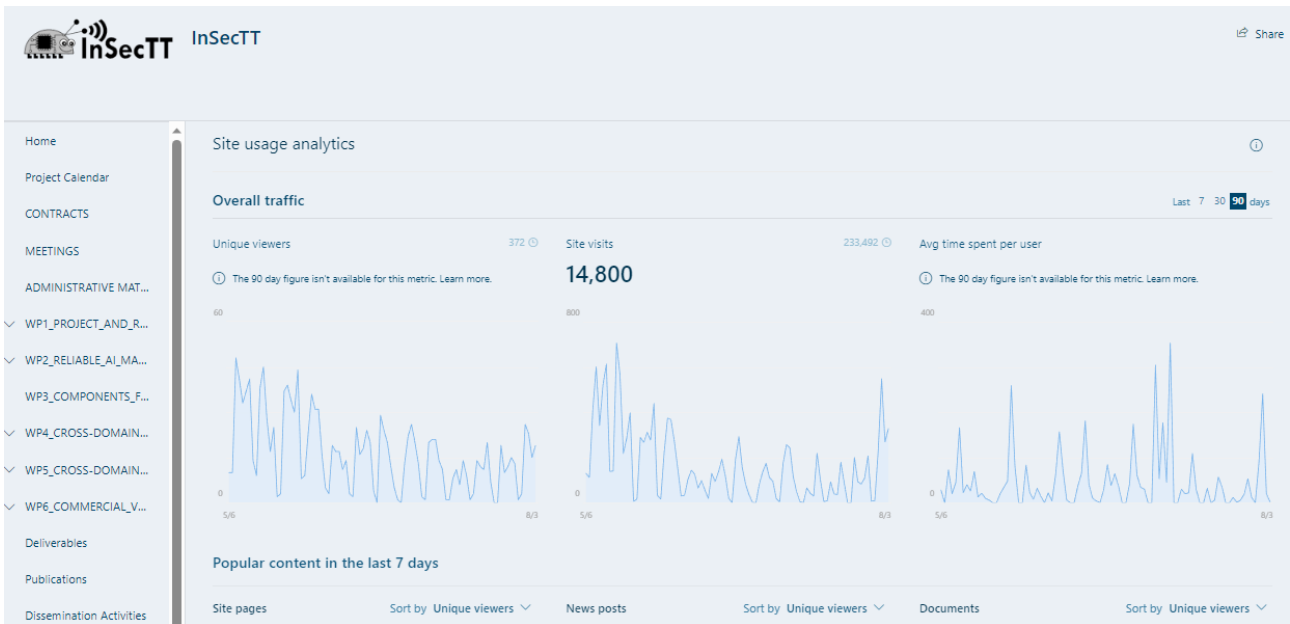




Figure 8 Project SharePoint usage analytics





### 3.1.4 InSecTT Social Media activities

InSecTT is highly active on multiple social network channels listed in Table 3, to promote the project and its results to a broad spectrum of potential stakeholders and interested citizens.

As of 2023-08-03, **more than 284 postings** (in total) have been published, each to multiple channels.

Social Network Channel	Link	Indicators [2023-08-03]
<b>LinkedIn</b> 	<a href="https://www.linkedin.com/in/eu-project-insectt-264294227/">https://www.linkedin.com/in/eu-project-insectt-264294227/</a>	286 Member (compared to 111 in July 2022, and 88 in July 2021)
<b>Facebook</b> 	<a href="https://www.facebook.com/Insectt-Project-105974577981213">https://www.facebook.com/Insectt-Project-105974577981213</a>	117 Follower (compared to 107 July 2022 and 99 in July 2021) 105 likes



Social Network Channel	Link	Indicators [2023-08-03]
<b>Research Gate</b> 	<a href="https://www.researchgate.net/project/InSecTT-Intelligent-Secure-Trustable-Things">https://www.researchgate.net/project/InSecTT-Intelligent-Secure-Trustable-Things</a>	Unfortunately, ResearchGate closed down the “projects” site per March 31, 2023  Project InSecTT had 419 reads per July 2022
<b>Twitter</b> 	<a href="https://twitter.com/InsecttProject">https://twitter.com/InsecttProject</a>	115 Follower  July 2022: 93 Followers, July 2021: 53)
<b>YouTube</b> 	<a href="https://www.youtube.com/channel/UC27HebrTM0MBHKS8yDvwucA">https://www.youtube.com/channel/UC27HebrTM0MBHKS8yDvwucA</a>	35 Subscribers 11 videos  Expected to rise at the end of the project (large number of demonstrator videos!)
<b>Instagram</b> 	<a href="https://www.instagram.com/insecttproject">https://www.instagram.com/insecttproject</a>	78 Follower  July 2022: 77 followers, July 2021: 52 followers

**Table 3 Social Network Channels used by InSecTT (per 2023-08-03)**

Content is provided by partners in a rotating sequence as defined in the Social Media Guideline.

All partners can additionally publish content "on demand".

A dedicated tool (*Buffer*) is used to dispatch content and report statistics.



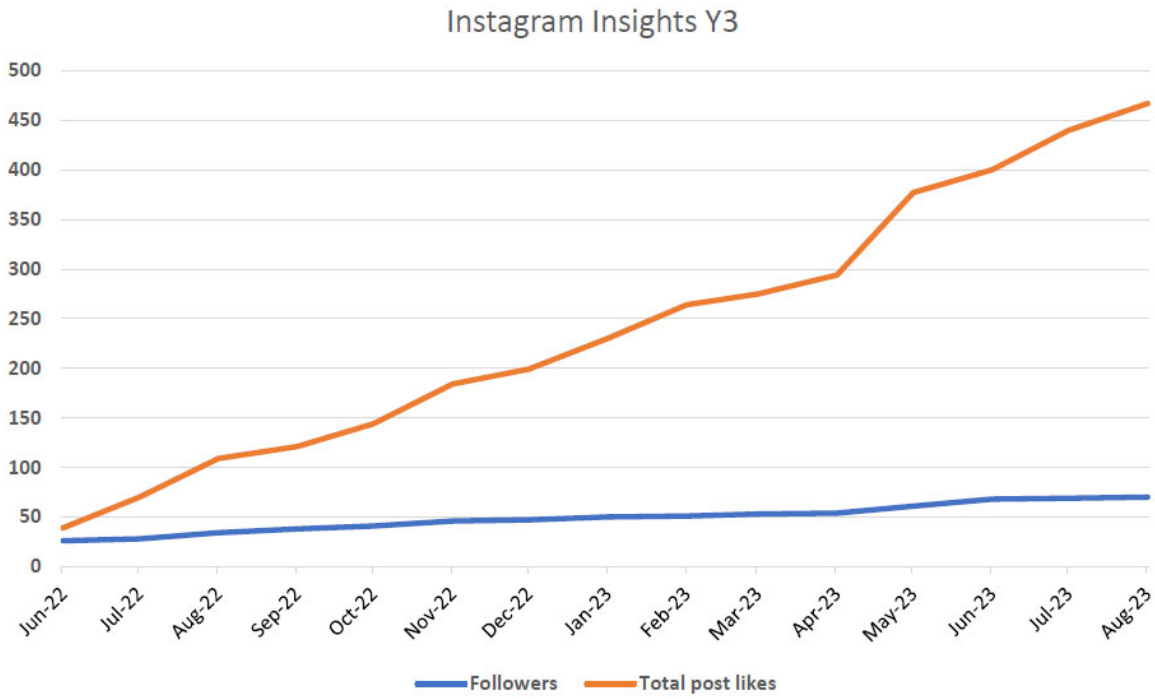


Figure 9 Instagram Statistics Y3

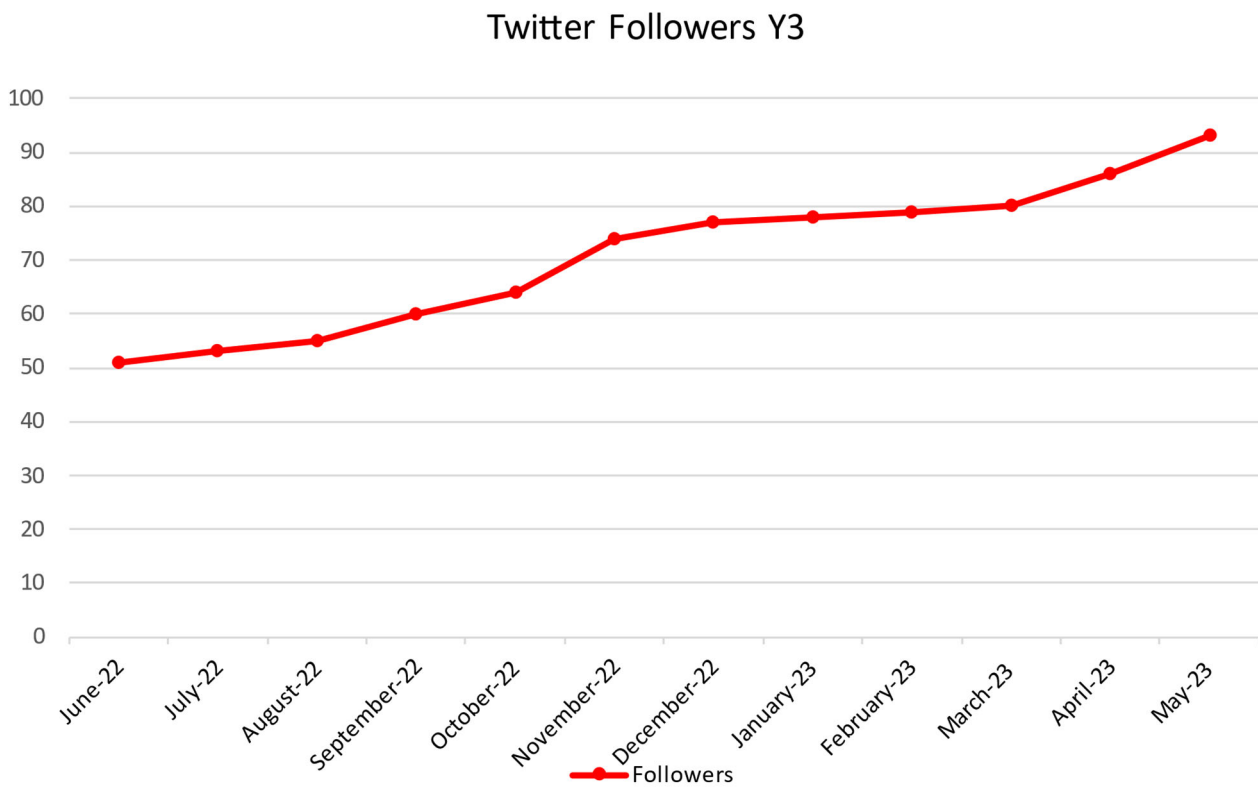
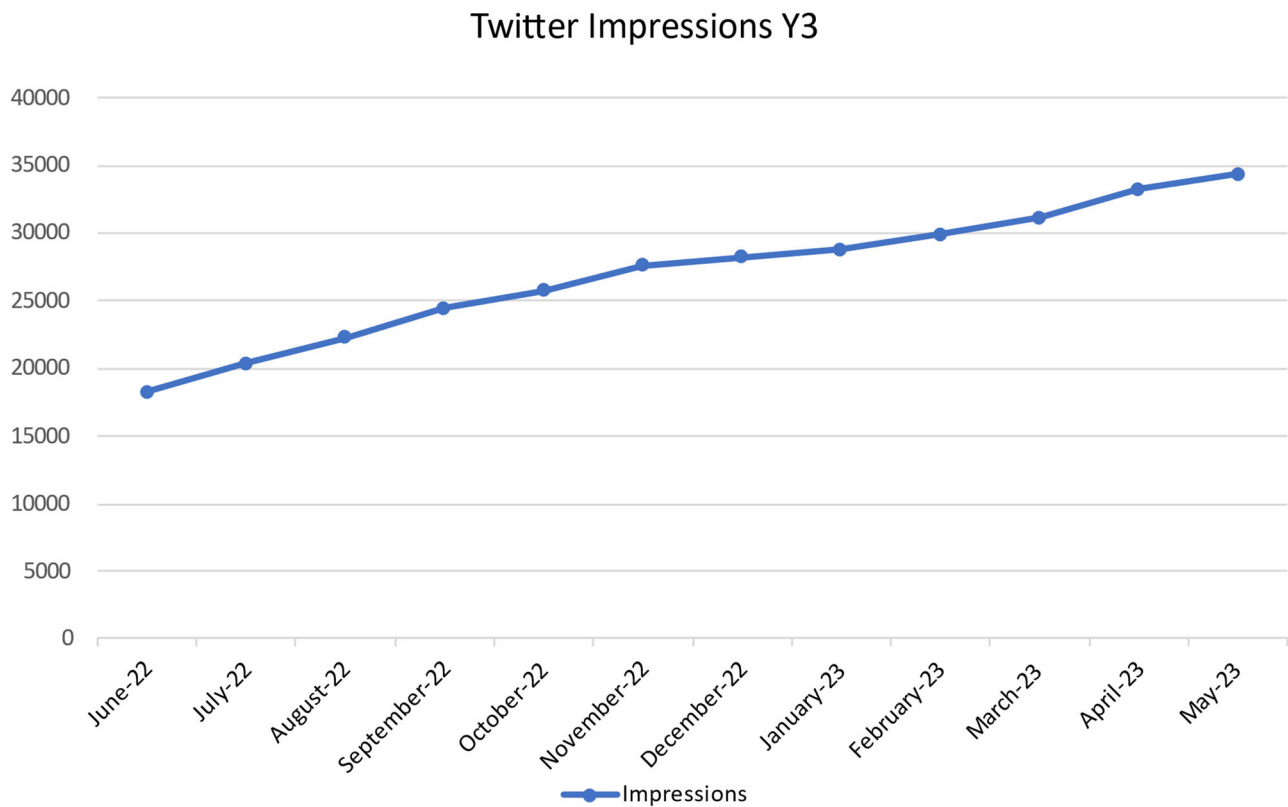


Figure 10 Twitter Followers Y3



**Figure 11 Twitter Impressions Y3**

### 3.1.5 InSecTT Newsletter

Every three months the “InSecTT newsletter” is published and distributed via email. The newsletter is sent out to all project partners with the request to further distribute it internally in their organizations. In addition, anyone can actively request to be put on the distribution list.

- Q4-2020 Issue on 2021-01-20
- Q1-2021 Issue on 2021-05-20
- Q2-2021 Issue on 2021-07-12
- Q3-2021 Issue on 2021-10-09
- Q4-2021 Issue on 2022-01-13
- Q1-2022 Issue on 2022-04-06
- Q2-2022 Issue on 2022-07-13
- Q3-2022 Issue on 2023-10-17
- Q4-2022 Issue on 2023-01-16
- Q1-2023 Issue on 2023-05-16 (see Figure 12)
- Q2-2023 Issue on 2023-08-07
- Q3-2023 (FINAL) expected after the final review, October 2023

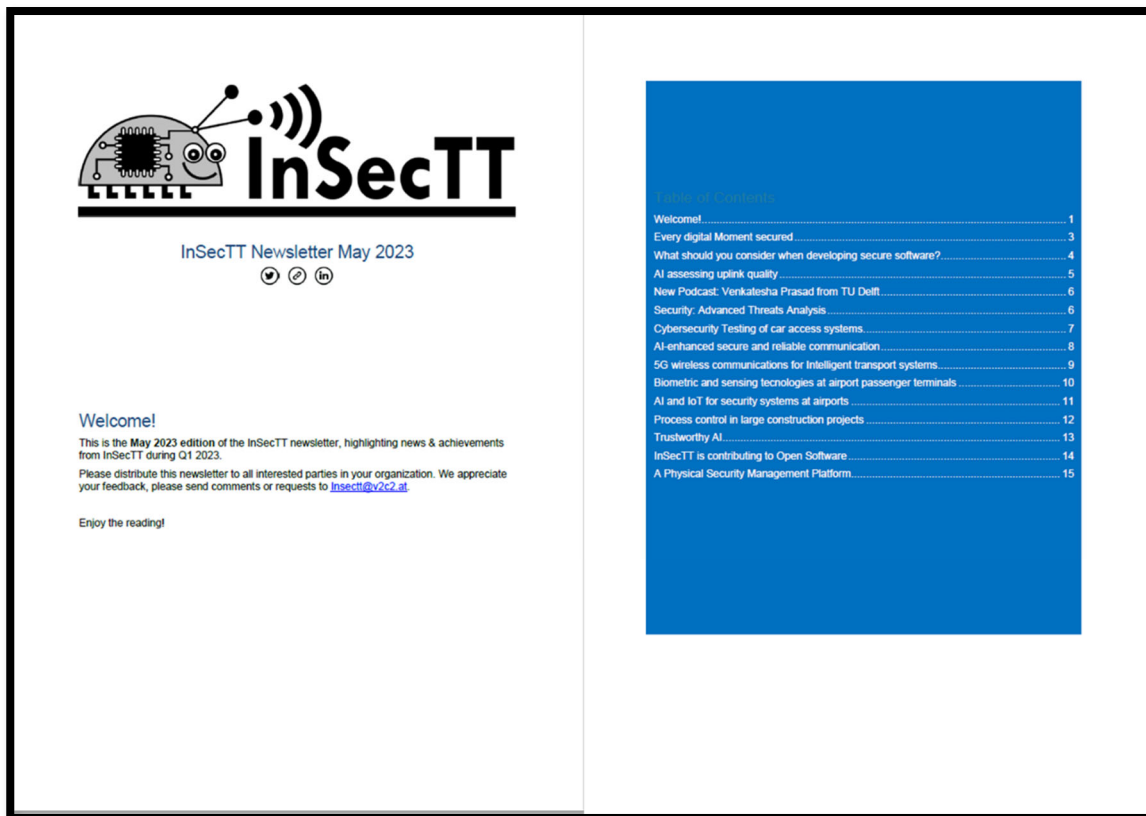


Figure 12 Q1-2023 Issue of the InSecTT Newsletter

### 3.1.6 InSecTT Podcast

Since January 2022, the InSecTT consortium publishes podcasts, typically on a monthly basis. Leading experts from consortium members are being interviewed to explain their goals and their challenges in the project, by that introducing the objectives and results in an enjoyable, lively manner.

The interviews are accessible via standard podcast catchers and appear on <https://podcasts.apple.com/at/podcast/project-insectt/id1605747720>

The following podcasts have been released:

1. January 2022:  
Stefan Marksteiner, AVL: What about automotive security
2. February 2022:  
Andreas Springer, JKU: From Narrow to Ultra-Wide Band
3. March 2022:  
Michael Jerne, NXP: managing lots of technology building blocks in WP3
4. April 2022:  
Ramiro Robles, ISEP: AIoT in *Aeronautics*
5. May 2022:  
Markus Pistauer, CISC: From sensor to cloud
6. June 2022

Johannes Peltola, VTT: AI technologies in WP2

7. August 2022

Michael Karner, VIF: Coordination of a large Research project: InSecTT

8. September 2022

Peter Mörtl, VIF: Do you trust AI? How to make things trustworthy

9. November 2022

Lukasz Kulas, GUT : Smart Ideas and Open Innovation

10. February 2023

Venkatesha Prasad, TU Delft: is the revolution of the Internet of Things already over, or are we still at the beginning?

11. March 2023

Laura Kankaala from F-Secure on cybersecurity in IoT: what are the threats out there, and what can we do to protect society?

12. May 2023

Hans-Peter Bernhard from Silicon Austria Labs on wireless communication systems

**Project InSecTT**  
Peter  
Technologie  
★★★★★ 5,0 • 2 Bewertungen

[Anhören in Apple Podcasts](#)

25. MAI 2023  
**Hans-Peter Bernhard from Silicon Austria Labs on wireless...**  
In this Podcast, Anamarija welcomes Hans-Peter Bernhard from Silicon Austria Labs (known as "SAL"). Hans-Peter introduces this still young Austrian research institute, and talks about some of the top-notch research topics he and his team work on. Hans-Peters also shares his predictions for futu...  
▶ **WIEDERGABE** 27 Min.

21. MÄRZ 2023  
**Laura Kankaala from F-Secure on cybersecurity in IoT: what are the...**  
Today, Peter (substituting for Anamarija) welcomes Laura Kankaala, security professional from F-Secure, Finland. Laura talks about cybersecurity threats, and how it affects consumer IoT, industries and nation-level infrastructure. What can developers do to make products more secure? What can...  
▶ **WIEDERGABE** 20 Min.

6. MÄRZ 2023  
**Venkatesha Prasad from TU Delft, Netherlands: is the revolution of the...**  
Today, Venkatesha Prasad (known as "VP") tells Anamarija about how he came from small-town India to TU Delft in the Netherlands. VP explains the research he and his team at TU Delft do in InSecTT, and what he expects to see in IoT for the near future coming up. So ... is the revolution of the Interne...  
▶ **WIEDERGABE** 27 Min.

11. NOV. 2022  
**Lukasz Kulas from University of Gdansk on smart ideas and open...**  
In this episode, Anamarija talks with Prof. Lukasz Kulas from Gdansk University about smart ideas for using secure connected things in real life. For example, about retrofitting ships and harbors, or localizing medical devices in a hospital. Lukasz has also organized Open Innovation and Student...

Figure 13 InSecTT Podcasts (retrieved 2023-08-03)

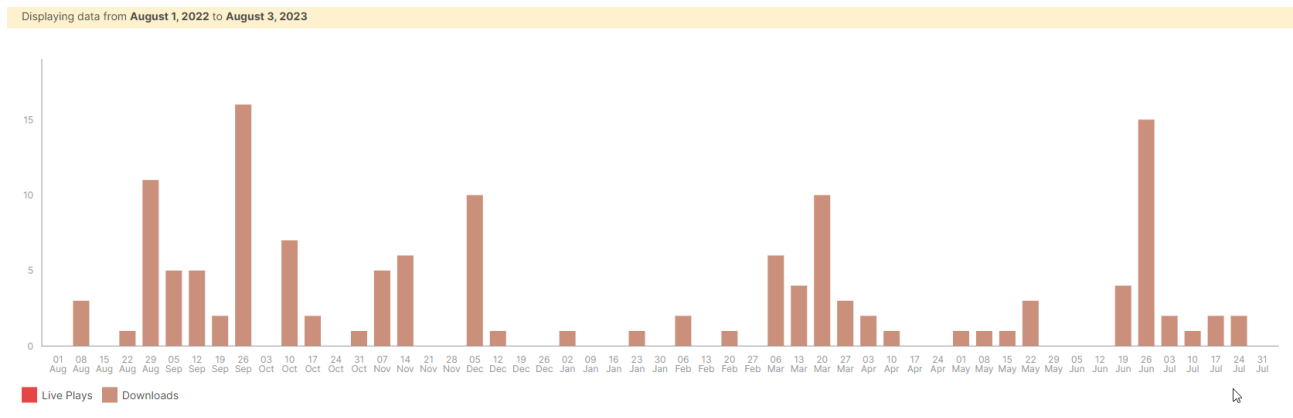


Figure 14 Podcast download statistics August 2022 – August 2023

In total, the podcast was downloaded 322 times from the Spreaker hosting service as per 2023-08-03.

### 3.2 Report of InSecTT dissemination activities in Y3

#### 3.2.1 Public deliverable, summarizing WP2 and WP3 technology results

Two public deliverables provide a summary of the technologies developed:

- D2.4, Publishable Summary of WP2 Results, 100 pages, see Figure 15
- D3.4, Publishable Summary of WP3 Results, 81 pages, see Figure 16

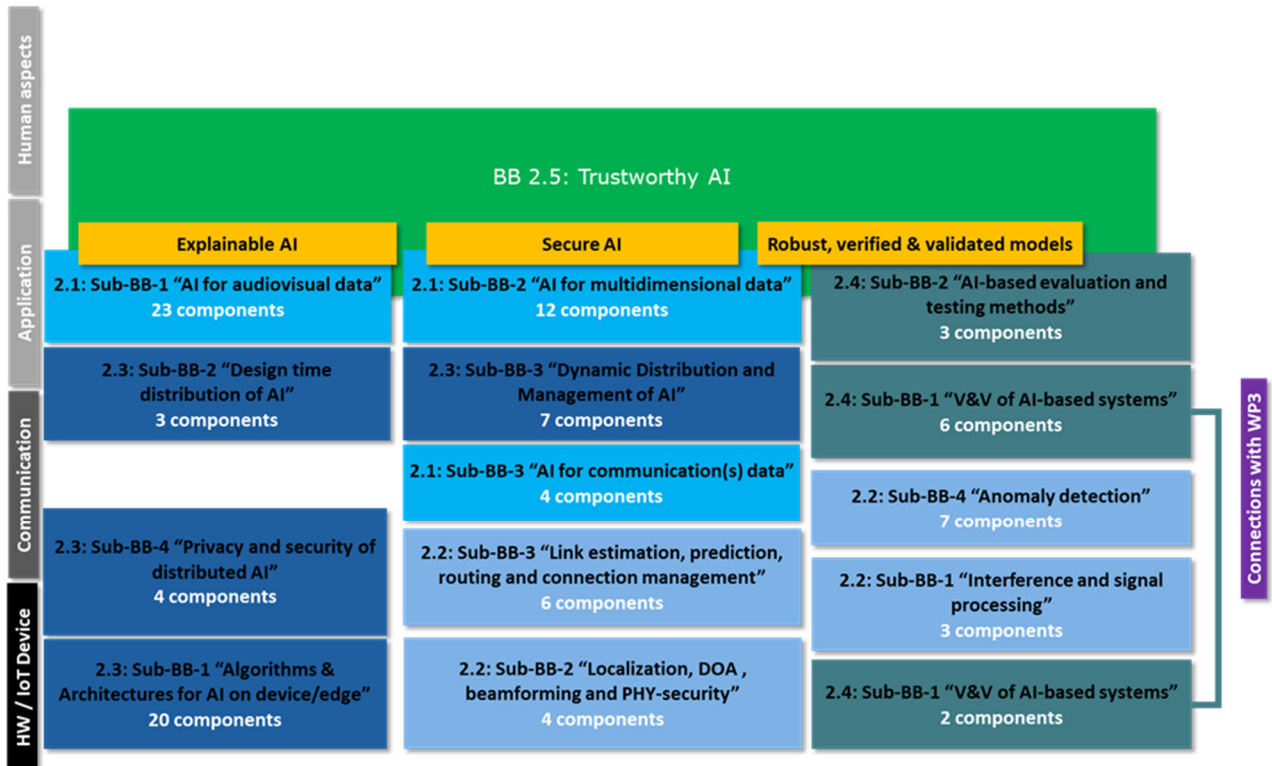


Figure 15 WP2 sub-building blocks BB2.1 – BB2.5

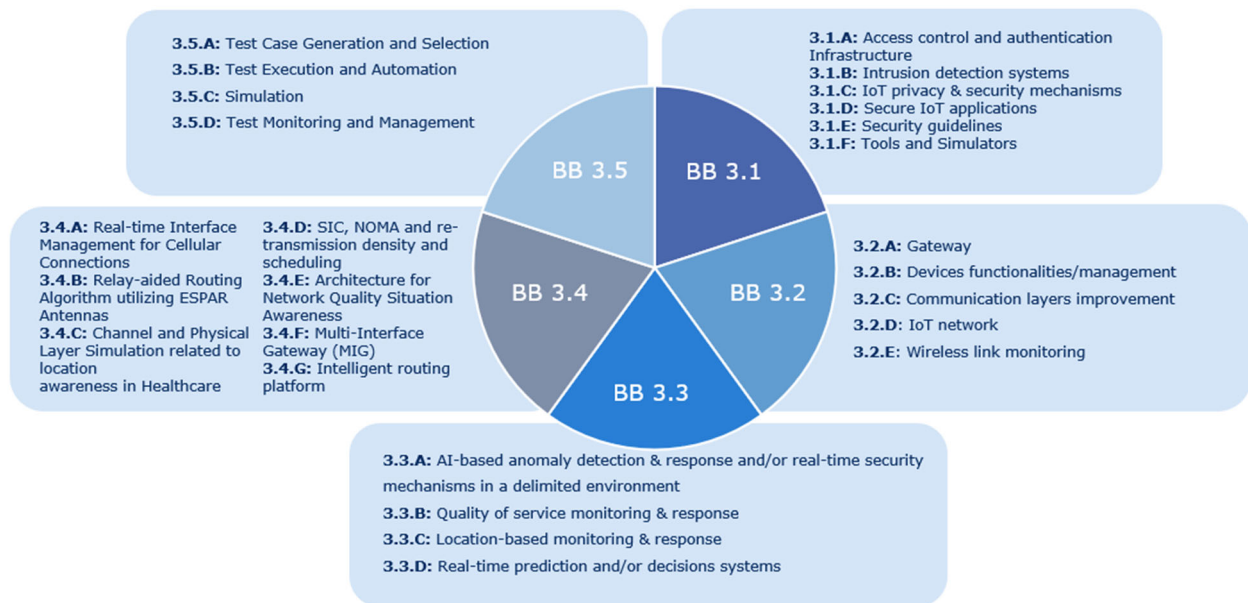


Figure 16 WP3 sub-building blocks BB3.1 – BB235

### 3.2.2 Publications in InSecTT

Addressed stakeholders:

- Academic communities
- Researchers / Experts from the field of policy, science, and industry;
- Students (PhD or Master thesis)
- Applied researchers in industry

InSecTT partners have produced an impressive number of publications also in Y3. Between M25 and the time the deliverable was written beginning of August 2023, there were **70 publications** additional reported (adding to the 50 reported in Y2, and another 38 reported from Y1), listed in the following table:

Title	Partner	Dissemination Type	Conference Short Name/Publisher
Sound Event Detection for Human Safety and Security in Noisy Environments	CINI	Journal Paper	IEEE
Biometric Recognition using Microwave Reflection Spectroscopy	CINI	Technical Paper (Conference)	MIKON
Cellular Interface Selection in Multi-Homed Vehicular Onboard Gateways	MTU	Technical Paper (Conference)	ETF A 2022
Developing and Evaluating MQTT Connectivity for an Industrial Controller	ABB AB	Technical Paper (Conference)	CPS&IoT'23

Title	Partner	Dissemination Type	Conference Short Name/Publisher
Anomaly Attack Detection in Wireless Networks Using DCNN	ABB AB	Technical Paper (Conference)	IEEE 8th World Forum on Internet of Things
The DEWI High-Level Architecture: Wireless Sensor Networks in Industrial Applications	ISEP	Journal Paper	doi.org/10.3390/technologies9040099
Orthogonal Space-Time Block Coding for V2V LOS Links with Ground Reflections	ISEP	Technical Paper (Conference)	MIKON
Wireless Channel Prediction Using Artificial Intelligence with Constrained Data Sets	ISEP	Technical Paper (Conference)	MIKON 2022
A Practical Study on Optimization of Big Data Streaming and Data Analytics Infrastructure for Efficient AI Based Processing	MARUN	Technical Paper (Conference)	MIKON
Implementation of High Performance Multi-Agent Position Feeding Framework	MARUN	Technical Paper (Conference)	MIKON
A Practical Introduction to Side-Channel Extraction of Deep Neural Network Parameters	CEA	Technical Paper (Conference)	CARDIS
A Sink-oriented Routing Protocol for Blue Light Link-based Mesh Network	CINI	Chapters in books	IET
Seamless IoT Mobile Sensing through Wi-Fi Mesh Networking	CINI	Chapters in books	IET
ParalMGC: Multiple Audio Representations for Synthetic Human Speech Attribution	CINI	Technical Paper (Conference)	EUVIP
Multi Hypothesis Interference Tracking in Wireless Networks	SAL	Journal Paper	IEEE Internet of Things Journal
Self-Attention Generative Distribution Adversarial Network for Few- and Zero-Shot Face Anti-Spoofing	U TWENTE	Technical Paper (Conference)	IJCB 2022
Control Predictivo por Modelo Robusto y Descentralizado para Acoplamiento Virtual de Trenes	UPM	Technical Paper (Conference)	XV Congreso Iberoamericano de Ingeniería Mecánica - CIBIM 2022



Title	Partner	Dissemination Type	Conference Short Name/Publisher
A Modular Ice Cream Factory Dataset on Anomalies in Sensors to Support Machine Learning Research in Manufacturing Systems	MDH	Journal Paper	IEEE Access Journal
Trade-off Analysis of Pruning Methods for Compact Neural Networks on Embedded Devices	U TWENTE	Technical Paper (Conference)	IFIP IoT
Firmware Updates Over The Air for LoRa using Random Linear Network Coding	TU DELFT	Thesis/dissertation	Master Thesis
Divide and Code: Efficient and Real-time Data Recovery from Corrupted LoRa Frames	TU DELFT	Technical Paper (Conference)	SECON
Data Trustworthiness for UWB Ranging in IoT	JKU	Technical Paper (Conference)	IEEE GLOBECOM
DL-based Physical Tamper Attack Detection in OFDM Systems with Multiple Receiver antennas: A Performance-Complexity Trade-off	JKU	Journal Paper	Sensors
Consistency-based Self-supervised Learning for Temporal Anomaly Localization	CINI	Technical Paper (Conference)	ECCV
Class-Incremental Continual Learning into the eXtended DER-verse	CINI	Journal Paper	TPAMI
Collective Perception: a Delay Evaluation With a Short Discussion on Channel Load	VIF	Journal Paper	IEEE Open Journal of Intelligent Transportation Systems
Anchor-agnostic Transformer: End-to-End Fingerprint-based Indoor Localization with Transformers	U TWENTE	Technical Paper (Conference)	PerCom 2023
Evaluating challenges, benefits, and dependability of virtual and physical testing of embedded systems software	WESTERM O	Thesis/dissertation	N/A
Reservoir Computing Approach for Network Intrusion Detection	MDH	Thesis/dissertation	N/A

Title	Partner	Dissemination Type	Conference Short Name/Publisher
Anomaly Detection in Networks Using Autoencoder and Unsupervised Learning Methods	MDH	Thesis/dissertation	N/A
Intrusion Detection Using Machine Learning for Industrial Control Systems	RISE	Thesis/dissertation	N/A
Using Supervised Learning and Data Fusion to Detect Network Attacks	MDH	Thesis/dissertation	N/A
Anomaly detection in Network data with unsupervised learning methods	MDH	Thesis/dissertation	N/A
Intrusion Detection and Attack Classification with Feature Selection: A Comparison of Unsupervised Machine Learning Algorithms	MDH	Thesis/dissertation	N/A
LoRa meets IP: a Container-based Architecture to Virtualize LoRaWAN End Nodes	CINI	Journal Paper	-
A Decentralized Model Predictive Control for Virtual Coupling in Train Sets	UPM	Journal Paper	MDPI
DL-Based Physical Tamper Attack Detection in OFDM Systems with Multiple Receiver Antennas: A Performance-Complexity Trade-Off	JKU	Journal Paper	MDPI
Combating air pollution through intelligent IoT systems	CINI	Other	Issue 03
Air Quality Estimation with Embedded AI-based Prediction Algorithms	CINI	Technical Paper (Conference)	IEEE ICC 2023
Harnessing Communication Heterogeneity: Analytical Modeling and Experimental Evaluation of an IoT Multi-Interface Gateway	CINI	Journal Paper	IEEE Internet of Things Journal
Edge-enabled Adaptive Shape Estimation of 3D Printed Soft Actuators with Gaussian Processes and Unscented Kalman Filters	KTH	Journal Paper	IEEE Transactions on Industrial Electronics

Title	Partner	Dissemination Type	Conference Short Name/Publisher
Performance Evaluation of Object Detection Models for Traffic Safety Applications on Edge	MARUN	Other	IPMV 2023
Ultra-Wideband based Indoor Localization: A Battle of End-to-End Deep Learning with Time Difference of Arrival Techniques	U TWENTE	Technical Paper (Conference)	IPIN 2023
A Decentralized Robust Control Approach for Virtually Coupled Train Sets	UPM	Journal Paper	Wiley
Gender-Specific Characteristics for Hand-Vein Biometric Recognition: Analysis and Exploitation	CINI	Journal Paper	IEEE
HistoTrust: tracing AI behavior with secure hardware and blockchain technology	CEA	Journal Paper	Springer Nature
Real-Time Jamming Detection in Wireless IoT Networks	MARUN	Journal Paper	MPDI
Time-series Anomaly Detection and Classification with Long Short-Term Memory Network on Industrial Manufacturing Systems	MDH	Technical Paper (Conference)	IJCNN
Multi-Objective Optimization on Autoencoder for Feature Encoding and Attack Detection on Network Data	MDH	Journal Paper	GECCO
A Systematic Approach to Automotive Security	AVL	Technical Paper (Conference)	FM'23
Internet of Things Technology for Train Positioning and Integrity in the Railway Industry Domain	UPM	Other	IEEE
Federated Learning with Tiny Bayesian Classifiers	MDH	Technical Paper (Conference)	ISIE Or ICIT by IEEE Industrial Engineering Society (IES)
RouMBLE: a Sink-Oriented Routing Protocol for BLE Mesh Networks	CINI	Journal Paper	IEEE
An Empirical Evaluation of Enhanced Performance Softmax Function in Deep Learning	JSI	Journal Paper	IEEE

Title	Partner	Dissemination Type	Conference Short Name/Publisher
Dependability and Security aspects of Network-Centric Control	ABB AB	Technical Paper (Conference)	ETFA
The Westermo network traffic data set	WESTERMO	Journal Paper	Elsevier's Data in Brief
ICSSIM — A framework for building industrial control systems security testbeds	RISE	Journal Paper	Comp.ind.
Anomaly Detection Dataset for Industrial Control Systems	RISE	Journal Paper	IEEEAccess
Time-multiplexed AoA Estimation and Ranging	JKU	Technical Paper (Conference)	ICL-GNSS 2023
Joint FMCW Radar and 5G/6G Communication	VTT	Technical Paper (Conference)	IEEE VTC2023-Fall
Transferring Knowledge, Enhancing Accuracy: Multi-Surrogate-Teacher Assistance in Fingerprint-Based Indoor Localization	U TWENTE	Technical Paper (Conference)	NeurIPS 2023
Machine Learning Testing in an ADAS Case Study Using Simulation-Integrated Bio-Inspired Search-Based Testing	RISE	Journal Paper	Journal of Software: Evolution and Process" (Wiley)
An Authorization Service supporting Dynamic Access Control in Manufacturing Systems	ABB AB	Technical Paper (Conference)	WF-IoT 2023
Evaluation of an OPC UA-based Access Control Enforcement Architecture	ABB AB	Technical Paper (Conference)	ESORICS 2023 workshop CyberICPS
Enhanced Simulation Environment to Support Research in Modular Manufacturing Systems	ABB AB	Technical Paper (Conference)	IECON 2023
Distracted Driving Behaviour Monitoring with Smartphones: An Extended Systematic Literature Review	RISE	Journal Paper	MDPI
Anomaly Detection for Network Traffic in a Resource Constrained Environment	WESTERMO	Thesis/dissertation	Mälardalen University
Biometric Recognition Based on Hand Electromagnetic Scattering at Microwaves	CINI	Journal Paper	IEEE
Federated Learning for Network Anomaly Detection in a Distributed Industrial Environment	RISE	Technical Paper (Conference)	IEEE ICMLA

Title	Partner	Dissemination Type	Conference Short Name/Publisher
A Distributed Testbed for Wireless Embedded Devices	LCM	Technical Paper (Conference)	IEEE MeditCom 2023
Title	Partner	Type	Conference / Publisher

**Table 4 Publications in InSecTT during Y3 as of 2023-08-03**

### 3.2.3 Other Dissemination Activities (Conferences, Events, Press Release)

Addressed stakeholders:

- Researchers / Experts from the field of policy, science, and industry;
- Applied researchers in industry
- Other related EU / national projects
- Domain-specific forums and exchange groups
- Academic communities

An impressive number of 99 dissemination activities have been reported in Y3, adding to 61 from Y2 and additionally 72 activities from Y1. A complete list of events from Y3 is given in Table 5.

Event	Title	Date	Location	Dissemination Activity
ENHANCE, FORECAST & STEADINESS workshops at HiPEAC22	CISTER/ISEP is in charge of the dissemination of three workshops in the HiPEAC22 conference (ENHANCE, FORECAST & STEADINESS)	June 20-22 2022	Budapest	Organisation of a conference;#Organisation of a workshop
IoTWeek 2022	Bringing Internet of Things and Artificial Intelligence together – But is it Trustworthy?	23.06.2022	Dublin, Ireland	Presentation
2022 59th ACM/EDAC/IEEE Design Automation Conference	Bringing Internet of Things And Artificial Intelligence Together: But Is It Trustworthy?	14.07.2022	San Francisco, USA	Presentation
BMTT Workshop @ CVPR 2022	Workshop on Benchmarking Tracking System BMTT at CVPR 2022	Jun 23 2022	New Orleans USA	Organisation of a workshop

Event	Title	Date	Location	Dissemination Activity
Notte della ricerca	Notte della ricerca	30/09/2022	Rome	Participation to an event other than a conference or a workshop
Maker Faire 2022	Maker Faire 2022	October 7-9 2022	Rome	Exhibition/booth
Microelectronic Systems Symposium 2022	Labeling for UWB in Weak NLOS Conditions	2022-06-01	Haus der Ingenieure, Vienna	Poster
Broadband Forum's BASE at BREKO Fiberdays	Future Proofing Connected Home Security via Research and Industry Collaboration	13.6.2022	Wiesbaden, Germany	Presentation
ETFA 2022, IEEE International Conference on Emerging Technologies and Factory Automation	2nd Workshop on Wireless Intelligent Secure Trustable Things AIoT: bringing AI and IoT together	06.09.2022	Stuttgart, Germany	Organisation of a workshop
InSecTT social media news	Project news (5 news)	2021-10-22	LinkedIn, Twitter, Facebook, and Instagram	Social Media
UPM-CEI Annual Meeting	Participation in UPM-CEI Annual Meeting	15/06/2022-17/06/2022	Madrid, Spain	Presentation;#Poster
IoTWeek 2022	Bringing Internet of Things and Artificial Intelligence together – But is it Trustworthy?	23.06.2022	Dublin, Ireland	Presentation
59th Design Automation Conference (DAC 2022)	Bringing Internet of Things and Artificial Intelligence together – But is it Trustworthy?	12.07.2022	San Francisco, USA	Presentation;#Poster
International Cybersecurity Forum 2022	Booth at Exhibition Area, Distributing InSecTT project Flyer/Poster	8.6.2022	Lille, France	Exhibition/booth

Event	Title	Date	Location	Dissemination Activity
Swedish National Computer Networking Workshop (SNCNW 2022)	Digital Twin-based Intrusion Detection for Industrial Control Systems	2022-06-16	Stockholm	Poster
Summer School CPSIoT2022	Reference architecture for trusted AIoT systems: certification, standardization and regulation	9-June-2022	Budva, montenegro	Presentation
Broadcast our participation and developments in companies related with rail, defense, health and other domains	INDRA website	2022-06-15	Online	Newsletter
Indra disseminated the activities at its stand associated with the developments made and linked to SHIFT2RAIL	Rail Live 2021	2022-11-30/2022-12-01	IFEMA Madrid	Participation to a conference
Product Development in Motion	InSecTT results in a booth	09.06.2022	Coventry, UK	Exhibition/booth
Facebook post	(Haltian) InsecTT project promotion post	22.08.22	Facebook	Social Media
EBSCON 2022	IoT and Security Belong Together	2022 10 05	Graz/ Austria	Participation to a conference;#Presentation

Event	Title	Date	Location	Dissemination Activity
AVL Research Networking Day 2022	InSecTT presentation at the AVL Research Networking Day 2022	17.10.2022 2	Seggau, Austria	Brokerage Event
SPECIES 2022, event for F-Secure's partners and customers	SPECIES Research Collaboration Presentation	20.9.- 21.9.2022	Helsinki, Finland	Organisation of a conference; #Participation to a conference;#Presentation
Hello IT Conference	Speech during Hello IT conference	13-09- 2022	DevOne Hub Gdansk	Speech/Keynote; #Participation to a conference;#Presentation
Social media post	Post for social media about Vemco's update in InSecTT - PSIM integrations	06-10- 2022	LinkedIn	Social Media
Workshop	Connected & Autonomous Cars Workshop - 2	2022-12- 06	Marmara University Mehmet Genc Campus Conference Center	Organisation of a workshop; #Poster;#Presentation
Guest lecture at "Autonomous Vehicle" course, Mälardalen University	"Assurance of Machine Learning in Autonomous Automotive Systems"	2022-11- 21	Mälardalen University, Sweden	Lecture
Guest seminar at Gdansk University of Technology, Oct and Nov. 2022.	"ML Systems: Powerful Engines to Drive Maritime Industry—From design principles to ML operation"	2022-10, 11	Gdansk University of Technology, Poland	Training seminars
Software Center Cybersecurity Workshop	Invited talk - Access Control in Industrial Automation and Control Systems	9 Sept, 2022	Mälardalen University	Lecture
Social media posts	Social media posts by IDEMIA (responsible for week 14, 2023)	17/04/202 3	online	Social Media



Event	Title	Date	Location	Dissemination Activity
Social Media	Social media post about Wapice Ai solution	9.11.2022	Social Media	Social Media
Augmenting humans with AI-driven knowledge seminar	Presentation in Augmenting humans with AI-driven knowledge	5.10.2022	Espoo, Finland	Presentation
Wapice web news	Machine vision enhanced security and safety in urban environment	31.5.2023	Online	Website
InSecTT social media news	Project results news (4)	2023-05-15	LinkedIn, Instagram, Facebook, Twitter	Social Media
Axis Open Day 2023	Axis conference	2023-05-10 - 2023-05-11	Lund, Sweden	Brokerage Event
Critical Communications World	Tradeshaw	2023-05-23 - 2023-05-24	Helsinki, Finland	Trade Fair;#Brokerage Event
VTT Demo Combo	Research results seminar of VTT Technical Resarch Centre of Finland	2023-04-19	Oulu, Finland	Brokerage Event
Verkosto	Trade fair for energy and information networks	2023-01-25 - 2023-01-26	Tampere, Finland	Trade Fair;#Brokerage Event
5G-Heart Public Event	5G-Heart EU project's public results seminar	2022-11-17	Oulu, Finland	Participation to a conference
Subcontracting Fair	Subcontracting Trade Fair	2022-09-27 - 2022-09-29	Tampere, Finland	Exhibition/booth;#Trade Fair
Kaitotek's web pages and LinkedIn	Kaitotek news from its results from the project	2023-06	Web pages and LinkedIn	Social Media;#Website
PyData Trójmiasto #22	Co-organizing PyData Trójmiasto event - spreading information about InSecTT. JKU's presentation.	15.03.2023	Gdańsk Science and Technology Park	Organisation of a conference;#Supporting PhD or Master theses work;#Presentation
InSecTT Podcast with Laura Kankaala from F-Secure	Cybersecurity in IoT: What are the threats out there, and what can we do to protect society?	21.3.2023	Online	Interview

Event	Title	Date	Location	Dissemination Activity
RTE company conference	Tucana use case	2022-09-28	Conference hotel, Strängnäs (Sweden)	Presentation
Customer meeting	ML in IoT systems	2023-01-27	RTE office	Presentation
InSecTT book	Working with AIoT solutions in embedded software applications	2023 Q3	Published book	Non-scientific and non-peer-reviewed publication (popularised publication)
White paper	Working with AIoT solutions in embedded software applications	2023-06-08	RTE website	Non-scientific and non-peer-reviewed publication (popularised publication)
Online promotion	Project Tucana	2023-05-17	InSecTT sharepoint	Vidoe/Film
Online promotion	Network camera study	2023-05-22	InSecTT sharepoint	Vidoe/Film
Meeting with client [ENERY SECTOR]	SECORUN Products Campaign (PSIM as part of SECORUN)	22.09.2022	Online	Social Media;#Website
CARDIS 2022	Participation to CARDIS 2022 Conference	07/11/2022	Birmingham, UK	Participation to a conference
IEEE IOLTS 2022	Participation to IOLTS 2022	12/09/2022	Torino, Italy	Participation to a conference
SafeComp 2023	Participation to SafeComp 2023	19/09/2023	Toulouse, France	Participation to a conference
IEEE International Mediterranean Conference on Communications and Networking (MeditCom 2023)	A Distributed Testbed for Wireless Embedded Devices	04.09.2023	Dubrovnik, Croatia	Presentation;#Participation to a conference
dissemination and stakeholder engagement	AI unplugged event	March 3 2023	modena	Organisation of a workshop
workshop talk on AI and industry	participation to Ital-IA workshop on AI and Industry	May 29 2023	Pisa Italy	Participation to a workshop

Event	Title	Date	Location	Dissemination Activity
Talk Nuova Didactica @ Confindustria Modena	Talk at Confindustria Modena (Association of Industry of Emilia Romagna filiera digital)	May 16 2023	Modena	Other
Research to Business Fair	participation to Research To Business Fair	June 6-9 2023	Bologna Italy	Trade Fair;#Pitch event
Modena AI schools on vision and Language for industry	AI School in Modena lecture on Visual anomaly	Sept 2022	Modena	Speech/Keynote
Meeting with client from MINING SECTOR	SECORUN Products Campaign (PSIM as part of SECORUN)	04.10.2022	Online	Presentation
Meeting with client from AUTOMOTIVE sector	SECORUN Products Campaign (PSIM as part of SECORUN)	16.05.2023	Client's venue	Presentation
Meeting with client from FARMACEUTICAL sector	SECORUN Products Campaign (PSIM as part of SECORUN)	08.05.2023	Online	Presentation
Roma Tre Open Day	Hands-on experience with demonstrator	24/01/2023	Rome	Participation to an event other than a conference or a workshop
Meeting with a client from ENERGY sector	SECORUN Products Campaign (PSIM as part of SECORUN)	28.04.2023	Online	Presentation
Meeting with a client from DELIVERY sector	SECORUN Products Campaign (PSIM as part of SECORUN)	17.03.2023	Online	Presentation
Meeting with a client from TRANSPORT sector	SECORUN Products Campaign (PSIM as part of SECORUN)	22.03.2023	Online	Presentation
Meeting with a client from TOYS PRODUCTION sector	SECORUN Products Campaign (PSIM as part of SECORUN)	13.02.2023	Online	Presentation

Event	Title	Date	Location	Dissemination Activity
Meeting with a client from BIOTECH sector	SECORUN Products Campaign (PSIM as part of SECORUN)	11.01.2023	Online	Presentation
Meeting with a client from GROCERY RETAIL sector	SECORUN Products Campaign (PSIM as part of SECORUN)	17.11.2022	Online	Presentation
Cooperative Interactive Vehicles Summer School 2022	Summer School Presentation	2022-08-01	California, USA	Participation to an event other than a conference or a workshop
Meeting with a client from LOGISTICS sector	SECORUN Products Campaign (PSIM as part of SECORUN)	15.12.2022	Online	Presentation
Post on linkedin	Social media post regarding PSIM integration	29.05.2023	Online, social media	Social Media
19TH IEEE International Conference on Automation Science and Engineering (CASE)	Presentation at the international conference	2023-08-26th - 30th	Auckland, New Zealand	Participation to a conference; #Presentation
10th Scandinavian Conference on SYSTEM & SOFTWARE SAFETY	Understanding CPS Trustworthiness	November 23, 2022	Gothenburg, Sweden	Organisation of a workshop
Interizon Day 2022	Interizon Day 2022	22.09.2022	Gdańsk, Poland	Presentation; #Participation to an event other than a conference or a workshop
meeting with client	Meeting with client from RETAIL sector	23.01.2023	Łódź, Poland	Presentation
meeting with client	Meeting with client from MANUFACTURING sector (machines)	23.01.2023	Łódź, Poland	Presentation
meeting with client	meeting with client from IT SOLUTIONS sector	23.01.2023	Łódź, Poland	Presentation

Event	Title	Date	Location	Dissemination Activity
meeting with client	meeting with client from manufacturing sector (furniture)	01.02-02.02.2023	Oleśnica, Poland	Presentation
meeting with client	meeting with client from manufacturing sector (aluminium profiles)	24-25.02.2023	Herby, Poland	Presentation;#Other
meeting with stakeholder	meeting with RF hardware manufacturer & distributor	28.02.2023	Gdynia, Poland	Presentation
meeting with client	meeting with client from manufacturing sector (roof rails)	24.03.2023	Łódź, Poland	Presentation
meeting with client	meeting with client from manufacturing sector (home appliances)	28.03.2023	Łódź, Poland	Presentation
meeting with stakeholder	meeting with RF hardware manufacturer & distributor	01.03.2023	Gdynia, Poland	Presentation
meeting with client	meeting with client from manufacturing sector (counterweights)	19.04.2023	Barlinek, Poland	Presentation; #Other
meeting with client	meeting with client from manufacturing sector (aluminium parts)	23-24.04.2023	Częstochowa, Poland	Presentation
Interizon Innovation Night 2023	Interizon Innovation Night 2023	20.04.2023	Gdańsk, Poland	Participation to an event other than a conference or a workshop; #Presentation
meeting with client	meeting with client from manufacturing sector (sweets)	10.05.2023	Tomaszów Mazowiecki, Poland	Presentation
meeting with client	meeting with client from recycling sector (regranulates manufacturing)	16-17.05.2023	Trzydnik Duży, Poland	Other; #Presentation
Warsaw Pack 2023	packaging & logistics expo in Warsaw	16-19.04.2023	Warszawa, Poland	Trade Fair
Logimat 2023	intralogistics expo in Stuttgart	24-28.04.2023	Stuttgart, Germany	Trade Fair

Event	Title	Date	Location	Dissemination Activity
Modernlog 2023	logistics expo in Poznan	31.05.2023	Poznań, Poland	Trade Fair
Workshop in NOMS 2023	4th Workshop on Management for Industry 5.0 - part of NOMS 2023	8 - 12 May 2023	Miami, Florida, USA	Organisation of a workshop
Podcast	InsecTT podcast about wireless communication systems	May 2023	online	Interview
5th Wellcomp workshop adjunct to Ubicomp Conference in Cambridge 2022	WellComp 2022: Fifth International Workshop on Computing for Well-Being	2022-09-11 - 2022-09-11-15	Cambridge, GB	Organisation of a workshop
Edge AI seminar co-organized by Finnish academy flagship programs FCAI and the 6G Flagship	What Cyberpunk'77 teaches us about the future of AI and edge computing	2022-05-19	Helsinki, Finland	Speech/Keynote;#Poster
Roma Tre open Nigh	Open Night	07/06/2023	Rome, Italy	Participation to an event other than a conference or a workshop
n.a. (Deliverable D3.4)	Dissemination of exploitable items	June 2023	Global	Deliverable
SAL presents in the Summer school supported by EPoSS and Aeneas.	Summer school "Fascinating Electronics for a Cool World"	20.8 - 25.8.2023	Bertinoro, Italy	Other

**Table 5 Dissemination Activities in Y3 per 2023-08-03**

### 3.2.4 Participation and Booth at the EF ECS 2022

EF ECS 2022 was one of the first large KDT events in presence since the pandemic (Amsterdam Beurs van Berlage, 24. – 25.11.2022).

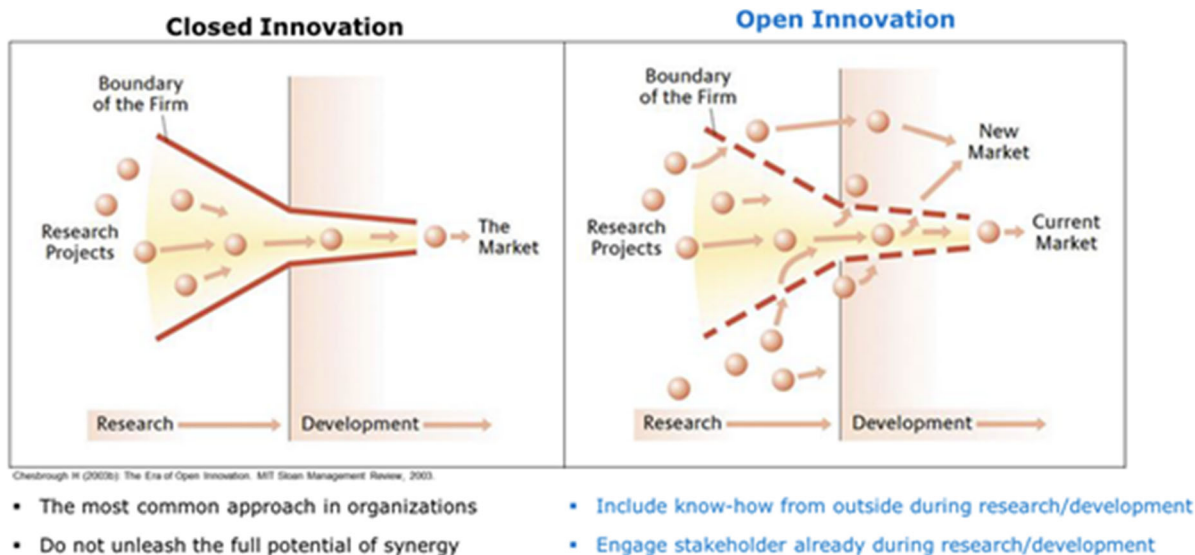
InSecTT was present with an own booth during both days, with many interested visitors and booth discussions during both days.F



Figure 17 InSecTT booth at the EFCS 2022, 24.-25. November

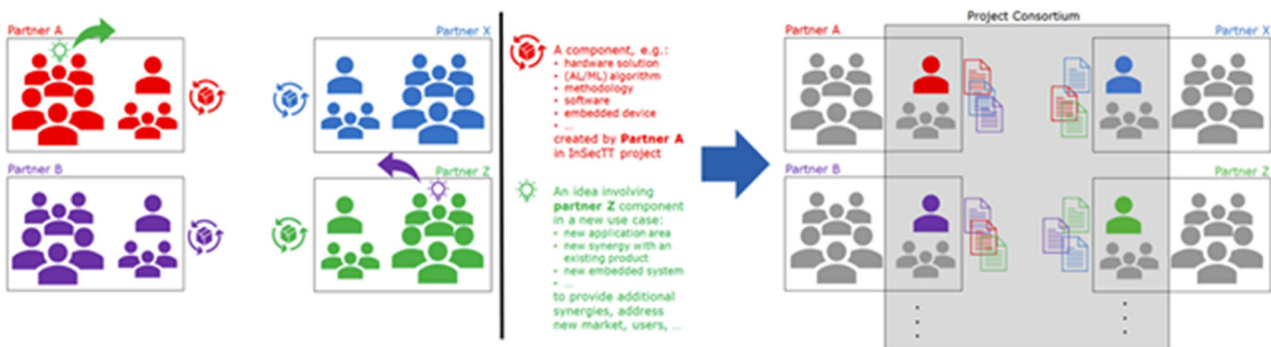
### 3.2.5 Development of InSecTT Open Innovation Framework

One of the key activities, which will were implemented in InSecTT to stimulate generation of innovations beyond the project boundaries, was open innovation approach. In its classical implementation, open innovation focuses on gathering new and potentially valuable research conducted outside the company to provide an additional flow of innovations and, at the same time, push the research outcomes that will not be used inside of the company to provide additional revenue streams via licenses, which is illustrated by the innovation funnel pictures below.



**Figure 18: Closed Innovation vs. Open Innovation**

This concept was adapted at the big EU project level in the InSecTT consortium, which allowed project partners to overcome isolation and stimulate additional collaboration not only on project partner level but also to involve external entities (outside of the consortium) for additional innovation spill-over to increase the chances for successful exploitation of particular project results outside companies participating in the use case utilizing the results. In the InSecTT project, open innovation activities led to form a unique mechanism, InSecTT Open Innovation Contest, as a repeatable process.



**Figure 19: A graphical description of the Open Innovation Contest developed during InSecTT project for maximizing exploitation results**

The InSecTT Open Innovation Contest has been launched several times and it was warmly received by the project partners and participating entities, as well as involved Interizon ICT Cluster (one of the key Polish clusters), which adopted the same idea as a meeting called “Open Innovation Night”, during which components were presented in person and then discussed during evening networking, to foster more collaboration between its members and possible end-users. The final step, developed within the InSecTT project, was public release of the best components on the InSecTT webpage that led to global interest in some of the InSecTT project innovations



(e.g. an entity from Canada is willing to implement one of the solutions) and resulted in one start-up company. It is planned, that InSecTT Open Innovation Framework will be further improved and extended, based on experiences gathered during InSecTT project so far. Especially, it has a potential to multiply the project exploitation-oriented momentum and create valuable synergies with the pan-European value chain network – e.g. when shared with 136 EUs European Digital Innovation Hubs (EDIHs).



Figure 20: Fotos from two OIC events (InSecTT F2F and Interizon ICT)

### 3.3 Report of InSecTT Exploitation Activities in Y3

#### 3.3.1 InSecTT Exploitation Board

The InSecTT Exploitation Board (“EB”) was defined in InSecTT’s project proposal with the goal to foster innovation with InSecTT’s results. Confidentiality is ensured via PCA.

The Exploitation Board has an **advisory function** regarding the exploitation strategy and forms a natural interface between confidential exploitation plans created by the parties and all important stakeholders of InSecTT.

In short: Exploitation Board activities are focused on (increased) monetization of the project outcomes.

#### Tasks

- To support partners in **building commercially viable networks**, to establish value chains, and to address existing and new markets. This is done by, e.g., building relations to commercial clusters in EU countries (e.g. GreenTech Cluster in Austria, Interizon cluster in Poland)

- To **build liaisons** with other research projects (see 3.3.2) and initiatives, addressing stakeholders in new domains like aeronautics.
- To **analyses exploitation plans** provided by the parties and to **look for synergies** within and also outside the consortium.
- To **support the parties** in development of common **exploitation strategy** and **corresponding activities** that should be undertaken; and

The InSecTT Exploitation Board was formed and staffed according to Table 6.

Web Meetings to refine strategy and plan events and activities have been held every 4 to 8 weeks since March 2021.

Role	Institution	Name
two representatives of large enterprises nominated by the large enterprise Parties	PRE	Frank van de Laar
	AVL	Peter Priller
one representative of SMEs nominated by the SME Parties	CISC	Markus Pistauer
one representative of the academic/research Parties nominated by the academic/research Parties	GUT	Lukasz Kulas
the leader of WP6 “Commercial and Social Viability” who shall chair the Exploitation Board	AVL/GUT	Peter Priller, Mateusz Rzymowski, Lukasz Kulas
the leader of WP2 “Reliable AI / Machine Learning”	HALTIAN	Matti Vakkuri
the leader of WP3 “Components for Secure, Safe and Reliable Wireless Systems”	NXP-AT	Michael Jerne
the leader of WP4 “UC Orchestration and Quality”	GUT	Lukasz Kulas, Mateusz Rzymowski, Lukasz Szczygielski
the leader of WP5 “Cross-domain Use Cases”	Indra/GUT	Francisco Parilla, Lukasz Kulas, Mateusz Rzymowski
the leaders of the different use cases as foreseen in WP5		
T5.1 Wireless Platooning communications based on AI-enhanced 5G	Altran (now: Capgemini)	Diana Fernandes Rodrigues
T5.2 AI-enriched Wireless Avionics Resource Management and Secure/Safe Operation	ISEP	Ramiro Robles

Role	Institution	Name
T5.3 Wireless Security Testing Environment for smart IOT	AVL	Peter Priller
T5.4 Intelligent wireless systems for smart port cross-domain applications	GUT	Lukasz Kulas
T5.5 Smart and adaptive connected solutions across health continuum	PRE	Raja Ramachandran
T5.6 Location awareness for improved outcomes and efficient care delivery in healthcare	PRE	Frank van de Laar
T5.7 Intelligent Transportation for Smart Cities	Indra	Francisco Parilla
T5.8 Intelligent Automation Services for Smart Transportation	Indra	Francisco Parilla
T5.9 Cybersecurity in Manufacturing	ARCELIK	Osman Er
T5.10 Robust resources management for construction large infrastructures	ACCIONA	Juan Luis Bote
T5.11 Smart Airport	GUT	Mateusz Rzymowski
T5.12 Driver Monitoring and Distraction Detection using AI	RISE	Efi Papatheocharous
T5.14 Secure and Resilient Collaborative Manufacturing Environments	ABB	Björn Leander
T5.15 Intelligent Safety and Security of Public Transport in urban environment	LDO	Donatella Ansaldo
		Mario Plissetto
T5.16 Airport Security - Biometric OnTheMove	LDO	Donatella Ansaldo
		Francesco Calabro
		Filippo Cerocchi
ViF as coordinator	ViF	Michael Karner
External member	Airbus	Martin Kubisch

**Table 6 EB members during Y3**

The exploitation board started to identify relevant **Business Platforms** and to contact them in order to set up opportunities to present InSecTT exploitable items.

#### **Business Platforms already involved**

- **AIRBUS** (via EB member M. Kubisch)
- Mobility Cluster (Austria) <https://www.acstyria.com>
- Greentech Cluster (Austria) <https://www.greentech.at/>
- Interizon ICT Cluster (Poland)
- Maritime and Port Industry (Poland)

### 3.3.2 Project Liaisons

To strengthen InSecTT’s communication, dissemination, and exploitation opportunities, the EB together with InSecTT’s strategic board (SB) has established liaisons to other research projects, active in fields relevant to InSecTT:

#### 3.3.2.1 Liaison with ERATOSTHENES

This project focuses on IoT Trust and Identity Management Framework (<https://eratosthenes-project.eu>).



Figure 21 Logo of project ERATOSTHENES

#### 3.3.2.2 Liaison with DAIS

Project DAIS (Distributed Artificial Intelligence Systems, <https://dais-project.eu>) aims to bring faster, more secure and energy efficient data processing solutions through the development of edge AI software and hardware components. Collaboration is mostly organized on technical level via partners being in both consortia.



Figure 22 Logo of project DAIS

#### 3.3.2.3 AI-NET-ANIARA

AI-NET-ANIARA (“Automation of Network edge Infrastructure & Applications with aRtificial intelligence”), is an EU flagship project, focusing on edge / cloud applications in networks.

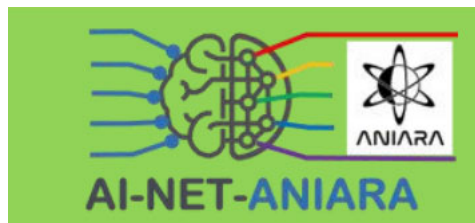


Figure 23 Logo of project AI-NET-ANIARA

### 3.3.3 Report on Patents

In total **four patents** were reported as coming from InSecTT, as listed in Table 7:

Title	Applicants	Reference
HALO – IR sensors (Patent)	TUE: Sujay Narayana, Vijay Rao, Ranga Rao Venkatesha Prasad	PCT/EP2021/054045
Hermes - Wind Energy Harvesting Wireless System for Sensing Angle of Attack and Wind Speed	TUE: Ranga Rao Venkatesha Prasad	P6102065NL
Fine-grained access control enforcement for industrial control systems using tokens, combining static roles with explicit permissions	ABB Schweiz AG	EP22155487.6
A channel sensing circuit and an apparatus comprising the circuit	Suryansh Sharma, Niels Hokke, Sujay Narayana, RangaRao Venkatesha Prasad"	P6108272NL

Table 7 Patents reported as of 2023-08-04

### 3.3.4 Report of Exploitable Foreground

The consortium is happy to report that in total **25** exploitable foreground items were identified per 2023-08-04, as listed in Table 8.

Title	By whom	Sector(s) of application	Potential/expected impact
Automated use case architecture alignment	ISEP	Industry in general	Automated trustworthiness metrics evaluation, validation and certification
OPEN-KTH: An open Lidar dataset of KTH campus Valhallavägen	KTH	Transportation, automated vehicles, road maintenance and operation, smart cities, and other innovative areas	Boost innovation, research and education in intelligent transportation, and in particular contributing to the KTH Digital Twin testbed based on AD-EYE
Network quality situation awareness	KAI	Industry networks, private wireless networks (4G/5G/WLAN).	This is expected to have a substantial impact on KAI's business and expanding the awareness of KAI and its products worldwide.

Title	By whom	Sector(s) of application	Potential/expected impact
Automated cybersecurity testing environment for wireless IoT in vehicles	AVL	Automotive Industry	Cybersecurity testing products will start a new segment in AVL's instrumentation & testing business (Instrumentation and Test Systems - Instrumentation and Test Systems - Content - avl.com)
Physical tamper attack detection algorithm	JKU	All kinds of wireless communication systems with fixed access points/base stations	Awareness in the scientific community, citation of our publication, could be applied in a commercial product if a company is interested. Potential increase of security and trust when operating wireless sensor networks
Physical Security Management platform / application with AI driven event detection engine	VEMCO	Large, industrial facilities / companies with critical infrastructure and hazardous zones.	Increase in the competitiveness of VEMCO's products portfolio. Covering additional area on security product market.
Digital Key Applet	NXP AT	primarily automotive; but can be extended to other IoT domains	ramp up of future car access systems easy as an end-2-end system is offered, certifiable system offered to the market, based on HW security certified products
ASN.1 encoded V2X messages - Converter for C/C++ and vice versa	VIF	Research and Development	Many people in R&D have to reinvent the wheel by creating a V2X message converter. We saw an opportunity to streamline that process, by offering a ready-to-use FOSS converter. Which brings out the name of VIF and adds the bonus of potential contribution to a central implementation.

<b>Title</b>	<b>By whom</b>	<b>Sector(s) of application</b>	<b>Potential/expected impact</b>
geoJSON server for location reporting	PRE	Research & Development, Logistics	Secured server solution based on geoJSON standard to exchange location data
FHIR server for healthcare data	PRE	Research & Development, Healthcare	Secured version of open source FHIR (R4) HAPI with token authentication.
Explainable AI in NXP eIQ Machine Learning	NXP NL	IoT, Industry	Increased competitiveness of NXP products
5G uplink data rate estimation	MTU	Intelligent Transportation Systems, Autonomous driving, any applications that require an estimation of available uplink resources	Provide estimations on available resources on 5G links. This can be used for load balancing, data traffic distribution and connection management, increasing the efficiency of resource usage.
Indoor navigation and localization app	JSI	Emergency logistic service, healthcare, building management	Increase efficiency of first responders in mass-casualty incidents, enable efficient indoor navigation with no gps signal
UWB weak-NLOS structured dataset	JKU	Research & Development, IoT	Comparability of NLOS detection algorithms. Could help other researchers to test their ranging/localization algorithms
UWB enabled sensor nodes for lab course	JKU	Education	Make students aware of indoor localization, various range estimation schemes and related issues.
Automated model learning system for cybersecurity checking	AVL	Potentially many; focus on automotive	Tremendous increase in the scalability of AVL's wireless security testing.

<b>Title</b>	<b>By whom</b>	<b>Sector(s) of application</b>	<b>Potential/expected impact</b>
CAN bus encryption protocol	NXP-AT	Automotive industry	easy start for interested customers doing a proof of concept of a smart car access system
UWB System Simulator	NXP AT	Automotive, Mobile, IOT	better understanding of future use cases and the requirements for future HW
Cloud-based ECG anomaly detection service	JSI	Health	Potential impact on health services development; potential solution for health related smartphone apps.
ICSSIM: An open-source generalizable framework for building customized virtual security testbeds for Industrial Control Systems (ICS)	RISE	Cybersecurity, IoT, Industrial Control Systems	Its open-source code repository has been already promoted by many users and has been approved and appreciated considerably by open-source community users.
ICSFlow: an open-source dataset for Intrusion Detection purposes.	RISE	Cybersecurity, IoT, Industrial Control Systems	It can be widely used by both academia and industry for developing AI models for Intrusion Detection purposes.
ML-driven Performance Anomaly Detection for time series datasets	RISE	IoT, Maritime (sensorized boats)	Impacting the maritime industry by addressing the challenge of making better sense out of data.
Quality Monitoring Platform	MarUn	Industry, Automotive, Smart City, Manufacturing, IoT	Provides smart services for network operators, and data from the network and services' performance in real-time.



Title	By whom	Sector(s) of application	Potential/expected impact
F-Secure SENSE container-based solution for connected home IoT security	FSC	Smart homes together with telecommunications operators and router manufacturers	Economic impact: aiming at market leadership in the target market. Societal impact: cyber resilience for smart homes.

Table 8 Exploitable Foreground reported by 2023-08-04

### 3.4 Evaluation of performance indicators and suggested improvements

Table 9 provides an overview of the KPIs defined in [1] and its actual measured value at the end of the project.

For some KPI's, [1] defines multiple sources in a sub-structure (e.g. KPI 1.1a "Ranking on Google search term "Intelligent Secure Trustable Things"; KPI 1.1.b same, but on Qwant. KPI 1.1.c: same, but on Baidu). For better readability, **only the first** of these sub-values is reported (in this example: only the Google ranking). Full information for all values can be found in Table 2 and Table 3.

For activities with performance indicators not meeting the initially planned goals, mitigation and improvements are suggested in section 3.4.1

KPI#	Objective D6.1 Section	Definition	Defined goal	Actual value
1.1	Accessible project website and social network channels 3.1.2, 3.1.3	Ranking of search term "INSECTT"	1 <sup>st</sup>	1
1.2		Ranking of search term "Intelligent Secure Trustable Things"	1 <sup>st</sup>	1
1.3		Ranking of search term "intelligent secure trustworthiness framework"	Ranked 10 <sup>th</sup> or better	11
1.4		Ranking of search term "intelligent secure trustworthy systems"	Ranked 10 <sup>th</sup> or better	1
1.6		Followers on LinkedIn	100	286
1.7		Subscribers on Facebook	100	117
1.8		Followers on ResearchGate	50	Discontinued by RG
1.9		Followers on Twitter/X	100	74

1.10		Subscribers on YouTube	100	35 Expected to rise at the end of the project (large number of demonstrator videos!)
1.11		Followers on Instagram	100	77
2.1	Efficient collaboration infrastructure for partners / 3.1.4	Number of SharePoint users	200	372
2.2		Number of SharePoint documents	500	>4700
3.1	Plan, support, and foster exploitation  3.1.6	Number of press conferences	2* <sup>1</sup>	1 + 1 planned
3.2		Number of ECSEL events participated	3*	2 (EF ECS) + 2 online (ARTEMISIA)
3.3		Number of hackathons held	1*	1 (Open Innovation Contest)
3.4		Number of Use Case booklets fabricated	1*	1
3.5		Number of Use Case markets held	2*	2
4.1	Empower high-quality dissemination  3.2.4	Number of journal papers	7*	50 (total)
4.2		Number of conference papers	30*	82 (total)
5	Regular reports of dissemination and exploitation results	successful submission of deliverables D6.3, D6.5 and D6.7	D6.3 D6.5 D6.7	D6.3 D6.5 D6.7

Table 9 KPI Overview and Y3 Evaluation

\* Aggregated number for full project time (36 months) given

### 3.4.1 Suggestions for Improvements in Y3

The following Table 10 lists explicitly the recommendations for the last year as defined after Y2 in D6.5, and how they have been addressed in Y3.

Suggestion #	Issue	Suggested improvement	Result in Y3
1	Increase number of Followers on ResearchGate (plan: 50 current: 21)	Promote in the research community (conferences, summer school, ...)	In total, 6 summer school activities were reported. Strong dissemination (82 conference papers)
2	Increase number of Followers on Twitter (plan: 100 current: 74)	Ask followers to actively re-tweet; promote feed on exploitation events	Networking (eg follow-back) done on LinkedIn
3	Increase number of Followers on YouTube (plan: 100 current: 33)	Create more content (movies) from InSecTT material	Expected to rise at the end of the project (large number of demonstrator videos!)
4	Increase number of Followers on Instagram (plan: 100 current: 77)	Create more content (pictures) from InSecTT material; promote in communities	further content was posted
5	Participate at ECSEL events (planned: 6; current: 1)	Participate as ECSEL events become accessible again (currently restricted due to COVID)	Participated at the EF ECS 2022 Several articles in ARTEMISIA newsletter
6	Organize hackathon (planned 1, currently 0)	will be organized in Y3 of project	Open Innovation Contest started

**Table 10 Summary of suggested improvement actions in InSecTT for Y3**

## 3.5 The InSecTT Book: Intelligent Secure Trustable Things

One of the main results in Dissemination (as well support of Exploitation) is the release of the Book “Intelligent Secure Trustable Things”:

- **Series title:** Studies in Computational Intelligence
- **Book title:** Intelligent Secure Trustable Things
- **Originator type (author or editor):** Editor
- **Names, affiliations, email addresses and sequence of the authors/editors:**
  - Michael Karner, Virtual Vehicle Research GmbH, Graz, Austria
  - Johannes Peltola, VTT, Oulu, Finland

- Michael Jerne, NXP Semiconductors Austria GmbH & Co. KG, Gratkorn, Steiermark, Austria
- Lukas Kulas, Politechnika Gdańska, Gdansk, Poland
- Peter Priller, AVL List GmbH, Graz, Austria

- **Marketing text:**

Artificial Intelligence of Things (AIoT) is the natural evolution for both Artificial Intelligence (AI) and Internet of Things (IoT) because they are mutually beneficial. AI increases the value of the IoT through machine learning by transforming the data into useful information, while the IoT increases the value of AI through connectivity and data exchange. Therefore, InSecTT – Intelligent Secure Trustable Things, a pan-European effort with over 50 key partners from 12 countries (EU and Turkey), provides intelligent, secure and trustworthy systems for industrial applications to provide comprehensive cost-efficient solutions of intelligent, end-to-end secure, trustworthy connectivity and interoperability to bring the Internet of Things and Artificial Intelligence together. This book provides an overview about results of the InSecTT project. InSecTT creates trust in AI-based intelligent systems and solutions as a major part of the AIoT. InSecTT fosters cooperation between big industrial players from various domains, a number of highly innovative SMEs distributed all over Europa and cutting-edge research organisations and university. The project features a big variety of industry-driven use cases embedded into various application domains where Europe is in a leading position, i.e. smart infrastructure, building, manufacturing, automotive, aeronautics, railway, urban public transport, maritime as well as health. The demonstration of InSecTT solutions in well-known real-world environments like airports, trains, ports, and the health sector shows their applicability on both high and broad level, going from citizens up to European stakeholders.

The first part of the book provides an introduction into the main topics of the InSecTT project: How to bring Internet of Things and Artificial Intelligence together to form the Artificial Intelligence of Things, a reference architecture for such kind of systems and how to develop trustworthy, ethical AI systems. In the second part, we show the development of essential technologies for creating trustworthy AIoT systems. The third part of the book is composed of a broad variety of examples on how to design, develop and validate trustworthy AIoT systems for industrial applications (including automotive, avionics, smart infrastructure, healthcare, manufacturing, and railway). This is an open access book.

The book is structured into three chapters, with subchapters shown in Table 11.

Subchapter	Main Chapter	Estimated Number of pages
Going to the edge: bringing Artificial Intelligence and Internet of Things together	1 Introduction	10
The Development of Trustworthy AI Systems Requires a Holistic, Human-Centered Research and Development Approach: A White Paper	1 Introduction	15
Reference architecture for AIoT systems	1 Introduction	15

<b>Subchapter</b>	<b>Main Chapter</b>	<b>Estimated Number of pages</b>
Structuring the Technology Landscape for successful innovation in AIoT	1 Introduction	15
InSecTT Technologies for the enhancement of Industrial Safety and Security	2 Technology Development	20
Algorithmic and Implementation-based Threats for the Security of Embedded Machine Learning Models	2 Technology Development	17
Explainable anomaly detection in medical signals with deep learning	2 Technology Development	15
Indoor navigation with smartphone	2 Technology Development	8
Reconfigurable Antennas for Trustable Things	2 Technology Development	15
AI-enhanced connection management for cellular networks	2 Technology Development	12
Vehicle CAPTAIN - a V2X platform for research and development	2 Technology Development	10
AI-enhanced UWB-based localization in wireless sensor networks	2 Technology Development	15
Approaches for automating cybersecurity testing of connected vehicles	3 Industrial Applications	15
Solar-based Energy Harvesting and Low-power Wireless Networks	3 Industrial Applications	15

<b>Subchapter</b>	<b>Main Chapter</b>	<b>Estimated Number of pages</b>
Location solutions in healthcare to improve workflow efficiency	3 Industrial Applications	30
Driver Distraction Detection Using Artificial Intelligence and Smart Devices	3 Industrial Applications	12
Working with AIoT solutions in embedded software systems. Recommendations, guidelines, and lessons learned.	3 Industrial Applications	15
AI for wireless avionics intra-communications	3 Industrial Applications	15
Use of artificial intelligence as an enabler for the implementation of ETCS L3 and other innovative rail services	3 Industrial Applications	15
Innovative solutions for maritime infrastructures monitoring and protection	3 Industrial Applications	10
Security of Wireless IoT in Smart Manufacturing: Vulnerabilities and Countermeasures	3 Industrial Applications	15

**Table 11 Main structure (chapter, subchapters) of the InSecTT Book**

## 4 CONCLUSIONS

This document summarizes communication, dissemination, and exploitation activities of InSecTT during the third year (M25-M39) of project work. Results are validated and whenever possible measured using performance indicators and compared with the plan laid out in D6.1 at the beginning of the project. Focus in Y3 was on continuing to raise awareness for dissemination and to support and strengthen exploitation activities and opportunities.

A main highlight in this respect is the upcoming publication of the InSecTT book “*Intelligent Secure Trustable Things*” as open access (Springer, Series: Studies in Computational Intelligence).

Efficient means were implemented for both communication within the project (SharePoint) and to the outside (Web site, social media presence). Scientific dissemination picked up strongly, with 70 publications (adding to the 50 reported in Y2, and another 38 reported from Y1), promoting InSecTT to appropriate communities.

In addition, an impressive number of **99 dissemination activities** have been reported in Y3, adding to 61 from Y2 and additionally 72 activities from Y1. A complete list of events from Y3 is given in Table 5, and includes also information about summer schools on Trustable AI, and related activities.

The evaluation of the performance indicators indicated that almost all planned KPI’s were met or exceeded.

The consortium has identified a total of **25 exploitable foreground items**, with **4 patent applications**. Project partners have described in detail the roadmap towards exploitation of their results (see WP5 final deliverables, D5.55 - D5.71 (“Use Case progress report Y3 for Task x”).

## 5 REFERENCES

- [1] D6.1: Initial Plan for Communication, Exploitation and Dissemination of Results (PCEDR), the InSecTT consortium, released 2020-10-29
- [2] D6.3 Year 1 Report on Communication, Exploitation and Dissemination of Results (PCEDR), the InSecTT consortium, released 2021-07-14
- [3] Call H2020-ECSEL-2019-1-IA-two-stage – Innovation Actions (IA) Stage 2: Full Project Proposal InSecTT, the InSecTT consortium, September 2019



## A. ABBREVIATIONS AND DEFINITIONS

<b>Term</b>	<b>Definition</b>
AIoT	Artificial Intelligence of Things
CfP	Call for Papers
EB	Exploitation Board
PCEDR	Plan for Communication, Exploitation and Dissemination of Results