



DIAS

Smart Adaptive Remote Diagnostic Antitampering Systems

EUROPEAN COMMISSION

HORIZON 2020

LC-MG-1-4-2018

Grant agreement ID: 814951

Deliverable No.	D6.4
Deliverable Title	Dissemination Report (final)
Issue Date	16/11/2022
Dissemination level	Public
Main Author(s)	Dimitrios Kontses (LAT/AUTH) Alexandros Papageorgiou-Koutoulas (LAT/AUTH) Ilias Vouitsis (LAT/AUTH)
Version	V1.0

DIAS Consortium



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 814951.

This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

Executive summary

The purpose of this deliverable is to present a report of the communications and dissemination activities that have been conducted within the whole period of the DIAS project or else 38 months in total i.e. September 2019 to October 2022. These activities aimed to maximise the impact of the project and position it among different stakeholders such as industry, research and academic community, media and the general public.

The current deliverable is the final Dissemination Report giving an overview of all dissemination actions of the DIAS project through traditional communication channels such as events/conferences, project publications, social media posts and project presentations (to various stakeholders and the general public). In this context, visibility and social media engagement data are also provided.

The DIAS consortium participated in a total of 14 conferences and made 16 presentations about the project reaching an estimated audience of more than 2000 people. Moreover, the DIAS consortium organised two hackathons where participants came up with creative technical ideas to find attack vectors that can be exploited to make tampering business out of them in environmental protection systems which have adopted the anti-tampering solutions developed in DIAS. One final dissemination event was also organised by the DIAS consortium a few days before the official end date of the project (i.e. on 25th October 2022). At this event, the DIAS colleagues along with representatives from other EU projects in synergy with the DIAS project presented and discussed with the industry, academic and general public representatives the findings regarding vehicle EPS tampering.

Furthermore, the website has been updated to offer content according to the current status and progress of the project. Moreover, the social media account (Twitter) has been essential to engage with stakeholders and share the latest updates about the DIAS project, reaching in total 28 posts and 79 followers. Finally, since the last dissemination report (February 2022), communication material has been greatly extended including:

- 2 new leaflets
- 2 newsletters
- 1 2-pager
- 2 videos
- 1 dissemination pack

Contents

Executive summary	3
List of Figures	5
List of Tables	5
1 Introduction	6
2 Dissemination and Communication Strategy	7
2.1 Implementation of the strategy.....	8
2.2 Overview of activities.....	10
3 Dissemination and exploitation activities.....	12
3.1 DIAS Website.....	12
3.1.1 Content	12
3.1.2 Statistics	13
3.2 Social media	15
3.3 Communication Material	20
3.3.1 Project Templates: PPT, Word	20
3.3.2 Leaflets.....	20
3.3.3 Newsletter.....	22
3.3.4 2-pager and journalistic project description.....	24
3.3.5 Videos.....	24
3.3.6 Fact sheet.....	27
3.3.7 Dissemination pack.....	27
3.4 Events (Conferences, exhibitions, presentations, etc)	27
3.5 Publications.....	31
4 Conclusions	36

List of Figures

Figure 1: Phases for the Communication and Dissemination strategy.....	7
Figure 2: Overview of DIAS website statistics for the last year of the project i.e. September 2021 to October 2022 (indicatively).....	14
Figure 3: Top tweets from 1 st year of the project (November 2019 to October 2020).....	16
Figure 4: Top tweets from 2 nd year of the project (November 2020 to October 2021).....	17
Figure 5: Top tweets from 3 rd year of the project (November 2021 to October 2022).....	18
Figure 6: Visits in DIAS Twitter account.....	20
Figure 7: DIAS 1 st leaflet.....	21
Figure 8: DIAS Hackathon part 1 leaflet.....	22
Figure 9: DIAS Hackathon part 2 leaflet.....	22
Figure 10: Cover page of the first DIAS newsletter (February 2022).....	23
Figure 11: Cover page of the second DIAS newsletter (October 2022).....	24
Figure 12: DIAS project film.....	26
Figure 13: DIAS demonstrator truck video.....	27

List of Tables

Table 1: Dissemination actions of the DIAS project.....	11
Table 2: Advisory Board members.....	11
Table 3: Basic analytics per tweet.....	15
Table 4: Analytics of DIAS Twitter account (Note: updates compared to the previous dissemination report are in blue font).....	19
Table 5: Events (Note: updates compared to the previous dissemination report are in blue font)	28
Table 6: Papers (Note: updates compared to the previous dissemination report are in blue font)	31
Table 7: Public DIAS deliverables (Note: updates compared to the previous dissemination report are in blue font).....	34

1 Introduction

The main purpose of this deliverable is to report the various activities that have been performed within Task 6.2: Dissemination & Exploitation activities [M4-M36], as well as to present an overview of the communication and dissemination strategy and its effectiveness over the whole DIAS reporting period comprehending M1-M38. Since this is the final deliverable addressing Task 6.2, it revises and summarizes all the dissemination and exploitation activities, and in turn, to this extent, it contains and complements all the information presented in the previous dissemination-related deliverable D6.3.

It is worth notable that due to Covid – 19 pandemic it was not always feasible to execute the different dissemination and communication activities in alignment with the technical development of the project, the milestones achieved, and the communication needs of each stage concerning the exploitation strategy and sustainability plans as originally planned in *Grant Agreement-814951-DIAS*. However, several actions have been performed to disseminate the project's results during the whole DIAS project period. Activities included publications, presentations, participation in events, presence and engagement in social media and the establishment of contacts with interested developers. The actions are either managed by the consortium (e.g. social media accounts, website, communication material) or hosted by external actors (e.g. conferences, events, web articles).

The relevant description of the D6.4 deliverable found in *Grant Agreement-814951-DIAS* (p. 115) is the following:

“ This report will not be open to the public since it will contain information on tampering methods that may assist tampering efforts in the market. It will contain all communication and data collected during the project to assist Commission Services and Officers for future legislative procedure needs. ”

2 Dissemination and Communication Strategy

This chapter briefly describes the dissemination and communication strategy followed. The corresponding objectives were defined as:

- *General objective:* Position DIAS among its stakeholders as a transparent and secure platform for building social networks, through the development and execution of a strategy involving creative actions that generate visibility, awareness, and impact of the project results.
- *Specific objectives:*
 - Implement a digital strategy through the execution of online communication activities including website and social media channels, targeting key audiences for the project to generate project/brand recognition;
 - generate online and offline visibility of the project by creating valuable and relevant content in different formats, related to the project activities and results, to be shared through DIAS channels;
 - maximise interest and impact among target audiences to generate engagement, interaction and feedback on different channels defined, which could lead to further business opportunities.

The dissemination & exploitation activities were planned in an iterative way – from an outline in the DoW, through the kick-off meeting discussions and further identification of activities and the development of methodology (presented in the initial dissemination report D6.2); however, these activities were constantly rearranged considering the course of the program but also external conditions and constraints (i.e., Covid 19 pandemic).

At the beginning of the project, we defined the goals to be achieved by the dissemination & exploitation strategy by answering the following five questions:

- what will be disseminated? – the message to be sent;
- to whom? – the audience;
- why? - the purpose;
- how? - the method;
- when? - the timing.

In D6.2 we loosely defined three phases for the Communication and Dissemination strategy in relation to the technical roadmap and the most important milestones of the project, which at the same time are aligned with each one of the objectives to deliver a comprehensive strategy.

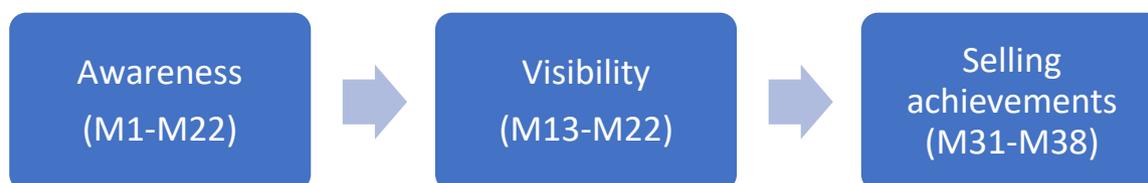


Figure 1: Phases for the Communication and Dissemination strategy

During the first phase, we worked on generating awareness about the project, its objectives, and expected outcomes through different channels, and on identifying key stakeholders to consolidate a strong message for the potential interest and relation of our target audiences. This has allowed us to position the project among stakeholders and the general public for fostering valuable relationships in the upcoming phases where technical results were available.

In terms of the development of activities, DIAS has participated in several events and conferences to present the project, with dissemination material that allowed us to gain visibility and deliver a consistent message about what DIAS is and will be. In addition, the digital network has been an essential channel to amplify the reach to stakeholders, always placing first a creative and relevant content strategy.

In the visibility phase of the strategy, we had been focusing on communicating the preliminary results of the project of different WPs. In the second half of this phase as well as in the selling achievements phase, the storytelling around DIAS was formed based on the demonstration of their tampering countermeasure success in events and webinars. Also, the publication of scientific papers was foreseen to increase the visibility of the results of the projects and foster relations for the future. In addition, the consortium generated more dissemination material with a special focus on promoting the results in a friendly way through the development of videos targeting developers and end-users to promote and demonstrate the capabilities of DIAS.

The last phase of the strategy was focused on maximising the impact of DIAS results by bringing the operation of these systems to the community by means such as conferences, scientific publications networking activities and encouraging outside observers to check, test and use the results of DIAS. The project involved the execution of specific activities such as hackathons, webinars, and forums to reach the identified target groups.

At this point, it is important to mention that there was some impact on the strategy due to Covid-19, as until now some events where we were planning on participating have been cancelled or postponed and restrictions did not make possible the organisation of events for large audiences. Nevertheless, participation in virtual events and webinars whenever possible allowed us to continue with the plan to reach our stakeholders, while at the same time, strengthening our presence on Twitter with relevant posts.

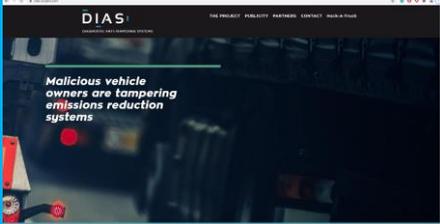
2.1 Implementation of the strategy

Material, targets, actions and channels were described in D6.2 as the answers to the above five questions in order to reach the objectives related to awareness, visibility and engagement and selling achievements. The participation of the DIAS partners in all these activities had been fundamental in order to deliver a unified message of what we developed and the expected benefits for both developers and users.

Initially, some channels were identified and had been used to communicate DIAS messages, but along the way, we incorporated some others that contribute to generating more impact and engagement with key stakeholders.

The following table describes the whole system of channels used currently in the communication and dissemination strategy:





DIAS website-
<https://www.dias-project.com/>

Presents the vision and the most important information about DIAS as the main informative channel



Newsletter

Newsletter issued by the project to distribute the progress of the public WPs and dedicated articles about specific topics and milestones of the project



Partners' external and internal communication channels

We have strived and encouraged partners to share and communicate DIAS messages/results on both personal and corporate accounts (websites, social media, communication offices etc)

2.2 Overview of activities

Even if not as intense as expected due to several restrictions imposed in response to the Covid 19 – pandemic, significant effort has been given in the communication and dissemination activities of DIAS on a both physical and digital level.

The adjacent table presents a summary of all the communication and dissemination activities performed until now. More information about each one of the categories can be found in the next chapter.

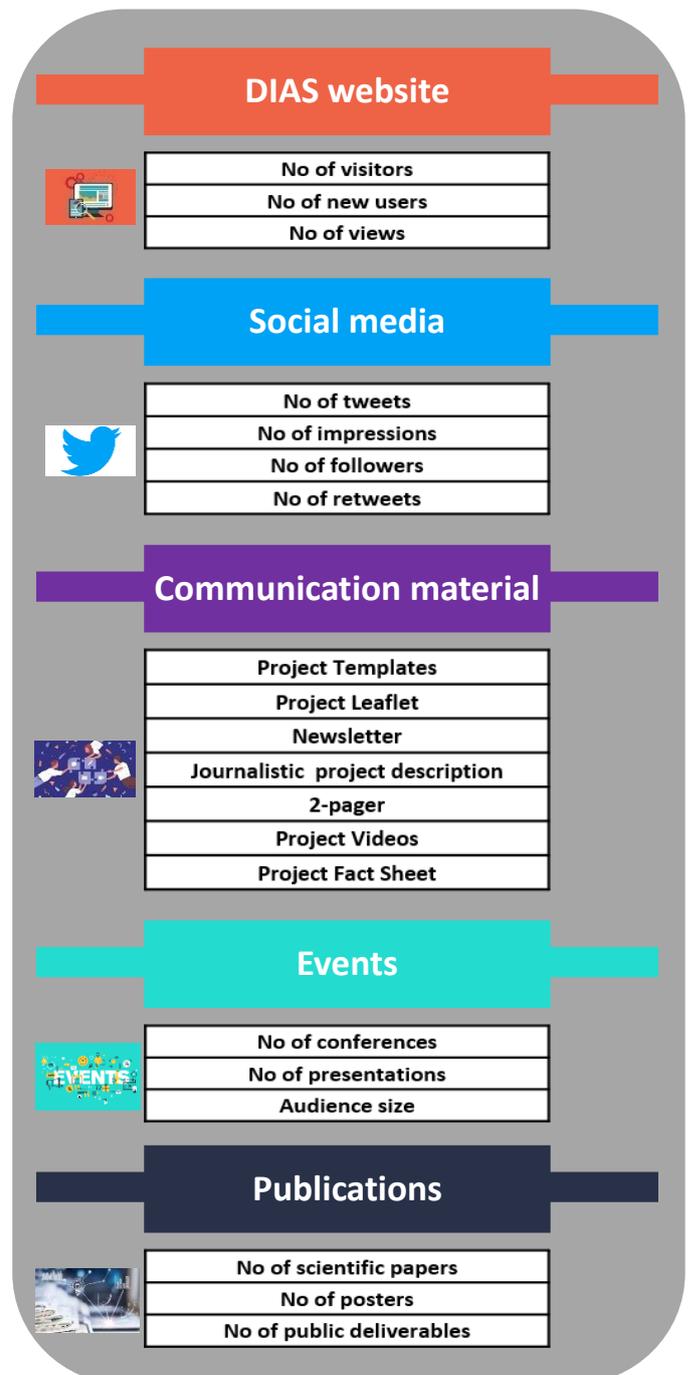


Table 1: Dissemination actions of the DIAS project

Type of action	Count
Web article	5
Local event	3
Conference paper	16
Hackathon	2
Open data pilot	0
Conference presentation or poster	18
Webinar	2
Interview	0
Social Media (Tweet)	28
Panel presentation	0
Press Release	0
Scientific paper	22
TV, Radio, YouTube	2

Additionally, to obtain technical support and advice, DIAS partners have contacted the Advisory Board (AB). The AB consists of a limited number of external experts that have been selected based on their profound and long-lasting expertise in the field of research (Table 2). The AB members are invited to general progress meetings of the project or technical WP meetings where they can advise the consortium and help DIAS to address and overcome technical issues that may arise.

Table 2: Advisory Board members

Name	Affiliation
Alexander Kleiser	ACEA
Paul Greening	ACEA

3 Dissemination and exploitation activities

This chapter presents more detailed information about the performance and activities carried out within Task 6.2.

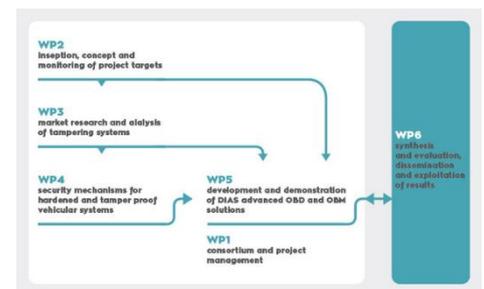
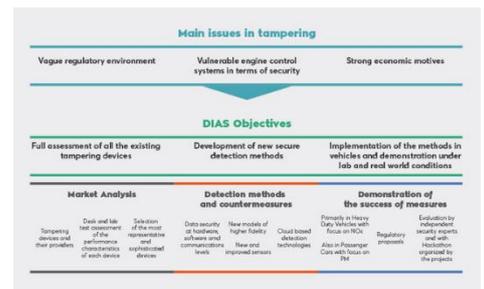
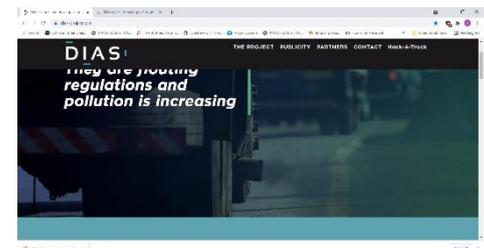
3.1 DIAS Website

DIAS website is the backbone of the project dissemination and communication strategy as it provides useful information about the project, progress, and activities done to different target audiences. The website was launched in December 2019 and consists of publicly accessible webpages which offer a general overview of the project, its methodology, workflow, partnership, and exploitation group.

3.1.1 Content

In terms of content, the website has the following sections:

- **Home page** (<https://dias-project.com/>): This section offers a comprehensive view of the different sections of the website and the content available with short and attractive descriptions of each one and internal links to facilitate the navigation and improve our SEO¹ score. The homepage also has a feed on Twitter, the latest news published, a carousel with partners' logos, and contact information.
- **The project**: This section is dedicated to the presentation of the project's objectives (<https://dias-project.com/objectives>), impacts (<https://dias-project.com/impacts>) and methodology (<https://dias-project.com/work-packages>).
- **Publicity** (<https://dias-project.com/dias-twitter-feed>): This section contains all the information related to participation at events, conferences, poster presentations, press releases, articles published, newsletters, deliverables (17 of them available in full text), videos, newsletters and any other type of material produced in terms of communication such as leaflets, roll-up, infographics, etc. In terms of new content, this section is being updated regularly, which contributes to the SEO positioning of the website, and helps us to have new content to post on social media.
- **Partners** (<https://dias-project.com/partners>): This section shows a map of the location of each member of the consortium, a short description of what makes the DIAS consortium unique and the description of each one of the participants with links to each website to improve the link-building strategy.
- **Contact** (<https://dias-project.com/contact-us>): This section contains contact information (with the project coordinator



¹ measure of how well the user-facing and technical aspects of your site contribute to search engine optimization, and ultimately, higher rankings and organic traffic



and project manager) for the public users to write to us directly and subscribe to the newsletter.

- *Hack-A-Truck part 1* (<https://dias-project.com/Hack-a-Truck-part-1>) and *part 2* (<https://dias-project.com/Hack-a-Truck-part-2>): This section is specifically devoted to the hackathons 1 and 2 of the project, held on May 2021 and March 2022 in the context of demonstration of Level 0, 1 and 2 solutions.

3.1.2 Statistics

An overall insight into the DIAS website's main statistics can be taken from Figure 2. Results shown in the figure concern the last year of the project (September 2021 to October 2022) and they are a representative example of the whole project's period. To extract these statistics Google Analytics was used (<https://analytics.google.com/>).

To better understand the results, the definitions of the basic terms used are provided below (alphabetically sorted):

- **Bounce Rate:** The percentage of sessions that last less than ten seconds with the user having no interaction with the page. By principle, these sessions include a one-page view.
- **New User:** User who visited the site for the first time. An individual can appear as a new user twice over the course of two sessions.
- **New Visitor:** User who visited the site for the first time. An individual can only appear as a new visitor once.
- **Pageview:** A pageview is reported when a user on the website has viewed a page. Pages are ordered by popularity based on views in the Google Analytics pages and screens report by default. This allows seeing which content is being viewed most often.
- **Returning Visitor:** User who visited the site at least 2 times in the past 2 years
- **Sessions:** The time a user is actively engaged with the website. When this time is zero the session is called a **bouncing session** which means the user had no interaction with the page and is not counted as a user or visitor. The default session timeout is 30 minutes, which means that if someone is inactive on the website for over 30 minutes, a new session will be reported if they perform another action, for example, viewing another page.
- **User:** An individual who interacts with the website. Each user can visit the website multiple times. For example, one user could create three sessions on the website, with each session containing multiple page views.

During the last year (or more specifically over the last 13 months), 1563 people visited the DIAS website for the first time (circa 120 per month) while the average session duration was about 2 minutes. Since the bouncing rate is near 60%, it can be concluded that about 4 out of 10 single-page engagements had the viewer spending some time learning more about the project. Furthermore, 313 users had visited the site at least 2 times in the past 2 years (Returning Visitors). Finally, the two most visited pages of the website were the home page and the page with the hackathons content. The great increase in users and other statistics observed early in 2022 can be attributed to the DIAS 2nd hackathon event conducted in March of 2022.

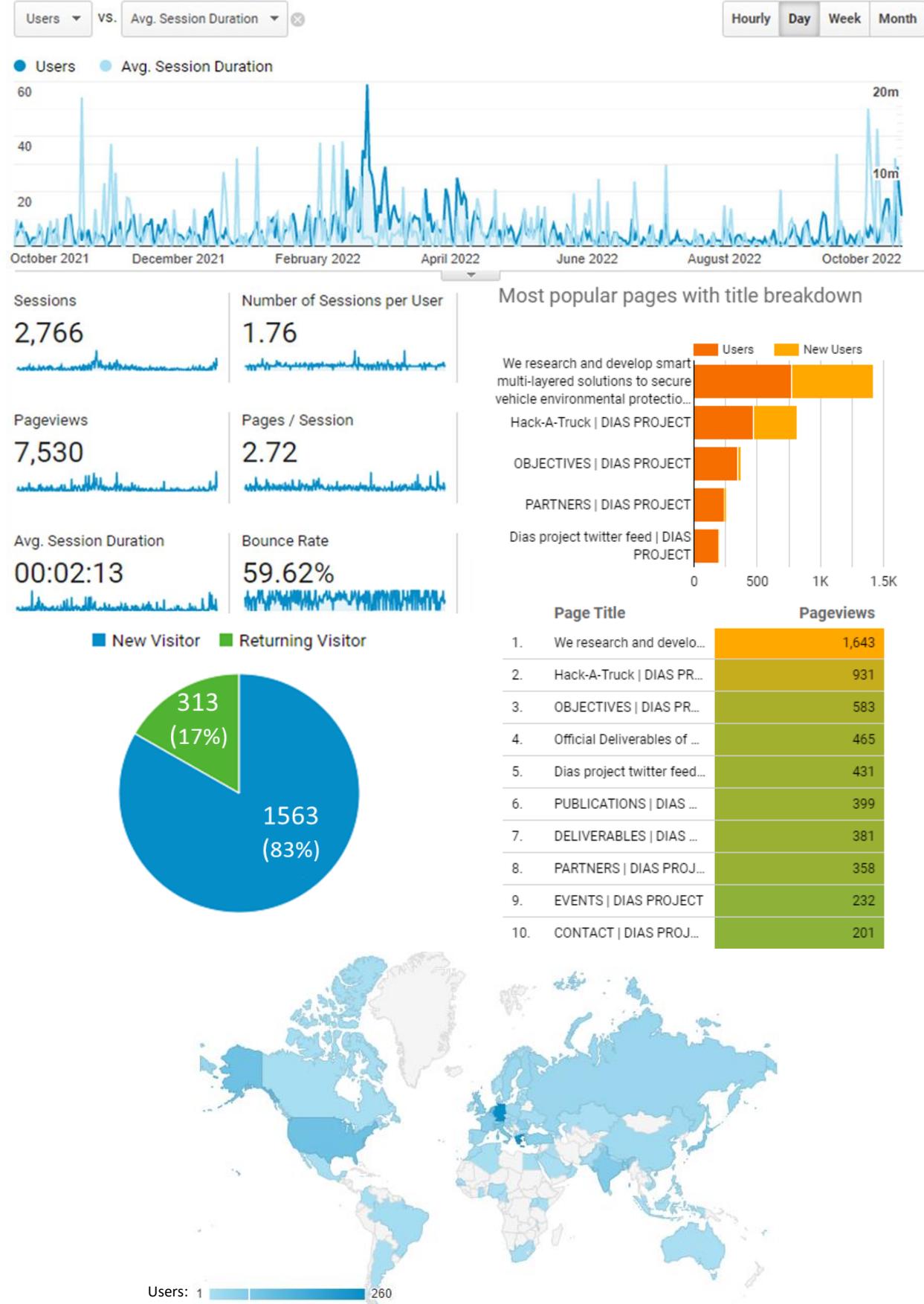


Figure 2: Overview of DIAS website statistics for the last year of the project i.e. September 2021 to October 2022 (indicatively)

3.2 Social media

Twitter is the social medium used by DIAS to disseminate news about the project, such as presentations of the project at conferences, in public or partner events, progress in the objectives and to share the newsletter. The definitions of the key terms on Twitter are briefly displayed below in alphabetical order:

- **Engagement:** The total number of times a user interacted with a tweet. This includes clicking anywhere on the tweet, including retweets, replies, followings, likes, etc.
- **Follow, Follower:** Following someone on Twitter means subscribing to their tweets or messages. A follower is someone who follows or subscribes to another person's tweets.
- **Impression:** Times a user is served a Tweet in timeline or search results regardless of whether they read it or interact with it.
- **Mention:** Refers to a tweet that includes a reference to any Twitter user by placing the @ symbol in front of their username (e.g. @username). Twitter tracks mentions of users when the @ symbol is included in the message.
- **Profile Visit:** The number of visits to a Twitter profile.
- **Retweet:** As a noun, a retweet is a tweet that had been forwarded or "resent" on Twitter by someone but was originally written and sent by someone else. Used as a verb, retweet means to send someone else's tweet to your followers. Retweeting is a common activity on Twitter and reflects the popularity of individual tweets.
- **Tweet:** A message posted (or the act of posting a message) on Twitter with 280 or fewer characters. It is also called a post or an update.

DIAS project joined Twitter (@DIAS_project) in November 2019 and has 79 followers. The most important analytics per tweet can be found in Table 3 while Figure 3, Figure 4 and Figure 5 represent some examples of the top tweets through the 3 years long project period (November 2019 to October 2022).

Table 3: Basic analytics per tweet

Tweet posted at:	Impressions	Engagements	Likes	Retweets
6:30 pm, Dec 9, 2019	1002	28	3	0
6:33 pm, Dec 9, 2019	1741	213	5	2
May 24, 2020	848	22	3	1
Jun 12, 2020	964	37	5	1
Sep 9, 2020	864	47	5	1
Oct 13, 2020	802	42	5	1
Nov 16, 2020	1922	27	6	5
Nov 25, 2020	1054	50	6	3
Nov 30, 2020	682	20	2	1
Mar 5, 2021	505	26	1	0
Mar 6, 2021	504	30	2	1
Jun 24, 2021	454	34	2	1
Sep 15, 2021	286	17	0	0
Nov 19, 2021	286	29	3	1
Dec 13, 2021	205	2	0	0
Jan 21, 2022	308	31	8	2

Feb 3, 2022	211	14	3	0
Feb 14, 2022	23249	54	19	2
Feb 17, 2022	788	60	13	6
Feb 23, 2022	149	12	2	0
Mar 2, 2022	282	12	4	4
Mar 29, 2022	217	10	5	1
Mar 31, 2022	166	28	4	0
Apr 8, 2022	651	149	7	5
Apr 29, 2022	157	13	4	0
Jun 10, 2022	134	24	2	1
Oct 16, 2022	126	21	2	2
Oct 20, 2022	64	13	2	1

DIAS project @DIAS_project · Dec 9, 2019
 DIAS kick-off meeting (23–24/10, 2019, Thessaloniki) was a great opportunity for DIAS partners and @inea_eu project officer Dr. Kousoulidou @MarinaKslid to present their targets and ambitions and start working towards anti-tampering systems!
[#H2020](#) [#InvestEU](#) [#ResearchImpactEU](#)



Promote

2 5

DIAS project @DIAS_project · Jun 12, 2020
 Our truck test platform is ready for use. 🧠🔧🚚
 Fitted with specialized measurement equipment, our test platform will be used to study the operating principles of tampering devices and their effect on the vehicle's behavior and emissions.
[#H2020](#) [#InvestEU](#) [#ResearchImpactEU](#)



Promote

1 5

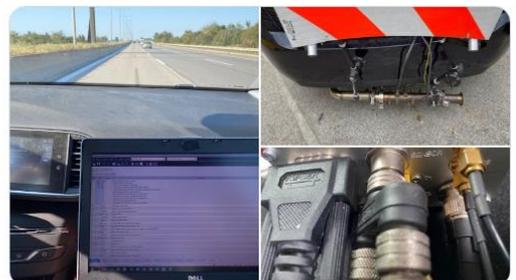
DIAS project @DIAS_project · Sep 9, 2020
 We are glad to announce that after successfully completing the first round of tests on tampering devices, our demonstrator Ford F-MAX truck has completed its return trip from TNO, Netherlands to Bosch, Germany.
[#H2020](#) [#InvestEU](#) [#ResearchImpactEU](#)



Promote

1 1 5

DIAS project @DIAS_project · Oct 13, 2020
 Our team is currently evaluating the performance of commonly used tampering devices and services. Having applied the tampering modifications to our test vehicle, we make use of specialized sensory equipment to record and analyze its road performance and emissions. 🚗📡📊



Promote

1 5

Figure 3: Top tweets from 1st year of the project (November 2019 to October 2020)

DIAS project @DIAS_project · Nov 16, 2020

First distributed DIAS Online Hackathon with 9 partners successfully concluded. CAN-to-Cloud solution using @EclipseFdn KUKSA stack eclipse.org/kuksa/ #H2020 #InvestEU #ResearchImpactEU 🚗 📶 🌐



Promote

🗨️ 5 ❤️ 6 📶 📊

DIAS project @DIAS_project · Nov 25, 2020

JRC team @EU_ScienceHub contributing to the project DIAS by measuring emissions from tampered NRRM engines. Helping build a low-emissions, sustainable future. 🚗 📶 #EUknowledge #EUscience #DIAS_project

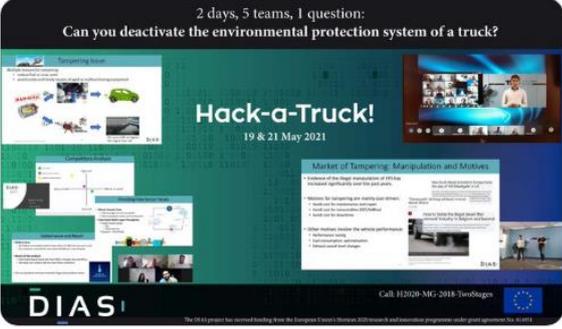


Promote

🗨️ 1 🔄 3 ❤️ 6 📶 📊

DIAS project @DIAS_project · Jun 24, 2021

Hack-A-Truck!
 During the 1st DIAS Hackathon, participants came up with creative technical ideas to find attack vectors and make tampering business out of them. A public report is currently prepared with all findings. Stay tuned! dias-project.com/Hack-a-Truck #H2020 ##ResearchImpactEU



Promote

🗨️ 1 ❤️ 2 📶 📊

Figure 4: Top tweets from 2nd year of the project (November 2020 to October 2021)

DIAS D6.4 Dissemination report (final), v1.0

DIAS DIAS project @DIAS_project · Nov 19, 2021
 Eclipse SAAM Best Paper Award for a DIAS-related study: "Eclipse KUKSA.val for SCR Anti-Tampering Monitoring in Heavy Vehicles". Congratulations to Bosch colleagues! eclipse.org/kuksa/blog/202... #H2020 #InvestEU



DIAS DIAS project @DIAS_project · Jan 21
 The start of 2022 found our partners at UMFST working hard on the demonstrators destined for the second Hack-A-Truck hackathon 🚀 Watch your step! There are works in progress here! 🛠️ #H2020 #InvestEU



DIAS DIAS project @DIAS_project · Feb 14
 Do you want to stay up to speed with all the latest updates regarding DIAS? Subscribe to our newsletter📧 here -> dias-project.com/contact-us #H2020 #InvestEU 🇪🇺 🌱

DIAS DIAS project @DIAS_project · Feb 17
 The 2nd DIAS Hackathon (Hack-a-Truck! part 2) is planned for week 13 (28th March-1st of April) 2022, apply now! More details: dias-project.com/Hack-a-Truck #H2020 #InvestEU 🇪🇺



DIAS DIAS project @DIAS_project · Apr 8
 The Hack-A-Truck#2 (30-31/3) was the first physical hacking event organized by DIAS. Judging by the results (and the smiling faces), it went great! A huge thank you to all the participants for the great insights and invaluable feedback they offered. 🇪🇺 #H2020 #InvestEU



DIAS DIAS project @DIAS_project · Oct 16
 The Final Dissemination Event of the DIAS project will take place on Tuesday 25th of October, 2022. The target is to present and discuss the project's results and proposals. Anyone interested can register and join remotely: dias-project.com/Publicity/Even... #H2020 #InvestEU #CINEA_EU



Figure 5: Top tweets from 3rd year of the project (November 2021 to October 2022)

More details about DIAS' twitter presence from November 2019 to October 2022 can be found in the following table and given graphs:

Table 4: Analytics of DIAS Twitter account (Note: updates compared to the previous dissemination report are in blue font)

Month	Tweets	Impressions	Profile Visits	New Followers	Mentions
Nov. 2019	0	0	0	0	0
Dec. 2019	2	667	0	13	0
Jan. 2020	0	103	0	3	0
Feb. 2020	0	56	14	2	0
Mar. 2020	0	27	3	0	0
Apr. 2020	0	240	69	5	1
May. 2020	1	208	24	1	0
Jun. 2020	1	689	57	0	0
Jul. 2020	0	241	10	2	0
Aug. 2020	0	110	4	0	0
Sept. 2020	1	363	20	2	1
Oct. 2020	1	424	28	2	0
Nov. 2020	3	1066	145	6	0
Dec. 2020	0	765	99	1	1
Jan. 2021	0	306	30	2	0
Feb. 2021	0	363	80	3	0
Mar. 2021	2	550	288	1	0
Apr. 2021	0	542	251	2	0
May. 2021	0	437	93	2	0
Jun. 2021	1	45100	855	12	3
Jul. 2021	0	186	295	0	0
Aug. 2021	0	228	114	1	0
Sept. 2021	1	368	983	1	0
Oct. 2021	0	172	1137	0	0
Nov. 2021	1	232	598	0	0
Dec. 2021	1	166	485	1	0
Jan. 2022	1	348	566	1	0
Feb. 2022	3	24200	2155	5	1
Mar. 2022	3	643	501	0	0
Apr. 2022	2	1210	1849	4	0
May. 2022	0	370	340	1	0
Jun. 2022	1	299	110	0	1
Jul. 2022	0	75	69	1	0
Aug. 2022	0	47	91	0	0
Sept. 2022	0	43	333	0	0
Oct. 2022	2	406	1121	0	0

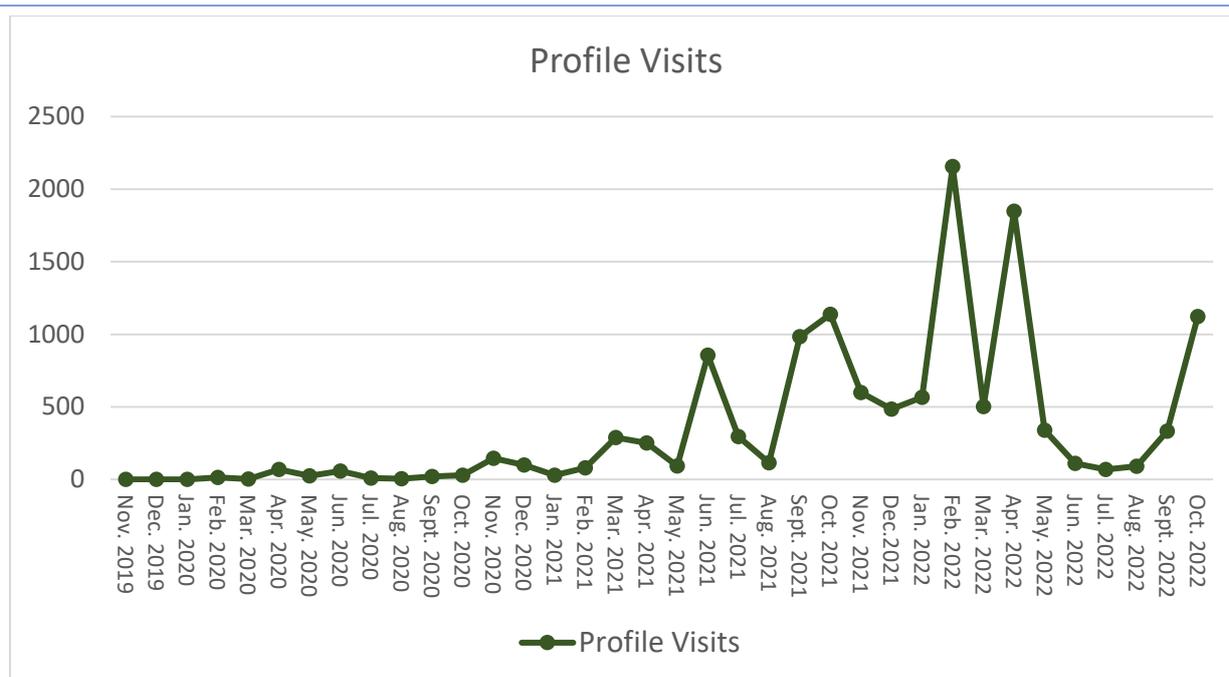


Figure 6: Visits in DIAS Twitter account

3.3 Communication Material

To spread the message and results of the DIAS project, we have developed different types of materials considering accessibility requirements that have been used on different scenarios such as website, social media and events. Since the last dissemination report (February 2022), communication material has been greatly extended including:

- 2 new leaflets
- 2 newsletters
- 1 2-pager
- 2 videos
- 1 dissemination pack

3.3.1 Project Templates: PPT, Word

DIAS-specific templates have been created and used for all communication activities.

3.3.2 Leaflets

A project leaflet was disseminated including basic information about the project objectives and expected outcomes. Additionally, achievements so far are distributed mainly including figures and a short summary of publicly available DIAS deliverables. Strong attention has been given also to the design (graphics etc) of the Leaflet to keep it simple, attractive, and professional (Figure 7).

Additional leaflets were created for the 1st and the 2nd Hackathon events (Figure 8 and Figure 9 correspondingly). These leaflets aimed to inform the public and attract potential participants for the Hackathon events. To fulfil this target, the basic structure followed included:

- Short introductory note for what is the DIAS project about
- Description of the hackathon event and its basic goals
- Preferable skills required from participants

- Motivations for participants to apply e.g. educational knowledge gain (combined with relevant certification of attendance), financial and other awards, etc.
- Friendly and simplified instructions for participants' application

Overview

→ Environmental protection systems are under threat
Environmental protection systems (EPS) play a vital role in reducing harmful vehicle emissions. However, there is increasing clear evidence of illegal manipulation of these systems by vehicle owners: a situation made possible by the fact that current on-board diagnostic systems (OBD) are not intended to detect extended malicious interventions to vehicle systems.

→ Key leaders are addressing tampering head on
DIAS combines leaders in industry, academia and regulatory authorities to research, develop and test multiple systems with the ability to eradicate tampering.

→ A thorough two-level plan to stamp out tampering
DIAS starts with current OBD and follows a two-level approach. The first level is the development of an enhanced OBD system, assessing its resistance to tampering and creating intermediate regulatory guidelines. The second level will be the development of more advanced cloud-based diagnostics systems involving two-way communication that foresees swift tampering detection.

Call: H2020-MG-2018-TwoStages

DIAS involves the major players and stakeholders from the main scientific, technical and logistical domains

CONTACTS

Coordination
Prof. Zisis Samaras
Tel: +302310.996014
E-mail: [zisis\(at\)auth.gr](mailto:zisis(at)auth.gr)

Project Management
Mrs. Georgia Parpori
Tel: +302310.996082
E-mail: [gparpori\(at\)auth.gr](mailto:gparpori(at)auth.gr)

Postal address
Lab of Applied Thermodynamics,
Dept of Mechanical Engineering,
Aristotle University,
University Campus 54124
Thessaloniki, Greece

The DIAS project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 814951.

Disclaimer
This document reflects the views of the author(s) and does not necessarily reflect the views or policy of the European Commission. Whilst efforts have been made to ensure the accuracy and completeness of this document, the DIAS consortium shall not be liable for any errors or omissions, however caused.

Call: H2020-MG-2018-TwoStages

DIAGNOSTIC ANTI-TAMPERING SYSTEMS

Research and development of smart multi-layered solutions to secure vehicle environmental protection systems from tampering

Objectives

The primary target of DIAS is to harden vehicle environmental protection systems (EPS) against tampering. This means that any changes in hardware or software that degrade the performance of the EPS will be prevented or detected. In the case of detection the tampering information becomes available and is used to introduce countermeasures such as the activation of the driver inducement system.

This target is broken down into four main objectives as follows:

- I. "Market" analysis and assessment of the operation of representative tampering systems and of their effect on the performance of existing on-board emission monitoring and emission control systems over real-world and laboratory testing
- II. Detection methods and counter-measures are identified and implemented (in vehicles)
- III. Testing and demonstration of the success of measures
- IV. Setup of guidelines and recommendations for future legislation for the introduction of future safe monitoring systems

Achievements so far

Market of tampering analysis

- Overview of environmental protection systems affected by tampering and the main motivations to tamper.
- Overview of environmental protection systems present on current (latest) vehicles, for what engines and in what vehicle category the environmental protection systems are used and the pollutants that are affected
- Overview of tampering devices and services per environmental protection system applicable for the latest emission regulation step (Euro 6/VI) and environmental protection systems that may appear on the market more frequently in the near future
- Draft test matrix. Proposed combinations of vehicles, tampering target and type of tampering to be tested.
- List of tampering providers and devices

Overview of system vulnerabilities, attack surfaces and tampering methods

EPS	SCR	EGR	DPF	TWC
Vulnerability	Emulate/modify signal	Change ECU maps	Clear DTC's	
Attack surface	CAN/OBD/UDS protocols	ECU	Digital sensor	Analogue sensor
Tampering method	Emulator/modifier	ECU reflashing	DTC cleaning	

Testing of tampering devices (example: On-road test with a truck)

In-vehicle security architecture and security components

Intrusion detection system architecture

Figure 7: DIAS 1st leaflet

DIAS
DIAGNOSTIC AND TAMPERING SYSTEMS

Hack-a-Truck! WEB EVENT

Malicious tampering of environmental protection systems turns very clean vehicles into heavy polluters. In the European project DIAS, countermeasures are developed to harden vehicles against malicious tampering and this needs to be thoroughly tested.

That is why we invite creative, ingenious people to hunt for bugs. A hackathon is organized where you will cooperate in teams containing people with various skills to work out a virtual plan, from finding a bug to making a business out of it.

Event description

Hack-a-Truck is an online automotive hackathon which lasts two days in total. To get you up to speed, three trainings will be hosted by experts from industry-leading companies and knowledge institutes, such as Ford Otosan, Bosch and TNO. The experts will inform you about the latest and the greatest new environmental protection systems, ECU and communication systems, tampering methods and the newly developed state-of-the-art countermeasures. In between these trainings, we invite you to some action: you will be assigned to a group of people with complementary skills and you will work together on finding bugs in a defined truck set-up. Together, you'll have to work out a business plan as if you were to commercially sell your bug as tampering on the internet. Other groups are your competition. Beat them and get rewarded.

Profile of participants

You are currently following or you have completed one of the following bachelor studies:

- Mechanical engineering
- Automotive engineering
- Computer science
- Electrical engineering

You should have an interest in and preferably experience with exhaust gas aftertreatment systems, (automotive) electronics, and/or (automotive) communication and security protocols.

Your communication skills in English are excellent.

You should bring expertise and skills to your team during the Hack-a-Truck.

Our offer

- Three trainings, hosted by experts from industry-leading companies and knowledge institutes.
- You will be assigned to form a group of 5 selected participants with complementary skills, 1 mentor and 1 professional hacker. You will work together on finding bugs in a defined truck set-up. Together you'll have to work out a technical plan and a business plan as if you were to find a bug and commercially sell your bug as a tampering 'product' on the internet.
- The winning team receives 2000 €, the second team 1000 €, the third team 500 € (to be divided between the 5 selected participants only).
- A certificate of being a laureate to the DIAS Hack-a-Truck 2021.
- An exclusive goodie package before the start of the event.

Application

The Hack-a-Truck is planned for week 20 (17-21 of May). Final dates will be announced soon.

To apply for this event, please enter your motivation letter and CV via the application form below before April 08th, 2021.

Apply now!

The selection procedure will be finished before the end of April 2021. If you are selected, you will be asked to sign an NDA.

For additional information and updates visit our [website](#) or send an e-mail to info@dias-project.com.

DIAS Call: H2020-MG-2018-TwoStages

The DIAS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 814951

Figure 8: DIAS Hackathon part 1 leaflet

DIAS
DIAGNOSTIC AND TAMPERING SYSTEMS

Hack-a-Truck! PART 2

Malicious tampering of environmental protection systems turns very clean vehicles into heavy polluters. In the European project DIAS, countermeasures are developed to harden vehicles against malicious tampering and this needs to be thoroughly tested. That is why we invite creative, ingenious and skilled people to hunt for bugs. A hacking event is organized where participants will put the new and improved security features to the test!

Event description

In the first Hack-a-Truck event held in May 2021, the onboard countermeasures for tampering detection and prevention of the vehicle were tested. New features for tampering prevention and detection have been added since May 2021. Hack-a-Truck part 2 revolves around a new system that reports information about a possible tampering suspicion wirelessly to a cloud or a supervising entity, to enable fast and easy detection and reporting of tampering of connected vehicles.

The goal is to find possible vulnerabilities which allow tampering while remaining undetected

Hack-a-Truck part 2 (H#2) is an automotive hacking event that lasts two days. Experts from the field, such as Bosch, FEV and UMFST, will inform you about the latest environmental protection systems and the newly developed state-of-the-art countermeasures. During the physical event held in the Netherlands, you will work on one of the two variants of the testbeds, one on the in-vehicle communication of control units and one on the wireless communication between the in-vehicle control units and the cloud, as well as participate in a central session discussing the tampering reporting system as a whole. You will be assigned to find vulnerabilities in a group setting and there will be time during the event to ask questions and have discussions with experts from the DIAS project consortium. We expect a presentation from the participants where the hacking approach is explained – this gives each participant the opportunity to challenge their own approach and get new insights.

The challenge

Both testbeds are Raspberry Pi based setups, with added encryption. These testbeds involve:

- (man-in-the-middle attacks on) CAN-bus and Autosar SecOC
- HTTP and SSL

If you can hack one (or both) of these challenges and if you have excellent English communication skills, then please do apply!

If you choose to accept this challenge, we offer you:

- A two-day physical hacking event in the Netherlands. Your costs for travel and stay will be compensated, including a fixed daily wage.
- Training sessions on the latest environmental protection systems and the newly developed state-of-the-art countermeasures.
- During the two days you will work together in small groups with other participants on finding vulnerabilities in the system.
- Access to a pool of experts from amongst others Bosch, FEV and UMFST during the event.
- A certificate of joining the DIAS Hack-a-Truck part 2 hacking event.

Application

Hack-a-Truck part 2 is planned for week 13 (28th March until 1st of April). Final dates will be announced soon.

To apply for this event, please send your motivation letter and CV to projectoffice@tno.nl via the button below before February 28th, 2022.

Apply now!

The selection procedure will be finished before the end of week 9 (6th of March). If you are selected, you will be asked to sign an NDA.

For additional information and updates visit our [website](#) or send an e-mail to info@dias-project.com.

DIAS Call: H2020-MG-2018-TwoStages

The DIAS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 814951

Figure 9: DIAS Hackathon part 2 leaflet

3.3.3 Newsletter

Similarly to the other communication material targeting the public audience, the newsletter needed the appropriate lead time to collect enough published project outcomes, since most of the findings during the first period of the project were confidential. This need was even more vital in the newsletter's development targeting to give valuable insight into the project's targets, achievements, and expected impact. Thus, more details from the published DIAS deliverables were included. Finally, the newsletter's material was the basis for the journalistic description of the project and the leaflet.

Two newsletters have been published till the end of the project. The newsletters are available on our website: <https://www.dias-project.com/newsletter>.

The 1st DIAS newsletter (Figure 10) was published in February of 2022 and it is structured as follows:

- Co-ordinator's editorial attempting a journalistic description of the project understandable for the public including: the significance of the tampering issue, where we are at in the project, how confident we are that we can prevent hacking and what is coming up in the next few months and how we expect legislation to be affected.
- The story so far that includes the summary of the latest (till February of 2022) public deliverables (D3.4, D4.3, D5.2)
- The summary for the 1st "Hack-A-Truck" event
- A short session dedicated to the partners (Bosch and FEV are included in this newsletter)
- An "Internet search challenge" that aims at public awareness of the tampering issue and the risks attributed to a tampering attempt



Figure 10: Cover page of the first DIAS newsletter (February 2022)

A similar structure was also followed for the 2nd DIAS newsletter (Figure 11) published in October of 2022 while the content was updated based on the latest DIAS findings and events. In short, the 2nd newsletter comprises:

- Co-ordinator's editorial setting and answering the questions mainly addressed in the last 8 months of the project regarding the commercialization of DIAS anti-tampering solutions

- The story so far focusing on the latest progress regarding the prototyping and testing of the DIAS anti-tampering solutions both on desktop test setups but also on the demonstrator vehicle
- The summary for the 2nd “Hack-A-Truck” event
- A short session dedicated to the partners (LAT AUTH and TNO are included in this newsletter)
- An “Internet search challenge” that aims at public awareness of the tampering issue (emphasis on ECU flashing is given in this newsletter)
- A reminder and a relevant link with respect to the Final Dissemination Event of the DIAS project taking place on Tuesday 25th of October 2022



Figure 11: Cover page of the second DIAS newsletter (October 2022)

3.3.4 2-pager and journalistic project description

A 2-pager which summarises the entire project was created (<https://dias-project.com/publicity/2-pager>). The target was to create:

- a summary of the context and overall objectives of the project
- an overview of the work performed and the key results
- a summary of the impact expected by the project

The initially planned journalistic project description was replaced by an extended video (3.3.5).

3.3.5 Videos

Since the previous dissemination report, a significant working effort was given to the creation of a film highlighting the DIAS project’s main targets and findings. Originally, the DIAS project film was planned to be 3-5 minutes long and to be published 1 year or 6 months before the end of the project. However, it was shown that it was practically infeasible to create a 5-minute long video without “cherry-picking”

only a part of the main findings of DIAS project. Furthermore, great progress towards the DIAS pre-set basic objectives was achieved in the last year of the project. Incorporating these achievements would better represent and give a more spherical view of the work done in DIAS. Contrariwise, there was communication material already disseminated that briefly presented the progress made during the first 2 years of the project (e.g. project leaflet). Therefore, the originally planned video would not have a lot to add. To overcome these limitations, a 20-minute long film was created representing the effort made during the whole DIAS project period and published through the DIAS project channel on YouTube on 17th of October 2022 (available at <https://www.youtube.com/watch?v=3u6-Oy0Wazo>, a screenshot can be seen in Figure 12).

The higher duration adopted allowed for more information and presentation of demonstrators. Technical details included were limited to ensure the film is understandable to any kind of audience. The film summarises the project's basic structural elements and findings, and incorporates interviews with DIAS staff to support its findings (e.g. how DIAS solutions work and how effective they will be). In this way, it places the role of the journalistic project description (3.3.4). In summary, the following topics are covered:

- Introduction to the problem:
 - Climate change and environmental degradation threat to Europe and the world
 - Targeting a toxic-free environment and accelerating the shift to sustainable and smart mobility
 - How significant is tampering with vehicles' EPS?
 - Who is tampering and why?
 - What is the DIAS approach?
- Which is the market of tampering? What are some examples of tampering devices and how do they work?
- What are the steps towards finding solutions?
- How has the DIAS project dealt with the multiple attack strategies?
- Which are the critical security categories and what corresponding solutions have been developed?
- With the Cloud becoming a standard data storage and processing location, what is the DIAS approach to the Cloud?
- What additional testing was conducted on the developed solutions?
- What is the contribution of hackathon events?
- What is the commercial viability of DIAS solutions?
- How will DIAS impact legislation?
- Closing remarks:
 - Is tampering a problem only for current vehicles?
 - The DIAS consortium
 - Link for DIAS website
 - Acknowledgements to the funders (i.e. European Union's Horizon 2020 research and innovation programme)

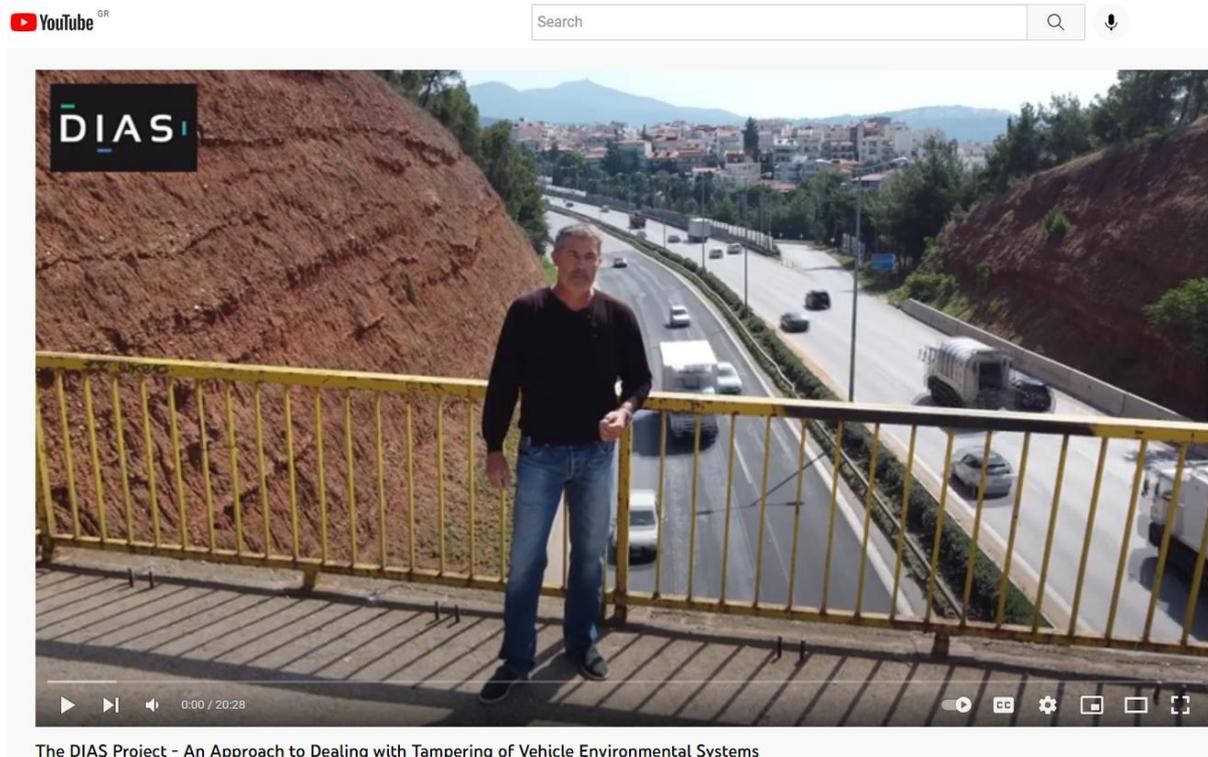


Figure 12: DIAS project film

In the context of DIAS task 5.4², the viability of DIAS solutions for vehicle anti-tampering was demonstrated through their integration into a commercial vehicle (i.e. demonstrator truck provided by Ford Otosan). A reference to this activity is included in the project's film but, to better support and disseminate it, another video has been created and made available to the public (available at <https://www.youtube.com/watch?v=m5zxeOzfKqg>, a relative screenshot can be seen in Figure 13).

²T5.4: Implementation of the chain containing ECU, CCU and Cloud and relevant products developed in other WPs into the demonstration vehicle



Figure 13: DIAS demonstrator truck video

3.3.6 Fact sheet

A project fact sheet was originally planned to summarize all key project details. Ultimately, this was covered via the 20-minute-long project film described in section 3.3.5.

3.3.7 Dissemination pack

To present in an aggregated and, at the same time, friendly form the project outcomes, a final dissemination event was held on the 25th of October 2022. During this event, representatives from the industry, academic and research community, and the general public got informed about project findings and submitted and discussed their queries with DIAS consortium leading members along with representatives from synergistic EU projects (i.e. CARES, MODALES, and uCARE). The corresponding presentations were finally all concentrated to form a project dissemination pack and published via the DIAS website (available at [https://dias-project.com/Publicity/Events/Final Dissemination Event](https://dias-project.com/Publicity/Events/Final_Dissemination_Event)).

3.4 Events (Conferences, exhibitions, presentations, etc)

Participation in different types of events has been essential for raising awareness and visibility of the project among external stakeholders. Participation in events was promoted through the website and social media channels. Until now, DIAS and its consortium have participated in 18 events and 16 presentations have been made in total. Note that the DIAS project was intended to participate in Transport Research Arena 2020 (Helsinki, Finland) which has been cancelled. 3 special events (two hackathons and a final dissemination event) were organised by the project.

The table below includes information about the events or conferences that DIAS has already participated in or organised:

Table 5: Events (Note: updates compared to the previous dissemination report are in blue font)

Event	Date	Place	Partner	Target audience	Participants	Link	Note
IFIP Networking Conference 2020	22-26/06/2020	Paris, France (virtual conference)	UMFST	Industry, Research and Academic Community	Unknown (Web-event)	https://ieeexplore.ieee.org/xpl/conhome/9139123/proceeding	Presentation
IEEE International Conference on Intelligent Computer Communication and Processing (ICCP) 2020	03-05/09/2020	Cluj-Napoca, Romania	UMFST	Industry, Research and Academic Community	Unknown (Web-event)	https://iccp.ro/iccp2020/	Presentation
15 th International Conference on Availability, Reliability and Security	20-28/08/2021	New York, USA	UMFST	Industry, Research and Academic Community	Unknown (Web-event)	https://dl.acm.org/doi/proceedings/10.1145/3407023	Presentation
11 th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)	28-31/10/2020	New York, USA	JRC	Industry, Research and Academic Community	Unknown (Web-event)	https://ieeexplore.ieee.org/xpl/conhome/9297925/proceeding	Presentation
IEEE International Conference on Blockchain (Blockchain) 2020	02-06/11/2020	Rhodes, Greece	CERTH	Industry, Research and Academic Community	Unknown (Web-event)	https://ieeexplore.ieee.org/xpl/conhome/9284404/proceeding	Presentation
PEMS 10 th Annual Conference	11-12/03/2021	Virtual conference	LAT/AUTH	Industry, Research and Academic Community	Unknown (Web-event)	https://www.cert.ucr.edu/pems	Presentation
DIAS Hackathon 1 (Hack-a-Truck part 1)	19 and 21/05/2021	web event	TNO	Research and Academic Community	-25 participants (5 teams) -3 technical trainings + Q&A	https://dias-project.com/Hack-a-Truck-part-1	(*)

					-2 brainstorm sessions to collect all possible attack vectors and select the most promising one(s)		
Eclipse SAAM Mobility Conference 2021	15-16/06/2021	Virtual conference	BOSCH	Industry, Research and Academic Community	Unknown (Web-event)	https://www.eclipse.org/kuksa/blog/2021/06/24/2021-06-24-eclipsesaam-scr-anti-tampering/	Presentation
IEEE 45 th Annual Computers Conference	12-16/07/2021	Virtual conference	CERTH	Industry, Research and Academic Community	Unknown (Web-event)	https://ieeexplore.ieee.org/document/9529366	Presentation
European Interdisciplinary Cybersecurity Conference (EICC) 2021	10-11/11/2021	Virtual conference	FEV	Industry, Research and Academic Community	Unknown (Web-event)	https://dl.acm.org/doi/proceedings/10.1145/3487405	Poster
			UMFST			https://dl.acm.org/doi/abs/10.1145/3487405.3487650	Presentation
15 th International Conference Interdisciplinarity in Engineering	7-8/10/2021	Virtual conference	UMFST	Industry, Research and Academic Community	Unknown (Web-event)	https://link.springer.com/chapter/10.1007/978-3-030-93817-8_71	Presentation
5 th European Conference on results from road transport R&I in H2020 projects	29-30/03/2022	Brussels, Belgium	LAT/AUTH	Industry, Research and Academic Community, Public	300	https://www.2zeroemission.eu/event/h2020rtr21-5th-edition/	Presentation
DIAS Hackathon 2 (Hack-a-Truck part 2)	30-31/03/2022	Rotterdam, Netherlands	TNO	Research and Academic Community	-15 participants (4 teams) -Online information session about DIAS level 2 countermeasures in advance of the event -Level 2 countermeasures integrated and hacked into two separate test beds	https://dias-project.com/Hack-a-Truck-part-2	(*)

IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) 2022	6-10/06/2022	Virtual conference	UMFST, LAT/AUTH	Industry, Research and Academic Community	Unknown (Web-event)	https://ieeexplore.ieee.org/xpl/conhome/9799286/proceeding	Presentation
OBD 2022 (Americas)	13-15/09/2022	Garden Grove, CA	LAT/AUTH	Industry, Research and Academic Community	Unknown (Web-event)	https://www.sae.org/attend/obd-na/2022	Presentation
ERMES Plenary 2022	11-12/10/2022	Web event	LAT/AUTH	Research and Academic Community	Unknown (Web-event)	https://ermes-group.eu/ermes-plenary-2022-draft-agenda-11-12-october-2022	Presentation
Transport Research Arena (TRA) Conference 2022	14-17/11/2022	Lisbon, Portugal	LAT/AUTH, TNO	Industry, Research and Academic Community, Public	Unknown	https://dias-project.com/publicity/publications/TRA2022	Poster and presentation
DIAS Final dissemination event	25/10/2022	Brussels, Belgium (hybrid event)	LAT/AUTH	Industry, Research and Academic Community, Public	Hybrid event (on-site participation only for the speakers and the consortium members and publicly available remote participation)	https://dias-project.com/Publicity/Events/Final_Dissemination_Event	Presentation and discussion of the project's results, achievements and proposals with high-level experts and speakers

(*)The participants were informed by the experts about the latest and the greatest new environmental protection systems, ECU and communication systems, tampering methods and the newly developed state-of-the-art countermeasures by the DIAS consortium. In between these training, the participants were assigned to a group of people with complementary skills and worked together on finding attack vectors in pre-defined test beds (e.g. truck set-up). Together, they worked out a business plan as if they were to commercialize the tampering product on the EU market. Via hackathon part 1 DIAS level 0 and 1 anti-tampering solutions were demonstrated, while hackathon part 2 dealt with DIAS level 2 solutions.

3.5 Publications

Overall, the consortium has published 22 papers (Table 6) along with 17 (full-text available) deliverables (Table 7) which can be found on the DIAS website (at <https://dias-project.com/dias-publications> and https://dias-project.com/Deliverables/All_WPs accordingly).

Table 6: Papers (Note: updates compared to the previous dissemination report are in blue font)

Partners	No.	Type	Title	Authors	Title of the Journal/Proc./Book	DOI or Repository link
LAT/BOSCH/FEV/TNO	1	Publication in Conference proceedings	Next generation of vehicle diagnostics based on advanced onboard monitoring and cloud-based diagnostics	Savas Geivanidis, Zissis Samaras, Markus Willimowski, Ian Faye, Obaid UrRehman, Christof Schernus, Robin Vermeulen	Proceedings of 2020 8 th Transport Research Arena TRA	http://lat.eng.auth.gr/share/publications/TRA2020_953_Geivanidis.pdf
UMFST	2	Publication in Conference proceedings	MixCAN: Mixed and Backward-Compatible Data Authentication Scheme for Controller Area Networks	T. Lenard, R. Bolboaca, B. Genge, P. Haller	Proceedings of the 2020 IFIP Networking Conference	https://dl.ifip.org/db/conf/networking/networking2020/1570620040.pdf
UMFST	3	Publication in Conference proceedings	Locality sensitive hashing for tampering detection in automotive systems	R. Bolboaca, T. Lenard, , B. Genge, P. Haller	Proceedings of the 2020 15th International Conference on Availability, Reliability and Security	https://doi.org/10.1145/3407023.3409206
UMFST	4	Article in Journal	Anomaly Detection in Aging Industrial Internet of Things	B. Genge, P. Haller, C. Enachescu	IEEE Access Journal	https://doi.org/10.1109/ACCESS.2019.2920699
UMFST	5	Publication in Conference proceedings	LOKI: A Lightweight Cryptographic Key Distribution Protocol for Controller Area Networks	T. Lenard, R. Bolboacă and B. Genge	2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP)	https://doi.org/10.1109/ICCP51029.2020.9266192
CERTH	6	Publication in Conference proceedings/ Workshop	Securing Emission Data of Smart Vehicles with Blockchain and Self-Sovereign Identities	S. Terzi, C. Savvaidis, K. Votis, D. Tzovaras and I. Stamelos	2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2020	https://doi.org/10.1109/Blockchain50366.2020.00067
JRC	7	Article in Journal	On the application of entropy measures with sliding window for intrusion detection in automotive in-vehicle networks	G. Baldini	Entropy Journal	https://doi.org/10.3390/e22091044

JRC	8	Publication in Conference proceedings	Mitigation of Odometer Fraud for In-Vehicle Security Using the Discrete Hartley Transform	Baldini, G., Giuliani, R., & Gemo	2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)	https://doi.org/10.1109/UEMCON51285.2020.9298039
BOSCH	9	Publication in Conference proceedings	Eclipse KUKSA.val for SCR Anti-Tampering Monitoring in Heavy Vehicles	Junhyung Ki, Sebastian Schildt, Andreas Hastall, Sven Erik Jeroschewski and Robert Höttger	Proceeding of the 2021 Eclipse SAAM Mobility Conference	https://dias-project.com/sites/default/files/2021-12/9.%20Eclipse%20KUKSA.val%20for%20SCR%20Anti-Tampering%20Monitoring%20in%20Heavy%20Vehicles%20-%20Bosch.pdf
FEV	10	Poster in Conference proceedings	Key Exchange and Management Schemes for Automotive Control Units	Miao Zhang, Shaoning Chen, Barbara Graziano	Proceeding of the 2021 European Interdisciplinary Cybersecurity Conference (EICC)	https://doi.org/10.1145/3487405.3487658
UMFST, JRC	11	Article in Journal	VetaDetect: Vehicle Tampering Detection with Closed-Loop Model ensemble	Piroska Haller, Bela Genge, Fabrizio Forloni, Gianmarco Baldini, Massimo Carriero, Georgios Fontaras	International Journal of Critical Infrastructure Protection	https://doi.org/10.1016/j.ijci.2022.100525
UMFST	12	Publication in Conference proceedings	A Statefull Firewall and Intrusion Detection System Enforced with Secure Logging for Controller Area Network	T. Lenard and R. Bolboacă	Proceeding of the 2021 European Interdisciplinary Cybersecurity Conference (EICC)	https://doi.org/10.1145/3487405.3487650
CERTH	13	Publication in Conference proceedings	Decentralizing Identity Management and Vehicle Rights Delegation through Self-Sovereign Identities and Blockchain	S. Terzi, C. Savvaïdis, A. Sersemis, K. Votis and D. Tzovaras	Proceedings of the 2021 IEEE 45th Annual Computers	https://ieeexplore.ieee.org/document/9529366
UMFST	14	Article in Journal	Privacy-Preserving Tampering Detection in Automotive Systems	A.-S Roman, B. Genge, A.-V. Duka, P Haller	Electronics Journal	https://www.mdpi.com/journal/electronics

UMFST	15	Publication in Conference proceedings	Cryptographic Key Distribution Protocol with Trusted Platform Module for Securing In-vehicle Communications	B. Genge, P. Haller	Proceedings of the 15th International Conference Interdisciplinarity in Engineering	https://link.springer.com/chapter/10.1007/978-3-030-93817-8_71
LAT/AUTH	16	Publication in Conference proceedings	DIAS-Smart Adaptive Remote Diagnostic Antitampering Systems	Dimitrios Kontses, Zissis Samaras	European conference on results from road transport R&I in H2020 projects	https://www.2zeroemission.eu/event/h2020rtr21-5th-edition/
LAT/AUTH	17	Publication in Conference proceedings	Tampering of Emission Controls and Countermeasures	Dimitrios Kontses, Zissis Samaras	SAE On-Board Diagnostics Symposium-Americas 2022	https://dias-project.com/publicity/publications/SAE2022
LAT/AUTH	18	Publication in Conference proceedings	Tampering of Emission Controls and Countermeasures-Emission Rates and Vehicle Shares	Dimitrios Kontses, Zissis Samaras	European Research for Mobile Emission Sources (ERMES) Plenary 2022	https://dias-project.com/publicity/publications/ERMES2022
LAT/AUTH, TNO	19	Publication and poster in Conference proceedings	Tampering of environmental protection systems on vehicles: Status quo and perspectives	Dimitrios Kontses, Robin Vermeulen, Pavlos Fragkiadoulakis, Zissis Samaras	Transport Research Arena (TRA) 2022	https://dias-project.com/publicity/publications/TRA2022
JRC, TNO, LAT/AUTH	20	Article in Journal	Effect of Tampering on On-Road and Off-Road Diesel Vehicle Emissions	Giechaskiel B, Forloni F, Carriero M, Baldini G, Castellano P, Vermeulen R, Kontses D, Fragkiadoulakis P, Samaras Z, Fontaras G.	Sustainability Journal	https://doi.org/10.3390/su14106065
UMFST, LAT/AUTH	21	Publication in Conference proceedings	Tampering Detection for Automotive Exhaust Aftertreatment Systems using Long Short-Term Memory Predictive Networks	Roland Bolboacă, Piroska Haller, Dimitris Kontses, Alexandros Papageorgiou-Koutoulas, Stylianos Doulgeris, Nikolaos Zingopis, Zissis Samaras	2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)	https://doi.org/10.1109/EuroSPW55150.2022.00043
UMFST	22	Article in Journal	Adaptive Ensemble Methods for Tampering Detection in Automotive Aftertreatment Systems	Roland Bolboacă	IEEE Internet of Things Journal	https://doi.org/10.1109/ACCSS.2022.3211387

Table 7: Public DIAS deliverables (Note: updates compared to the previous dissemination report are in blue font)

WP No	Del Rel. No	Title	Lead Beneficiary	Repository link in DIAS website
WP1	D1.1	DIAS Project Handbook - inception version	LAT/AUTH	https://www.dias-project.com/sites/default/files/Deliverables/D1.1-Handbook%20v2.pdf
WP1	D1.2	DIAS Project Handbook - final version	LAT/AUTH	https://dias-project.com/sites/default/files/DIAS-D1.2_v1.0.pdf
WP3	D3.1	The market of cheating devices and testing matrix with a prioritization for testing of vehicle tampering technique combinations	TNO	https://www.dias-project.com/sites/default/files/Deliverables/D3.1-Cheating%20devices%20and%20testing%20matrix_0.pdf
WP3	D3.2	Status quo of critical tampering techniques and proposal of required new OBD monitoring functions	TNO	https://dias-project.com/sites/default/files/Deliverables/D3.2%20-%20Status%20quo%20of%20critical%20tampering%20techniques%20and%20proposal%20of%20required%20new%20OBD%20monitoring%20functions.pdf
WP3	D3.3	Anti-tampering test protocol for use in future type approval test	TNO	https://dias-project.com/sites/default/files/DIAS-D3.3_v1.0.pdf
WP3	D3.4	Summary of the hackathon and security and resilience evaluation of the level 1 concept	TNO	https://dias-project.com/sites/default/files/2021-11/D3.4%20Outcome%20of%20the%20evaluation%20with%20the%20CE%97ackathon.pdf
WP3	D3.5	Summary of the hackathon and security and resilience evaluation of the level 2 concept	TNO	https://dias-project.com/sites/default/files/DIAS-D3.5v1.0.pdf
WP4	D4.2	In-vehicular antitampering security techniques and integration	UMFST	https://dias-project.com/sites/default/files/D4.2%20In-vehicular%20antitampering%20security%20techniques%20and%20integration.pdf
WP4	D4.3	Blockchain and cloud-based methods for provision of certified data	BOSCH-IoT	https://dias-project.com/sites/default/files/Deliverables/DIAS-D4.3_v1.0.pdf
WP4	D4.4	Validation and verification methodology and results	FEV	https://dias-project.com/sites/default/files/DIAS-D4.4_v1.0.pdf
WP5	D5.3	Advanced detection system against unknown (future) tampering (Level 2)	UMFST	https://dias-project.com/sites/default/files/DIAS-D5.3_v1.0.pdf
WP5	D5.4	DIAS antitampering system demonstration	BOSCH	https://dias-project.com/sites/default/files/DIAS-D5.4_v1.0.pdf
WP6	D6.1	Website of the project	LAT/AUTH	https://www.dias-project.com/sites/default/files/Deliverables/DIAS%20D6.1%20DIAS%20website_final%20version%20(v1.0).pdf
WP6	D6.2	Dissemination and Exploitation plan	LAT/AUTH	https://dias-project.com/sites/default/files/D6.2%20-%20DIAS%20-%20Executive%20summary.pdf

WP6	D6.3	Dissemination report (mid-term)	LAT/AUTH	https://dias-project.com/sites/default/files/DIAS_D6.3_v2.0%20(summary).pdf
WP6	D6.4	Dissemination report (final)	LAT/AUTH	https://dias-project.com/sites/default/files/DIAS-D6.4_v1.0.pdf
WP6	D6.5	Guidelines, impact assessments and text for future legislation	LAT/AUTH	https://dias-project.com/sites/default/files/DIAS-D6.5_v1.0.pdf

4 Conclusions

Several actions were taken during the whole period of the DIAS project to increase the awareness and visibility of the project outputs within the consortium and to external audiences. Due to Covid-19, a significant part of the actions were realized within a virtual context and therefore the dissemination and communication plan had to adapt to the new conditions.

The success of the strategy had been related to the ability to spread the word and communicate relevant messages to the automotive community. Based on the main targeted audiences, the most appropriate channels, tactics, and activities were implemented to keep them engaged and updated about project progress and the most relevant results.

In time-wise steps, the focus during the first year of the project was on raising awareness about the general project objectives, while, in the rest period, emphasis was given on disseminating the project achievements so far and the expected benefits of the project results.

Ultimately, these steps were successfully addressed via the following activities:

- A project website had been created and continuously updated with new content
- A variety of news and events have been posted on social media (i.e. Twitter)
- The project outcomes have been spread through the publication of 39 scientific publications and active participation (via presentation or poster) in 18 international events and conferences. 3 events were organised by the DIAS consortium including 2 hackathons to test and evaluate DIAS anti-tampering solutions, and one event near the end of the project to disseminate and discuss project outcomes with the industry, academic and general public beneficiaries. The final phase of the strategy focused on the achievement of the main milestones of the project such as the demonstrator vehicle equipped with enhanced tamper-proofing measures, software and electronic component security systems and the regulatory proposals made in a uniform and technology-neutral way.
- A significant amount of communication material had been utilized including:
 - DIAS logo and template for all document and slideshow material
 - 3 leaflets
 - 2 newsletters
 - 1 2-pager
 - 2 videos
 - 1 dissemination pack